ORIGINAL RESEARCH
published: 22 July 2022
doi: 10.3389/fenrg.2022.950611

Fifth Generation Mobile Communication Technology Network Attack Defense Based on Software Defined network Technology in Power Internet of Things

Tong Li[1,2], *Hai Zhao*[1], *Shouyou Song*[3,4]*, *Chao Yang*[5], *Chunlai Du*[6,7] *and Yang Liu*[2]

[1]*School Of Computer Science and Engineering Northeastern University, Shenyang, China,* [2]*Liaoning Electric Power Research Institute of State Grid Corporation of China, Shenyang, China,* [3]*Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, Beijing University of Posts and Telecommunications, Beijing, China,* [4]*DigApis Information Security Technology (Jiangsu) Co. Ltd, Nantong, China,* [5]*State Grid Liaoning Electric Power Co. Ltd, Shenyang, China,* [6]*North China University of Technology, Beijing, China,* [7]*Beijing DigApis Technology Co. Ltd, Beijing, China*

OPEN ACCESS

Edited by:
Chunhe Song,
Shenyang Institute of Automation (CAS), China

Reviewed by:
Shudong Li,
Guangzhou University, China
Wang Zhongru,
Bucharest Academy of Economic Studies, Romania

Correspondence:
Shouyou Song
songshouyou@bupt.edu.cn

Specialty section:
This article was submitted to Smart Grids, a section of the journal Frontiers in Energy Research

Received: *23 May 2022*
Accepted: *14 June 2022*
Published: *22 July 2022*

Citation:
Li T, Zhao H, Song S, Yang C, Du C and Liu Y (2022) Fifth Generation Mobile Communication Technology Network Attack Defense Based on Software Defined network Technology in Power Internet of Things. Front. Energy Res. 10:950611. doi: 10.3389/fenrg.2022.950611

The purpose is to guarantee the security of fifth generation mobile communication technology (5G) network in power Internet of Things environment and improve the ability of wireless network communication to resist attacks. First, in terms of attack prevention, the 5G network security structure is proposed to replace the plaintext information commonly used in the original system with Ciphertext based on software defined network (SDN), thereby alleviating the security risks of the data dimension. Second, concerning attack detection, the signal is identified by using the imperfections and differences of equipment manufacturing based on the above security structure, preventing the attacker from further harming the sensitive data leaked. Researchers found that the SDN-based 5G network attack prevention scheme avoids the centralized exposure of sensitive data, improves security, reduces computational overhead, and simplifies encryption logic. Without affecting the bandwidth, the existing 5G network system is greatly prevented from attacks. The detection mechanism is not limited by the low-dimensional feature space, and it demonstrates strong robustness and stability. It can effectively detect the attacks on 5G network system in power Internet of Things (IoT). This study provides an important reference for the protection of 5G communication network attacks under IoT.

Keywords: power Internet of Things, SDN, 5G, network attack prevention, network attack detection

INTRODUCTION

Wireless communication systems are vulnerable to security threats from the beginning (Kuleshov et al., 2018; Lonzetta et al., 2018). The information of mobile phones and wireless channels in 1G wireless networks is easy to be cloned illegally and falsified (Bu et al., 2017). In 2G wireless networks, garbage information not only attacks the system, but it also spreads false information or broadcasts unnecessary marketing information (Goel and Jain, 2018). In 3G wireless networks, the increase in internet protocol (IP)–based communication requirements lead to an endless stream of network security vulnerabilities (Mohd Aman et al., 2021). Next, in

4G wireless networks, the emergence of smart devices, multimedia traffic, and new applications brings more complex and dynamic threats to mobile communication (Bilal et al., 2018). Then, the 5G wireless communication system meets the requirements of ubiquitous broadband access, mobility of high-quality devices, and connectivity of a large number of devices in a super-reliable and affordable way, which will face more complex security threats than before. In the smart grid, 5G technology can make the power Internet of Things more reliable and efficient. Moreover, once the 5G communication network is attacked, the normal operation of the power system can be interrupted or execute incorrectly instructions. More seriously, it maybe leads to a series of security incidents related to it. For example, the power cut of Ukrainian power companies caused by an attack brought a series of livelihood crises in 2016. Therefore, the research on 5G communication network security in the power Internet of Things is of great significance to ensure the security of power system.

