University of Kaiserslautern
Department of Computer Science

Physical Layer Security in Next Generation Mobile Networks:

Design, Implementation and Validation of a LTE Testbed

Master Thesis
by

Sachinkumar Bavikatti Mallikarjun

Matriculation Number:	403581
Supervisor:	Prof. Dr. Christoph Grimm
	Prof. Dr.-Ing. Hans D. Schotten
Degree Course:	Masters in Computer Science
E-Mail:	bmsachin03@gmail.com
Date:	Wednesday 22nd January, 2020

I would like to dedicate this thesis to my loving family for which I am highly grateful…

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this thesis are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This thesis is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and references.

January 2020

Acknowledgements

First of all, I would like to extend my gratitude and appreciation to my supervisors Mathias Strufe, Christoph Lipps, Christopher Heinz for always being there for guiding me throughout the challenging times of this thesis. Their supportive advise, brainstorming and engagement throughout the development of this thesis were valuable.
Finally, I would like to thank my friends who supported me throughout the process of this thesis and gave their valuable opinions, that helped me not only in this thesis but throughout my daily life.

Abstract

With the advent of the Internet-of-Things (IoT) together with the fourth industrial revolution and its fusion of technologies into so-called Cyber Physical Production Systems (CPPS) and Industrial Internet of Things (IIoT) new application scenarios arise. Due to the driving forces of mobility and flexibility, the number of interconnected entities is constantly increasing.

The cyber security of these entities is an important factor in strengthening confidence in the systems. The key enablers of this development are at first the mobility and flexibility of the components due to the use of wireless connections, and secondly the possibility of actively influencing the network management with Software Defined Network (SDN) approaches.

Nevertheless, the use of this wireless communication solutions are accompanied by great risks, new attack vectors and cyber security threats. The open nature and the broadcast characteristic suffer a huge potential for miscellaneous cyber-attacks. Pertaining not only to these, there is a fundamental need for sound and secure authentication of participating entities and reliable encryption of transmitted data. However, traditional cryptographic application come along with a lot of overhead in form of complex computations and communication. Besides that, new system often no longer has any interface to enter conventional credentials. In order to achieve this requirements, new methods have to be developed, which meets the demands of the industry such as low latency, low cost and reliable communication.

A potential solution is to use Physical Layer Security (PhySec) methods. Characteristic properties of the wireless channel are used to obtain cryptographic credentials. In WLAN IEEE 802.11 the functionality and applicability of these methods have already been validated. New wireless and cellular solutions are being investigated for future industrial applications, academic research and in campus networks.

In current research projects, solutions for the Future Industrial Internet, the Tactile Network approaches are being developed in an industrial environment. PhySec approaches are used to derive and establish shared secret keys between participating entities. This Secret

Key Generation (SKG) is based on characteristics of the wireless channel and easy to use, low cost, resource saving, and efficient method to enable confidence and trust into IIoT systems with already existing hardware.

The aim of this thesis is to transfer, adapt and improve the existing methods towards Next Generation Mobile Networks and evaluate if they perform as expected. SKG method have four steps namely, measuring the channel variations within coherence time, enhancing the channel profile to increase the reciprocity factor, quantising the channel profile to generate the preliminary key and finally increase the entropy of the key using privacy amplification. The entropy of key generated depends on the quantisation method used, so different quantisation methods are tested and evaluated using Shannon's entropy. To increase the channel profile reciprocity two different methods are used, namely: DCT normalisation and methods from Machine Learning such as, Linear Regression with polynomial features. The entire process of SKG is implemented in real time by developing prototype using SDR's such as srsLTE. The evaluation of the key generated is done by calculating the bit disagreement rate, key generation rate and Shannon's entropy.

Table of Contents

List of Figures

List of Tables

Acronyms

Acronyms / Abbreviations

AI	Artificial Intelligence
CIR	Channel Impulse Response
CPPS	Cyber Physical Production Systems
CPS	Cyber Physical Systems
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
eNodeb	Evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
FDD	Frequency Division Duplex
HSS	Home Subscriber Server
IIoT	Industrial Internet of Things
LR	Linear regression
LTE	Long Term Evolutionn
ME	Mobile Environment
MIMO	Multiple-Input-Multiple-Out
MME	Mobility Management Entity

NAS	Non Access Stratum
NGWN	Next Generation Wireless Networks
OAI	Openairinterface
OFDMA	Orthogonal Frequency Division Multiplex Access
OFDM	Orthogonal Frequency Division Multiplex
P-GW	PDN gateway
PDN	Packet Data Network
PhySec	Physical Layer Security
PUFs	Physically Unclonable Functions
QCI	QoS Class Identifier
RRC	Radio Resource Control
RSRP	Reference Signal Received Power
RSSI	Received Signal Strength Indicator
S-GW	serving gateway
SAE	System Architecture Evolution
SDN	Software Defined Network
SDR	Software Defined Radio
SE	Static Environment
SKG	Secret Key Generation
TDD	Time Division Duplex
TPM	Trusted Platform Modules
UE	User equipment
UHD	Universal Hardware Driver
USRP	Universal Software Radio Peripheral

VoLTE	Voice over LTE
WLAN	Wireless LAN
WPAN	Wireless Personal Area Networks

1. Introduction

1.1 Motivation

We currently are on the brink of Fourth Industrial Revolution, with all the forms of machines merging in both private and industrial sectors. This fusion of technologies and different devices leads to universally known CPPS and the IIoT across technological boundaries. Mobility, flexibility and portability are the driving forces of this process, enabling developments and improvements in the wireless communication industry. Without the use of this technology, the IIoT would be inconceivable. Wireless connectivity makes it possible to overcome the constraints and limitations created by the use of wired and static connectors.The major task is to guarantee a sound and reliable implementation of these processes. The participating entities throughout the IIoT should be able to independently verify an optimal key management system and capable of managing the significant number of interconnected devices.

Traditional solutions use cryptographic procedures that come along with an overhead in the form of computational complexity and communication. Along with this, new system often no longer have any interface to enter conventional credentials. In contrast, while using wireless communications, there is yet another problem. In general, they are vulnerable to diverse cyber attacks because of the open nature of both devices and the broadcast attributes. This just does not apply to IEEE 802.11 Wireless LAN (WLAN) or short-range systems such as IEEE 802.15 Wireless Personal Area Networks (WPAN), such as Bluetooth or ZigBee, however, comparable flaws remain for all wireless networks, as well as for cellular networks.

The popularity of the smart devices and demand for immense web content is increasing in rapid speed, which in turn is creating more mobile radio solutions [4]. To meet such demands Next Generation Mobile Networks (NGMN) are been developed, but still security flaws are not been resolved. Physical Layer Security (PhySec) solutions offers a worthwhile approach

in alleviating the security vulnerabilities. PhySec has been successfully implemented in wireless technologies like WLAN.

1.2 Structure of Thesis

The structure of the thesis is categorized into following sections. First, in Chapter 2, the content of the thesis is defined through the explanation of several principle concepts such as PhySec, and current work on PhySec's SKG methods and Cellular Networks (Long Term Evolution (LTE)). Moreover, an introduction of the real-time Software Defined Radio (SDR) used in this thesis that consists of the srsLTE EPC, Evolved Node B (eNodeB), User Equipment (UE), and lastly, the methods of SKG are explained to understand the nuts and bolts of the thesis. In Chapter 3, the methodology that is pursued to carry out this thesis has been discussed in detail. In Chapter 4, the developed testbed to test the different SKG methods is discussed. In Chapter 5, results and evaluation of the different methods of SKG is discussed. Finally Chapter 6, concludes the work and provides an outline for future work, to extend the current concepts.

1.3 Aim of Thesis

In this thesis PhySec methods used in WLAN IEEE 802.11 to develop the secret key based on the randomness and variation of the channel properties is put to use with enhanced methods for private and campus related cellular networks, such as LTE. Furthermore the testbed is evaluated to see if PhySec method's SKG provide the symmetric and random secret key for secure communication between eNodeB and UE.

2. Physical Layer Security and Cellular Networks

In this chapter, principle concepts of this thesis are discussed such as, brief introduction of PhySec, previous and current ongoing research of PhySec, brief explanation of LTE components, characteristics, advantages, concepts of SDR and software's which is used to build the LTE testbed, and the building blocks of SKG using PhySec concept.

2.1 The Wireless Channels/Cellular Networks

Understanding of wireless channel is much needed for this thesis, wireless channel properties, parameters, physical modeling and variations acts as a core for building this thesis. Based on the variations of the channel and noise factor of the environment helps generating the secret key. LTE is a wireless broadband technology that employs wide channels to reach elevated data rates and serve many customers. SKG method is applied for LTE technology in this thesis.

2.1.1 Long Term Evolution Architecture

A review for nuts and bolts of the LTE is given in this section, for the clear and better comprehension of the thesis. The fundamental segments of LTE are:

- Evolved Packet Core (EPC),
- Evolved Node B (eNodeB),
- User equipment (UE);

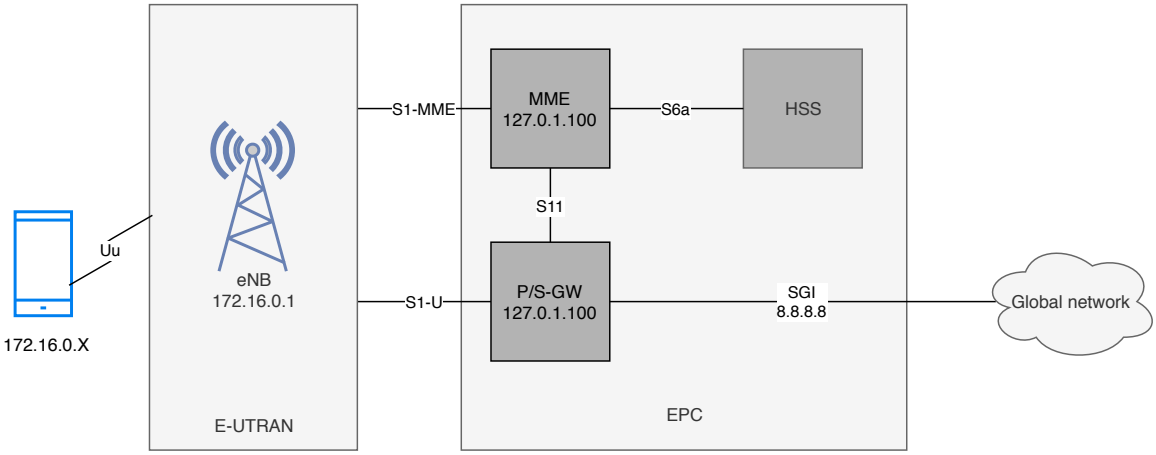

Fig. 2.1 LTE Architecture

Evolved Packet Core (EPC): The EPC is the core network. An all-IP E2E network means that all traffic flows from an UE to a Packet Data Network (PDN) connecting to a service entity are transferred within Evolved Packet System (EPS) on the basis of an IP protocol. The primary elements of EPC are as follows

- **Mobility Management Entity (MME):** MME is the principle component of the EPC control plane to manage UE access via Evolved Universal Terrestrial Radio Access Network (E-UTRAN). Every UE that is enrolled in the LTE network and available via E-UTRAN has a MME entity allocated. The MME is responsible for managing connection with the Radio Resource Control (RRC) in E-UTRAN and positioning of the UE's in the idle mode to save battery, discontinuation of the Non Access Stratum (NAS) signalling protocols, and it does selection of entities for Serving gateway and PDN-gateway, and finally, supports the transfer of tasks between eNodeBs and intra system handover.

- **Home Subscriber Server (HSS):** UE's data is stored in the HSS entity, which is a database, it includes, user subscription, data on network efficiency and other related data. The MME can access the HSS through the S6a interface to regulate service accessibility connectivity as shown in Figure 2.1. S6a is the critical path for managing subscribers data.

- **Serving and Packet Data Network gateway:** The data plane communication between E-UTRAN and EPC is provided by S/PGW. Depending on the terminal geographical location and loads balancing criteria, EPC assigns S-GW entity for every registered UE in LTE, entity can be accessed by the MME via the S11 interface as shown in Figure 2.1 and by the P-GW via the S5 interfaces. P-GW is the gateway that provides

connectivity to external Packet Data Networks (PDNs) via the SGI. At least one P-GW entity shall be assigned to an UE after registration with LTE. S-GW acts as a local mobility support for transferring inter-eNodeB and inter-3GPP. S-GW is responsible for the routing and temporary storage of user IP packets from terminals in idle mode and initiates the service request operation caused by the network. S-GW routes the user traffic to / from one or more P-GWs and responsible for UL and DL charging per UE, PDN, and QCI, Granularity of the accounting and QoS Class Identifier (QCI) for inter-operator charge. Use policies, accounting and lawful interception are controlled by S-GW.

P-GW is responsible for assigning IP addresses for the UE and acts as a local mobility support for transferring inter-eNodeB and non-3GPP, P-GW applies control guidelines for the quality of service parameters from the LTE network's information sessions and finally responsible for uplink, downlink service level charging, gating and rate enforcement.

E-UTRAN: E-UTRAN can be referred as a replacement of the Universal Mobile Telecommunications Service (UMTS) and High Speed Downlink Packet Access/High Speed Uplink Packet Access (HSDPA/HSUPA) technologies specified in 3GPP. E-UTRAN has an entirely new air interface system, which is completely unrelated and unsuited with W-CDMA and it has higher data rates, lower latency and is optimized for packet data. E-UTRA uses Orthogonal Frequency Division Multiplex Access (OFDMA) radio-access for the downlink and Signal Carrier-FDMA (SC-FDMA) on the uplink. E-UTRAN is the combination of E-UTRA, user equipment (UE), and E-UTRAN/eNodeB.

eNodeB performs RRC fucntions such as Radio Bearer Control, Radio Admission Control, Connection Mobility Control, Dynamic allocation of resources to UEs in both uplink and downlink. Mobility and scheduling measurement report and measurements are configured by eNodeB. Access Stratum (AS) security which is responsible for securely delivering the RRC messages between a UE and an eNodeB is handled by eNodeB. when no routing to a MME can be determined from the information provided by the UE attachment procedure, eNodeB Selects MME entity. eNodeB schedule and transmits paging messages and broadcast information originated from the MME.

2.1.2 Characteristics of Long Term Evolution Network

LTE has a number of characteristics that allow immediate radio channel conditions to be operated with a very high efficiency. Few important characteristics are briefed here.

Orthogonal Frequency Division Multiplex (OFDM) technology is used to the signal format for LTE because of its high data bandwidths, and this technology is highly resilient to reflections and interference and in addition, the battery life of mobile handset increases. OFDM technology uses OFDMA for downlink channel and SC-FDMA for uplink channel. Multiple-Input-Multiple-Out (MIMO) technology helps to be resilient to reflection of signals and have high throughput and antennas with matrices 2x2, 4x2, 4x4 can be used. System Architecture Evolution (SAE) provides Core Network functions to periphery and is it flat form of network architecture with low latency and efficient routing methods. And finally, LTE is all IP data system, so Voice over LTE (VoLTE) technology helps the network provider in market even after huge scope of internet calls.

2.1.3 Advantages of Long Term Evolution Network

There are many advantages of LTE, few important advantages of LTE are briefed here. LTE has high speed when compared to 3G, as it uses 1800 to 2300 MHz frequency bands and high data rate with high capacity with support of MIMO, as it can support upto 200 clients per cell. Low latency helps the system to perform better in real time, lower the latency, better the performance and LTE offers low latency compared to 3G technology. SC-FDMA in uplink channel helps using battery efficiently and OFDMA in downlink helps efficient usage of channel resources and thus increasing the capacity of users in LTE and the improved architecture helps uninterrupted data transfer while changing the region.

2.2 Software Defined Radio

Software Defined Radio (SDR) is re-programmable radios which are completely software-based and can modify the physical layer characteristics, to put it more simple SDR are any radio where all or some functions of the physical layer are software-defined. Instead of hardware devices like mixers and amplifiers, SDR uses the software on embedded or computer system and it is cost-efficient and flexible. Usually, SDR includes sound card, analog to digital converter and a processor for signal processing. Modifications like modulation, demodulation, filtering, error correction, configurable bandwidth, and carrier frequency can be programmed and it has a versatile platform for different applications. SDR application can be seen in various areas such as, using a single hardware platform called the Joint Tactical Radio System, which utilizes distinct waveforms by configuring the software, military communication takes place. Satellite modems use programmable processing devices for intermediate signal processing. Using System on Chip (SOC) in cell phones, programmable

digital signal processing is integrated and cellular infrastructure utilizes programmable processing equipment to create various protocol base stations.

2.2.1 The Openairinterface

The Openairinterface (OAI) is the open-source full protocol stack implementation of the 3GPP, LTE, and 5G(ongoing). OAI has built-in tools like emulation modes, debugging, protocol analyzer, performance, and configurable logging systems for all the layers and channels [5]. OAI can be used to build the customized base station, core network and UE, and can connect to real-time mobile devices with appropriate configurations. Radio front end connected to the computer acts as a transceiver for processing. The software is divided into two parts openairinterface5G and openair-cn

- openairinterface5G acts as an E-UTRAN and take care of all the functionalities of the eNodeB and the UE. And it can be integrated with other platforms for different purposes. C++ language is used to develop the openairinterface5G package.
- openair-cn is core of the network, it acts as EPC engraving all the functionalities of the HSS, MME, S-GW ad P-GW and all the functionalities can be changed as per requirements of the user.

