EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Physical layer identification of LoRa devices using constellation trace figure

Yu Jiang[1]*, Linning Peng[1], Aiqun Hu[1], Sheng Wang[1], Yi Huang[1,2] and Lu Zhang[3]

Abstract

LoRa wireless technology is a revolutionary wireless network access technology with a wide application prospect. An identification method for Lora devices based on physical layer fingerprinting is proposed to provide identities for authentication. Contrary to previous works, a differential constellation trace figure is established from the radio frequency (RF) fingerprinting features of LoRa devices, which transforms the feature matching to the image recognition. A classification method based on Euclidean distance of clustering center of LoRa signal is performed to analyze the differential constellation trace figure. The experimental results show that six LoRa transmission modules can be recognized accurately, and even in a low signal-to-noise ratio (SNR) environment, the different LoRa devices can still be distinguished and identified effectively.

Keywords: Internet of Things, LoRa, RF fingerprinting, Wireless identification, Constellation trace figure

1 Introduction

The concept of Internet of Things (IoT) has been proposed in the past decade and attracted extensive attention worldwide [1–3]. With the development of mobile communication networks and the deployment of IoT systems, IoT applications have penetrated into every aspect of people's life [4, 5].

Meanwhile, with the rapid growth of IoT devices, security risks have become a major problem that constrains the development of IoT [6–8]. Due to the large number of IoT terminals and complex application environments, the security protection capability is weak, which brings threats to the entire IoT system. Once IoT is under attack, it may cause shutdown of factories, disorder of society and even the safety of human life [9, 10]. Attacks against IoT have already emerged and their scope and impact have increased year by year. With the severe security situation in the IoT, it is extremely urgent to strengthen the security of IoT.

The integration and diversification of IoT terminals has brought many security uncertainties to the IoT business, and the problems are mainly reflected in the following points [11–16]:

- Most of the IoT terminals cannot integrate software and hardware for security protection because of the limitation of cost and performance.
- Many application scenarios are open and unattended, so this self-running mode is vulnerable to external attacks.
- It is necessary to study efficient and lightweight security algorithms, taking security and efficiency both into account.
- Vertical applications of IoT are directly related to users' life safety, so the damage will be greater than that of traditional networks.
- The scale of IoT terminals will be much larger than the traditional network terminals, so a large-scale security attack may happen, which is difficult and costly to prevent.
- Many users are not deeply aware of the IoT security. When a large number of traditional devices without the protection capability join the IoT, they will affect the overall security and reliability.

At present, most IoT interconnections still rely on Internet and mobile networks. The private protocol of IoT is lacked, which restricts the large-scale popularization of IoT to a certain extent. Therefore, the low power wide area network (LPWAN) emerges [17]. Compared with the

*Correspondence: jiangyu@seu.edu.cn
[1] School of Cyber Science and Engineering, Southeast University, Sipai Lou, 210096 Nanjing, China
Full list of author information is available at the end of the article

traditional IoT communication technology, LPWAN technology has the advantages of wide coverage, long distance, massive connection, low power consumption, low cost, etc. It has become a new hotspot in the research and application development of IoT.

Among many technologies of LPWAN, the most competitive technologies are LoRa [18] and NB-IoT [19]. LoRa standard developed early with mature technology among many LPWAN technologies and has a complete industrial chain. As the main technical representative of LPWAN, LoRa standard has drawn worldwide attentions in the field of IoT and its security issues and technologies will become important research contents. LoRaWAN [20] is a standardized specification defined by the LoRa Alliance for low power consumption and network device compatibility of LoRa terminals, and it mainly includes the communication protocol and system architecture, while LoRa only defines the physical layer.

LoRaWAN network architecture consists of an end device (ED), a gateway (GW), a network server (NS), an application server (AS), and a joining server (JS) [21]. A typical star topology is employed in LoRaWAN and the messages are transmitted between the end device and the network server by the gateway. The gateway accesses the network server through a standard IP connection, while the end device communicates with one or more gateways by a single-hop LoRa or frequency-shift keying (FSK). The gateway only completes the forwarding of the data packets without any security protection.

In addition, LoRaWAN considers network security issues in its design. LoRaWAN's security policy is to encrypt data from the end device node to the network server and the application server. The former ensures that the legal node can access the network, authenticate the data packet, and perform integrity verification, and the latter ensures the end-to-end security of the application through the encryption of application data. The joining server is responsible for node authentication and session key distribution.

At present, the network architecture of IoT is not clearly defined, while it is generally accepted that the network architecture of IoT consists of three parts: the sensing layer, the transport layer, and the application layer [22]. There are already mature security management technologies for the transport and application layer, but the authentication technologies are missing in the sensing layer[23]. LoRa terminal security issues are mainly reflected in the following four aspects:

- Vulnerable to attacks. LoRa technology chooses the unlicensed frequency band and the public protocol, which brings vulnerability to the network. The attacker can eavesdrop on the address of the legal terminal and generate forged packets to the gateway to cause congestion. In addition, the attacker can use his own LoRa device to send the maximum length preamble to occupy the channel maliciously.
- Authentication with pre-storage key. The LoRa terminal is configured with a pre-allocation key of AES-128 during manufacturing, so attackers can use the side channel attack to capture the root key. Once the root key is stolen, the communication information will be completely cracked.
- Unauthorized authentication protocol. The authentication mechanism between LoRa terminal and network is simple, and the random number used in the authentication process is too short, resulting in the possibility of replay attacks.
- Weak key management. The keys of the network layer and the application layer are generated by the same root key and random number, so the two keys are not isolated from each other. At the same time, the integrity protection key is produced by AES-128 encryption, and thus the security level and encryption strength are insufficient.

This paper proposes an identification method based on the RF fingerprinting feature of LoRa signal to solve the security issue of terminal authentication. The fingerprint extraction technology of wireless RF equipment has received wide attention in recent years.

By analyzing the RF signals of different devices, the RF fingerprint based on the hardware characteristics can be extracted. The extraction of the RF fingerprint is generally based on the physical layer of the device and can be combined with the traditional wireless network authentication technology to improve the efficiency and accuracy of device classification and recognition.

Different devices have different RF fingerprint characteristics, which makes the identities difficult to be modified or cloned. Therefore, the RF fingerprint of accessing terminal can be identified and verified to improve the security of authentication. As the main contributions of this work, the proposed physical layer-based method can solve the security issues for the LoRa terminal as described in the previous part.

