様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ５ 月 １９ 日現在

機関番号：３２６６３
研究種目：若手研究
研究期間：2020～2022
課題番号：２０Ｋ１９８０１

研究課題名（和文）Experimental and theoretical study on physical layer authentication for IoT systems

研究課題名（英文）Experimental and theoretical study on physical layer authentication for 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）　　3,200,000円

研究成果の概要（和文）：IoTネットワークに接続する無線機器が増えている一方，IoTネットワークで効果的な認証システムを設定することは非常に重要な課題である．本研究では，IoTネットワークにおける無線機器認証の課題の解決へ向けて，実験システムを構築し，無線機器のハードウェアの欠陥で生成された無線信号特徴（RF Fingerprints，無線指紋）を実験システム上で捕え，これらの特徴データを活かした無線機器の認証技術を研究開発した．また，実験とシミュレーションにより開発した認証技術の有効性を示した．

研究成果の学術的意義や社会的意義
本研究の目的は，IoTネットワークにおける無線機器認証の課題を解決することである．従来の認証方法では，無線機器の身分情報を暗号鍵で暗号化して認証を行っていましたが，IoTでは膨大な数の無線機器に対して鍵の配布や管理が非常に困難である．本研究では，暗号鍵を使わない物理層認証方法を研究した．具体的には，実験システムを構築し，人間の指紋のようなデバイス指紋を研究開発して実験システムでその有効性を示した．

研究成果の概要（英文）：With the wide application of internet of things (IoT), setting up an effective authentication system in those networks becomes overwhelming difficult yet urgent. To solve the authentication issue, this project focused on studying radiometric features generated by wireless devices for device authentication from both experimental and theoretical aspects. Specifically, we constructed an experiment system, collected raw radiometric feature data of wireless devices from the system, and designed several identification schemes with the data for device authentication. About the identification schemes, we explored two main approaches: identification with hand-crafted radiometric feature and identification with automatically-generated radiometric feature by deep learning algorithms. Finally, the efficiency of the proposed identification schemes have been verified by experiment and simulation studies.

研究分野：ネットワークセキュリティ

キーワード：物理層認証　無線通信　セキュリティ　デバイス識別

※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、研究者個人に帰属します。

１．研究開始当初の背景

With the wide application of internet of things (IoT), setting up an effective authentication system in those networks becomes overwhelmingly difficult yet urgent. Conventional authentication solutions are usually implemented at upper layers of network OSI (Open Systems Interconnection) model, e.g., IPsec at layer 3, TLS at layer 4, application layer authentications, etc., and **assumes** a cryptographic key is safely shared without any leakage to attackers. ***However, the security relying on such assumption is increasingly questioned in the IoT scenario due to the following concerns*** [Thiele17]. 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 and possibly in unprotected environments. Third, IoT nodes are typically resource limited, indicating that an attacker would possess relatively more computation resources to break the adopted cryptography system.

In this project, I will study physical layer authentication (PLA) to address the above concerns. In contrast with conventional authentication solutions (that place a burden on managing secret keys), the PLA scheme identifies a device by exploring some “born” physical features of radio waves transmitted by the device (please see **Fig. 1** for the relation between PLA and conventional authentications). Such physical features are induced in the *radio frequency* (**RF**) chain, which presents hardware imperfections being randomly generated during manufacturing and is out of human’s control. Thus, they can serve as unforgeable identities for authentication of wireless devices. Observing that most of existing PLA studies are analyzed based on idealized theoretical assumptions, this project is motivated to study PLA by extracting physical features from real experiment dataset.

２．研究の目的

The general objective of this research is to study a novel PLA scheme to enhance the authentication ability of communication systems and protect IoT systems against impersonation attack. As illustrated in **Fig. 1**, our study will be conducted towards the following targets: (i) construct an experiment testbed; (ii) collect and build one dataset for RF feature extraction; (iii) find at least one novel RF feature based on the dataset collecting from real chips; (iv) design multiple-feature joint authentication for a discrimination scale over 400 devices.

