2版

様　式　C－１９、F－１９－１、Z－１９　（共通）

科研費
KAKENHI

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月　 ２ 日現在

機関番号： ３２６６３

研究種目： 研究活動スタート支援

研究期間： 2018～2019

課題番号： １８H０６４７０・１９K２１５３８

研究課題名（和文）Study on a physical layer security framework for establishing trustworthy IoT systems

研究課題名（英文）Study on a physical layer security framework for establishing trustworthy IoT systems

研究代表者

朱　金暁（ZHU, Jinxiao）

東洋大学・情報連携学部・助教

研究者番号：３０７５４３２９

交付決定額（研究期間全体）：（直接経費）　　2,300,000円

研究成果の概要（和文）：IoTネットワークのセキュリティ問題の解決に向けて、3つの重要なセキュリティトピックを研究した。これらは、物理層セキュリティ（PLS)方法論の基盤技術であり、ワイヤレスセキュリティを実現するために、斬新で有望なアプローチとして広く研究されてきたものである。具体的には、①暗号鍵を使用せずに機密情報を受信機に送信する技術、②物理層でユーザーを識別・認証する技術、③ワイヤレスチャネルのランダム性を使用して暗号化用の鍵を生成する技術について研究した。

研究成果の学術的意義や社会的意義
従来の研究とは異なり、IoTシステムにおける物理層セキュリティ（PLS）に関する3つのトピックを研究した。IoTシステムは、物理デバイスと伝送環境の多様性が特徴であり、この多様性は従来の通信方法に潜在的なセキュリティリスクをもたらしたが、物理層セキュリティ方法は、これらの特徴を利用してセキュリティスキームを設計することができる。
このことから、本研究成果は学術的な研究促進だけでなく、IoT技術の開発の持続的成功にも貢献できる。

研究成果の概要（英文）：Towards solving security issues in the future IoT networks, we studied three important security topics as the fundamentals to support a novel paradigm of security framework. The new paradigm relies on physical layer security (PLS) methodology rather than the traditional cryptography. In particular, we have studied how to transmit confidential information to a receiver without using cryptographic keys, how to identify a user at the physical layer, and how to generate secret keys for cryptography by exploring the intrinsic randomness of wireless channels.

研究分野： 情報学

キーワード： 認証　セキュリティ　PLA　無線通信

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。

１．研究開始当初の背景

As Internet of Things (IoT) systems have been dominating many key application areas, such as factory, transportation and city management, the security issue becomes one of the major concerns there (please see **Figure 1** for some security issues). Traditional security solution mainly relies on cryptography, such as secret key cryptography and public key cryptography, of which the security relies on the assumption either that secret keys have been securely distributed between legitimate users previously or that a malicious user has limited computing power. However, the security established on such assumptions is increasingly questioned in the IoT scenario for the following concerns. First, the increasing number of devices in IoT systems make it extremely hard if not impossible to distribute and manage secret keys. Second, IoT nodes are often vulnerable to physical attacks since they are deployed in a distributed fashion. Third, IoT nodes are typically resource limited, indicating that an attacker would possess relatively more computation resources to break the adopted cryptography system.

① PLS based secret key generation
② PLS based confidential communication
③ PLS based identification and authentication