- Vulnerable to attacks. Although it is impossible to prevent such denial of service (DoS) attacks, it is possible to effectively identify the existence of illegal devices for further protection.
- Authentication with pre-storage key. The physical layer identity authentication can replace or cooperate with the original key authentication. The attacker cannot copy and clone the physical layer identity, so the security of the authentication is improved.
- Unauthorized authentication protocol. The physical layer identity can be extracted from the physical signal

of each packet. As long as the physical characteristics can be correctly identified, the data injection of unauthorized device can be effectively prevented.

- Weak key management. The authentication mechanism cannot prevent information eavesdropping, but the security of the key update mechanism can be improved after cooperating with the physical layer identities.

The remainder of the paper is arranged as follows: Section 2 discusses the related works and the LoRa signal is analyzed in Section 3. Section 4 presents the procedure for fingerprinting LoRa with LoRa hardware platforms, and the experiments and results are shown in Section 5. Finally, the conclusions are given in Section 6.

2 Related work

The current research on LoRa security mainly includes three aspects: transport layer, physical layer, and application layer.

The security strategy for transport layer is defined in LoRaWAN. Han et al. [24] proposed a root key update scheme to strengthen the security of session key derivation. The proposed scheme applies a Rabbit stream cipher-based key derivation function to make cryptoanalysis of security keys in LoRaWAN more difficult. Sanchez-Iborra et al. [25] applied a specified Ephemeral Diffie-Hellman Over COSE (EDHOC) as a convenient solution for the update of session keys with flexibility, low computational cost, and limited message exchanges. A complete communication stack has been also presented for enabling the inclusion of the proposed security solution within the LoRaWAN architecture. Laufenberg [26] analyzed the possibility of two particular scenarios of impersonating a LoRaWAN gateway combining existing attacks and presented different approaches to either make the attack harder to implement or even completely prevent it. Some other researches [27–29] provided the security analysis of the LoRaWAN and introduced possible vulnerabilities.

The physical layer security was first studied on other IoT platforms. In 2008, Brik et al. [30] designed an identification system for the 802.11b wireless network card, and the signal characteristics in the modulation domain were using as the RF fingerprint. The frequency offset, synchronization correlation, I/Q offset, amplitude error, and phase error of the modulation signal were selected as the RF fingerprint of the device, and the RF fingerprint was classified by K-nearest algorithm and support vector machine (SVM). In 2016, Noubir et al. [31] extracted the features for fingerprint recognition from the physical layer and data link layer of wireless local area network (WLAN) device. Carrier frequency offset, sampling frequency offset, transmitter switching transient, and scrambling factor were extracted. Through the above features, the recognition schemes for different types of network cards based on the 802.11a/g/p were designed. For the same type of WLAN devices, the correct recognition rate was very high. Peng et al. [32] modeled the O-QPSK modulation signal and explained the differential constellation trajectory in detail from the theoretical level. They used the proposed method to identify and authenticate ZigBee devices effectively. For the research of radio frequency fingerprint of LoRa signal, in 2017, Robyns et al. [33] proposed a new method of fingerprint recognition based on machine learning. Unlike other methods, this method does not extract the local features of the signal, but takes the pre-processed data of the signal as the whole object of recognition and the input data of machine learning.

The application layer focuses on data processing security and data privacy protection. Xu et al. [34] designed an IoT-oriented data placement method with privacy preservation, which can achieve high resource usage, energy saving and efficient data access, and realize privacy preservation of the IoT data. An edge computing-enabled computation offloading method with privacy preservation [35] is proposed to realize multi-objective optimization to reduce the execution time and energy consumption and prevent privacy conflicts of the computing tasks. Xu et al. [36] proposed a computation offloading method for IoT-enabled cloud-edge computing to address the multi-objective optimization problem of task offloading in cloud-edge computing. An energy-aware computation offloading method [37] is designed to reduce the offloading time of the computing tasks and the energy consumption of wireless metropolitan area networks (WMAN).

3 LoRa signal analysis

In order to extract physical identities from the wireless signals, it is necessary to analyze the physical layer of LoRa signal firstly. As a LPWAN technology, LoRa operates in the global free band. By raising the receiving sensitivity, LoRa reduces the link budget and the transmitting power. A high spreading factor, typically 6-12, is used to transmit data signals over a wider frequency band. Forward error correction and redundant information in data encoding are utilized to combat the effects of channel noise on LoRa signals. Although the data throughput rate is small, it has strong transmission reliability.

3.1 LoRa modulation principle

The LoRa modulation scheme was improved by the chirp spread spectrum (CSS) scheme, which was originally designed for radar. A linear frequency modulation (LFM) signal, also known as a chirp signal, has constant amplitude and sweeps across the entire bandwidth linearly over a defined period of time. The implementation of LoRa signal modulation mainly relies on the chirp pulse, which is used to encode the information.

The chirp pulse signal is an essential element of CSS modulation technology and the time domain waveform with duration time T can be expressed as follows:

$$c(t) = \mathrm{rect}\left(\tfrac{t}{T}\right) \cdot e^{j\varphi(t)} \tag{1}$$

where rect $\left(\frac{t}{T}\right)$ is a rectangular signal and

$$rect\left(\frac{t}{T}\right) = \begin{cases} 1, & \left|\frac{t}{T}\right| \leq \frac{1}{2} \\ 0, & otherwise \end{cases} \tag{2}$$

In Eq. 1, $\varphi(t)$ represents the phase of the chirp signal, and the relationship between the chirp signal phase and the instantaneous frequency $f(t)$ can be expressed as

$$f(t) = \frac{1}{2\pi} \cdot \frac{d\varphi(t)}{dt} \tag{3}$$

For CSS, the instantaneous frequency of the chirp signal is a time-dependent linear function, so there is

$$f(t) = f_C + \mu \cdot \frac{B}{T} \cdot t = f_C + \mu Kt \tag{4}$$

where f_C represents the carrier frequency, μ represents the instantaneous frequency changing slope of the chirp signal, B represents the bandwidth, and $K = \frac{B}{T}$ represents the frequency modulation slope. $\mu = 1$ means up-chirp and $\mu = -1$ means down-chirp.

According to Eqs. 3 and 4, Eq. 1 can be represented as

$$c\,(t) = \mathrm{rect}\left(\tfrac{t}{T}\right) \cdot e^{j\left(2\pi f_c t + \pi \mu K t^2\right)} \tag{5}$$

By signal spreading, the energy of the signal is evenly distributed throughout the symbol period, so the system can use a low instantaneous power to transmit high energy for a longer distance.

