Scientific Research Publishing

Journal of Computer and Communications, 2020, 8, 88-101
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A W-EAP Algorithm for IEC 61850 Protocol against DoS/Replay Attack

Minmin Xie[1], Yong Wang[1*], Chunming Zou[2], Yingjie Tian[3], Naiwang Guo[3]

[1]College of Computer Science and Technology, Shanghai University of Electric Power, Shanghai, China
[2]The Third Research Institute of Ministry of Public Security, National Quality Supervision and Testing Center of Security Products for Network and Information Systems, Shanghai, China
[3]State Grid Shanghai Municipal Electric Power Company, Shanghai Electric Power Research Institute, Shanghai, China
Email: *wy616@126.com

How to cite this paper: Xie, M.M., Wang, Y., Zou, C.M., Tian, Y.J. and Guo, N.W. (2020) A W-EAP Algorithm for IEC 61850 Protocol against DoS/Replay Attack. *Journal of Computer and Communications*, **8**, 88-101.
https://doi.org/10.4236/jcc.2020.811007

Received: October 23, 2020
Accepted: November 21, 2020
Published: November 24, 2020

Abstract

Substation automation system uses IEC 61850 protocol for the data transmission between different equipment manufacturers. However, the IEC 61850 protocol lacks an authentication security mechanism, which will make the communication face four threats: eavesdropping, interception, forgery, and alteration. In order to verify the IEC 61850 protocol communication problems, we used the simulation software to build the main operating equipment in the IEC 61850 network environment of the communication system. We verified IEC 61850 transmission protocol security defects, under DoS attack and Reply attack. In order to enhance security agreement, an improved algorithm was proposed based on identity authentication (W-EAP, Whitelist Based ECC & AES Protocol). Experimental results showed that the method can enhance the ability to resist attacks.

Keywords

IEC 61850, DoS Attack, Replay Attack, W-EAP, Identity Authentication

1. Introduction

IEC 61850 is an international standard for power systems. It is a communication standard for substations based on Ethernet. This standard defined the services, tasks and functions of all devices in power system automation and can be mapped to many traditional protocols [1] [2]. Many devices in the substation system are connected by a communication network, which leads to higher efficiency while making the traditional closed power components and communication protocols more vulnerable to network attacks. Various attacks against

Ethernet can affect the IEC 61850 communication security.

The IEC 61850 protocol pays more attention to functions and commands at the beginning of the design. Research on information identity authentication, message integrity and confidentiality do not pay much attention, so the realization of the IEC 61850 communication protocol with identity authentication and message encryption functions is of great significance to enhancing the IEC 61850 communication security.

Based on the analysis of the frequent network attacks against the substation system in the past few years, IEC 61850 messages are easily intercepted, interrupted, tampered and forged. Attackers can use DoS attack and replay attacks to seriously affect the IEC 61850 communication process. In order to improve the security of the IEC 61850 protocol, the main difficulties are as follows: 1) The existing security measures cannot be applied to the running industrial equipment; 2) The mainstream security measure is to use message encryption, but it lacks integrity check and the authentication mechanism. It is difficult to ensure that the message is not tampered with during transmission; 3) Compared with the traditional password authentication, the authentication protocol based on the principle of cryptography is more secure. However, the authentication cannot prevent replay attacks.

To solve the above problems, the current protective measures are mainly divided into the following tasks [3]: according to the characteristics of the IEC 61850 protocol, the early warning function of abnormal behavior can be adopted [4] [5] [6]; increasing message encryption, integrity verification and identity authentication in the protocol application stage [7] [8]; adopting industrial firewall and intrusion detection technology [9] [10].

In the field of IEC 61850 anomaly detection, Zhang Yue designed an online communication detection system for smart substations by analyzing the structural characteristics of the three communication protocols of the IEC 61850 protocol [4]. By analyzing the message, judging the message type, and reporting abnormalities. This paper designs parameters such as hazard level, abnormal code and abnormal name. These parameters can be used as a means of triggering an alarm to realize safety detection and early warning. By studying the problems of the IEC 61850 protocol and related secondary equipment, Jing Ke and others built an intelligent substation detection and early warning system including network data acquisition layer, data analysis process layer and monitoring management layer. Through the implementation of full flow monitoring, Discover known and unknown malicious code activities, and conduct early warning responses [5]. Hou Lianquan and others proposed a network attack detection strategy for the secure transmission of sampled measured values (SMV), and designed 9 abnormal indicators, which can detect abnormal intrusions online, determine the attack form and possible attack location [6].

In the field of message encryption, integrity verification and identity authentication, Yang Yang *et al.* [7], by studying the requirements of IEC 61850 for real-time transmission in substations, proposed a method of implementing identity authentication with extended secure messages. This method used secure hash algorithms and the DES encryption algorithm which can realize the secure exchange of messages, and the simulation results showed that it can effectively meet the integrity requirements of communication messages. Shaik Mullapathi Farooq and others developed an S-GoSV software framework [8], the framework can generate custom GOOSE and sample value messages. This security function can protect them from different security attacks in the substation. Yu Hao and others focused on the application-layer authentication encryption method, and proposed a hybrid encryption method for data content based on a symmetric encryption algorithm [9]. The three message structures can be unified in the form of transformation, and can effectively improve encryption efficiency and ensure the integrity, confidentiality and non-repudiation of data transmission.

