ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

Radio Frequency Fingerprint-Based Intelligent Mobile Edge Computing for Internet of Things Authentication

B.Usha, Assistant Professor, Department of CSE, Pallavi Engg College
Firdose Fathima, Assistant Professor, Department of CSE, Pallavi Engg College

Abstract: In this paper, a light-weight radio frequency fingerprinting identification (RFFID) scheme that combines with a two-layer model is proposed to realize authentications for a large number of resource-constrained terminals under the mobile edge computing (MEC) scenario without depending on encryption-based methods. In the first layer, signal collection, extraction of RF fingerprint features, dynamic feature database storage, and access authentication decision are carried out by the MEC devices. In the second layer, learning features, generating decision models, and implementing machine learning algorithms for recognition are performed by the remote cloud. By this means, the authentication rate can be improved by taking advantage of the machine-learning training methods and computing resource support of the cloud. The results shows that the novel method can achieve higher recognition rate when compare with traditional RFFID method by using wavelet feature effectively, which demonstrates the efficiency of our proposed method.

Introduction: Earlier we have observe an innovative Internet-of-Things (IoT) paradigm, which includes mobile edge computing (MEC) with traditional IoT architecture which raises many security protection requirements. Later many researchers have focused on physical (PHY) layer information to enhance wireless security. Radio Frequency Fingerprint ID is very precious to physical layer security technology. In fact, Radio Frequency Fingerprint, which embody the hardware property of the wireless transmitter to be identified and have the characteristics difficult to be cloned, are a good candidate to be used to enhance device identification. Therefore, it is especially suitable for the source-constrained terminals of IoT to perform access identification.

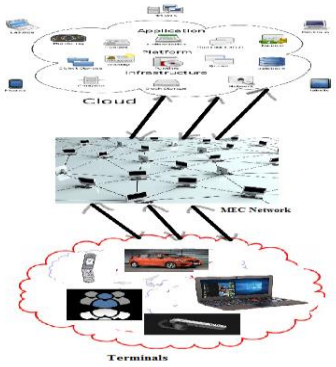

Figure 1. Mobile edge computing-Internet-of-Things (MEC-IoT) architecture

As shown in Figure 1, the MEC-IoT architecture encompasses three different layers, the IoT devices, MEC, and the remote cloud platform.

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

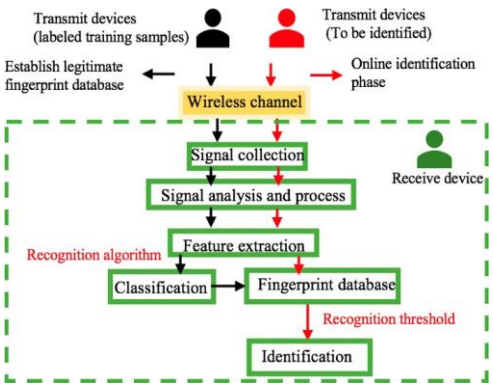

Figure 2. Radio Frequency Fingerprinting Identification (RFFID) authentication method.

As shown in Figure 2, the RFFID method consists of six steps: Signal collection, signal analysis and process, feature extraction and classification, fingerprint database, and identification. RFFID mainly includes two processes. The first one is offline to establish a fingerprint database for legitimate wireless devices by implementing, analyzing and processing the radiation signals after collecting the signals of legitimate devices. The second process is an online authentication process. The signals of the wireless devices to be identified are collected and the fingerprint features are extracted through signal analysis and processing. Then, matching and recognition are carried out in the existing legitimate fingerprint database. Tthis method consumes resources in offline samples learning due to a large number of samples training required to ensure the authentication effect.

Proposed System: Our authentication scheme is light-weight to the IoT terminals. Here Radio Frequency Fingerprint based authentication that combines physical characteristics of wireless device radio frequency and machine learning algorithms under grouping the work of edge computing and cloud computing to achieve fast and efficient authentication.

Here we use lightweight algorithm for resource-constrained terminals to accomplish access authentication with a satisfied authentication rate. The architecture of the proposed RFFID-MEC authentication consists of two layers: The first layer provides signal collection, signal analysis, and process, feature extraction and classification, and establish fingerprint feature database, which will be performed on the MEC layer. The second layer includes learning features, generating decision models, and implementing machine learning algorithms for recognition, which need the powerful computing support for much more complex and resource-consuming tasks, will be implemented on the remote cloud due to the limited computing resources of MEC. Figure 3 shows a detailed logical flow of this authentication process.

The authentication process includes two processes that are an offline training process and an online decision-making process.