The LoRa modulation technology mainly has four key parameters: carrier frequency (f_C), bandwidth (BW), spreading factor (SF), and code rate (CR). LoRa uses the above parameters to realize the control of signal modulation and entire wireless communication system.

3.2 LoRa frame structure

The LoRa frame structure [38] is shown in Fig. 1. The LoRa physical layer frame starts with a preamble, which is used to keep the receiver synchronized with the transmitter. There are two types of physical layer headers (PHDR): explicit headers and implicit headers. When communicating with the explicit header, PHDR contains the length of the data information, error correction coding rate, and the indication whether the end of the frame carries the cyclic redundancy check (CRC) of the data load. In addition, PHDR also contains its own CRC, so the receiver can firstly check the PHDR_CRC to verify the integrity of the packet. If the payload length, CR, and CRC are known or fixed, the implicit header mode can be selected, which will improve efficiency and reduce transmission time and power consumption.

It can be seen from the frame structure that the physical layer load is related to the data information while the previous part is independent of the data, which provides conditions for extracting data-independent RF fingerprinting features in the frame.

4 Fingerprinting LoRa

Although LoRa devices are designed according to the same standard, there are differences existed in the specific circuit implementations and chip solutions. Especially when the number of terminals is very large, the differences between the Rf fingerprint will be huge, which provides the premise for terminal identification based on the RF fingerprinting features.

4.1 Acquisition of LoRa signal

The LoRa signal is generated by the SX1278 wireless transmitting module of Semtech company. A total of six LoRa transmitting modules are sampled, as shown in Fig. 2. f_C is set to 433 MHz, SF is set to 7, BW is set to 125 kHz, PHDR is set to implicit header mode, and data sending interval is 50 ms.

The experiment uses the Universal Software Radio Peripheral (USRP) equipment for data sampling with the sampling frequency f_s of 5 MHz, and the LoRa transmitter modules are placed in a fixed position. The sampling process starts after the LoRa transmitter works for a while to be stabilized.

4.2 Signal preprocessing

In order to analyze and extract the RF fingerprints of different LoRa devices, it is necessary to preprocess the

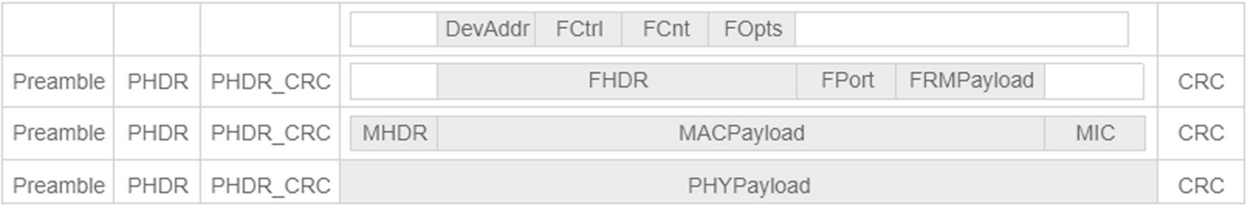

Fig. 1 LoRa frame structure

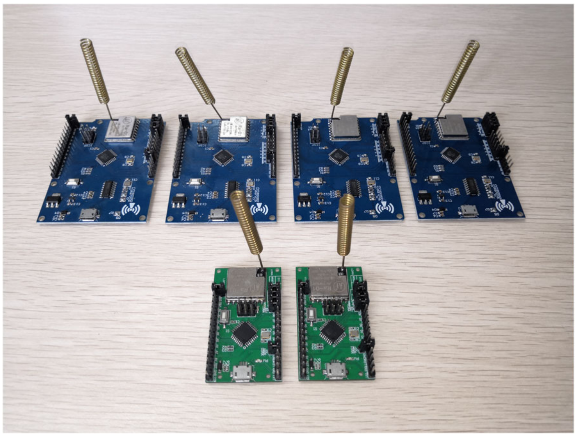

Fig. 2 LoRa signal transmitter

collected data. For each data sample, the valid signal in the sampled data needs to be extracted firstly, and then do normalization and other pre-processing operations to the signal. After the pre-processing operation, RF fingerprint transformation are executed to extract the device-related features.

According to the transmitter setting parameters, the symbol rate of LoRa modulation R_S can be represented as

$$R_S = \frac{BW}{2^{SF}} = \frac{125kHz}{2^7} = 976.5625 \text{ symbol}/s \tag{6}$$

and the sampling points for each LoRa symbol can be calculated as

$$N = \frac{f_S}{R_S} = \frac{5MHz}{976.5625Hz} = 5120 \tag{7}$$

The original LoRa signal is sampled with fixed length of sampling points and its waveform is shown in Fig. 3. The time interval between adjacent data segments is 50 ms, and the amplitude of the data segments are equal, indicating that the transmitter is under steady state.

Then, each valid segment is extracted for analysis. The data shown in Fig. 4a is one segment with energy normalization and Fig. 4b is the data segment enlarged from part of Fig. 4a. As shown in Fig. 4b, the LoRa signal is composed of continuous chirp symbols.

4096-point fast Fourier transformation (FFT) are performed on the signal shown in Fig. 4a, and the result is shown in Fig. 5 with the frequency shifted to the spectrum center. It can be seen that the center frequency of the LoRa signal is 433 MHz and the signal bandwidth is about 125 kHz.

4.3 Differential constellation trace figure

The features including the transient part and the modulation part are extracted from receiving signals for identification. The transient part measures the turn-on/off signal or transmitting signal variations, while the modulation part evaluates the frequency, phase, amplitude, and I/Q samples for the entire signal. Differential constellation trace figure is leveraged for identification extraction of LoRa device in the proposed method for three reasons. The first is that the differential constellation trace figure is belonged to the modulation part, which is proved to be more stable than the transient part. The second is that the features of the modulation part are extracted with different methods respectively, but the differential constellation trace figure can evaluate the frequency error, synchronization correlation, I/Q origin offset, magnitude errors, and phase errors in one figure. The third is that comparing to the traditional constellation figure, the unique physical characteristics of the signal can be reflected in the trace of constellation trace figure by oversampling. The detailed proposed method is described as follows.

