Physical Layer Key Generation in 5G Wireless Networks

Long Jiao, Ning Wang, Pu Wang, Amir Alipour-Fanid, Jie Tang, and Kai Zeng

Abstract

The bloom of 5G communication and beyond serves as a catalyst for physical layer key generation techniques. In 5G communications systems, many challenges in traditional physical layer key generation schemes, such as co-located eavesdroppers, the high bit disagreement ratio, and high temporal correlation, could be overcome. This article lists the key enabling techniques in 5G wireless networks, which offer opportunities to address existing issues in physical layer key generation. We survey the existing key generation methods and introduce possible solutions for the existing issues. The new solutions include applying the high signal directionality in beamforming to resist co-located eavesdroppers, utilizing the sparsity of millimeter-wave channel to achieve a low bit disagreement ratio under low signal-to-noise ratio, and exploiting hybrid precoding to reduce the temporal correlation among measured samples. Finally, the future trends of physical layer key generation in 5G and beyond communications are discussed.

Introduction

Over the past few years, the fifth generation (5G) communication has come a long way, thanks to booming wireless technologies such as millimeter-wave (mmWave), massive multiple-input multiple-output (MIMO), highly directional beamforming, and hybrid precoding [1]. Compared to the current 4G network, 5G networks can satisfy the increasing demand by providing high data rate, ultra-reliable low latency, and massive machine-type communications. In the design of 5G networks, providing reliable and secure communication service is one of the top priorities. Specifically, in this article, we focus on one of the promising physical layer security mechanisms, physical layer key generation, and explore the benefits offered by the new technologies applied in 5G wireless networks.

Different from the traditional Diffie-Hellman (D-H) key exchange mechanism, physical layer key generation mechanisms do not require expensive computation and have the potential to achieve information-theoretic security [2]. That is, the secrecy of the generated key is not dependent on the hardness of a computational problem but relies on the physical laws of wireless fading channels. For instance, wireless devices measure highly correlated wireless channel characteristics and use them as shared random sources to generate a shared key [3]. In theory, in a rich multi-path scattering environment, a passive eavesdropper who is more than a half-wavelength away from legitimate users will obtain uncorrelated channel measurements, and thus cannot infer much information about the generated key.

Physical layer key generation has gained much attention in the literature [4]. Based on the number of antennas in the transceivers, physical layer key generation schemes under sub-6 GHz can be generally classified into two categories: single-antenna- and MIMO-based key generation. In single-antenna-based mechanisms, various channel characteristics have been proposed to generate the secret key, including received signal strength (RSS) [5], channel state information (CSI) [4], and angle of arrival (AoA)[6]. In MIMO-based mechanisms, the authors in [7] conducted an indoor MIMO measurement in the 2.51–2.59 GHz band and studied the number of available key bits in both line-of-sight (LoS) and non-line-of-sight (NLoS) environments. In [7], a theoretical upper bound for the maximum size of the generated secret key is derived based on the mutual information of channel estimates at the two legitimate nodes. But the number of antennas considered is still relatively small, and the carrier frequency is not as high as mmWave. Furthermore, all the theoretical analyses are based on the Gaussian channel assumption, which cannot be directly utilized in mmWave channels because of their unique scattering nature [8, 9].

Although significant efforts and progress on physical layer key generation have been made in recent years, many issues and challenges remain elusive. For example, most existing key generation schemes cannot combat the co-located eavesdropping in sub-6 GHz systems. That is, a common assumption that eavesdroppers locate at least a half a wavelength apart from legitimate users is required in most key generation schemes. Furthermore, some existing works have a high bit disagreement ratio in the low signal-to-noise ratio (SNR) regime, which leads to a high reconciliation overhead and low efficiency of key generation. In addition, a high probing rate is chosen to increase the key generation rate in most of the existing works; however, it leads to high temporal correlation among samples along with a large number of repeated quantization bits.

With unique features, 5G and beyond technologies may offer a better solution to the aforementioned issues or challenges remaining in existing

Digital Object Identifier:
10.1109/MWC.001.1900061

Long Jiao, Ning Wang, Amir Alipour-Fanid, Jie Tang, and Kai Zeng are with George Mason University. Pu Wang is with Xidian University.

1536-1284/19/$25.00 © 2019 IEEE

works. For instance, the high directionality enabled by massive MIMO-based beamforming is exploited in [10] to defend against co-located eavesdroppers in key generation. The authors also propose a scheme by utilizing the sparsity of mmWave channel to estimate virtual AoA and angle of departure (AoD) [6]. Due to the sparsity of mmWave channel, the scheme is anti-noise and can achieve a low bit disagreement ratio. Moreover, based on the fact that hybrid precoding can form mmWave beams with multiple resolutions, it can be adopted in the channel probing stage to reduce the temporal correlation among samples.