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

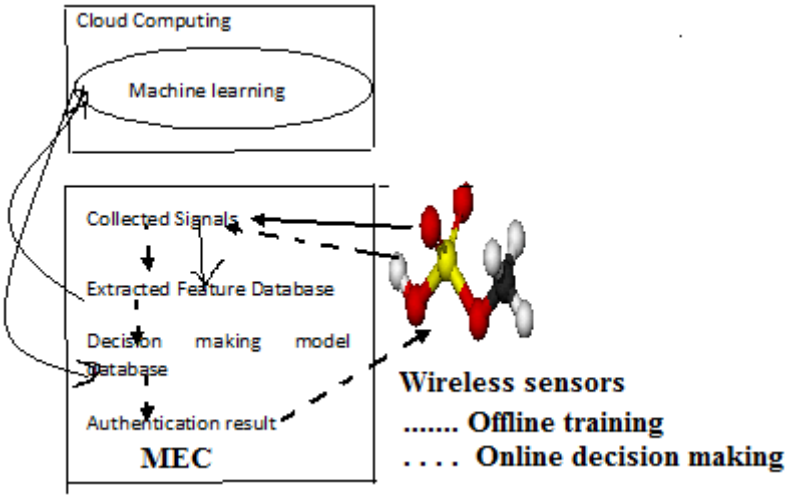

Figure 3. Detailed authentication process

In the offline training authentication process, a terminal initiates an access request to the MEC platform. After that, the MEC platform collects the signal of the terminal with the identity information, and then performs feature extraction and establishes dynamic fingerprint feature database. The feature information is transmitted to the cloud computing platform. The cloud computing platform makes use of the machine learning algorithm to generate the authentication decision-making model, and transmits the resulted decision model that meets the target authentication rate back to the MEC platform. At this time, the offline training authentication process ends. In the online decision-making authentication process, a terminal initiates an access request to the MEC platform, and the MEC platform collects signals, extracts features, and performs fast identity authentication through the trained authentication model that was established from the previous step.

The Radio Frequency Fingerprint - MEC algorithm is illustrated below. Steps 1–3, 5, 6 are carried out by the first layer and Step 4 carried out by the second layer.

Step 1: The MEC platform continuously acquires signals
Step 2: Data preprocessing in MEC platform
Step 3: The MEC platform generates training and testing data sets
Step 4: The cloud platform generates a decision-making model
Step 5: The MEC platform stores the decision-making model and data set in the database.
Step 6: The MEC platform implements access authentication to determine whether it is legal.
Step 7: The MEC platform continuously collects the RF signals of the IoT devices with identity tags

The MEC platform collects the signal and preprocesses the data, and then passes the processed data and the training data set in the database through the decision model to judge whether the terminal identity is legal. If it is the legal device, MEC platform consents the access request. If it is not legal, the MEC platform refuses to access the request.The main features of the RFFID-MEC architecture are lesser complexity and latency along with more authentication accuracy.

Conclusion: Present paper has proposes a lightweight Radio Frequency Fingerprinting

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

Identification-MEC authentication method by taking advantage of attributes-based MEC, cloud, and non-encryption Radio Frequency Fingerprinting Identification for IoT terminals. The presented two-layer model is extremely suitable for the MEC-based IoT paradigms. Compared with the traditional RFFID security access authentication, our light-weight Radio Frequency Fingerprinting Identification -MEC authentication method has achieved higher authentication accuracy and improved the work efficiency of IoT terminals, in which all the computing burdens are taken by the edge devices and the cloud.

References

1. Kawamoto Y., Yamada N., Nishiyama H., Kato N., Shimizu Y., Zheng Y. A feedback control-based crowd dynamics management in IoT system. IEEE Internet Things J. 2017;4:1466–1476. doi: 10.1109/JIOT.2017.2724642.

2. Verma S., Kawamoto Y., Fadlullah Z.M., Nishiyama H., Kato N. A survey on network methodologies for real-time analytics of massive IoT data and open research issues. IEEE Commun. Surv. Tutor. 2017;19:1457–1477. doi: 10.1109/COMST.2017.2694469.

3. Massouri, A., Cardoso, L., Guillon, B., Hutu, F., Villemaud, G., Risset, T., Gorce, J.M.: Cortexlab: An open FPGA-based facility for testing SDR & cognitive radio networks in a reproducible environment. In: Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on. pp. 103–104. IEEE (2014). https://doi.org/10.1109/INFCOMW.2014.6849176

4. Merchant, K., Revay, S., Stantchev, G., Nousain, B.: Deep learning for RF device fingerprinting in cognitive communication networks. IEEE Journal of Selected Topics in Signal Processing 12(1), 160–167 (feb 2018). https://doi.org/10.1109/JSTSP.2018.2796446

5. Nachmani, E., Beery, Y., Burshtein, D.: Learning to decode linear codes using deep learning (jul 2016), http://arxiv.org/abs/1607.04793 7. O'Shea, T.J., Clancy, T.C., McGwier, R.W.: Recurrent neural radio anomaly detection (nov 2016), http://arxiv.org/abs/1611.00301

6. Sankhe, K., Belgiovine, M., Zhou, F., Riyaz, S., Ioannidis, S., Chowdhury, K.: ORACLE: Optimized Radio clAssification through Convolutional neuraL nEtworks (dec 2018), http://arxiv.org/abs/1812.01124.

7. Harase S. On the F-2-linear relations of Mersenne Twister pseudorandom number generators. Math. Comput. Simul. 2014;100:103–113. doi: 10.1016/j.matcom.2014.02.002.

8. Borle K.M., Chen B.A., Du W.L. Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation. IEEE Trans. Inf. Forensics Secur. 2015;10:2225–2235. doi: 10.1109/TIFS.2015.2452893.