

AES RSA-SM2 Algorithm against Man-in-the-Middle Attack in IEC 60870-5-104 Protocol

Shan Shi¹, Yong Wang^{1*}, Cunming Zou², Yingjie Tian³

¹College of Computer Science and Technology, Shanghai University of Electric, Shanghai, China

²Third Institute of Ministry of Public Security, National Network and Information System Safety Product Quality Supervision and Testing Center, Shanghai, China

³Institute of Electric Power Science, State Grid Shanghai Electric Power Company, Shanghai, China

Email: 18351801151@163.com, *wy616@126.com

How to cite this paper: Shi, S., Wang, Y., Zou, C.M. and Tian, Y.J. (2022) AES RSA-SM2 Algorithm against Man-in-the-Middle Attack in IEC 60870-5-104 Protocol. *Journal of Computer and Communications*, 10, 27-41.
<https://doi.org/10.4236/jcc.2022.101002>

Received: January 25, 2021

Accepted: January 10, 2022

Published: January 13, 2022

Copyright © 2022 by author(s) and Scientific Research Publishing Inc. This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

The IEC60870-5-104 protocol lacks an integrated authentication mechanism during plaintext transmission, and is vulnerable to security threats, monitoring, tampering, or cutting off communication connections. In order to verify the security problems of 104 protocol, the 104 master-slave communication implemented DoS attacks, ARP spoofing and Ettercap packet filtering and other man-in-the-middle attacks. DoS attacks may damage the network functions of the 104 communication host, resulting in communication interruption. ARP spoofing damaged the data privacy of the 104 protocol, and Ettercap packet filtering cut off the communication connection between the master and the slave. In order to resist the man-in-the-middle attack, the AES and RSA hybrid encryption signature algorithm and the national secret SM2 elliptic curve algorithm are proposed. AES and RSA hybrid encryption increases the security strength of communication data and realizes identity authentication. The digital signature implemented by the SM2 algorithm can realize identity verification, ensure that the data has not been tampered with, and can ensure the integrity of the data. Both of them improve the communication security of the 104 protocol.

Keywords

104 Protocol, Man in the Middle Attack, AES and RSA Hybrid Encryption Signature, National Secret SM2 Algorithm

1. Overview

IEC 60870-5-104 (*i.e.*, IEC 104) protocol [1] is a communication protocol for

Ethernet in the IEC60870-5 series, which specifies the combination of the application layer of the IEC 101 protocol and the transmission function provided by TCP/IP. When transmitting messages between the master station and the slave station of the SCADA system, the 104 protocol transmits the real-time data from the slave station to the master station and sends the upper command to the slave station [2]. Since 104 protocol is based on TCP/IP protocol, its conflict detection of Internet network protocol and error retransmission mechanism is more stable and reliable than the IEC 101 protocol. The 104 protocol has been widely used in power systems. Since 104 protocol does not integrate encryption authentication and identity authentication, messages are easily tampered with. Wang Yong and Wang Xiang [3] constructed the communication system between FTU and master station, and verified the 104 protocol data intercepted by man in the middle attack. In order to enhance the protocol security, an improved method based on identity authentication (bm-rap) is proposed. The effectiveness of anti-man in the middle attack is verified through experiments, It provides a more secure and reliable environment for 104 protocol communication. Liu Yuanyuan [4] designed and implemented a secure communication protocol with message encryption and access authentication in response to the problem that the message content of the 104 protocol may be tampered with, and developed a remote control terminal application software based on the security mechanism. It improves the security of message transmission. Jiang Zexin [5] proposed three attack methods against the insecurity of the 104 protocol remote control process: ARP spoofing, transparent proxy attack, and bridge filtering, and proposed the use of secure sockets such as SSL for TCP connection protection, in order to realize the mutual identity authentication and the establishment of shared key between the front-end computer and the distribution terminal based on 104 protocol. Ma Jun [6] proposed a security protocol based on one-way digital signature and one-way hash authentication code algorithm. The security analysis of the protocol proves that the protocol can resist external attacks, replay attacks and impersonation attacks, and has higher security and efficiency.

To some extent, the above method solves the security transmission threat of 104 protocol due to the lack of integrated authentication mechanism in plaintext transmission, and realizes the encryption of the protocol. However, for example, in [4], DES encryption algorithm and hamc-md5 authentication algorithm are used to realize the security protection of IEC60870-5-104 protocol. The two algorithms are used for data encryption and verification respectively, and the two algorithms are not combined. In this paper, AES and RSA hybrid encryption signature algorithm is used to combine data encryption and signature verification, which makes message transmission more convenient, safe and reliable, and can resist man in the middle attack to a certain extent. We focus on the security of the IEC104 protocol [7] and propose a defense algorithm. The TCP/IP protocol uses clear text for data exchange and transmission, and telemetry, remote signaling and remote control information are all transmitted in clear text, without any authentication mechanism [8]. This means that communication data is

easy to be eavesdropped or tampered with. The non-authentication mechanism of 104 protocol control commands may also cause replay attacks, ARP spoofing and Denial of Service (DoS) attacks [9]. DoS attacks may disrupt network functions, leading to consequences such as power outages and blackouts. Replay attacks may cause physical damage to the power system, such as Stuxnet attacks. Man-in-the-middle attacks can compromise data privacy. The importance of power system information security has also promoted Research and application of national secret algorithm. The national secret algorithm is applied to the field of electric power system and can complete functions such as identity authentication and data encryption and decryption. This article did the following:

- 1) Use the PMA communication protocol analysis tool to build a 104 protocol master station and slave station, get the communication message of master and slave station;
- 2) In view of the security vulnerabilities in the 104 protocol, use DoS attacks and ARP spoofing methods to conduct attack tests, and analyze the communication between the master and slave stations after the attack;
- 3) In order to improve the communication security of 104 protocol, AES and RSA hybrid encryption signature algorithm and national secret SM2 elliptic curve algorithm are proposed.

