Scientific Research Publishing

Journal of Computer and Communications, 2019, 7, 38-49
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

An Anti-Eavesdropping Method in Data Collection of Smart Meter

Weiwei Dong, Yong Wang, Lin Zhou, Kanghua Cao, Haiming Li

College of Information and Technology, Shanghai University of Electric, Shanghai, China
Email: dongweiwei6288@163.com

How to cite this paper: Dong, W.W., Wang, Y., Zhou, L., Cao, K.H. and Li, H.M. (2019) An Anti-Eavesdropping Method in Data Collection of Smart Meter. *Journal of Computer and Communications*, **7**, 38-49.
https://doi.org/10.4236/jcc.2019.79004

Received: June 27, 2019
Accepted: September 17, 2019
Published: September 20, 2019

Abstract

At present, DL/T 645-2007 communication protocol is used to collect data for smart meters. However, in the beginning, this protocol is not designed to be a secure protocol and only the function and reliability were taken into account. Plaintext is used in the protocol for data transmission, as a result, attackers can easily sniff the information and cause information leakage. In this paper, man-in-the-middle attack was used to verify that the smart meter data acquisition process was vulnerable when facing third-party attacks, and this can result in data eavesdropping. In order to resist such risks and prevent information being eavesdropped, a real ammeter communication experimental environment was built, it realized two-way identity authentication between data acquisition center and ammeter data center. At the same time, RSA (Rivest-Shamir-Adleman) was used to encrypt the meter data, which encrypted the collection, storage process of meter data and ensured the confidentiality and integrity of the meter data transmission. Compared with other methods, this method had obvious advantages. The analysis showed that this method can effectively prevent the data of smart meters from being eavesdropped.

Keywords

Smart Meter, Data Acquisition, Transmission, Eavesdropping, RSA, Two-Way Authentication

1. Introduction

In December 2015, due to the malicious software attacks in Ukrainian State Grid by hackers, the power grid in many regions was attacked by hacker and 225 thousand people lost power supply [1] [2] [3], it caused great financial loss. Therefore, it is critical to ensure the security of the State Grid, it is closely linked

to the national economy and people's livelihood. In China, DL/T645 communication protocol is mostly used in smart meter system. At the beginning of the design, the protocol only took the integrity of functions and the reliability of transmission into account, data is transmitted in plaintext form and its security was ignored. In addition, the data acquisition terminal is under unsupervised status, which is vulnerable to a physical, protocol and program attacks. When an illegal man-in-the-middle attack occurs, it will result in data tampering, network congestion and other risks. In serious cases, it will lead to misjudgment of the main station system [4], which seriously threatens the communication security of smart meters.

Under such background, many researchers have proposed different solutions. Taimin Zhang, Xin Lu *et al.* [5] proposed a communication method based on the encryption of session key data in order to deal with this problem. Zhao Bing, Qi Feng *et al.* [6] proposed a two-way interactive, multi-protection communication protocol (BIMP), the number of times communication parties exchanged encryption and decryption information is 5 times, but the burden is too heavy for the smart meter with weak computing power. Wei Yong [7] *et al.* proposed an effective integration method between smart terminals and GIS/PMS systems in order to ensure efficient collection of grid data resources, but it is not effective for solutions against man-in-the-middle attacks and replay attacks.

Based on the above background, this paper successfully implemented ARP spoofing by building a real experimental environment to attack the process of meter data acquisition. It proved that the process of meter data acquisition was vulnerable to man-in-the-middle attack, which made communication data eavesdropped. To solve this problem, this paper presents a method of data security acquisition for smart meters based on RSA algorithm and bidirectional authentication and encryption. In the process of data acquisition, it prevents malicious third parties from capturing and eavesdropping communication data, avoids leakage of electricity data, and finally achieves the purpose of preventing man-in-the-middle attack, replay attack and eavesdropping.

Tests show that the scheme can effectively deal with man-in-the-middle attack, replay attack and eavesdropping. Moreover, the scheme has strict security communication mechanism. Its security depends entirely on the security of asymmetric algorithm, so this scheme has good expansibility.

