Mobile Networks and Applications (2020) 25:173–178
https://doi.org/10.1007/s11036-019-01219-5

A Physical-Layer Key Distribution Mechanism for IoT Networks

Mohanad Alhasanat[1] · Saud Althunibat[2] · Khalid A. Darabkh[3] · Abdullah Alhasanat[1,4] · Moath Alsafasfeh[1]

Published online: 13 February 2019

Abstract

Physical layer security has gained an increasing attention due to its efficiency and simplicity as compared to other conventional security protocols. Thus, it has been recently nominated for Internet of Things (IoT) applications. In this paper, a novel key distribution mechanism is proposed for IoT networks. The proposed mechanism exploits the channel diversity to distribute encryption keys among nodes within the network. A main novelty aspect of the proposed mechanism is that it guarantees distributing different keys with different lengths to all nodes at the same time. In addition, an intelligent eavesdropper model has been considered. Simulation results prove the high performance of the proposed scheme and its robustness against channel estimation errors, and immunity against eavesdroppers.

Keywords Physical layer security · Key distribution · Internet of things

1 Introduction

Internet of Things (IoT) paradigm enables all objects around us to interact with each other over the Internet [1]. Unlimited number of IoT applications are being developed concerning all the fields such as agricultural, military, health care, and industrial fields [2]. As such, a huge investment is being directed towards IoT, which is expected to reach tens of trillions by 2020 [3].

Due to the widespread nature of IoT and the different standards and technologies included, security is a main concern. As such, a significant amount of recent research is paid for security in IoT [4]. Improving the confidentiality, privacy and integrity by means of encryption and authentication in the conventional security protocols usually requires secret keys to be shared among the nodes of the network. Employing conventional key distribution mechanisms for IoT networks might be not secure enough to hide keys from eavesdroppers. In addition, overhead and complexity will consume the limited resources equipped at the distributed nodes in IoT networks [5].

Physical layer security presents an efficient and lightweight secure solutions for the different aspects of security [6]. In physical layer security, parameters of the physical layer, such as channel characteristics, modulation, channel coding, bit-to-symbol mapping, power control and others, are exploited to attain a secure link between communicators. For example, transmit power control is used to accomplish confidentiality of the transmitted data in [7, 8], where it is tuned to degrade the signal-to-noise ratio (SNR) at the eavesdropper side. Also, hiding the modulation order and type from eavesdroppers are also used for the same purpose in [9, 10]. Random and unique channel characteristics are exploited to accomplish authentication and verification in [11–13].

✉ Mohanad Alhasanat
mohanadhasanat@ahu.edu.jo

Saud Althunibat
saud.althunibat@ahu.edu.jo

Khalid A. Darabkh
k.darabkeh@ju.edu.jo

Abdullah Alhasanat
abad@ahu.edu.jo; a.ismail@unizwa.edu.om

Moath Alsafasfeh
moath.alsafasfeh@ahu.edu.jo

1 Department of Computer Engineering, Al-Hussein Bin Talal University, Ma'an, Jordan

2 Department of Communications Engineering, Al-Hussein Bin Talal University, Ma'an, Jordan

3 Computer Engineering Department, School of Engineering, The University of Jordan, Amman 11942, Jordan

4 Department of Electrical and Computer Engineering, College of Engineering and Architecture, University of Nizwa, P.O. 33 Postal Code 616, Nizwa, Oman

In the literature, many key distribution mechanisms have been built based on the physical-layer security. In [14], the phase of the channel coefficients is quantized to obtain the key, while the differential phase of two frequency channels is also quantized to obtain the key in [15]. In [16], the deep feed that occurs in the channel envelope is exploited to generate correlated bit streams at the two communicating nodes. Specifically, both nodes estimate the channel envelope, and once the channel envelope falls below a threshold value a bit 1 is added to the stream. Otherwise, a bit 0 is added. Due to the channel reciprocity, both streams should be correlated, and thus, they can be used to agree on a common key. In [17], the Received Signal Strength (RSS) is sampled several times and passed to a quantizer to extract the key. An adaptive quantizer that adapts the quantization thresholds for each block of sampled values is used to overcome active attackers. In [18], the impact of the random noise on the proposal of [17] is eliminated by considering the relative difference between RSS sampled values. Apart from the RSS based generation, the channel phase has been used due to its high robustness against attackers. Channel phase is unrelated to the transmission distance, and thus, it is hard to be predicted [19]. In [20–22], the channel phase is estimated and quantized to generate the key. The range of the channel phase is divided into regions, where each region refers to a specific quantization level. Aiming at reducing the key mismatch due to the imperfect phase estimation especially at the region boundaries, [23] proposes guard intervals between regions to reduce the estimation errors. Specifically, if an estimated value lies in a guard interval, it will be neglected. Other physical layer security key distributions have been built on the above discussed works can be found in [19, 24–27] and references therein.

