IOP Conference Series: Earth and Environmental Science

PAPER • OPEN ACCESS

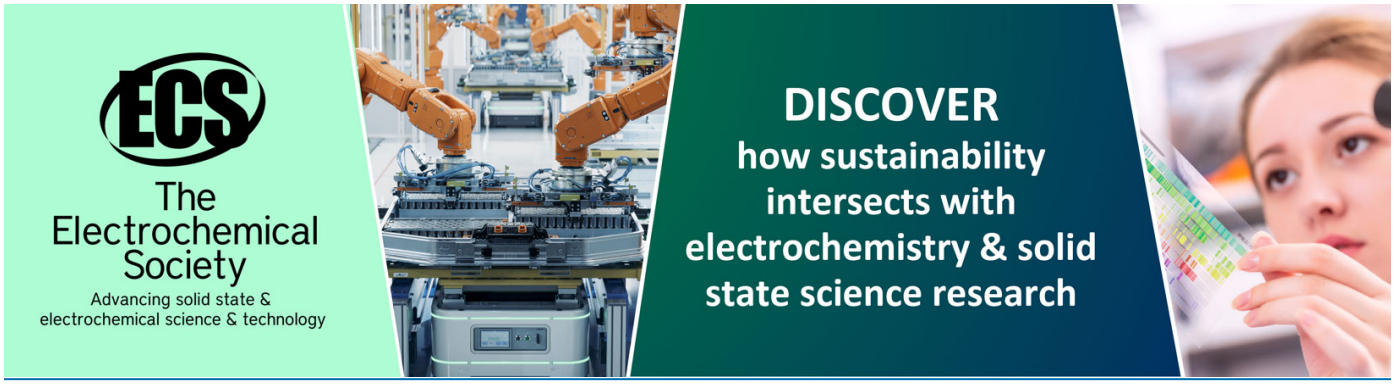
Channel Fingerprint Packet Authentication Method Based on Edge Computing Cooperation

To cite this article: Aidong Xu *et al* 2021 *IOP Conf. Ser.: Earth Environ. Sci.* **693** 012007

View the article online for updates and enhancements.

You may also like

- Real Time Implementation of Terminal Security Policies Selection Based on Edge Computing
Aidong Xu, Qianru Wang, Yixin Jiang et al.
- Falcon: a highly flexible open-source software for closed-loop neuroscience
Davide Ciliberti and Fabian Kloosterman
- Dynamic trust security approach for edge computing-based mobile IoT devices using artificial intelligence
Ahmed Jedidi



This content was downloaded from IP address 3.14.253.152 on 08/05/2024 at 19:38

IOP Conf. Series: Earth and Environmental Science **693** (2021) 012007 doi:10.1088/1755-1315/693/1/012007

Channel Fingerprint Packet Authentication Method Based on Edge Computing Cooperation

Aidong Xu[1*], Tengyue Zhang[2], Qicong Yang[3], Yixin Jiang[1] and Yunan Zhang[1]

[1]Electric Power Research Institute, China Southern Power Grid Co., Ltd. Guangzhou, China
[2]School of Aeronautics and Astronautics, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China
[3]Sichuan Jiuzhou Electric Group Co., Ltd., Mianyang 621000, China
Email: xuad@csg.cn; uestczty@163.com; yangqicong9@163.com; jiangyx@csg.cn; zhangyn@csg.cn; Corresponding Author Email: xuad@csg.cn

Abstract. With the emergence of various low-latency application scenarios in the Internet of things (IoT), edge computing provides a series of low-latency computing modes such as real-time data processing and real-time decision-making, supports multiple terminals, and solves the problems of the existing cloud computing architecture. This paper proposes a channel fingerprint data packet authentication method based on edge computing cooperation. The edge server and smart terminal perform cooperative computing, make full use of the computing power of the smart terminal, reasonably allocate the amount of computing tasks, and effectively realize lightweight data packet authentication. The task running time is shortened and the authentication efficiency is improved.

