International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 10 • Issue 2 pp. 665-672 June 2018-Dec 2018 www.csjournals.com

Analysis of Quantization schemes in Secure Key Generation for Internet of Things

U.R. Bhatt[1], R. Sharma[1], A. Soni[1], R. Upadhyay [1]
[1]Electronics and Telecommunication, Institute of Engineering & Technology, Devi Ahilya University, Indore, India

Abstract: The Internet of Things (IOT) is expected to be a technical revolution in the forthcoming era. It will impact on business, governments, and consumers to interact with the physical world. Studies forecast that there will be 34 billion devices connected to the Internet by 2020. IoT systems generally work on the wireless network. Because of the broadcast natures of the wireless channel, it needs robust key management systems for secure communication. Physical layer security is novel method to utilize the random and reciprocal nature of the wireless channel to extract secret key. The process of secure key generation consists of four steps, namely; channel measurement, quantization, information reconciliation, and privacy amplification. The efficiency of the secure key generation process depends on the method of channel measurement and quantization. In this thesis, we focus on quantization schemes to generate a secure key. There are two types of quantization schemes, namely: Lossless and Lossy. In the present work for secure communication in IOT system, we propose an algorithm which is based on Llyod-max Algorithm for Lossless Quantizer**.** In this paper, the process of secure key generation is implemented on MATLAB platform. We measure real-world channel parameter like received signal strength indicator using a test setup comprised with802.11n wireless USB adapter and smart phone with supporting software. The performance of the proposed lossless quantizer based on Llyod-max algorithm is evaluated by comparing its performance in terms of key disagreement rate, quantization factor, and quantization noise power with other traditional quantization schemes. It has been observed that proposed algorithm gives low quantization error. Besides, for the constant value of SQNR we use low power signal for a secure key generation hence the proposed work will be best suited for IoT based applications.

Keywords: Secure key generation, Quantization, Key Disagreement Rate.

INTRODUCTION

A. The Internet of Things

Interconnection between internet features like redundant storage, search engines, worldwide connectivity and physical systems like sensors, actuators, interfaces, displays will be everywhere in the future [1]. IoT is a collection of many interconnected objects, services, humans and devices that can communicate, and share data through wireless and internet [2]. Internets of Things (IoT) are becoming important for many applications like agriculture to industrial automation, smart cities and health care [3]. By 2020, there could be over 50 billion devices that would communicate wirelessly and hence it is necessary to concentrate over the security concern of these nodes as the data propagates wirelessly and covers a broad variety of data [4]. Independently connected devices will operate and intercommunicate without user interaction mainly via Low Power Wireless Networks (LPWN) which are used in IoT. These networks may include RFID, Bluetooth, ZigBee, 6LoWPAN and solutions based on sub- GHz technologies [5]. A common feature of all these technologies and standards is low-energy consumption. These networks operate at a very low data rate and transmission power, targeting at extended lifetime. The maximum transmission power of a regular LPWN device is typically 1 mW. While in WiFi access pointsit is in the range of 30 mW to 800 mW, in WiFi mobile nodes(laptops) it is 32 mW, in cellular access points it is around 105 mW and in cellular phones it varies from 500mW to 2 W [4].

B. Physical Layer Security for IoT

Due to the open and heterogeneous nature of the wireless medium, data exchange may suffer from various attacks, resulting major threat to the security which is a critical concern in wireless network and so in IoT. Physical layer security (PLS) is the primary security solution that focuses on utilizing the physical (PHY) layer properties of the wireless channels to safe guard the confidential information transmission against various attacks and is applicable for IoT [6]

The concept of physical layer security means to achieve perfect secrecy of data transmission between intended network nodes. For example Alice (node) and Bob (node) want to secure communication, but eve (node) may steel information through the channel as shown in figure 1 [7]. In the wireless network, the Jamming and Eavesdropping are the primary attacks at the physical layer. For wireless network security, authentication, confidentiality, Integrity and availability are required [8].There are many Approaches to achieve security in the physical layer, e.g. Preprocessing scheme Coding, Key Generation**,** Artificial Noise Scheme, Signal Processing, and Co-operation Communication.