In the field of industrial firewall and intrusion detection, Guo Yawen proposed a whitelist-based access control strategy to set a whitelist to prevent SYN Flood attacks from fake IP addresses, restrict unauthorized devices from illegally accessing the control system, and enhanced the security of the control system [10]. Hermes Eslava analyzed the main features of an electric power substation and cyber-attacks, and then he introduced a firewall system, which can protect the target distribution network security system [11]. Junsik Kim proposed an FPGA-based network intrusion detection system. The Shift-And algorithm can detect malicious network packets within IEC 61850 messages [12].

We can find the security problem of IEC 61850 communication and transmission is solved to a certain extent, and the encryption of the protocol is realized. However, such as Guo Yawen's far whitelist access control strategy only enhances the security of the control system by restricting unauthorized devices, this only adds a layer of authentication outside the protocol, and does not improve data security. Aiming at the current problems, this paper proposes an improved method of the IEC 61850 protocol (W-EAP, Whitelist based ECC & AES Protocol), this method based on identity authentication for the IEC 61850 communication system, which have the ability to resist DoS and replay attacks. In the computer experiment environment, one authentication encryption is completed, which enhances the ability to resist DoS and replay attacks.

The subsequent chapters of this article are arranged as follows: The second part is a detailed problem analysis of the IEC 61850 protocol. In the third part we build an environment, where the security test and analysis of the IEC 61850 protocol are carried out, and the fourth part is a detailed analysis of the proposed W-EAP algorithm. At the end of the article, we summarize the research in this article and propose further research works in the future.

2. Problem Analysis

2.1. Introducing the IEC 61850 Standard

IEC 61850 divides the substation communication system into three layers

(Figure 1): substation layer, bay layer, and process layer. The IEC 61850 standard provides three types of communication protocols to meet the three-tier structure requirements of substations [1]: MMS, GOOSE, SV. The first type: MMS peer service, which is used to protect the monitoring host for communication between bay layer and station control layer equipment. The second category: GOOSE communication service, satisfies the data transmission service between bay layer devices and between bay layer and process layer devices. The third type is SV transmission service, which completes the real-time voltage and current data sampling of equipment from the process layer to the bay layer.

2.2. IEC 61850 Data Structure Analysis

General object-oriented substation event (GOOSE) messages and sampled value (SV) messages are composed of MAC address, protocol identification (TPID), identification control information (TCI), and Ethernet message type (EtherType), Application identifier (APPID), length (Length), reserved 1 (Reserved 1), reserved 2 (Reserved 2) and application protocol data unit (APDU) and other information fields, as shown in Figure 2.

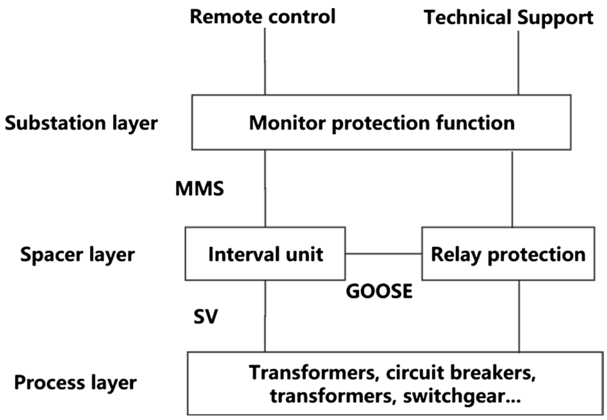


Figure 1. Substation communication system.

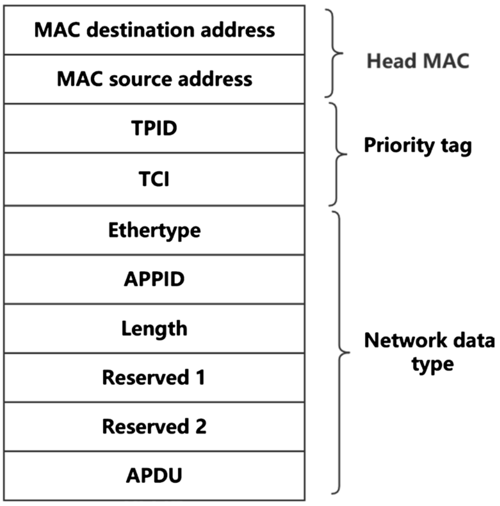


Figure 2. Structure of GOOSE and SV packet.

The important information of the substation system is mainly concentrated in the APDU field. APDU [8] is mainly composed of three main parts: type tag (Tag), length (Length) and specific content (Value), among which Tag and Length do not carry messages from the substation system information.