1. Introduction

In the past few years, the network architecture of Internet of things (IoT) relies on remote cloud computing for mobile computing, network management control and data storage [1]. However, this architecture cannot achieve low latency applications in some scenarios. Many industrial control systems, such as manufacturing systems, smart grids, oil and gas systems and cargo packaging systems, often require end-to-end delays between sensors and control nodes to be kept within milliseconds [1-3]. With the increasing number of IoT devices, a large amount of data is generated, It needs a lot of network bandwidth to transmit all these data to the cloud, and the delay is uncontrollable. But for the IoT devices themselves, their resources are very limited, they cannot only rely on their own limited resources to meet all their computing needs. In general, the traditional IoT network architecture based on remote cloud mainly has the following three problems: (1) How to deal with low delay; (2) How to transmit more data in the case of limited network bandwidth; (3) How to solve the energy consumption of asymmetric resources.

In recent years, in order to solve the above problems, cloud computing mode has begun to turn to the edge computing network. By introducing edge computing, edge intelligent services are provided at the network edge side of the device or data source[2-5]. The basic architecture is shown in Figure 1. The IoT devices form an edge computing network at the edge end, and then transmit to the remote cloud computing network through the edge computing network. In this architecture, the IoT devices interact with the edge computing nodes, and then preprocess the data, so as to reduce the data exchange with the cloud, improve the efficiency of the solution in real time, and reduce the delay and energy consumption of IoT solutions based on traditional cloud computing [3-6]. The IoT architecture

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

after introducing edge computing mainly includes three layers: perception layer, edge computing network layer and remote cloud computing network layer. This architecture is a feasible solution, which has the characteristics of low energy consumption and low time delay, and has become a new generation of IoT architecture [4].

The channel fingerprint data packet authentication method needs to be within the relevant time of the channel, and the required real-time performance is high[7-15]. This paper proposes an edge computing cooperative channel fingerprint data packet authentication method. The edge end collaborates with an authenticated terminal to perform computational tasks based on task complexity. Finally, the edge terminal will integrate the computing results and make corresponding judgments on the data packet authentication terminal. This model can make full use of computing resources to achieve real-time high authentication rate.

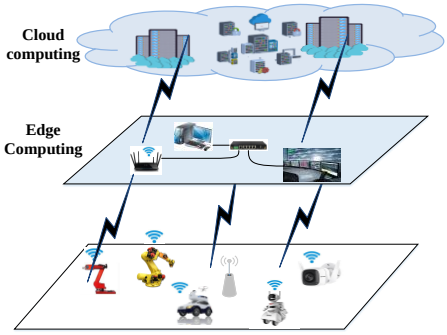


Figure 1. Edge computing framework.

2. Channel Fingerprint Packet Authentication Method Based on Edge Computing Cooperation

The channel fingerprint data packet authentication method based on edge computing collaboration is different from the radio frequency (RF) fingerprint identification authentication method based on edge computing cooperation. Because the channel fingerprint data packet authentication process needs to be within the channel fingerprint correlation time, its processing complexity is relatively small, but the required real-time performance is high, so in the end-side cooperative computing mode under the edge computing architecture, usually only a certified terminal device is selected for cooperative computing with the edge end. This method can not only effectively realize lightweight data packet authentication, but also realize real-time high authentication rate.

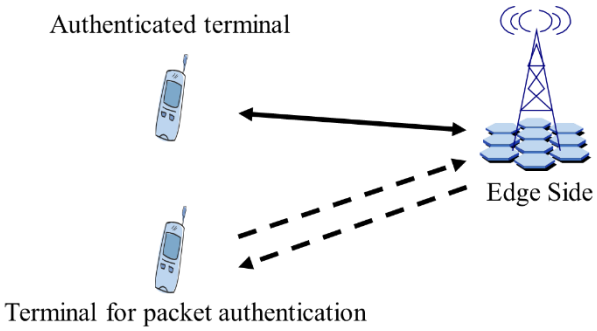


Figure 2. Cooperative computing between terminal and edge side under the channel fingerprint data packet authentication method.