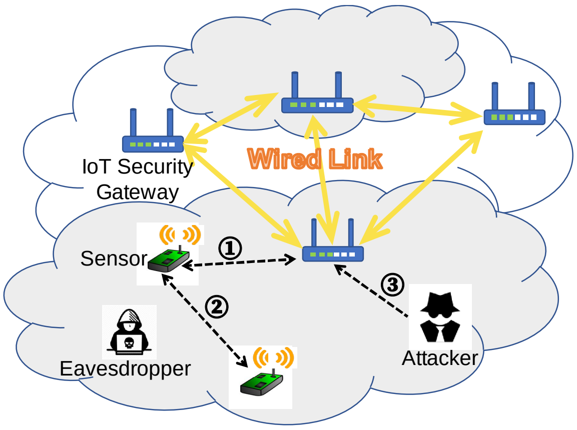

Figure 1 Overview of the PLS-based security framework

２．研究の目的

In this project, we will study physical layer security (PLS) to address these concerns. PLS, of which the security is achieved by exploring the intrinsic randomness of wireless channels, has been widely proved as a novel and promising approach to fulfilling wireless security. Compared with cryptographic solutions in higher layers, PLS achieves ever-lasting information theoretical security without requiring the pre-distribution of secret keys or limited computation power of adversaries. Furthermore, IoT systems are usually deployed in versatile environment, which would serve as potential sources of randomness for PLS method.

The goal of this research is to study a novel IoT security framework integrating PLS and cryptographic solutions in order to establish trustworthy IoT systems. In particular, we will first study three novel PLS schemes in key generation, confidential communication and authentication, respectively, and then integrates the proposed study together with existing cryptographic solution into a unified framework.

３．研究の方法

(1) PLS based secret key generation: This research is to generate secret keys real-timely by channel state information (CSI) between paired users in IoT network. The basic idea is summarized as follows. Two terminals Alice and Bob observe the same random source, e.g., the wireless communication channel between them, and get correlated observation sequences, based on which they agree on the same secret key.

(2) PLS based confidential communication: This research is to apply PLS to transmit confidential information in the presence of an eavesdropper. By applying wiretap channel coding, it has been proved that non-zero secrecy capacity can be achieved as long as the channel to the legitimate user and that to the eavesdropper are not exactly the same. While extensive research effort has been devoted to evaluating capacity without any limit on the block-length of code, our target in this topic is to study the performance of finite-length wiretap coding over channels with random states.

(3) PLS based identification and authentication: This research is to identify if a received signal is from the claimed transmitter using physical layer security approach. Currently, the study of physical layer authentication can be roughly categorized into two types: **channel state information (CSI)** based authentication scheme and **radio-frequency fingerprints (RFF)** based authentication scheme. While CSI based authentication scheme is more suitable for applications in which devices keep online, as the CSI can vary over time and position, RFF based authentication scheme is more suitable for applications with low noise interference, as the RFF are commonly micro-characteristics that can be largely covered up by channel noise. In this project, we will try to find a device-specific RFF feature or CSI feature to identify a device.

(4) IoT Security Framework: Finally, we hope to propose a unified framework to improve the security of IoT networks from physical layer and network layer to service layers by integrating the research results of PLS and traditional cryptographic solutions. For example, the key generated from the above (1) can be provided to upper layers for encryption. Also, the authentication can be used for detection of attackers. Theoretical/simulation evaluation against active and passive attacks will be conducted to provide quantitative understanding on the security performance of the proposed scheme.

４．研究成果

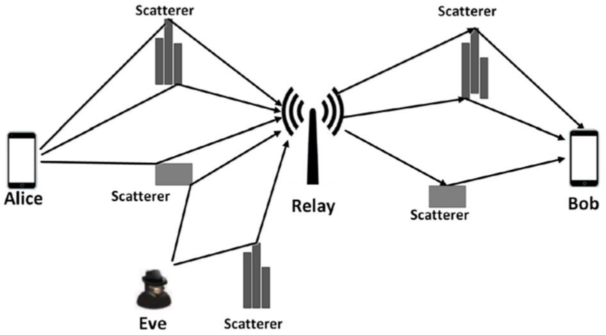

Figure 2 A dual-hop wireless network with an untrusted relay and an adversary (Eve) impersonating the transmitter (Alice)