By analyzing the specific content of the APDU field of the GOOSE message, it is found that the allowable time to live (Times Allowed to Live), GOOSE identifier (GoID), maintenance bit (Test), configuration version number (Conf Rev) and other contents are just the basic attributes of the Goose message, which does not contain substantial information. Only the control block reference name (GoCB Reference), the data set reference name (Data Set) and the application service data unit (AllData) contains the IEC 61850 model, information path, and switch status and operation commands of the substation system. Among them, AllData is the most core information in the entire GOOSE message, and it is also the main target of the attacker.

The PDU segment of the SV message is the main body of the entire message. IEC 61850 stipulates that a PDU contains a maximum of 8 Application Service Data Units (ASDU). Each ASDU includes an SV identifier (svID) and a counter (Sample Count), version number (conf Rev), synchronization flag (smp Synch) and other message configuration information. The most important information reflects the current and voltage values are located in the Data Set fields in the second half of the ASDU. The Data Set field contains 8 electrical quantities, each of which occupies 8 bytes of space. The first 4 bytes are the specific electrical quantity value domain inst Mag.i, which is the most important data in the power system.

Manufacturing Message Specification (MMS), which is a set of data communication protocols defined by the ISO/IEC9506 protocol standard and suitable for the current industrial control environment. MMS realizes the transmission of monitoring data and real-time information between the terminal and each intelligent IED in a complex network. The MMS protocol can directly define and use the exchanged message and the characteristics of the system to express various data hierarchically, so that this feature can be used to demonstrate various complex data structures with the MMS protocol, which is more practical in the mainstream systems' transmission.

2.3. Security Issues

The power system based on IEC 61850 realizes the interconnection and communication between substation equipment through Ethernet. Although the application prospect is broad, the security loopholes of the IEC 61850 protocol and the fragility of the computer network make the network security risk issue increasingly prominent. Attackers can easily attack communication systems based on IEC-61850 by using these vulnerabilities, which will threaten the safety of the entire power system.

Security threats faced by communications on the IEC 61850 protocol network are as following:

SV and GOOSE protocols transmit messages in clear text on the Ethernet, and are sent to the network without encrypting the device commands. Therefore, the 61850 protocol faces threats to information confidentiality and data integrity, and the messages transmitted by the protocol are easy. If SV information and GOOSE information are intercepted by the attacker, the attacker can easily decode the message, modify the measured value (SV) or trip command (GOOSE) and send them. The attackers can also change the state of the circuit breaker, which may cause casualties and physical equipment damage.

The sender and receiver did not verify the message commands, so the attacker could pretend to be the sender and send false control commands to the receiver, causing the entire system to be paralyzed.

The system did not conduct legal identity verification audits of internal personnel, or early warning of internal threats. Attackers use authorized identities to borrow software, hardware, and network tools to try to prevent authorized users or machines from accessing a certain service, which has a huge impact on the IEC 61850 communication system.

3. Experimental Test and Analysis

The substation is based on the IEC 61850 standard for data transmission. The IEC 61850 protocol is based on the TCP/IP protocol, and the data is transmitted through the Ethernet. Therefore, the attacks on the Ethernet include: ARP attacks, DoS attacks, identity theft, and replay attacks. This section carries out DoS attacks and replay attacks on the IEC 61850 communication network to further affect normal communication.

3.1. Experimental Environment

The server is installed in the 61850 server software provided by Netted Automation of the Windows XP system, which simulates the parameters returned by the main operating equipment in the real environment. The client is 61850 Brow developed by Li tong corp, which is deployed in the Window 10 environment. Obtain a data message constructed based on the IEC 61850 standard, and return read and write instructions to the server according to the address in the data packet. The IEC 61850 server responds and returns the read and write results, which initially realizes the communication between the IEC 61850 server and client [2]. The experimental environment topology is shown in **Figure 3**.

Figure 4 shows the data packets captured during the IEC 61850 network communication using Wireshark.

3.2. Analysis of DoS Attack Experiment

Before the attack experiment, the Window 10 host first opened the packet capture view, and then pinged the window host on the kali end to confirm the connection.

This attack experiment uses Kali Linux, which is a Debian Linux-based distribution that contains about 600 security tools, mainly used for digital forensics, penetration testing, and hacker defense.

Enter a password on the Kali side:

root@bogon:~# hping3 -i u10 -a 1.1.1.1 -p 3389 -S 192.168.189.100

The attack result is shown in Figure 5.

It can be seen that a denial of service (DoS) attack exploits the flaws in the transmission protocol of the attacked host to create a large amount of useless data, causing the attacked host to be unable to process the request, which eventually made the attacked host stops providing services.