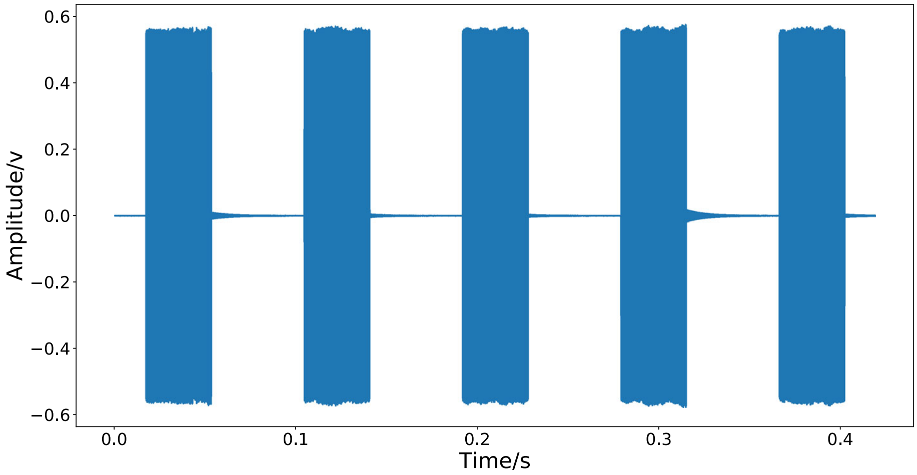

Fig. 3 Original sampled signal

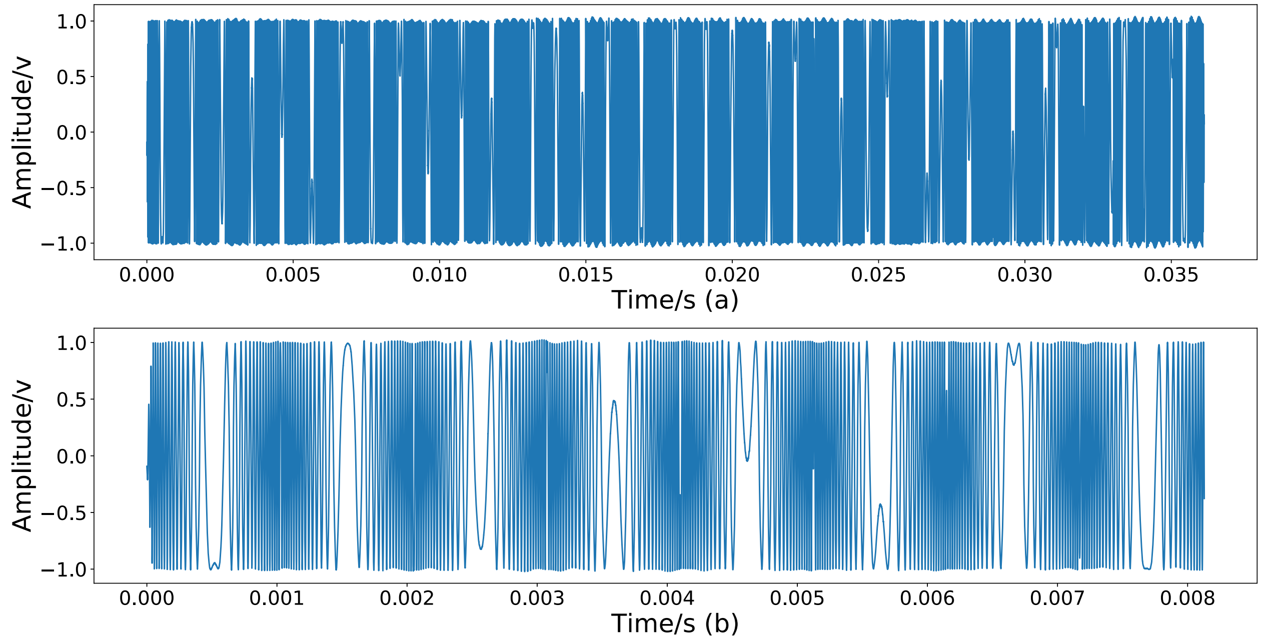

Fig. 4 Valid data extraction

The oversampled data of I/Q signal are drawn on the coordinate plane to obtain the constellation trace figure, which intuitively reflects the characteristics and relationships between signals and provides a convenient way to study the digital communication system. Image recognition methods can be used to extract RF fingerprinting features in the constellation trace figure to distinguish different devices. However, when the constellation trace figure is used to analyze the RF characteristics of the device directly, the receiving symbol deviates from its original position due to the influence of the frequency offset. As the time accumulates, a concentric ring is finally obtained for different devices, as shown in Fig. 6, which leads to a confused result of recognition. By performing differential processing on the received baseband signal, the rotation of the received symbol due to the frequency offset can be eliminated.

Under normal circumstances, the transmitter and the receiver have errors such as frequency offset, resulting in instability of the constellation trace figure. If the transmitter carrier frequency is f_{ct1} and the baseband signal is $X(t)$, the transmit signal $S(t)$ can be expressed as

$$S(t) = X(t)e^{-j2\pi f_{ct1}t} \tag{8}$$

For an ideal channel environment, the received signal $R(t)$ is equal to $S(t)$. After the frequency down conversion, $R(t)$ is converted to $Y(t)$, and the procedure can be expressed as