In this paper, a novel physical-layer key distribution mechanism is proposed. The proposed mechanism exploits the random, independent and unique channel characteristics between any two communicators to deliver the key. Briefly, the Central Entity (CE) broadcasts a number of random signals that are demodulated and decoded at each node based on a different modulation type. As such, each node will obtain a different key with a different length from its own decoded bits. The modulation order used at each node is decided based on the magnitude of its channel to the CE, and the corresponding constellation diagram is rotated by an angle equals to the phase of the estimated channel to the CE. Notice that a channel estimation process is run before commencing the key distribution, and the estimated channel between the CE and a node is kept secret and is unavailable at any other parties. Simulation results show the high performance of the proposed mechanism, the robustness against channel estimation errors, and immunity against eavesdroppers.

Compared to the previous works, the proposed key distribution mechanism has the following differences: i) It distributes the keys among all nodes within the network (regardless of their number) at the same time, ii) It guarantees that all keys are independent due to the dependency to the random channel characteristics, and iii) The distributed keys are of different lengths, which will complicates the eavesdropper task.

The rest of the paper is organized as follows. Section 2 describes the system model. The proposed mechanism is proposed in Section 3. The considered eavesdropper model is presented in Section 4. Simulation results are shown and discussed in Section 5, and conclusions are drawn in Section 6.

2 System model

A network of N nodes and managed by a CE is considered. Nodes are all assumed to be distributed within the communication range of the CE. The channel distribution between the N nodes and the CE is assumed independent and identically distributed. For a specific time instant, the channel vector is denoted by $\mathbf{h} = [h_1, h_2, \cdots, h_N]$, where h_n represents the channel between the n^{th} node and the CE. Without loss of generality, Rayleigh fading model is considered in this work.

As usual, data exchanged between the CE and the nodes must be protected against probable nearby eavesdroppers. As such, data before being transmitted through the channel are encrypted, and, once detected at the receiver's side, are decrypted to retrieve the original data. Among the different types of encryption methods, the symmetric encryption is the most popular one. In symmetric encryption, an identical encryption key is used at both sides.

A primary step in initializing communication links with the nodes is the channel estimation process. This process is performed successively between each node and the CE. In detail, the CE transmits a set of channel estimation signals towards a node. The node is aware of the transmitted signals, and thus, it can obtain the channel values from the received signals. In the next time slot, the node transmits the channel estimation signals towards the CE, which also can obtain an estimate of the channel with the corresponding node. This process is repeated for all nodes. Such a design keeps the channel values hidden from any other parties like eavesdroppers.

3 Physical-layer key distribution mechanism

The proposed mechanism guarantees distributing independent keys for all nodes within the network at the same

time. The basic assumption of the proposed mechanism is that the channel value is known only at the CE and the corresponding node.

Upon estimating the channel values h's , the CE starts by broadcasting L random signals, denoted by $\mathbf{s} = [s_1, s_2, \cdots, s_L]$, towards all the nodes. Each node will receive a corrupted version of the L signals due to the channel effect and the added noise. Specifically, the received signal at the n^{th} node during the ℓ^{th} transmission can be expressed as follows

$$y_{n\ell} = h_{n\ell} s_\ell + w_\ell \tag{1}$$

where w_ℓ is the additive white complex Gaussian noise with zero mean and a variance of σ^2.