2. Safety Problems in Data Acquisition of Electric Meter

Data is often transmitted in plaintext in the process of transmission. Illegal persons attack the communication network by means of man-in-the-middle attacks, obtain control rights. It can intercept measurement data, resulting in measurement data disordered and key parameter errors, leading to major safety accidents [8] [9]. Once there is man-in-the-middle attack on the network, the data of both sides of the communication will be transmitted through the attacker's machine. At this time, the attacker will easily steal and intercept the data informa-

tion of the meter.

Most smart meters in China to communicate via DL/T645-2007 protocol. Since information transmission based on DL/T645-2007 protocol in plaintext forms, the attacker can sniff and analysis the data easily by means of sniffer software. In order to test this kind of risk, this paper has done a security problem detection experiment.

Safety Problem Detection

The key point of security problem detection experiment is to realize ARP deception by means of man-in-the-middle attack, deceive the local machine and intercept normal meter communication data, so that the data acquisition terminal can't normally collect the voltage, current, forward active power and other data of smart meters. The topological structure of the experiment is shown in Figure 1.

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire journals, and not as an independent document. Please do not revise any of the current designations.

ARP spoofing attack on target is carried out by using ettercap tool in Kali Linux system. By attacking the gateway, the attacker replaces the gateway and establishes independent connections with both sides of the communication. In this way, the conversation between the two sides of the communication is monitored. The configuration of the network environment in this experiment is shown in Table 1.

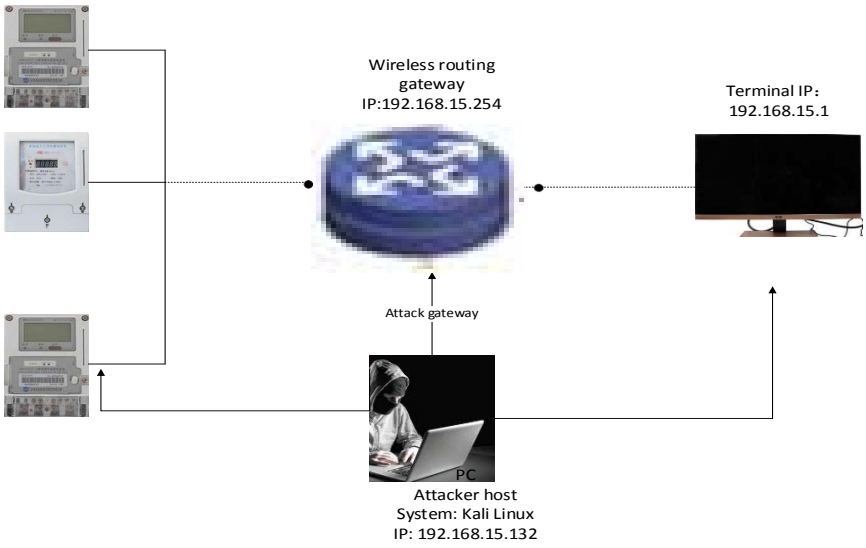

Figure 1. Topology of the experiment.

Table 1. Configuration of the network environment.

Attribute name	Attribute value
Attacker IP	192.168.15.132
Physical address (MAC)	00-0c-29-12-08-cf
Spoofed host (target host)	192.168.15.1
Routing (gateway) IP	192.16815.254
Physical address (MAC)	00-50-56-f1-7b-1d

Before attack, the ARP list of the target host is queried by the "arp-a" command. As shown in Figure 2, the man-in-the-middle attack code is written in Python language to attack the target host. A screenshot of the main attack code is shown in Figure 3.

By looking at the ARP table of the target host again, it is clear that the MAC address of the gateway in the ARP cache list has been changed from 00-50-56-f1-7b-1d before the attack to 00-0c-29-12-08-cf of the attacker, the results are shown in Figure 4. The experimental results show that the attacker successfully deceived the target host and smart meter, and meanwhile forged the gateway between the target host and the meter. Under this circumstance, all the information flow between the target host and the gateway will be eavesdropped by the attacker, and the communication between the smart meter is in an unsafe environment.