By identifying possible solutions and benefits offered by 5G communication technologies, the purpose of this article is to provide new insights about the physical key generation in 5G wireless networks, and this article is expected to advance and stimulate the corresponding research under the context of 5G and beyond communication systems. It should be noted that existing surveys and tutorial papers [4] on physical layer key generation mainly focus on sub-6 GHz systems. A comprehensive study of physical layer key generation in 5G wireless networks, identifying challenges and opportunities, is still lacking, which is the major contribution of this article.

In the following section, we introduce the basics of key generation and analyze limitations of existing works. Following that, the specific benefits and improvements accompanying 5G communication systems are discussed. Then we show the benefits of 5G communication technologies on physical layer key generation with three typical cases. Future trends and research topics are then discussed, while the conclusions are given in the final section.

Key Generation and Existing Issues

In this section, we review the typical key generation process and analyze the limitations of existing schemes. Here, two devices, denoted by Alice and Bob, wish to generate a common secret key based on channel measurements. To extract the secret key, Alice and Bob generally perform five steps: channel probing, randomness extraction, quantization, information reconciliation, and privacy amplification.

Typical Key Generation Process

Channel Probing: In this step, Alice and Bob exchange channel probing signals with each other to collect enough channel measurements as a shared random source. The channel measurements can be CSI, phase, or AoA and AoD. If the channel reciprocity holds, the received measurements at Alice and Bob are highly correlated.

Randomness Extraction: The received signals at Alice and Bob may contain deterministic parts that can be inferred by an attacker. Randomness extraction is adopted here to remove deterministic parts and extract randomness of the channel fading.

Quantization: This is used to quantize the random channel measurements into binary bits.

Information Reconciliation: Information reconciliation is a form of error correction carried out between Alice and Bob to ensure identical keys generated separately on both sides. The extracted bits at Alice's and Bob's sides after quantization are usually not identical due to imperfect reciprocity and measurement noise. During reconciliation, Alice and Bob exchange side information to correct errors, and a certain amount of bit information could be revealed to the eavesdropper.

Privacy Amplification: This step is used to eliminate the leaked bits during channel probing and reconciliation. After this step, the eavesdropper's partial information by observation will be largely reduced.

Limitations of Existing Schemes

Although there have already been various studies of physical layer key generation for sub-6 GHz systems, there remain several challenges and limitations for the existing key generation schemes in practice. We list three challenges that exist in previous works.

Co-Located Attacks: The correlation of channel measurements is determined by the distance between the eavesdropper and Alice/Bob. In the existing works [3, 4], if the eavesdropper is co-located with Alice or Bob, he/she will observe channel measurements that are highly correlated with Alice or Bob. Therefore, most existing works are vulnerable to co-located eavesdroppers. How to design a security-proven physical key generation scheme under co-located attacks has not been well explored.

High Bit Disagreement Ratio in Low SNR Regimes: The similarity of channel measurements at Alice and Bob is highly determined by the SNR level. In low SNR regimes, the noise leads to a high bit disagreement ratio after quantization, which could cause a high reconciliation overhead and thus lead to a low key generation rate. Generally, existing works try to decrease the bit disagreement ratio by enhancing the SNR or reducing the quantization level. Obviously, a scheme achieving a low bit disagreement ratio in low SNR regimes is desired.

High Temporal Correlation: In previous works, in order to increase the key generation rate, a high probing rate is adopted in the channel probing stage to obtain more channel measurements, which can be quantized into more binary bits. However, within the coherence time, the temporal channel measurements are highly correlated, which leads to duplicated key bits. Obviously, a scheme that can maintain a high probing rate while reducing temporal correlation is of great interest.

5G-Enabled Secure and Efficient Key Generation

Before we point out the solution to the existing issues in key generation, we first introduce some disruptive technologies in 5G wireless networks. The opportunities and challenges of key generation based on these technologies are then discussed.

mmWave Communication

In 5G wireless networks, mmWave communication systems with the frequency range of 30–300 GHz are considered as a promising solution to increase communication capacity; that is, mmWave cellular systems will enable gigabit-per-second data rates thanks to the large bandwidth available at mmWave frequencies. But

RF signals in mmWave communication have a short transmission range due to its heavy free-space path loss. This may restrict the ability of eavesdroppers because passive eavesdroppers need to be aware of their distance to a legitimate user. In other words, the information leakage of the key generation process in mmWave communication is more sensitive to the location than in sub-6 GHz systems.