This article used the IEC 104 protocol security detection as the background to study the attack technology in the 104 protocol communication environment, as well as the defense technology based on the data encryption and signature of the communicating parties to achieve more secure communication environment.

The structure of the paper is as follows: The first chapter is the introduction. Chapter two elaborates on the security problems of 104 Statute. The third chapter is the security test of 104 protocol, including DoS attack, ARP spoofing and Ettercap packet filtering experiment. Chapter four proposes a hybrid encryption signature algorithm based on 104 protocol AES and RSA and a digital signature based on 104 protocol SM2 algorithm. Chapter five analyzes the experimental results of the two algorithms. Chapter six is the conclusion.

2. Safety Issues of IEC 60870-5-104 Protocol

The function of IEC-104 is based on the TCP/IP protocol, so the 104 protocol has the security issues of the TCP/IP protocol [10]. Although the solutions and guidelines provided by the IEC62351 [11] standard enhance the security of the IEC104 protocol, the industrial nature of the SCADA system that uses the 104 protocol hinders the upgrade of the protocol.

- 1) TCP data verification: In order to ensure the integrity of data transmission, an end-to-end checksum is used. The sender calculates the data, and the receiver uses the same arithmetic method to check. If the calculated value at both ends is the same, it proves that the data transmission is complete. However, such calculations can only ensure the complete transmission of the data. If the data is tampered with, the data security of the application layer 104 protocol cannot be

guaranteed.

2) Plain text transmission: When the application layer transmits data, there is no integrated encryption and identity authentication mechanism, that is, 104 data is transmitted in plain text, and it is easy for attackers to implement MiTM on 104 protocol communication [3]. If MiTM succeeds, data tampering, monitoring or discarding may occur. PMA can directly obtain the communication message of 104 protocol master-slave station, as shown in **Figure 1**.

In order to verify that the 104 protocol communication data is transmitted in plain text, the data packet sent from the master station is marked in **Figure 1**, and the data packet captured by WireShark shows that the data packet is included. The verification result is shown in **Figure 2**.

3) Accept the problem of discontinuous serial numbers: There are three message formats in the IEC 104 protocol, namely the I format for effective data transmission, the S format for number confirmation, and the U format for connection maintenance. I frame is divided into two parts, APCI and ASDU, collectively referred to as APDU [12], while S frame and U message have only APCI part.

When receiving an I format data frame, compare the sending sequence number with the local receiving sequence number, if they are the same, then receive it, otherwise decide whether to discard it according to the situation. This guarantees data to a certain extent. However, when the network delay is large, the application layer data packets may arrive out of order. When a data packet is discarded due to out of order, subsequent messages will be out of order. The way to solve the problem of serial number discontinuity is to adopt the window receiving method, as shown in **Figure 3**.

4) The problem of data retransmission: The 104 protocol provides a mechanism to prevent message loss and retransmission. According to the received sequence number of the message, confirm the correct number of messages transmitted to the other party, and confirm whether there is any message loss according to the comparison of the sent message counter. If the sequence number is correct, the message transmission is normal, otherwise it is confirmed that the

Master station sending

68 0e 04 00 04 00 2d 01 06 00 01 00 00 00 00 df

Start byte= 68 Data unit length(ARDU)=14 I Format frame Send serial number(NS)=2

Receive serial number(NR)=2 TI=45 VSQ=01 SQ=0 INFONUM=1 COT=06 T=0 PN=0 CAUSE=6 COA=1

Figure 1. 104 protocol communication message.

0000	00 50 56 c0 00 08 00 0c	29 8b 55 f7 08 00 45 00	.PV.....).U...E.
0010	00 38 63 d3 40 00 80 06	d5 18 c0 a8 20 82 c0 a8	.8c.@...
0020	20 01 c2 1b 09 64 c1 81	62 d4 2b 4c 0e 7a 50 18	...d.. b.+L.zP.
0030	01 00 1e 5e 00 00 68 0e	04 00 04 00 2d 01 06 00	...^..h.
0040	01 00 00 00 00 df	

Figure 2. WireShark packet capture results.

message is lost, and the connection needs to be disconnected to continue the transmission. Therefore, if the attacker predicts the confirmation sequence number by monitoring the message, the attacker is likely to forge the message for transmission, thereby posing a threat to the system. If 104 protocol communication continuously receives 12 out-of-sequence data packets, the master station will close the connection and reconnect. After the new network connection is established, the slave station re-uploads all real-time data, and the real-time data before the disconnection can be directly discarded as appropriate in **Figure 4**.

