Scientific Research Publishing

Journal of Computer and Communications, 2021, 9, 91-108
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Dual Detection Method for Siemens Inverter Motor Modbus RTU Attack

Yong Wang[1], Xiunan Feng[1], Yixuan Chen[1], Lin Zhou[1], Yiwen Zhu[2], Jinyuan Wu[3]

[1]ITAcademy, Shanghai University of Electric Power, Shanghai, China
[2]Shanghai Yunjian Information Technology Co., Ltd., Shanghai, China
[3]Datang Baoding Thermal Power Plant, Baoding, China
Email: 2331389330@qq.com

How to cite this paper: Wang, Y., Feng, X.N., Chen, Y.X., Zhou, L., Zhu, Y.W. and Wu, J.Y. (2021) A Dual Detection Method for Siemens Inverter Motor Modbus RTU Attack. *Journal of Computer and Communications*, **9**, 91-108.
https://doi.org/10.4236/jcc.2021.97008

Received: April 16, 2021
Accepted: July 27, 2021
Published: July 30, 2021

Abstract

Since the Modbus RTU wired communication protocol of Siemens variable frequency motors is unstable and lacks a protection mechanism, there is a risk of user information leakage. Aiming at the problems of insufficient flexibility of traditional defense methods and poor defense effects, The present work proposed a new dual detection method based on MODBUS RTU, which combines the dual monitoring mechanism of "Address Resolution Protocol (ARP) request detection" and "ARP response detection". In order to improve detection efficiency, two real-time updated linear tables are introduced, which can effectively deal with the three ARP spoofing methods of updating the ARP buffer. Based on the analysis of the hidden dangers of the Modbus RTU wired communication protocol, a wired connection between the S7-1200 PLC and the variable frequency motor was established, and a real experimental platform was constructed to demonstrate the attack. The intensity of ARP attacks has gradually increased over time. Through comparative experiments with traditional defense methods, it is proved that the algorithm enhances the protocol mechanism in principle, and is more flexible and reliable than traditional methods.

Keywords

Siemens Motor, Man-in-the-Middle (MITM) Attack, S7-1200PLC, Modbus RTU Communication Protocol

1. Introduction

As an important part of the national economy, the application of motor involves every link of modern industrial production and every aspect of daily life. While

the application of electric motors improves the quality of production and life, it is usually unavoidable to be used in harsh environments with high temperature and dust. This complex environment usually leads to locked-rotor, voltage instability and lack of equivalence problems in the motor [1]. As the main force of the industry, the electric motor has been the main driving force of the industry for decades, acting as the driving force of almost all dynamic machinery, and will still occupy such a position in the next few years [2]. With the development of digital transformation, higher requirements are put forward for motors. While ensuring the safe and stable operation of motors, they are also relying on digital power to achieve a more efficient, safer and more intelligent operation and control experience. Traditional motors can no longer meet the requirements. Motors are gradually becoming intelligent and networked to adapt to the complex and changeable working environment. Inverter motors are being combined with the development of science and technology so that in the same control system, there is no need to add other hardware devices, and only need to modify the program to achieve real-time measurement, monitoring and protection functions.

With the wide application of Siemens variable frequency motor wired communication, the security of wired communication of Siemens motor has also attracted more and more attention. In wired connection, the stable operation of intelligent digital motors and connected equipment will not only be affected by the voltage and current configuration environment [3], it is also facing the threat of information leakage caused by hacker attacks. In recent years, more and more intelligent digital motors are combined with PLC programmable controllers. Siemens S7-1200 is a small PLC with integrated PROFINET interface, superior network functions, compact design, and flexible configuration [4], the network port supports the standard TCP/IP protocol and has a powerful instruction set, which represents the future development direction of small programmable controllers [5] [6]. As its wired communication protocol is Modbus RTU protocol, there are a variety of protocol loopholes and security risks, it is difficult to ensure the integrity of the transmitted data [7], and the communication protocol itself is not stable, so it is vulnerable toman-in-the-middle (MITM) attack. This paper focuses on Address Resolution Protocol (ARP) attack, because this attack will lead to the leakage of communication information of the motor, and the attacker can do malicious damage to stolen data [8] [9].

Aiming at the above problems, this paper proposes a new dual detection method based on Modbus RTU, which combines the dual monitoring mechanism of "ARP request detection" and "ARP response detection". In order to improve detection efficiency, two real-time updated linear tables are introduced, which can effectively deal with the three ARP spoofing methods of updating the ARP buffer. It has the advantage of real-time refreshing. Demonstrate the attack by building a real experimental environment, breaking through the traditional manual speed control method, designing the control interface, realizing the start and stopping control of the Siemens variable frequency motor through the jog of

the control panel, and testing the effectiveness and reliability of the algorithm. Experimental results show that the algorithm can resist high-intensity attacks and is more flexible and reliable than traditional defense methods.

2. Related Research

At present, there has been a lot of research on the principle of ARP spoofing attacks at home and abroad, but the defense effect of ARP spoofing is not ideal. There are many traditional methods to defend against ARP spoofing, such as setting up an ARP firewall, binding the correct Internet Protocol (IP) and Media Access Contro (MAC) mapping, and automatically identifying ARP scanning and spoofing behaviors existing in the local area network according to the characteristics of network packets, which protects the security of the host to a certain extent and has the advantage of active defense, but it also means that the ARP firewall needs to continuously transmit ARP correct data packets to the outside, thereby increasing the burden on the network. The speed of active defense is limited, once it is exceeded by the attacker, it will cause the defense to fail; the use of ARP servers is also a common method. Among all hosts, one host is designated to act as the ARP server to respond to ARP requests from the remaining hosts, but this relationship is not unique. Other hosts can still accept ARP responses from other servers; Bind the port or MAC address on the switch or host, add static ARP cache entries on each host to compare the IP address and MAC address of the data packet, and compare according to the principle of the same data packet can also mitigate ARP attacks; With the limitation that ARP spoofing cannot be attacked across network segments, the network is divided into multiple network segments to narrow the scope. The advantage is that it can narrow the attack scope of ARP spoofing, but the disadvantage is that it is not flexible enough to avoid attacks on the gateway.

It can be seen that although traditional prevention means have advantages, they also have disadvantages. Only relying on one method cannot achieve the ideal ARP defense effect. It is necessary to combine several methods according to the actual needs and play their respective roles, but this will also cause the burden of technical personnel and the waste of resources. Literature [10] proposed an attack detection method based on ARP cache timeout. A single machine can achieve ARP detection, but it is not flexible. Thomas Girdler *et al.* [10] used software-defined network (SDN) for defense detection, Khalid *et al.* [11] used data from Dynamic Host Configuration Protocol (DHCP) server for detection, Jacob H *et al.* [12] used hash processing on the physical address of the host to reject ARP spoof in real time. Alharbi *et al.* used centralized network control to "clean up" fraudulent ARP requests with dummy values. The widely popular research on SDN protection ARP attack focuses on the separation of control interface and data interface, but the problem of limited experimental sampling points is difficult to be solved perfectly. Therefore, there is an urgent need for an efficient and reliable defense method to resist ARP attacks.