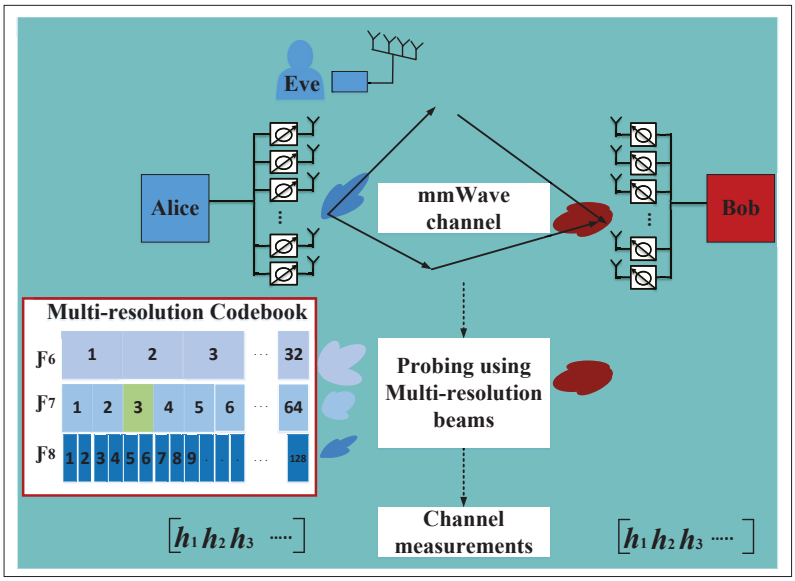

FIGURE 1. Key generation for mmWave massive MIMO with multi-resolution beams.

radio frequency (RF) signals in mmWave communication has a short transmission range due to its heavy free-space path loss.

This may restrict the ability of the eavesdroppers because passive eavesdroppers need to be aware of their distance to a legitimate user [1]. In other words, the information leakage of the key generation process in mmWave communication is more sensitive to the location than in sub-6 GHz systems.

Different from sub-6 GHz systems, which model the correlation of channel as Jake's correlation model [11], mmWave channels are location-specific and cannot be directly modeled as Jake's model. The proper eavesdropping model is under-explored. Also, the propagation of mmWave signals at high frequency has a higher outage probability compared to sub-6 GHz systems. The blockage effect of mmWave has effects on physical layer key generation and needs to be considered in the future analysis of secrecy key rate.

Beamforming and Massive MIMO

Beamforming (BF), typically realized with an antenna array, can be applied to provide a high antenna gain and mitigate the severe path loss at mmWave frequencies. In BF, the phase of antenna elements is adaptively shifted to form a concentrated and directed beam pattern [12].

In sub-6 GHz systems, BF is usually performed with several antenna elements in an antenna array. In mmWave communication, the number of antenna elements in the antenna array is greatly increased to enlarge the antenna gain of BF. MIMO systems with a great number of antennas are named massive MIMO. Thanks to the small wavelength of mmWave signals, a large number of antenna elements can be packaged on a chip. For example, in [13], the author proposes a small antenna array (40 mm × 41 mm) with 256 antenna elements, which thus enables the tiny antenna array to be embedded in Tx and Rx.

Massive-MIMO-based BF brings many benefits for physical layer key generation. At first, the ability of eavesdroppers is limited. The power level in massive MIMO is reduced, which cuts the SNR received at eavesdroppers. Apart from this, massive MIMO can generate very narrow beams by focusing on legitimate users without the signal power spilling over in other directions [14]. Due to the narrow beamwidth, an eavesdropper without beam tracking capabilities has high probabilities to lose eavesdropping links due to factors like slight rotation of the antenna array [10]. On the contrary, beam tracking techniques are required at the eavesdroppers to maintain a high SNR while eavesdropping.

The main challenge accompanying massive MIMO is the large channel estimation overhead. In existing works, most schemes choose the CSI as common randomness for physical layer key generation, which, however, is nontrivial to obtain in mmWave systems with massive MIMO. The large number of antenna elements causes large channel estimation overhead [15]. Consequently, if Alice and Bob need to do bidirectional probing for channel estimation, the efficiency of key generation is going to be affected by large channel estimation overhead, which needs to be tackled in future research. New schemes to combat these issues must be investigated.

Hybrid Precoding

Due to the short wavelength of mmWave, massive MIMO is quite promising for mmWave systems since antenna elements can be packaged on a chip. The increasing number of antenna elements requires larger phase array shifter networks. However, the number of BF chains controlling a phase shifter array cannot be increased linearly with the number of antenna elements. In order to provide high precoding gain with fewer RF chains, the hybrid precoding structure is proposed [15].