The disconnection retransmission mechanism can solve the problem of intermittent data transmission after accidental connection disconnection to a certain extent, and improve the communication capacity of the 104 protocol network. 104 Protocol sending and receiving sequence numbers can resist replay attacks to a certain extent, but the replay resistance is relatively weak.

104 Protocol is based on TCP/IP protocol to establish network communication, lack of integrated encryption and identity authentication mechanism, and

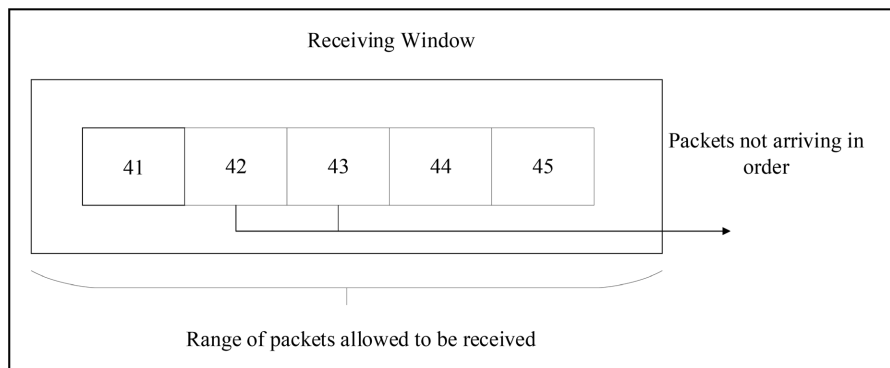


Figure 3. Schematic diagram of window receiving mode.

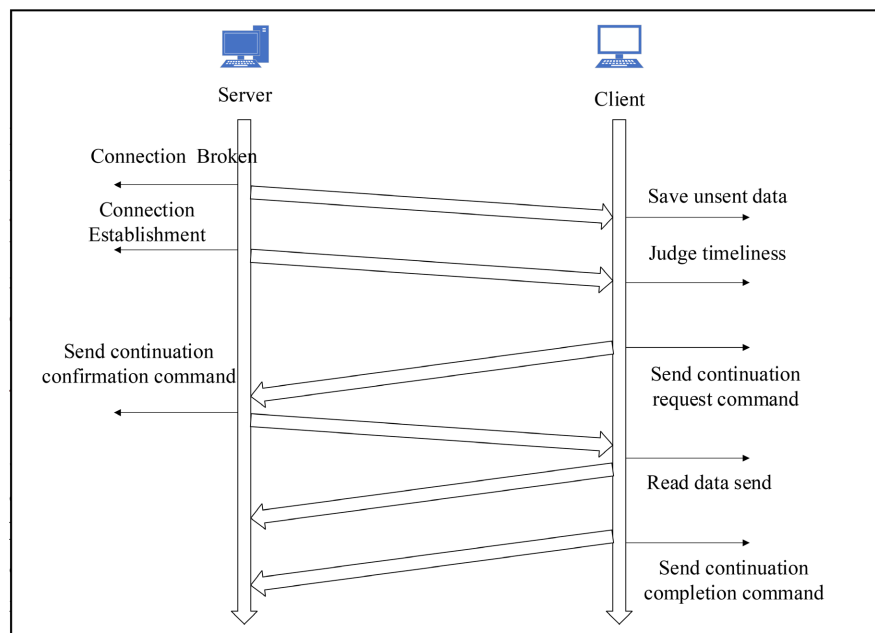


Figure 4. Schematic diagram of the retransmission process after disconnection.

TCP checksum cannot guarantee the security of application layer protocols, etc., which can easily lead to 104 protocol being eavesdropped, forged or tampered with by middlemen.

3. Security Test and Analysis

In this experiment, we use the PMA tool to simulate the communication between the 104 protocol master station and the slave station, and attack the target host, DoS attacks and ARP spoofing. The host computer is used as the 104 protocol slave station, virtual machine 1 is used as the master station, while the master station is the victim, and Kali Linux is used as the attacker to carry out the attack. The test environment of this experiment is shown in **Table 1**.

PMA can send commands such as single-point remote control (C_SC_NA_1), dual-point remote control (C_DC_NA_1) and total call (C_IC_NA_1) when simulating master station communication, and it can send single-point remote signal displacement (M_SP_NA_1) and dual-point remote signal when simulating slave stations. Displacement (M_DP_NA_1) and other information, you can manually test various remote control types. After the master-slave connection is successful, the communication message information of IEC 104 protocol data transmission will be displayed.

3.1. DoS Attack

The TCP SYN flood attack is a common DoS attack. The TCP SYN flood attack is where the attacker sends a large number of SYN request packets to the TCP port of the target host, but does not complete the TCP “three-way handshake” process. This attack uses the TCP protocol Defect, sending a large number of forged TCP connection requests, thereby exhausting the resources of the attacked party. In this experiment, the attacker will continuously send a large number of concurrent cyclic SYN packets to the attacked (IP: 192.168.32.130) without retaining the corresponding answer (SYN + ACK). When simulating the SYN flood attack, we use the program of `syn_flood.py` and the `scapy` module to send a large number of cyclic SYN packets to the target host port. This attack did not interrupt the communication between the slave and the master. However, it should be noted that this attack may be more successful in an actual environment

Table 1. Experimental test environment.