Due to the lack of reliable encryption logic and authentication mechanism, resisting advanced network attack technology is difficult for a 5G network, which will eventually lead to security problems such as vulnerable system communication and sensitive data leakage (Wu et al., 2020). Therefore, there is a needed to design a strong security structure and establish an effective security mechanism (Ting et al., 2019). In traditional wireless networks, two types of methods to solve communication security are found, namely the network attack prevention scheme and the network attack detection scheme (Abu Talib et al., 2018). Moreover, the network attack prevention scheme can be divided into two types. One is to design a new network security structure combined with the key network technologies, but no security structure fully applicable to 5G networks exists (Yılmaz and Gönen, 2018). The other is to use the knowledge of cryptography to encrypt the transmission data, achieving the goal of protecting network communication security (Senarak, 2021). However, the existing cryptography-based methods exhibit two limitations: 1) some encryption algorithms need high computational overhead (Kaaniche and Laurent, 2017); 2) some password-based methods are vulnerable to the attack of the protocol layer. Besides, the traditional network attack detection scheme also needs to be improved (Saracevic et al., 2021). First, most existing physical identification systems rely on data and cannot protect the channel security of wireless networks. Second, physical layer recognition technology is vulnerable to some uncertain or signal acquisition factors.

Therefore, with the application and popularization of the 5G network, prospective research of emerging technologies should be conducted. Here, the advantages of new technologies are combined to design a comprehensive security protection scheme for 5G network, the security challenges faced by 5G system communication are comprehensively analyzed, and a 5G network security structure and the mechanism is designed from the perspectives of network attack prevention and detection to improving the communication security of the 5G network system.

NETWORK SECURITY AND AUTHENTICATION

Network Security Architecture

The security of the network structure attracts the attention of many scholars. Among them, Yao et al. proposed a 5G network security architecture based on the concept of domain and hierarchy, which solves the security problem of 5G network load caused by Internet of Things equipment deployment by capturing a new trust model and identifying security control points (Yao et al., 2019). Abdulqadder et al. proposed a multilayer network security structure, which is based on the host identity protocol to achieve the goal of secure communication between network elements, in addition to the backhaul device from the source address spoofing and denial of service attacks (Abdulqadder et al., 2020). Next, Mrabet et al. proposed a 5G network security structure composed of the data layer, control layer, security application layer, and program layer, but the biggest problem of the system is that the coupling degree between security and 5G network management is not close enough, when the security layer cannot work (Mrabet et al., 2020). Cao et al. proposed a robust 5G network security architecture by studying the security standards of the 5G network, which can protect WLAN and mobile access devices from network attacks at the same time. However, the scheme is expensive and demonstrates no practical application value (Cao et al., 2020). Next, Fang et al. proposed a new 5G wireless security architecture, which studied the 5G network handover process and signaling load scheme, achieving the effect of reducing signaling load and ensuring 5G security service quality (Fang and Qian, 2020). Song et al. proposed a novel intrusion detection method combining a deep learning–based method and a feature-based method for smart grid (Song et al., 2021a).

Security Authentication Scheme

Vinodha proposed a new data transmission planning for wireless sensor networks (WSNs) based on elliptic curve cryptography and homomorphic encryption. The encryption scheme uses a genetic algorithm to construct the best network structure in cluster form (Vinodha et al., 2020). Baek established a new wireless network transmission data sWIFI algorithm to cut the energy consumption of the network by using homomorphic encryption technology. The sWIFI algorithm demonstrates a higher performance than the hash message authentication code cipher algorithm (Baek et al., 2020). Wang put forward a location-based data encryption scheme for WSNs. The scheme can only complete key updates through conversion, but it cannot resist the denial of service attack (Wang et al., 2019). Vivekrabinson suggested a secure data exchange scheme for wireless fault-tolerant networks based on attribute encryption. The scheme makes the content data only accessible by authorized nodes and authenticated by routing messages (Vivekrabinson and Muneeswaran, 2021). Jerbi made a new data encryption transmission scheme, which adopts lightweight encryption technology to make multiple sensor nodes cooperate to encrypt and transmit data, thus reducing the load of a single sensor node and ensuring communication security (Jerbi et al., 2021). Zhang gave a lightweight block cipher scheme under chaos mapping and genetic operation, which uses elliptic curve points to prove communication nodes, which is nine times faster than led protocol (Zhang et al., 2021).

A Review of Related Research Issues

As a whole, the existing solutions only use a single method to protect the traditional network or detect or prevent 5G network communication security, and some problems in actual use are still found. To overcome the shortcomings of the existing research, a comprehensive 5G network security protection scheme is proposed from the following two aspects. First, a 5G network security structure based on software defined network (SDN) is designed for 5G network attack prevention, and it can prevent the network attack through establishing a data encryption authentication mechanism between the control layer and the data transmission layer. This method can decrease the possibility of attacks, while the transmission overhead is small, and does not affect the existing network bandwidth. Second, a network attack detection mechanism based on radio frequency (RF) fingerprint is proposed for 5G network attack detection based on the above network security structure. The method can reduce the security risk of 5G network system effectively, and it demonstrates great application prospects.