2.2.2 Software Radio Systems LTE

Similar to OAI, srsLTE is an open-source full protocol stack implementation of the 4G LTE software suite. srsLTE supports end-to-end software radio mobile network. srsLTE platform is with nominal external dependencies and it stands as high performer among SDRs. srsLTE has a whole software suite including eNodeB, UE, EPC with L1 (Physical layer), L2 (Medium Access Layer , Packet Data Convergence Control, Radio Link Control) and L3 (NAS Protocols, IP, RRC) protocol stacks implemented in the library. srsLTE library has modular approach as shown in Figure 2.2, the modular library approach allows user to easily customize improve or completely replace components without affecting the rest of the code. The srsLTE library is divided into four components Core, Physical Channels, UE Processes, Example Applications. Core module deals with the building blocks of the physical layer, Physical Channel module deals with uplink and downlink channel, these modules uses the core building block for signal processing, physical channel procedures for UE is taken care by UE Processes module, further explaination of the modules is given in [1]. In this thesis, srsLTE is used to build the LTE testbed as the code complexity of OAI is high compared to srsLTE and tracking measurement is user friendly in srsLTE than OAI.

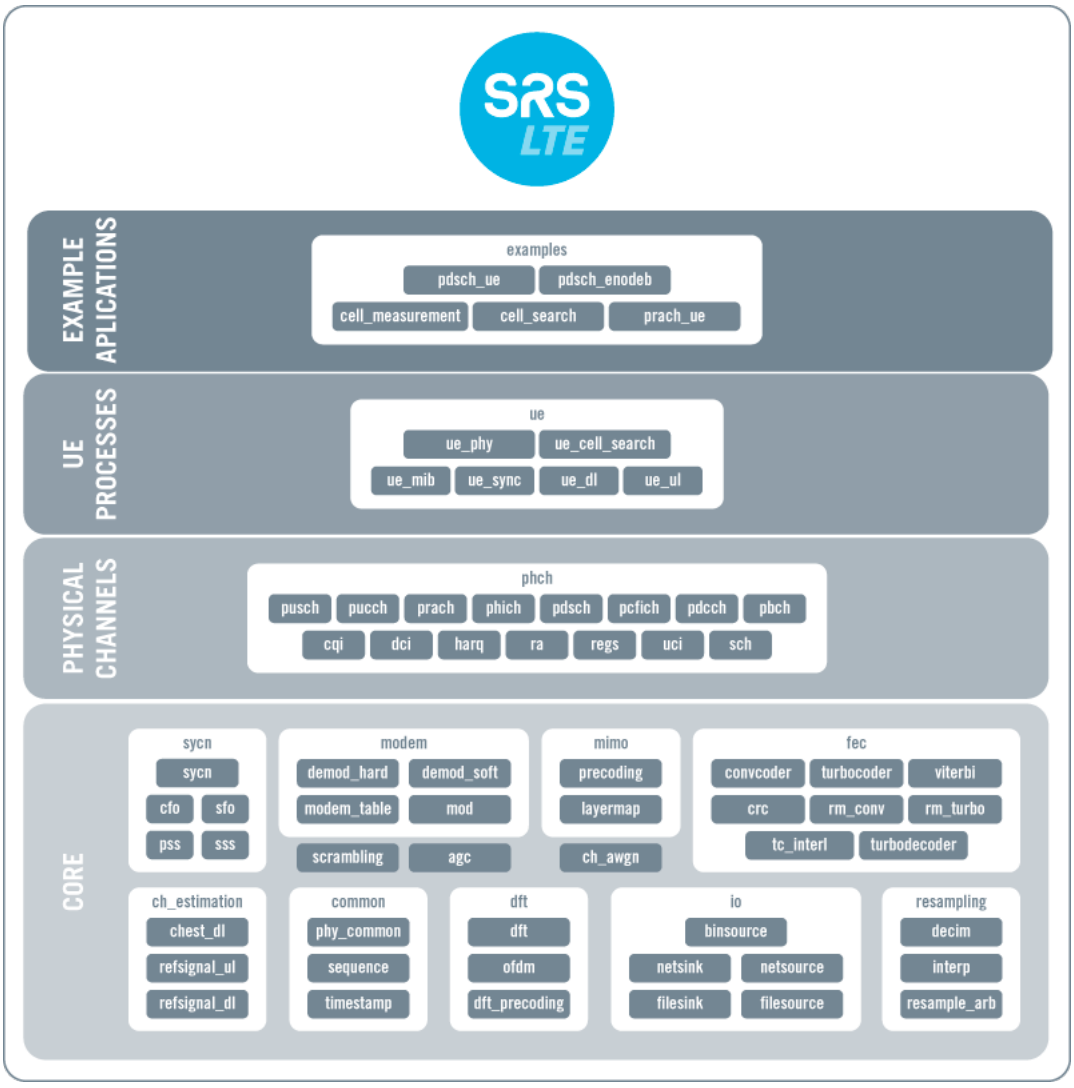

Fig. 2.2 srsLTE modular library, from [1]

The srsLTE suite includes:

srsUE runs on Linux based operating systems and it acts as LTE UE modem written in C++ language.SrsUE connects to any LTE network on configuring it to required settings. For transmission of radio signals transceivers like Universal Software Radio Peripheral (USRP), bladeRF limeSDR are supported. srsUE supports both FDD and TDD configuration and high data rates like 36 Mbps DL in 10 MHz Single Input Single Output (SISO) configuration in i5 Dual-Core CPU and 75 Mbps DL in 20 MHz SISO configuration in i7 Quad-Core CPU. srsUE is responsible for cell search, synchronisation procedures and on network attach, an virtual network interface tun_srsrue is created and supports QoS

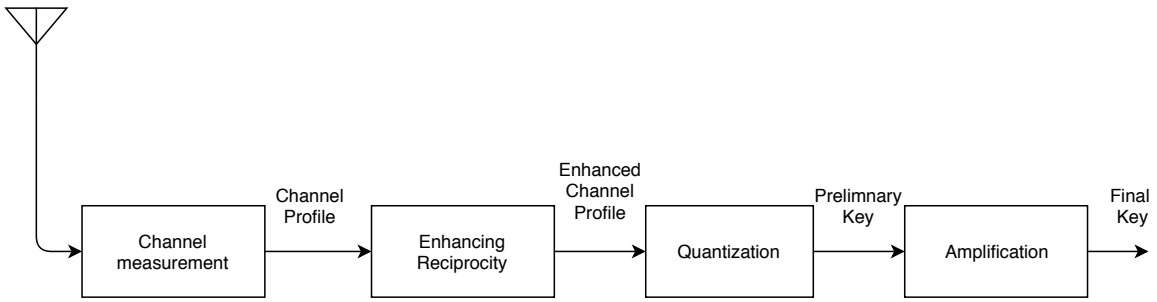

Fig. 2.3 Building Blocks of Secret Key Generation

srsENB runs on Linux based operating systems and it acts as LTE eNodeB written in C++ language. srseNodeB is a versatile package which connects to any LTE core network (EPC) and creates a local cell. For transmission of radio signals transceivers like USRP, bladeRF limeSDR are supported. Although srsUE supports both FDD and TDD but srseNodeB supports only FDD configuration and have data rates like 150 Mbps DL in 20 MHz MIMO TM3/TM4, 75 Mbps DL in SISO configuration, 50 Mbps UL in 20 MHz with commercial UEs.

srsEPC is a light-weight core of the network, written in C++language and operates on Linux based operating systems, it acts as EPC engraving all the functionalities of the HSS with configurable user database in CSV format, MME - with standard S1AP and GTP-U interface to eNodeB, S/P-GW - S/P-GW with standard SGI exposed as virtual network interface and all the functionalities can be changed as per requirements of the user

2.3 Physical Layer Security

In contrast with the past, people are heavily relying on wireless technology in their day-to-day life, it has become a necessary entity in everyone's life, so the security of wireless networks is one of the critical issues in research. There are many drawbacks of the current security technologies like high computational capacity, high cost and unsecured public wireless networks. The main idea behind PhySec is to use the transmission channel's intrinsic randomness to ensure security in the physical layer.

There are many methods or technologies based on PhySec for wireless systems like PhySec Coding [6], PhySec in massive Multiple-Input-Multiple-Output systems [7], PhySec for Millimeter-Wave communications [8], PhySec for Heterogeneous networks [9], PhySec for Non-orthogonal multiple access [10], PhySec for Full duplex technology [11]. The main advantage of PhySec over cryptographic methods are PhySec needs less computational power and have high scalability. Many of the commonly used cryptographic procedures use

complex computations to establish a secure key. In addition to certain computing time, this requires computing power and thus also resources in the form of power. Furthermore, the generated key must be exchanged in a secure manner and stored securely in the memory of the participating entities. Alternatively, a key is integrated into the device like Trusted Platform Modules (TPM), from the outside before it is delivered. The addressed benefit of the PhySec method is, that nothing has to be exchanged over an (insecure) channel

There are currently two major branches of this PhySec. First of all, there are silicon or electrical approaches that exploit the physical randomness out of components, that results of slightest deviation occurring during the manufacturing process of the individual components. These procedures are also referred to as Physically Unclonable Functions (PUFs) [12] [13]. They can be further subdivided into procedures that are timing-based, which means that they make use of individual delays within the signal processing. This includes, other Arbiter, Ring-Oscillator (RO), and Butterfly-PUFs [14]. Furthermore, there are approaches such as SRAM-PUFs [15] that uses the individual, voltage based threshold values of semiconductor devices to derive a cryptographic key. Secondly, PhySec includes approaches that exploit the special characteristics of a wireless channel like the Received Signal Strength Indicator (RSSI), the Reference Signal Received Power (RSRP) and the Uplink power. In this thesis, these approaches are used to generate the secret key as shown in Figure 4.11. In [16], correlated observations of noisy phenomena is exploited to generate the secret key by exchanging information over a public channel and this was the first-ever approach.

After the introduction of the general PhySec approaches, in the previous section, this section gives the brief idea of the ongoing research in the field of PhySec and their findings to understand the insight of PhySec. Currently, researchers are trying different approaches like, secure video transmission using physical layer technique [4]. The fundamental notion of PUFs was implemented in 2002, while a lot of studies is being done in this field, however, the amount of wireless alternatives can be managed, particularly in the region of cellular approaches. Moreover most of the job is theoretical. A survey of different PhySec approaches, including Next Generation Wireless Networks (NGWN) as mentioned in [17]. These approaches provide an overview of existing work and also point out different focus issues of wireless systems. Such as, integration of fading influences or deviations while using MIMO systems and including multi-antenna technologies.

Using Wireless Open-Access Research Platform (WARP) hardware, a testbed was developed for wireless communication systems to study SKG, based on PhySec method by [18]. A detailed work on different channel types and multi channel antenna, broadcast channels, multiple channel, and interface channel providing metrics for application of PhySec prin-

ciple in multi user wireless network is given by [19]. Improvement and suggestions of the individual steps in SKG is given by [20].

Apart from WLAN approaches, PhySec methods are been researched for cellular networks. PhySec for heterogeneous cellular networks and mmWave networks have been researched by [21] [22]. In these works, a system model has been created that integrates different scenarios, such as directional beam forming, small scale fading, and path loss. Performance model for information-theoretical secrecy in vast cellular networks is provided by [23]. Additionally, [22] compares the outcome of mmWave cellular communication with standard microwave networks in bands below 6GHz. A study of PhySec methods in the downlink of cellular networks, where each Base Station (BS) simultaneously transmit confidential messages to several users and where the confidential messages to each user can easily be eavesdropped by an attacker, this has been analyzed by [24].

A stochastic geometry approach for PhySec in cellular networks is proposed by [25]. They extend the information theoretic secrecy performance in large scale cellular networks and provide a system model with orthogonal multiple access, and a single class BS. Thereby they focus on the performance achieved by randomly chosen typical mobile users. Within their work of safeguarding 5G wireless communication with PhySec, [4] utilize the unique characteristics of different ad-hoc networks and carrier operated, high-speed back haul networks while connecting to individual base stations. Research about key generation over biased PUFs by using polar codes is done by [26].

2.4 The Building Blocks of Secret Key Generation

The steps used for extracting secret keys in this thesis consists of four basic steps as shown in Figure 2.3 namely:

- Channel profiling
- Enhancing reciprocity
- Quantisation
- Privacy amplification

At first, the measurements like RSSI, RSRP, Uplink power values are taken at both ends of the channel (eNodeB, UE) to build a channel profiles, and to increase the reciprocity of the built channel profile certain methods are implied in second step Enhancing channel reciprocity. In quantisation step the built profile is quantised to bits to generate the initial key, the

key generated in quantisation steps might not be similar at both ends of the profile if channel profile is not enhanced in the second step of Enhancing Reciprocity. The security of the initial key is enhanced by the privacy amplification step to obtain the final secure key The following subsection provides a comprehensive explanation of each step with an adequate reference.

Channel Profiling The channel profile is constructed by measuring the channel variation within a specific duration of time after UE connecting to the network. Few methods followed to construct channel profile by using channel properties like RSSI, RSRP, Power and Channel Impulse Response (CIR).

- Received Signal Strength Indicator (RSSI): RSSI is an indicator of the received signal strength at the receiver. RSSI can be easily measured by most mobile devices and other wireless infrastructures, so it is commonly used to build channel profile to generate a secret key.
- Channel Impulse Response: Channel profile can be constructed by using the factors like the number of multi path, amplitude coefficient and phase of the channel. In a real indoor environment, reference exploits the channel impulse response to generate the channel profile.
- Referenced Signal Received Power: It is received signal strength type of measurement. It is referred to as average received power of single reference signal of the recourse element. It gives the measurement of power excluding the factors of noise and interference from the sectors hence it helps to build a channel profile with high reciprocity even in the environment where the noise is unpredictable.
- Uplink power: The Uplink power is measured at both ends, Power used by UE to send the signal in uplink channel and power received by the eNodeB in the up-link channel. On considering only one channel for recording the measurements to build the channel profile, so only uplink channel's noise factor is considered. The measurement upholds the principle of reciprocity so it can be considered as ideal channel property to measure and to build the channel profile.

Enhancing Reciprocity Generally, secret keys are generated by quantising the measured channel profile but due to variations in hardware, noise and half-duplex nature of transceivers make the measured channel profiles from eNodeB and UE to have less reciprocity factor. So the channel profile is processed to increase the reciprocity of the measured channel

profiles. The enhanced profile has better bit disagreement rate than the raw channel profiles. Few methods to enhance reciprocity have been followed by other researchers, [27] have used methods like l1-norm minimization, hierarchical clustering, Kalman filtering, and polynomial regression to enhance the channel profile to obtain better key generation rate and bit disagreement rate.

Quantisation The initial key or preliminary key is obtained by quantising the measured channel profile into bits. Different methods of quantisation can be followed, the channel profile is quantised as a whole or block by block. Apart from the above-mentioned methods quantisation can be classified into lossless and lossy quantisation.

- Lossless quantisation: All measurements are considered while quantising in this method. Channel profile is quantised into bits based on the threshold values. One or more levels based on threshold value can be considered to quantise the channel profile. In [28] binary quantisation is used to quantise the channel profile and in [29] median quantisation is used as lossless quantisation
- Lossy quantisation: In this method, few measurement values are dropped based on the threshold values. Dropped values can be intermediate to threshold values and above or below the threshold value.

Privacy Amplification If the key extracted by eNodeB and UE are identical, then chances are that third party can predict the key by accessing the information from information reconciliation step, few secret key extraction methods use information reconciliation step to detect and correct the errors in the generated secret key. Privacy amplification step helps to decrease the chances for third party to predict the generated key. Methods like linear mapping [27], hashing or by using some extractors like fuzzy can be used to amplify the privacy of the secret key.

2.5 Artificial Intelligence based Secret Key Generation

Recently, Artificial Intelligence (AI) has prevailed. People across distinct fields are attempting to apply AI to make their assignments permissive. Artificial intelligence and potential mobile operators have shown immense interest to improve cellular network and take its usage to the next level by collaborating business and academic interest.

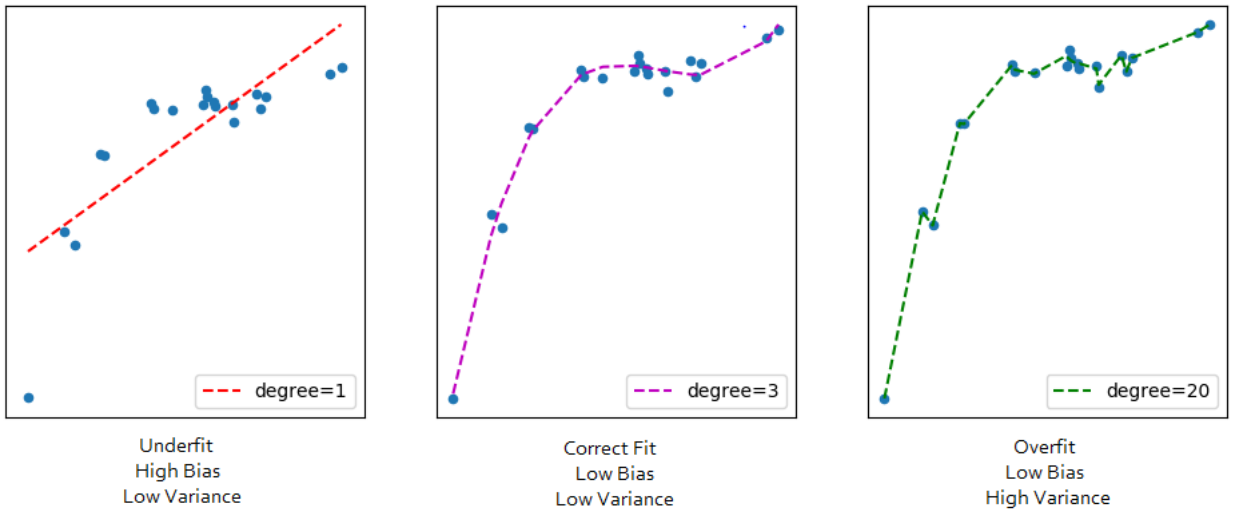

Fig. 2.4 Linear Regression, from [2]

2.5.1 Linear Regression:

Linear regression (LR) is one of the supervised Machine Learning (ML) algorithms. LR model predicts based on the independent variable, the algorithm is based on finding the relationship between the dependent and independent variable. In [30] the author uses linear regression to predict the behavior of the radio-frequency identification tag based on RSSI. Similarly, other works like to predict the cell range or signal strength are using linear regression model. Furthermore explanation on LR is given in Section 3.2.2

Polynomial Features

LR works on basis of co-relating dependent and independent variables. If the data distributed is complex then linear regression will be in under-fit state, as it cannot cover all the pattern in data, so the complexity of the model is increased by adding to higher power to the original feature, adding as new features and hence overcoming under-fit nature as shown in Figure 2.4. On increasing complexity, linearity of the model remain same but curve fitting would be polynomial in nature.