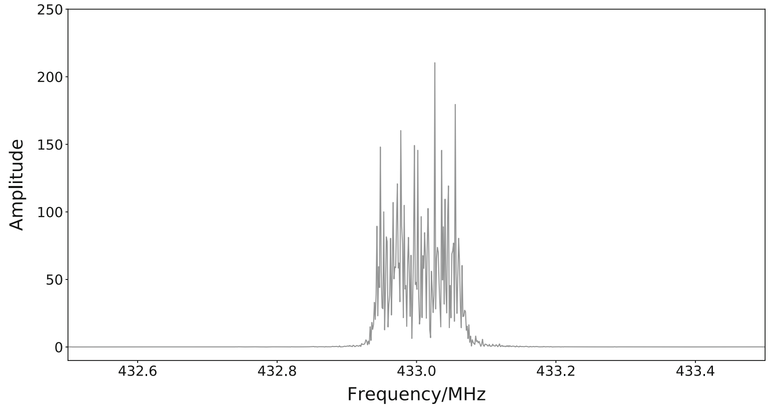

Fig. 5 LoRa signal frequency spectrum

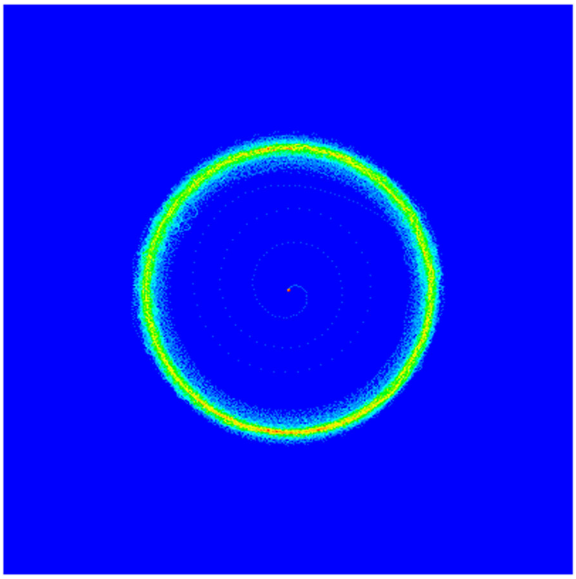

Fig. 6 Constellation figure without differential processing

$$Y(t) = R(t)e^{j(2\pi f_{ct2}t+\varphi)} = S(t)e^{j(2\pi f_{ct2}t+\varphi)} \quad (9)$$

where f_{ct2} is the carrier frequency of receiver and φ is the received signal phase offset. Since the transmitter and receiver have a frequency offset $\Delta f = f_{ct2} - f_{ct1}$, so

$$Y(t) = X(t) \cdot e^{-j2\pi f_{ct1}t} \cdot e^{j(2\pi f_{ct2}t+\varphi)} = X(t) \cdot e^{j(2\pi \Delta ft+\varphi)} \quad (10)$$

The received signal contains a rotation factor $e^{j2\pi \Delta ft}$, so that the constellation trace figure continuously rotates with time t, which erases the characteristics of the RF signal due to the position rotation of the constellation point. In order to solve the problem of instability of the constellation figure and let the frequency offset stably reflected on the figure, differential operation is processed to the data that

$$\begin{aligned} D(t) &= Y(t) * Y^*(t+n) \\ &= X(t) \cdot e^{j(2\pi \Delta ft+\varphi)} \cdot X^*(t+n) \cdot e^{-j(2\pi \Delta f(t+n)+\varphi)} \\ &= X(t) \cdot X^*(t+n) \cdot e^{-j2\pi \Delta fn} \end{aligned} \quad (11)$$

where $X^*(t)$ is the conjugated value of $X(t)$ and n is the differential interval.

After differential operation of signals, the result still has a rotation factor $e^{-j2\pi \Delta fn}$, but it is a stable value determined by n and Δf. The rotation factor directly reflects the frequency offset characteristic of the signal in the constellation trace figure, which makes it feasible to perform subsequent differential constellation trace figure based RF fingerprint extraction.

Differential operation is processed to the sampled data to obtain a differential constellation trace figure. By adding different delays to the I/Q data respectively, the characteristics of the signal differential constellation trace figure can be more obvious and convenient for RF feature extraction. In order to show the image features of differential constellation trace figure more intuitively, different colors are utilized to represent the density of symbols at different positions in the constellation figure. The larger the density of the symbols, the closer to red the color of a point. Then, the final differential constellation trace figure is drawn as shown in Fig. 7.

As shown in the figure, the differential constellation trace figure of the LoRa signal has only one clustering center with red color. The symbol distribution is very concentrated with little noise interference and the signal energy is stable. Therefore, the coordinate of the clustering center can be considered as the steady characteristic of the device.

By adding delay to the I/Q channel of the LoRa signal, the feature of the differential constellation trace figure can be more obvious. The distribution and shape features will appear in the high-density clustering area as shown in Fig. 8, which increases the discrimination between different differential constellation trace figures.

5 Experiments and results

5.1 Identification method based on clustering center

Due to the hardware differences between different LoRa devices, the differential constellation trace figures drawn by different modules' sampled data are different in the position and shape of accumulation points of symbol data, while the figure features of the same LoRa device are approximately the same. Unlike other modulation methods such as QPSK and MSK, the differential constellation

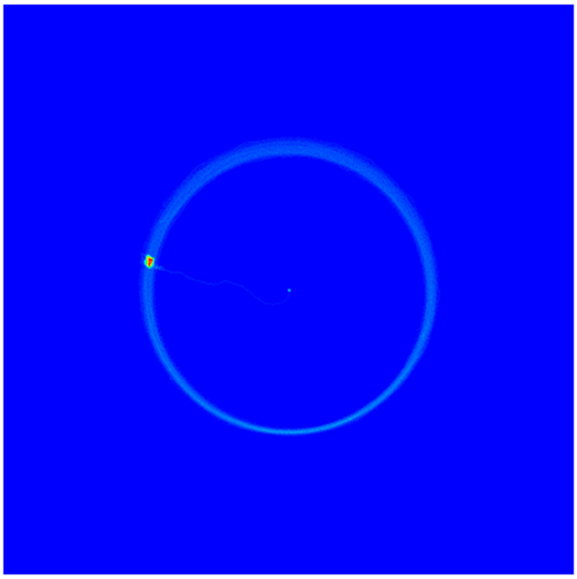

Fig. 7 Differential constellation trace figure of LoRa signal

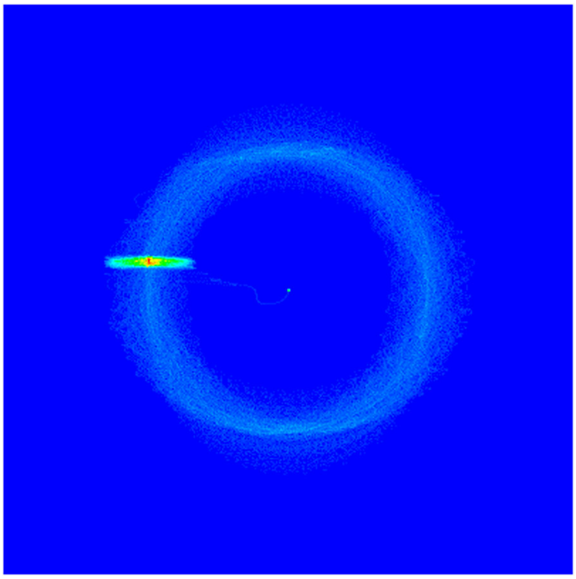

Fig. 8 Differential constellation trace figure with I/Q delay

trace figure of the LoRa modulation signal has only one cluster center in the figure.

