Machine Learning-Based Security Authentication for IoT Networks

Xiaoying Qiu(✉), Xuan Sun, and Xiameng Si

School of Information Management, Beijing Information Science and Technology University, Beijing 100192, China
{20192329,Sunxuan,Sixiameng}@bistu.edu.cn

Abstract. In this paper, we propose a security authentication scheme based on machine learning algorithms to detect spoofing attacks in the Internet of Things (IoT) network. This authentication method exploits the physical layer properties of the wireless channel to identify sensors and applies neural networks to learn channel fingerprints without being aware of the communication network model. We propose a channel differences-based security framework to provide lightweight authentication and a Long Short-Term Memory (LSTM) network-based detection approach to further enhance the authentication performance for sinks that support intelligent algorithms. Experiments and simulations were carried out in an indoor conference room. The results show that our strategy improves the authentication accuracy rate compared with the existing non-learning security authentication methods.

Keywords: Wireless communication · Security authentication · Physical layer security · Machine learning

1 Introduction

A growing number of smart devices are being connected to large-scale heterogeneous networks at an unprecedented speed, realizing the concept of the Internet of Things (IoT) [1]. There are many application fields in which the IoT plays a remarkable role, including smart home, smart grids, and smart industrial automation. Advanced communication technologies enable a wide variety of devices to see, hear, talk, and share information. However, the heterogeneity of the IoT has brought huge challenges to existing security authentication schemes [2,3]. In this complex scenario, traditional security standards and protocols may not be sufficient to completely protect wireless devices. In addition, the overhead and complexity of available security algorithms greatly consume the limited resources in IoT networks.

While digital key-based cryptographic methods already enjoy a large literature, they are still based on a promise that eavesdroppers lack the computational

Supported by school research foundation of BISTU (No.2035009).

Y.-B. Lin and D.-J. Deng (Eds.): SGIoT 2020, LNICST 354, pp. 106–115, 2021.
https://doi.org/10.1007/978-3-030-69514-9_10

power to successfully attack the network. Through impersonation, the attacker can modify the message so that it is mistaken for the message sent by a legitimate device. Due to the rapidly growing computational capability of wireless devices, it is becoming more and more feasible to crack the security key from the intercepted information by eavesdropping. For practical implementation, current classical security methodologies also require appropriate key management and distribution, which may cause excessive network communication delays. These problems exist in any communication networks and are not necessarily limited to wireless IoT networks.

Physical layer authentication (PLA), which safeguards communications by using the intrinsic characteristics of wireless channels, is a promising lightweight security method [4]. These kind of analog-domain attributes are essentially related to the unique defects of communication equipment and the corresponding wireless communication environment, which are difficult to impersonate or imitate by opponents [5–7]. Despite existing physical layer authentication have obvious advantages such as low power consumption, low network overhead and lightweight, most approaches are based on a single, static channel characteristic [8–11]. Therefore, they are unsuitable for providing accurate authentication in real time-varying environments. Incomplete channel estimation and interference errors constitute the main challenge factors in the authentication process.

In this paper, we propose a security authentication scheme that uses the physical layer properties of the wireless channel to improve the accuracy of spoofing detection. Specifically, the solution reuses the channel estimation result of the wireless device and extracts the received signal strength to construct channel vectors, which is compared with the channel record of the required communication device in a hypothesis test. The channel features extracted in the authentication scheme greatly affect the recognition effect of the classifier. The performance accuracy usually depends on the variation of the wireless channel, the spatial decorrelation characteristics, and the channel estimation method, which are difficult to predict in advance by the wireless devices in the IoT network. Therefore, this solution uses a deep learning method to extract channel characteristics based on the current received signal strength. We propose a Long Short Term Memory (LSTM)-based physical layer authentication scheme to enhance the detection performance of sinks that support deep learning, especially when the sink need to authenticate a large number of access nodes in the IoT network. Specifically, the proposed LSTM network is used to learn the deep features of each legitimate device automatically and authenticate the attacker simultaneously.

The proposed authentication scheme can be implemented on the Universal software radio peripheral in an indoor conference room to detect spoofing attacks. Experiments performed with universal software radio peripheral transceivers show that the proposed scheme have better anti-interference, higher authentication accuracy, and intelligent learning algorithm further improves the detection performance.

The rest of the paper is organized as follows. We present the system model in Sect. 2. The LSTM-based security authentication scheme is proposed in Sect. 3.