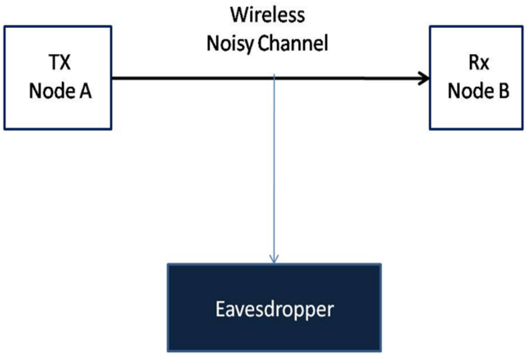

Figure 1: General concept of physical layer security

For the IoT system, physical layer security is a novel method of profitably utilizing the random and reciprocal variations of the wireless channel to extract secret key. By measuring the characteristics of the wireless channel within its coherence time, reciprocal variations of the channel can be observed between a pair of legitimate nodes. Using these reciprocal characteristics of the wireless channel, a common shared secret key is extracted between a pair of the legitimate nodes [9]. The process of key extraction consists of four steps, namely; channel measurement, quantization, information reconciliation, and privacy amplification. The reciprocal channel variations are measured and quantized to obtain a preliminary key of vector bits (0; 1). Due to errors in measurement, quantization, and additive Gaussian noise, disagreement in the bits of preliminary keys exists. These errors are corrected by using, error detection and correction methods to obtain a synchronized key at both the nodes. Further, by the method of secure hashing, the entropy of the key is enhanced in the privacy amplification stage.

The efficiency of the key generation process depends on the method of channel measurement and quantization. There are many channel characteristic parameters like channel estimates, received signal strength indicator (RSSI), distance, angle of arrival from which channel can be measured [10]. Quantization is the process of conversion channel profiles into digital vectors to obtain preliminary key material. A number of algorithms for quantization have been shown in the literature and are divided into two categories: lossless and lossy quantization schemes. Lossless quantization maps every sample to an n-bit symbol, whereas lossy quantization schemes may drop certain samples in favor of a more robust key generation and to maintain a high bit entropy. The original intention was that the output stream could be used directly as a shared symmetric key without using posterior information reconciliation and privacy amplification [11].

The rest of the paper is organized as follows. Section II we summarize the secure key generation method and literature survey on quantization schemes applied for key generation. In section III we describe our practical system setup with data collection, steps of secure key generation and the observations. The paper is then concluded in Section IV.

KEY GENERATION & QUANTIZATION SCHEMES

A. Key Generation

Secret key generation is a method in which randomness of wireless channel is used to generate the keys for legitimate pair of nodes. Since the wireless channel between Alice and Bob is reciprocal and varies randomly over space and time hence these nodes measure the characteristic of the wireless channel and generate the secret keys.

The method of generating secret keys consists of four major steps namely Channel estimation, Quantization, Information reconciliation and Privacy amplification as shown in figure 2. As a first step, the channel is probed at both the nodes to measure the variations of the channel within the coherence time, to obtain a channel profile. The channel profile is then quantized to obtain a preliminary key. Due to variations in the channel profile, the preliminary key constructed at both the ends does not match for all the bits. Hence to synchronize the preliminary keys, error detection and correction methods are used during the information reconciliation stage. During the reconciliation process, the eavesdropper will also have access to the error detection and correction bits. Thus to minimize the possibility of key prediction, the security of the synchronized keys is enhanced in the privacy amplification stage to obtain a final secure key [11].

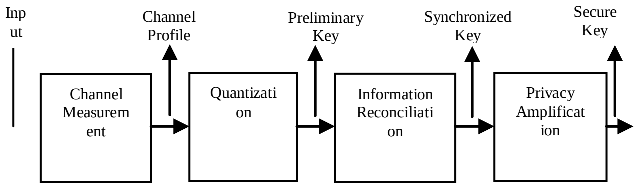

Figure 2: Standard Method of Key Generation

B. Quantization Schemes

Quantization is the process of mapping a set of continuous-valued as well as discrete samples into a smaller, finite number of output levels [20].In secure key generation we used mainly four type –

1) Conventional Quantization

In this quantization schemes the step size is defined using, minimum and maximum value of the input signal, and number of bits which is used to encode one sample [22].

2) Lossless Quantization

It is similar to our conventional quantizer but the only difference is to define in step size. In this quantization the step size is define in term of mean, median, and standard deviation of input signal. Firstly, Ambekar et al. [16] proposed this quantization schemes.