3.3. Experimental Analysis of Replay Attack

Replay attack means that the attacker can achieve the purpose of deceiving the

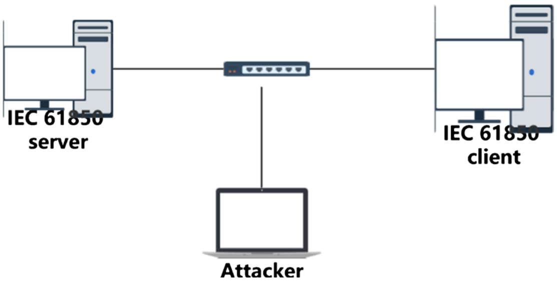
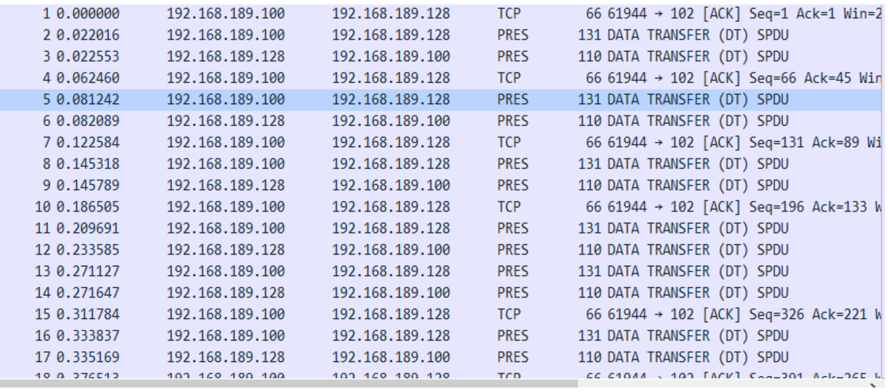
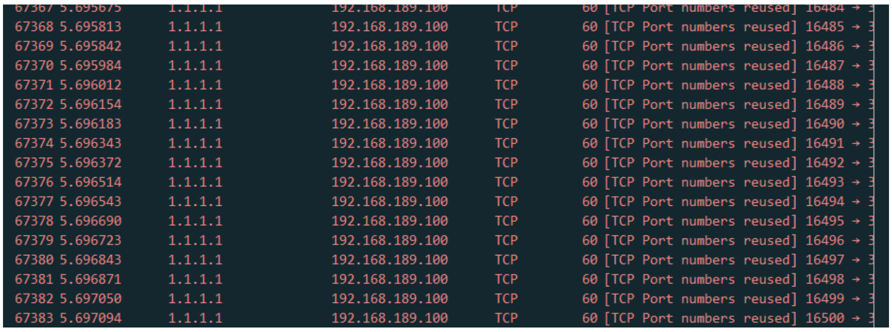


Figure 3. Topology of experimental environment.



```
 1 0.000000    192.168.189.100    192.168.189.128    TCP       66 61944 → 102 [ACK] Seq=1 Ack=1 Win=2
 2 0.022016    192.168.189.100    192.168.189.128    PRES     131 DATA TRANSFER (DT) SPDU
 3 0.022553    192.168.189.128    192.168.189.100    PRES     110 DATA TRANSFER (DT) SPDU
 4 0.062460    192.168.189.100    192.168.189.128    TCP       66 61944 → 102 [ACK] Seq=66 Ack=45 Wir
 5 0.081242    192.168.189.100    192.168.189.128    PRES     131 DATA TRANSFER (DT) SPDU
 6 0.082089    192.168.189.128    192.168.189.100    PRES     110 DATA TRANSFER (DT) SPDU
 7 0.122584    192.168.189.100    192.168.189.128    TCP       66 61944 → 102 [ACK] Seq=131 Ack=89 Wi
 8 0.145318    192.168.189.100    192.168.189.128    PRES     131 DATA TRANSFER (DT) SPDU
 9 0.145789    192.168.189.128    192.168.189.100    PRES     110 DATA TRANSFER (DT) SPDU
10 0.186505    192.168.189.100    192.168.189.128    TCP       66 61944 → 102 [ACK] Seq=196 Ack=133 W
11 0.209691    192.168.189.100    192.168.189.128    PRES     131 DATA TRANSFER (DT) SPDU
12 0.233585    192.168.189.128    192.168.189.100    PRES     110 DATA TRANSFER (DT) SPDU
13 0.271127    192.168.189.100    192.168.189.128    PRES     131 DATA TRANSFER (DT) SPDU
14 0.271647    192.168.189.128    192.168.189.100    PRES     110 DATA TRANSFER (DT) SPDU
15 0.311784    192.168.189.100    192.168.189.128    TCP       66 61944 → 102 [ACK] Seq=326 Ack=221 W
16 0.333837    192.168.189.100    192.168.189.128    PRES     131 DATA TRANSFER (DT) SPDU
17 0.335169    192.168.189.128    192.168.189.100    PRES     110 DATA TRANSFER (DT) SPDU
18 0.376513    192.168.189.100    192.168.189.128    TCP       66 61944 → 102 [ACK] Seq=391 Ack=265 W
```