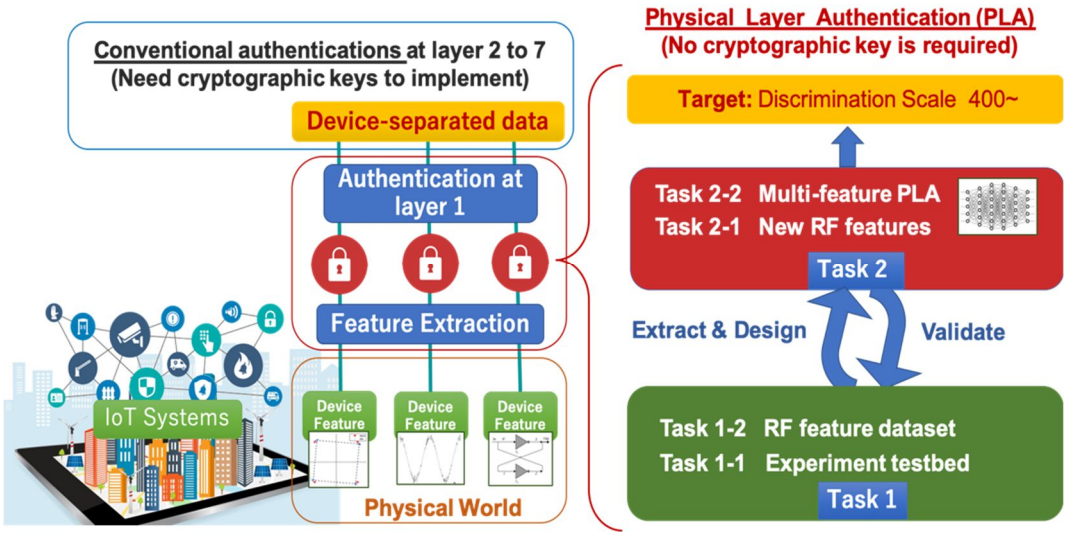


Fig. 1　Our tasks and targets in physical layer authentication (PLA), together with its relation with conventional authentications.

３．研究の方法

Our research was conducted by following the steps below.

(1) Firstly, develop an experiment system and collect raw radiometric data from the system

In **Fig. 2**, we illustrated a typical experiment system in our project, where wireless devices, such as smart phones, USB NICs were used as transmitters, USRP device was configured as a receiver, and the GNU radio software and Python environment running on a work station were used for signal processing, feature calculation and device identification.

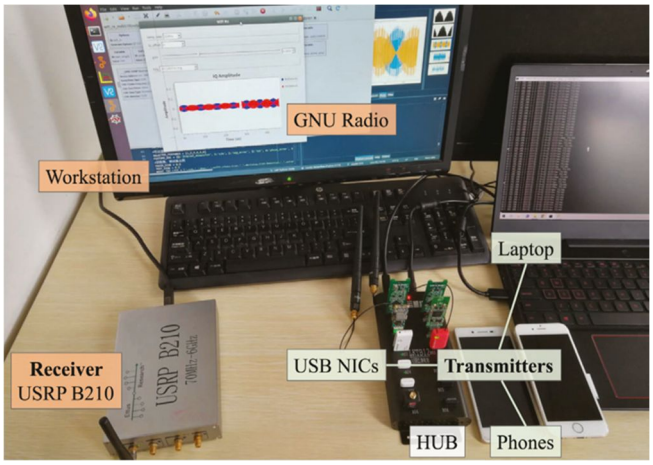


Fig. 2　An experiment system

(2) Design feature extracted algorithms to capture radiometric features of wireless devices

After collecting raw data from the experiment system, we have to extract possible features from various aspects of view. In particular, we first checked the RF chain of a transmitter-receiver pair, analyzed and confirmed possible deviations in time and frequency domains that could be brought by the devices in the RF chain, then designed algorithms to extract the features. It is noted that the number of developed radiometric features is still limited and the corresponding authentication performance is also limited. Thus, we were aimed to propose more features to increase the authentication accuracy.

(3) Study authentication/identification schemes with radiometric features and verify the efficiency of the schemes

After we extracted a radiometric feature, we usually need to verify the efficiency of it from both theoretical and experiment studies. Firstly, we calculated the correlation between the new feature and the existing features. Secondly, we designed parameters of machine learning algorithms to optimize the identification performance of the feature in a certain SNR range.