Based on the feature of differential constellation trace figure, a recognition method based on the clustering center is proposed. Firstly, by filtering the differential constellation trace figure, only the pixels whose density are higher than the presented threshold are retained. Sixty sets of data are collected from 6 different LoRa modules with 12 sets as training data and the remaining for testing. After processing the training samples, the clustering centers for different device data are drawn in Fig. 9.

As shown in Fig. 9, the six modules can be recognized intuitively, so the coordinates can be used as the identities of each LoRa device. In identification process, the coordinates of the cluster center are first obtained, and the distance between the obtained and known cluster centers is calculated respectively. When the distance is less than the preset value, the device can be identified as the known terminal. Otherwise, it is recognized as an unknown device.

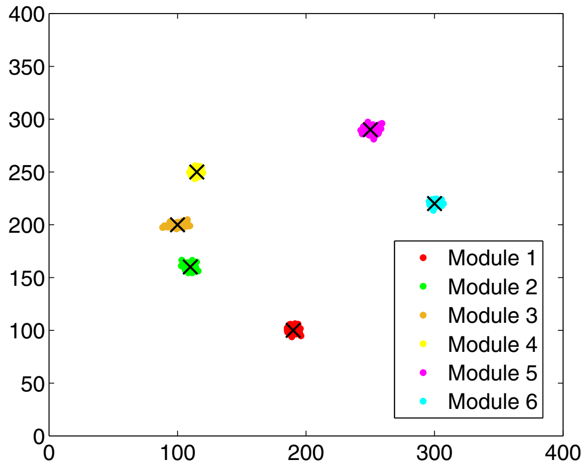

Fig. 9 Clustering centers of different LoRa modules

5.2 Recognition results with noise

The above classification and identification methods for LoRa devices are performed in a high SNR environment. Good classification results are achieved under low noise conditions and all devices can be classified correctly. In this section, the influence of artificial noise on the differential constellation trace figure based identification method is discussed.

Under the condition of negative SNR, valid RF fingerprinting features of devices can still be extracted due to the modulation way adopted by LoRa technology. The LoRa communication can be correctly performed in a low SNR environment, because the signal is transmitted within a large frequency band by using high spreading factor. When the received signal is completely submerged in the noise, the autocorrelation of the chirp pulse signal can be utilized to extract the data from the noise. The noise signal has no correlation, so it can be separated from useful signal.

The accuracy of the classification and identification methods of LoRa devices based on clustering center is evaluated with artificial noise and the result is shown in Fig. 10.

As shown in Fig. 10, when the SNR is higher than − 10 dB, the identification accuracy of the system for the six LoRa modules can reach 100% even under the condition of negative SNR. As the SNR decreases, the system identification accuracy begins to decline rapidly. In general, the proposed method has certain resistance to the channel noise interference.

5.3 Comparative experiments

The proposed method belongs to the security mechanism of physical layer, while as mentioned in Section 1 , most of the recent security mechanisms for LoRa are based on transport layer and application layer.

Firstly, we compare the security methods of these three layers from four aspects. In contrast to the traditional upper-layer security policies, physical layer-based identity is difficult to be counterfeited or tampered. The enhanced security method based on physical layer do not need to modify the original system architecture and the terminals, so it is convenient to add physical layer security policies to the system. The authentication process of the physical layer is simple and no information interaction is required, which reduces the risk of protocol attacks.

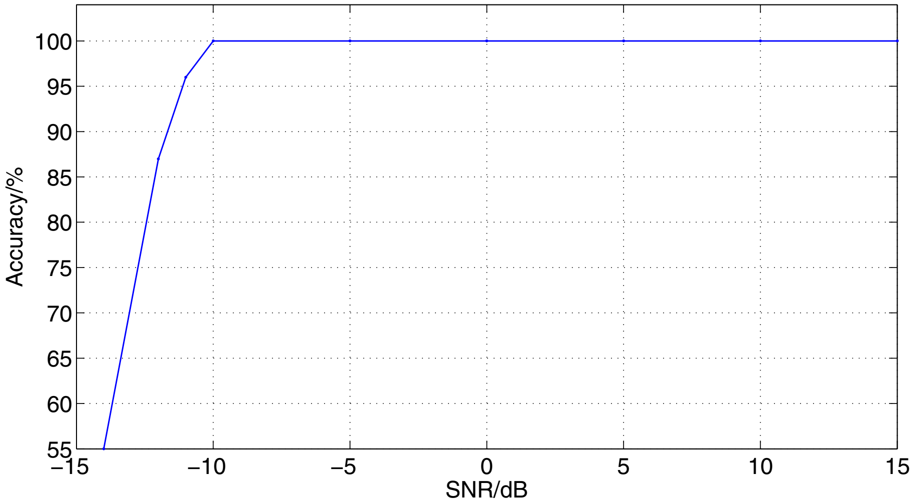

Fig. 10 Accuracy under different SNR

The physical layer-based authentication method has high requirements on the signal quality, and therefore, the anti-interference ability is poor. The comparison results are shown in Table 1.

Secondly, the proposed method is compared with the existing physical layer-based methods. Unfortunately, most of the current methods are designed for specific wireless terminals and cannot be directly used for the LoRa module. The supervised machine learning (SML) method in [33] applied to LoRa terminals is compared with the proposed method. In general, these two methods belong to different types and the main differences are summarized as follows.

The proposed method is designed for the features of LoRa signal and the SML method can be considered as a universal method for wireless signal. In contrast to the SML method, the proposed method used the dedicated algorithm which brings high efficiency. As long as the stable features are determined, the proposed algorithm does not need training for new terminals. Then, we evaluate the performance of the two types of methods with different fingerprinting experiments and the SML methods involved in the assessment includes multilayer perceptron (MLP), convolutional neural network (CNN), and SVM.

The first experiment is the accuracy test with the configuration same as Section 4.2. The LoRa terminal and USRP are 5 m apart without obstacles and 1500 symbols are collected for the six terminals with sample rate of 5 Msps. The comparisons in Table 2 are consistent with the results in [33], and the proposed method obtains a high accuracy under the current experimental conditions.

The next experiment is the effect of sample rate. The SML method can classify devices at low sample rates and the proposed method needs high sample rate to present the constellation trace figure. The other conditions are the same as experiment one, and the average accuracy of six terminals are shown in Table 3. The comparison results indicate that the change of sample rate has higher influence on the proposed method than the SML method, especially when the sample rate is as low as 1 Msps.

The third experiment is the effect of location. The terminals are placed in three different locations successively to acquire the average accuracy. The training data are collected at location 1 (L1) with the same conditions of experiment 1 and the results for three locations are shown in Table 4. When training on signals from their respective location, the results are shown in Table 5.