3. Problem Analysis

3.1. Analysis of Modbus RTU Wired Communication Protocol

Modbus RTU protocol belongs to a category of Modbus communication protocol, which provides an effective way for communication between Siemens S7-1200 PLC and intelligent digital motor. The Modbus RTU protocol was developed in 1979 and is widely used in various wired communication modes. Its communication follows the following steps:

1) The client prepares the request and sends it to the server.

2) The server will analyzes and processes the client request, and then sends the result to the client.

3) Once an error occurs, the server will immediately return the abnormal function code.

Modbus RTU communication protocol follows the master-slave mode for data transmission. To realize data transmission, the slave station needs to receive a request from the master station, otherwise it is not allowed to send. In the master-slave mode, the master station can only send one message request to the slave station at a time. After the master station sends a message request, the slave station prepares to respond. First, the slave station checks and analyzes the received message, then starts to execute the message, and finally sends the response message to the waiting master station to complete the task. The master station needs to check and confirm the message sent by the slave station. If no error is detected, the message data will be processed. If the message is found to be wrong, it needs to repeat the above steps to resend the message request until the check is correct. The slave station of Modbus RTU serial communication bus may not be unique, and the slave station has the address range, while the number of master station is only one, and there is no station address. The data exchange between the master station and the slave station depends on the selection of function codes. Different data areas correspond to different function codes. The operation of function codes can be divided into status bit operations and 16-bit register operations. The correspondence between function codes and data areas, as well as user-level addresses (decimal) is shown in Table 1.

The function code is generally used in Siemens PLC programming. In other cases, it is not necessary to use the function code, but only the user-level address. The meaning of the user-level address is introduced below: the user-level address 00001 corresponds to the function code FC01/FC05/FC15, which represents a number Output address 1; user-level address 10001 corresponds to function

Table 1. User-level address representation and access authority in data area.

function code	Data area	User-level address	access permission
01, 05, 15	Output status bit	0xxxx	Read, write
02	Input status bit	1xxxx	Read only
04	16-bit input register	3xxxx	Read only
03, 06, 16	16-bit output register	4xxxx	Read, write

code FC02, which means "digital input address 1"; user-level address 30012 corresponds to function code FC04; user-level address 40012 corresponds to function code FC03/FC06/FC16; but the former means 16 bits The integer input address of 12, the latter represents the 16-bit integer output address 12. The request message sent to the master station is composed of multiple structures. At the same time, Modbus RTU provides users with formats such as parity.

Modbus RTU serial port communication technology can adapt to the transmission of data between different systems, support for almost all of the automation system, have very strong reliability and practicability, can be transmitted over a long distance, communication is open, transparent, and the cost is not high, so has been widely applied in the field and automation control.

3.2. Existing Security Risks

1) Because devices in the same network segment need to turn off the firewall, there is a lack of an important security line.

2) The safe operation of Siemens inverters requires a stable voltage and current configuration environment. It is very susceptible to electromagnetic interference, and the stability of the Modbus protocol is insufficient [13]. Therefore, it will bring a lot of security risks.

3) As smart digital motors are connected to the network, more and more devices use Modbus ports to query PLC/RTU units through the Web. But even with some encryption actions, the commands sent by these interfaces are often attacked [14]. Directed side-channel attacks on encrypted data packets may still cause information leakage through the encrypted TCP/IP function of the Modbus RTU protocol [15]. Due to the small number of potential Modbus commands, the size of the data packet causes the difference in traffic size. This affects some encrypted web interfaces to varying degrees. Therefore, it is necessary to set up encrypted web traffic [16].

4) Modbus RTU is one of the most widely used industrial communication protocols. But it has limitations in modern automation and control systems [17], including low transmission rate, the limited number of networked devices, single main topology and lack of main network. The integrity of data transmitted between Modbus RTU devices needs to be improved.

3.3. The Principle of Man-in-the-Middle Attack

MITM attack, as a common attack means in wireless network, the attacker only needs to have the same service set identifier (SSID) as the legal AP, and make use of the characteristics of SSID constantly transmitting to attack. The attacker can intercept the data information between the attacked and the legitimate AP, act as a middleman, and forward or monitor the legitimate data and traffic. The MITM attack model under the wireless local area network is shown in **Figure 1**.

MITM attacks can be used for information tampering as well as information theft. The so-called information tampering is to modify or delete the original

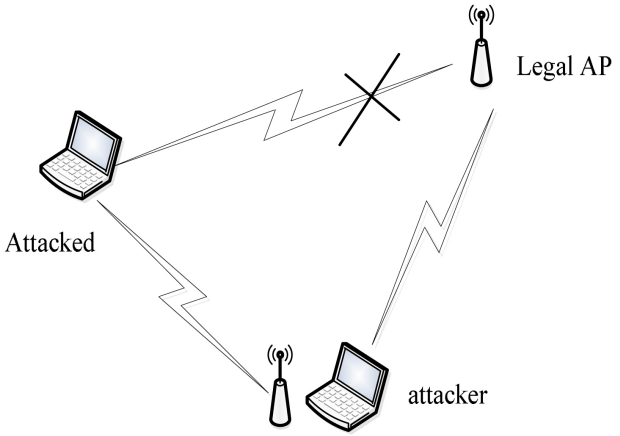


Figure 1. MITM Attack model.

authentic communication information, and the previous information recipients will receive these false data. ARP spoofing is also known as ARP poisoning [18] [19] [20], mainly due to the fact that when one end sends a reply message and the other end receives such ARP reply, the packet data is included in the ARP cache list without checking whether the data is true or correct, which gives the attacker an opportunity to take advantage of it. For example, computer A originally planned to send a message request to computer B, but due to the appearance of forged messages, computer A cannot successfully send the message request to computer B, or send it to computer C, resulting in an error in the data transmission object, causing ARP spoofing.