Figure 4. Screenshot of IEC 61850 network communication message.



```
67367 5.695675    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16484 → 3
67368 5.695813    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16485 → 3
67369 5.695842    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16486 → 3
67370 5.695984    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16487 → 3
67371 5.696012    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16488 → 3
67372 5.696154    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16489 → 3
67373 5.696183    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16490 → 3
67374 5.696343    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16491 → 3
67375 5.696372    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16492 → 3
67376 5.696514    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16493 → 3
67377 5.696543    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16494 → 3
67378 5.696690    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16495 → 3
67379 5.696723    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16496 → 3
67380 5.696843    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16497 → 3
67381 5.696871    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16498 → 3
67382 5.697050    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16499 → 3
67383 5.697094    1.1.1.1            192.168.189.100    TCP      60 [TCP Port numbers reused] 16500 → 3
```

Figure 5. Captured message after DoS attack.

system by sending a message that the destination host has already received. The meaning is that the attacker intercepts the message A which was sent by the server to the client on the network. Then the attacker performs a replay attack on message A, and sends the message encrypted by the server to the client, making the client mistakenly believe that the intruder is the server, the client finally sends a message B to the attacker who pretends to be the server. The flowchart of the attacking is shown in Figure 6.

This attack experiment uses Burp Suite, which is a penetration test tool that can replay attacks during communication transmission.

Before using burp suite, you need to manually configure the browser, and then capture the packet, and finally click on the word to see the response data attack result on the page. The result is shown in Figure 7.

Comparing the original receipt package and the replay receipt package, it can be found that the length of the two is the same, indicating that the replay attack was successful.

4. Against DoS/Replay Attack Algorithm

4.1. Security Model

IEC 61850 protocol is used in the communication network environment, the W-EAP (Whitelist based ECC & AES Protocol) algorithm is applied to the

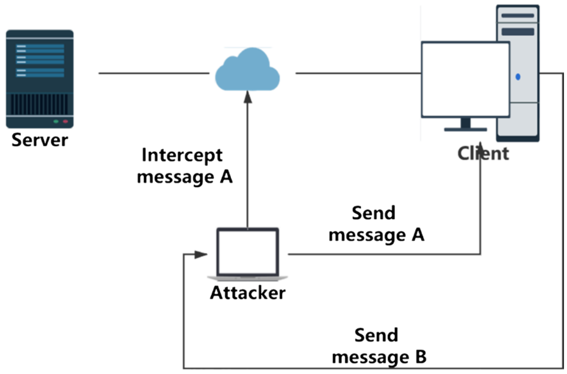
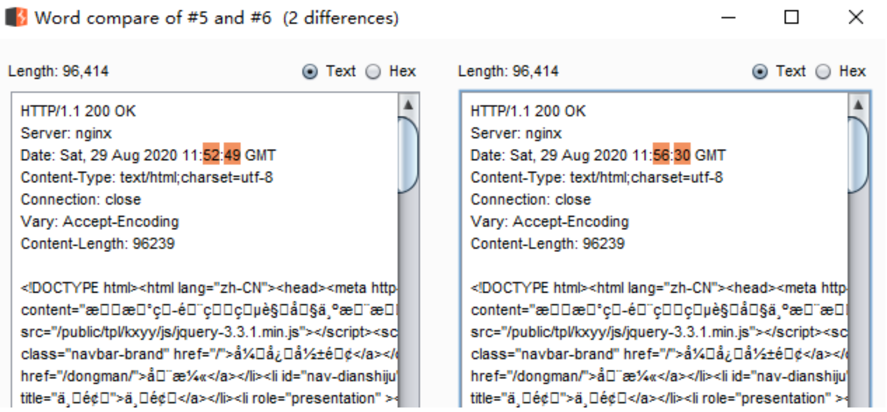


Figure 6. Replay attacks flow chart.


Word compare of #5 and #6 (2 differences)
Length: 96,414 ● Text ○ Hex
Length: 96,414 ● Text ○ Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 29 Aug 2020 11:52:49 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Vary: Accept-Encoding
Content-Length: 96239

<!DOCTYPE html><html lang="zh-CN"><head><meta http
content="æ□□æ□°ç□-é□¨ç□□ç□µè§□å□§ä¸°æ□¨æ□
src="/public/tpl/kxyy/js/jquery-3.3.1.min.js"></script><sc
class="navbar-brand" href="/">å¼□å¿□å½±é□¢</a></
href="/dongman/">å□¨æ¼«</a></li><li id="nav-dianshiju
title="ä¸□é¢□">ä¸□é¢□</a></li><li role="presentation" >
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 29 Aug 2020 11:56:30 GMT
Content-Type: text/html;charset=utf-8
Connection: close
Vary: Accept-Encoding
Content-Length: 96239