Equipment	System/Software	IP, MAC address
Host operating system	Windows 10	IP:192.168.32.1 MAC: 00:50:56:c0:00:08
Virtual machine 1	Windows Server 2008	IP:192.168.32.130 MAC:00:0c:29:8b:55:f7
Virtual machine 2	Kali Linux	IP:192.168.32.133 00:0c:29:75:29:30
Gateway		IP:192.168.32.2 MAC:00:50:56:e1:4e:bc

where the target host has the characteristics of limited computing resources. In addition, if there are more network attackers, the effect of the attack will be different. When multiple hosts perform an SYN flood attack on a server at the same time, the running speed of the server will become very slow.

The main code:

```
def synflood (target,port):
    while 0==0:
        x = random.randint(0,65535)
        send (IP(dst=target) /
            TCP(dport=port,sport=x), verbose=0)
        for x in range (0,threads): thread.start_new_thread(synflood,(target,port))
```

The TCP SYN flood attack occupies a large number of TCP ports, although the communication between the slave station and the master station was not interrupted. However, it should be noted that this attack may be more successful in an actual environment where the target host has the characteristics of limited computing resources. In addition, if there are more network attackers, the effect of the attack will be different. When multiple hosts carry out an SYN attack on a server at the same time, the server's operating speed will become very slow.

3.2. ARP Spoofing

In this experiment, ARP spoofing is performed on the target host and gateway in the local area network [13], and the ARP cache table of the target host and gateway is changed. Through ARP spoofing, the entire network can be deceived. The experiment uses the Ettercap tool to carry out ARP spoofing attacks on the target host.

In ARP Spoofing experiment, the client, server and attacker are all in the same LAN, The topology of the experiment is as follows in **Figure 5**.

The attack result is shown in **Figure 5**.

Compare the IP-MAC addresses before and after ARP spoofing, and get the ARP table of the IP-MAC relationship between the attacker (IP: 192.168.32.133) and the gateway (IP: 192.168.32.2) in the LAN before ARP spoofing, as shown in **Figure 6**.

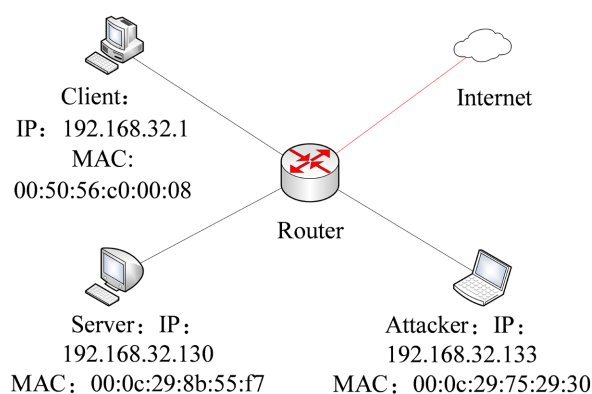


Figure 5. Experimental topology diagram.

Scan the hosts in the local area network, select the target host address, add it to target 1, deceive the target host “I am a gateway”. Select the gateway address in the host list and add it to target 2, deceiving the gateway “I am the target host”.

Turn on the ARP poisoning function and launch an attack on the target host. Looking at the ARP table, we can find that the MAC address of the gateway has been changed from 00:50:56:e1:4e:bc before the attack to the attacker’s MAC address 00:0c:29:75:29:30, that is, the attacker successfully implemented ARP spoofing and acted as a middleman in the communication between the target host and the gateway. All communication data traffic between the target host and the gateway will be sent to the attacker’s host. tapping. After the successful ARP spoofing attack, the ARP of the gateway address is shown in **Figure 7**.

In order to verify whether the ARP spoofing is successful, the attacker uses the packet capture tool WireShark to capture data packets with the command ip.addr == 192.168.32.130 && 104asdu. The filtered data packets contain a large amount of data information of 104asdu from the target host. The result of WireShark packet capture is shown in **Figure 8**.

After the implementation of ARP spoofing, because 104 communication data

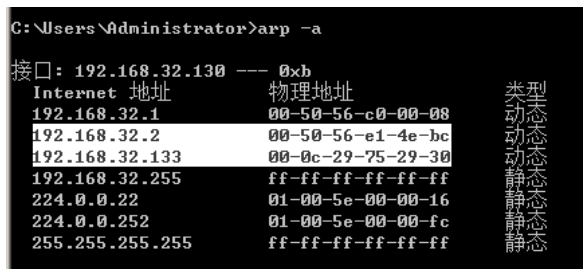


Figure 6. Experimental topology diagram.

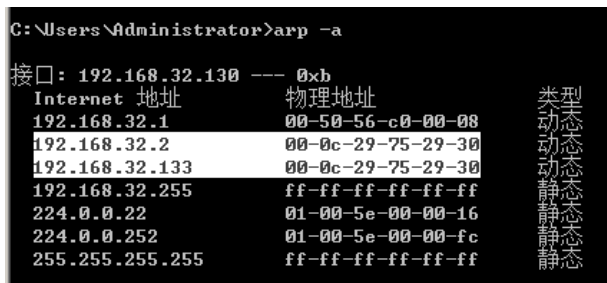


Figure 7. ARP table of target host after successful attack.