Once a signal is received, it is passed to a demodulator whose properties are determined based on the channel value of the corresponding node. Specifically, the order of demodulator M is decided based on the channel magnitude, and the selected signal constellation is rotated by an angle equal to the estimated channel phase. Consequently, each node will detect different bits from the received signals. All the detected bits from the L signals represent the encryption key, which might be different in length from node to another.

Aiming at selecting the modulation order, the range of the channel magnitude is divided into K intervals I_1, I_2, ... I_K, where I_k denotes the k^{th} interval. Consequently, if the channel magnitude of a specific node lies in the I_k interval, the demodulator order is set to 2^k. Also, the constellation diagram of the selected demodulator is rotated by an angle that is equal to the estimated channel phase.

The detection at the nodes side can be mathematically expressed as follows

$$\tilde{x}_\ell = \arg\min_{x \in \mathcal{X}_n} \|y_{n\ell} - x\|^2, \tag{2}$$

where $\mathcal{X}_n$ is the signal set of the adopted signal at the n^{th} node.

3.1 An example

Consider a network of 4 nodes and a CE. The results of the channel estimation process between each node and the CE are as follows $h_1 = 2.3\angle 15^o$, $h_2 = 4.1\angle 3^o$, $h_3 = 0.6\angle 75^o$ and $h_4 = 6.8\angle 195^o$, as shown in Table 1. The predefined set of modulation orders includes BPSK, QPSK, 8PSK, 16PSK, and 32PSK. Each modulation order refers to an interval on the channel magnitude range as shown in Table 2. Based on the estimated channel magnitudes, nodes will use the following modulations 16PSK, 64PSK, BPSK and 128PSK, respectively. Also, based on the estimated channel phases, nodes will rotate the constellation diagrams by 15^o, 3^o, 75^o and 195^o, respectively. Consider that the first emitted signal from the CE is $s = 0.9\angle 65^o$, and for simplicity, assume no noise is present at the receivers' side. Therefore, the received signals at the nodes are as follows $y_1 = 2.07\angle 80^o$, $y_2 = 3.69\angle 68^o$, $y_3 = 0.54\angle 140^o$ and $y_4 = 6.12\angle 260^o$. As such, based on the selected constellation diagrams, nodes will detect the following: 0010 for node 1, 001010 for node 2, 0 for node 3, and 0011100 for node 4. Notice that each node interprets the received signal to different bits with different lengths. The CE will resume broadcasting the rest of the L signals, and nodes will individually detect them to different symbols. Upon delivering the whole L signals, each node will detect its own key. Notice that the CE will also obtain all the nodes' keys as it is aware of the channel values of each node.

Table 1 An example of the proposed key distribution mechanism $s = 0.9\angle 65^o$

Node	Channel Magnitude	Channel phase	Selected Modulation	Received Signal	Detected bits
Node 1	2.3	15^o	16PSK	$2.07\angle 80^o$	0010
Node 2	4.1	3^o	64PSK	$3.69\angle 68^o$	001010
Node 3	0.6	75^o	BPSK	$0.54\angle 140^o$	0
Node 4	6.8	195^o	128PSK	$6.12\angle 260^o$	0011100

It is worth highlighting that a key can be incorrectly detected due to either the channel estimation errors or the added white noise at the nodes' sides. Although improving the signal-to-noise ratio by controlling the transmitted power can decrease the probability of erroneous keys, a reconciliation phase is a popular technique to correct the key for each node.

4 Eavesdropper model

Aiming to evaluate the robustness of the proposed mechanism against eavesdroppers, we consider the presence of an intelligent eavesdropper model. The considered eavesdropper has the ability to estimate/ predict the channel values between the CE and the distributed nodes with an error margin. Mathematically, the estimated value of h_n at the eavesdropper side is denoted by $\tilde{h}_n$ and expressed as follows

$$\tilde{h}_n = h_n + e_n, \tag{3}$$

where e_n is a random variable representing the estimation/prediction error at the eavesdropper. e_n is assumed a complex Gaussian random variable with 0 mean and α variance.