3. Methodology

3.1 Introduction

The thesis establishes shared secret keys using reciprocal and random variations of the wireless channel and considers that it is a worthwhile idea for deploying key management systems in cellular networks systems especially campus networks like mobile and static ad-hoc networks, which are being deployed in large numbers in the current industry and campus networks. Secret key management systems are an integral part of any security infrastructure and security of such networks is a necessary condition, which should be met for the successful deployment. The inherent fading characteristic of the wireless channel is used to generate a shared secret key between a pair of eNodeB and UE. The SKG process consists of measuring the channel profile, enhancing it, quantifying it to get preliminary keys and finally obtaining a secure key. By covering some variety of key generation methods, the different methods explored in the state of the art and prototype have been developed to verify the validity of the methods in different environments.

In this chapter, details about the different methods used to generate the secret key using physical layer properties are discussed.

3.2 Methods of key Generation

As discussed in the previous Chapter the building blocks (as depicted in Figure 2.3) of Secret Key Generation are

- Channel Profiling,
- Enhance Reciprocity,
- Quantisation,

- Privacy amplification;

All the above methods are discussed in below section.

3.2.1 Channel profiling

The inherent characteristic of wireless channel is fading, which is the reason for the variation in the amplitude and phase of the transmitted signal. The channel profile is constructed by measuring the channel variation within a specific duration of time after UE connects to the network. The variations occuring on eNodeB and connected UE are quite similar, as they adhere to the channel reciprocity principle. The variations of the channel measurements can be caused by factors like noise, attenuation and interference from other base station or other devices transmitting signals. In this thesis, channel measurements like RSSI, RSRP, Uplink power values are used to build the channel profile. The details of the method are discussed below:

Received Signal Strength Indicator

RSSI value can differ based on distance and power used to broadcast signal, in general, RSSI value can vary from -26 to -100 dBm depending on the distance and type of the device used for broadcasting the signal. RSSI is the measurement of the power of the received signal strength. The value measured can be influenced by factors like noise, interference, and attenuation. In this thesis, the setup described in Chapter 4 is been used and the system setup is depicted in Figure 3.1.

The channel measurements are recorded from two devices, one is eNodeB and other is from the UE. The device USRP B210 helps reading the received signal strength. Channel measurements are recorded from the moment UE gets connected to the network i.e to the Base Station (BS). The RSSI value measured is in terms of dBm which is the absolute number representing power levels in mW (milliwatts).

srsLTE software is used to build a LTE base station prototype. srsENB provides the feature where the user can record the metrics or view the metrics from the console by typing the command t while running the base station. The period of recording the measurement can be set in *eNodeB.conf* by setting the parameter *expert.metrics_period_secs*, regarding configuration, furthermore, the explanation can be found in Chapter 4. The measurements are recorded for every second, for building the channel profile and to maintain the variation in RSSI value measured.

On the other end, UE, srsUE package does provide the same facilities as srsENB, but unfortunately RSSI values are not calculated, so the RSSI values are not obtained from the

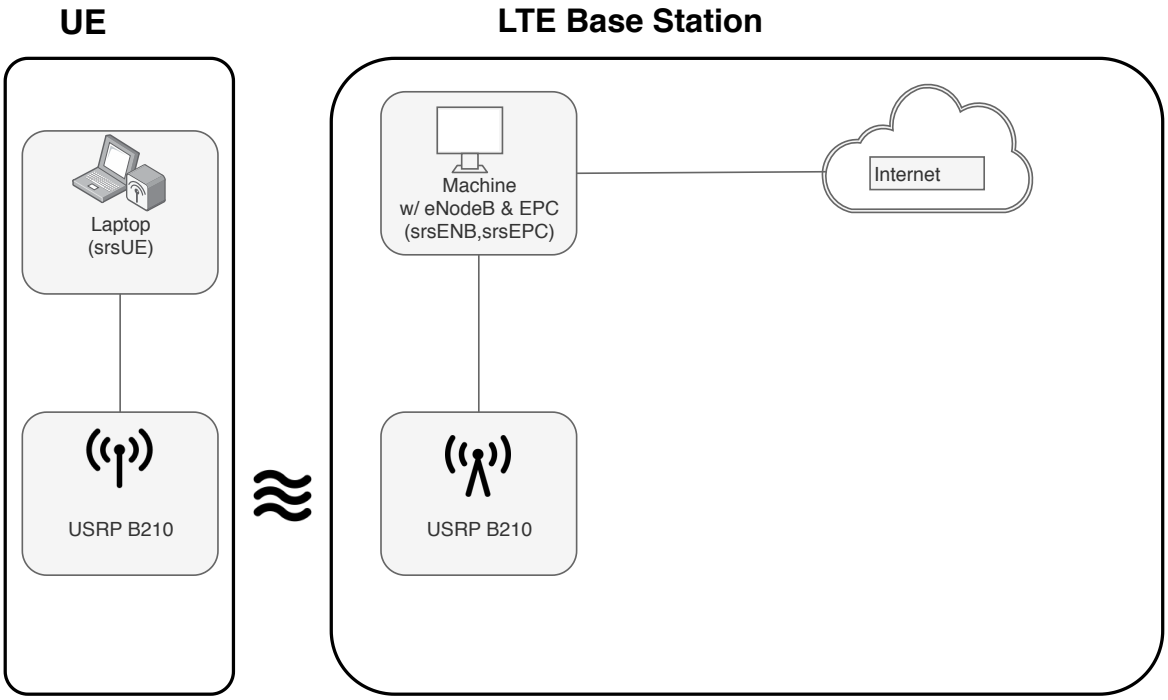

Fig. 3.1 LTE Testbed setup from [3]

tools given in the package. The codebase is modified accordingly, to calculate the RSSI values from USRP B210. srsUE code library has few radio functionalities, radio functions given in this library are used to derive the RSSI values from the same codebase. The RSSI values recorded from the modified codebase were not matching the values given by srsENB metrics trace, so similar changes were made in the codebase of srsENB to get related (adhering to reciprocity principle) RSSI measured from srsUE.

Referenced Signal Received Power

RSRP value can differ based on distance and power used to transmit signals. In general, RSRP value can vary from -40 to -150 dBm depending on the distance and type of the device used for broadcasting the signal. Although RSRP is a type of RSSI measurement, we consider it is better suited for channel profiling. The reason behind is the basic power measurement of signal sub-carrier excluding disturbing factors like noise and interference power. It is the power measurement of the signal resource element averaging the power received signal symbols within the narrow band. On the other hand, RSSI is a combination of noise, signal power, interference power and other factors, so RSRP channel profile is considered to be a good fit for channel profiling.

As discussed in the previous section of RSSI, srsENB provides the feature where user can record the metrics but the RSRP is not calculated by this feature, so some changes were made in the codebase of srsENB to calculate the RSRP.

To build another channel profile from srsUE, to generate the symmetric secret-key, srsUE provide the same feature to record the metrics and RSRP is pre-calculated from the srsUE package. On running the srsUE, the metrics are recorded in background for every second. The period of recording the measurement can be set in *ue.conf* by setting the parameter *expert.metrics_period_secs*, regarding configuration, furthermore, the explanation can be found in Chapter 4.

Uplink Power

The Channel profile built from RSSI and RSRP is from different channels, i.e. Uplink and Downlink channel. The noise ratio of the uplink channel and downlink channel may differ, which might be an obstacle to uphold the principle of reciprocity. The possibility of using one channel to build the channel profile is considered. Power used for transmission of the signal from User End and power received by eNodeB is measured to create two channel profiles, which have more reciprocity factor.

srsUE traces the metrics of the transmitted power used by UE to send the signal to eNodeB and the power values provided by srsUE is taken to build the channel profile. On the other hand, srsENB does not calculate the power received by the signal sent from srsUE. Estimated pilot power calculated by srsENB and converted to dBm metrics (unit of measurement in srsUE is also in dBm) is used to create channel profile on the srsENB side.

3.2.2 Enhancing Reciprocity

Usually, in other SKG methods, the channel profile is directly quantised to get the preliminary key and these keys tend to have more bit disagreement rate even though adhering to channel reciprocity principle. The enhancing reciprocity step is adapted to enhance the reciprocity of the channel profile, so the preliminary key produced after quantising step have less bit disagreement rate.

Two different methods adapted to enhance the reciprocity of the channel are:

- Discrete Cosine Transformation (DCT) Normalisation,
- AI-based with DCT normalisation;

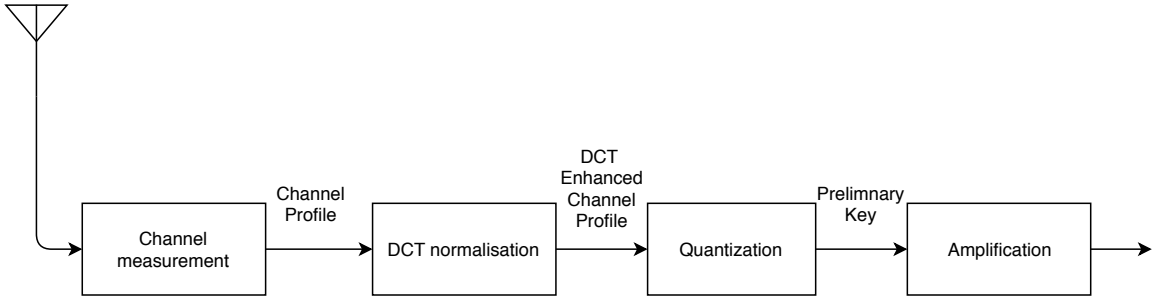

Fig. 3.2 Enhancing Reciprocity through DCT normalisation.

Discrete Cosine Transformation normalisation

DCT can be expressed as a series of finite cosine function oscillating at different frequencies. DCT uses real number and it Fourier transform similar to Discrete Fourier Transformation (DFT). DCT is twice the length of DFT and symmetric in nature. Its property is to transform the majority of the coefficient which represents energy sequence. Based on this property, DCT matrix is opted to enhance the channel profile.
The mathematical representation of the DCT can be written as:

$$y(k) = \sqrt{\frac{2}{N-1}} \sum_{n=1}^{N} x(n) \frac{1}{\sqrt{1+\delta_{n1}+\delta_{nN}}} \frac{1}{\sqrt{1+\delta_{k1}+\delta_{kN}}} \cos\left(\frac{\pi}{(N-1)}(n-1)(k-1)\right) \quad (3.1)$$

Where x is signal of length N, and with δ_{kl} the Kronecker delta [31]

The DCT matrix is obtained from image processing toolbox software, which is available in MATLAB. The function D = dctmtx(n) returns the (n x n) DCT matrix. The matrix (T_{pq}) is generated based on the below formula

$$T_{pq} = \begin{cases} \frac{1}{\sqrt{M}} & p = 0, 0 \le q \le M-1 \\ \sqrt{2/M} \cos \frac{\pi(2q+1)p}{2M} & 1 \le p \le M-1, 0 \le q \le M-1 \end{cases} \quad (3.2)$$

In this thesis, by using the above mentioned MATLAB function we generate DCT matrix Y of size (128x128). The size of the DCT matrix is set to (128x128) as the channel profile have 128 channel measurements and the end product that is enhanced channel profile should

have 128 enhanced channel measurements.

$$Y = dctmtx(128) = \begin{bmatrix} x_{1x1} & x_{1x2} & .... & x_{1x128} \\ x_{2x1} & x_{2x2} & .... & x_{2x128} \\ x_{3x1} & x_{3x2} & .... & x_{3x128} \\ ..... & ..... & ..... & ..... \\ ..... & ..... & ..... & ..... \\ x_{128x1} & x_{128x2} & .... & x_{128x128} \end{bmatrix} \tag{3.3}$$

Channel profile is converted into an array/matrix X of size (1x128).

$$X = \begin{bmatrix} x_{1x1} & x_{1x2} & .... & x_{1x128} \end{bmatrix} \tag{3.4}$$

The channel profile matrix X is multiplied with DCT matrix Y to obtain the product X'

$$X' = XY = \begin{bmatrix} x'_{1x1} & x'_{1x2} & .... & x'_{1x128} \end{bmatrix} \tag{3.5}$$

The matrix X' obtained is the new enhanced channel profile, which is later passed to amplification step as shown in Figure 3.2

AI-based Reciprocity Enhancement

LR is one of the supervised Machine Learning (ML) Algorithm. The LR model predicts based on the independent variable and the algorithm is based on finding the relationship between the dependent and independent variable. The LR model developed in this thesis predicts the average of eNodeB and UE. The designed model takes the values from eNodeB or UE channel profile and predicts the average of eNodeB and UE to create an enhanced profile. Since the channel profiles of eNodeB and UE adhere to the principle of Reciprocity property, the average predicted by both the models (eNodeB and UE) should be similar. From the above definition of Linear regression for currently developed model, the independent variable will be the values from eNodeB or UE channel profile and the dependent variable will be average of eNodeB and UE, i.e. the predicted value. The predicted values are used to build enhanced channel profiles for eNodeB and UE, which have more reciprocity and enhanced channel profile is passed to amplification stage to generate the final key as shown in Figure 3.3.

The sklearn package available in python is used to fit, standardize, train and predict the data. Apart from sklearn there are other packages to implement linear regression or it can be done from scratch. To understand the working of sklearn package, for better understanding

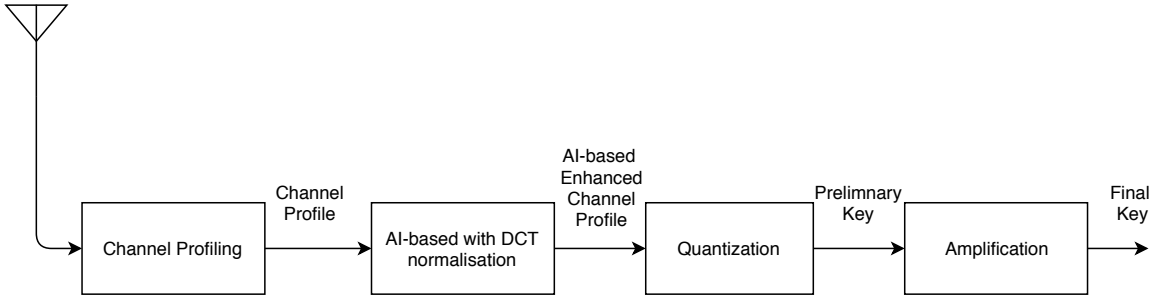

Fig. 3.3 AI-based with DCT normalisation Secret Key Generation.

of linear regression and its working, the concepts of linear regression and how LR is used to generate the enhanced profile have been discussed in below section .

The representation of linear equation is the combination of a set of inputs values X and predicted set of output values Y. A coefficient scale factor β_0 and another coefficient β_1, called the bias coefficient which gives the degree of freedom to the equation, is assigned to a linear equation. For simple regression, the formula can be represented as

$$Y = \beta_0 + \beta_1 X \tag{3.6}$$

The values of β_0 and β_1 are really important to predict the Y. To get the best-fit, cost function is used, cost function J is sort of minimization problem where it tries to minimize the error between the predicted and actual value. The mathematical representation of the cost function is given below

$$\min \frac{1}{n} \sum_{i=1}^{n} (X_i - Y_i)^2 \tag{3.7}$$

$$J = \frac{1}{n} \sum_{i=1}^{n} (X_i - Y_i)^2 \tag{3.8}$$

The difference between ground truth and the predicted value is termed as error difference. The error difference is squared and summed all over the data values and divided by the total number of data values which provides the average squared error and is commonly known as Mean Squared Error (MSE) in Machine Learning (ML) terms. With help of MSE, the values of β_0 and β_1 are changed to find the best fit of the linear regression model. Gradient descent method is used to reduce the MSE value and find the best fit for β_0 and β_1. β_0 and β_1 are changed iteratively to reduce the cost. Gradient descent also helps on how to change the values of β_0 and β_1.