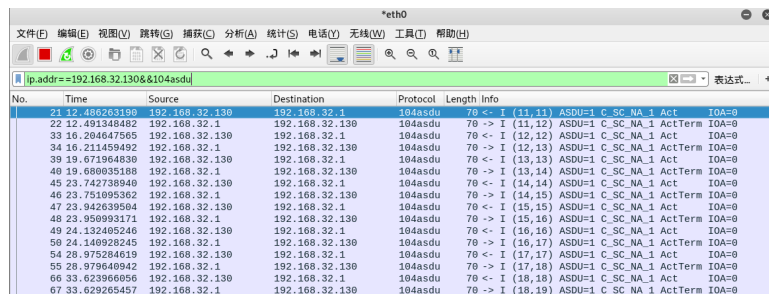


Figure 8. Wireshark packet capture results after ARP spoofing.

packets are transmitted in plaintext, it is easy for an attacker to monitor the intercepted data to obtain the communication content of both parties.

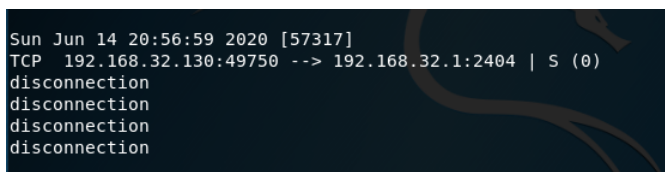
3.3. Ettercap Packet Filtering

Etterfilter is a very powerful man-in-the-middle attack tool. KaliLinux puts itself between the master station and the slave station to control the communication process of the system, tampering with communication or deleting communication by filtering data packets. This article uses Etterfilter packet filtering to delete master-slave communication. This article aims to use Ettercap filter in Kali Linux to use Etterfilter to compile the filter and load it into Ettercap to process network requests. First, create the filter script drop.filter, and then use the command `etterfilterdrop.filter -o drop.ef` to compile the filter script drop.filter into a binary file drop.ef that Ettercap can recognize. Compile the filter and finally use the Ettercap command to load the filter script: `ettercap -i eth0 -T -F drop.ef`. Realize the discarding of 104 master-slave system data packets and cut off their connection. The filter script drop.filter is designed to filter 104 protocol packets of the master and slave stations, and then set ettercap not to forward the 104 packets, and cut off the communication connection between the 104 master station and the slave station, and the execution effect can be seen when the connection is cut off “Disconnection” will be displayed.

The codes for shutting off 104 master and slave stations are as follows.

```
if (ip.proto == TCP) {
  if (tcp.src == 2404 || tcp.dst == 2404) {
    drop();
    kill ();
    msg("disconnection");
  }
}
```

After the attacker executes drop.ef, it will cut off the communication connection between the target host and the slave. The attack result is shown in **Figure 9**. At this time, the connection failure will be displayed on the master station and the slave station. **Figure 10** shows the connection result of the master station.



```
Sun Jun 14 20:56:59 2020 [57317]
TCP 192.168.32.130:49750 --> 192.168.32.1:2404 | S (0)
disconnection
disconnection
disconnection
disconnection
```

Figure 9. Data drop attack results.

```
68 04 01 00 02 00
```

```
Start byte= 68 Data unit length(ARDU)=4 S Format frame Receive serial number(NR)=1
```

```
Receiving failure, Re-link!:10054
```

Figure 10. Connection result of the master station.

4. AES RSA-SM2 Algorithm Based on 104 Protocol

In view of the threat of 104 protocol lacking encryption and identity authentication, this paper proposes two algorithms, namely AES and RSA hybrid encryption signature and national secret SM2 elliptic curve algorithm. The hybrid encryption algorithm is used to encrypt transmitted 104 protocol messages to prevent middlemen from seeing. The transmission of plaintext results in information leakage. The signature is to prevent the middleman from impersonating himself or being tampered with. The data received by the receiver through algorithm identification is sent by the sender and has not been tampered with.

4.1. Hybrid Encryption Signature Algorithm of AES and RSA

AES is a symmetric encryption algorithm with high encryption and decryption processing efficiency, RSA is an asymmetric encryption algorithm [14], and RSA algorithm encryption and decryption processing efficiency is low. If the AES symmetric cryptographic system is used to encrypt the transmitted data, and the RSA asymmetric cryptographic system is used to transmit the AES key, the advantages of AES and RSA can be comprehensively utilized and the client can authenticate the server at the same time. As shown in **Figure 11** [15], it is the mixed encryption signature algorithm flow of AES and RSA.