ARP protocol can improve the efficiency of network operation. The premise of this advantage is that each host in the network trusts each other. However, ARP protocol has no authentication mechanism [21] [22], which can neither judge whether ARP request has been sent nor verify the identity information of the respondent. It can be seen that this "statelessness" is reflected in that any host has the ability to forge response packets, and it can respond even if it does not receive ARP request. The local cache of ARP continues to update with the sending of forged packets, which undoubtedly gives a chance to network viruses and hackers. Due to the lack of authentication mechanism, the data cannot be authenticated, so the host will update the ARP cache unconditionally as soon as a valid packet protocol is received. The lack of this authentication mechanism makes it easy for an attacker to create fake ARP packets to refresh the host's ARP cache. At the beginning of spoofing, the attacker has already obtained the IP addresses of both communication parties, and this kind of address spoofing transmits the forged IP address and MAC address mapping to the attacker. The attacker then sends ARP packets to the MAC addresses of one of the hosts, and then performs ARP response grouping. In this case, the source address of host 1 is the IP address of host 1, and the MAC address of host 3 is generated from the source MAC address. The ARP spoofing topology is shown **Figure 2**.

The computer under ARP attack will disturb the order of the internal wireless

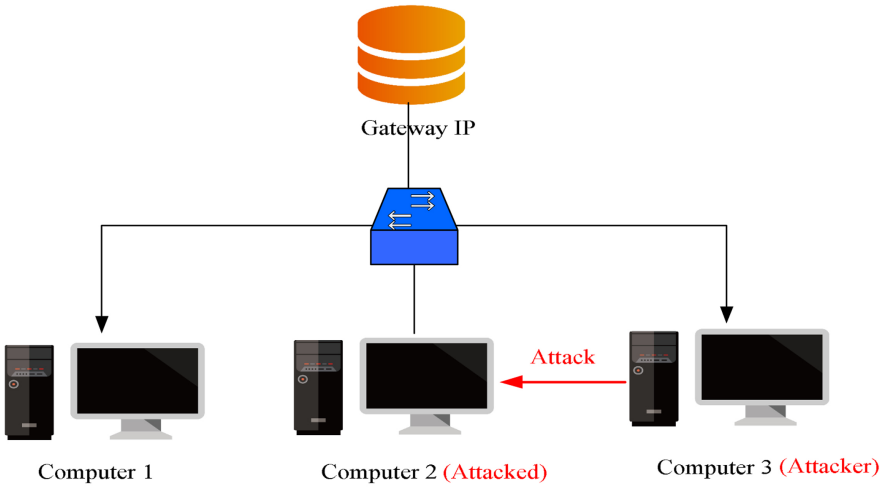


Figure 2. ARP (Address Resolution Protocol) spoofing topology diagram.

network and continuously send large quantities of ARP spoofed data packets to the wireless local area network. At this time, the host under attack cannot access the internal and external network, thus blocking the data transmission between the client and the gateway. If the ARP man-in-the-middle attack is successful, the user's private data and sensitive information will be completely exposed to the attacker.

In the process of ARP spoofing attacks, if attackers forge an ARP message, tell the target host IP routing with another MAC address binding, will not find A router, the target host cannot provide Internet services, namely the attacker A tell victims B router address, and the victims B has no doubt on the accuracy of the news, At this point, Victim B will look for the router address he was told each time, but in fact, the router address is not located here, so Victim B cannot find the router, which is the MAC address. If the MAC address is a forged address, the address will never be found. A more serious situation is that the MAC address points to another host, which simulates the router to act as the middleman for information forwarding, so all the information of the user will be exposed to the attacker. If the information is modified and fed back at this time, there will be more serious consequences.

In the wired communication process of Siemens Motor, once an ARP attack is encountered, the ARP cache list will be changed, and the MAC address corresponding to the host IP will be changed from the actual physical address before the attack to the attacker's MAC address. Attackers can maliciously tamper with the ARP cache of the target host in the following three ways:

1) After the target host receives the attacker's ARP request, it finds that the target IP of the request is itself. For example, the attacker's attacker IP is 192.168.0.88, and the source MAC address is 00-0C-29-33-AD-7C, but the attacker's request for a fake message sent by the target host shows that the target IP is 192.168.0.88, and the source MAC address is 0C-4B-54-17-0C-8C. The ARP buffer is updated, resulting in a successful ARP spoofing.

2) When the target host does not send an ARP request message to the attacker, the attacker forges a fake ARP message and sends it to the target host. At this time, the source IP is 192.168.1.1 and the source MAC address is 00-0C-29. -33-AD-7C, the target IP is 192.168.0.88, and the target MAC is 0C-4B-54-17-0C-8C. At this time, the host receives the fake ARP packet and then maps it according to the fake IP-MAC the relationship updates the ARP table, resulting in a successful ARP spoofing.

3) The target host broadcasts an ARP request message and sends a request to the MAC address of the inverter. At this time, the IP of the inverter is 192.168.1.1. After the inverter sends the correct ARP response message, the attacker then sends a false At this time, the source IP is 192.168.1.1, the source MAC address is 00-0C-29-33-AD-7C, the destination IP is 192.168.0.88, and the destination MAC is 0C-4B-54-17-0C-8C, This attack method in which the attacker sends a false message after the broadcast can also achieve ARP spoofing, thereby updating the ARP cache of the target host.

4. Address Resolution Protocol Spoofing "Dual Detection" Defense Algorithm

According to the analysis of ARP spoofing, the target host can update the ARP buffer whether it receives the ARP request message first or delays receiving the ARP reply message sent by the attacker. Therefore, a new algorithm is proposed, which can provide a dual detection mechanism of "ARP request detection" and "ARP reply detection". It can simultaneously solve the three ways of ARP deception, so as to achieve the purpose of defense. The ARP request detection part of the algorithm is shown in **Figure 3**, if the request message received by the target host shows that the target of the request is itself, it can reject the update and send an ARP request message to the source host at the same time. When the target host receives the ARP request message before the attacker, it judges the response message while receiving the ARP response of the target IP. If the received response message is sent by the target host for the first time, the buffer is updated. Otherwise, the received response packets will be compared with it, and those response packets sent to the host without ARP request will be deleted.

The ARP response detection part is shown in **Figure 4**.

In order to improve detection efficiency, the Request table and the Respond table are introduced for real-time dynamic update. Parse the source IP in the ARP response packet and store it in the Request request table, add the IP-MAC mapping to the Respond table. If the message has not been updated for a long time in the linear table, it can be automatically filtered and deleted, thus achieving the purpose of improving the detection efficiency.