The data have to be prepossessed before training the LR model to have a more accurate prediction. The channel profile data is not linearly distributed but it is more complex, the distribution of data in the channel profile is shown in Figure 3.4, the data of eNodeb is

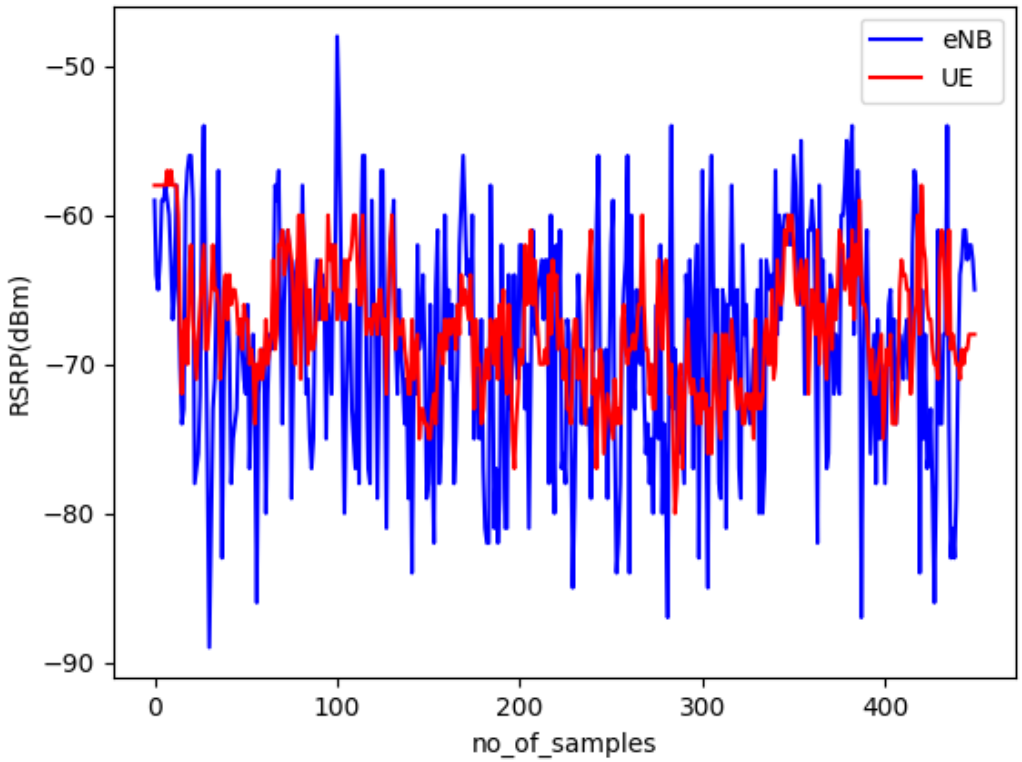

Fig. 3.4 Data distribution in eNodeB and UE channel profile

represented in blue and the data of UE is represented in red, even though the data distributed is reciprocal in nature but there are spikes in eNodeb data which has to be normalised. Initially, the data features are normalized and standardized using the *StandardScaler* and *PolynomialFeatures* function available in *sklearn.preprocessing* package. Linear features can not fit the data and so the data lies in underfitting state, which means that the Linear Regression linear model cannot be used. So the degree of the equation of linear regression is increased in Equation 3.9 to overcome the underfitting state and to fit more data. To generate higher order of equation or complexity of the model, additional power is added to original features to add as new features, the transformed equation for polynomial regression would be

$$Y = \beta_0 + \beta_1 X + \beta_2 x^2 + ... + \beta_n x^n \tag{3.9}$$

Although the curve fitting, is polynomial in nature, the model remains linear as the coefficients associated are linear.

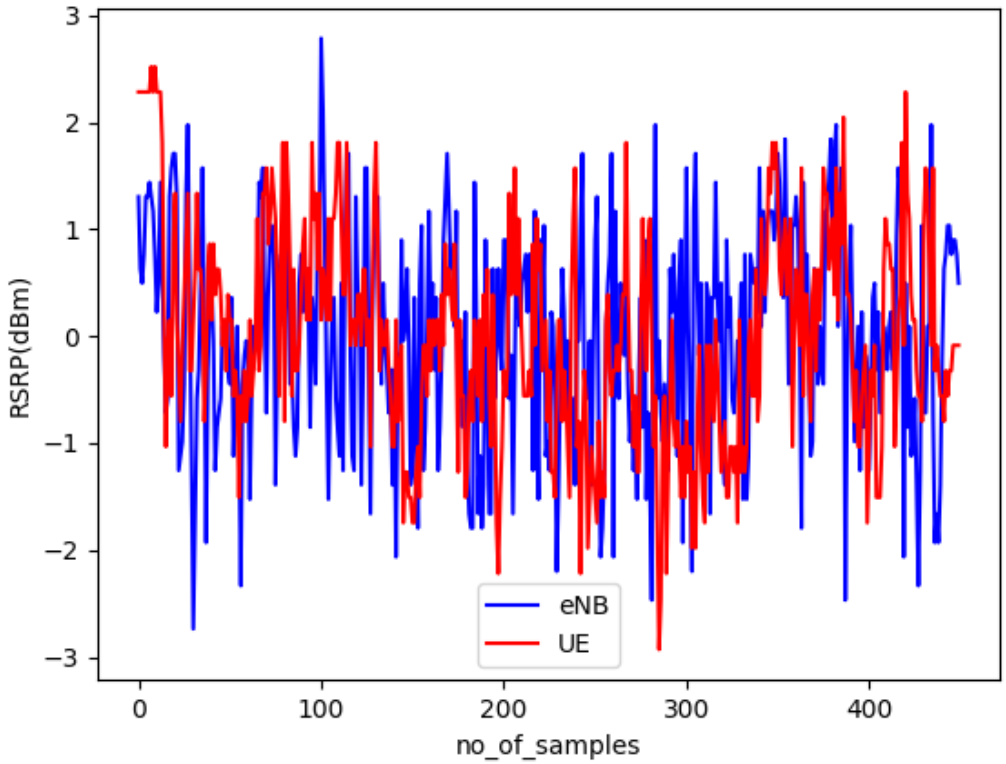

Fig. 3.5 Data distribution in eNodeB and UE channel profile after applying Scaler transformation function

The advantage of using polynomial feature is, that it gives the best approximation of the relationship between the dependent and independent variable with a broad range of function fitting under it but the presence of outliers can damage the learning process of model, which might result in inaccurate prediction. So the outliers are removed by using the *StandardScaler.fit_transform* function which removes the mean and scaled to unit variance. The standard score of a sample is calculated as:

$$score = (sample - mean)/standard\_deviation$$

where *mean* is the mean of the training samples and *standard_deviation* is the standard deviation of the training samples. Learning algorithm might behave badly if the individual features do not look like normally distributed data so standardization is considered to be a common requirement for learning algorithms. The transformed data, as shown in Figure 3.5 is now normally distributed and is compressed to be between -1 to 1 but still the spikes exists in data distributed. The normalised data is then transformed using *PolynomialFea-*

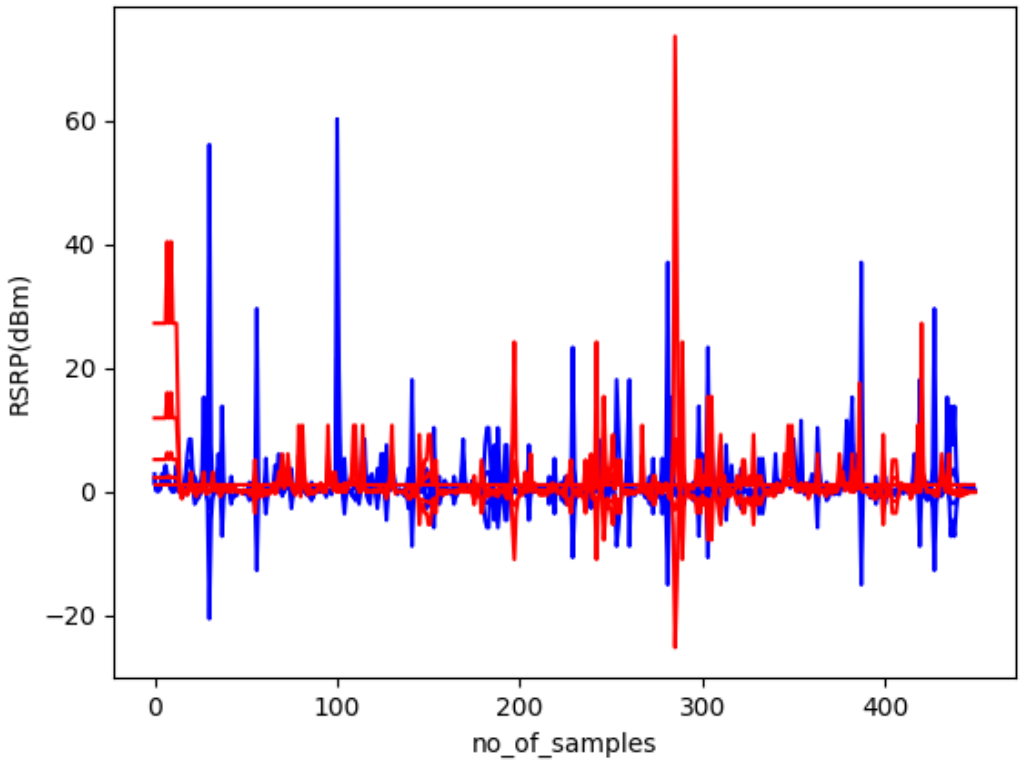

Fig. 3.6 Data distribution in eNodeB and UE channel profile after applying polynomial transformation function

tures(degree=n).fit_transform(data) function to fit the data in curve and the data distribution after standardising looks as shown in Figure 3.6. The value of the degree has to be varied to fit the data in the curve. Low degree value might result in under-fit state and high degree value might result is over-fit state so the degree value has too varied accordingly to fit the data in the curve.

After pre-processing the raw data from the channel profile, the model is trained with the processed data. *sklearn.linear_model* package allows to use the LR model. Model is trained with ground truth values that is pre-processed channel measurements and the average of eNodeB and UE for the current eNodeB value given, to the train the model.

The trained model is used to predict the average for the new test data. The test data or in real data has to be pre-processed in the same manner done for training data to get more accurate and proper results. Predicted data is then de-normalised using *Standard-Scaler.inverse_transform* function, to get the result in the original format. The de-normalized data still have spikes in the channel variation measurements as the model does not normalises

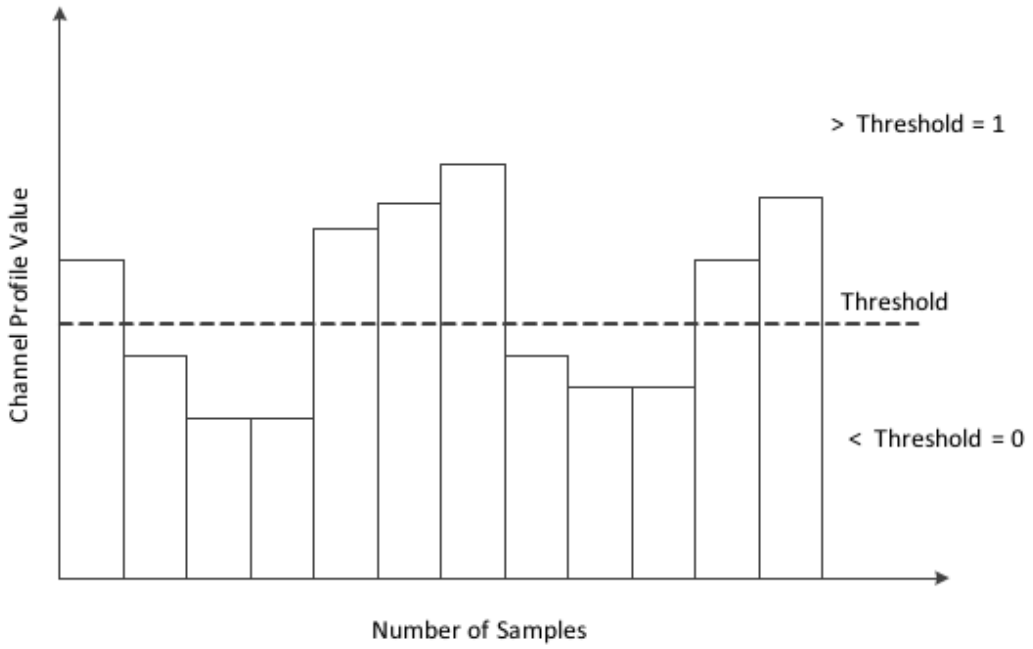

Fig. 3.7 Binary quantisation

the spikes in the measurement, because the model just predicts the spikes if the channel measurement is having the spikes in the measurement measured and the data spikes are normalised by multiplying the channel profile got from LR model with DCT matrix which was discussed in previous section and the product is than used to generate an enhanced channel profile.

3.2.3 Quantisation

As discussed in the previous chapter, the enhanced channel profile is quantised to create the preliminary key and two types of quantisation methods are used, namely lossy and lossless quantisation. Lossless quantisation method is adopted in this thesis, to generate the preliminary secret key. Furthermore, lossless block quantisation and lossless non-block quantisation are implemented.

In block quantisation, the channel profile is divided into a specific size of blocks and each block is processed separately and quantised to generate the key. In normal or non-block quantisation the whole channel profile is considered and processed to generate the preliminary key.

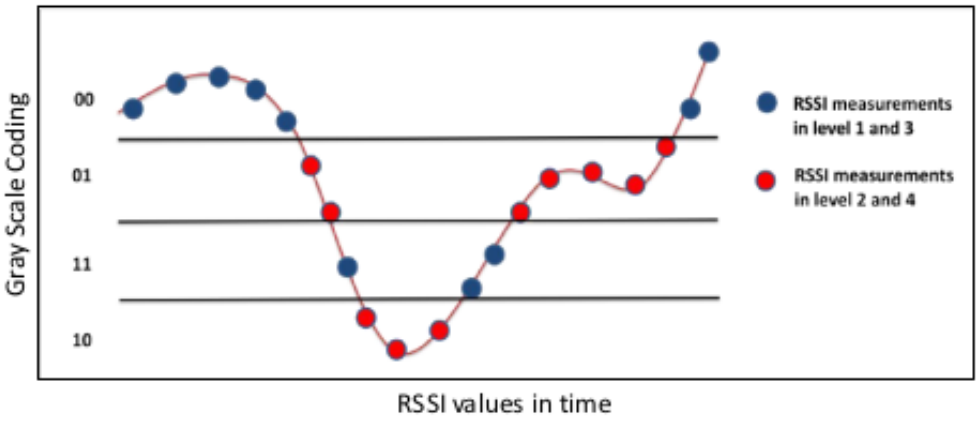

Fig. 3.8 Adaptive Quantisation

To quantise the channel profile, the threshold value is considered, which can be of one level or more levels. For one level of the threshold, the mean or median of the whole or block of the channel profile acts as a threshold based on the block or whole quantisation. Single level threshold quantisation is referred to as binary quantisation. Figure 3.7 gives a more clear picture of binary quantisation. The values above the threshold are assigned with binary value 0 or 1 and vise verse for values below the threshold.

For multi-level quantisation, there are more than one threshold values. In this thesis, different methods are used to choose the threshold values. Statistics values like mean, standard deviation and variance are used to calculate the threshold values for different levels. For each level unique binary value like 00,01,10,11 is assigned.

The formula for threshold values for different level based on mean and standard deviation is given below:

- Level 1 = [$-\infty$, mean - (deviation * standard_deviation)]
- Level 2 = [mean - (deviation * standard_deviation), mean]
- Level 3 = [mean, mean + (deviation * standard_deviation)]
- Level 4 = [mean + (deviation * standard_deviation), ∞]

The formula for threshold values for different level based on mean and variance is given below:

- Level 1 = [$-\infty$, mean - variance/2]

- Level 2 = [mean - variance/2, mean]
- Level 3 = [mean, mean + variance/2]
- Level 4 = [mean + variance/2, ∞]

The order of the level need not be the same but can be arranged differently also. Figure 3.8 portrays the idea of multi level quantisation in brief. This sort of quantisation is also referred to as adaptive quantisation.

Adaptive and binary quantisation for block and normal/normal quantisation, which gives six varieties of quantisation option to quantise the enhanced channel profile to generate the secret key.

3.2.4 Privacy Amplification

In this thesis for privacy amplification step, Secure Hashing Algorithm-3 (SHA-3) is used. SHA-3 was designed by the United States National Security Agency as a Federal Information Processing Standard. The algorithm takes input and produces arbitrary hash value which is also referred to as a message digest. This algorithm produces unique and irreversible hash value, that means the input cannot be predicted based on the hash value and every input produces a different and unique hash value. These properties help us to produce the unique and unpredictable secured secret key based on the preliminary key generated from the quantisation step. The hashlib package available in python is used to hash the key using different algorithms available.

3.3 Evaluation

Once the key generated for different reciprocity enhanced channel profile, the keys of eNodeb and UE are evaluated by checking the number of bits disagreed between the eNodeb and UE key and entropy of the keys are calculated using Shannon's entropy method. The number of disagreed bits are calculated by XOR'ing the two keys i.e. eNodeb and UE keys. Entropy is measure of unpredictability of the state. The Shannon entropy is represented in form of Equation 3.10

$$H = -\sum_{i} p_i \log_b p_i \tag{3.10}$$

Where p_i is the probability of the character appearing the given stream , in this thesis it would be the probability of bit(0,1) occurring in the secret key generated after quantising.

4. Long Term Evolution Testbed

The prototype for the method discussed in the previous Chapter, is been explained in this Chapter. This Chapter gives the details of the software and hardware used to set up the testbed and their requirements and dependencies. Conditions for the mobile and static environment is discussed in this Chapter.

4.1 Design and Implementation of testbed

The testbed consists of a one PC, one laptop, two USRP B210 device. The Figure 4.2 depicts the testbed, that is been used in this thesis. The laptop and PC have Intel i5 CPU at 2.30 GHz and 8GB of RAM and runs on Ubuntu 18.04 Operating system. The USRP B210 (Figure 4.1) is fully integrated, a single board with frequency coverage from 70 MHz - 6 GHz, single-chip direct-conversion transceiver capable of streaming up to 56 MHz of real-time RF bandwidth. The UHD driver is essential to use USRP and version 3.13.0.1 UHD driver has been installed in machine(PC/Laptop). USRP B210 is interfaced with PC through USB 3.0. In Figure 4.2, the right part shows the LTE base station where srsENB and srsEPC are running in same machine and left part is UE, where srsUE is running to act as UE and it is connected to USRP B210 which acts transceiver for UE

srsLTE is free open source LTE software suite developed by Software Radio Systems, In this testbed, we use srsENB and srsEPC. srsLTE has been built and installed in one PC and so we operate EPC and eNodeb under one PC. Once srsLTE is installed, variables like Mobile Country Code (MCC) and Mobile Network Code (MNC) in configuration files like enb.conf, epc.conf are to be modified based on USIM(Universal Subscriber Identity Module) configuration to get connected to the virtual base station's network. The software and hardware requirement to setup the srsLTE is been discussed below.