In this article, we propose a physical layer key generation scheme utilizing the hybrid precoding structure for mmWave massive MIMO systems, as depicted in Fig. 1. The hybrid precoder is the combination of an analog precoder in the RF domain and a digital precoder in the baseband domain. The RF precoder is composed of several analog phase shifter networks. In the digital domain, the baseband precoder is usually designed using compressive sensing techniques. For each round of bidirectional probing, Alice/Bob would select beams with different resolutions and angles. After all probings and getting enough samples, Alice and Bob would perform the remaining steps of physical layer key generation.

As depicted in Fig. 1, a multi-resolution codebook is utilized for precoding in our proposed scheme, which enables Alice and Bob to provide multi-resolution beams in the quantized angle space. Our scheme, based on hybrid precoding, can reduce the high temporal correlation under the high sampling rate in two aspects: the steering angle and the beam resolution. At first, by extracting every multi-path in the sparse mmWave channels, the hybrid-precoding-based key generation scheme can reduce the high temporal correlation of the channel measurements. The multi-paths belonging to different clusters experience independent scattering effects and thus possess independent statistical information. This effect can degrade the temporal correlation among channel measurements and improve the key generation rate.

Second, by adopting different beam resolutions in each round of bidirectional probing, the temporal correlation can be further decreased. For each round of bidirectional probing, the received signal in each round can be viewed as a weighted combination of multi-paths. By adjusting the beam resolution in each round, the weights on multi-paths can be affected. Selecting appropriate beam resolution can further reduce the temporal correlation. The performance of the proposed scheme is given and discussed below.

Although hybrid precoding is promising in key generation, the challenges associated with hybrid precoding cannot be ignored. The precoding gain of hybrid precoding is superposed by the analog precoder and baseband precoder. Precoding errors can be introduced due to the imperfection of analog components and thus need to be considered in the theoretical analysis of secrecy key rate.

Improving Security of Physical Layer Key Generation in mmWave Massive MIMO Systems

The implementation of physical layer key generation in mmWave massive MIMO communication systems is highly rewarding. In this section, we discuss the benefits in three specific cases: countering co-located eavesdroppers, achieving a low bit disagreement ratio under low SNR, and reducing the temporal correlation under high probing rates.

Countering Co-Located Eavesdroppers with High Directional Beams

In mmWave systems, transceivers deploy narrow beams with high directionality to suppress the interference from neighbors, which means eavesdroppers on the sidelobes have very low SNR. In order to achieve high SNR, the eavesdroppers in mmWave systems will approach legitimate transceivers as close as possible, which may bring threats for current physical layer key generation schemes, which mainly relies on location decorrelation to ensure security.

Enabled by the massive-MIMO-based beamforming techniques, the high directionality of beams offers a solution to counter the co-located eavesdroppers. In [10], we developed a key generation scheme for mmWave massive MIMO communication systems called "Secret Beam," where small random perturbation angles on the beamformer are chosen as the common random source. The overall process in Secret Beam includes the following steps: inter-perturbation, quantization, and XOR operation.

Due to the sparsity of mmWave channel and the narrow beamwidth of the massive MIMO communication system, the eavesdropper needs to approach Alice or Bob so that the narrow beams from certain directions can be received. For the eavesdropper co-located with Alice/Bob, Alice and Bob conduct the inter-probing strategy and adjust the perturbation on BF vectors to perform key generation. In the worst case, the eavesdropper may get the same bits as Alice or Bob but not both. However, by no means can the eavesdropper determine the key, which is the result of XORing bits generated at the Alice and Bob sides.

The mmWave massive MIMO system adopts analog phase-shifter with a single RF chain. We discuss the uniform planar array (UPA) adopted at Alice and Bob with two dimensions, 32 × 16 and 16 × 8. The narrowband mmWave operates on 28 GHz, and the channel reciprocity holds in the coherence time. The mmWave channel contains an LoS path and an NLoS path, where the amplitude of the NLoS path is typically 10 dB weaker than the LoS path.