Following up from that, the simulation results of the proposed authentication solution are discussed in Sect. 4. Finally, Sect. 5 concludes the paper.

2 System Model and Problem Statement

2.1 System Model

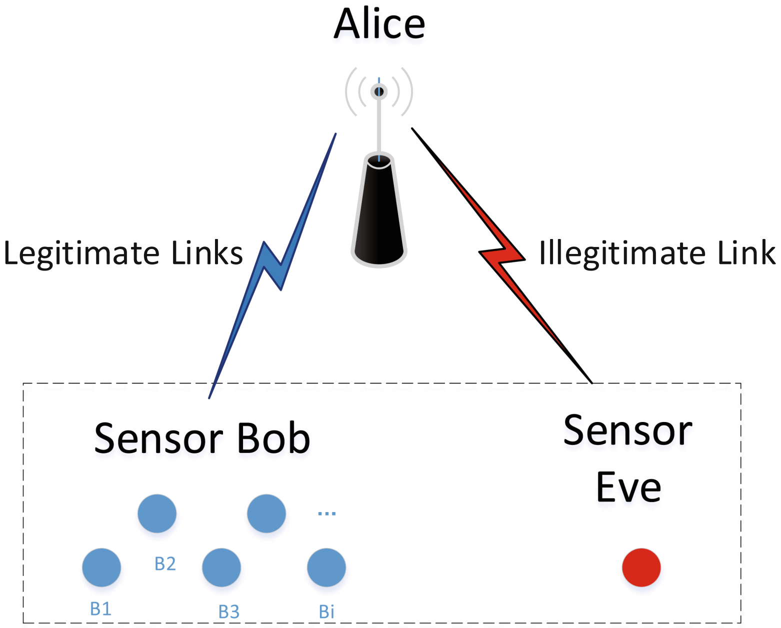

Fig. 1. The system model diagram describes the physical layer authentication scheme to consider.

As shown in Fig. 1, we consider three types of devices. The first type is smart device, which is capable of performing advanced tasks, such as data storage, transmission, and communication; in our security model, this type of device refers to smart device "Alice" for collecting data from other sensors. The second type is called "Bob", and its resources are limited. For the persistence of life, Bob spends most of his time on sensing and data recording. Once activated, Bob will run in data transfer mode, transfer its stored data to Alice, and clear memory for upcoming data. In our scenario, Eve is a potential spoofer who pretends to be a legitimate device Bobi, and then sends the false message to smart Alice. More explicitly, Eve not only tries to access the wireless network, but also to forge authorized identities for obtaining illegitimate benefits. Notably, since the presence of scatters and reflectors in the wireless communication environment, there will be multiple copies of the transmitted signal through different paths.

Therefore, the physical layer properties of the wireless channel between legitimate transceivers is independent of that between the spoofer and the receiver. The system model diagram describes the physical layer authentication scheme that needs to be considered, as shown in Fig. 1.

2.2 Problem Statement

We can reasonably assume that the initial transmission between Alice and Bobi was established before Eve arrived, which allowed smart Alice to obtain an estimate of the wireless channel. M estimates of the selected physical layer attributes of legitimate channel can be obtained during the initial authentication phase of the establishment, which are given by

$$\mathbf{H}_{Bobi} = [H_{Bobi,1}, H_{Bobi,2}, \cdots, H_{Bobi,M}]^T \tag{1}$$

where each $H_{Bobi,m}$ denotes the channel vector estimated from legitimate transmitter, $m \in \{1, 2, ..., M\}$ represents an time index, and M denotes the number of estimates during the initial authentication phase.

Smart Alice must verify the received message at time $t + 1$ and authenticate whether it is coming from Bob_i.

$$\mathrm{H}_0 : |\mathrm{F}(\mathbf{H_{Bob_i}(t)} - \mathbf{H(t+1)})| \leq \gamma \tag{2}$$

$$\mathrm{H}_1 : |\mathrm{F}(\mathbf{H_{Bob_i}(t)} - \mathbf{H(t+1)})| > \gamma \tag{3}$$

where H_0 represents that the received message come from the sender Bob_i, H_1 indicates the hypothesis that the sensor is spoofer Eve, F is the proposed learning authentication function, $\mathbf{H}(t)$ denotes the estimated physical properties of the channel at instantaneous time t, and γ is the threshold.