Fig. 4.1 USRP B210

4.1.1 srsLTE setup

As discussed in Chapter 2, srsLTE software suite contains the SRSUE, srsENB and srsEPC. Setup and configuration of each component of srsLTE are discussed below. The srsLTE software suite has some mandatory requirements to be followed before installation. The softwares like cmake, libfftw, PolarSSL/mbedTLS, Boost, lksctp and config should be pre installed to support the build of srsLTE suite and this can be done by running the command below:

```
sudo apt-get install cmake libfftw3-dev libmbedtls-dev
libboost-program-options-dev libconfig++-dev libsctp-dev
```

srsLTE library deals with buffers of samples in system memory, thus it is able to work with any RF front-end. It currently provides interfaces to the Universal Hardware Driver (UHD), giving support to the Ettus USRP family of devices like USRP B210, USRPB205mini, USRP X300 and other RF's like limeSDR and bladeRF. Before setting up the srsENB, UHD constitutes the necessary hardware equipment for the implementation of srsUE and srsENB, so the details of UHD driver setup is given below.

UHD driver setup

The following steps have to be implemented in both machines in which you plan to run the srsENB and srsUE. Following dependencies have to be installed to support the installation of UHD driver with the command below:

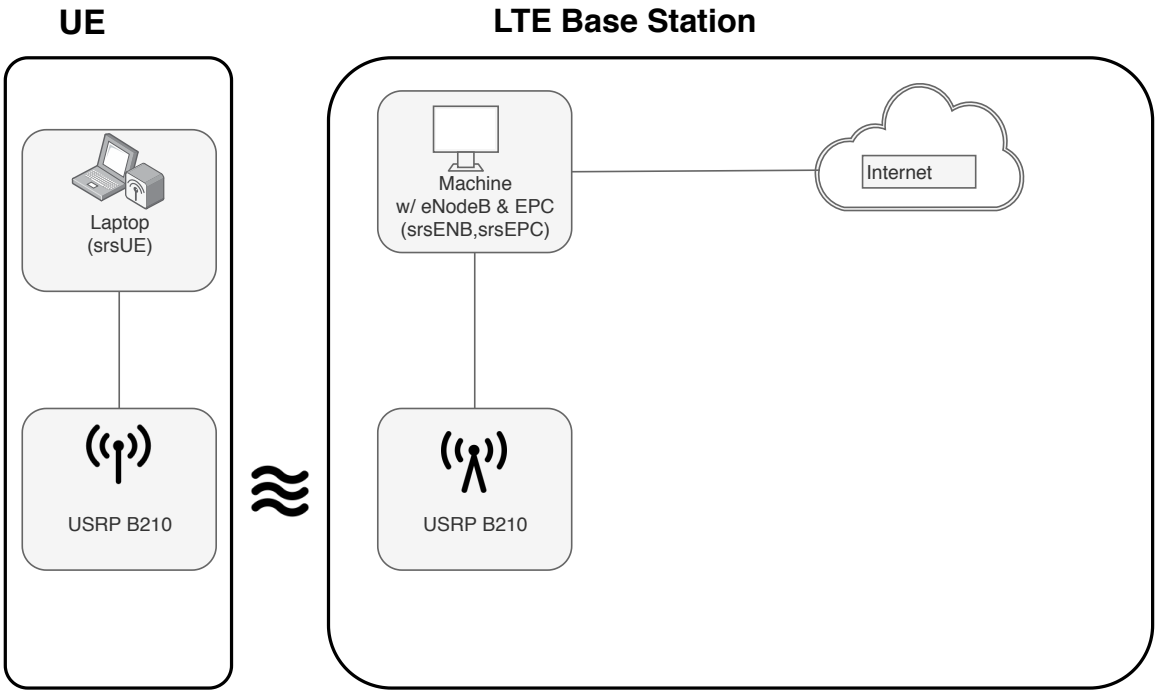

Fig. 4.2 LTE Testbed

```
sudo apt-get install libboost-all-dev libusb-1.0-0-dev python-mako
doxygen python-docutils cmake build-essential
```

The source code of UHD driver can be obtained from Git repository [32]. Once the source code is downloaded, change it to the required version, in this thesis, version 3.13.0.1 is been used. To generate makefiles of UHD, following commands have to be executed.

```
cd <uhd-repo-path>/host
mkdir build
cd build
cmake ../
```

After generating makefiles, to build and install UHD drivers , run the below commands

```
make
make test
sudo make install
```

On successful installation of UHD driver, library path for UHD have to be set, this can be done by running

```
sudo ldconfig
```

Fig. 4.3 VERT2450-Antenna

srsENB and srsEPC setup

To install eNodeb and EPC above mentioned dependencies have to be installed before the installation of EPC and eNodeb. And the machine on which eNodeb and EPC are going to be installed should have Linux based operating system running and RF device should be connected to the machine via USB3 port and suitable antennas. In this thesis VERT2450 antennas (Figure 4.3) are used which supports dual-band 2.4 to 2.48 GHz and 4.9 to 5.9 GHz and are Omni-directional vertical antenna with 3dBi gain. As srsENB is designed to run on user-space, for better performance CPU frequency scaling is disabled(which is optional) and this is done by running the below script

```
for f in /sys/devices/system/cpu/cpu[0-9]*/cpufreq/scaling_governor ; do
    echo performance > $f
done
```

srsEPC and srsENB can be installed in a different machine or in a single machine, in this thesis only one machine is used to install srsENB and srsEPC.

Run the below commands to install srsENB and srsEPC in one machine.

```
git clone https://github.com/srsLTE/srsLTE.git
cd srsLTE
mkdir build
cd build
cmake ../
make
make test (optional)
sudo make install (This installs the whole suite which includes
srsEPC, srsENB and srsUE)
sudo srslte_install_configs.sh
```

All the default srsLTE config files are copied to user's home directory *~/.srs*.

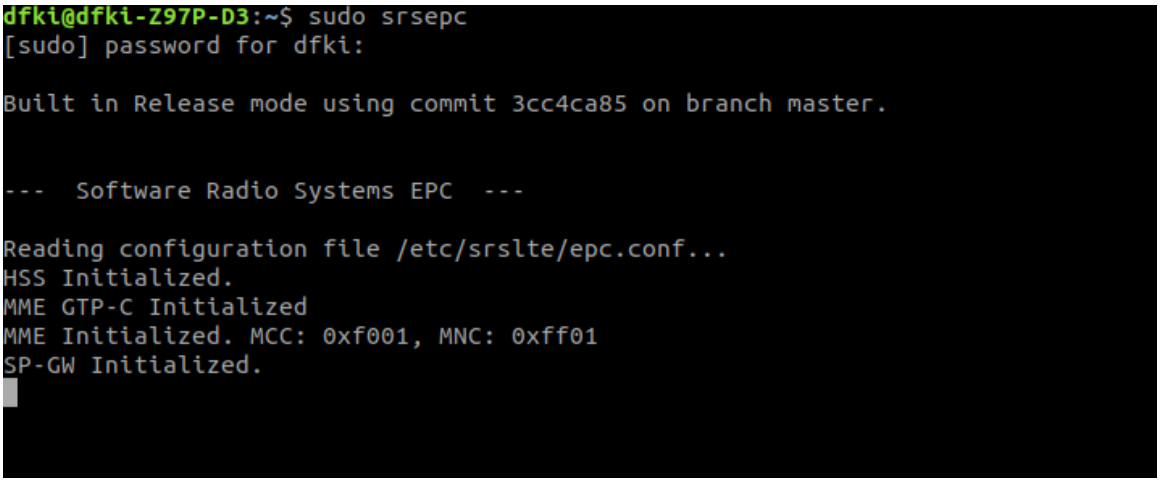

Fig. 4.4 srsEPC start

Configuring srsENB and srsEPC

The srsEPC can be configured through the *epc.conf* configuration file which is available in the home directory after installing srsLTE. The parameters like MCC, MNC, Access Point Name (APN), DNS address can be configured as per requirement in MME configuration section and authentication algorithm in HSS section and SGi IP address, GTP-U bind address in SPGW section of epc.conf.

The srsEPC can be configured through the *enb.conf* configuration file which is available in the home directory after installing srsLTE. The parameters like cell configuration, frequencies, power levels, and other parameters can be configured as per requirement. Apart from above mentioned parameters, high-level parameters can be configured through sib.conf, rr.conf(radio resource), drb.conf(data bearers) files present in the same home directory.

If srsEPC and srsENB are being installed in a single machine then there are no configuration changes to be done with respect to eNodeb and EPC connection, the default configuration will suffice to run both eNodeb and EPC. If EPC and eNodeb are installed in the different machine then *mme_bind_addr* which specifies where the MME will listen for eNodeb S1AP connections and *gtpu_bind_addr* should be the same as MME bind address. To run on user plane on a different subnet then the S1AP connection address will be same as GTPU bind address.

Running the Base station

In this thesis, srsENB and srsEPC are built and installed in one machine, so the default configurations of the srsLTE are taken to run the eNodeb and EPC. First, start the EPC and then eNodeb. On running the below command in machine 1, EPC will start running with

configurations saved in epc.conf file and initializing the MME, HSS, SP-GW as shown in Figure 4.4.

```
sudo srsepc
```

With the configuration given, EPC creates a virtual network interface *srs_spgw_sgi* with 172.16.0.1 IP address(using the default configurations).

When srsEPC gets connection request from srsENB and srsUE, EPC creates the session and verifies the UE number, IMSI and other details with UE, once the verification is complete, EPC(SP-GW) allocates IP address to the UE starting from 172.16.0.2 Figure 4.5

Open another console to run the srseNB with below command

```
sudo srsenb
```

srsENB starts running with default configurations saved in enb.conf, initialises the CODEC, radio control and set the clock frequency and start the cell with the predefined band in configuration file, as shown in Figure 4.6

. On connecting to UE, srsENB directs the UE details to EPC for verification, once the UE is verified eNodeb gets connected to UE and assign radio network temporary identifier as shown in Figure 4.7.

srsUE setup

On Machine 2 i.e. laptop in this thesis, srsUE will be set up, all the dependencies mentioned above in srsENB block should also be installed in machine 2. USRP B210 has to be connected to machine 2 via USB3 and for better performance frequency scaling can be disabled. Machine 2 should be running on Linux based operating system and srsUE can be installed from running the below code:

```
sudo add-apt-repository ppa:srslte/releases
sudo apt-get update
sudo apt-get install srsue
```

After successful installation of the srsUE, the configuration files are stored in the home directory. The configuration file ue.conf helps configure the UE and provides parameters relating to frequencies, transmit power levels, USIM properties, logging level, and many other related settings. In this thesis, default configurations have been used with dl_earfcn set to 3400 where the uplink frequency is 2565MHz and downlink frequency is 2865MHz, as shown in Figure 4.8.

```
S1 Setup Request - MCC:001, MNC:01, PLMN: 61712
S1 Setup Request - TAC 7, B-PLMN 0
S1 Setup Request - Paging DRX 2
Sending S1 Setup Response
Initial UE message: LIBLTE_MME_MSG_TYPE_ATTACH_REQUEST
Received Initial UE message -- Attach Request
Attach request -- GUTI Style Attach request
Attach request -- M-TMSI: 0x1423c9fc
Attach request -- eNB-UE S1AP Id: 1
Attach request -- Attach type: 1
Attach Request -- UE Network Capabilities EEA: 11100000
Attach Request -- UE Network Capabilities EIA: 01100000
Attach Request -- MS Network Capabilities Present: false
PDN Connectivity Request -- EPS Bearer Identity requested: 0
PDN Connectivity Request -- Procedure Transaction Id: 1
PDN Connectivity Request -- ESM Information Transfer requested: false
UL NAS: Received Identity Response
ID Response -- IMSI: 001010123456789
Downlink NAS: Sent Authentication Request
UL NAS: Received Authentication Response
Authentication Response -- IMSI 001010123456789
UE Authentication Accepted.
Generating KeNB with UL NAS COUNT: 0
Downlink NAS: Sending NAS Security Mode Command.
UL NAS: Received Security Mode Complete
Security Mode Command Complete -- IMSI: 001010123456789
Getting subscription information -- QCI 7
Sending Create Session Request.
Creating Session Response -- IMSI: 1010123456789
Creating Session Response -- MME control TEID: 1
SPGW: Allocated Ctrl TEID 1
SPGW: Allocated User TEID 1
SPGW: Allocate UE IP 172.16.0.2
Received Create Session Response
Create Session Response -- SPGW control TEID 1
Create Session Response -- SPGW S1-U Address: 127.0.1.100
SPGW Allocated IP 172.16.0.2 to ISMI 001010123456789
Adding attach accept to Initial Context Setup Request
Initial Context Setup Request -- eNB UE S1AP Id 1, MME UE S1AP Id 1
Initial Context Setup Request -- E-RAB id 5
Initial Context Setup Request -- S1-U TEID 0x1. IP 127.0.1.100
Initial Context Setup Request -- S1-U TEID 0x1. IP 127.0.1.100
Initial Context Setup Request -- QCI 7
Received Initial Context Setup Response
E-RAB Context Setup. E-RAB id 5
E-RAB Context -- eNB TEID 0x470003; eNB GTP-U Address 127.0.1.1
UL NAS: Received Attach Complete
Unpacked Attached Complete Message. IMSI 1010123456789
Unpacked Activate Default EPS Bearer message. EPS Bearer id 5
Sending EMM Information
```

Fig. 4.5 srsEPC Connected to srsENB and srsUE

```
[sudo] password for dfki:

Built in Release mode using commit 3cc4ca85 on branch master.

---  Software Radio Systems LTE eNodeB  ---

Reading configuration file /etc/srslte/enb.conf...
[INFO] [UHD] linux; GNU C++ version 7.3.0; Boost_106501; UHD_3.13.1.0-release
Opening USRP with args: type=b200,master_clock_rate=30.72e6
[INFO] [B200] Detected Device: B210
[INFO] [B200] Operating over USB 3.
[INFO] [B200] Initialize CODEC control...
[INFO] [B200] Initialize Radio control...
[INFO] [B200] Performing register loopback test...
[INFO] [B200] Register loopback test passed
[INFO] [B200] Performing register loopback test...
[INFO] [B200] Register loopback test passed
[INFO] [B200] Asking for clock rate 30.720000 MHz...
[INFO] [B200] Actually got clock rate 30.720000 MHz.
Setting frequency: DL=2125.0 Mhz, UL=1725.0 MHz
[INFO] [B200] Asking for clock rate 11.520000 MHz...
[INFO] [B200] Actually got clock rate 11.520000 MHz.
Setting Sampling frequency 11.52 MHz

==== eNodeB started ===
Type <t> to view trace
```

Fig. 4.6 srsENB start

```
Built in Release mode using commit 3cc4ca85 on branch master.

---  Software Radio Systems LTE eNodeB  ---

Reading configuration file /etc/srslte/enb.conf...
[INFO] [UHD] linux; GNU C++ version 7.3.0; Boost_106501; UHD_3.13.1.0-release
Opening USRP with args: type=b200,master_clock_rate=30.72e6
[INFO] [B200] Detected Device: B210
[INFO] [B200] Operating over USB 3.
[INFO] [B200] Initialize CODEC control...
[INFO] [B200] Initialize Radio control...
[INFO] [B200] Performing register loopback test...
[INFO] [B200] Register loopback test passed
[INFO] [B200] Performing register loopback test...
[INFO] [B200] Register loopback test passed
[INFO] [B200] Asking for clock rate 30.720000 MHz...
[INFO] [B200] Actually got clock rate 30.720000 MHz.
Setting frequency: DL=2125.0 Mhz, UL=1725.0 MHz
[INFO] [B200] Asking for clock rate 11.520000 MHz...
[INFO] [B200] Actually got clock rate 11.520000 MHz.
Setting Sampling frequency 11.52 MHz

==== eNodeB started ===
Type <t> to view trace
RACH:  tti=7111, preamble=0, offset=8, temp_crnti=0x46
Invalid field access for choice type "c1" ("measurementReport"!="rrcConnectionSetupComplete")
Invalid field access for choice type "c1" ("measurementReport"!="ulInformationTransfer")
Invalid field access for choice type "c1" ("measurementReport"!="ulInformationTransfer")
Invalid field access for choice type "c1" ("measurementReport"!="ulInformationTransfer")
Invalid field access for choice type "c1" ("measurementReport"!="securityModeComplete")
Invalid field access for choice type "c1" ("measurementReport"!="rrcConnectionReconfigurationComplete")
User 0x46 connected
```

Fig. 4.7 srsENB on connecting to UE

```
#####################################################################
[rf]
dl_earfcn = 3400
freq_offset = 0
tx_gain = 80
rx_gain = 40

#nof_rx_ant = 1
#device_name = auto
#device_args = auto
#time_adv_nsamples = auto
#burst_preamble_us = auto
#continuous_tx     = auto


#####################################################################
```

Fig. 4.8 EARFCN configuration in ue.conf file

Running the srsUE

To run the srsUE below command have to be executed on machine 2 with USRP B210 connected via USB3 port.

```
sudo srsue
```

On executing the srsUE starts searching for the cell (as shown in Figure 4.9)with configured *dl_earfcn* as shown Figure 4.8 On connecting to the basestation, srsUE creates *tun_srsue*, a virtual network interface on machine 2 with 172.16.0.X IP in the network as shown in Figure 4.10

4.2 Environment

In this thesis, the methods discussed in Chapter 3, as shown in figure 4.11 are put into real world prototype and tested in two environments:

- Static Environment (SE)
- Mobile Environment (ME)