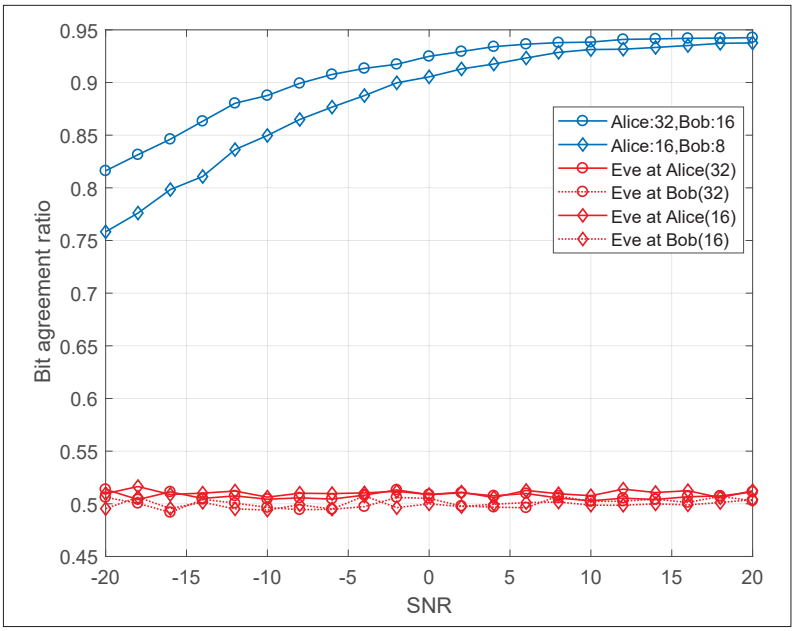

FIGURE 2. The bit agreement ratio under co-located eavesdroppers.

In Fig. 2, we compare the bit agreement ratio (BAR) in two cases with a fixed quantization level of 16. In the first case, the dimensions of UPA at Alice and Bob are 32 and 16, respectively (i.e., 32 × 16), and the blue curve marked with circles represents the BARs under different SNRs. In the second case, the blue curve marked with diamonds represents the BARs while adopting the smaller antenna number, 16 × 8, at Alice and Bob. We can observe that a higher BAR can be achieved with more antenna elements. There are four red curves representing four different cases, where the eavesdropper can either be co-located with Alice or Bob under two antenna dimensions (32 × 16 or 16 × 8). Based on the four red curves, we can observe that the eavesdropper's BAR in four cases after XOR operation is around 50 percent under various SNRs. As a result, this scheme is robust against a co-located eavesdropper.

Achieving a Low Bit Disagreement Ratio under Low SNR Regimes

A high bit disagreement ratio after the channel sounding can greatly increase the reconciliation overhead and slow down the key generation rate. For example, if the existing reconciliation cascade algorithm is used to reconcile two bit strings with a 10 percent bit mismatch rate, 60 percent of bits need to be discarded [6]. Therefore, having a low bit mismatch before reconciliation is critical in physical layer key generation.

In low SNR environments, existing works utilize a low quantization level to achieve the high key agreement ratio. However, in these schemes, fewer bits are quantized due to the low quantization level, which results in a low key generation rate. In contrast, we proposed a new key gen-

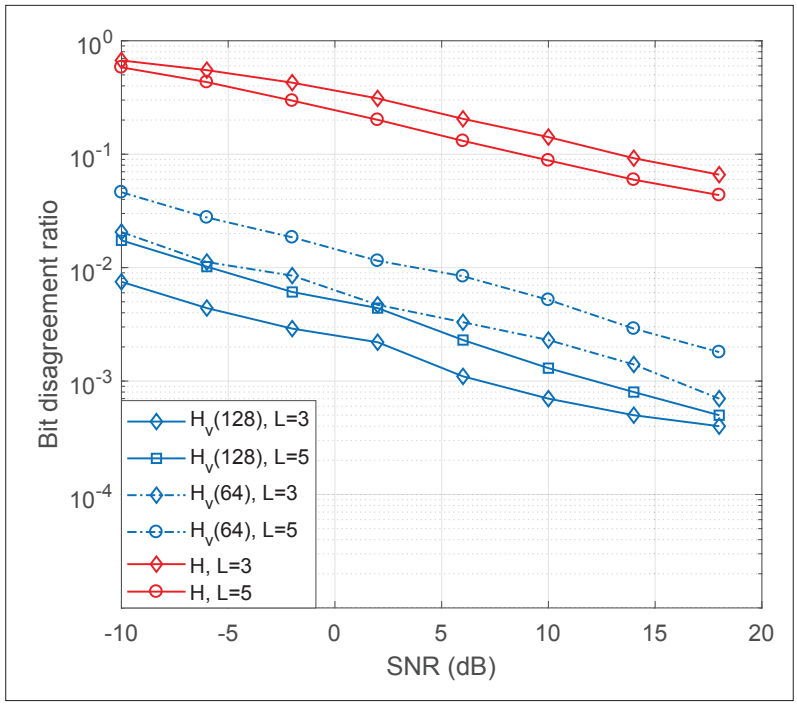

FIGURE 3. Bit disagreement ratio for channel estimate quantization and virtual AoAs and AoDs while $N_t = N_r = 128$.