It is also assumed that the eavesdropper is aware of its channel value with the CE, which is denoted by g_ℓ where ℓ refers to the transmission time index. Once the

Table 2 An example for the magnitude interval design in the proposed mechanism

Modulation	BPSK	QPSK	8PSK	16PSK	32PSK	64PSK	128PSK
Magnitude Interval	(0, 0.7)	[0.7, 1.4)	[1.4, 2.1)	[2.1, 2.8)	[2.8, 3.5)	[3.5, 4.2)	[4.2, ∞)

CE broadcasts a signal, say s_ℓ, the received signal at the eavesdropper r_ℓ can be expressed as follows

$$r_\ell = g_\ell s_\ell + z_\ell, \tag{4}$$

where z_ℓ is the additive white complex Gaussian noise with zero mean and σ^2 variance.

Before decoding the signal, the eavesdropper equalizes the impact of the channel to obtain a corrupted version of the transmitted signal, denoted by $\tilde{s}_\ell$, which is given as follows

$$\tilde{s}_\ell = \frac{g_\ell^*}{|g_\ell|^2} r_\ell = s_\ell + \frac{g_\ell^*}{|g_\ell|^2} z_\ell, \tag{5}$$

where g_ℓ^* and $|g_\ell|^2$ represent the complex conjugate and the squared value of g_ℓ, respectively.

Now, to obtain the decoded key bits included in the message at the n^{th} node,

$$\tilde{x}_\ell = \arg \min_{x \in \tilde{\mathcal{X}}_n} \|\tilde{h}_n \tilde{s}_\ell - x\|^2, \tag{6}$$

where $\tilde{\mathcal{X}}_n$ denotes the adopted constellation of the n^{th} node, obtained by the estimated channel at the eavesdropper side (i.e., $\tilde{h}_n$).

5 Performance evaluation and simulation results

In this section, the performance of the proposed physical-layer key distribution mechanism is evaluated through simulations. The evaluation is in terms of the average bit error rate in the distributed key at the nodes, and the immunity against eavesdropper. Also, the impact of the channel estimation errors at either the CE or the nodes is analyzed and discussed. In the simulations, 7 modulation orders as follows 2,4,8,16,32,64 and 128, where PSK modulation type is adopted. The interval width for all modulation orders is fixed and set to Δ. The average power of the broad-casted signals from the CE is set to unity. As such, the signal-to-noise ratio is defined as $\frac{1}{\sigma^2}$.

As explained earlier, the proposed schemes assigns different keys with different lengths to the nodes at the same time. Fig. 1 shows the key length for each node from a random iteration. As shown, different key lengths are obtained based on the channel characteristics for each node with the CE. For example, node 1 obtains a key of 68 bits, while node 4 obtains a key of length 39 bits.

The average BER of the obtained keys at the nodes is plotted versus the average SNR in Fig. 2 at different values of Δ. The number of nodes is set to $N = 10$, and the number of signals is $L = 20$. Different values of the parameter $\Delta = 0.25, 0.5, 0.75$ and 1 are considered. Increasing the SNR value will definitely improves the performance of the proposed mechanism as the impact of the added noise diminishes. The impact of the parameter Δ which represents the interval width can be realized from the figure. Specifically, as Δ increases the BER decreases. This is due to the fact that narrow intervals (i.e. low values of Δ) magnifies the impact of the noise, which consequently, increases the added noise at the nodes' sides.

Figure 3 depicts the impact of the probable errors in the channel estimation process. It is expected that both sides (i.e., the CE and the nodes) suffer from the added noise, and hence, their estimated channel values will not be perfect. It is widely accepted that the channel estimation error can be modeled as a complex Gaussian random variable with zero mean and a variance equal to the noise variance σ^2. The average BER versus the average SNR in presence of the channel estimation error is shown in Fig. 3 for $N = 10$, $L = 20$ and $\Delta = 0.5$. The curve referred to the perfect channel estimation process is added for comparison reasons. As shown, less than 1 dB performance loss due to the channel estimation error, which decreases as the average SNR increases.