5. PLC S7-1200 Control Siemens Motor Attack Demonstration

In this section, through the interconnection of Kingview, ForceControl, and TIA

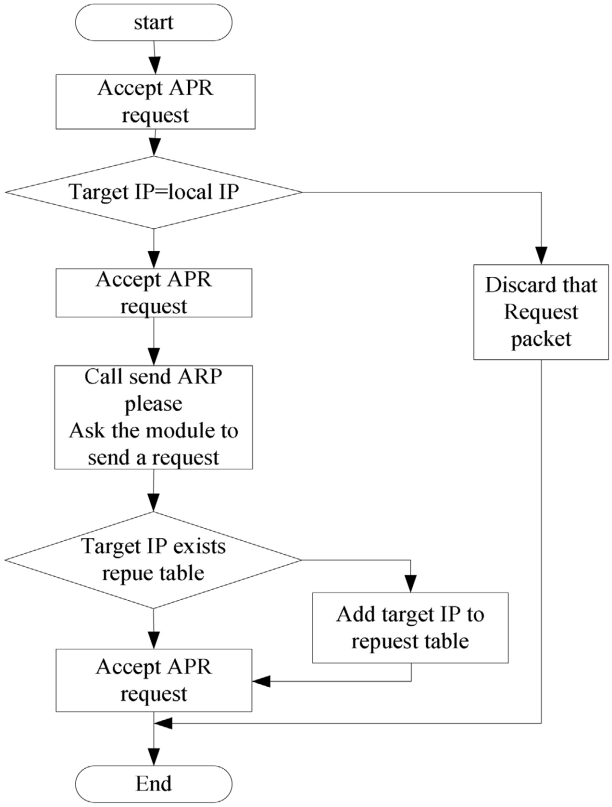


Figure 3. ARP (Address Resolution Protocol) request detection module.

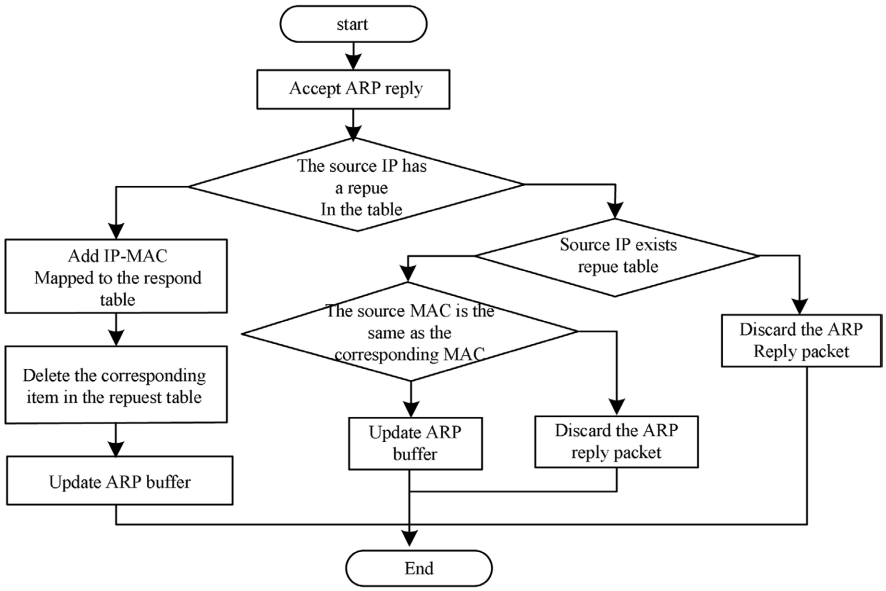


Figure 4. Flowchart of ARP (Address Resolution Protocol) reply packet detection algorithm.

PORTAL, the PLC S7-1200 and Siemens inverters are wiredly connected, and the MITM attack demonstration is carried out in a real experimental environment.

5.1. Experiment Procedure

In order to realize the control of Siemens variable frequency motor to S7-1200 PLC, it is necessary to connect RS485 port. ForceControl establishes a connection with Kingview through the OLE for Process Control (OPC) port, and establishes a connection with TIA Portal through TCP/IP Ethernet. Kingview and TIA Portal are interconnected through a data dictionary. Finally, the interconnection of the three will be realized. The relationship topology diagram of the three is shown in Figure 5.

Kingview can be used to design the interface to simulate the real environment. By clicking the button, the forward rotation, reverse and stop of Siemens inverter motor can be easily controlled. Similarly, ForceControl is used to design the panel, in which the red circle represents the indicator light. When the enabling value is set to 1, the motor is started to control, and the operation is more simple and intuitive. Users can input the corresponding decimal number in the text box to control the device operation. In the monitor table of TIA Portal, hexadecimal numbers are needed for operation, but in Kingview and ForceControl, the control parameter input needs to be converted to the corresponding decimal number to achieve the desired effect, as shown in Figure 6 and Figure 7.

In order to realize the attack experiment of PLC and inverter, PLC S7-1200 on TIA Portal was programmed after the physical connection between frequency converter and PLC device was completed, and the construction of hardware environment was shown in Figure 8.

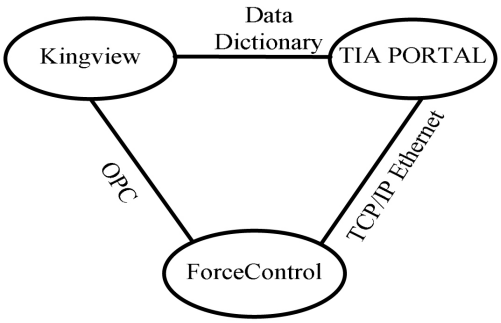


Figure 5. Interconnection graph between the three.

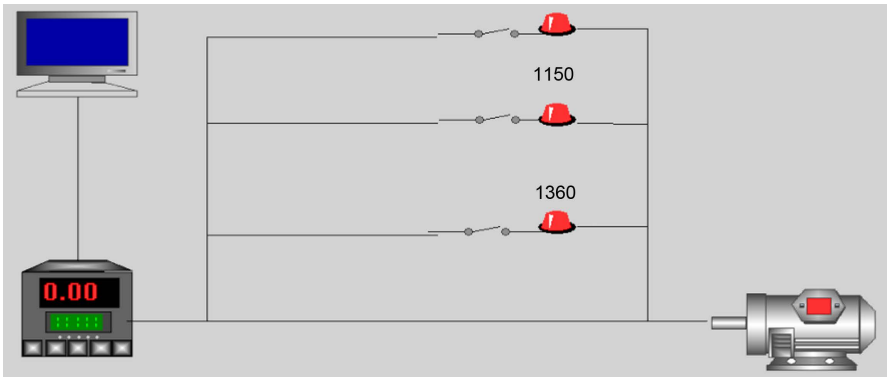


Figure 6. Control interface diagram.