CONSTRUCTION AND ANALYSIS OF THE MODEL

Component Deployment of Network Security Architecture

According to the 5G business scenario requirements and the trend of technology development, the communication security of the 5G network system should be ensured, and the flexible deployment of 5G network function, the network scalability and programming, and low cost and low energy consumption should be achieved before a new 5G network security structure is designed (Muthanna et al., 2019). A 5G network security structure based on SDN is put forward. As shown in **Supplementary Figure S1**, three layers are found in the structure, which are application layer, control layer, and data transmission layer. Next, a new security entity (SecE) is added to the control layer as the control entity to control SecE and other security functions, protect the hash table and seed of all devices, and offer encryption authentication during data transmission (Boero et al., 2018). This structure not only reduces the operation and maintenance cost of the 5G network, but it also prevents the data leakage caused by network attacks when the equipment and users communicate in different scenarios (Huang et al., 2019).

The application layer is composed of end-user business applications and other control entities. The control layer includes logically centralized controllers, which perform unified control functions. A distributed security gateway (SecGW) is an intermediate device between the control layer and the data transmission layer, and it refers to the gateway that serves as the point of decryption and encryption for the network. SecGW can relay authentication messages between SecE and data plane switch (DPS). The lowest data transmission layer contains a wireless access network and a core transmission network (Xu et al., 2017).

Authentication Strategy of Data Encryption

The authentication mechanism of data encryption demonstrates two endpoints. As shown in **Supplementary Figure S2**, the above end is the SDN device, which is equivalent to a switch controlled by SDN. The key storage in each device is composed of three parts: a unique ID, a preload hash table $\mathrm{H_i}$ given by the backend, and a synchronized key $\mathrm{S_i}$. Next, the key is randomly generated when the device requests to establish a communication channel(Deep et al., 2019). After the device authentication is completed, the back end will generate a new key and reload it into the device. The degree difference of authentication adaptive node is D_i, the residual node energy is η_i, and the node motion similarity is M_i. The equation of the weight of the model is as follows:

$$w_i = \frac{q_i}{\sum_{k=1,m} q_i} \tag{1}$$

i can be taken as 1,2, . . . m. w is the weight of the parameter, q is the reference factor, and $w_i \in (0,1)$, $\sum_i w_i = 1$.

$$W_i = w_1 D_i + w_2 \eta_i + w_3 M_i \tag{2}$$

When $w_1 + w_2 + w_3 = 1$, the outage probability p is determined by the equation in the core network:

$$p = \frac{S}{\pi N r^2} \tag{3}$$

Radius is a function of the total energy E, which is consumed by the network in data collection:

$$\begin{cases} \min: E \\ s.t. 0 < r < 1 \end{cases} \tag{4}$$

If n nodes are found, the average node degree is as follows:

$$\bar{D} = \frac{\sum_{i=0}^{n} D_i}{n} \tag{5}$$

The degree difference of adaptive nodes is obtained by subtracting the degree of each subnode from the degree of the average node:

$$\varepsilon_i = \left| D_i - \bar{D} \right| \tag{6}$$

In the core network, the smaller degree difference of the node is, the worse the degree of the adaptive node is:

$$D_i = e^{-\varepsilon_i} \tag{7}$$

To calculate the residual energy of nodes, the initial energy of the network is set as E, and the residual energy is Es. When the node exhibits a noncluster head, the energy consumption per unit time is e_1. When the node demonstrates a cluster head, the energy consumption per unit time is e_2. Therefore, the equation of the residual energy of the node is as follows (14):

$$E_s = \mathrm{E} - \sum_{1}^{i} e_1 D_{ni} t_i - \sum_{1}^{j} e_2 D_{nj} t_j \tag{8}$$