The main objective of the receiver Alice is to determine whether the source of the received message is Bobi by using the difference between the legitimate estimates $H_{Bobi,1}, H_{Bobi,2}, \cdots, H_{Bobi,M}$ and the newly estimated physical layer signatures. The problem with conventional physical layer authentication methods is that wireless channels are likely to be time-varying, but the channel estimates are static and incomplete, which greatly reduces the accuracy of the authentication scheme. It is for this reason that we use LSTM networks to learn time-varying channel features and perform spoofer detection concurrently. If the difference between the channel vectors is large, it is considered that the signal to be authenticated comes from a spoofing attacker, otherwise, from Bobi. We assume that the estimated noises of Bobi and Eve are independent and identically distributed, which is caused by interference factors, such as measurement errors and channel noises.

3 LSTM-based Physical Layer Authentication

In this section, we discuss the overall architecture of the physical layer authentication scheme based on the LSTM network. First, we quantify the difference between the legitimate channel vectors $H_{Bobi,1}, H_{Bobi,2}, \cdots, H_{Bobi,M}$ and the new estimates $\mathbf{H}_{t+1}$, which will be followed by the LSTM network. Finally, we discuss the implementation details. The step involved in physical layer authentication process based on LSTM network is shown in Fig. 2.

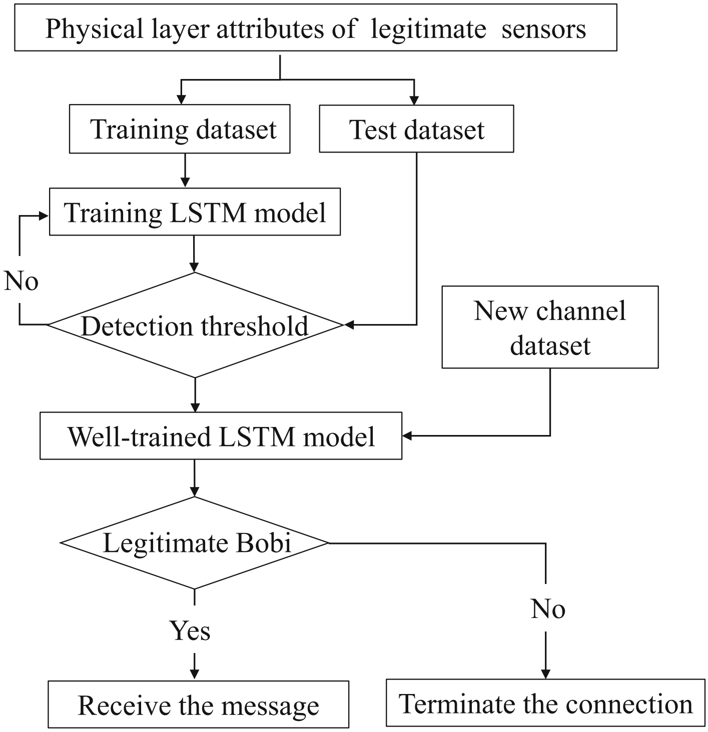

Fig. 2. Block diagram of proposed physical layer authentication.

As discussed in the overview, it is difficult to manually capture channel characteristics with high robustness, so the back-end utilizes the LSTM network to learn deep features. Inspired by image classification, the LSTM network is used to automatically extract channel characteristics and detect the attacker. One of the main advantages of the LSTM network is to ensure that our authentication model adapts to time-varying environments to provide reliable protection. Generally, the physical layer attributes have patterns according to the time-varying channel. These dynamic characteristics that do not appear in a single channel vector can be dispersed into multiple data vectors. Existing machine learning approaches for physical layer security authentication failed to track such attributes, and do not have the ability to extract time-varying characteristics that appear in multiple channel vectors.

Note that the transformation from the estimates into high-dimensional feature space is nonlinear. Therefore, to learn local characteristics and global features, the LSTM layer is used by introducing three gates (input, forget and output). The cell states CS_t in LSTM module can be formulated as

$$CS_t = Forg_t \odot CS_{t-1} + Inp_t \odot tanh(U * Hid_{t-1} + Wx_t + b) \quad (4)$$

and the hidden states Hid_t is given by

$$Hid_t = Out_t \odot tanh(CS_t) \quad (5)$$

where $\odot$ is the element-wise multiplication operation. As shown in Fig. 3, the input gate Inp_t, forget gate $Forg_t$ and output gate Out_t are expressed as

$$Inp_t = \sigma(W_{Inp} * x_t + U_{Inp} * Hid_{t-1} + b_{Inp}) \quad (6)$$

$$Forg_t = \sigma(W_{Forg} * x_t + U_{Forg} * Hid_{t-1} + b_{Forg}) \quad (7)$$

$$Out_t = \sigma(W_{Out} * x_t + U_{Out} * Hid_{t-1} + b_{Out}) \quad (8)$$

where σ denotes the sigmoid function, U, W, and b represent parameters. The idea of the LSTM layer is to learn efficiently from variable channel vectors.