The immunity of the proposed key distribution mechanism against the considered eavesdropper is depicted in Fig. 4, where the average BER in the obtained keys at the nodes and the eavesdropper versus the average SNR is plotted. The variance of the estimation/prediction errors made

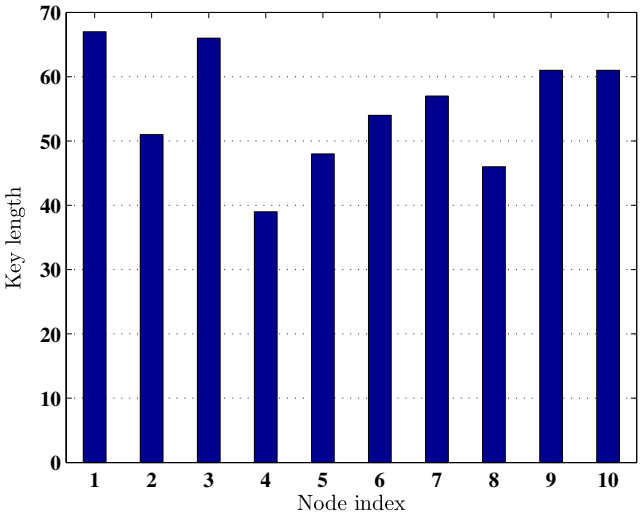

Fig. 1 The key length for each node in a random iteration. ($N = 10$, $L = 20$, and $\Delta = 0.5$)

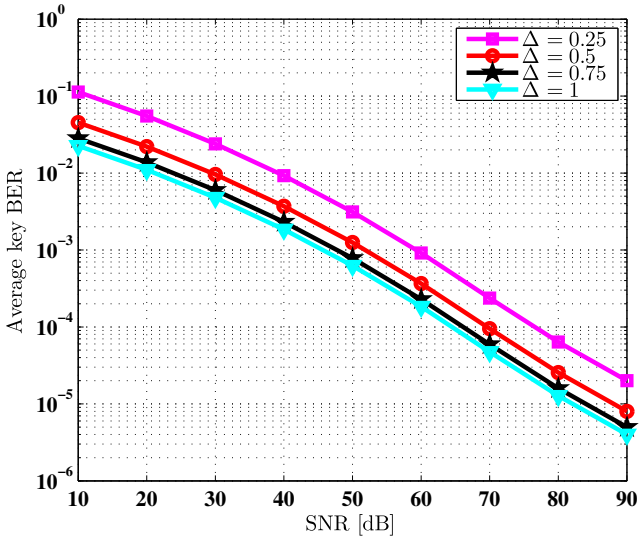

Fig. 2 The average BER at the obtained keys versus the average SNR at different values of Δ. ($N = 10$, $L = 20$, and $\Delta = 0.25, 0.5, 0.75$ and 1)

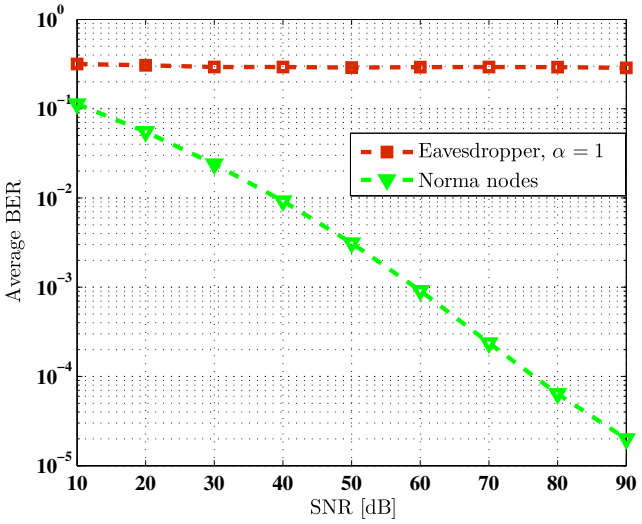

Fig. 4 The average BER at the obtained keys versus the average SNR for the normal nodes and the considered eavesdropper. ($N = 10$, $L = 20$, $\Delta = 0.25$ and $\alpha = 1$)

by the eavesdropper is set to $\alpha = 1$, and the width interval is set to $\Delta = 0.25$. It is evident that the eavesdropper has a very low performance and will not be able to obtain the keys of the normal nodes.