In the equation, i is the number of the nodes exhibiting noncluster head, D_{ni} is the degree of the node acting as noncluster head for the *ith* times, and t_i is the time of the nodes acting as noncluster head; j is the times of the nodes acting as the cluster head, D_{nj} is the degree of the nodes acting as the cluster head, and t_j is the time of the nodes acting as the cluster head for the *j*th times. Thus, in each round of cluster head election, the efficiency equation is as follows:

$$\eta = \frac{E_s}{E} \tag{9}$$

The average velocity difference equation is as follows:

$$\bar{v}_{Ax} = \frac{\sum_{i=1}^{n} (v_A \cos\alpha - v_i \cos\theta_i)}{n} \tag{10}$$

$$\bar{v}_{Ay} = \frac{\sum_{i=1}^{n} (v_A \sin\alpha - v_i \sin\theta_i)}{n} \tag{11}$$

Therefore, the difference of the average speed is the following:

$$\bar{v}_A = \sqrt{\bar{v}_{Ax}^2 + \bar{v}_{Ay}^2} \tag{12}$$

Then, the variance of velocity difference between adjacent nodes on the x-axis and y-axis is the following:

$$\sigma_{Ax}^2 = \frac{\sum_{i=1}^{n} (\bar{v}_{Ax} - v_{Aix})^2}{n} \tag{13}$$

$$\sigma_{Ay}^2 = \frac{\sum_{i=1}^{n} \left(\bar{v}_{Ay} - v_{Aiy}\right)^2}{n} \tag{14}$$

Therefore, the variance between A and adjacent nodes can be expressed as the following:

$$\sigma_A^2 = \frac{\sigma_{Ax}^2 + \sigma_{Ay}^2}{2} \tag{15}$$

Therefore, the motion similarity equation is as follows:

$$M_A = e^{-\left(\sigma_A^2 + \bar{v}_A^2\right)} \tag{16}$$

Authentication Mechanism Interaction of Data Encryption

As shown in **Supplementary Figure S3**, the switch first sends the authentication request M_1 to SecGW. Moreover, M_1 consists of two parts: the unique ID and the preloaded hash table Hi provided by the back end. To conclude, SecGW forwards the authentication message to DPS (Khalid et al., 2020). If DPS passes the authentication, it will update its key and allow communication between control layer devices. If DPS fails, it will not perform any action or make another request. The specific equation of the weight of object i in service node k is as follows:

$$Weight_j = \frac{t_i/T}{s_i} * \frac{1}{f_n + 1} \tag{17}$$

T is the latest T accesses, and it is a constant. t_i is the number of times when the object i is accessed in the latest T accesses of users, s_i is the size of the object, and f_n is the number of nodes where the object i is adjacent to the cache object i of the fog node j during the access.

$$S_{OHHR} = \frac{\sum \mathrm{h}_i}{\sum r_i}, i = 1, 2, \cdots, m \tag{18}$$

$$S_{SHR} = \frac{\sum SH_i}{\sum r_i}, i = 1, 2, \cdots, m \tag{19}$$

SH_i is the hits of file i in the system, and r is the total number of accesses of object i. The response delay of the system is calculated as follows:

$$S_{ARR} = \frac{\sum R_i * S_i}{\sum T_i}, i = 1, 2, \cdots, m \tag{20}$$

R_i is the total number of accesses of object i, S_i is the size of object i, and T_i is the total response time of object i. A reasonable bandwidth is used:

$$S_{BC} = \sum (c_i * h_i + (c_i + c_0) * sh_i + (c_i + c_0) * ch_i) * f_j \quad i = 1, 2, \cdots, p; j = 1, 2, \cdots, m \tag{21}$$

h_i is the hits of the node i, sh_i is the hits of adjacent nodes, and ch_i is the times of the hits.

As shown in **Supplementary Figure S4**, information interaction of control layer devices is established between DPS1 and DPS2. First, DPS1 sends the request M1 to DPS2, which is composed of the device ID and relevant hash value. After the request from DPS1 is received, DPS2 sends the authentication request REQ to SecGW. SecGW sends the authentication message acknowledge character (ACK) associated with DPS1 and DPS2 to DPS2. If the request passes the authentication, DPS2 sends the authentication message M2 to DPS1. If one of the DPS fails, they will no longer perform any operations (Gupta et al., 2019).

Experimental Deployment and Performance Analysis

To verify the feasibility and security of the proposed authentication mechanism of data encryption, the network simulator Mininet is used to simulate the 5G network experiment scenario. The scheme uses four laptops and two Ethernet hubs on the test bench. OpenVSwitch version 1.10.0 is installed on every laptop. As shown in **Supplementary Figure S5**, the scheme uses a virtual machine to simulate the host. Next, one of the laptops acts as the SDN controller, and the POX controller runs on this laptop. The other three laptops are connected through two D-LINKDSR-250N routers. According to the experimental scenario, the attacker is connected to each hub.