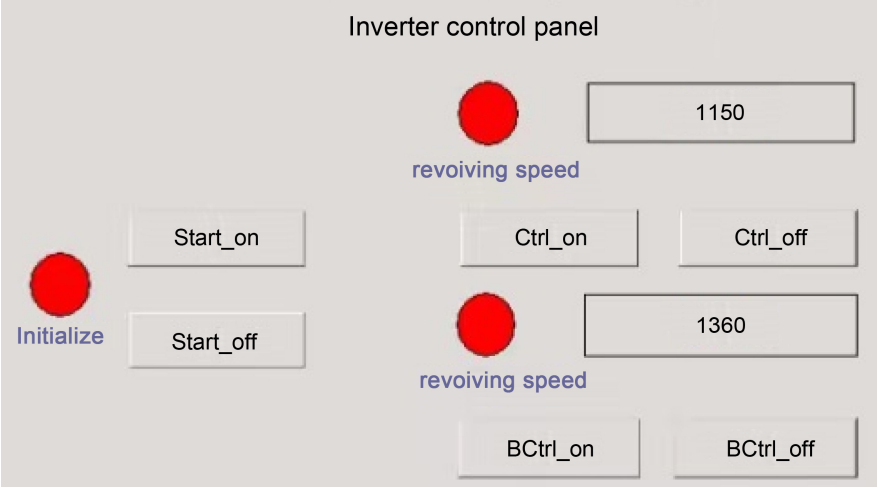


Figure 7. Force control panel design.

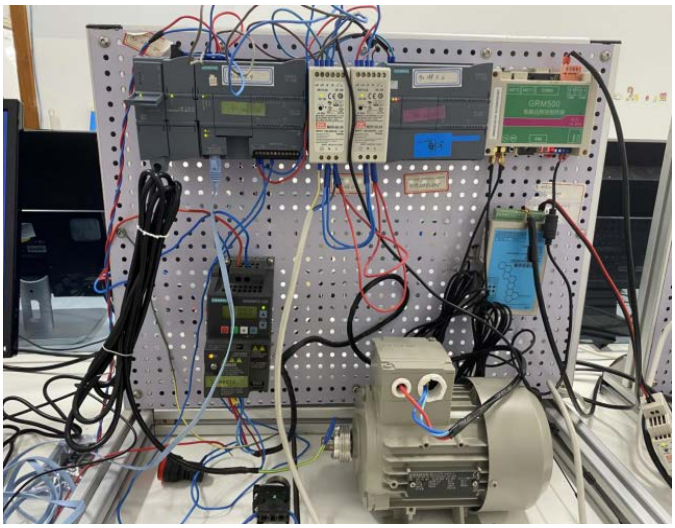


Figure 8. Construction of the hardware environment.

5.2. SYN Flood Attack

The SYN flooding attack is a malicious attack that consumes the target machine's resources and causes the target machine's memory to be insufficient, thereby denial of service. In order to realize MITM attack, SYN flood attack was carried out on the host under the premise of normal communication between the host and PLC equipment. The data packets during communication were shown in Figure 9.

In Linux, the Python language is used to construct fake data packets. At this time, in order to prevent the exposure of the identity, the attacker uses a forged IP address to carry out an anonymous attack on the host. A large number of forged IP addresses can cause serious interface freezes. In order to further enhance the effect of the SYN Flood attack, continue to forge a large number of data packets to attack the PLC device until the attacked party runs out of resources due to continuous waiting, causing the PLC device to disconnect from

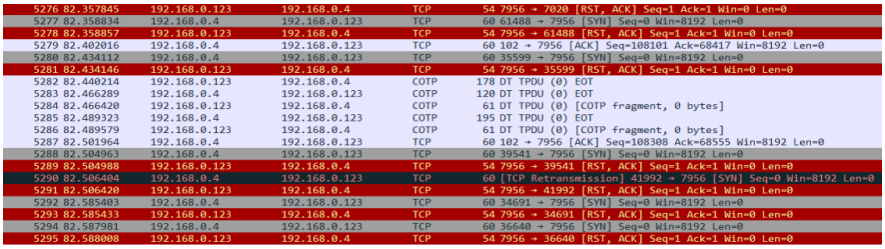


Figure 9. Packets during normal wired communication.

the TIA Portal. About 18 seconds after the attack, the human-computer interface showed that the device could not be connected, as shown in **Figure 10**. At this time, the SYN Flood attack was successful, but the motor did not stop rotating.

5.3. Address Resolution Protocol Address Spoofing Attack

ARP spoofing can enable attackers to sniff or even tamper with data packets, thereby disrupting normal communication. After the Siemens 1LA7070-4AB10-Z motor is successfully connected to the S7-1200 PLC, the indicator light on the control panel is green, indicating that the communication function is normal.

The experimental network environment is configured as follows.

Attacker IP address: 192.168.0.88;

Physical Address (MAC): 00-0c-29-33-ad-7c;

Gateway IP address: 192.168.0.1;

Physical Address (MAC): 0c-4b-54-17-0c-8c;

PLC device IP address: 192.168.1.1.

Bridging the virtual machine and the physical host and connecting the S7-1200 PLC device, the attacker and the virtual machine to the same local area network to sniff the information of the target network, thereby reducing the routing process and making the attack easier to achieve. The network topology is shown in **Figure 11**.

In order to build data packages and program design, the present work needs to install scapy library, easygui library and Tkinter library. The Python language is chosen to implement the ARP attack on the experimental environment. The changes in the ARP cache table in the target machine are shown in **Table 2**.

According to the change of ARP cache list spoofing, it can be obtained that the MAC address corresponding to the gateway IP has changed from the actual physical address before the attack to the MAC address of the attacker, thus realizing the purpose of two-way spoofing. The ARP address spoofing attack is shown in **Figure 12**.

At this time, the attacker acted as a middleman in the communication between the two parties and successfully deceived the PLC device and the target host.

6. Defense Testing and Result Analysis

In order to verify the effectiveness of the proposed algorithm, the following

Figure 10. Human-machine interface display failed to connect.

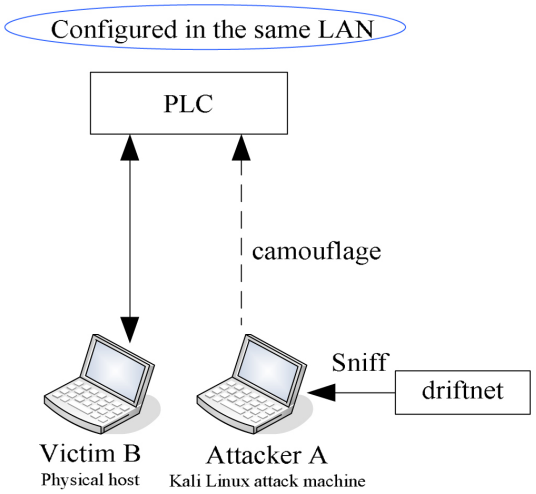


Figure 11. Network topology diagram.