<!DOCTYPE html><html lang="zh-CN"><head><meta http
content="æ□□æ□°ç□-é□¨ç□□ç□µè§□å□§ä¸°æ□¨æ□
src="/public/tpl/kxyy/js/jquery-3.3.1.min.js"></script><sc
class="navbar-brand" href="/">å¼□å¿□å½±é□¢</a></
href="/dongman/">å□¨æ¼«</a></li><li id="nav-dianshiju
title="ä¸□é¢□">ä¸□é¢□</a></li><li role="presentation" >
```

Figure 7. Replay attack screenshots.

communication process. In the transmission process of starting communication, the access device is analyzed, and only the hosts in the whitelist are allowed to access the target server. After the host ip and port authentication is successful, the transmitted message data is encrypted and digitally signed, which can resist DoS attacks and replay attacks to improve the security and feasibility of the IEC 61850 protocol communication environment.

In the IEC 61850 communication environment, the Server and Client are connected under the same local area network to verify the devices connected to the power system network, and only devices in the whitelist can be connected to the network. In this way, a reliable and safe local area network can be constructed, and illegal devices including attackers can be blocked by configuring whitelist rules through the firewall. In order to prevent insider attacks, a layer of encryption authentication technology is added to the whitelist. In the process of transmitting IEC 61850 messages, the message data is encrypted and digitally signed to prevent the message from being tampered with and sending wrong commands, which will cause large impact on the power system. The topology is shown in Figure 8.

4.2. W-EAP Algorithm against DoS/ Replay Attacks

Since the design of the IEC 61850 protocol lacked information security considerations at the beginning, the attackers generally have clear targets and no fixed pattern of attack behavior. Therefore, the most effective protection method is to actively protect the target. In order to avoid the above attacks, the W-EAP algorithm is proposed, and two important security requirements are added to the communication: message integrity and identity verification. Only after successfully verifying the integrity and source of the message can the message be accepted at the receiver, providing a more secure and reliable environment for IEC 61850 message data transmission.

The W-EAP algorithm uses an industrial control protocol whitelist technical solution, an AES (Advanced Encryption Standard, Advanced Encryption Standard) symmetric encryption scheme, an ECC (Elliptic Curve Cryptography, elliptic

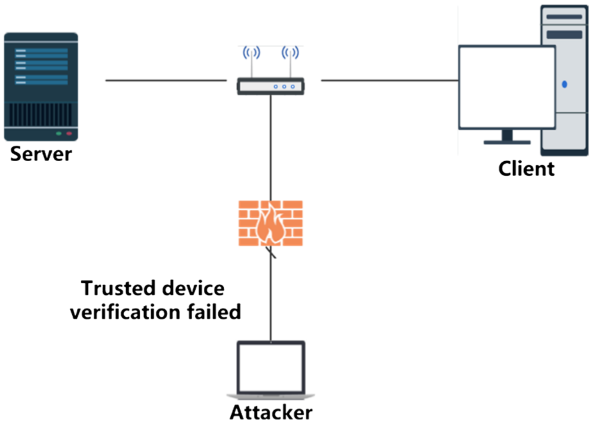


Figure 8. Secure network topology.

curve encryption) asymmetric encryption scheme and an SHA (Secure Hash Algorithm, secure hash algorithm)message authentication scheme. The industrial firewall whitelist is to manually generate the IEC 61850 protocol firewall whitelist by capturing the IEC 61850 protocol message, deep analysis of its application layer, obtaining the IP address and port. The AES symmetric encryption algorithm encrypts APDU message data, the SHA encrypted message generates a message digest, and the ECC asymmetric encryption algorithm generates a digital signature. This digital signature is unique to the sender and its message. The receiver uses the sender's public key to verify this digital signature. In the case of success, we have the guarantee of the sender and the integrity of the message. Specific steps are as follows:

Trusted authentication:

1) Enable the IEC 61850 protocol firewall whitelist to verify trusted devices.

Sender (flow chart shown in Figure 9):

1) Grab the message, read the IEC 61850 APDU module, use AES to encrypt the APDU module, get the ciphertext block and encryption key;

2) Perform ECC encryption processing on the key to obtain the AES key block;

3) Use SHA algorithm to encrypt IEC 61850 APDU module to generate digest, and use ECC to encrypt to generate signature block;

4) Transmit the cipher text block, AES key block, and signature block to the receiving end through the IEC 61850 network transmission.

Receiver (flow chart shown in Figure 10):

1) The receiving end extracts the ciphertext block, AES key block, and signature block from the message sent by the receiving end;