Five hosts are found in the sparse networks, with 50 hosts in the medium networks and 500 hosts in the dense network. The connection outage rate is used to evaluate the performance of the scheme. The connection outage rate is the most important index when the network is attacked. The spatial modeling equation is as follows:

$$H(u(t+r)) = A(d)\left(1 + pow(u(t+r))\right)e^{i(w+\Delta w)(t+r)} \tag{22}$$

$A(d)$ is not just a constant, $pow(u(t+r))^{i(w+\Delta w)(t+r)}$ is an amplitude nonlinear term, and $H(u(t+r))$ is a phase nonlinear term. The received signal C can be expressed as the following:

$$C \approx \sum_{i=1}^{n} H(i) \cdot H(u(t+r)) \tag{23}$$

t is the time, r is the transmission path, and u is the transmission energy. The connection interruption rate of the experiment is expressed as follows:

$$r = num_{dis}/100 \tag{24}$$

$nnum_{dis}$ is the number of times the connection is interrupted in the simulation. The similarity is used for analysis, and the calculation is as follows:

$$w = 1 - \sum_{i=1}^{N}\left(V_{pred} - V_{true}\right)^2 \Big/ \sum_{i=1}^{N}\left(V_{true} - \overline{V_{true}}\right)^2 \tag{25}$$

V_{pred} is the RF signal output by the prediction device, and V_{true} is the RF signal output by the device. The most advanced TFSv1 and SDSecurity are compared to explore their performance. TFSV1 is commonly used in the commercial SDN, but it is usually subjected to the above three attacks due to the lack of authentication (Song et al., 2021b).

RESULTS OF THE PERFORMANCE TEST FOR THE MODEL

Spoofing Simulation of Internet Protocol Address

As shown in **Supplementary Figure S6**, the result of disconnection rate under the spoofing of IP address is achieved. The number of attacks is slowly adjusted from 0 to 500, and the disconnection rate is recorded to test the feasibility of the scheme. When the number of attacks is 500, the disconnection rate is less than 0.1%.

Supplementary Figure S7 shows that the connection interruption rate of Robust, TFSv1, and SDSecurity is increasing with the increase of the number of attacks. The disconnection rate of Robust is very low. Even if the attacks are 500, the maximum disconnection rate of Robust is still lower than 0.01%, which is much less than that of TFSv1 and SDSecurity. With the increase of the number of hosts, SDSecurity will experience a great loss. The disconnection rate of Robust does not change much. Under the interference of the spoofing of IP address, the performance of Robust is much better than that of the existing schemes.

Man-In-The-Middle Attack Simulation

Supplementary Figure S8 shows the simulation results under man-in-the-middle (MITM) attack. Similar to the simulation in the spoofing of IP address, the number of attacks is slowly adjusted from 0 to 500, and the related disconnection rate is recorded. When the number of attacks reaches 500, the disconnection rate is less than 0.1%.

Supplementary Figure S9 shows that when the host is medium, the disconnection rate of Robust is still lower than 0.01%, which is much better than that of TFSv1 and SDSecurity. Due to the lack of authentication in TFSv1 communication, the performance of TFSv1 decreases greatly with the increase of attacks. Next, for SDSecurity, if it is used in dense scenes, its performance will still degrade a lot, and it cannot be used in large scenes. These observations show that the scheme demonstrates better performance in detecting MITM.

Replay Attack Simulation

Supplementary Figure S10 shows the simulation result under replay attack. The attacker steals the information between the devices in the control layer and records the messages from the devices, and then, it makes the attacker repeat the messages to the SecE. When the number of attacks reaches 500, the disconnection rate is less than 0.1%.

As shown in **Supplementary Figure S11**, Robust demonstrates the lowest disconnection rate under replay attack. Under these three attacks, the disconnection rate of this scheme is less than 0.01%, which is the lowest of the three security architectures. For the other two architectures, the disconnection rate of TFSv1 is about 75%, and that of SDSecurity is 8%. Although the disconnection rate of SDSecurity is relatively low, and at the medium level, its performance will degrade a lot in dense scenarios, the disconnection rate increases as high as 73%. Researchers concluded that the scheme can meet the requirements of commercial use.

Results of Accuracy Test

Supplementary Figure S12 shows that the accuracy of the proposed method is more than 90%. Also, the accuracy of PARADIS, FBSleuth, and SP decreases from 97 to 88%, 93–75%, and 92–37%, respectively. This shows that the scheme overcomes the problem of insufficient robustness of the authentication of another physical layer.