Take the example of sending data from the slave to the master, the specific process is as follows:

- 1) The master station generates its own RSA key pair, and provides an interface for the slave station to obtain the RSA public key, and the RSA private key is stored at the master station;
- 2) The random function of the slave station generates the AES key;
- 3) Use the RSA private key of the slave station to sign the original data to get the Sign;
- 4) The slave uses its own AES key to encrypt the requested plaintext data (data) to obtain the encrypted request data encryptData;
- 5) The slave uses the RSA public key to encrypt the AES key, and obtains the encrypted AES key encryptAesKey;
- 6) The slave station transmits encryptAesKey and encryptData to the master station together through the Internet;
- 7) After receiving the data, the master station uses its own RSA private key to decrypt the encryptAesKey to obtain the aesKey. If the decryption succeeds, it can be determined that it is the data sent from the slave station and the data has not been tampered with;
- 8) The master station uses the decrypted aesKey to AES decrypt the encrypted request data encryptData to obtain the decrypted data;
- 9) Sign and encryptData are verified by the RSA public key of the slave station. If the verification succeeds, it means that the data is not forged.

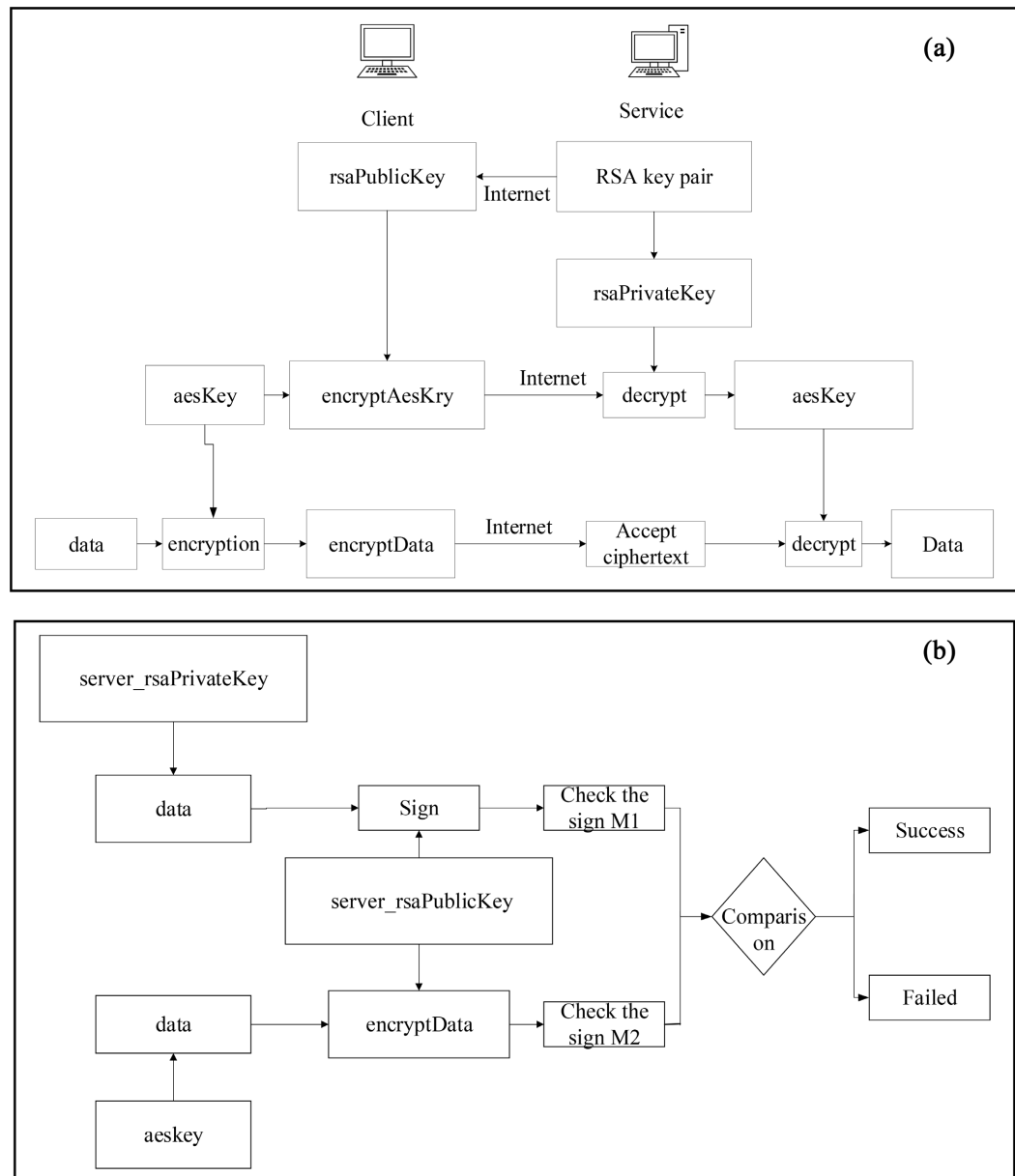


Figure 11. AES and RSA hybrid encryption and signature process. (a) Hybrid encryption and decryption process; (b) Signing and verification process.

4.2. National Secret SM2 Algorithm

The national secret algorithm is a series of data encryption processing algorithms with independent intellectual property rights in my country. The SM1-SM4 algorithms implement symmetric, asymmetric, and abstract algorithm functions. The national secret algorithm is used in the power system industry to realize identity authentication and data encryption and decryption function. The SM2 digital signature algorithm uses the private key of the signature side to sign the original data, and the verifier uses the public key of the signature side to verify whether the signature is correct. The signature has a public key and a private key.