2) Use the ECC decryption algorithm to get the key;

3) Use the key to decrypt the ciphertext to obtain the original message data, and use the SHA algorithm to encrypt and generate digest A;

4) Decrypt the signature block to get digest B;

5) If Digest A = Digest B, the message has not been tampered with and the

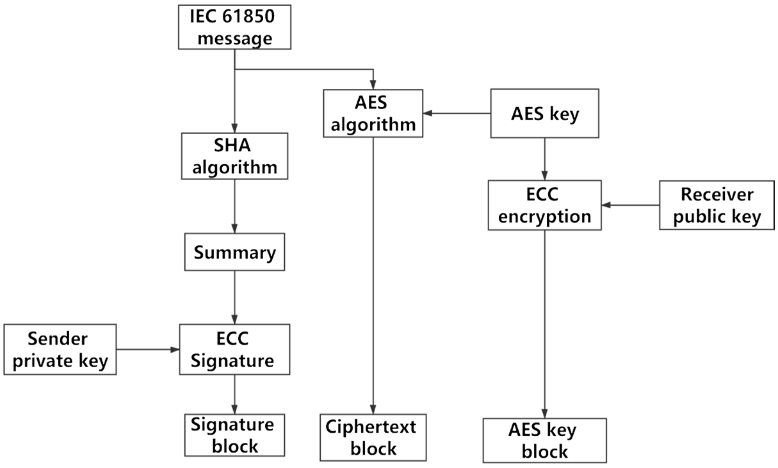


Figure 9. Flow chart of W-EAP at sender.

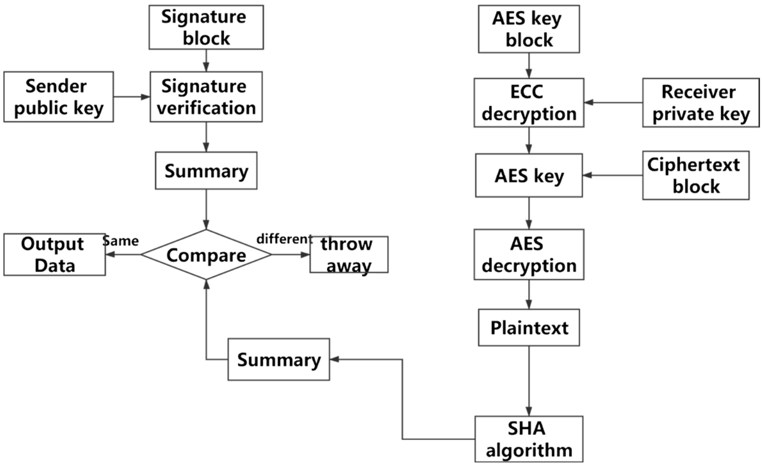


Figure 10. Flow chart of W-EAP at receiver.

communication is normal; otherwise, the message verification fails and the message is discarded.

When step 1 of the firewall verifies the trusted device, subsequent communications will not continue; the summary of step 5 of the receiving end is incorrectly compared, and the packet is discarded.

The W-EAP algorithm adopts two technical solutions to resist the above-mentioned experimental attacks:

First, establish a whitelist of agreements. Only the terminal can verify the trusted device. When the attacking computer is connected to the switch, the switch will require the attacking computer to perform identity verification. If the attacking computer does not have a legal identity, it cannot pass the verification and cannot access the IEC 61850 communication network;

Second, the adoption of multiple encryption verification techniques makes it difficult for an attacker to obtain the key and tamper with the message. Even if the attacker obtains the public key and ciphertext in network communication, the key is generated and stored by the data receiver; even if it is stolen illegally, the ciphertext cannot be decrypted because of the localized storage of the key, which makes the security of the plaintext.

4.3. Comparison Algorithm

Choosing an efficient encryption algorithm is the key to improving message confidentiality. Combining the encryption and authentication features of the W-EAP algorithm in further experiments, the same message is used as the encrypted data. In this article we use AES, DES, and classic encryption algorithms to compare with W-EAP to verify the ability of the algorithm to resist attacks..

Table 1 shows the security comparison before and after the W-EAP algorithm is added to the IEC 61850 protocol.

4.4. Experimental Analysis

Only when the client side verifies the authenticity of the access device, can the

IEC 61850 protocol communication be carried out. If the attacker's IP is not in the whitelist, the communication connection will be terminated, making it impossible to conduct network attacks. When an external attacker tries to access the IEC 61850 communication network, the whitelist verification result is shown in Figure 11.

If it is not an external attacker, or an external attacker has passed the whitelist verification, the algorithm verification result is shown in Figure 12.

Since the attacker cannot obtain the local private key, and therefore cannot pass the digest comparison authentication, it is also impossible to tamper with the message data and send wrong instructions to the substation equipment to attack.

5. Conclusions

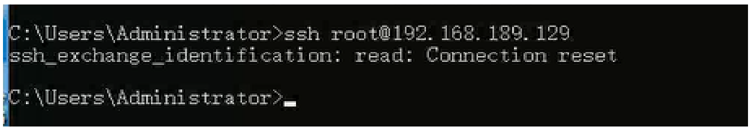
This paper conducts deep-research on DoS attacks and replay attacks of the IEC 61850 protocol and its defense methods. It is found that multiple encryption algorithms and whitelist mechanisms can be combined, and a whitelist algorithm for the IEC 61850 protocol based on hybrid encryption authentication W-EAP algorithm. The algorithm made not only the theoretical analysis but also the experimental simulation verification on effectively resist DoS and replay attacks. Although the W-EAP algorithm improves the security of the IEC 61850 protocol to a certain extent, it still has limitations, which are mainly reflected in the following:

1) The program relies on the Python environment, which is difficult to deploy in the IEC 61850 network.

2) The W-EAP algorithm only conducted experimental tests on encryption

Table 1. Security comparison.

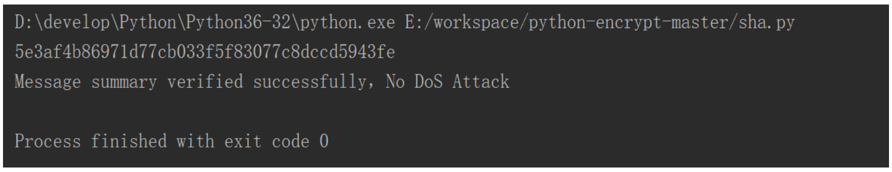
	Access restrictions	Mixed encryption authentication	Defend against attacks
IEC 61850 protocol with AES algorithm	×	×	×
IEC 61850 protocol with DES algorithm	×	×	×
IEC 61850 protocol with W-EAP algorithm	√	√	√