3. Anti-Middleman Attack Method

The basic data acquisition system of smart meter system consists of smart meter (SM), data collector and back-end server (MDMS). Its structure is shown in Figure 5.

The whole communication line from smart meter to back-end server MDMS is in an unsafe environment. A kind of method to prevent man-in-the-middle attack was proposed in this paper, it can be divided into two parts. Firstly, RSA two-way authentication was realized between meter data center and data acquisition, effectively avoid brute force attack. Secondly, after successful authentication, RSA encryption is applied to the data transmission of the meter to ensure that the data on the whole transmission line is transmitted in ciphertext mode, thus ensuring the security of the whole communication process.

3.1. Two-Way Authentication Scheme

The two-way authentication scheme designed in this paper is combined with the main interface designed by Qt Designer. The main authentication process is as follows, the collection center uses the authorization number (unique ID) of the collector to send an authentication request to the data center. The meter data center receives the request and randomly generates a set of challenges number, it encrypts the challenge number through the local public key and generates a

```
192.168.15.131          00-0c-29-1d-21-f2
192.168.15.132          00-0c-29-12-08-cf
192.168.15.254          00-50-56-f1-7b-1d
192.168.15.255          ff-ff-ff-ff-ff-ff
224.0.0.22              01-00-5e-00-00-16
224.0.0.251             01-00-5e-00-00-fb
224.0.0.252             01-00-5e-00-00-fc
239.255.255.250         01-00-5e-7f-ff-fa
255.255.255.255         ff-ff-ff-ff-ff-ff
```

Figure 2. Target host ARP cache table before spoofing.

```
def restore_target(gateway_ip, gateway_mac, target_ip, target_mac):
    print '[*] Restoring targets...'
    send(ARP(op=2, psrc=gateway_ip, pdst=target_ip, hwdst='ff:ff:ff:ff:ff:ff', \
        hwsrc=gateway_mac), count=5)
    send(ARP(op=2, psrc=target_ip, pdst=gateway_ip, hwdst="ff:ff:ff:ff:ff:ff", \
        hwsrc=target_mac), count=5)
    os.kill(os.getpid(), signal.SIGINT)
```

Figure 3. Main code of python attack.

```
192.168.15.131          00-0c-29-1d-21-f2
192.168.15.132          00-0c-29-12-08-cf
192.168.15.254          00-0c-29-12-08-cf
192.168.15.255          ff-ff-ff-ff-ff-ff
224.0.0.22              01-00-5e-00-00-16
224.0.0.251             01-00-5e-00-00-fb
224.0.0.252             01-00-5e-00-00-fc
239.255.255.250         01-00-5e-7f-ff-fa
255.255.255.255         ff-ff-ff-ff-ff-ff
```

Figure 4. Target host ARP cache table after spoofing.

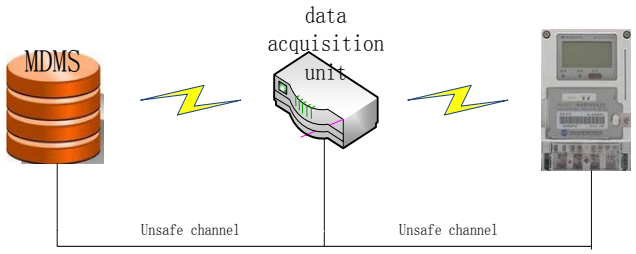

Figure 5. Structure of the meter system.

challenge code. Send it to the data center of the collection. The data center of the acquisition end decodes it into the challenge number and returns it to the smart meter data center which receives the challenge number before itself. The number of generated challenges is compared. If the comparison is the same, the authentication of the collector is successful, otherwise, the service is denied. After the data center successfully authenticates the collector, the authentication result is sent to the collection center. The collection center generates the random challenge number and encrypts the data into the data center of the power meter. The decryption, backhaul and comparison challenges are implemented. After the two authentications are successful, the meter data center transmits an acquisition instruction to the meter which requires the smart meter to transmit data. This method can effectively prevent eavesdropping and resist man-in-the-middle attacks. The two-way authentication diagram is shown in **Figure 6**.