(1) We studied end-to-end (E2E) physical layer authentication in a dual-hop wireless network with an untrusted relay (see **Figure 2**) and proposed a corresponding CSI-based physical layer authentication scheme. This scheme utilizes the location-specific features of both channel amplitude and delay interval of cascaded channels to discriminate transmitters and adopts the artificial jamming technique to resist against possible replay attack from untrusted relay. More specifically, our scheme was designed based on the fact that it is difficult for an adversary to precisely build the same channel that is being used by a legitimate transmitter-receiver pair, and that the channel for a transmitter-receiver pair is highly correlated over time. Since the relay node is not trustful, the legitimate receiver (named as Bob in our model) sends a jamming signal concurrently with the message frames sent by Alice to confusing the relay node. After receiving the composite signal of jamming and message frames, Bob evaluates the channel amplitude and delay interval and then makes a decision whether the current frame is from Alice or not by binary hypothesis testing. We then derived theoretical formulas to calculate performance of the proposed authentication scheme and wrote a MATLAB simulator to verify the theoretical results. According to our theoretical analysis and simulation results, our scheme is not only resistant to the impersonate attack from an unauthorized transmitter but also resilient to the replay attack from the untrusted relay. It is worth noting that the dual-hop wireless networks we studied serve as a foundation for the study of general multi-hop wireless networks.

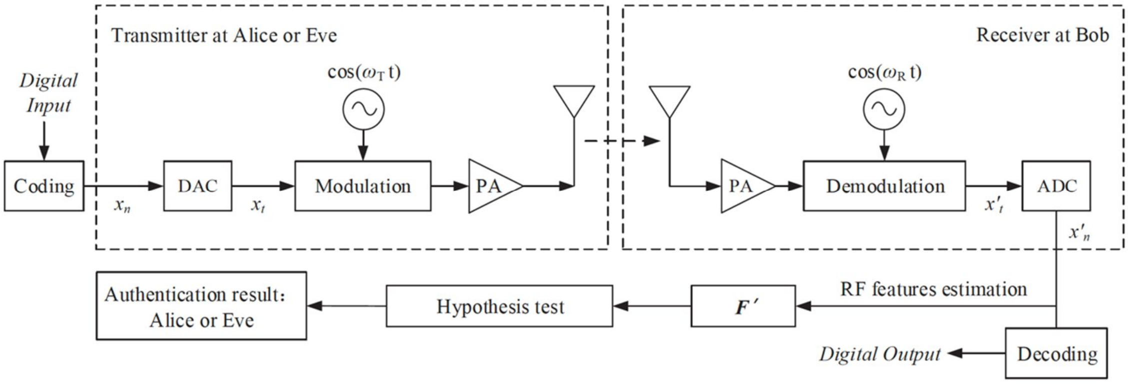

Figure 3 Radio-frequency fingerprints (RFF) based authentication model

(2)For general one-hop communications, we studied how to identify a user with RFF-based authentication. As illustrated in **Figure 3**, the authentication model in our study is composed of radio-frequency (RF) chain at the transmitter, where hardware imperfections cause unforgeable RF features into the transmitted signal, and RF chain at the receiver together with RF features estimation process. In contrast to existing studies on RFF-based authentication, we focused on two non-negligible factors in RF chain, i.e., clock jitter and electronic noise, in the hope of exploring new RF features. Particularly, clock jitter derives from the unstable period of oscillator and electronic noise derives from the random motion of electrons in a resistive materials. These two factors will cause extra jittery of the analog signals, which together with other jittery impacts on the analog signals is called volatility of analog output (VAO). We built a mathematical model of VAO and then studied its fractal dimension, which turns out be a new RF feature. The performance of using the new feature to authenticate devices has been studied both theoretically and numerically. **Figure 4** shows the fractal dimension of the RF signals from two Universal Software Radio Peripheral (USRP) B210 devices. 200 data frames are captured under Quadrature Amplitude Modulation (QAM) and SNR=30dB for each USRP. We can find in **Figure 4** clearly that the fractal dimensions of the two USRP are distinguishable, implying that the fractal dimension can be used as an RF feature. A draft of this research has been written for the publication in the near future.