As shown in **Supplementary Figure S13**, physical layer function (PLF) demonstrates good stability. At the same time, the false negative rate of PLF is close to the false positive rate, which is usually called equal error rate in the training model. The closer the two probabilities are, the more effective the parameter threshold selection is and the higher the overall recognition ability of the mechanism is. This shows that the threshold selected in the experiment is very effective.

Training Time Analysis

As shown in **Supplementary Figure S14**, the training time of the model largely depends on the amount of bit data. If the number of the bit data is large, the training time will be long. Also, the accuracy is proportional to the amount of bit data. The more bit data there are, the higher the accuracy is. PLF achieves more than 95% accuracy when the amount of bit data is more than 35MB, which takes less than 7 min. When the amount of bit data of convolutional neural network (CNN) is more than 35MB, the accuracy is more than 86%, and the training time is as long as 30 min.

Supplementary Figure S15 shows that the accuracy of recurrent neural network (RNN) is more than 92% when the amount of bit data is more than 35MB, but the training time is more than 30 min, which proves that it takes more than 30 min for CNN and RNN to identify 5G signals, and their accuracy is not high. Therefore, researchers concluded that PLF is the most reliable authentication method for 5G devices.

DISCUSSION AND ANALYSIS OF RESEARCH RESULTS

A comprehensive communication protection scheme for the 5G network system is proposed from the perspective of network attack prevention and detection, aiming at the problem that the existing 5G network structure demonstrates no reliable encryption logic and is difficult to resist advanced network attack technology. The scheme uses the current advanced network security technology SDN to separate the control of the existing network from the data stream, so that the system users can control and observe the abnormal behavior of network transmission and effectively prevent attacks. To further improve the security of data transmission in the network structure, a new distributed security gateway is designed between the control layer and the data transmission layer, and a new encryption authentication mechanism based on cryptography is established. Next, after SDN data communication is masked, the possibility of sensitive information leakage is further reduced, and the reliability is strong. The results of the experiment show that the scheme can prevent several traditional attacks, and it can improve the communication security of the 5G system. Based on the network security structure, a reliable mechanism based on RF fingerprint is proposed to detect 5G network attacks from the perspective of network attack detection, which makes up for the lack of security of attack prevention scheme. Meanwhile, a mechanism of encryption attack prevention is established between the control layer and the data transmission layer to improve the security of data transmission in the network system. Moreover, Ciphertext is used to replace the plaintext used in the communication of the original system components and prevent it from attacks. The research and analysis of three typical attacks are carried out. The Mininet design experiment of the network emulator used verifies the security and stability of the proposed scheme.

CONCLUSION

The communication security of 5G network system is deeply analyzed, and a comprehensive communication protection scheme for 5G network system from the perspectives of network attack prevention and network attack detection is proposed. Moreover, a new distributed security gateway is designed between the control layer and the data transmission layer, and a new data encryption authentication mechanism based on cryptography is established to protect the security of data transmission in the network structure. The 5G network attack prevention scheme based on SDN avoids the centralized exposure of sensitive data, improves the security, reduces the computational overhead, and demonstrates simple encryption logic. Although a more comprehensive system is proposed, many shortcomings are still found in this study; first, the 5G network attack prevention scheme based on SDN proposed doesn't detect any possible security threats, so taking a targeted design is necessary to strengthen the security of the algorithm; second, the 5G network attack detection mechanism based on RF fingerprint is a successful attempt to break the traditional mode of feature–based radio frequency identification system. However, if the attacker uses a high-end RF transceiver, the copied signal will be very similar to the real signal. Therefore, how to use the scheme to resist this kind of attack is challenging.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/**Supplementary Material**, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

TL performed the data analyses and wrote the manuscript. HZ and SS performed the experiment. CY contributed significantly to analysis and manuscript preparation. CD and YL helped perform the analysis with constructive discussions.

FUNDING

This work was supported by the Research Program of Liaoning Electric Power Research Institute of State Grid Corporation of China under Grant No. 2021YF-55, the Fundamental Research Funds for the Central Universities of China under Grant No. 2020GFZD014.