4.2.1 Static Environment

In a SE the base station and UE are kept in stationary position with certain distance apart. As shown in Figure 4.12.

```
Reading configuration file /home/sachin/.srs/ue.conf...

Built in Release mode using commit 3d9baebf on branch agent.

---  Software Radio Systems LTE UE  ---

Opening RF device with 1 RX antennas...
[INFO] [UHD] linux; GNU C++ version 7.4.0; Boost_106501; UHD_3.14.0.HEAD-0-g6875d061
Opening USRP with args: type=b200,master_clock_rate=30.72e6
[INFO] [B200] Detected Device: B210
[INFO] [B200] Operating over USB 3.
[INFO] [B200] Initialize CODEC control...
[INFO] [B200] Initialize Radio control...
[INFO] [B200] Performing register loopback test...
[INFO] [B200] Register loopback test passed
[INFO] [B200] Performing register loopback test...
[INFO] [B200] Register loopback test passed
[INFO] [B200] Asking for clock rate 30.720000 MHz...
[INFO] [B200] Actually got clock rate 30.720000 MHz.
Waiting PHY to initialize...
...
Attaching UE...
Searching cell in DL EARFCN=2100, f_dl=2125.0 MHz, f_ul=1725.0 MHz
............
```

Fig. 4.9 UE Cell search

```
Reading configuration file /home/sachin/.srs/ue.conf...

Built in Release mode using commit 3d9baebf on branch agent.

---  Software Radio Systems LTE UE  ---

Opening RF device with 1 RX antennas...
[INFO] [UHD] linux; GNU C++ version 7.4.0; Boost_106501; UHD_3.14.0.HEAD-0-g6875d061
Opening USRP with args: type=b200,master_clock_rate=30.72e6
[INFO] [B200] Detected Device: B210
[INFO] [B200] Operating over USB 3.
[INFO] [B200] Initialize CODEC control...
[INFO] [B200] Initialize Radio control...
[INFO] [B200] Performing register loopback test...
[INFO] [B200] Register loopback test passed
[INFO] [B200] Performing register loopback test...
[INFO] [B200] Register loopback test passed
[INFO] [B200] Asking for clock rate 30.720000 MHz...
[INFO] [B200] Actually got clock rate 30.720000 MHz.
Waiting PHY to initialize...
...
Attaching UE...
Searching cell in DL EARFCN=2100, f_dl=2125.0 MHz, f_ul=1725.0 MHz
.....................
Found Cell:  PCI=1, PRB=50, Ports=1, CFO=6.2 KHz
[INFO] [B200] Asking for clock rate 11.520000 MHz...
[INFO] [B200] Actually got clock rate 11.520000 MHz.
Found PLMN:  Id=00101, TAC=7
Random Access Transmission: seq=8, ra-rnti=0x2
Random Access Complete.     c-rnti=0x46, ta=8
RRC Connected
Network attach successful. IP: 172.16.0.2
Software Radio Systems LTE (srsLTE)
```

Fig. 4.10 UE connected to Basestation

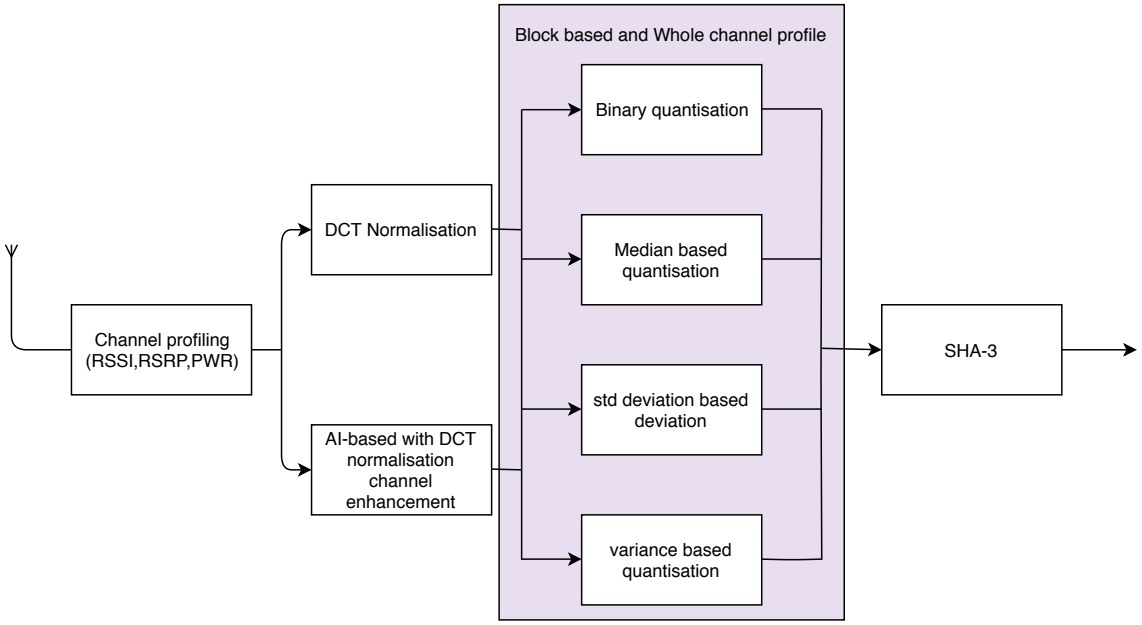

Fig. 4.11 Secret Key generation methods summarised

The BS (eNodeb - machine 1) and UE (Laptop) are connected to USRP B210 and positioned at distance of 1, 2 and 5 meters to each other, antennas of UE and eNodeb are in line of sight to each other and the environment is induced with noise with some Bluetooth devices and the channel measurements are recorded for every second after UE is connected to base station.

4.2.2 Mobile environment

In the ME, the base station is in a static position and UE is moved around the base station within room space using iRobot ROOMBA vacuum cleaner to create irregular patterns of movement, the room space and devices used are shown in Figure 4.13. Similar to the SE, eNodeb-machine 1 and UE-Laptop is connected to USRP B210 via USB3 port, antennas of UE and eNodeb are in the line of sight to each other and the environment is induced with noise with some Bluetooth devices and the channel measurements are recorded for every second after UE is connected to the base station.

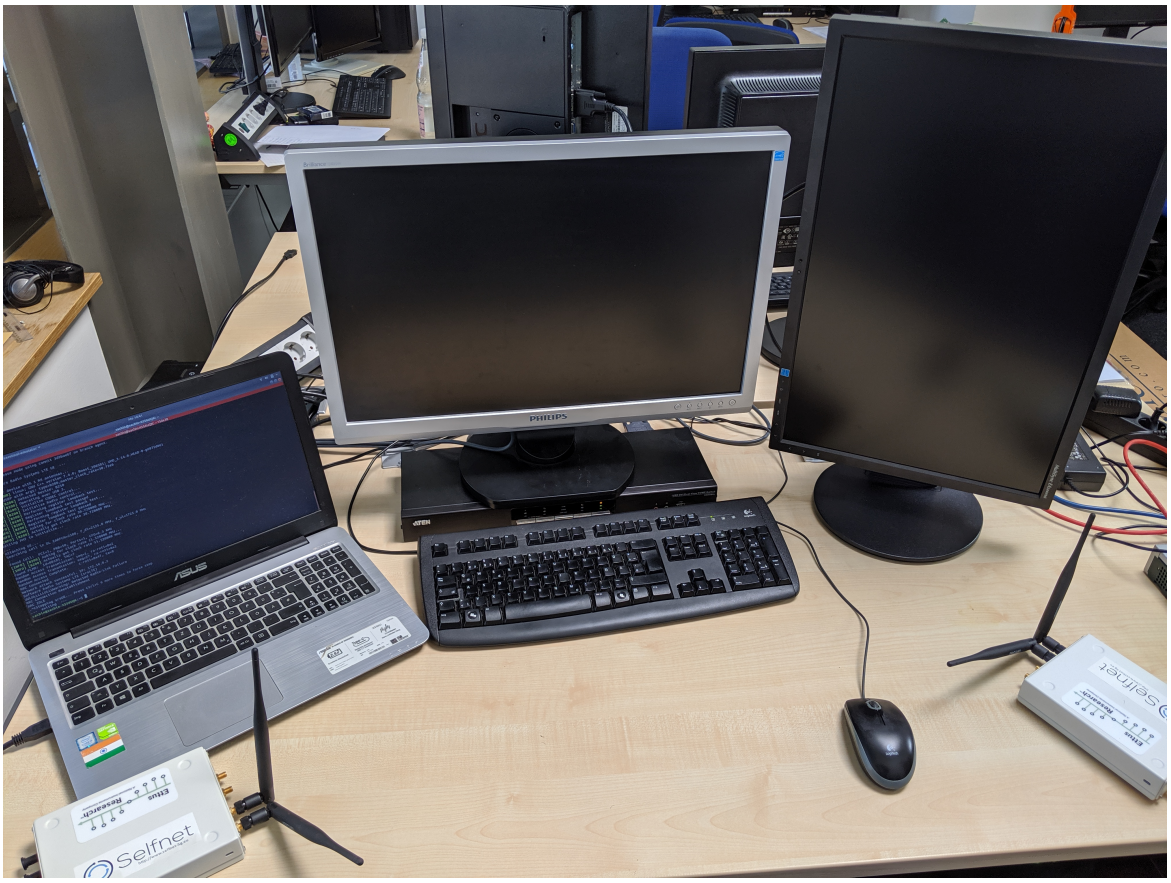

Fig. 4.12 Static Environment

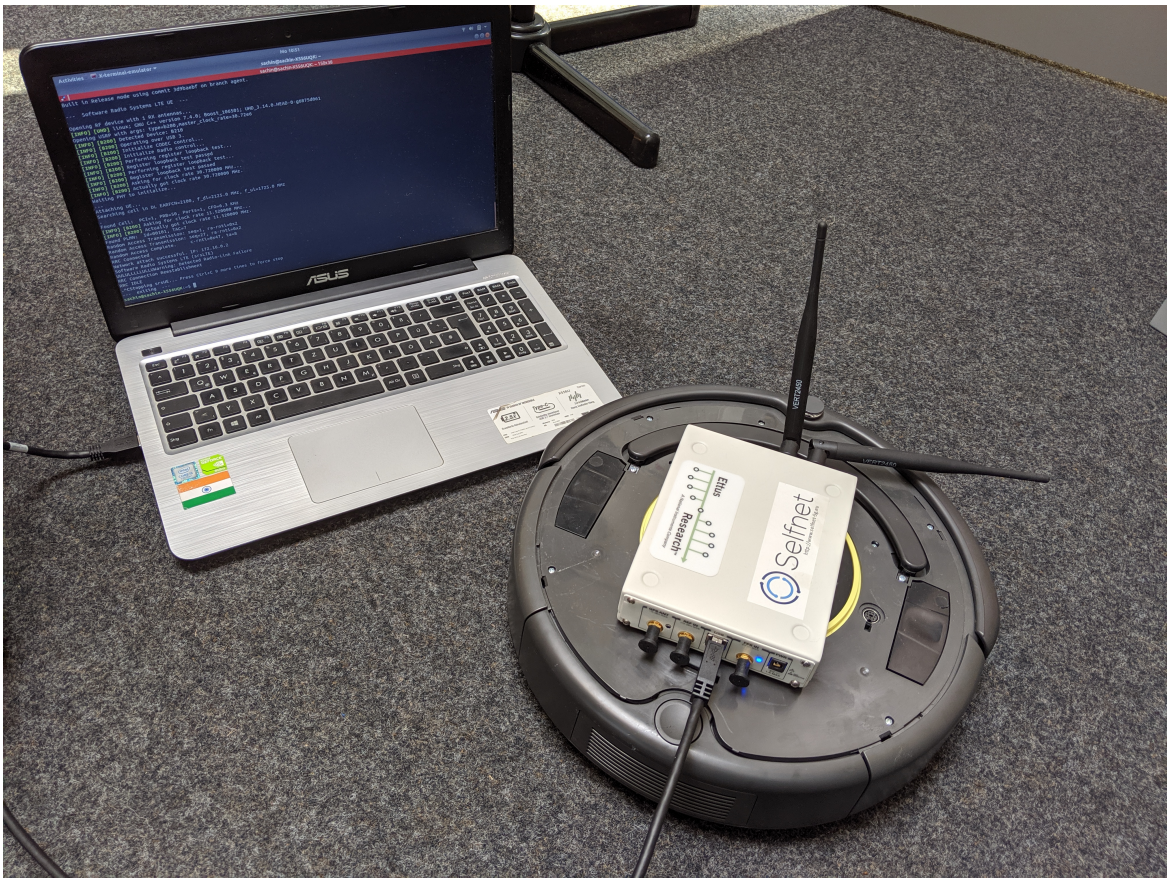

Fig. 4.13 Mobile Environment

5. Results and Evaluation

As described in the Figure 2.2, different channel profiles are enhanced using DCT normalisation and by using Linear Regression model, enhanced profiles are quantised by blocks and non block using lossless quantisation methods with different statistical parameters like mean, standard deviation, variation as threshold to convert the measured channel values into binary values. Lastly, the possibility of predicting the preliminary secret key generated from quantisation method is reduced by hashing the preliminary key with SHA-3 algorithm in privacy amplification stage.

In this chapter, the results of the methods discussed in Chapter 3 for SKG are discussed. Evaluation of the secret key generated is done by measuring the disagreement of bits between the SKG in eNB and UE and Enhanced method bit disagreement is compared with Non-Enhanced SKG methods with same set of channel profiles used in enhanced method, and the entropy of the key is calculated using Shannon's entropy method.

5.1 Non-Enhanced Secret Key Generation Results

Initially, secret key is generated using the Non-Enhanced method (i.e without enhancing the channel profile) for the SE and ME and bit disagreement rate is measured. The results for different channel profiles are been discussed in below section. Every channel profile (RSSI, RSRP, Uplink Power) value is converted to 2 bits in standard deviation block quantisation, variance quantisation, standard deviation quantisation and variance block quantisation process, so the length of the key generated is 256 bits. And, for mean quantisation, mean block quantisation, median quantisation, median block quantisation process every channel profile value is converted into 1 bit, so the length of the key generated is 128 bits. so the key generation rate can be considered as 128 seconds in this case.

The method used to measure the channel RSSI, RSRP, Uplink Power is same as the method used for enhanced methods. The SE results for RSSI, RSRP, Uplink Power channel

Table 5.1 Non-Enhanced SKG method's Bit Disagreement Rate of RSSI channel profile in SE

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
SE	none	standard deviation quantisation	94	36.719
		standard deviation block quantisation	90	35.156
		variance quantisation	93	36.719
		variance block quantisation	84	32.812
		mean quantisation	64	50
		mean block quantisation	70	54.688
		median quantisation	63	49.219
		median block quantisation	39	30.469

Table 5.2 Non-Enhanced SKG method's Bit Disagreement Rate of RSSI channel profile in ME

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
ME	none	standard deviation quantisation	85	33.547
		standard deviation block quantisation	91	35.547
		variance quantisation	58	22.656
		variance block quantisation	91	35.547
		mean quantisation	45	35.156
		mean block quantisation	59	46.094
		median quantisation	43	33.594
		median block quantisation	59	46.094

profile are shown in Table 5.1, 5.3, 5.5 respectively and for ME the results are shown in Table 5.2, 5.4, 5.6. The values Bit Disagreement Rate and Number of Disagreed bits are the average of the 10 channel profile's secret key.

In this thesis, Bit error detection and correction step, information reconciliation is not adopted to avoid prior unsecured communication and from the results shown above for RSSI, RSRP, Uplink power channel profiles in SE and ME have quite high bit disagreement rate for SKG from non enhanced channel profile. The bit disagreement rate of SKG depends on the

Table 5.3 Non-Enhanced SKG method's Bit Disagreement Rate of RSRP channel profile in SE

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
SE	none	standard deviation quantisation	72	28.125
		standard deviation block quantisation	80	31.250
		variance quantisation	114	44.531
		variance block quantisation	126	49.219
		mean quantisation	51	39.844
		mean block quantisation	49	38.281
		median quantisation	40	31.250
		median block quantisation	54	42.188

Table 5.4 Non-Enhanced SKG method's Bit Disagreement Rate of RSRP channel profile in ME

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
ME	none	standard deviation quantisation	85	33.203
		standard deviation block quantisation	91	35.547
		variance quantisation	52	20.312
		variance block quantisation	77	30.078
		mean quantisation	38	29.688
		mean block quantisation	57	44.531
		median quantisation	38	29.688
		median block quantisation	53	41.406

Table 5.5 Non-Enhanced SKG method's Bit Disagreement Rate of Uplink Power channel profile in SE

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
SE	none	standard deviation quantisation	85	33.203
		standard deviation block quantisation	95	37.109
		variance quantisation	143	55.859
		variance block quantisation	100	39.062
		mean quantisation	68	53.125
		mean block quantisation	67	52.344
		median quantisation	62	48.438
		median block quantisation	64	50

Table 5.6 Non-Enhanced SKG method's Bit Disagreement Rate of Uplink Power channel profile in ME

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
ME	none	standard deviation quantisation	116	45.312
		standard deviation block quantisation	99	38.672
		variance quantisation	97	37.891
		variance block quantisation	104	40.625
		mean quantisation	78	60.938
		mean block quantisation	63	49.219
		median quantisation	80	62.500
		median block quantisation	70	54.688

Table 5.7 DCT normalized SKG method's Bit Disagreement Rate of RSSI channel profile in SE

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
SE	DCT normalisation	standard deviation quantisation	6	2.344
		standard deviation block quantisation	10	3.906
		variance quantisation	10	3.906
		variance block quantisation	35	13.672
		mean quantisation	6	4.688
		mean block quantisation	8	6.250
		median quantisation	10	7.812
		median block quantisation	64	7.812

methods of channel measurement and quantisation method adopted for the non enhanced channel profile and the channel measurement needs to adhere to the principle of reciprocity, to generate symmetric key on eNB and UE, but the channel measurement may not be adhering to the reciprocity principle, due the noise in channel.

srsLTE used in thesis is FDD configured, the channels for uplink and downlink are different and they have different frequencies and noise may not be same at both uplink and downlink channel. On lower band the difference between the uplink and downlink channel might be less when compared to higher bands, so noise in uplink and downlink channel will be different and so the channel measurements measured in eNB and UE will not be completely reciprocal in nature. The quantisation method also plays an important role in generating symmetric secret key in eNB and UE, but the variations in channel profile like some unwanted spikes will lead to asymmetric key generation.

