A Malicious Node Identification Method Based on Edge Computing

Aidong Xu1, Minggui Cao2, Runfa Liao2, Yunan Zhang1, Yixin Jiang1, Yi Chen1, Hong Wen1 and Jinran Du1

1. Electric Power Research Institute, China Southern Power Grid Co., Ltd. Guangzhou, China
2. School of Aeronautics and Astronautics, University of Elec. Science and Tech. of China, Chengdu 610054, China

Abstract. Edge computing can meet the needs of many industries in real-time business control, security and privacy protection. In the process of massive heterogeneous terminals accessing the network through edge devices, it is very challenging to achieve fast and reliable authentication. The physical layer authentication technology authenticates through the channel characteristics, which has the characteristics of lightweight, and can well adapt to the authentication scenario of massive heterogeneous terminal access. In order to identify malicious nodes, this paper proposes an attack identification scheme of malicious nodes under edge computing. The new channel response information vector is constructed by using the correlation between the channel information of consecutive frames. Two or more time slot channel frequency response vectors are averaged to obtain a new channel response vector. It has the advantages of low computational complexity and high recognition accuracy. And combined with the channel frequency response based on the deep neural network to identify malicious nodes, the data set in the factory environment is simulated.

1. Introduction

Edge computing is deployed near nodes, close to IoT nodes. It overcomes long-distance transmission delays, computing loads, and reduces network congestion in cloud computing centers [1]. Edge computing has rich application scenarios, such as smart home, video surveillance, smart medical, smart transportation, unmanned factories, smart grid and other applications [2].

However, edge computing nodes are widely distributed and vulnerable to attack. Edge computing nodes face a series of security challenges such as clone node and Sybil node attacks. The principle of clone node attack is that the attacker captures the legal nodes in the network and obtains all their legal information [3]; Sybil node attacks use hardware nodes to carry multiple captured ids on hardware nodes to implement multiple network attacks [4]. How to quickly and effectively identify these malicious attacks and isolate the nodes has become the key to prevent malicious node attacks and improve the security of edge computing [5].

Because these attack methods adopt the method of capturing hardware nodes and possess the same ID and key information as legitimate nodes, traditional cryptographic security mechanisms cannot identify these attack methods [6]. The physical layer feature identification method utilizes the space-time uniqueness of wireless channel information [7], and judges the user identity by comparing the similarity of channel information between consecutive frames without the need for complicated upper-layer encryption operations, which has the advantage of being fast and efficient. The physical layer feature identification method is very suitable for resource-constrained micro terminals [8]. However, in practical applications, the limited availability of channel information data makes it more time-
consuming for feature extraction to have a certain amount of data. If the amount of data is insufficient, it can also lead to low recognition accuracy and affect the recognition accuracy.

The purpose of this paper is to overcome the shortcomings of the prior art and provide a method for identifying malicious nodes in edge computing. This method is an improvement on the malicious node identification method that used the unique channel information formed by the channel passing through the packet to determine the location characteristics of each terminal in the edge system [9]. The method of judging the position characteristics of each terminal in the edge system through the unique channel information requires a certain amount of channel information data to extract the channel characteristics. The currently adopted method is to extract channel information through channel estimation from the demodulated synchronization header. Insufficient channel characteristic data obtained in this way will result in low recognition accuracy and affect the recognition accuracy [10]. This method uses the correlation between consecutive multi-frame channel information to construct a new channel response information vector. More specifically, two or more time slot channel frequency response vectors are averaged to obtain a new channel response vector. It has the advantages of low computational complexity and high recognition accuracy.

2. Technical Solutions

The purpose of this article is achieved by the following technical solutions: A method for edge computing malicious node identification, including the following steps:

For the channel information data set that has been collected for the $k$ node:

$$D_k : D_k = \{X_k, Y_k\}$$ (1)

Among them, the input sample (that is, the channel information matrix composed of the channel frequency response vector) set:

$$X_k = \left[ H_1^k, H_2^k, \ldots, H_{N_t}^k \right]$$ (2)

The method of collecting channel information through the above steps may be a channel estimation method such as minimum mean square error (MMSE), least squares (LS), or an improved channel estimation method of these methods.

The corresponding label (node number), that is, the output sample set is:

$$Y_k = \left[ I_1, I_2, \ldots, I_k \right]_{N_t}$$ (3)

All channel information of the data set $D_k$ belongs to one node (the $k$ node). $H_t^k$ represents the channel frequency response vector of the $k$ node in the $t$ time slot. $N_t$ represents the number of channel frequency responses of the $k$ node, that is, the total number of time slots.

Then, construct a new input channel information sample according to the following formula:

$$H_k^t = \frac{1}{\alpha_0 + 1} \sum_{i=0}^{\infty} H_i^k, 1 \leq \alpha_0 < N_k, n + \alpha_0 \leq N_k$$ (4)

Where $\alpha_0$ is a positive integer representing the number of samples constructed for each parameter evaluation sample.

The input sample set after average data enhancement on $H_k$ is:

$$X_k^* = \left[ H_1^k, H_2^k, \ldots, H_{N_t}^k, H_1^k, \ldots, H_{M_t}^k \right]$$ (5)

Where $M_t$ represents the number of channel information vectors after average data enhancement. The label matrix after average sample construction, that is, the output sample set is:
\[ Y^\dagger_k = \left[ I_k, I_k, \cdots, I_k \right]_{N_k+M_k} \]  

(6)

Through the above operations, we get a new training sample set as:

\[ D^\dagger_k : D^\dagger_k = \{ X^\dagger_k, X^\dagger_k \} \]  

(7)

The beneficial effect of this paper is: in this paper, the correlation between successive multi-frame channel information that has been collected is used to construct a new channel response information vector. That is, two or more time slot channel frequency response vectors are averaged to obtain a new channel response vector. It overcomes the shortcomings of low recognition rate caused by insufficient data amount in channel information extraction and channel characteristics for malicious node identification.