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fenrg.2022.950611/full#supplementary-material

REFERENCES

Abdulqadder, I. H., Zhou, S., Zou, D., Aziz, I. T., and Akber, S. M. A. (2020). Multi-layered Intrusion Detection and Prevention in the SDN/NFV Enabled Cloud of 5G Networks Using AI-Based Defense Mechanisms. *Comput. Netw.* 179, 107364. doi:10.1016/j.comnet.2020.107364

Abu Talib, M., Abbas, S., Nasir, Q., and Mowakeh, M. F. (2018). Systematic Literature Review on Internet-Of-Vehicles Communication Security. *Int. J. Distributed Sens. Netw.* 14 (12), 155014771881505. doi:10.1177/1550147718815054

Baek, J., Han, S. I., and Han, Y. (2020). Optimal UAV Route in Wireless Charging Sensor Networks. *IEEE Internet Things J.* 7 (2), 1327–1335. doi:10.1109/jiot.2019.2954530

Bilal, K., Khalid, O., Erbad, A., and Khan, S. U. (2018). Potentials, Trends, and Prospects in Edge Technologies: Fog, Cloudlet, Mobile Edge, and Micro Data Centers. *Comput. Netw.* 130, 94–120. doi:10.1016/j.comnet.2017.10.002

Boero, L., Bruschi, R., Davoli, F., Marchese, M., and Patrone, F. (2018). Satellite Networking Integration in the 5G Ecosystem: Research Trends and Open Challenges. *IEEE Netw.* 32 (5), 9–15. doi:10.1109/mnet.2018.1800052

Bu, K., Weng, M., Zheng, Y., Xiao, B., and Liu, X. (2017). You Can Clone but You Cannot Hide: A Survey of Clone Prevention and Detection for RFID. *IEEE Commun. Surv. Tutorials* 19 (3), 1682–1700. doi:10.1109/comst.2017.2688411

Cao, J., Yan, Z., Ma, R., Zhang, Y., Fu, Y., and Li, H. (2020). LSAA: A Lightweight and Secure Access Authentication Scheme for Both UE and mMTC Devices in 5G Networks. *IEEE Internet Things J.* 7 (6), 5329–5344. doi:10.1109/jiot.2020.2976740

Deep, G., Mohana, R., Nayyar, A., Sanjeevikumar, P., and Hossain, E. (2019). Authentication Protocol for Cloud Databases Using Blockchain Mechanism. *Sensors* 19 (20), 4444. doi:10.3390/s19204444

Fang, D., and Qian, Y. (2020). 5G Wireless Security and Privacy: Architecture and Flexible Mechanisms. *IEEE Veh. Technol. Mag.* 15 (2), 58–64. doi:10.1109/mvt.2020.2979261

Goel, D., and Jain, A. K. (2018). Mobile Phishing Attacks and Defence Mechanisms: State of Art and Open Research Challenges. *Comput. Secur.* 73, 519–544. doi:10.1016/j.cose.2017.12.006

Gupta, S., Buriro, A., and Crispo, B. (2019). DriverAuth: Behavioral Biometric-Based Driver Authentication Mechanism for On-Demand Ride and Ridesharing Infrastructure. *ICT Express* 5 (1), 16–20. doi:10.1016/j.icte.2018.01.010

Huang, X., Cheng, S., Cao, K., Cong, P., Wei, T., and Hu, S. (2019). A Survey of Deployment Solutions and Optimization Strategies for Hybrid SDN Networks. *IEEE Commun. Surv. Tutorials* 21 (2), 1483–1507. doi:10.1109/comst.2018.2871061

Jerbi, W., Guermazi, A., Cheikhrouhou, O., and Trabelsi, H. (2021). CoopECC: A Collaborative Cryptographic Mechanism for the Internet of Things. *J. Sensors* 2021, 1–8. doi:10.1155/2021/8878513

Kaaniche, N., and Laurent, M. (2017). Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms. *Comput. Commun.* 111, 120–141. doi:10.1016/j.comcom.2017.07.006

Khalid, U., Asim, M., Baker, T., Hung, P. C. K., Tariq, M. A., and Rafferty, L. (2020). A Decentralized Lightweight Blockchain-Based Authentication Mechanism for IoT Systems. *Clust. Comput.* 23 (3), 2067–2087. doi:10.1007/s10586-020-03058-6

Kuleshov, S. V., Zaytseva, A., and Aksenov, A. Y. (2018). The Conceptual View of Unmanned Aerial Vehicle Implementation as a Mobile Communication Node of Active Data Transmission Network. *Int. J. Intelligent Unmanned Syst.* 6 (4), 174–183. doi:10.1108/ijius-04-2018-0010

Lonzetta, A., Cope, P., Campbell, J., Mohd, B., and Hayajneh, T. (2018). Security Vulnerabilities in Bluetooth Technology as Used in IoT. *J. Sens. Actuator Netw.* 7 (3), 28. doi:10.3390/jsan7030028