3) Lossy Quantization

It is One bit quantization schemes shown in the figure, which tolerate some amount of information loss to increase their reliability. In N.Patwari et. al. [15] proposed lossy quantizer based on two thresholds ϒ+ and ϒ- for converting channel measurement RSS into random bits Q such that-

$$Q\ (RSS)=1 \text{ if } RSS>\Upsilon+$$

$$Q\ (RSS)=0 \text{ if } RSS<\Upsilon-$$

Otherwise RSS is dropped. Upper and lower threshold of the quantizer decided by the mean and standard deviation of the input sample.

4) Llyods-max based Quantization

It is also called optimal quantizer which gives minimum quantization error. It gives quantization interval and quantization level such that the quantization error is minimum. It describes non-uniform quantization if the pdf of the input variable is not uniform. This is expected, since we should perform finer quantization (that is, the quantization intervals more closely packed and consequently more number of quantization levels) wherever the pdf is large and coarser quantization (that is, quantization intervals widely spaced apart and hence, less number of reconstruction levels), wherever pdf is low [23].

C. Evaluation Metrics

In order to validate the effectiveness of the key generation methods, a set of metrics is necessary. Various metrics used in the state of art are-

Key Disagreement Rate (KDR): KDR indicates the percentage of bits that are in disagreement between the preliminary keys of Alice and Bob. A higher KDR, indicates higher number of bits in disagreement in a preliminary key, thereby increasing the effort needed to synchronize them. A lower KDR indicates, greater percentage of bits in agreement, thereby decreasing the effort needed to synchronize.

Quantization Noise Power (QNP): It is the noise power which is generate during the quantization process. QNP should be minimum for low power input signal.

Quantization Factor (QF): Quantization factor is the percentage of bits retained after quantization. For lossless quantization, QF = 100 %, while for a lossy quantization QF <100 %.

PRACTICAL SETUP AND RESULTS

A. Practical Setup to measure RSS

Statistical channel models based on Additive White Gaussian Noise (AWGN) or Rayleigh fading characteristics are usually used to model the behavior of wireless channels during software simulations. Such statistical models give a good approximation of the nature of fading, noise and the Doppler effects on the transmitted signal. They are a good starting point invalidating transmitter and receiver systems. However for effective deployment, a working proof-of-concept based on channel measurements from real world would be beneficial. Hence in order to develop proof-of-concepts, test beds reflecting real world channel measurements are constructed and used for validation.

The test beds include; IEEE 802.11n based wireless cards, smart phone 'Redmi note 3'which consist IEEE 802.11a/b/g/n/ac supported wi-fi standard, net-spot software tool and wi-fi analyzer android application.Net Spot and wi-fi analyzer are software tool for wireless network assessment, scanning, and surveys, analyzing Wi-Fi coverage and performance. In this setup, the methodology is to build databases of channel profiles (RSSI) and process it offline, using the framework shown in Figure 3 and 4. For the internet of things (IoT) world is given the wide deployment of static networks (e.g. wireless sensor networks), the problem of extracting secret keys in such networks is important. As the variations in static channels are relatively flat, it is difficult to extract secret keys. Hence methodologies for extracting keys in static networks need to be determined.

B. Framework

1) Secure Key Generation

To develop a secure key generation system, an offline key generation framework is built as shown in the Figure 3. It includes:

a) MATLAB based channel profile creation using AWGN function.

b) MATLAB based quantization algorithms such as; uniform quantizer, Median quantizer, binary quantizer, and Adaptive quantizer.

c) MATLAB based Linear Block Code encoder-decoder is used for information reconciliation [24].

d) The secure hashes SHA-1 are derived using the open source MATLAB code provided by NIST [25]