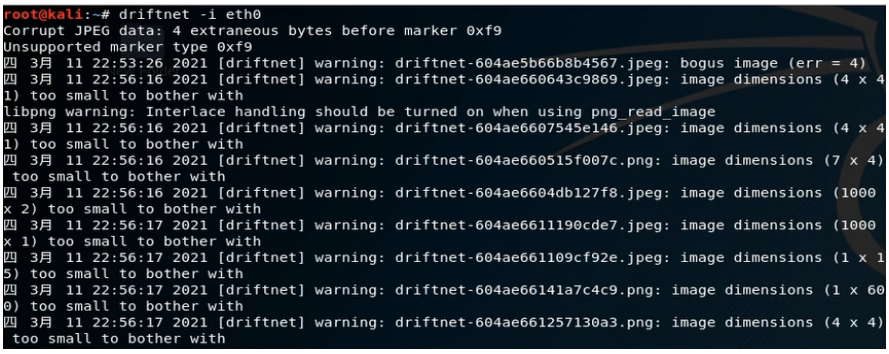


Figure 12. Attacker steals the access record of the target aircraft.

Table 2. ARP (Address Resolution Protocol) table changes before and after the attack.

Configuration item	Before attack	After attack
Attacker IP	192.168.0.88	192.168.0.88
Attacker MAC	00-0c-29-33-ad-7c	00-0c-29-33-ad-7c
Gateway IP	192.168.0.1	192.168.0.1
Gateway MAC	0c-4b-54-17-0c-8c	00-0c-29-33-ad-7c

defensive tests were carried out and compared with traditional defensive methods. The test flow chart is shown in Figure 13.

Test Steps

The environment needs to be configured before the test starts. In the ubuntu environment, configure the cross-compilation environment (arm-linux-gcc) and the basic build environment, and then test under the Ubuntu (attack machine) and Windows10 (target machine) operating systems. Use the C language to program. It should be noted that the use of the program requires access to administrator privileges, so the sudo statement must be called. In order to implement an ARP attack, it is necessary to customize the number of packets and forge a large number of packets to send to the target host to reduce the response speed of the host. At this time, the target machine mistakenly believes that the attacker is the gateway. The attacker used sniffing tools to steal user-defined parameters, which caused the information of the variable frequency motor to be completely exposed to the attacker, as shown in Figure 14.

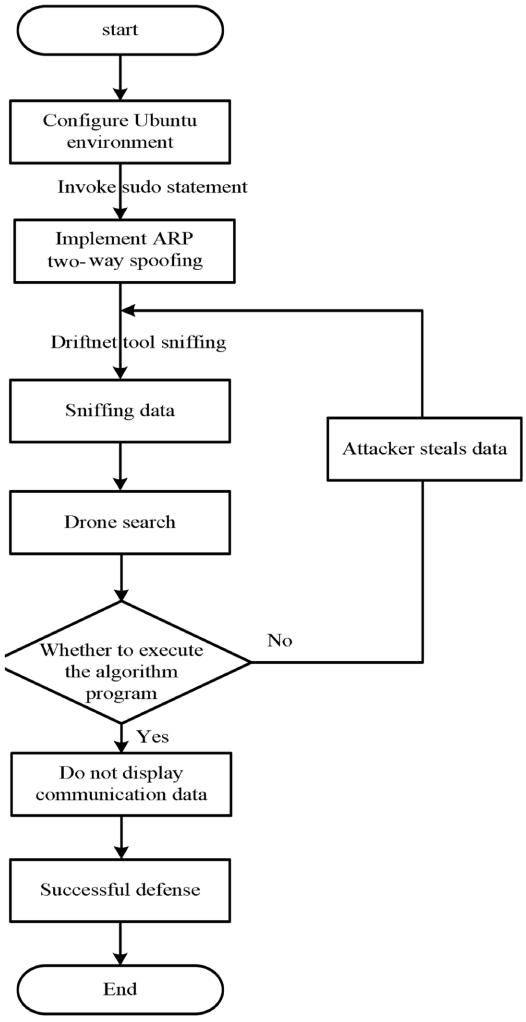


Figure 13. Defense test flowchart.

The method of firewall is adopted to defend against SYN flood attack. At the same time, binding the right IP and MAC mapping can actively defend against ARP address spoofing attack. Both traditional defense methods can establish a normal connection between the S7-1200 PLC and the Tia Portal, and restore the human-computer interaction interface to normal, as shown in Figure 15.

In order to verify the validity of the static binding, firstly, obtain the authority of administrator, and then set the IP static binding on the command prompt interface. At this time, the sniffing tool is used again and it is found that the attacker cannot sniff the information of user.

Figure 16 shows that the static binding is successful, so that ARP address spoofing is avoided.

The ARP attack custom data packet is reset to send 10 data packets per second and gradually increase. With the increase of attack intensity, the traditional static binding method fails statically, as shown in Figure 17.

Therefore, traditional defense methods cannot cope with ARP attacks that have increased over time. Maintain the strength of the attack, execute the "double detection" defense algorithm, and then use driftnetagain. At this time, the attacker cannot steal the sensitive information of the variable frequency motor. Check the ARP cache at this time and find that the ARP list is restored, as shown in Figure 18.

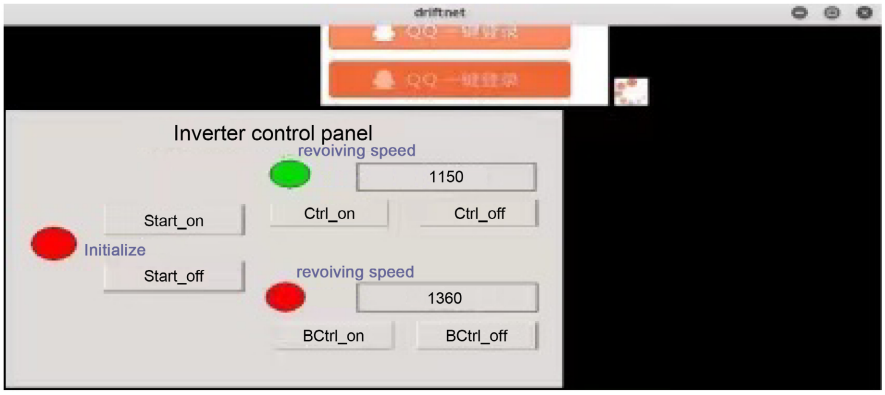


Figure 14. Attack planes steal information from frequency conversion motors.