Figure 2 shows the cooperative computing between a single terminal and an edge terminal based on the channel fingerprint data packet authentication method. First, a handshaking connection is established between a data packet authentication terminal and an edge terminal. After the handshake is

completed, the edge terminal will execute a data packet authentication method based on channel fingerprints and classify tasks according to its computational complexity, and then perform computing tasks in coordination with an authenticated terminal. In the end, the edge terminal will integrate the computing results and make corresponding judgments on the terminal for packet authentication. The detailed process of the channel fingerprint data packet authentication method based on edge computing collaboration is as follows.

(1) Since the computing task of the data packet authentication algorithm based on channel fingerprint is less than that of radio frequency fingerprint identification, the total computing task W is decomposed into the following forms

$$W = K_1 w_1 \tag{1}$$

Where K_1, w_1 are the amount of computing tasks to execute the packet authentication algorithm, assuming that there is only one computing complexity task.

(2) Configure the corresponding parameter properties of the edge end and an authenticated terminal device, including physical distance, storage calculation, transmission bandwidth, calculation speed, etc., as follows:

$$(l, r, b, c) \rightarrow (distance,\ storage,\ bandwidth,\ calculation\ speed) \tag{2}$$

The edge end parameter attribute E_0 is

$$E_0 : (l_0 = 0,\ r_0,\ b_0 = 0,\ s_0) \tag{3}$$

The parameter attribute D_1 of a certified terminal device is:

$$D_1 : (l_1,\ r_1,\ b_1,\ s_1) \tag{4}$$

(3) Total time required for cooperative computing at the edge side

$$t_{sum} = \arg\min_k \frac{1}{s_0}\sum_{i=1}^{1} w_i k_{i0} + \sum_{j=1}^{1}\frac{1}{s_j}\sum_{i=1}^{1} w_i k_{ij} + \sum_{j=1}^{1}\frac{1}{b_j}\sum_{i=1}^{1} w_i k_{ij} + \sum_{j=1}^{1}\frac{2l_j}{c} \tag{5}$$

$$\begin{aligned} s.t\quad & \sum_{j=0}^{1} k_{1j} = K_1, W = K_1 w_1 \\ & 0 < k_{1j} < K_1 \\ & w_1 k_{10} < r_0, w_1 k_{11} < r_1, w_1 k_{12} < r_2 \\ & r_0 > r_1, r_2 \\ & s_0 > s_1, b_1 > (b_0 = 0), l_1 > (l_0 = 0) \end{aligned}$$

Equivalent to matrix form

$$t_{sum} = \arg\min_{\mathbf{x}} \mathbf{w}^T \mathbf{X}\bar{\mathbf{s}} + \mathbf{w}^T \mathbf{X}\mathbf{b} + 2\mathbf{l}^T \mathbf{c} \tag{6}$$

$$\begin{aligned} s.t\quad & \mathbf{w}^T X \le \mathbf{r}^T, X\mathbf{e} = \bar{k}, W = \mathbf{w}^T \bar{k} \\ & (s_1, b_0 = 0, l_0 = 0) < (s_0, b_1, l_1) \\ & w_1 < w_2 < \ldots < w_n \end{aligned}$$

Where $w = \mathrm{w}_1$ is the total computing task consisting of only one complexity of computing task. $\mathbf{r} = (r_0, r_1)^T$ is the computing capacity of the edge end and one authenticated terminal device. $\mathbf{l} = (l_0 = 0, l_1)^T$ is the physical distance between one authenticated terminal device and the edge end, where l_0 is to construct an equivalent matrix operation model, which means that the physical distance of the edge end itself is always zero; $\mathbf{c} = (1/c, 1/c)^T$, where c is the propagation speed of light; $\mathbf{e} = (1,1)^T$ represents the unit vector; $\bar{k} = K_1$ represents the number of executions required for each computing task of one computational complexity; $\mathbf{b} = (0, 1/b_1)^T$, where b_1 is the transmission bandwidth between the edge end and the first authenticated terminal device. $\bar{\mathbf{s}} = (1/s, 1/s_1)^T$, where s and s_1 represent the computing speed of the edge end and one authenticated terminal device respectively.

