A Novel Physical-layer Security Scheme for Internet of Things

Yu Jiang¹,∗ and Siqing Chen¹
¹School of Cyber Science and Engineering, Southeast University, Nanjing, China

*Corresponding author e-mail: jiangyu@seu.edu.cn

Abstract. Addressing the security of Internet of Things from the physical layer is a promising study. This paper proposes a security strategy for authentication and conversation key generation between IoT devices at the physical layer. The physical layer parameters are constructed according to the received signal strengths of different frequencies. With the help of packet interleaving, smoothing and normalization, the double threshold quantized data are used for the key agreement and location-based authentication. We deploy the IoT nodes to evaluate the performance of the proposed method and demonstrate the feasibility of implementation in low cost and static environments.

1. Introduction

Modern communication technology has brought us into the era of Internet of Things (IoT). When the IoT provides us with convenience, it also creates many security problems [1]. The openness of wireless channel causes attackers to launch various active and passive attacks [2], so security must be considered during the design phase of IoT. Researchers use traditional identity authentication [3] and encryption technologies [4] to solve the security problems of IoT. However, traditional security mechanisms are not designed for IoT applications [5]. Existing work using pre-allocated keys and simplified public key methods have many limitations. Therefore, the IoT liking Zigbee network requires new security strategies.

As a new wireless security technology, the physical layer security strategy has become a hot research topic [6]. The research is divided into wireless device identification and key generation. Identification method by radio frequency (RF) fingerprinting for wireless devices belongs to the physical layer authentication [7]. The RF fingerprint reflects the internal characteristics of wireless device and can be used for its unique identification [8]. The key generated from the radio channel feature reflects the channel uniqueness, which offers a opportunity to realize the key sharing between both parties [9].

This paper proposes a security strategy for authentication and encryption between IoT platforms at physical layer. The signal strength of multi-frequency is used to generate the key and identity. We deploy the IoT nodes to evaluate the performance of the proposed method and demonstrate the feasibility of implementation in low cost and static environments.

The remaining part of this paper is organized as follows: Section 2 shows the related work. Section 3 introduces the communication model. Section 4 describes the key agreement process. Section 5 introduces the experiment of the IoT platform and conclusions can be found in Section 6.
2. Background

2.1. Related work of physical-layer identification
In previous works, [9] introduced the principle on physical-layer identification of wireless devices. A large quantity of the works demonstrated the feasibility and validity of RF fingerprint approach for wireless device identification among different wireless systems. Theoretically, all wireless communication devices can extract radio frequency fingerprints for identification. So far, a variety of wireless devices have been researched on RF fingerprint extraction and recognition. The most state-of-art RF fingerprint identification methods can be divided into transient-based techniques and modulation based techniques.

The transient-based techniques measure the variations of RF signal over time for device identification. It is worth noting that high receiver sensitivity and linearity is required to extract slight transient features from the received signal in most of the transient-based systems.

The modulation-based techniques obtain the stable features by signal processing. Frequency error, SYNC correlation, I/Q origin offset, magnitude errors and phase errors are extracted for identification.

2.2. Related work of key generation
Different from the traditional mathematical theory of cryptography, wireless key generation utilizes the randomness of channel parameters to achieve security and the most commonly used parameters are received-signal strength (RSS) and channel state information (CSI).

RSS is easy to obtain but vulnerable to the noise, which limits the consistency of key generation. At present, many hardware terminals support RSS output, making it the most commonly used channel parameter in key generation. Most RSS-based research works on IEEE 802.11 or IEEE 802.15.4 platforms.

CSI including channel frequency response (CFR) and channel impulse response (CIR) describes the channel properties of the communication link. Based on the current research results, CSI is more accurate than RSS to produce a high key generation rate (KGR).

2.3. Summary
In the above study, many physical layer parameters are obtained in the laboratory through high-end instruments. It is of practical significance to use high-end instruments for security protection of high-value terminals, but for low-cost IoT, the cost of the security solution needs to correspond to the value of the node itself. Most existing physical layer security methods use high-end instruments to collect data, making it difficult to go to the actual application scenario. Thus, the IoT needs a lightweight and low-cost physical layer security strategy urgently.

3. Communication model
The wireless communication model is shown in Fig. 1. A and B are the legal users and C is the illegal user who can obtain the communication data between the normal users. The model satisfies the following conditions:
1) Reciprocity: the legal users share the same characteristics of wireless channel.
2) Spatial decorrelation: The distance between the legal and illegal users are greater than $\lambda/2$, where $\lambda$ is the wavelength of communication frequency.
3) Space and time variation: temporal and spatial changes of channel cause the changes in channel characteristics.
4. Key agreement process
The key agreement process mainly includes the following four steps: channel measurement, parameter quantization, information reconciliation and privacy amplification. The proposed key agreement process is shown in Fig. 2, where A is the master and B is the slave.

As shown in Fig. 2, the first step is to measure the RSS parameters of different frequencies between the master and slave. Before the parameter quantization, the pretreatments need to be executed for the original measurement data. Then the processed data are quantified in the next step. We use the mean and standard deviation to determine the quantization threshold, which is shown in equation 1.

$$t_+ = mean + k \times \text{std}$$

$$t_- = mean - k \times \text{std}$$

(1)

where $k$ is the adjustment parameter and $k \in (0,1)$. The value greater than $t_+$ is quantized to 1 and the value less than $t_-$ is quantized to 0. Then, all other values are discarded directly and the quantization equation is represented as
In most cases, the quantified keys obtained by both parties may be different. The error correction method of traditional cryptosystem is not suitable for use in the IoT platform due to the high computational complexity. Due to the high consistency of key negotiation in our method, we ignore the error correction process to save the energy of node.