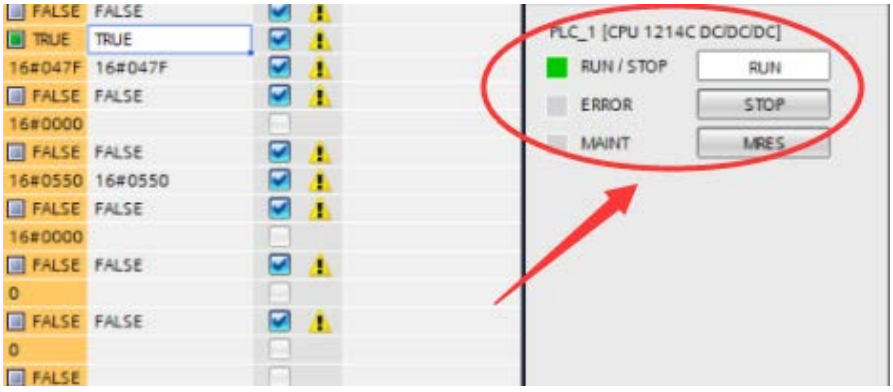
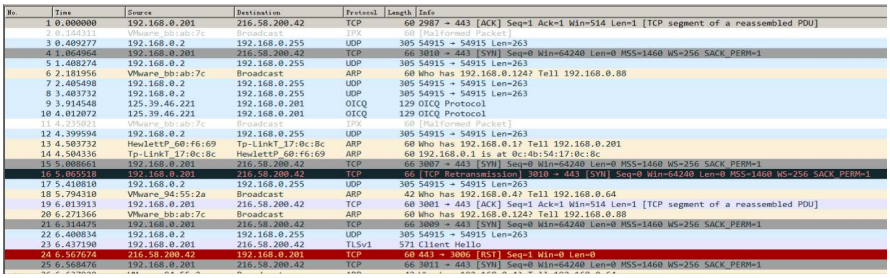


Figure 15. The human-computer interface returns to normal.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.201	216.58.200.42	TCP	60	2987 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
2	0.144311	VMware_bb:ab:7c	Broadcast	IPX	60	[Malformed Packet]
3	0.409277	192.168.0.2	192.168.0.255	UDP	305	54915 → 54915 Len=263
4	1.064964	192.168.0.201	216.58.200.42	TCP	66	3010 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	1.408274	192.168.0.2	192.168.0.255	UDP	305	54915 → 54915 Len=263
6	2.181956	VMware_bb:ab:7c	Broadcast	ARP	60	Who has 192.168.0.124? Tell 192.168.0.88
7	2.405498	192.168.0.2	192.168.0.255	UDP	305	54915 → 54915 Len=263
8	3.403732	192.168.0.2	192.168.0.255	UDP	305	54915 → 54915 Len=263
9	3.914548	125.39.46.221	192.168.0.201	OICQ	129	OICQ Protocol
10	4.012072	125.39.46.221	192.168.0.201	OICQ	129	OICQ Protocol
11	4.239674	VMware_bb:ab:7c	Broadcast	IPX	60	[Malformed Packet]
12	4.399594	192.168.0.2	192.168.0.255	UDP	305	54915 → 54915 Len=263
13	4.503732	HewlettP_60:f6:69	Tp-LinkT_17:0c:8c	ARP	60	Who has 192.168.0.1? Tell 192.168.0.201
14	4.504336	Tp-LinkT_17:0c:8c	HewlettP_60:f6:69	ARP	60	192.168.0.1 is at 0c:4b:54:17:0c:8c
15	5.000861	192.168.0.201	216.58.200.42	TCP	66	3007 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	5.065518	192.168.0.201	216.58.200.42	TCP	66	[TCP Retransmission] 3010 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	5.410810	192.168.0.2	192.168.0.255	UDP	305	54915 → 54915 Len=263
18	5.794310	VMware_94:55:2a	Broadcast	ARP	42	Who has 192.168.0.4? Tell 192.168.0.64
19	6.013913	192.168.0.201	216.58.200.42	TCP	60	3001 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
20	6.271366	VMware_bb:ab:7c	Broadcast	ARP	60	Who has 192.168.0.124? Tell 192.168.0.88
21	6.314475	192.168.0.201	216.58.200.42	TCP	66	3009 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	6.400834	192.168.0.2	192.168.0.255	UDP	305	54915 → 54915 Len=263
23	6.437190	192.168.0.201	216.58.200.42	TLSv1	571	Client Hello
24	6.567674	216.58.200.42	192.168.0.201	TCP	60	443 → 3006 [RST] Seq=1 Win=0 Len=0
25	6.568476	192.168.0.201	216.58.200.42	TCP	66	3011 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

Figure 16. ARP (Address Resolution Protocol) address spoofing is avoided.

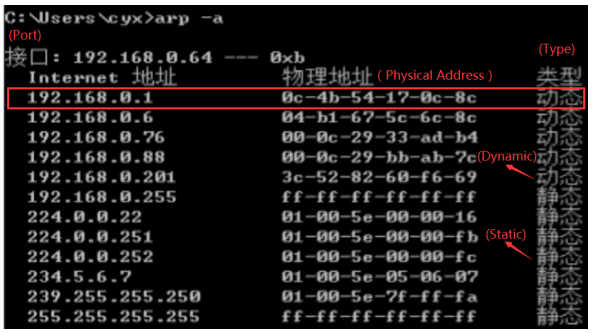


Figure 17. Static binding method fails.

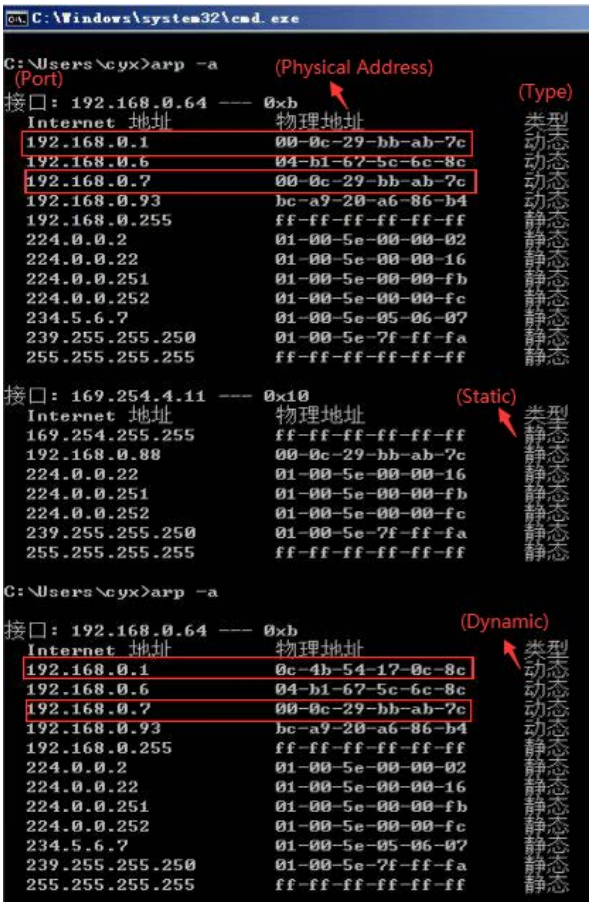


Figure 18. ARP (Address Resolution Protocol) cache list restored successfully.