5.2 DCT normalisation Secret Key Generation Results

To compensate for the drawbacks and reduce the bit disagreement rate, in this thesis, channel enhancement is done using DCT normalisation and AI-based with DCT normalisation channel enhancement methods. In this section, the results based on DCT normalized enhanced channel profiles are discussed. In quantisation method, deviation factor in standard deviation quantisation (normal) is adjusted accordingly for different channel profile, i.e. different deviation values for RSSI, RSRP, Uplink power channel profiles, as the variations of the RSSI, RSRP, Uplink power are different in nature. The number of bits generated and key generation rate is similar to non enhanced method.

The channel values are recorded for every second. The SE results for RSSI, RSRP and Uplink power channel profiles are shown in Table 5.7, 5.9, 5.11 respectively and the results

Table 5.8 DCT normalized SKG method's Bit Disagreement Rate of RSSI channel profile in ME

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
ME	DCT normalisation	standard deviation quantisation	21	8.203
		standard deviation block quantisation	18	7.031
		variance quantisation	24	9.375
		variance block quantisation	41	16.016
		mean quantisation	21	16.406
		mean block quantisation	28	21.875
		median quantisation	24	18.750
		median block quantisation	26	20.312

Table 5.9 DCT normalized SKG method's Bit Disagreement Rate of RSRP channel profile in SE

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
SE	DCT normalisation	standard deviation quantisation	9	3.156
		standard deviation block quantisation	6	2.344
		variance quantisation	8	3.125
		variance block quantisation	24	9.375
		mean quantisation	8	6.250
		mean block quantisation	3	2.344
		median quantisation	8	6.250
		median block quantisation	4	3.125

of ME is shown in Table 5.8, 5.10, 5.12. The values Bit Disagreement Rate and Number of Disagreed bits are the average of the 10 channel profiles.

When compared to non-enhanced SKG methods for RSSI, RSRP and Uplink power channel profiles, the bit disagreement rate for all quantisation method is reduced to single digits apart from variance block quantisation in SE which is due to outliers in the channel profile. In ME, standard deviation quantisation method gives better result compared to other quantisation methods used due to the noise induced. The deviation factor used standard deviation quantisation method is -0.25 for normal quantisation and -1.25 for block quantisation of standard deviation. The deviation factor is decided based on trial and error method keeping entropy of the key high and bit disagreement rate low.

On comparing with SE and ME in all channel profiles with different quantisation methods, the bit disagreement rate is high for ME. In SE, the noise induced to the channel is constant or zero, as the antennas stay in line of sight and environment setup in lab has no disturbance induced. While for ME, the UE keeps moving in random direction and factors like attenuation, noise, interference come into play. Channel profiles measured in ME have lot of variation and DCT normalisation tries to reduce the high variation, but it does not reduce the bit

Table 5.10 DCT normalized SKG method's Bit Disagreement Rate of RSRP channel profile in ME

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
ME	DCT normalisation	standard deviation quantisation	21	8.203
		standard deviation block quantisation	18	7.031
		variance quantisation	28	10.938
		variance block quantisation	38	14.844
		mean quantisation	15	11.719
		mean block quantisation	29	22.656
		median quantisation	28	21.875
		median block quantisation	28	21.875

Table 5.11 DCT normalized SKG method's Bit Disagreement Rate of Uplink power channel profile in SE

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
SE	DCT normalisation	standard deviation quantisation	5	1.953
		standard deviation block quantisation	6	2.344
		variance quantisation	8	3.125
		variance block quantisation	25	9.766
		mean quantisation	4	3.125
		mean block quantisation	7	5.469
		median quantisation	8	6.250
		median block quantisation	6	4.688

Table 5.12 DCT normalized SKG method's Bit Disagreement Rate of Uplink power channel profile in ME

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
ME	DCT normalisation	standard deviation quantisation	14	5.469
		standard deviation block quantisation	21	8.203
		variance quantisation	63	24.609
		variance block quantisation	89	34.766
		mean quantisation	15	11.719
		mean block quantisation	29	22.656
		median quantisation	62	48.438
		median block quantisation	55	42.969

Table 5.13 AI-based with DCT normalized SKG method's Bit Disagreement Rate of RSSI channel profile in SE

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
SE	AI-based with DCT normalisation	standard deviation quantisation	2	0.781
		standard deviation block quantisation	23	8.984
		variance quantisation	1	0.391
		variance block quantisation	7	2.734
		mean quantisation	1	0.781
		mean block quantisation	4	3.125
		median quantisation	4	3.125
		median block quantisation	6	4.688

disagreement rate for all quantisation methods apart from standard deviation quantisation. Futhermore discussion on results in done in Evaluation section.

5.3 AI-based with DCT normalisation Secret Key Generation Results

The results from DCT normalisation shows that the bit disagreement rate is reduced to a good extent when channel profile is multiplied with DCT matrix, the enhanced profile have less high variations. In this method, initially, the channel profile is transformed to the values predicted by LR model designed and transformed channel profile is DCT normalised to get better channel profile.

LR model gives the channel profile where the values are average of eNB and UE, the LR model based on polynomial features predicts the average based on either eNB or UE channel profile measurement. The basic idea behind using the AI is to create a similar channel profile in both the machines (eNB and UE) to generate the symmetric keys. Even though the channel profile is enhanced through LR model, if there are any spikes in measured channel values, then the model predicts the average which is also higher, so to normalise the spikes in AI enhanced channel profile, channel profile is normalised with DCT matrix as explained in Section 3.2.2.

In this section, the results based on AI-based with DCT normalized enhanced channel profiles are shown. In quantisation method, deviation factor in standard deviation quantisation (normal) is adjusted accordingly for different channel profile, i.e. different deviation value for RSSI, RSRP, Uplink power channel profiles, as the variations of the RSSI, RSRP, Uplink power are different in nature. The number of bits generated and key generation rate is similar to non enhanced method.

Table 5.14 AI-based with DCT normalized SKG method's Bit Disagreement Rate of RSSI channel profile in ME

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
ME	AI-based with DCT normalized	standard deviation quantisation	9	3.125
		standard deviation block quantisation	19	7.422
		variance quantisation	8	3.125
		variance block quantisation	32	12.500
		mean quantisation	8	6.250
		mean block quantisation	11	8.594
		median quantisation	10	7.812
		median block quantisation	8	6.250

Table 5.15 AI-based with DCT normalized SKG method's Bit Disagreement Rate of RSRP channel profile in SE

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
SE	AI-based with DCT normalized	standard deviation quantisation	7	2.734
		standard deviation block quantisation	9	3.156
		variance quantisation	6	2.344
		variance block quantisation	26	10.156
		mean quantisation	6	4.688
		mean block quantisation	4	3.125
		median quantisation	6	4.688
		median block quantisation	4	3.125

The Channel values are recorded for every second. The SE results for RSSI, RSRP and Uplink power channel profiles are shown in Table 5.13, 5.15, 5.17 respectively and the results of ME are shown in Table 5.14, 5.16, 5.18 respectively. The values, Bit Disagreement Rate and Number of Disagreed bits are the average of the 10 channel profile's secret key bit disagreement.

The non-enhanced SKG methods and DCT normalisation methods for RSSI, RSRP, Uplink power channel profiles when compared with AI-based with DCT normalisation method, the bit disagreement rate for all quantisation method in both the environment is reduced. The deviation factor used in standard deviation quantisation method is 0.5 for normal quantisation and 1.5 for block quantisation. The deviation factor is decided based on trial and error method keeping entropy of the generated key high and bit disagreement rate low. The degree of transform to fit the curve with all data points using polynomial regression is 2, the degree can be changed if the curve is not fitting all the data point, too high degree value will lead to over fitting state and low value will lead to under fitting state.

Table 5.16 AI-based with DCT normalized SKG method's Bit Disagreement Rate of RSRP channel profile in ME

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
ME	AI-based with DCT normalized	standard deviation quantisation	6	2.344
		standard deviation block quantisation	21	8.203
		variance quantisation	6	2.344
		variance block quantisation	31	12.109
		mean quantisation	6	4.688
		mean block quantisation	12	9.375
		median quantisation	10	7.812
		median block quantisation	10	7.812

Table 5.17 AI-based with DCT normalized SKG method's Bit Disagreement Rate of Uplink Power channel profile in SE

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
SE	AI-based with DCT normalized	standard deviation quantisation	9	3.516
		standard deviation block quantisation	24	9.375
		variance quantisation	9	3.516
		variance block quantisation	38	14.844
		mean quantisation	9	7.031
		mean block quantisation	13	10.156
		median quantisation	18	14.062
		median block quantisation	14	10.938

Table 5.18 AI-based with DCT normalized SKG method's Bit Disagreement Rate of Uplink Power channel profile in ME

Environment	Enhancing Reciprocity method	Quantisation method	Number of Disagreed Bits	Bit Disagreement Rate (%)
ME	AI-based with DCT normalized	standard deviation quantisation	15	5.859
		standard deviation block quantisation	37	14.453
		variance quantisation	14	5.469
		variance block quantisation	63	24.609
		mean quantisation	14	10.398
		mean block quantisation	22	17.188
		median quantisation	20	15.625
		median block quantisation	22	17.188

5.4 Evaluation

All the results are summarized in below section with graphs comparing the BDR of different reciprocity enhancement used. RSSI channel profiles BDR of different enhancement methods used is shown in Figure 5.1 for SE and Figure 5.2 for ME, the BDR for the AI-based with DCT normalized enhancement method has less BDR than compared to DCT normalized and non-enhanced method used.

The Shannon's entropy for RSSI channel profile is around 0.88 to 0.99, the worst entropy value is 0.88 for median quantisation method in DCT normalised SKG and best entropy value is 0.99 for mean and median block quantisation in both DCT normalised and AI-based with DCT normalised SKG. Comparing BDR and entropy of the secret key generated, the standard deviation quantisation method of AI-based with DCT normalisation SKG method have better combination, BDR = 0.391 percent and entropy = 0.97, so for RSSI channel profile standard deviation quantisation method of AI-based with DCT normalisation SKG is more suitable for SKG in SE and ME than the other combination of methods used.

RSRP channel profiles BDR of different enhancement used is shown in Figure 5.3 for SE and Figure 5.4 for ME, the BDR for the AI-based with DCT normalized enhancement method has less BDR than compared to DCT normalized and non-enhanced method used.

For RSRP channel profiles, the Shannon's entropy is from 0.84 to 0.99, the worst entropy value is 0.88 for standard deviation block quantisation method in AI-based with DCT normalised SKG and best entropy value is 0.99 for mean and median block quantisation in both DCT normalised and AI-based with DCT normalised SKG. Comparing BDR and entropy of the secret key generated, the standard deviation quantisation method of AI-based with DCT normalisation SKG have better combination, BDR = 2.344 percent and entropy = 0.98, so for RSRP channel profile standard deviation quantisation method of AI-based with DCT normalisation SKG is more suitable for SKG in SE and ME than the other combination of methods used. Close to standard deviation quantisation method, stands variance quantisation methods with BDR = 2.344 and entropy = 0.95 of AI-based with DCT normalisation SKG. On comparing RSSI and RSRP channel profiles, RSRP channel profiles have better entropy of the key and similar with BDR.

Uplink power Channel Profiles channel profiles BDR of different enhancement used is shown in Figure 5.5 for SE and Figure 5.6 for ME, the BDR for the AI-based with DCT normalized enhancement method has less BDR than compared to DCT normalized and non-enhanced method used in ME and vice verse in SE.

The worst entropy value is 0.86 for variance block quantisation method in DCT normalised SKG and mean quantisation of AI-based with DCT normalised SKG and the best

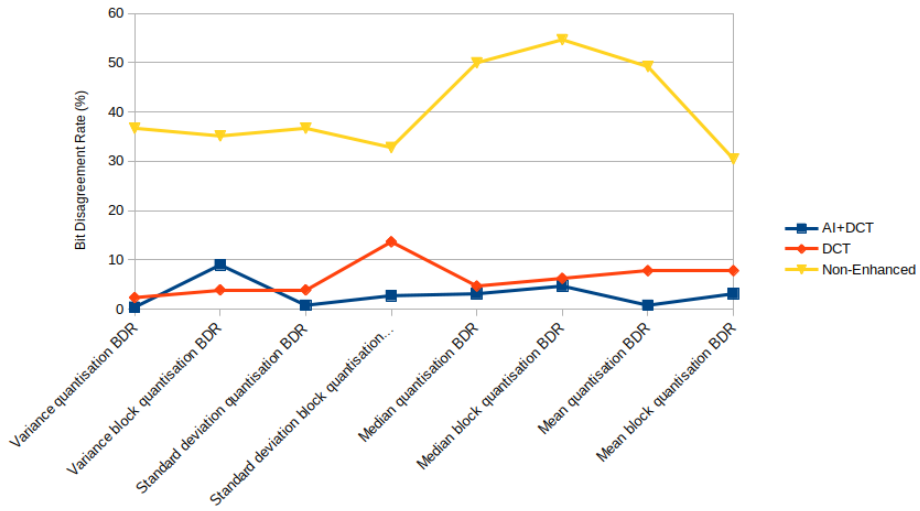

Fig. 5.1 Bit Disagreement Rate Comparison of Enhanced and Non-Enhanced RSSI channel profiles in SE

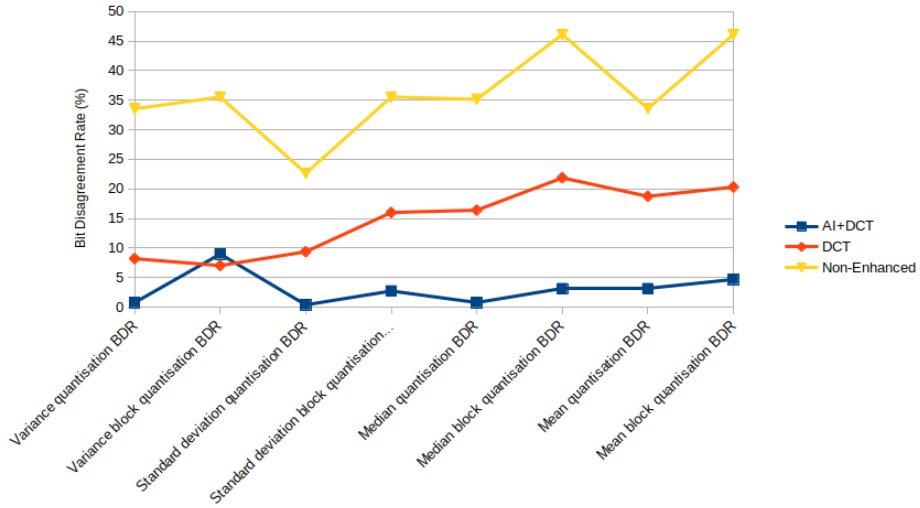

Fig. 5.2 Bit Disagreement Rate Comparison of Enhanced and Non-Enhanced RSSI channel profiles in ME

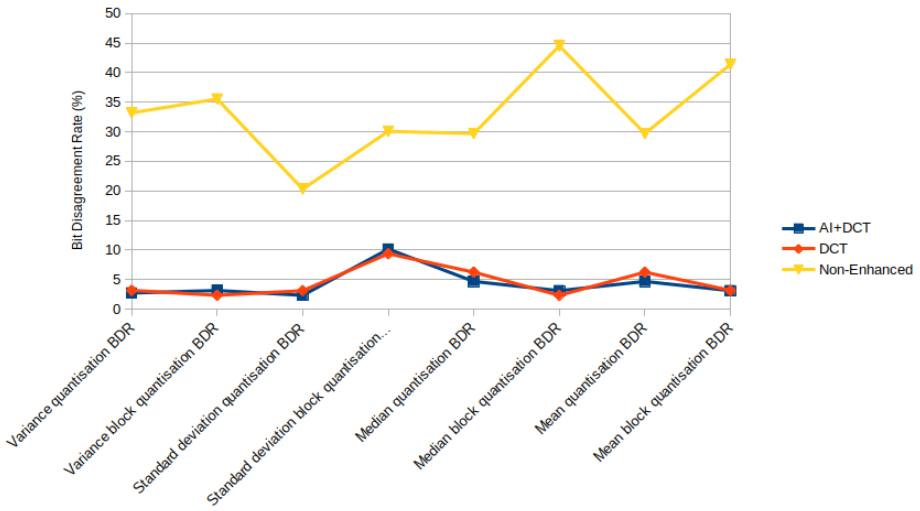

Fig. 5.3 Bit Disagreement Rate Comparison of Enhanced and Non-Enhanced RSRP channel profiles in SE