To better analyze the impact of the parameter α on the performance of the eavesdropper, Fig. 5 plots the average BER versus the parameter α at different values of Δ and average SNR of 30 dB. Intuitively, as the variance of the estimation/prediction error performed by the eavesdropper increases, the BER increases as clearly shown in the figure for all values of Δ. The other important observation is that, at a fixed value of α, the BER at the eavesdropper decreases as the interval width increases. This is due to the fact that large values of the interval width alleviate the effect of the errors made by the eavesdropper, and hence, it can select the correct modulation order, and decode the signals to obtain a correct key bits.

Comparing the effect of Δ on the BER of the nodes (Fig. 2) and on the BER of the eavesdropper (Fig. 5), it can be concluded that Δ should be carefully adjusted in order to degrade the BER at the eavesdropper without degrading the BER performance at the normal nodes.

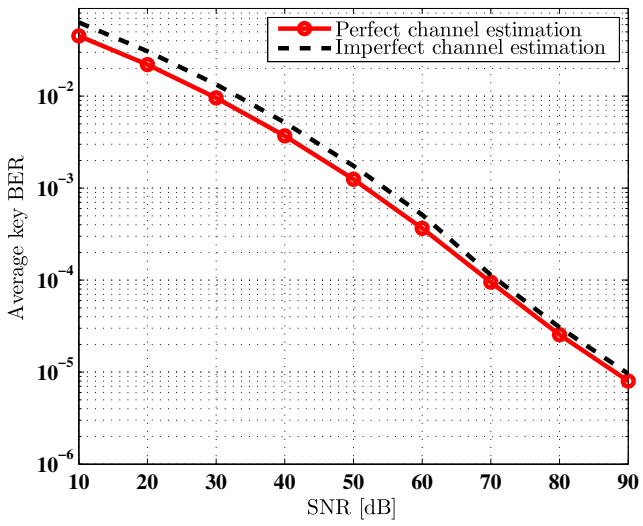

Fig. 3 The average BER at the obtained keys versus the average SNR with the presence of channel estimation error. ($N = 10$, $L = 20$, and $\Delta = 0.5$)

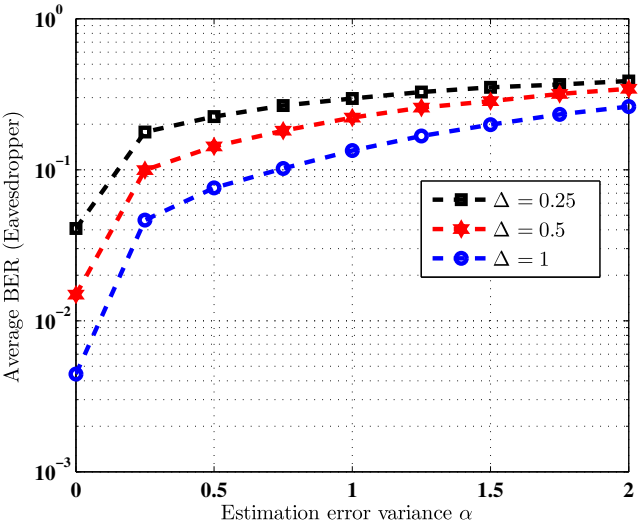

Fig. 5 The average BER at the obtained keys versus the variance of the estimation errors at the eavesdropper at different values of Δ. ($N = 10$, $L = 20$, and SNR = 30)

6 Conclusion

A novel physical layer key distribution mechanism for IoT networks has been proposed in this paper. The diverse, independent and random channel characteristics between each node and the central entity can guarantee extracting uncorrelated keys. The proposed mechanism implies broadcasting random signals to the nodes from the central entity. Each node will decode the received signal by independent signal modulation type and order. The order of the modulation is selected based on the channel magnitude, and its corresponding constellation diagram is rotated by an angle equal to the channel phase. Simulation results demonstrate the high performance of the proposed scheme, robustness against channel estimation error, and immunity against intelligent eavesdroppers.