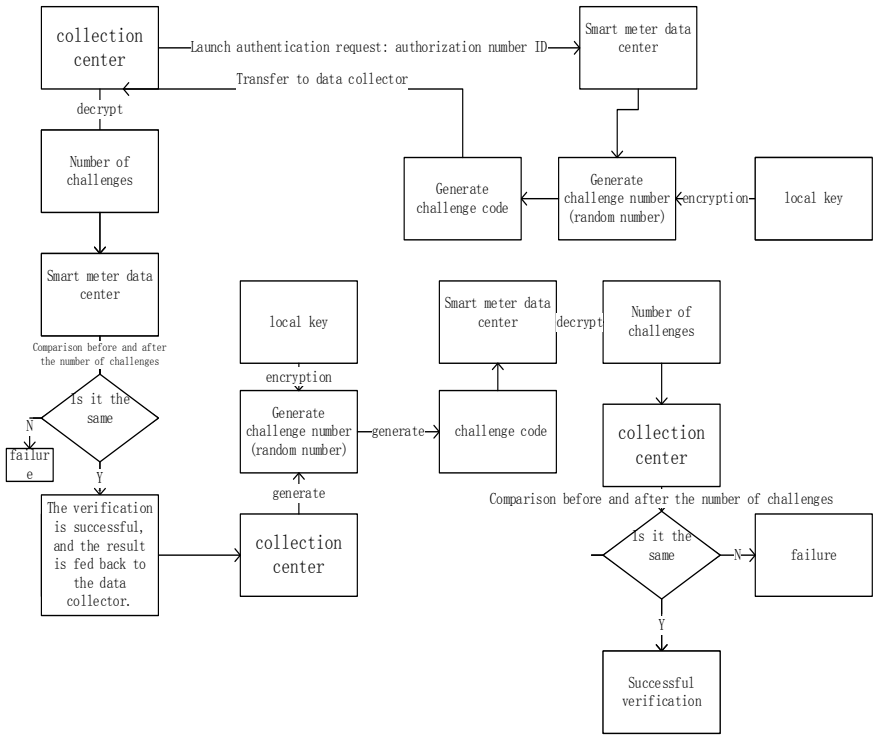

Figure 6. Two-way authentication diagram.

3.2. Data Protection of Meter Feedback

After successful authorization between data center and collector, smarter meter begins to transmit data to collector. In order to ensure the security of data transmission line, RSA encryption is needed for the collected data of smart ammeter transmission, then avoid the interception of communication data. The overall framework of the scheme is shown in **Figure 7**.

The scheme of data acquisition and protection for smart meters after successful identity authentication consists of three modules. The configuration of each parameter is shown in **Table 2**.

1) The first module is designed for the data acquisition node of smarter meter. Its main function is to detect whether the collected smart message data P is complete or not. If the data is complete, EK (encryption key) is used to encrypt the data. If the data is incomplete, the system automatically clears the incomplete data. Its purpose is to ensure that the data is complete.

2) The second module is to further process the meter data on the basis of the first module, which is called encryption module. The module uses RSA-1024 bit algorithm to encrypt the smart meter data. The core idea of data acquisition by RSA encryption module is as follows:

a) The key pair is created by the meter data collector. The complete key pair includes two parts, public key and private key.

b) In the process of smart meter data acquisition, the sender encrypts the plaintext data after receiving the public key, and forms the ciphertext C after encrypting.

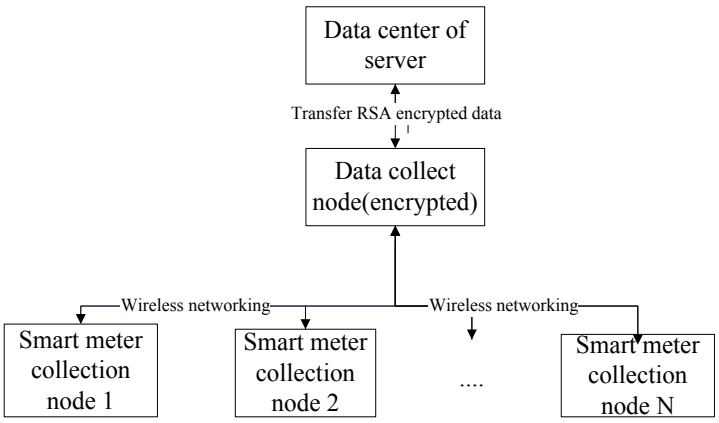

Figure 7. Structure of the anti-listening acquisition scheme.