eration scheme in [6] exploiting the sparsity of mmWave massive MIMO channel and the virtual AoAs and AoDs to obtain a high BAR (99 percent) even under low SNR regimes. In the mmWave massive MIMO channel, virtual AoAs/AoDs are transformed from physical AoAs/AoDs after projecting the mmWave channel onto the unitary matrix as the virtual channel matrix. In this way, we can observe that the entries corresponding to physical AoAs/AoDs have large amplitudes, as well as virtual AoAs and AoDs associated with physical AoAs and AoDs. On the other hand, if the entries in a virtual channel matrix do not correspond to physical AoAs/AoDs, the amplitudes are very small. In [6], for each side (Alice or Bob), the virtual AoAs and AoDs are estimated and selected as the common randomness. The sparsity reflected in the virtual angle domain makes the estimation process of virtual AoAs/AoDs against noise, which enables virtual AoAs/AoDs estimated at Alice and Bob to be highly identical. Consequently, quantized bits at Alice and Bob have a low bit disagreement ratio within low SNR regimes.

Figure 3 denotes the performance of the scheme achieving a low bit disagreement ratio. Using the quantization method in work [7], virtual AoAs and AoDs based key generation scheme achieves a very low bit disagreement ratio under low SNR regimes. For example, we compare bit disagreement ratio under two antenna dimensions, 128 × 128 and 64 × 64, where Alice has 128 or 64 antenna elements and Bob has 128 or 64 antenna elements, respectively. The blue curves represent the bit disagreement ratio of the scheme in [6] under different antenna dimensions and multi-path numbers. The red curves represent bit disagreement ratio of the existing scheme with antenna dimensions 128 × 128. L represents the number of multi-paths. The numerical result shows that the scheme in [6] achieves much lower bit disagreement ratio than the existing scheme [7]. For instance, when we consider the case where Alice and Bob have 128 antenna elements with $L = 3$, the bit disagreement ratio is under 10^{-2} even when the SNR is −10 dB, which outperforms the existing schemes.

Reducing Temporal Correlation under a High Probing Rate Using Multi-Resolution Beams

Even though a high channel probing rate provides more samples in a period of time, the key generation rate does not increase linearly with the probing rate. Within the coherence time, a high probing frequency leads to temporal redundancy along with a large number of repeated bits. In order to reduce the temporal correlation among samples, the random initial phase can be set to achieve multiple probes in one coherence time. However, it cannot be against noise and thus cannot reduce the temporal correlation under a low SNR value.

Hybrid precoding is popular in mmWave massive MIMO channel estimation, where it not only enables the codebook design for mmWave massive MIMO systems but also facilitates beamwidth adjustment in an easy way. The beams with adjustable width may focus on different multi-path and angles, which can reduce the correlation among the samples of the channel gain. Thus, we propose a scheme utilizing the multi-resolution beams in the channel probing stage to reduce the temporal correlation as illustrated in Fig. 1. In our simulation, the hybrid precoding scheme is implemented using the hierarchical codebook, while the system operates at 28 GHz where Alice has 64 antennas and Bob has 32 antennas, and a uniformly quantized phase shifter is considered. In Fig. 1, Alice selects beams with different resolutions or angles to send probing sequences, while Bob uses a fixed beam pattern in the coherence time. The beams are carefully selected from the hierarchical codebook to maintain the channel gain within a certain range, which enables this scheme to work under the low SNR regime.

Figure 4 illustrates the key entropy rate. In the coherence time, we use 5 beams with different resolutions and angles (P = 5). From the figure, we can observe that the key entropy rate approaches 1 as the SNR increases for the fixed beam. However, our scheme has the key entropy rate approximately 5 times of the fixed beams and thus can reduce the temporal correlation efficiently. The channel probing with multi-resolution beams can reduce the temporal correlation among samples so as to further improve the key generation rate with the carefully selected beam combinations. Also, the issue of how to maintain the channel gain in a certain range is critical because a big fluctuation of channel gain can affect the key generation rate.

Future Topics

In this section, we discuss the potential research directions and future trends of physical-layer key generation for 5G and beyond, including the mobility effect on key generation, multi-user massive MIMO, and backscatter communication.

The Effect of Mobility on Key Generation

In mmWave communication, the high path loss and limited scattering effects lead to a high blockage rate. In this case, the mobility patterns of

users may have an effect on physical layer key generation. How to maintain a stable key generation rate under this case is an open problem. Also, beam tracking is developed in mmWave communication to maintain the communication link. Existing key generation schemes need to consider the effect of beam tracking.