3. Specific Implementation Mode

Deep neural networks have excellent fitting and classification capabilities, so the use of deep neural networks for malicious node recognition has good performance [11]. Figure 1 shows the deep neural network model. However, when the data set is relatively small, the deep neural network has its limitations, the time correlation requirement of wireless channel information, or some other restrictive requirements, which cannot obtain a relatively large channel sample set [12]. Then, in the case where it is very important to obtain enough data sets from the collection channel response in the relevant time, data augmentation can regenerate the data set from the existing data set through some calculation operations. This is to extend the limited training data set to implement the neural network Training, an effective way to improve recognition rate.

As shown in Figure 2, a method for identifying malicious nodes based on channel frequency response based on deep neural network combined with data enhancement is divided into two phases, namely a training phase and an authentication phase. There are three steps in the training phase: First, obtain the channel frequency response vector of the received signal of the known sending node and its corresponding label. Then, use the data enhancement module to construct some new effective channel information vectors. The newly generated channel information vector and the original channel information vector have the same label, that is, they belong to the same node. Finally, an input matrix composed of all channel information vectors and an output matrix composed of its corresponding labels are used to train a deep neural network.

As shown in Figure 3, the data set in the factory environment identifies the malicious nodes in multiple users under dynamic conditions. Under the condition of two users, the recognition rate is more than 90%, which is about 5% higher than the existing results. The data enhancement achieves better recognition performance.
**Figure 1.** Deep Neural Network Model

**Figure 2.** A Model of Channel Frequency Response Malicious Node Identification Based on Deep Neural Network Combined with Data Enhancement
4. Conclusion
Taking edge computing as the application background, this paper proposes a malicious node attack recognition scheme based on channel characteristics for edge computing. It is a new idea and supplement for the research of physical layer certification and the field of information security. The innovation of this paper is to overcome the shortcomings of low recognition rate caused by insufficient data volume in the extraction of channel characteristics for malicious node identification.

5. Acknowledgement
This work is supported by National major R&D program (2018YFB0904900, 2018YFB0904905).

6. References
[1] Fei Pan, Zhibo Pang, Michele Luvisotto, Ming Xiao, Hong Wen, Physical-Layer Security for Industrial Wireless Control Systems: Basics and Future Directions, IEEE Industrial Electronics Magazine, vol. 12, Issue 4, pp. 18-27, Dec. 2018.
[2] Feiyi Xie, Hong Wen, Yushan Li, Songlin Chen, Lin Hu, Yi Chen, and Huanhuan Song, Optimized Coherent Integration-Based Radio Frequency Fingerprinting in Internet of Things, IEEE Internet of Things Journal, Vol. 5, Issue 5, pp. 3967-3977, Oct. 2018.
[3] Songlin Chen, Hong Wen, Jinsong Wu, Wenxin Lei, Wenjing Hou, Wenjie Liu, Aidong Xu, Yixin Jiang, Internet of Things Based Smart Grids Supported by Intelligent Edge Computing, IEEE Access, vol.7, pp. 74089–74102, 03 June 2019.
[4] Fei Pan, Zhibo Pang, Ming Xiao, Hong Wen, Run-Fa Liao, "Clone Detection Based on Physical Layer Reputation for Proximity Service", IEEE Access, vol. 7, pp. 3948-3957, Feb. 2019.
[5] DemiRas M, Song Y. An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks[C]. World of Wireless, Mobile and Multimedia Networks, 2006: 565-570
[6] Liu J, Wang X. Physical Layer Authentication Enhancement Using Two-Dimensional Channel Quantization, IEEE Transactions on Wireless Communications, 2016, 15(6):4171-4182
[7] Lin Hu, Hong Wen, Bin Wu, Fei Pan, Run-Fa Liao, Huanhuan Song, Jie Tang, Xiumin Wang, Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things, IEEE Internet of Things Journal, Vol. 5, Issue 1, pp. 219-228, 2018.
[8] Dan S, Kai Z, Xiang W, et al. PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks [J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 1817-1827

[9] Jinling Zhang, Hong Wen, Huanhuan Song, Yixin Jiang, Zhengguang Zhang, Luping Zhang, Xiping Zhu, Using Basis Expansion Model for Physical Layer Authentication in Time-Variant System, in Proceedings of CNS 2016, 17-19 October 2016 // Philadelphia, PA USA

[10] Yuanpeng Xie, Hong Wen, Bin Wu, Yixin Jiang, Jiaxiao Meng, A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing, IEEE Transaction on Cloud Computing, vol.7, no2, PP. 383 - 391, April 2019. SCI

[11] Yi Chen, Hong Wen, Huanhuan Song, Songlin Chen, Feiyi Xie, Qing Yang, Lin Hu, Lightweight one-time password authentication scheme based on radio frequency fingerprinting, IET Communications, 12(12): 14477-1484, March 2018.

[12] Huanhuan Song, Hong Wen, Lin Hu, Yi Chen, and Run-fa Liao, Optimal Power Allocation for Secrecy Rate Maximization in Broadcast Wiretap Channels, IEEE Wireless Communications Letters, 2018, 7(4): 514-517.