Table 2. Encryption process input/output description.

Input		Description of the input
P	Plaintext data	Data content to be encrypted
EK	Ncryption key	A key that encrypts plaintext
IV	Initialization vector	That is, the counter CTR, which is used together with EK for plaintext encryption.
	Output	
C	Ciphertext	Encrypted ciphertext

3) On the basis of the second module, the third module transfers the processed ammeter data to the server data center, it can ensure the confidentiality of the data and effectively deal with the man-in-the-middle attack. Its core ideas are as follows.

Data collector is transferring ciphertext C to storage center or server data center. Server data center, also known as receiver, can decrypt the received ciphertext ammeter data by saving RSA private key, thus converting it into plaintext and realizing the safe transmission of ammeter data.

The data acquisition and transmission of smart meter includes 8 parts: clearing use resources, data initialization, establishing connection with meter, sending acquisition instructions, data integrity judgment, secondary processing data, transmitting meter data and decrypting data. The flow chart of the main algorithm is shown in **Figure 8**. Calling an encryption function RSA_SUAN in secondary processing of meter data.

4. Experimental Results and Security Analysis

In order to verify the feasibility of this scheme, a real test environment is built based on the topological structure diagram of **Figure 5**, it was shown in **Figure 9**. The experimental environment includes DTZY341 three-phase four-wire smart meter, DTZL341 three-phase four-wire smart meter and DDY102-Z single-phase smart meter.

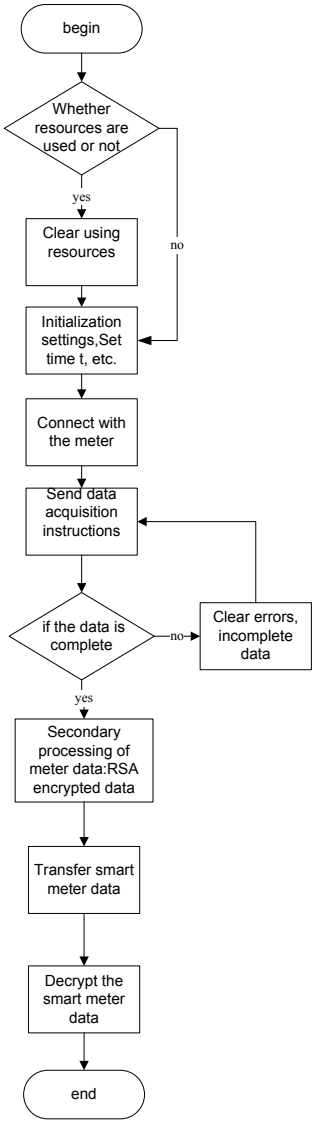

Figure 8. Flow chart of the main algorithm.

Figure 9. Smart meter data acquisition experimental environment.

4.1. Identity Authentication Core Part Testing

The results of bidirectional authentication using symmetric encryption are shown in Figure 10.

4.2. Data Acquisition Part Testing

Smarter meter data transmission in ciphertext form, it can effectively resist the problem of eavesdropping in man-in-the-middle attack. Even if the data is intercepted during transmission, the data acquired by the intermediary is those data which processed by RSA algorithm. The attacker cannot process and apply these data, thus ensuring the security of the meter communication data on the transmission line and achieving the purpose of anti-eavesdropping. As shown in Figure 11, it is the ciphertext data collected by RSA algorithm. When this part of data is needed, the client calls the reserved RSA private key to decrypt and obtain the data information.