Mohd Aman, A. H., Shaari, N., and Ibrahim, R. (2021). Internet of Things Energy System: Smart Applications, Technology Advancement, and Open Issues. *Int. J. Energy Res.* 45 (6), 8389–8419. doi:10.1002/er.6451

Mrabet, H., Belguith, S., Alhomoud, A., and Jemai, A. (2020). A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors* 20 (13), 3625. doi:10.3390/s20133625

Muthanna, A., Ateya, A., Gudkova, I., Abuarqoub, A., Samouylov, K., Koucheryavy, A., et al. (2019). Secure and Reliable IoT Networks Using Fog Computing with Software-Defined Networking and Blockchain. *J. Sens. Actuator Netw.* 8 (1), 15. doi:10.3390/jsan8010015

Saracevic, M. H., Adamovic, S. Z., Miskovic, V. A., Elhoseny, M., Macek, N. D., Selim, M. M., et al. (2021). Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures. *IEEE Trans. Rel.* 70 (2), 819–830. doi:10.1109/tr.2020.3010973

Senarak, C. (2021). Port Cybersecurity and Threat: A Structural Model for Prevention and Policy Development. *Asian J. Shipp. Logist.* 37 (1), 20–36. doi:10.1016/j.ajsl.2020.05.001

Song, C., Sun, Y., Han, G., and Rodrigues, J. J. P. C. (2021). Intrusion Detection Based on Hybrid Classifiers for Smart Grid. *Comput. Electr. Eng.* 93, 107212. doi:10.1016/j.compeleceng.2021.107212

Song, C., Xu, W., Han, G., Zeng, P., Wang, Z., and Yu, S. (2021). A Cloud Edge Collaborative Intelligence Method of Insulator String Defect Detection for Power IIoT. *IEEE Internet Things J.* 8 (9), 7510–7520. doi:10.1109/jiot.2020.3039226

Ting, T. H., Lin, T. N., Shen, S. H., and Chang, Y. W. (2019). Guidelines for 5G End to End Architecture and Security Issues. *arXiv Prepr. arXiv:1912.10318* 26 (26), 115–123.

Vinodha, D., Mary Anita, E. A., and Mohana Geetha, D. (2020). A Novel Multi Functional Multi Parameter Concealed Cluster Based Data Aggregation Scheme for Wireless Sensor Networks (NMFMP-CDA). *Wirel. Netw.* 27 (2), 1111–1128. doi:10.1007/s11276-020-02499-6

Vivekrabinson, K., and Muneeswaran, K. (2021). Fault-Tolerant Based Group Key Servers with Enhancement of Utilizing the Contributory Server for Cloud Storage Applications. *IETE J. Res.* 2021, 1–16. doi:10.1080/03772063.2021.1893842

Wang, H., Han, G., Zhang, W., Guizani, M., and Chan, S. (2019). A Probabilistic Source Location Privacy Protection Scheme in Wireless Sensor Networks. *IEEE Trans. Veh. Technol.* 68 (6), 5917–5927. doi:10.1109/tvt.2019.2909505

Wu, T.-Y., Lee, Z., Obaidat, M. S., Kumari, S., Kumar, S., and Chen, C.-M. (2020). An Authenticated Key Exchange Protocol for Multi-Server Architecture in 5G Networks. *IEEE Access* 8, 28096–28108. doi:10.1109/access.2020.2969986

Xu, G., Cao, Y., Ren, Y., Li, X., and Feng, Z. (2017). Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things. *IEEE Access* 5, 21046–21056. doi:10.1109/access.2017.2734681

Yao, J., Han, Z., Sohail, M., and Wang, L. (2019). A Robust Security Architecture for SDN-Based 5G Networks. *Future Internet* 11 (4), 85. doi:10.3390/fi11040085

Yılmaz, E., and Gönen, S. (2018). Attack Detection/prevention System against Cyber Attack in Industrial Control Systems. *Comput. Secur.* 77, 94–105.

Zhang, Y.-Q., Huang, H.-F., Wang, X.-Y., and Huang, X.-H. (2021). A Secure Image Encryption Scheme Based on Genetic Mutation and MLNCML Chaotic System. *Multimed. Tools Appl.* 80 (13), 19291–19305. doi:10.1007/s11042-021-10724-3

Conflict of Interest: Author SS is employed by DigApis Information Security Technology (Jiangsu) Co., Ltd., CD is employed by Beijing DigApis Technology Co., Ltd., CY is employed by State Grid Liaoning Electric Power Co., Ltd., and TL and YL is employed by Liaoning Electric Power Co. Ltd.

The remaining author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors, and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.