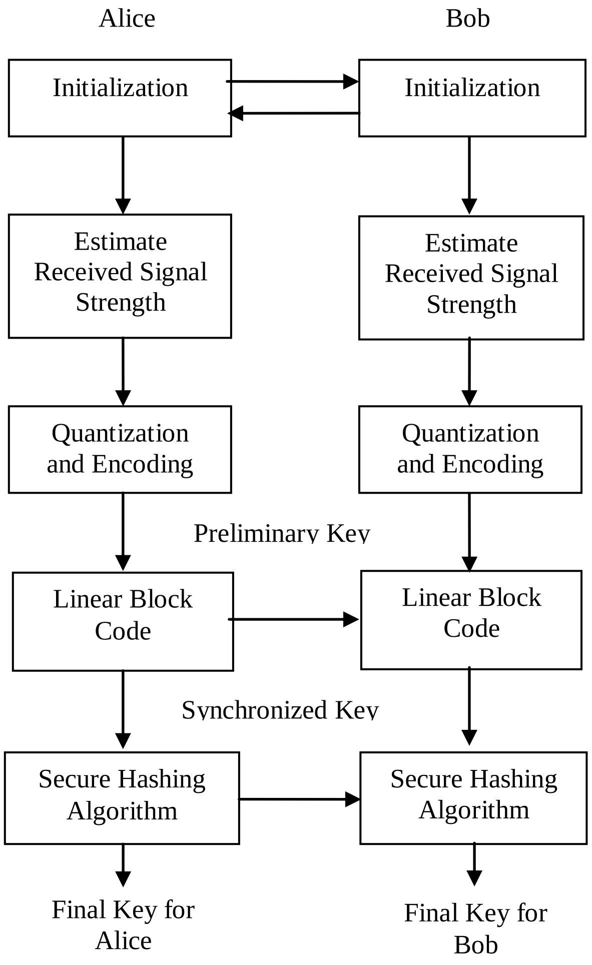

Figure 3: Framework for Secret Key Generation

C. Performance Evaluation

1) Quantization schemes used in Secure Key Generation

To analysis of quantization schemes used in secure key generation system, an offline key generation framework is built as shown in the Figure 4. It includes:
a) Practical Data based on channel profile for key generation.
b) Implementation of quantization algorithms such as; conventional quantizer, lossless quantizer, llyods-max based quantizer using MATLAB.
c) Implementation of Linear Block Code encoder-decoder is used for information reconciliation [24] using MATLAB.
d) The secure hashes SHA-1 are derived using the open source code provided by NIST [25].

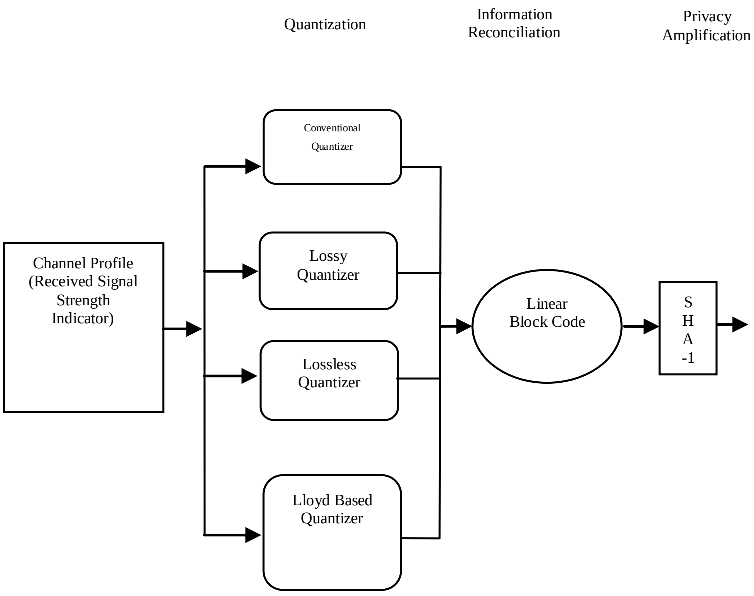

Figure 4: Different Quantization Schemes in Key Generation

2) Effect of Quantization Bits on Key Disagreement Rate

The results of the KDR as the function of quantization bits indicated in Figure 5. The results indicated as-
a) No. of quantization bit increases KDR also increases.
b) 2-Bit Quantizer gives lowest KDR for all possible value of SNR.
c) In 2-Bit Quantizer KDR is zero at SNR equal to 40 dB i.e Alice and Bob get the same Key.