```
C:\Users\Administrator>ssh root@192.168.189.129
ssh_exchange_identification: read: Connection reset

C:\Users\Administrator>_
```

Figure 11. Whitelist authentication for access devices.



```
D:\develop\Python\Python36-32\python.exe E:/workspace/python-encrypt-master/sha.py
5e3af4b86971d77cb033f5f83077c8dccd5943fe
Message summary verified successfully， No DoS Attack

Process finished with exit code 0
```

Figure 12. Verification of message integrity.

security and device access verification, and did not design a simulated attack to test the entire scheme. Therefore, experimental testing of the attack model is also one of the follow-up work.

3) The W-EAP algorithm uses an international algorithm. Compared with the national secr*et al*gorithm promoted in China, its security is relatively low, and the key information infrastructure in the future needs to support the national secr*et al*gorithm. Therefore, the application of national secr*et al*gorithm in the IEC 61850 protocol will be the top priority of future research tasks.

Fund Projects

General Project of the National Natural Science Foundation of China (No. 61772327); General Project of the Shanghai Natural Science Foundation of China (20ZR1455900); Qi'anxin Big Data Collaborative Security National Engineering Laboratory Open Project (No. QAX-201803); Shanghai Branch Committee Science and Technology Innovation Action Plan (No. 18511105700); Shanghai Science and Technology Commission Electric Power Artificial Intelligence Engineering Technology Research Center Project (No. 19DZ2252800); Zhejiang University State Key Laboratory of Industrial Control Technology Open Fund (No. ICT1800380).

Conflicts of Interest

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

References

[1] Dong, Y., Xiong, Y. and Wang, B. (2019) Security Threat and Defense Technology of Smart Grid Communication Protocol. *Computer Technology and Development*, **29**, 1-6.

[2] Wang, M. and Wang, Y., Deng, L., *et al.* (2019) IEC 61850 Data Security Transmission Method Based on AES-RSA. *Journal of Automation and Information Security for Industrial Control Systems*, **36**, 63-66.

[3] Lu, F., Liu, S., Yan, H., *et al.* (2015) Vulnerability Analysis and Protective Measures of mainstream Communication Protocols in industrial Control Systems. *Industrial Technology Innovation*, **5**, 63-66.

[4] Zhang, Y. (2017) Intelligent Substation Network Communication Online Monitoring System. Nanjing University of Science and Technology, Nanjing.

[5] Jing, K., Dong, L., Sun, Y. (2015) Research and Application of Intelligent Substation Monitoring and Early Warning System. *Electric Power Information and Communication Technology*, **13**, 153-157.

[6] Hou, L., Zhang, J., Jin, N., *et al.* (2016) Design of Network Attack Detection and Forensics for Substation Process Layer and SMV Security Transmission. *Power System Automation*, **40**, 87-92+155.

[7] Yang, Y., Huang, X., Cao, J., *et al.* (2011) Security Authentication and Real-Time Simulation of substation Communication Message. *Power System Automation*, **35**, 77-82.

[8] Farooq, S.M., Suhail Hussain, S.M., Ustun, T.S. (2019) S-GoSV: Framework for Generating Secure IEC 61850 GOOSE and Sample Value. *Messages*, **12**, 2536.

https://doi.org/10.3390/en12132536

[9] Yu, H., Jia, X. and Wang, Q. (2016) Research on Security Protection Strategy of Intelligent Substation Application Layer Data Encryption. *Computer and Modernization*, **2**, 82-85.

[10] Guo, Y. (2018) Research and Implementation of power EMS Network Security Protection Strategy. University of Electronic Science and Technology of China, Chengdu.

[11] Eslava, H., Rojas, L.A. and Pineda, D. (2015) An Algorithm for Optimal Firewall Placement in IEC 61850 Substations. *Proceedings of the* 7*th Asia-Pacific Power and Energy Engineering Conference* (*APPEEC* 2015), Beijing, 12-14 April 2015, 7-23.

[12] Kim, J. and Park, J. (2018) FPGA-Based Network Intrusion Detection for IEC 61850-Based Industrial Network. *ICT Express*, **4**, 1-5. https://doi.org/10.1016/j.icte.2018.01.002