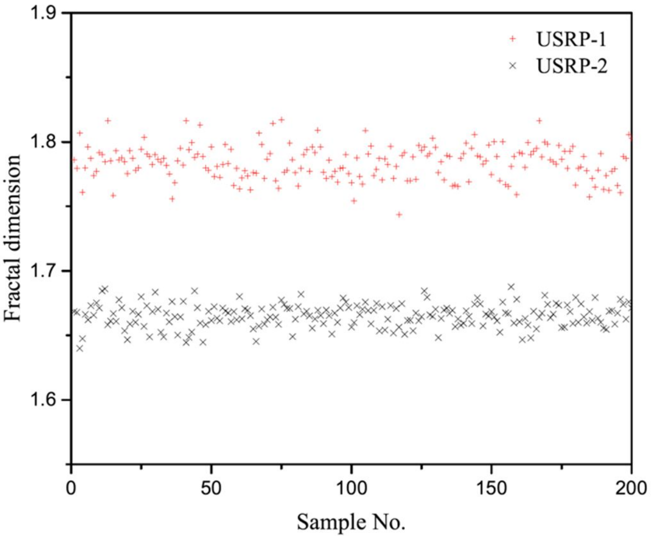

Figure 4 Fractal dimension results of 200 RF signal samples from two different USRPs.

(3) For PLS-based confidential communication, we first studied information rate of finite-length coding over channels with random state. Under the assumption that the channel state information is available at the transmitter and the receiver causally, we proposed a general coding and transmission scheme, and then derived a closed-form outage probability bound based on Sanov's theorem. The outage probability is then applied to establish the maximum rate that is achievable at a given code length and decoding error probability. Next, we also extended the above maximum achievable rate to

the scenarios that CSI is known noncausally. Finally, we developed a simulator in Java to verify our theoretical results. Interestingly, as can be observed from **Figure 5**, our result shows that the maximum achievable rate for the finite block-length under the causal and noncausal assumptions are different while the same capacity for unlimited block-length under the two assumptions is observed in the literature, and that the maximum achievable rate for causal CSI assumption is smaller than the one for noncausal CSI assumption and both rates approach to the capacity as the block-length, *N*, of code increases. A draft of this research has been written for the publication in the near future.

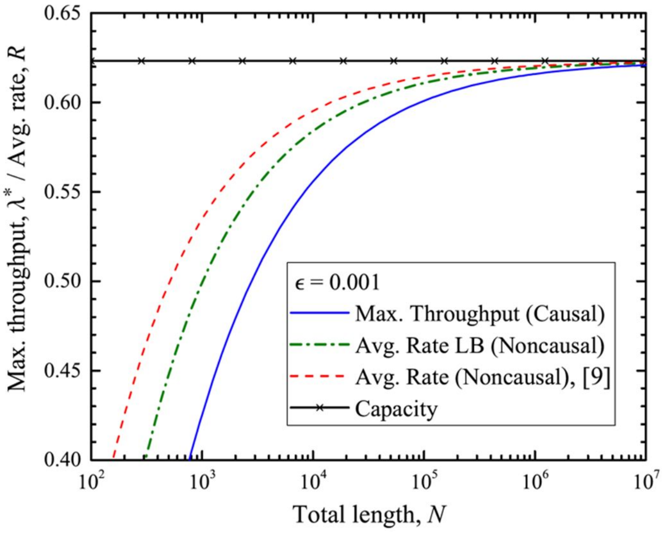

Figure 5 Maximum achievable rate for causal and noncausal CSI assumptions vs. block-length N

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　1件／うちオープンアクセス　1件）

１．著者名 Zhang Pinchang、Zhu Jinxiao、Chen Yin、Jiang Xiaohong	４．巻 7
２．論文標題 End-to-End Physical Layer Authentication for Dual-Hop Wireless Networks	５．発行年 2019年
３．雑誌名 IEEE Access	６．最初と最後の頁 1～15
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2906699	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

〔学会発表〕　計0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考