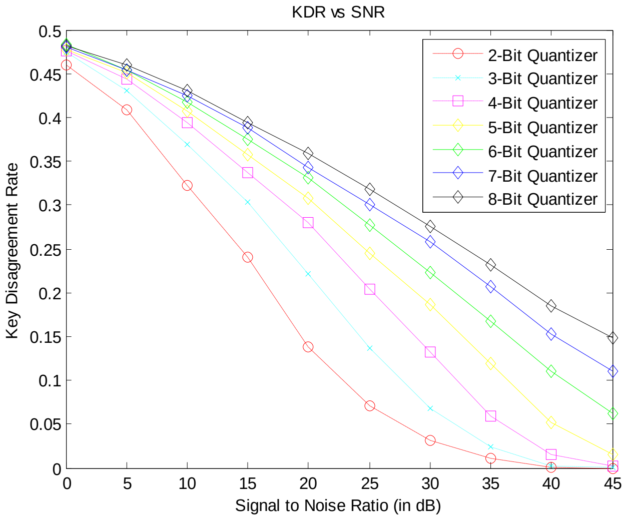

Figure 5: KDR and SNR for different Quantization Bits

3) Effects of Quantization Schemes on KDR

The results of the KDR for different quantizers like Conventional Quantizer, Lossless Quantizer, Llyod-max based Quantizer and LossyQuantizer indicated in Figure 6. The results indicated as-
a) At lower SNR, the performance of Llyods-max based Quantizer is better than the others, except Lossy Quantizer, and further information reconciliation block is used to reduce disagreement.
b) In the middle, performance of Lossless Quantizer is better. c) At higher SNR, performance of Conventional Quantizer, Llyod-max based, Lossless Quantizer is almost comparable.

4) Comparison between Llyod-max based Quantizer and Lossy Quantizer
The results of the KDR for Llyod-max based Quantizer and Lossy Quantizer indicated in Figure 7. Lossy Quantizer gives lower KDR.

5) Effects of Quantization Noise Power (QNP) on Quantization Schemes
The results of the QNP for different quantizers like Conventional Quantizer, Lossless Quantizer, and Llyod-max based Quantizer indicated in Table 1and 2. The results indicated as, Lloyd-max based Quantizer gives better noise immunity than Conventional as well as Lossless Quantizer.

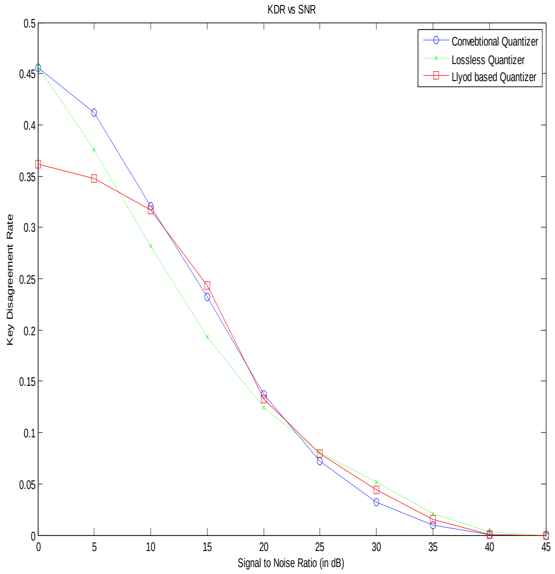

Figure 6: KDR and SNR for different Quantizers

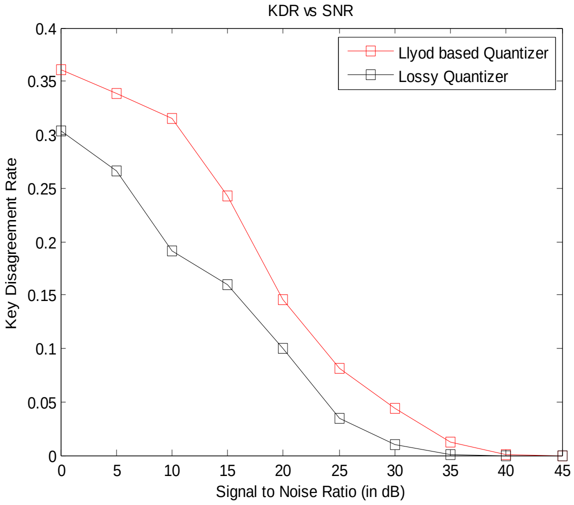

Figure 7: Graph between KDR and SNR for LQ and LYQ

Table 1: Comparison between CQ and LYQ on the basis of QNP

S.No	SNR	Conventional Quantizer ($P_n$in nw)	Lloyd-max Quantizer ($P_n$in nw)	Improvement (%)
1	0	0.78805	0.42176	46
2	5	0.21629	0.11752	46
3	10	0.06797	0.03895	43
4	15	0.02208	0.01156	48
5	20	0.00678	0.00339	50
6	25	0.00233	0.00123	47
7	30	0.00076	0.00041	46
8	35	0.00022	0.00011	50
9	40	0.00007	0.00003	57
10	45	0.00002	0.00001	50