Multi-User Massive MIMO

To have efficient system performance, each BS is expected to serve a number of mobile stations simultaneously. Thus, hybrid precoding is popular to multiplex different data streams to different users. The digital precoding layer in hybrid precoding structure provides more freedom to reduce the interference among users. In this case, when it comes to physical layer group key generation, hybrid precoding may offer an opportunity to decrease the interference from other users and to maximize the group key generation rate. However, problems like how to decrease the channel estimation overhead in the group key generation and how to optimally tune channel probing rate and power need further investigation.

Backscatter Communication

Backscatter communication is an important enabling technology for the Internet of Things (IoT) because of its ultra-low power consumption and lower manufacturing cost. Based on this new technique, IoT devices can transmit data by reflecting and modulating incident RF signals without any power-thirsty RF transmitter. In addition, the newest ambient backscatter communications do not rely on any dedicated RF BS, but utilize ambient RF signals, such as TV radio, cellular, and WiFi, to communicate with other devices. However, in such scenarios, the devices cannot directly measure the channel characteristics among themselves as shared randomness to generate secret keys, which makes the conventional physical layer key generation approaches inapplicable. In massive MIMO mmWave backscatter systems, special channel models, such as round-trip multipath channel and dyadic backscatter channel, will bring new challenges and opportunities to exact randomness for shared secret key generation. Thus, new physical key generation schemes in backscatter communications should be considered to obtain a secret key with low computation and communication overhead.

Conclusion

In this article, we review the existing physical layer key generation schemes, and discuss the limitations and opportunities in 5G and beyond. Through three case studies, including combating co-located eavesdroppers, achieving a low bit disagreement ratio within low SNR regimes, and reducing temporal correlation under high prob ing rates, we demonstrate the benefits offered by 5G communication technologies for physical layer key generation. We also discuss future topics and potential research trends related to physical-layer key generation in 5G and beyond.

References

[1] N. Yang *et al.*, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Commun. Mag.*, vol. 53, no. 4, Apr. 2015, pp. 20–27.

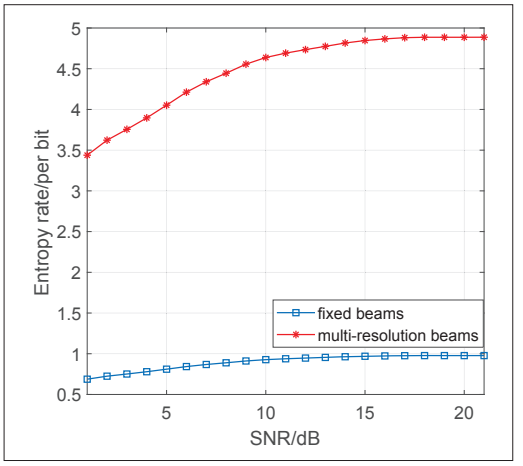

FIGURE 4. Key entropy rate.

[2] U. M. Maurer, "Secret Key Agreement by Public Discussion From Common Information," *IEEE Trans. Info. Theory*, vol. 39, no. 3, 1993, pp. 733–42.
[3] R. Jin *et al.*, "Delay Analysis of Physical-Layer Key Generation in Dynamic Roadside-to-Vehicle Networks," *IEEE Trans. Vehic. Tech.*, vol. 66, no. 3, Mar. 2017, pp. 2526–35.
[4] K. Zeng, "Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, June 2015, pp. 33–39.
[5] K. Zeng *et al.*, "Exploiting Multipleantenna Diversity for Shared Secret Key Generation in Wireless Networks," *Proc. 2010 IEEE INFOCOM*, 2010, pp. 1–9.
[6] L. Jiao, J. Tang, and K. Zeng, "Physical Layer Key Generation Using Virtual AOA and AOD of Mmwave Massive MIMO Channel," *Proc. 2018 IEEE Conf. Commun. Network Security*, 2018, pp. 1–9.
[7] J. W. Wallace and R. K. Sharma, "Automatic Secret Keys from Reciprocal Mimo Wireless Channels: Measurement and Analysis," *IEEE Trans. Info. Forensics and Security*, vol. 5, no. 3, Sept. 2010, pp. 381–92.
[8] T. S. Rappaport *et al.*, "Broadband Millimeter-Wave Propagation Measurements and Models Using Adaptive-Beam Antennas for Outdoor Urban Cellular Communications," *IEEE Trans. Antennas and Propagation*, vol. 61, no. 4, 2013, pp. 1850–59.
[9] H. Zhang, S. Venkateswaran, and U. Madhow, "Channel Modeling and MIMO Capacity for Outdoor Millimeter Wave Links," *Proc. 2010 IEEE Wireless Commun. and Networking Conf.*, 2010, pp. 1–6.
[10] L. Jiao, N. Wang, and K. Zeng, "Secret Beam: Robust Secret Key Agreement for Mmwave Massive MIMO 5G Commun.," *Proc. 2018 IEEE GLOBECOM*, 2018, pp. 1–6.
[11] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive Wireless Channel Probing for Shared Key Generation Based on pid Controller," *IEEE Trans. Mobile Computing*, vol. 12, no. 9, 2013, pp. 1842–52.
[12] S. Sun *et al.*, "MIMO for Millimeter-Wave Wireless Communications: Beamforming, Spatial Multiplexing, or Both?" *IEEE Commun. Mag.*, vol. 52, no. 12, Dec. 2014, pp. 110–21.
[13] S. Zihir *et al.*, "A 60 GHz Single-Chip 256-Element Wafer-Scale Phased Array With EIRP of 45 DBM Using Sub-Reticle Stitching," *Proc. 2015 IEEE Radio Frequency Integrated Circuits Symp.*, 2015, pp. 23–26.
[14] Y. Wu *et al.*, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE JSAC*, 2018.
[15] A. Alkhateeb *et al.*, "Channel Estimation and Hybrid Precoding for Millimeter Wave Cellular Systems," *IEEE J. Selected Topics in Signal Processing*, vol. 8, no. 5, 2014, pp. 831–46.