During training, each channel vector will be input to the LSTM network, and time-varying features will be obtained through the LSTM layer. The classifier following the LSTM layer will process the output of the LSTM and make decisions on the softmax loss function. The parameters of the authentication system we proposed are updated by the background propagation algorithm. After iteratively updating the learning model using the physical layer attributes, the loss value of eventually tends to zero gradually.

During the test, the test dataset is feed into the LSTM network, and the probability of the channel vectors belonging to different transmitters is calculated after network processing. The prediction used in the model can be expressed as

$$\Pr = \frac{e^{V_{class}}}{\sum_{class'=1}^{2} e^{V_{class'}}} \quad (9)$$

In conclusion, our security authentication scheme based on the LSTM network is summarized at a glance in Fig. 2. In summary, the channel vector is transformed from single dimensional to multi-dimensional features, the authentication is modelled as an intelligent system. Therefore, it dramatically maps the physical layer authentication to a intelligent process that can learn time-varying features and perform authentication tasks.

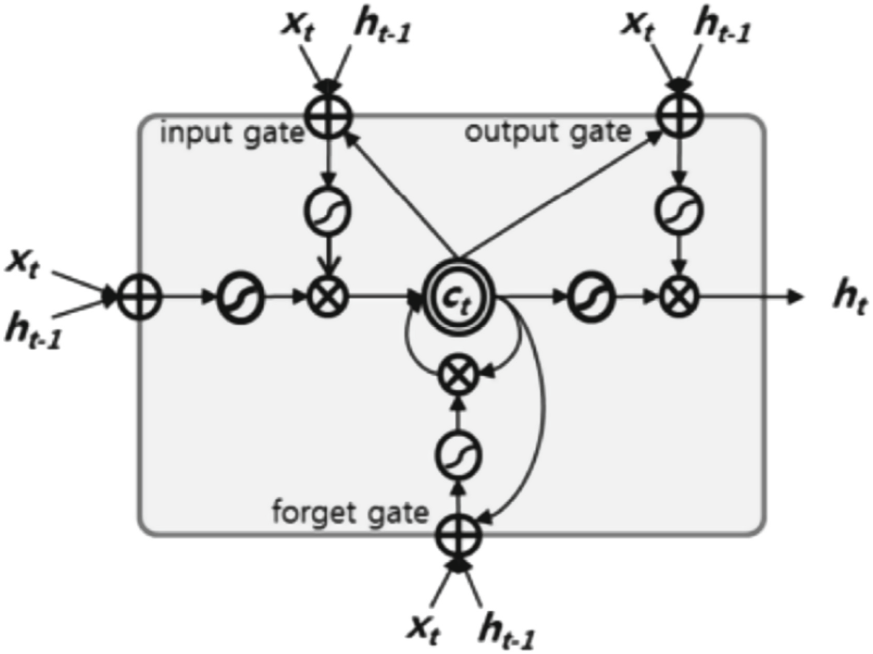

Fig. 3. Structure of LSTM layer [12].

4 Experimental Results

In this section, we first give the experimental setup of the LSTM network. Then, we verify the effectiveness of our authentication process through research and characterize the convergence. In addition, a brief comparison between our and other schemes is given. To emulate the learning-based physical layer authentication method, we set the Universal Software Radio Peripheral (USRP) transceiver to operate in IEEE 802.11a/g mode, working at 2.4 GHz and having a bandwidth of 20 MHz. We investigate the performance of the proposed intelligent model in the binary classification (Bob1 and Bob2). All estimates of received signal strength constitute a park with two classification targets. The sampled data set used for authentication provides a more realistic basis for theoretical verification. To automate the training model generation and detection authentication process, we created the script using the Python language.

We collect data for each transmitter-receiver combination. As shown in Fig. 4, two types of samples are involved in the proposed USRP data set, each of which contains 2000 × 256 channel feature sampling points, a total of 4000 × 256 samples. During the training process, 1000 × 256 sampling points are randomly selected for each type of channel feature data.