Table 2: Comparison between LLQ and LYQ on the basis of QNP

S.No	SNR	Lossless Quantizer ($P_n$in nw)	Lloyd-max Quantizer ($P_n$in nw)	Improvement (%)
1	0	4.2143	0.42176	90
2	5	1.0978	0.11752	89
3	10	0.36277	0.03895	89
4	15	0.11286	0.01156	90
5	20	0.03764	0.00339	91
6	25	0.01272	0.00123	90
7	30	0.00398	0.00041	90
8	35	0.0012	0.00011	91
9	40	0.00039	0.00003	92
10	45	0.00012	0.00001	92

D. Observation

The following observations are deduced from the results:

1. Testbed: The testbed used to validate the methods of secure key generation with wireless cards from laptops, smart phone and the software defined netspot, wifi analyzer. The wireless cards yield real-world RSSI profiles.
2. From Figure 4.5 it can be observed that key disagreement rate depends on the no. of quantization bits. As no. of quantization bits increases the key disagreement rate also increases.
3. From Figure 4.6 it can be observed that the proposed quantizer namely Llyods-max based quantizer has decreased key disagreement rates, at lower SNR condition, compared to the other methods.
4. we compare proposed quantizer with lossy quantizer shown in the Figure 4.7 and observed that the KDR is better for Lossy Quantizer. But Quantization factor for Lossy Quantizer is less than 100%. So the length of preliminary key will be small, hence eavesdropper can easily extract key. But for lossless quantizers length of key is high which results in better security.
5. From Table 4.1 and 4.2 it can be observed that proposed quantizer gives low quantization error, so for the constant value of SQNR we can used low power signal for secure key generation. Hence this llyods-max based quantizer can be used for Internet of Things (IoT).

CONCLUSION

Fading is built-in characteristic of the wireless channel due to which variations in the amplitude and phase of the received signal exist. By using the properties of the wireless channel, we establish secure communication between two legitimate nodes. The process consists of measuring the channel profile, quantizing it to get preliminary keys; The disagreeing bits of the preliminary keys are detected and corrected using Linear Block Codes to obtain a synchronized key. To prevent any possibilities of key prediction, secure hash (SHA-1) of the synchronized key are generated to obtain, secure keys. It is also concluded that, proposed quantizer gives low quantization error, so for the constant value of SQNR we can use low power signal for secure key generation. Hence this Llyods-max based quantizer can be used for low power IoT nodes. In future, other optimizing algorithms such as rate-distortion theory can also be used for further improvement in key disagreement rate.

REFERENCES

[1] Gurpreet Singh Matharu, Priyanka Upadhyay, Lalita Chaudhary, “The Internet of Things: Challenges & Security Issues”, 10th IEEE Workshop onFactory Communication Systems (WFCS), 2014.

[2] RwanMahmoud, TasneemYousuf, FadiAloul, Imran Zualkernan,“Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures”, The 3rdIEEE ISCC 2015 workshop on Smart City and Ubiquitous Computing Application, 2015.

[3] Ioannis Andrea, ChrysostomosChrysostomou, George Hadjichristofi, “Internet of Things: Security Vulnerabilities and Challenges”, The 3rd IEEE ISCC 2015 workshop on Smart City and Ubiquitous Computing Application, 2015.

[4] Cisco’s Internet Business Solutions Group (IBSG). The internet of things. http://share.cisco.com/internet-of-things.html, December 2014.