References

1. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Comput Netw 54.15:2787–2805
2. Luong NC, Hoang DT, Wang P, Niyato D, Kim DI, Han Z (2016) Data collection and wireless communication in internet of things (IoT) using economic analysis and pricing models: a survey. IEEE Commun Surv Tutorials 18(4):2546–2590
3. Wortmann F, Flüchter K (2015) Internet of things. Business Inf Syst Eng 57.3:221–224
4. Granjal J, Monteiro E, Silva JS (2015) Security for the internet of things: a survey of existing protocols and open research issues. IEEE Commun Surv Tutorials 17(3):1294–1312
5. Mukherjee A (2015) Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints. Proc IEEE 103.10:1747–1761
6. Shiu YS, Chang SY, Wu HC, Huang SCH, Chen HH (2011) Physical layer security in wireless networks: a tutorial. IEEE Wireless Commun 18(2):66–74
7. Khisti A, Wornell GW (2010) Secure transmission with multiple antennas: the MIMOME channel. IEEE Trans Inform Theory 56(11):5515–5532
8. Liang Y, Poor HV (2008) Multiple-access channels with confidential messages. IEEE Trans Inform Theory 54(3):976–1002
9. Husain MI et al (2012) CD-PHY: physical layer security in wireless networks through constellation diversity. In: Proceedings IEEE MILCOM, pp 1–9
10. Althunibat S et al (2017) A physical-layer security scheme by phase-based adaptive modulation. IEEE Trans Veh Technol 66(11):9931–9942
11. Hou W, Wang X, Chouinard JY, Refaey A (2014) Physical Layer Authentication for Mobile Systems with Time-Varying Carrier Frequency Offsets. IEEE Trans Commun 62(5):1658–1667
12. Xiao L et al (2007) Fingerprints in the ether: Using the physical layer for wireless authentication. IEEE ICC, Glasgow, 4646–4651
13. Althunibat S et al (2018) Physical-layer entity authentication scheme for mobile MIMO systems. IET Commun 12.6:712–718
14. Sayeed A, Perrig A (2008) Secure wireless communications: secret keys through multipath. IEEE ICASSP
15. Hassan AA, Stark WE, Hershey JE, Chennakeshu S (1996) Cryptographic key agreement for mobile radio. Digital Signal Process 207-212:6
16. Azimi-sadjadi B et al (2007) Robust key generation from signal envelopes in wireless networks. In: Proceedings of the 14th ACM conference on computer and communications security. ACM
17. Premnath SN, Jana S, Croft J, Gowda PL, Clark M, Kasera SK et al (2013) Secret key extraction from wireless signal strength in real environments. IEEE Trans Mob Comput 12(5):917–930. https://doi.org/10.1109/TMC.2012.63
18. Zan B, Gruteser M, Hu F (2012) Improving robustness of key extraction from wireless channels with differential techniques. IEEE ICNC, 980–984
19. Wang T, Liu Y, Vasilakos AV (2015) Survey on channel reciprocity based key establishment techniques for wireless systems. Wireless Netw 21.6:1835–1846
20. Mathur S, Miller R, Varshavsky A, Trappe W, Mandayam N (2011) Proximate: proximity-based secure pairing using ambient wireless signals. In: Proceedings of ACM Mobisys, New York, NY, USA
21. E.Shehadeh Y, Alfandi O, Hogrefe D (2012) On improving the robustness of physical-layer key extraction mechanisms against delay and mobility. IEEE IWCMC, 1028–1033
22. Wang Q et al (2011) Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In: Proceedings of IEEE INFOCOM, pp 1422–1430
23. El Hajj Shehadeh Y, Hogrefe D (2011) An optimal guardintervals based mechanism for key generation from multipath wireless channels. In: Proceedings of IFIP NTMS, pp 1–5
24. Liu Y et al (2012) Exploiting channel diversity in secret key generation from multipath fading randomness. IEEE Trans Inf Forensics Secur 7(5):1484–1497
25. Zeng K (2015) Physical layer key generation in wireless networks: challenges and opportunities. IEEE Commun Mag 53.6:33–39
26. Edman M et al (2016) On the security of key extraction from measuring physical quantities. IEEE Trans Inf Forensics Secur 11.8:1796–1806
27. Zhang J et al (2016) Key generation from wireless channels: a review. IEEE Access 4:614–626