４．研究成果

In the project, besides the approach we proposed in the beginning of the study, we also studied a new approach for physical layer identification. The first approach is the one we planned before starting and it is to calculate features from the received frames by carefully designed feature extraction algorithms. These features will then be exploited with machine learning algorithms or binary hypothesis to identify and authenticate transmitters. The second approach is to extract features automatically by applying deep learning-based methods, including fully connected neural network (FNN), convolutional neural network (CNN), and recurrent neural network (RNN). In this approach, hidden features can be automatically extracted from wireless frames without using explicit feature calculation algorithms. The research achievements of these two approaches will be listed in the following paragraphs.

About the first approach, we proposed two new radiometric features, namely, normalized horizontal

visibility graph Shannon entropy (HVGE) and fractal dimension of DSSS frame preamble.

- HVGE: Most of the existing features are derived from the view of the time, frequency, or phase domain. In this study, we explored the graph domain of wireless frame's preambles and proposed a new radiometric feature called normalized horizontal visibility graph Shannon entropy (HVGE). At first, we introduced a preprocessing consisting of sample truncation and downsampling to enable the adjustment between the computational time of visibility graph (VG) conversion and the identification performance. Secondly, we propose the calculation method of the new HVGE feature from the VG representation. Finally, an experimental study using 50 off-the shelf wireless devices was conducted to investigate the impact of the preprocessing parameters and the effect of noise and feature combinations on the identification performance gain, which has been illustrated in **Fig. 3**. Here, AF1 score is the average of F1 score, which is a machine learning evaluation metric that measures a model's accuracy by combing the precision and recall scores of the model. The performance is verified with four machine learning methods, including support vector machine (SVM), k-nearest neighbor (KNN), random forest (RandF), and boosting (BST). W_0^N refers to natural visibility graph Shannon entropy (NVGE) and W_0 refers to HVGE, and they are two kinds of VG features proposed in our research, while W_6 is performance without the proposed features. **Fig. 3** shows that both the NVGE and HVGE can improve the identification performance of any of the four machine-learning algorithms.

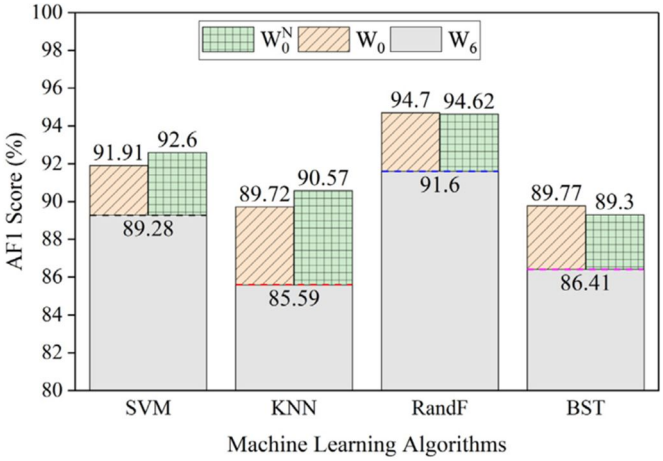
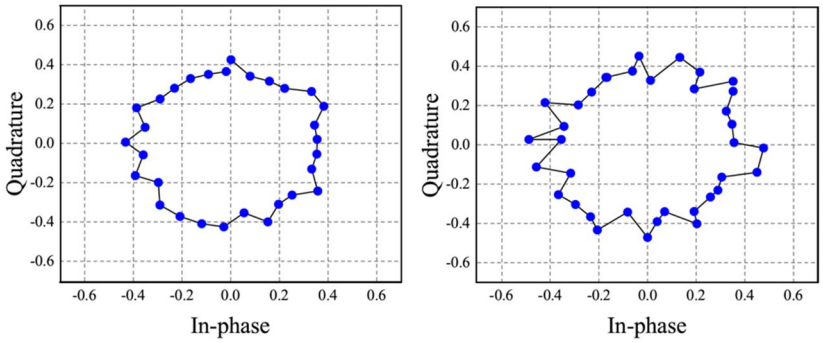