The curve equation of SM2 is as follows:

$$y^2 = x^3 + ax + b \quad (1)$$

SM2's signature and verification algorithm flow steps are as follows:

M is the message to be signed, the digital signature result is (r, s) , and the user key pair is (d, P) , where d is the private key and P is the public key;

The signer side implements the following steps:

1) Get the message hash value:

$$e = \text{hash}(M) \quad (2)$$

Convert the data type of e to an integer;

2) Generate random numbers $k \in [1, n-1]$;

3) Use random number k to calculate elliptic curve points

$$(x_1, y_1) = [k]G \quad (3)$$

Convert the data type of x_1 to an integer;

4) Calculation

$$r = (e + x_1) \bmod n \quad (4)$$

If $r = 0$ or $r + k = n$, continue to step (2);

5) Calculation

$$s = ((1 + d)^{-1} * (k - r * d)) \bmod n \quad (5)$$

If $s = 0$, continue to step (2);

6) The signature of message M is (r, s) .

The steps at the verifier end are as follows:

a) Check whether $r \in [1, n-1]$ is valid, if not, the verification cannot be passed;

b) Check whether $s \in [1, n-1]$ is valid, if not, the verification cannot be passed;

c) Apply formula (2) to obtain the message hash value and convert the data type of e to an integer;

d) Calculation

$$t = (r + s) \bmod n \quad (6)$$

If $t = 0$, the verification fails;

e) Calculate elliptic curve points

$$(x_1, y_1) = [s]G + [t]P \quad (7)$$

Convert the data type of x_1 to an integer;

f) Calculation

$$R = (e + x_1) \bmod n \quad (8)$$

If $R = r$, the verification is passed, otherwise the verification cannot be passed.

5. Experiment Analysis

5.1. Experimental Analysis of AES-RSA Algorithm

The hybrid encryption algorithm based on AES and RSA realizes the identity authentication of the slave station and the encryption of data. Even if the en-

encrypted message sent by the master station is intercepted, it will not cause leakage, because only the RSA private key of the master station can decrypt the AES Key to perform AES operation on encrypt Data to obtain the decrypted plaintext data. Using this encryption algorithm to encrypt the transmission data between the master and slave can prevent monitoring and tampering, thereby ensuring the security of the system transmission data, ensuring the integrity of the data, and verifying the identity of the slave, for example, when the master and slave During data communication, the slave station transmits encrypt Aes Key and encrypt Data to the master station through the network. At this time, the data is transmitted in the form of cipher text, and the AES key is encrypted with the RSA public key. After encryption, it will be stored safely or through a secure channel. During transmission, it is difficult for an attacker to monitor or tamper with the data.

Figure 12 shows the cipher text and decrypted data of the AES and RSA mixed encryption used to sign 104 data.

5.2. Experimental Analysis of SM2 Algorithm

In this experiment, we apply the national secret SM2 algorithm to 104 protocol data communication. If the master station wants to send a single point remote control signal data M “680e040004002d0106000100000000df” to the slave station, the master station uses the private key as the signature end “00B9AB0B828FF68872F21A837FC303668428DEA11DCD1B24429D0C99E24EED83D5” to sign the data M to get (r, s) , and the slave station acts as the verification end Use the public key “B9C9A6E04E9C91F7BA880429273747D7EF5DDEB0BB2FF6317EB00BEF331A83081A6994B8993F3F5D6EADDD81872266C87C018FB4162F5AF347B483E24620207” to calculate the elliptic curve points (x_1, y_1) and R , If $R = r$ means that the verification is established, the data integrity and non-repudiation are guaranteed. We adopt the national secret SM2 elliptic curve algorithm, which can improve the autonomy of information security in our country. The SM2 algorithm is a secure communication protocol based on an asymmetric key. It can prevent DoS attacks through pre-authentication and can improve data

```

root@kali:~# python AES_RSA_sign.py
104的数据报文: 680e040004002d0106000100000000df
客户端经过aes加密后的数据: pJnI0BCQuzPuLhLZnjKsGf/4HJNIIUNCSvlyvhqmdm7d0B3TnNm
dIMZfHYrLKxsn
客户端使用Client私钥对104签名:
r8dkitaQknHt2MvQeYpMBgC5VjHBbNg6Fx2I/moUTrVsnQAa60BJUs11CFtM0G/+yYWyhpsVRL4kKbbX
l03ujESxw9b9+0Y0SSGgFZv2Kkalg2sgvJh/rCvgr1uKtn8iB0prwLZZHjofJnPyeuy6wbtGLXJxnmGs
SPGI3AIInm4=
使用Server端公钥加密后的aes密钥:
aRPf/y1pERpmbU4hFkuI3j6jZVPWk20Em5+ncEyfcoBcS28kV0xzqeBzXwI7jCc21ELLAU1Qyt65jUn0
vK+wQ8LXl8l+t/ZX3nC7uXXKb86gtZM7uq79laaGn474f2yoyhY39XuoARNX3BJE8zHjck7puB0TjiqD
WeCsJL/XZrs=
*****
Server端使用Client端公钥对104报文验签结果:
True
Server端经过aes解密后的数据: 680e040004002d0106000100000000df

```

Figure 12. AES and RSA hybrid encryption for 104 data signature.

security when applied to 104 protocol communications. We adopt the national secret SM2 elliptic curve algorithm, which can improve the autonomy of information security in our country. The SM2 algorithm is a secure communication protocol based on an asymmetric key. It can prevent DoS attacks through pre-authentication and can improve data security when applied to 104 protocol communications.