(4) Optimal solution of objective function:

$$X = \left[x_{10}, x_{11}\right] \tag{7}$$

According to the optimal solution of the objective function, the amount of computing tasks to be performed by the edge terminal and a certified terminal are as follows. The amount of computing tasks at the edge end is

$$W^{Edge} = w_1 x_{10} \tag{8}$$

The amount of computing tasks of the certified terminal equipment is:

$$W^{1devices} = w_1 x_{11} \tag{9}$$

Finally, by reasonably distributing the amount of computing tasks, the edge end and an authenticated terminal device cooperate to perform data packet authentication based on channel fingerprint.

3. Experiment and Simulation Analysis

The detailed process of the cooperative computing task between the edge end and a single terminal is shown in Figure 3. It is assumed that the total computing task W to be processed by the edge end is composed of computing tasks of one complexity, and the total number of times is K_1. According to the parameter attributes of the terminal and itself, the edge node gives a reasonable execution times allocation strategy with the goal of the fastest cooperative computing speed. The edge node executes k_{10} times, and the terminal node executes k_{11} times, so as to realize the process of edge computing cooperatively allocating computing tasks.

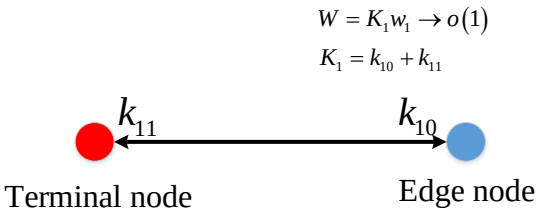


Figure 3. The process of edge computing cooperatively assigning computing tasks.

In order to verify the effectiveness of the channel fingerprint data packet authentication method based on edge computing cooperation, this paper has done related comparative experiments. The experiment is based on an adaptive enhancement learning channel fingerprint packet authentication

method. The algorithm based on adaptive enhancement learning needs to perform the training of the offline decision model to realize the adaptive adjustment of the decision threshold in the data packet authentication stage. In this paper, we will conduct the cooperative and non-cooperative task assignment experiments of edge computing for the offline training process. The experiment is carried out for the real MIMO-OFDM communication system. Through the realization of the three-party authentication experiment, 500 channel fingerprints from different users based on amplitude statistics were collected as offline training samples. In the adaptive enhancement learning algorithm, the decision tree is selected as the weak classifier, the learning rate is set to 0.1, and the authentication rate of the target offline decision model is set to 95%.

Aiming at the offline training process of edge computing collaboration, the experiment assigns training samples to the edge end and a terminal device respectively, and the computing power of the mobile terminal is weaker than that of the edge end. When the offline training model meets the target authentication rate, the decision model is output, and the offline training process ends at this time. The comparison experiment adopts the same parameter configuration, where the edge end needs to perform an offline training process with the same amount of training samples until the target authentication rate is met. By comparing the time delay in the offline training process of the two experiments, the effectiveness of the method proposed in this paper is analyzed. The experimental results are shown in Table 1. It can be seen from the results that the channel fingerprint data packet authentication method using edge computing cooperative training is 0.95s faster than the non-cooperative method. The method proposed in this paper provides a reliable guarantee for further realizing fast execution of data packet authentication.

Table 1. Time delay comparison analysis results.