Fig. 3 AF1 scores with several feature combinations

- Fractal dimension of DSSS frame preamble: This new feature is impacted mainly by the clock jitter effect at the digital-to-analog converter (DAC) and also carrier frequency offset (CFO) effect caused by oscillator frequency error. In Fig. 4, we illustrated an example of constellation diagram of received preambles from two IEEE 802.11b Wi-Fi NICs, whose fractal dimension is 1.54 and 1.86, respectively. In our research, we proposed and proved that the fractal dimension of DSSS frame preamble as a new radiometric feature for device identification. In our study, we demonstrated how the fractal dimension varies over the clock jitter and CFO, and then conduct simulation and numerical studies to validate the mathematical analysis and to explore the impact of wireless channels on the estimation of the feature. Finally, we conduct the experiments based on 20 wireless NICs and one USRP to evaluate the performance gain from jointly using fractal dimension with the five existing features. We find that we can achieve a performance gain of 4.3% for the SVM classifier and 5.3% for the kNN classifier in the cable-connection scenario, and can achieve a performance gain of 2.14% for the kNN classifier and 2.43% for the SVM classifier in the over-the-air scenario. Also, we find that a

lower SNR results in a larger performance gain.



(a) NIC 1: $\mathcal{D} = 1.54$ (b) NIC 2: $\mathcal{D} = 1.86$

Fig. 4 Constellation diagram of received preambles from two IEEE 802.11b Wi-Fi NICs with fractal dimension, D, 1.54 and 1.86, resp.

About the second approach, we designed three general fusion frameworks, i.e., input, feature, and decision fusions, and integrate them with three typical deep neural network architectures, i.e., FNN, CNN, and RNN, to form fusion identification schemes. Existing studies on deep learning-based physical layer identification have mainly exploited raw in-phase/quadrature (IQ) samples or power spectral density (PSD) samples as inputs independently. The raw IQ and PSD samples represent the information in the time and frequency domains, respectively. It has been observed from the results of existing studies that identification using raw IQ samples outperforms that using PSD in low signal-to-noise ratio (SNR) regimes, and that identification using PSD outperforms that using raw IQ in high SNR regimes. That's why we proposed to use the fusion of raw IQ and PSD samples to enhance deep learning-based physical layer identification. Finally, we conducted experiments using 50 off-the-shelf Wi-Fi devices to validate the concerned fusion schemes and investigate their performance gains in identification and model training. Our experimental results validated that for the three deep neural networks studied in this paper, the input, feature, and decision fusion identification schemes can achieve comparable or superior identification performances to the state-of-the-art schemes in the entire SNR regime.

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　4件／うち国際共著　4件／うちオープンアクセス　0件）

１．著者名 Zeng Shuiguang、Chen Yin、Li Xufei、Zhu Jinxiao、Shen Yulong、Shiratori Norio	４．巻 127
２．論文標題 Visibility graph entropy based radiometric feature for physical layer identification	５．発行年 2022年
３．雑誌名 Ad Hoc Networks	６．最初と最後の頁 102780～102780
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.adhoc.2022.102780	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Zeng Shuiguang、Chen Yin、Li Xufei、Shen Yulong、Zhao Dongmei、Zhu Jinxiao、Shiratori Norio	４．巻 2022
２．論文標題 On the Performance Supremum of CFO Based Physical Layer Identification	５．発行年 2022年
３．雑誌名 Wireless Communications and Mobile Computing	６．最初と最後の頁 1～14
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2022/3657706	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Li Xufei、Chen Yin、Zhu Jinxiao、Zeng Shuiguang、Shen Yulong、Jiang Xiaohong、Zhang Daqing	４．巻 0
２．論文標題 Fractal Dimension of DSSS Frame Preamble: Radiometric Feature for Wireless Device Identification	５．発行年 2023年
３．雑誌名 IEEE Transactions on Mobile Computing	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/TMC.2023.3235497	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Zeng Shuiguang、Chen Yin、Li Xufei、Zhu Jinxiao、Shen Yulong、Shiratori Norio	４．巻 142
２．論文標題 Time-frequency fusion for enhancement of deep learning-based physical layer identification	５．発行年 2023年
３．雑誌名 Ad Hoc Networks	６．最初と最後の頁 103099～103099
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.adhoc.2023.103099	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 Jinxiao Zhu
２．発表標題 New Radiometric Feature for Wireless Device Recognition
３．学会等名 The 1st Workshop on Intelligent IoT for Empowering the People’s Lifestyle and Well-being
４．発表年 2021年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称 通信装置及びプログラム	発明者 陳寅、中澤仁、朱金暁	権利者 学校法人慶應義塾[60%]、学校法人東洋大学[40%]
産業財産権の種類、番号 特許、特願2021-087819	出願年 2021年	国内・外国の別 国内

〔取得〕　計0件

〔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

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関