The data collected by smart meters include voltage, current, active power, reactive power, reverse active power, reverse reactive power and other parameters. Taking the combined active power data of 41106000037 and 411060000038 as examples, the data before and after encryption by RSA algorithm are compared in Table 3.

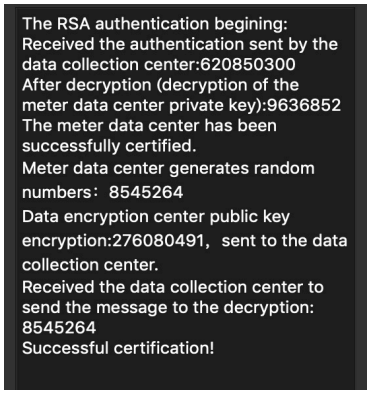

Figure 10. Identity authentication.

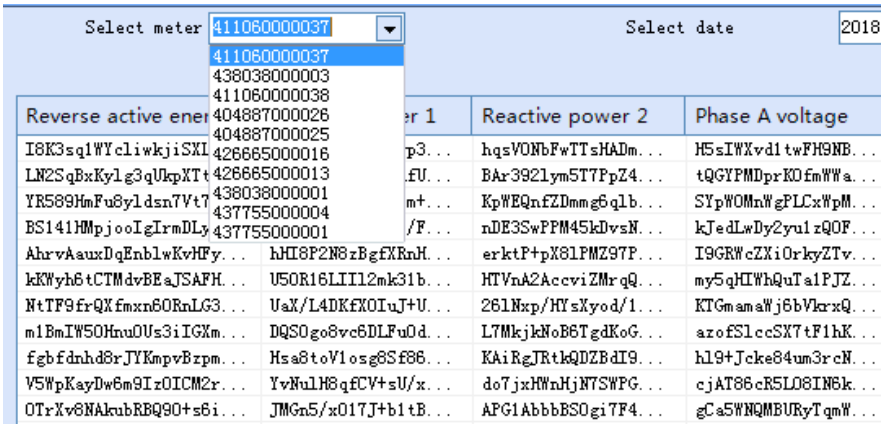

Figure 11. Smart meter communication data encrypted by RSA.

Table 3. Comparison of data before and after algorithm encryption.

Meter number	Active data	Calculated combined active data	Encrypted combined active data (Powerh)
411060 000037	6837000 60104168 91083333 3333C734 33337E16	01.94	NpRsLnpAhN5n4i9c OnotpIvZhlesPl/LiU IhLo6qL5twJI/fNbuK ffOxcoiKqU6+JCHe3 XInbcE1qE9DuRVbP rGpXprybqGsBYKIYp uQ5plyxvxOCt6CjpU 2H81IiThNVohcoqZ M0gJEEM1UsJL/xni5 0pTIesn0VKRe2zpsldo=
4110600 00038	68380000 60104168 91083333 33338437 33333F16	04.51	HgI9y5medptA/dwKfW 0eIJG2EXgjvdTgFeUIMt Jik44osBajOf4EwaIy9Eq lo3j+8XAPqZ14K/Xrm0 Fi3yAKZIr/aFj3Q/TioxT Q8owmGbix4VyxFTO+ gxldbJJQHT4hGJFdmJ3 TW33RnKxFLHs0w1rbN ho7dP5gST20uVUBFsg=

4.3. Safety Analysis

Anti-eavesdrop data acquisition and transmission system is designed for the smarter meter. It realizes two-way authentication for both sides of communication and safe acquisition of meter data for transmission, then, the problem of eavesdropping against man-in-the-middle attack and attack is realized. The safety analyzes in three aspects.

1) Two-way authentication between the collection center and the meter data center. The two-way authentication is completed before the smart meter data transmission. When the attacker maliciously pretends to be the collection and the meter data center, it will not pass, which greatly improves the security of the system.

2) RSA encryption is used for the transmitted data. If the attacker wants to use the man-in-the-middle attack to achieve the purpose, the key must be known. RSA algorithm uses a public key system, so the possibility of violent cracking by attackers is minimal. By comparing the data before and after the scheme with that in Table 4, the attacker cannot parse the data according to the DLT/645 protocol, thereby preventing the leakage of information. Therefore, the confidentiality of data collection and transmission is guaranteed, and the solution can well cope with the eavesdropping problem in the middleman attack.