6. Conclusion

This paper firstly studies and analyzes the communication security of the 104 protocol, using the characteristics of man-in-the-middle attacks to carry out DoS attacks, ARP spoofing and Ettercap tools on the target host to cut off the communication between the master and slave stations. In a DoS attack, the attacker sends a large number of TCP connection requests to the target host. If a large number of hosts are used to make SYN requests to the server, it will cause service device to run slowly or even interrupt. When ARP spoofs the target host, it pretends to be the communication gateway between the master and the slave. After the attack is successful, the data packets passing through the target host will be intercepted by the attacker to obtain all the communication information. Ettercap compiles the filter and loads it to Ettercap; you can control the communication at both ends to change the target's communication. For man-in-the-middle attacks, the AES and RSA hybrid encryption signature and the national secret SM2 algorithm are proposed. The advantages of the AES and RSA hybrid encryption collection of the two parties' keys implement double protection for the communication data. At this time, it is difficult for the attacker to monitor or tamper with the data. Digital signature can realize the authentication of both sides of communication. The SM2 algorithm of the state secrets mainly replaces the RSA algorithm. The SM2 digital signature algorithm implemented in this paper ensures the integrity and non-repudiation of the message, and resists man-in-the-middle attacks to a certain extent.

Fund Projects

National Natural Science Foundation of China (61772327); Shanghai Natural Science Foundation (20ZR1455900); Development fund of National Engineering Laboratory for big data collaborative security (QAX-201803).

Conflicts of Interest

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

References

- [1] Wang, Z.J. (2013) Research on IEC 60870-5-104 Communication Protocol Test Method Based on Network Monitoring. School of Electronic Information and Electrical Engineering. Shanghai Jiao Tong University, Shanghai.
- [2] Zhang, J.J. (2013) Research and Development of Information Live Broadcast System

- for Visualized Monitoring of Power Grid Operation Safety. North China Electric Power University, Beijing.
- [3] Wang, Y., Wang, X., Liu, L.L., *et al.* (2019) Anti-Man-in-the-Middle Attack Algorithm Based on IEC60870-5-104 Protocol for Distribution Network. *Journal of Information Security*, **4**, 56-66.
- [4] Liu, Y.Y. (2015) Research and Implementation of IEC 60870-5-104 Protocol Based on Network Security. M.S. Dissertation, Xi'an Polytechnic University, Xi'an.
- [5] Jiang, Z.X. (2018) IEC60870-5-104 Protocol Security Analysis and Attack Experiment. *Microcomputers and Applications*, **37**, 1-4, 14.
- [6] Ma, J. and Zhang, Y.B. (2013) Distribution Automation Communication Security Protocol Based on IEC60870-5-104. *Computer Science*, **40**, 81-84.
- [7] Matoušek, P. (2017) Description and Analysis of IEC 104 Protocol. Tech. Rep., Faculty of Information Technology, Brno University of Technology, Brno.
- [8] Yang, Y., McLaughlin, K., Littler, T., *et al.* (2013) Intrusion Detection System for IEC 60870-5-104 Based SCADA Networks. *IEEE Power & Energy Society General Meeting*, Vancouver, 21-25 July, 2013, 1-5.
<https://doi.org/10.1109/PESMG.2013.6672100>
- [9] Radoglou-Grammatikis, P., Sarigiannidis, P., Giannoulakis, I., *et al.* (2019) Attacking IEC60870-5-104 SCADA Systems. 2019 *IEEE World Congress on Services*, Vol. 2642, 41-46. <https://doi.org/10.1109/SERVICES.2019.00022>
- [10] Liu, L. (2013) Security Evaluation of Electric Power Communication Transmission Network for SCADA Business. North China Electric Power University, Beijing.
- [11] Schlegel, R., Obermeier, S. and Schneider, J. (2017) A Security Evaluation of IEC 62351. *Journal of Information Security and Applications*, **34**, 197-204.
<https://doi.org/10.1016/j.jisa.2016.05.007>
- [12] Ye, L., Chen, W.M. and Cao, X. (2018) The Application of IEC60870-5-104 Protocol in Monitoring System. *Electronic Measurement Technology*, No. 6, 26.
- [13] Hong, S., Oh, M. and Lee, S. (2013) Design and Implementation of an Efficient Defense Mechanism against ARP Spoofing Attacks Using AES and RSA. *Mathematical and Computer Modelling*, **58**, 254-260. <https://doi.org/10.1016/j.mcm.2012.08.008>
- [14] Xiao, Z.J., Hu, C., Jiang, Z.T., *et al.* (2014) Optimization of AES and RSA Algorithms and Their Hybrid Encryption System. *Computer Application Research*, **31**, 1189-1194.
- [15] Xu, C. (2016) Application of AES and RSA Hybrid Encryption Technology in Network Data Transmission. *Wireless Internet Technology*, No. 13, 3.