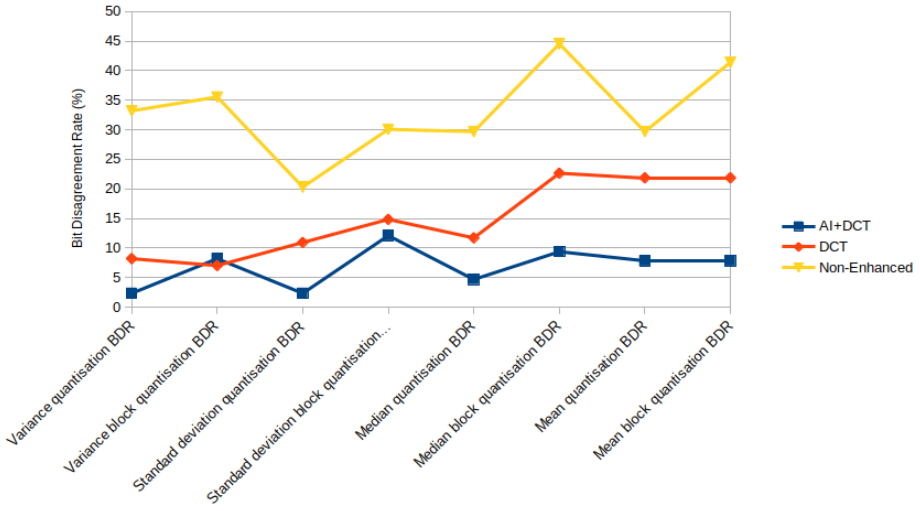

Fig. 5.4 Bit Disagreement Rate Comparison of Enhanced and Non-Enhanced RSRP channel profiles in ME

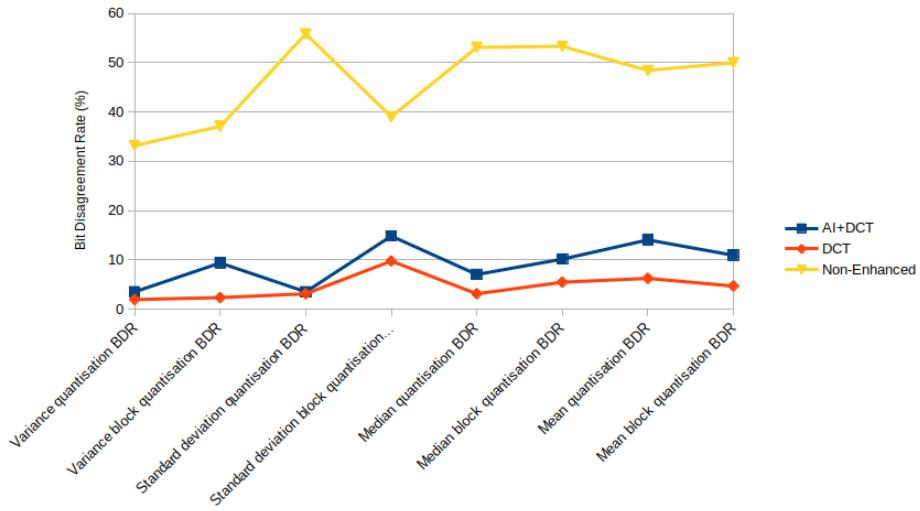

Fig. 5.5 Bit Disagreement Rate Comparison of Enhanced and Non-Enhanced Uplink power channel profiles in SE

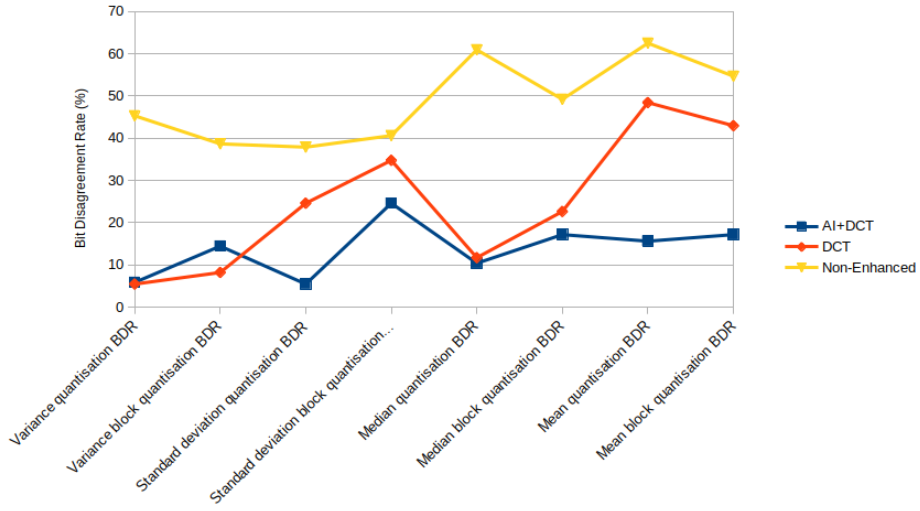

Fig. 5.6 Bit Disagreement Rate Comparison of Enhanced and Non-Enhanced Uplink power channel profiles in ME

entropy value is 0.99 for mean, mean block and median block quantisation in both DCT normalised and AI-based with DCT normalised SKG. comparing BDR and entropy of the secret key generated, the standard deviation quantisation method of AI-based with DCT normalisation SKG have better combination, BDR = 5.47 percent and entropy = .97, so for Uplink power channel profile, the standard deviation quantisation method of AI-based with DCT normalisation SKG is more suitable in SE and ME than the other combination of methods used. Close to standard deviation quantisation method, stands variance quantisation methods with BDR = 5.859 and entropy = 0.93 of AI-based with DCT normalisation SKG. On comparing Uplink power channel profile with other channel profile, Uplink power channel stands close to RSRP channel profile to produce better secret key but not as better as RSRP channel profile.

To test if the third party can generate the same key when placed in same environment with the same distance, another UE was placed in same environment and positioned similar to the UE used to generate the first key. Even though two UE placed in same distance, the channel variation captured by two UE were bit different, which was enough to generate the different key. The difference was checked by comparing the bit disagreement rate of the two UE's channel profile and every channel profiles has at least 5 percent of difference.

6. Conclusion and Future Work

6.1 Conclusion

In contrast to cryptography methods, the thesis uses existing methods of PhySec and adjusts them to the LTE. The main idea of this thesis, is to create a symmetric key between a pair of eNodeb and UE without any prior insecure communication, by using the physical layer measurements. A LTE testbed is proposed in this thesis, using srsLTE SDR, a prototype is developed and measurements like RSSI, RSRP, Uplink Power are captured on both side of the eNodeb and UE within the coherent time maintaining the real world scenarios. Wireless channels have inherent characteristics like fading property, which is used to capture the physical layer measurements and quantised to generate the preliminary key between the pair of eNodeb and UE.

The existing methods are enhanced adding a additional step like enhancing reciprocity of channel profile. The main reason to use enhancing reciprocity step is to exploit the principle of reciprocity adhered to channel profiles created in eNodeb and UE to the maximum extent. Based on this idea, existing methods are used and enhanced. Below section briefs about the ideas implemented and contributions of the thesis.

Firstly, thorough study of past and current research of PhySec methods implemented in WLAN and ideas in LTE. In LTE, there were no proper result oriented research but just the ideas that PhySec methods can be implemented in LTE. So next step is to design the baseline architecture for SKG in LTE adapting the methods used in WLAN. SKG method used in this thesis have four steps namely Channel Profiling, Enhancing reciprocity, Quantisation and Privacy amplification which is discussed in more detail in Chapter 3. In Chapter 4, details of setting the LTE testbed using SDR's like srsLTE is discussed and the codebase of srsLTE is modified to get the channel measurements like RSSI, RSRP and Uplink power in eNodeB and UE. The design and implementation idea of the testbed is published in [3] and [33]. In Enhancing reciprocity step of SKG, two different methods for enhancing

reciprocity are introduced namely, DCT normalisation and AI-based with DCT normalisation. In DCT normalisation, DCT matrix generated from MATHLAB tool is multiplied with channel profile to reduce the spikes in variation of the channel measurements. In AI-based with DCT normalisation method, LR algorithm with polynomial feature is used to predict the average of eNodeB and UE channel measurements, the predicted channel profile in UE and eNodeb adhere to principle of reciprocity but the spikes in the measurements are normalised by multiplying predicted channel profile with DCT matrix. The entropy of the secret key depends on quantisation method used. So 8 different methods of lossless quantisation methods are used. Two methods of Enhancing reciprocity is combined with different quantisation methods to generate the secret key. And finally the results are been discussed and evaluated in Chapter 5, evaluation of the current used SKG methods with non enhanced methods is done by comparing the number of bits disagreeing between the eNodeb and UE secret key. The entropy of the key is calculated using Shannon's entropy.

RSRP channel profile with AI-based with DCT normalisation and standard deviation quantisation method provide the better secret key than other methods, with BDR = 2.344 percent and entropy = 0.98. RSSI channel profile produce better key with standard deviation quantisation and AI-based with DCT normalisation, with BDR = 0.391 and entropy = 0.97. Uplink power channel profile produce better key with standard deviation quantisation and AI-based with DCT normalisation, with BDR = 5.47 and entropy = 0.97. RSSI channel profiles have less BDR compared to RSRP and Uplink power channel profiles but the entropy of the keys are low but close enough to be the best combination to use for SKG. Quantisation methods like mean and median (block and normal) are not suitable for ME as the BDR and entropy of the keys are high but for SE these methods can be adopted but the key size is half the size of keys produced by standard deviation and variance quantisation method used. On Comparing the BDR , key generation rate and entropy of all the different methods of quantisation tried on DCT normalisation and AI-based with DCT normalisation in this thesis, RSRP channel profile with AI-based with DCT normalisation and standard deviation method is the best.

6.2 Future Work

Currently FDD bands and configurations are used in testbed and tested, the methods used in this thesis can be extended to TDD bands and configurations which have only one channel for uplink and downlink. AI-based with DCT normalised method can be improved to generate the channel profile with better reciprocity factor by considering the noise factor and other factors helping the signal to fade while training the model and other option to improve the

LR model is by training the model with channel measurements of different environments. Currently, researchers are working on ML algorithm for channel predictions which leads to possibility that other algorithms can be used to develop the AI model to predict the enhanced channel profile with better MSE. All the methods have not been tested in crowded environments due to the range of devices used in the thesis, so methods can be deployed in real world devices in real world crowded places to adapt to more realistic scenarios. Finally, generating secret key using other physical layer properties like CQI, CIR and other properties

References

[1] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D Sutton, Pablo Serrano, Cristina Cano, and Doug J Leith. srslte: an open-source platform for lte evolution and experimentation. In *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization*, pages 25–32. ACM, 2016.

[2] Animesh Agarwal. Polynomial Regression, Oct 2018. URL https://towardsdatascience.com/polynomial-regression-bbe8b9d97491.

[3] C. Lipps, M. Strufe, S. B. Mallikarjun, and H. D. Schotten. Physical Layer Security for IIoT and CPPS: A Cellular-Network Security Approach. In *Mobile Communication - Technologies and Applications; 24. ITG-Symposium*, pages 1–5, May 2019.

[4] Nan Yang, Lifeng Wang, Giovanni Geraci, Maged Elkashlan, Jinhong Yuan, and Marco Di Renzo. Safeguarding 5G Wireless Communication Networks Using Physical Layer Security. *Communications Magazine, IEEE*, 53:20–27, 04 2015. doi:10.1109/MCOM.2015.7081071.

[5] Towards Open Cellular Ecosystem, . URL https://www.openairinterface.org/?page_id=864.

[6] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla. Applications of LDPC Codes to the Wiretap Channel. *IEEE Transactions on Information Theory*, 53(8):2933–2945, Aug 2007. ISSN 0018-9448. doi:10.1109/TIT.2007.901143.

[7] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire. Secure Massive MIMO Transmission With an Active Eavesdropper. *IEEE Transactions on Information Theory*, 62(7):3880–3900, July 2016. ISSN 0018-9448. doi:10.1109/TIT.2016.2569118.

[8] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez. Millimeter Wave Mobile Communications for 5G Cellular: It Will Work! *IEEE Access*, 1:335–349, 2013. ISSN 2169-3536. doi:10.1109/ACCESS.2013.2260813.

[9] Tiejun Lv, Hui Gao, and Shaoshi Yang. Secrecy Transmit Beamforming for Heterogeneous Networks. *IEEE Journal on Selected Areas in Communications*, 33(6): 1154–1170, 2015.

[10] Y. Zhang, H. Wang, Q. Yang, and Z. Ding. Secrecy Sum Rate Maximization in Non-orthogonal Multiple Access. *IEEE Communications Letters*, 20(5):930–933, May 2016. ISSN 1089-7798. doi:10.1109/LCOMM.2016.2539162.

[11] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten. Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers. *IEEE Transactions on Signal Processing*, 61(20):4962–4974, Oct 2013. ISSN 1053-587X. doi:10.1109/TSP.2013.2269049.

[12] Blaise Gassend, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. Silicon Physical Random Functions. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, CCS '02, pages 148–160, New York, NY, USA, 2002. ACM. ISBN 1-58113-612-9. doi:10.1145/586110.586132. URL http://doi.acm.org/10.1145/586110.586132.

[13] G. E. Suh and S. Devadas. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In *2007 44th ACM/IEEE Design Automation Conference*, pages 9–14, June 2007.

[14] C. Herder, M. Yu, F. Koushanfar, and S. Devadas. Physical Unclonable Functions and Applications: A Tutorial. *Proceedings of the IEEE*, 102(8):1126–1141, Aug 2014. ISSN 0018-9219. doi:10.1109/JPROC.2014.2320516.

[15] C. Lipps, A. Weinand, D. Krummacker, C. Fischer, and H. D. Schotten. Proof of Concept for IoT Device Authentication Based on SRAM PUFs Using ATMEGA 2560-MCU. In *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, pages 36–42, April 2018. doi:10.1109/ICDIS.2018.00013.

[16] J. E. Hershey, A. A. Hassan, and R. Yarlagadda. Unconventional Cryptographic Keying Variable Management. *IEEE Transactions on Communications*, 43(1):3–6, Jan 1995. ISSN 0090-6778. doi:10.1109/26.385951.

[17] Y. Liu, H. Chen, and L. Wang. Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges. *IEEE Communications Surveys Tutorials*, 19(1):347–376, Firstquarter 2017. ISSN 1553-877X. doi:10.1109/COMST.2016.2598968.

[18] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu. Experimental Study on Key Generation for Physical Layer Security in Wireless Communications. *IEEE Access*, 4:4464–4477, 2016. ISSN 2169-3536. doi:10.1109/ACCESS.2016.2604618.

[19] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Communications Surveys Tutorials*, 16(3):1550–1573, Third 2014. ISSN 1553-877X. doi:10.1109/SURV.2014.012314.00178.

[20] A. Ambekar, N. Kuruvatti, and H. D. Schotten. Improved Method of Secret Key Generation Based on Variations in Wireless Channel. In *2012 19th International Conference on Systems, Signals and Image Processing (IWSSIP)*, pages 60–63, April 2012.

[21] H. Wang, T. Zheng, J. Yuan, D. Towsley, and M. H. Lee. Physical Layer Security in Heterogeneous Cellular Networks. *IEEE Transactions on Communications*, 64(3): 1204–1219, March 2016. ISSN 0090-6778. doi:10.1109/TCOMM.2016.2519402.

[22] C. Wang and H. Wang. Physical Layer Security in Millimeter Wave Cellular Networks. *IEEE Transactions on Wireless Communications*, 15(8):5569–5585, Aug 2016. ISSN 1536-1276. doi:10.1109/TWC.2016.2562010.

[23] H. Wang, X. Zhou, and M. C. Reed. On The Physical Layer security in Large Scale Cellular Networks. In *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2462–2467, April 2013. doi:10.1109/WCNC.2013.6554947.

[24] G. Geraci, H. S. Dhillon, J. G. Andrews, J. Yuan, and I. B. Collings. Physical Layer Security in Downlink Multi-Antenna Cellular Networks. *IEEE Transactions on Communications*, 62(6):2006–2021, June 2014. ISSN 0090-6778. doi:10.1109/TCOMM.2014.2314664.

[25] H. Wang, X. Zhou, and M. C. Reed. Physical Layer Security in Cellular Networks: A Stochastic Geometry Approach. *IEEE Transactions on Wireless Communications*, 12 (6):2776–2787, June 2013. ISSN 1536-1276. doi:10.1109/TWC.2013.041713.120865.

[26] B. Chen and F. M. J. Willems. Secret Key Generation Over Biased Physical Unclonable Functions With Polar Codes. *IEEE Internet of Things Journal*, 6(1):435–445, Feb 2019. ISSN 2327-4662. doi:10.1109/JIOT.2018.2864594.

[27] A. Ambekar and H. D. Schotten. Enhancing Channel Reciprocity for Effective Key Management in Wireless Ad-Hoc Networks. In *2014 IEEE 79th Vehicular Technology Conference (VTC Spring)*, pages 1–5, May 2014. doi:10.1109/VTCSpring.2014.7022913.

[28] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka. Wireless Secret Key Generation Exploiting Reactance-domain Scalar Response of Multipath Fading Channels. *IEEE Transactions on Antennas and Propagation*, 53(11):3776–3784, Nov 2005. doi:10.1109/TAP.2005.858853.

[29] T. Shimizu, N. Otani, T. Kitano, H. Iwai, and H. Sasaoka. Experimental validation of wireless secret key agreement using array antennas. In *2011 XXXth URSI General Assembly and Scientific Symposium*, pages 1–4, Aug 2011. doi:10.1109/URSIGASS.2011.6050501.

[30] V. Priyashman and W. Ismail. Signal Strength and Read Rate Prediction Modeling Using Machine Learning Algorithms for Vehicular Access Control and Identification. *IEEE Sensors Journal*, 19(4):1400–1411, Feb 2019. doi:10.1109/JSEN.2018.2880736.

[31] Kronecker delta — Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/w/index.php?title=Kronecker%20delta&oldid=911570884, 2019. [Online; accessed 17-September-2019].

[32] USRP Hardware Driver and USRP Manual: Building and Installing UHD from Source Build Dependencies, . URL http://files.ettus.com/manual/page_build_guide.html.

[33] Christoph Lipps, Mathias Strufe, Sachinkumar Bavikatti Mallikarjun, and Hans Dieter Schotten. PhySec in Cellular Networks: Enhancing Security in the IIoT. In *European Conference on Cyber Warfare and Security*, pages 297–XVI. Academic Conferences International Limited, 2019.