We train the LSTM network as a whole. Given the estimated channel vectors, as the input to our intelligent authentication model. First of all, one physical

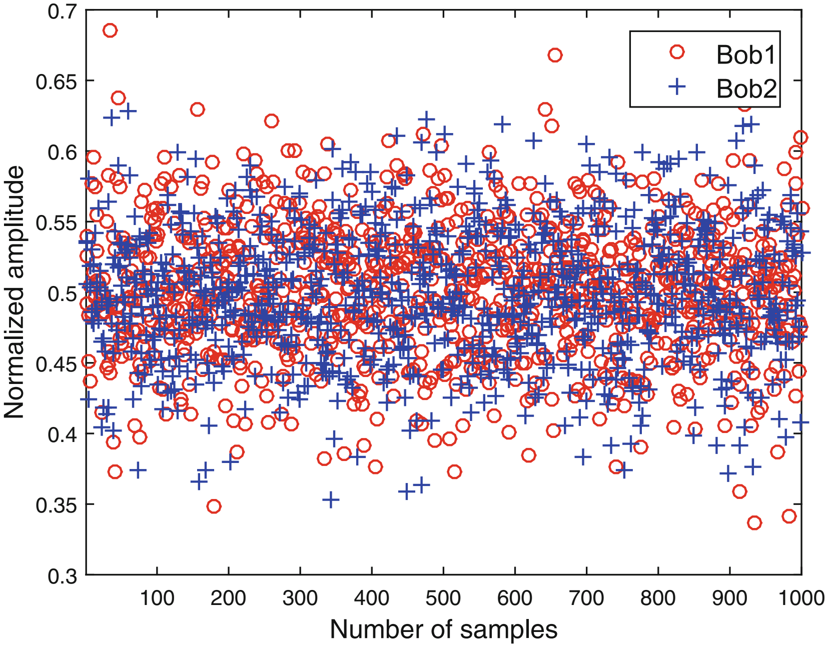

Fig. 4. Original channel estimation of different transmitters.

layer attribute, namely received signal strength is considered in the experiment to verify the viability of the LSTM network. The mathematical formulation of the received signal strength can be written as $P_{loss} = 75 + 36.1 \log(d/10)$, where P_{loss} represents the path loss, and d denotes the distance between the transceivers. We randomly set the initial parameters of the network model before training. Then, our intelligent process is validated in an indoor conference room to show its performance. Once the LSTM network is trained, we evaluate the model on the test subset. Then we verify the authentication performance of the proposed system by calculating the detection accuracy and the false alarm rate.

Figure 5 characterizes the training performance of the proposed LSTM network scheme (see Sect. 3) relying on the channel attribute. We consider the use of the received signal strength to authenticate malicious attackers. We can observe from Fig. 5 that with the increasing iteration index, the loss values of our intelligent process dramatically decrease. The reason for this trend is that the LSTM network is an adaptive algorithm that can update the system according to the dynamic characteristics of the channel, so as to adapt to the time-varying wireless network environment.

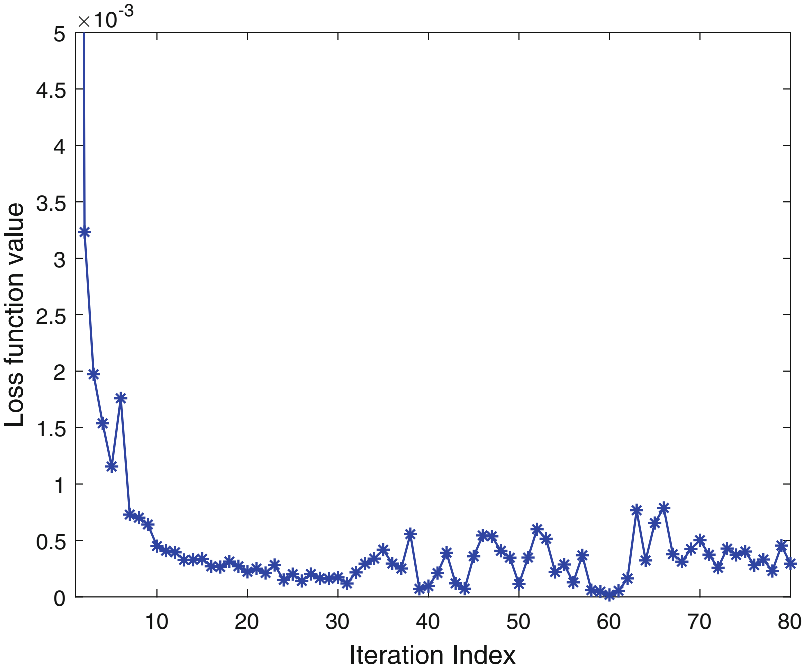

Fig. 5. Convergence performance of our intelligent authentication scheme.