Biographies

Long Jiao (ljiao@gmu.edu) received his B.Sc. degree in information security from Xidian University, Xian, China, in 2016. He has been with George Mason University, Fairfax, Virginia, since 2016, where he is currently a Ph.D. student. His current fields of interest include 5G physical layer security, mmWave communication, mmWave HetNets, and deep learning.

Ning Wang (nwang5@gmu.edu) is currently a postdoctoral scholar in the Electrical and Computer Engineering Department at George Mason University. He was an engineer at Huaxin Post and Telecommunications Consulting Design Co.,

In massive MIMO mmWave backscatter systems, the special channel model, such as round-trip multi-path channel and dyadic backscatter channel, will bring new challenges and opportunities to exact randomness for shared secret key generation. Thus, a new physical key generation schemes in backscatter communications should be considered to obtain a secret key with low computation and communication overhead.

Ltd., Hangzhou, Zhejiang, Chain, from 2012 to 2013. He received his PhD degree in information and communication engineering from Beijing University of Post and Telecommunication, China, in 2017. His current research interests are in physical layer security, machine learning, device identification, and RF fingerprinting.

PU WANG (pwang20@gmu.edu) received his B.S. degree in telecommunications engineering from Xidian University, Xi'an, China in 2014. Currently, he is working toward a Ph.D. in cyber engineering at Xidian University. His research interests are in trust management in the Internet of Things and cloud computing, anonymous authentication, backscatter communication, wireless information and power transfer, and physical layer security.

AMIR ALIPOUR-FANID (aalipour@gmu.edu) received his B.S. degree in electrical engineering-power from the Islamic Azad University of Ardabil, Iran, in 2005, and his M.S. degree in electrical engineering-communication from the University of Tabriz, Iran, in 2008. He is currently pursuing a Ph.D. degree with the Electrical and Computer Engineering Department, George Mason University. His research interests include machine learning applications in security and privacy of cyber-physical systems, the Internet of Things, vehicle-to-vehicle communication, 5G, and wireless networks.

JIE TANG (jtang20@gmu.edu) received his Ph.D. degree from the University of Electronic Science and Technology of China. He is currently a visiting scholar at George Mason University. His main interests lie in fundamental mathematical optimization algorithms in wireless communication and networks.

KAI ZENG (kzeng2@gmu.edu) received his Ph.D. degree in electrical and computer engineering from the Worcester Polytechnic Institute (WPI) in 2008. He was a postdoctoral scholar with the Department of Computer Science, University of California at Davis (UCD) from 2008 to 2011. He was with the Department of Computer and Information Science, University of Michigan-Dearborn as an assistant professor from 2011 to 2014. He is currently an associate professor with the Department of Electrical and Computer Engineering, Cyber Security Engineering, and the Department of Computer Science at George Mason University. His current research interests are in cyber-physical system security and privacy, 5G physical layer security, network forensics, and spectrum sharing networks. He was a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) Award in 2012. He received the Excellence in Postdoctoral Research Award from UCD in 2011 and the Sigma Xi Outstanding Ph.D. Dissertation Award from WPI in 2008. He is an Editor of *IEEE Transactions on Information Forensics and Security*, *IEEE Transactions on Wireless Communications*, and *IEEE Transactions on Cognitive Communications and Networking*.