Scheme contrast	Cooperative mode of edge computing	Non-cooperative mode of edge computing
Delay (s)	2.23	3.18

4. Conclusion

This paper presents a method for channel fingerprint data packet authentication with edge computing cooperation. This paper adopts the channel fingerprint data packet authentication method of adaptive enhancement learning, and conducts the edge computing cooperative and non-cooperative task assignment experiments in the offline training process. The experiment is carried out for the real MIMO-OFDM communication system. The channel fingerprint data packet authentication method using edge computing collaborative training is 0.95s faster than the non-cooperative method. The method proposed in this paper provides a reliable guarantee for further realizing fast execution of data packet authentication.

5. Acknowledgments

This work is supported by the National major R & D program (No. 2018YFB0904900, 2018YFB0904905).

6. References

[1] Rani K, Sagar R K 2017 Enhanced data storage security in cloud environment using encryption, compression and splitting technique *2017 2nd International Conference on Telecommunication and Networks (TEL-NET) IEEE* pp 1-5.
[2] Mao Y, You C, Zhang J, Huang K, Letaief K B 2017 A survey on mobile edge computing: The communication perspective *IEEE Communications Surveys & Tutorials* vol. 19 pp 2322-2358.
[3] Yu Y 2016 Mobile edge computing towards 5G: Vision, recent progress, and open challenges *China Communication* vol. 13 pp 89-99.
[4] Chen S, Wen H, Wu J, Lei W, Hou W, Liu W and Jiang Y 2019 Internet of things based smart grids supported by intelligent edge computing *IEEE Access* vol 7 pp 74089-74102

[5] Ji B, Li Y, Zhou B, Li C, Song K and Wen H 2019 Performance analysis of UAV relay assisted IoT communication network enhanced with energy harvesting *IEEE Access* vol 7 p 38738-38747
[6] Hu L, Wen H, Wu B, Pan F, Liao R F, Song H, Tang J, Wang X 2018 Cooperative jamming for physical layer security enhancement in Internet of Things *IEEE Internet of Things Journal* vol 5 pp 219-228.
[7] Hu L, Wen H, Wu B, Tang J, Pan F, Liao R F 2017 Cooperative-jamming-aided secrecy enhancement in wireless networks with passive eavesdroppers *IEEE Transactions on Vehicular Technology* vol 67 pp 2108-2117.
[8] Liao R F, Wen H, Wu J, Song H, Pan F and Dong L 2018 The rayleigh fading channel prediction via deep learning *Wireless Communications and Mobile Computing 2018*
[9] Wen H, Ho P H, Qi C and Gong G 2010 Physical layer assisted authentication for distributed ad hoc wireless sensor networks *IET information security* vol 4 pp 390-396.
[10] Wen H, Ho P H and Wu B 2014 Achieving secure communications over wiretap channels via security codes from resilient functions *IEEE Wireless Communications Letters* vol 3 pp 273-276
[11] Wen H, Tang J, Wu J, Song H, Wu T, Wu B and Sun L M 2014 A cross-layer secure communication model based on Discrete Fractional Fourier Fransform (DFRFT) *IEEE Transactions on emerging topics in computing* vol 3 pp 119-126
[12] Xie F, Wen H, Li Y, Chen S, Hu L, Chen Y, Song H 2018 Optimized Coherent Integration-Based Radio Frequency Fingerprinting in Internet of Things *IEEE Internet of Things Journal* vol 5 pp 3967-3977.
[13] Wen H, Wang Y, Zhu X, Li J and Zhou L 2013 Physical layer assist authentication technique for smart meter system *IET Communications* vol 7 pp 189-197
[14] Wen H, Ho P, Gong G 2009 A Novel Framework for Message Authentication in Vehicular Communication Networks *Global communications conference* pp 3067-3072.
[15] Wen H, Li S, Zhu X, Zhou L 2013 A framework of the PHY-layer approach to defense against security threats in cognitive radio networks *IEEE Network* vol 27 pp 34-39.