At the last step of key verification, the two parties exchange and compare the hash values of the generated key. As shown in Fig. 2, the SHA1 is used as the hash calculation method. After the comparison, both parties will inform the other party of the result. If the keys are equal, the key negotiation process ends, otherwise the process is repeated.

5. Result analysis

5.1. Platform construction
We use the CC1101 module as the IoT experimental platform, which is able to obtain RSSs by packets. The experiments are executed in indoor and outdoor environments for more than 100 times. A and B use the cc1101 platforms for key negotiation. The mean values of RSS' measurement for both parties are very close in Fig. 3, which indicates that the channel has good reciprocity.

Then, we process the original RSS values according to the flow of the proposed algorithm until the keys are obtained. The generated keys of both parties are shown in Fig. 4. As shown in the Figure, the two curves coincide, which means the generated keys are equal. Therefore, the shared key can be used for subsequent secure communication between the legal users.

5.2. Key changes in static environments
When the channel state is stable, the proposed method can obtain stable keys. In order to ensure sufficient security, the key needs to be changed periodically. In the traditional communication model, channel state changes are generated by motion, but in the IoT environment, the node and the
surrounding environment are usually fixed. Fortunately, the CC1101 module provides a way to change the channel state. Different channel states can be obtained by configuring the RF parameters of the cc1101 module.

Through the modification of CC1101 RF parameters including frequency step, transmission data rate, modulation mode, we conduct actual experimental measurements. Based on the experimental results, changing the frequency step size and the transmission data rate can change the channel state to obtain a shared and variable key. It is worth noting that when the step size is too large or the transmission rate is too high, the key disagreement rate will significantly increase. Therefore, modifying the RF parameters can change the channel status to update the key within a certain range.

5.3. Identity authentication strategy
Existing physical layer authentication schemes utilize parasitic device features in transmitted signals, but these features require expensive instrument to extract, which is not suitable for IoT platform. Accordingly, this paper designs a node authentication strategy based on channel state characteristics. When a node is deployed to the IoT network, it sets a special parameter configuration for authentication. Next, the node and its neighbor node execute the proposed key generation process and they use the key as the identity of the other. In the process of node authentication, both sides set the RF parameters for authentication to measure each other.

In the process of key generation, the keys are required to be identical, while the requirement of authentication is not so strict. We can set an authentication threshold and compare it with the key consistency. When the key consistency exceeds the threshold, the authentication succeeds. The setting of specific threshold is determined by the complexity of the channel environment, so this method is suitable for IoT nodes in static environment.

6. Conclusion
This paper proposes a security strategy for authentication and conversation key generation between IoT devices at the physical layer. The physical layer parameters are constructed according to the received signal strengths of different frequencies. Through the data preprocessing methods such as packet interleaving, smoothing and normalization, the double threshold quantized data are used for the key generation and identification. We use the IoT nodes to evaluate the performance of the proposed method and demonstrate the feasibility of implementation in low cost and static environments.

Acknowledgments
This work was supported by the National Natural Science Foundation of China (Grant No. 61601114, No. 61602113, No. 61571110).

References
[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, ”A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends”, IEEE Proceedings, vol. 104, no. 9, Sep. 2016, pp. 1727-1765
[2] B. Wu, J. Chen, J. Wu, and M. Cardei, “A survey of attacks and countermeasures in mobile ad hoc networks,” in Wireless Network Security, Y. Xiao, X. Shen, and D.-Z. Du, Eds. New York, NY, USA: Springer, 2007, pp. 103–135
[3] X. Wang, P. Hao, and L. Hanzo, ”Physical-layer authentication for wireless security enhancement: current challenges and future developments”, IEEE Communications Magazine, vol. 54, no. 6, Jun. 2016, pp. 152-158.
[4] L. Chen, J. Ji, and Z. Zhang, Eds., Wireless Network Security : Theories and Applications. Springer, 2013
[5] J. Jung and J. Lee, ”ZigBee device design and implementation for context-aware U-healthcare system”, in Proceedings of 2nd International Conference of Systems and Networks Communications, 2007.
[6] Zhang J, Duong T Q, Marshall A, et al. "Key Generation From Wireless Channels: A Review." IEEE Access 4.3(2017):614-626.
[7] P.L. Yu, G. Verma, and B.M. Sadler, "Wireless physical layer authentication via fingerprint embedding", IEEE Communications Magazine, vol. 53, no. 6, Jun. 2015, pp. 48-53.

[8] B. Danev, D. Zanetti and S. Capkun, "On Physical-Layer Identification of Wireless Devices", Computing Surveys (CSUR), vol. 45, no. 1, Nov. 2012, pp. 1-29.

[9] Sayeed, Akbar, and A. Perrig. "Secure wireless communications: Secret keys through multipath." IEEE International Conference on Acoustics, Speech and Signal Processing IEEE, 2008:3013-3016.