Table 1. The authentication performance

Reference	Approach	False alarm rate	Accuracy
Scheme [14]	PCA + GMM	7.92%	94.50%
Scheme [13]	KLT + GMM	7.72%	92.80%
Scheme [15]	CNN	5.72%	95.81%
Our scheme	LSTM	0.80%	97.15%

In Table 1, we can observe the comparison results between our proposed solution and the existing methods using the USRP dataset. We can see that the proposed security authentication scheme has better performance in terms of accuracy and false alarm rate. Specifically, compared with the security method based on Gaussian mixture model, the recognition rate of the LSTM algorithm is greatly improved.

5 Conclusion

In this paper, we proposed a lightweight physical layer authentication scheme based on a long Short Term Memory network. Since manual selection of channel static characteristics will reduce the robustness of security authentication, we use the LSTM network to learn the channel characteristics while performing authentication tasks. To validate the effectiveness of utilizing the intelligent scheme, USRP prototype systems are set up in an indoor conference room. Furthermore, the rigorous security analysis and convergence of the proposed scheme are comprehensively evaluated.

References

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. **17**(4), 2347–2376 (2015). https://doi.org/10.1109/COMST.2015.2444095
2. Xu, T., Darwazeh, I.: Design and prototyping of neural network compression for non-orthogonal IoT signals. In: IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, vol. 2019, pp. 1–6 (2019)
3. Xu, T.: Waveform-defined security: a framework for secure communications. In: IEEE/IET 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP2020), Porto, Portugal (2020)
4. Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., Zeng, K.: Physical-layer security of 5G wireless networks for IoT: challenges and opportunities. IEEE Internet Things J. **6**(5), 8169–8181 (2019)
5. Wang, N., Jiao, L., Alipour-Fanid, A., Dabaghchian, M., Zeng, K.: Pilot contamination attack detection for NOMA in 5G mm-wave massive MIMO networks. IEEE Trans. Inf. Forensics Secur. **15**, 1363–1378 (2020)
6. Gui, G., Liu, F., Sun, J., Yang, J., Zhou, Z., Zhao, D.: Flight delay prediction based on aviation big data and machine learning. IEEE Trans. Veh. Technol. **69**(1), 140–150 (2020)
7. Huang, H., et al.: Deep learning for physical-layer 5G wireless techniques: opportunities, challenges and solutions. IEEE Wirel. Commun. **27**(1), 214–222 (2020)
8. Wang, N., Jiang, T., Lv, S., Xiao, L.: Physical-layer authentication based on extreme learning machine. IEEE Commun. Lett. **21**(7), 1557–1560 (2017)
9. Qiu, X., Jiang, T., Wang, N.: Safeguarding multiuser communication using full-duplex jamming and Q-learning algorithm. IET Commun. **12**(15), 1805–1811 (2018)
10. Wang, N., Li, W., Jiang, T., Lv, S.: Physical layer spoofing detection based on sparse signal processing and fuzzy recognition. IET Signal Process. **11**(5), 640–646 (2017)
11. Wang, N., Jiang, T., Li, W., Lv, S.: Physical-layer security in Internet of Things based on compressed sensing and frequency selection. IET Commun. **11**(9), 1431–1437 (2017)
12. Moon, T., Choi, H., Lee, H., Song, I.: Rnndrop: a novel dropout for RNNs in ASR. In: ASRU, pp. 65–70 (2015). https://doi.org/10.1109/ASRU.2015.7404775
13. Qiu, X., et al: Wireless user authentication based on KLT and Gaussian mixture model. IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, vol. 2019, pp. 1–5 (2019)
14. Qiu, X., Jiang, T., Wu, S., Hayes, M.: Physical layer authentication enhancement using a Gaussian mixture model. IEEE Access **6**, 53583–53592 (2018)
15. Qiu, X., Dai, J., Hayes, M.: A learning approach for physical layer authentication using adaptive neural network. IEEE Access **8**, 26139–26149 (2020)