Table 1 Security comparison of three layers

	Physical	Transport	Application
Anti-counterfeiting	Strong	Weak	Weak
Portability	Strong	Weak	Weak
Protocol complexity	Simple	Medium	Complex
Anti-interference	Weak	Medium	Medium

Table 2 Accuracy comparison for six terminals

	Dev 1 (%)	Dev 2 (%)	Dev 3 (%)	Dev 4 (%)	Dev 5 (%)	Dev 6 (%)
SVM	71.47	71.20	68.87	72.53	70.67	73.13
CNN	86.6	82.56	83.07	83.67	82.56	82.87
MLP	90.00	88.93	90.27	91.73	90.47	89.23
Proposed	99.00	99.03	99.03	99.33	99.93	98.98

Table 3 Accuracy comparison for different sample rates

	1 Msps (%)	2 Msps (%)	5 Msps (%)	10 Msps (%)
SVM	49.40	58.87	70.07	79.87
CNN	55.27	65.07	82.87	94.80
MLP	56.53	66.33	90.53	96.53
Proposed	52.13	70.03	98.83	99.67

As shows in Tables 4 and 5, the SML method achieves low accuracy when the model was previously trained on signals from a different location. Therefore, we can conclude that the different channel conditions significantly impact the accuracy of SML method. Fortunately, the proposed method can resist the channel influence to a certain extent, which means the extracted characteristics are more stable than the those of SML method. As the distance increases and the SNR decreases, the accuracy of the proposed method decreases, which is consistent with the results in Section 5.2.

6 Conclusion

In this paper, the principle and implementation of LoRa modulation technology are analyzed. According to LoRa modulation, a differential constellation trace figure is proposed to extract the RF fingerprinting features of LoRa devices. The unique physical characteristics of the device are reflected in the trace of the constellation trace figure. By analyzing the characteristics of the differential constellation trace figure with the image recognition algorithm, a classification method based on Euclidean distance of clustering center of LoRa signal is presented. In contrast to the security mechanisms of transport and application layer, the physical layer authentication method can effectively improve the accessing security of the IoT device. The experimental results show that six LoRa transmission modules can be recognized accurately from the differential constellation trace figures. The proposed method can achieve higher recognition accuracy and more stable features than the machine learning method, which makes it more practical. When the SNR or sample rate is reduced, the performance of the proposed method will decrease, which will be considered in future work.

Table 4 Accuracy comparison for different locations with training set at L1

	L1 (5m to USRP) (%)	L2 (10m to USRP) (%)	L3 (50m to USRP) (%)
SVM	71.20	20.13	19.73
CNN	83.67	21.73	20.80
MLP	90.27	23.20	24.47
Proposed	99.03	98.27	63.07

Table 5 Accuracy comparison for different locations with training set at respective location

	L1 (5m to USRP) (%)	L2 (10m to USRP) (%)	L3 (50m to USRP) (%)
SVM	71.20	72.53	70.67
CNN	83.67	82.17	82.80
MLP	90.27	89.67	90.27
Proposed	99.03	98.50	70.07

Abbreviations

AS: Application server; BW: Bandwidth; CNN: Convolutional neural network; CR: Code rate; CRC: Cyclic redundancy check; CSS: Chirp spread spectrum; DoS: Denial of service; ED: End device; EDHOC: Ephemeral Diffie-Hellman over COSE; FFT: Fast Fourier transformation; FSK: Frequency-shift keying; GW: Gateway; IoT: Internet of Things; JS: Joining server; LFM: Linear frequency modulation; LPWAN: Low power wide area network; MLP: Multilayer perceptron; NS: Network server; PHDR: Physical layer header; RF: Radio frequency; SF: Spreading factor; SML: Supervised machine learning; SNR: Signal-to-noise ratio; SVM: Support vector machine; USRP: Universal Software Radio Peripheral; WLAN: Wireless local area network; WMAN: Wireless metropolitan area networks

Acknowledgements

The authors would like to thank all kinds of funds for funding.

Authors' contributions

YJ is the main author of this article and the idea was proposed by him. SW and LP were in charge of the major theoretical analysis, algorithm design, and numerical simulations. YH drew parts of the figures. AH and LZ contributed to the writing and revisions. All authors read and approved the final manuscript.

Funding

This work was supported in part by the National Natural Science Foundation of China under Grant 61571110, 61601114, 61602113, 61801115, Natural Science Foundation of Jiangsu Province under Grant BK20160692, Key Laboratory of Computer Network Technology of Jiangsu Province, and Purple Mountain Laboratories (PML).

Competing interests

The authors declare that they have no competing interests.

Author details

[1] School of Cyber Science and Engineering, Southeast University, Sipai Lou, 210096 Nanjing, China. [2] Zhangjiagang Campus of Jiangsu University of Science and Technology, Changxing Road, 215600 Suzhou, China. [3] INSA Rennes, 20 Avenue des Buttes de Coesmes, 35700 Rennes, France.

Received: 16 May 2019 Accepted: 20 August 2019
Published online: 04 September 2019

References

1. A. Tiwary, M. Mahato, A. Chidar, M. K. Chandrol, M. Shrivastava, M. Tripathi, Internet of things (iot): research, architectures and applications. Int. J. Futur. Revolution. Comput. Sci. Commun. Eng. **4**, 2454–4248 (2018)
2. C. Yan, X. Cui, L. Qi, X. Xu, X. Zhang, Privacy-aware data publishing and integration for collaborative service recommendation. IEEE Access. **6**, 43021–43028 (2018)
3. W. Gong, L. Qi, Y. Xu, Privacy-aware multidimensional mobile service quality prediction and recommendation in distributed fog environment. Wirel. Commun. Mob. Comput. **2018**, 1–8 (2018)
4. L. Qi, R. Wang, C. Hu, S. Li, Q. He, X. Xu, Time-aware distributed service recommendation with privacy-preservation. Inf. Sci. **480**, 354–364 (2019)
5. L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang, J. Chen, A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment. Futur. Gener. Comput. Syst. Int. J. Escience. **88**, 636–643 (2018)
6. M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of Things security and forensics: challenges and opportunities. Futur. Gener. Comput. Syst. **78**, 544–546 (2018)