The results show that the algorithm can be used to defend against ARP address spoofs, and compared with the traditional defense methods, it can deal with enhanced attacks. Even when the packet transmission frequency is from 10 packets per second and gradually increases with time, the algorithm is also effective. It can be seen that the algorithm is more adaptable and flexible.

7. Conclusion

The detection and defense of MITM attacks play an important role in the wired communication of motors. In this paper, a new defense algorithm is proposed for the security risks of the Modbus RTU wired communication protocol. According to the changes in the ARP list, three ARP spoofing methods of updating the ARP buffer can be avoided effectively. Build a real experimental platform for wired connection of variable frequency motors, design a control interface to realize the control function of Siemens variable frequency motors, and perform a variety of attack demonstrations. Through comparative experiments with traditional defense methods, it is verified that the algorithm enhances the protocol mechanism in principle. With the increase of ARP attack intensity, it shows stronger reliability and stability. This algorithm has practical reference significance for ARP defense of complex communication equipment.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Li, D.F. (2011) The Application and Advantages of Intelligent Motor Protectors in the Production of Various Industries. *Heilongjiang Science and Technology Information*, 44 p.

[2] Dol, S. and Bhinge, R. (2018) SMART Motor for Industry 4.0. 2018 *IEEMA Engineer Infinite Conference* (*eTechNxT*). New Delhi, India, 13-14 March 2018. https://doi.org/10.1109/ETECHNXT.2018.8385291

[3] Zhang, F., Kodituwakku, H.A., Hines, J.W., *et al.* (2019) Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. *IEEE Transactions on Industrial Informatics*, **15**, 4362-4369. https://doi.org/10.1109/TII.2019.2891261

[4] Li, J.J. (2018) Research on Siemens S7-1200PLC Data Storage. *Digital Technology and Application*, **36**, 6769 p.

[5] Sun, X.M. (2018) Discussion on the Application of Siemens PLC in Stepper Motor Control. *Journal of Science & Technology Economics*, **26**, 83.

[6] Zhang, G. (2018) The Design and Application of Stepping Motor Based on Siemens S7-200PLC Drive Control. *Modern Industrial Economy and Information Technology*, **8**, 38-39.

[7] Wang, L. and Scrinivasan, B. (2010) Analysis and Improvements over DoS Attacks Against IEEE 802.11i Standard. 2010 *Second International Conference on Networks Security, Wireless Communications and Trusted Computing* (*NSWCTC*), Wuhan,

Chian, 24-25 April 2010, 109-113. https://doi.org/10.1109/NSWCTC.2010.251

[8] Liu, C. and Yu, J. Rogue access point based DoS attacks against 802.11 WLANs. *Fourth Advanced International Conference on Telecommunications*, Athens, Greece, 8-13 June 2008, 271–276. https://doi.org/10.1109/AICT.2008.54

[9] Housley, R. and Arbaugh, W. (2003) Security Problems in 802.11-Based Networks. *Communications of the ACM*, **46**, 31-34. https://doi.org/10.1145/769800.769822

[10] Girdler, T. and Vassilakis, V.G. (2021) Implementing an Intrusion Detection and Prevention System Using Software-Defined Networking: Defending against ARP Spoofing Attacks and Blacklisted MAC Addresses. *Computers & Electrical Engineering*, **90**, Article No. 106990.

[11] Khalid, H.Y.I., Ismael, P.M. and Al-Khalil, A.B. (2019) Efficient Mechanism for Securing Software Defined Network Against ARP Spoofing Attack. *Journal of Duhok University*, **22**, 124-131. https://doi.org/10.26682/sjuod.2019.22.1.14

[12] Cox, J.H., Clark, R.J. and Owen, H.L. (2016) Leveraging SDN for ARP Security. *SoutheastCon* 2016, Norfolk, VA, USA, 30 March-3 April 2016, 1-8. https://doi.org/10.1109/SECON.2016.7506644

[13] Parian, C., Guldimann, T. and Bhatia, S. (2020) Fooling the Master: Exploiting Weaknesses in the Modbus Protocol. *Procedia Computer Science*, **171**, 2453-2458. https://doi.org/10.1016/j.procs.2020.04.265

[14] Jie, Y.H. (2016) Design of Embedded Industrial Robot Based on PLC Servo Control. *Proceedings of the* 2016 5*th International Conference on Environment, Materials, Chemistry and Power Electronics*, Atlantis Press, Netherlands, 11-15. https://doi.org/10.2991/emcpe-16.2016.3

[15] Liu, J., Guo, W., Huang, F. and Xiao, B.l. (2007) An Adaptive RTS Threshold Adjustment Algorithm in Wireless Local Area Network. *Chinese Journal of Computers*, **30**, 547-554.

[16] Alcaraz, C., Bernieri, G., Pascucci, F., *et al.* (2019) Covert Channels-Based Stealth Attacks in Industry 4.0. *IEEE Systems Journal*, **13**, 3980-3988. https://doi.org/10.1109/JSYST.2019.2912308

[17] Feng, L.P. and Liu, X.N. (2005) DoS Attack Based on IEEE802.11 Authentication Protocol. *Computer Application*, **25**, 546-547.

[18] Xia, X.J., Yu, N.H. and Liu, Y. (2005) Research on Denial of Service Attacks in WLAN Environment. *Computer Engineering and Applications*, **41**, 129-132.

[19] Hu, Z.M. (2020) Research on Man-In-The-Middle Attack and Defense Technology Based on ARP Spoofing. *Information Technology and Informatization*, **12**, 111-114.

[20] Shen, L.H. (2014) Application of Modbus RTU Serial Communication in Industrial Automation System. *Chemical Industry Automation and Instrumentation*, **41**, 207-211.

[21] Qin, F.L., Duan, H.X. and Guo, R.T. (2009) Overview of ARP Spoofing Monitoring and Prevention Technology. *Computer Application Research*, **26**, 30-33.

[22] Zhao, J. and Chen, K.F. (2006) Analysis of ARP Protocol Security Vulnerability and Its Defense Methods. Information Security and Communication Confidentiality, **8**, 72-74+77.