[5] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications” IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 4, 2015

[6] Ankit Soni, RakshaUpadhyay and Anjana Jain, “Internet of Things and Wireless Physical Layer Security A Survey” Proceedings of ICT3, vol. 5, pp. 115-124, 2016

[7] Xiangyun Zhou , Lingyang Song , Yan Zhang, “Physical Layer Security in Wireless Communications” CRC press , 2013

[8] Yi-sheng shiu and Shih yuchang, Hsiao-chunwu, Scott c.-h. Huang, Hsiao-hwachen, “Physical Layer Security InWireless Networks: A Tutorial”, IEEE Wireless Communication , pp. 66-74, 2011

[9] Junqing Zhang, Trung Q. Duong, Alan Marshall, And Roger Woods “Key Generation From Wireless Channels: A Review”, IEEE Access, vol. 4, pp. 614-626, 2016.

[10] Ahmed Badawya, Tarek Elfouly, Tamer Khattab, Amr Mohamedb,MohsenGuizani,” Unleashing the secure potential of the wireless physical layer: Secret key generation methods” physical communication, pp. 1-10, 2016

[11] C. T. Zenger, J. Zimmer, and C. Paar, ``Security analysis of quantizationschemes for channel-based key extraction,'' in *Proc. Workshop Wireless +-Commun. Secur. Phys. Layer*, Coimbra, Portugal, Jul. 2015.

[12] Z. Li, W. Xu, R. Miller, and W. Trappe, “Securing wirelesssystems via lower layer enforcements,” in WiSe06:Proceedings of the 5th ACM workshop on Wireless security,2006, pp. 33–42.

[13] SuhasMathur, Wade Trappe, Narayan B. Mandayam, Chunxuan Ye, and Alex Reznik, “Radio-telepathy: extracting a secret key from an unauthenticated wireless channel” Proceedings of the 14th Annual International Conference on Mobile Computing and Networking, MOBICOM 2008, pages 128–139. 2008.

[14] Suman Jana, SriramNandhaPremnath, Mike Clark, Sneha Kumar Kasera, Neal Patwari, and Srikanth V. Krishnamurthy, “On the effectiveness of secret key extraction fromwireless signal strength in real environments”, Proceedings of the 15th Annual InternationalConference on Mobile Computing and Networking, MOBICOM 2009, pages 321–332, 2009.

[15] Neal Patwari, Jessica Croft, Suman Jana, and Sneha Kumar Kasera. High-rate uncorrelatedbit extraction for shared secret key generation from channel measurements. IEEETrans. Mob. Comput. , pages 17–30, 2010.

[16] A. Ambekar, M. Hassan, and H.D. Schotten. Improving channel reciprocity for effectivekey management systems. In Signals, Systems, and Electronics (ISSSE), 2012 InternationalSymposium on, pages 1–4, Oct 2012.

[17] Christian T. Zenger, Markus-Julian Chur, Jan-Felix Posielek, Christof Paar, and Gerhard Wunder, “A novel key generating architecture for wireless low-resource devices”, International Workshop on Secure Internet of Things, SIoT 2014, pages 26–34, 2014.

[18] Ren´e Guillaume, Andreas Mueller Christian T. Zenger, Christof Paar Andreas Czylwik “Fair Comparison and Evaluation of QuantizationSchemes for PHY-based Key Generation” 18th International OFDM Workshop 2014, pages 150-154.

[19] Xuanxuan Wang, Lars Thiele, Thomas Haustein and Yongming Wang “Secret Key Generation UsingEntropy-Constrained-Like Quantization Scheme” 23rd International Conference on Telecommunications (ICT),2016

[20] S. Sengupta, “Digital voice and picture communication”, video lecture, www.nptel .com

[21] S. Haykin, “Communication System”, wileyindiapvt. Ltd., Fourth edition, 193-231, 2012.

[22] U.R. Bhatt, R. Sharma, A. Soni, R. Upadhyay, “A Survey on Quantization Schemes for Secure Key Generation” in International Journal of Scientific Research in Computer Science and Engineering,Volume-5, Issue-3, Jun 2017

[23] Sarah J. Johnson, “Introducing Low-Density Parity-Check Codes”, Online Notes, ACoRN Spring School, 1-20

[24] Soni, A., Upadhyay, R., Jain, A.: ‘Internet of Things & Wireless Physical Layer Security: A Survey’, Proc. Int. Conf. Computer Communication Networking and Internet Security, Vijayawada, November 2016, pp. 115-123

[25] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pd