7. L. Qi, X. Zhang, W. Dou, Q. Ni, A Distributed locality-sensitive hashing-based approach for cloud service recommendation from multi-source data. IEEE J Sel. Areas Commun. **35**(11), 2616–2624 (2017)
8. L. Qi, Y. Chen, Y. Yuan, S. Fu, X. Zhang, X. Xu, A QoS-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems. World Wide Web J. (2019). https://doi.org/10.1007/s11280-019-00684-y
9. L. Qi, S. Meng, X. Zhang, R. Wang, X. Xu, Z. Zhou, W. Dou, An exception handling approach for privacy-preserving service recommendation failure in a cloud environment. Sensors. **18**(7) (2018)
10. L. Qi, W. Dou, W. Wang, G. Li, H. Yu, S. Wan, Dynamic mobile crowdsourcing selection for electricity load forecasting. IEEE Access. **6**, 46926–46937 (2018)
11. A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. Blockchain for iot security and privacy: The case study of a smart home (IEEE, 2017), pp. 618–623. https://doi.org/10.1109/percomw.2017.7917634
12. M. A. Khan, K. Salah, Iot security: Review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. **82**, 395–411 (2018)
13. R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan, in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. Internet of things (iot) security: Current status, challenges and prospective measures (IEEE, 2015), pp. 336–341. https://doi.org/10.1109/icitst.2015.7412116
14. C. Shi, A novel ensemble learning algorithm based on DS evidence theory for IoT security. Comput. Mater. Continua. **57**(3), 635–652 (2018)
15. B. Wang, W. Kong, W. Li, N. N. Xiong, A dual-chaining watermark scheme for data integrity protection in internet of things. CMC-Comput. Mater. Continua. **58**(3), 679–695 (2019)
16. L. Kou, Y. Shi, L. Zhang, D. Liu, Q. Yang, A lightweight three-factor user authentication protocol for the information perception of IoT. CMC-Comput. Mater. Continua. **58**(2), 545–565 (2019)
17. L. Krupka, L. Vojtech, M. Neruda, in *2016 17th International Conference on Mechatronics-Mechatronika (ME)*. The issue of lpwan technology coexistence in iot environment (IEEE, Prague, 2016), pp. 1–8
18. M. C. Bor, J. Vidler, U. Roedig, in *LoRa for the internet of things*. International Conference on Embedded Wireless Systems and Networks (EWSN), vol. 16 (Graz, 2016), pp. 361–366
19. R. S. Sinha, Y. Wei, S.-H. Hwang, A survey on LPWA technology: LoRa and NB-IoT. Ict Express. **3**(1), 14–21 (2017)
20. N. Sornin, M. Luis, T. Eirich, et al., in *LoRaWAN specification*. LoRa alliance (2015)
21. J. de Carvalho Silva, J. J. Rodrigues, A. M. Alberti, P. Solic, A. L. Aquino, in *2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech)*. LoRaWAN-a low power wan protocol for internet of things: A review and opportunities (IEEE, Split, 2017), pp. 1–6
22. I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, M. Guizani, Internet of things architecture: recent advances, taxonomy, requirements, and open challenges. IEEE Wirel. Commun. **24**(3), 10–16 (2017)
23. F. Olivier, G. Carlos, N. Florent, New security architecture for IoT network. Procedia Comput. Sci. **52**, 1028–1033 (2015)
24. J. Han, J. Wang, An enhanced key management scheme for LoRaWAN. Cryptography. **2**(4), 34 (2018)
25. R. Sanchez-Iborra, J. Sánchez-Gómez, S. Pérez, P. Fernández, J. Santa, J. Hernández-Ramos, A. Skarmeta, Enhancing LoRaWAN security through a lightweight and authenticated key management approach. Sensors. **18**(6), 1833 (2018)
26. L. S. Laufenberg, Impersonating LoRaWAN gateways using Semtech Packet Forwarder (2019). arXiv preprint arXiv:1904.10728
27. E. Aras, G. S. Ramachandran, P. Lawrence, D. Hughes, in *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*. Exploring the security vulnerabilities of LoRa (IEEE, 2017), pp. 1–6. https://doi.org/10.1109/cybconf.2017.7985777
28. T. Stefano, Z. Simone, V. Lorenzo, in *IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. Security analysis of LoRaWANTM Join Procedure for Internet of Things Networks, (2017). https://doi.org/10.1109/wcncw.2017.7919091
29. M. Eldefrawy, I. Butun, N. Pereira, M. Gidlund, Formal security analysis of LoRaWAN. Comput. Netw. **148**, 328–339 (2019)
30. V. Brik, S. Banerjee, M. Gruteser, S. Oh, in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*. Wireless device identification with radiometric signatures (ACM, 2008), pp. 116–127. https://doi.org/10.1145/1409944.1409959
31. T. D. Vo-Huu, T. D. Vo-Huu, G. Noubir, in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. Fingerprinting Wi-Fi devices using software defined radios (ACM, 2016), pp. 3–14. https://doi.org/10.1145/2939918.2939936
32. L. Peng, A. Hu, Y. Jiang, Y. Yan, C. Zhu, in *2016 8th International Conference on Wireless Communications & Signal Processing (WCSP)*. A differential constellation trace figure based device identification method for ZigBee nodes (IEEE, 2016), pp. 1–6. https://doi.org/10.1109/wcsp.2016.7752534
33. P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelée, B. Preneel, in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning (ACM, 2017), pp. 58–63. https://doi.org/10.1145/3098243.3098267
34. X. Xu, S. Fu, L. Qi, X. Zhang, Q. Liu, Q. He, S. Li, An IoT-oriented data placement method with privacy preservation in cloud environment. J. Netw. Comput. Appl. **124**, 148–157 (2018)
35. X. Xu, Y. Xue, L. Qi, Y. Yuan, X. Zhang, T. Umer, S. Wan, An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles. Futur. Gener. Comput. Syst. **96**, 89–100 (2019)
36. X. Xu, Q. Liu, Y. Luo, K. Peng, X. Zhang, S. Meng, L. Qi, A computation offloading method over big data for IoT-enabled cloud-edge computing. Futur. Gener. Comput. Syst. **95**, 522–533 (2019)
37. X. Xu, Y. Li, T. Huang, Y. Xue, K. Peng, L. Qi, W. Dou, An energy-aware computation offloading method for smart edge computing in wireless metropolitan area networks. J. Netw. Comput. Appl. **133**, 75–85 (2019)
38. A. Augustin, J. Yi, T. Clausen, W. Townsley, A study of LoRa: long range & low power networks for the internet of things. Sensors. **16**(9), 1466 (2016)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.