3) Resilience replay attack, when performing identity authentication, the number of challenges is the random number, it generated by the meter data center and the data collection center. The purpose of this method is to ensure the uniqueness and non-repeatable authentication information. Even if the attacker acquires the authentication key at a certain time, it cannot be reused and effectively defending the authentication process.

Table 4. Data comparison before and after eavesdropping.

Pre-use data	6837000 60104168 91083333 3333C734 33337E16
Data after using this scheme	NpRsLnpAhN5n4i9cOnotpIvZhlesPl/LiU IhLo6qL5twJI/fNbuKffOxcoiKqU6+JCHe3 XInbcE1qE9DuRVbPrGpXprybqGsBYKIYp uQ5plyxvxOCt6CjpU2H81IiThNVohcoq **M0gJEEM1UsJL/xni50pTIesn0VKRe2zpsldo=**

Table 5. Security comparison.

Program	Middle Man attack	Replay attack	Tapping
Original meter collection scheme	no	no	no
Sha K. *et al.*, literature [5]	no	no	yes
Wei Yong *et al.*, literature [7]	no	no	yes
This program	yes	yes	yes

The comparison of this security method about smart meters which presented in this paper with other methods is shown in Table 5. The data acquisition method of smart meter proposed in this paper can effectively deal with man-in-the-middle attack, replay attack, eavesdropping, it has better security. In the table, "yes" means that it can resist such attacks, and "no" means that it cannot resist such attacks.

5. Conclusion

In this paper, man-in-the-middle attack with ARP deception is used to deceive the local machine to intercept normal ammeter communication data. It is verified that there are communication security problems when smart ammeter communicates with data acquisition center, from the point of view of safe communication of smart meter. According to the risk of man-in-the-middle attack being eavesdropped and replayed in data acquisition of original smart meters, using RSA bidirectional identity authentication and data encryption technology, the wireless collection and transmission of meter data are realized. It ensures the security and integrity of the collected data, avoids man-in-the-middle attack and replay attack, achieves the purpose of anti-eavesdropping and ensures the security of communication lines.

Fund

This paper was supported by the National Natural Science Foundation of China under Grant61772327, Shanghai Municipal Natural Science Foundation under Grant 16ZR1436300, Shanghai University of Electric Power, Department of Smart Grid Center under Grant A-0009-17-002-05. Shanghai Science and Technology Committee under Grant 15110500700.

Conflicts of Interest

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

References

[1] Guo, Q.L., Xin, Y.J., Wang, J.H. and Sun, H.B. (2016) Viewing the Comprehensive Safety Assessment of Information Energy System from the Blackout Event in Ukraine. *Automation of Electric Power System*, **40**, 145-147.

[2] Wei, F. (2016) Thoughts on Grid Information Security Prevention Caused by Power Outages in Ukraine. *Proceedings of the International Symposium on Smart City and Informatization Construction* II, Beijing, 1.

[3] Liu, N., Yu, X.H. and Zhang, J.H. (2016) Network Collaborative Attack: Deduction and Enlightenment of Ukrainian Blackouts. *Automation of Electric Power Systems*, **40**, 144-147.

[4] State Grid Corporation (2013) Q/GDW 1365-2013 Smart Energy Meter Information Exchange Safety Certification Technical Specification. China Electric Power Press, Beijing.

[5] Sha, K., Xu, C. and Wang, Z. (2014) One-Time Symmetric Key Based Cloud Supported Secure Smart Meter Reading. *International Conference on Computer Communication & Networks*, Shanghai, 4-7 August 2014. https://doi.org/10.1109/ICCCN.2014.6911854

[6] Deng, P., Han, G.H., Fan, B. and Sheng, Y.F. (2015) A Safe Communication Scheme for Smart Meters. *Power Information and Communication Technology*, **13**, 16-20.

[7] Wei, Y., Zhou, Q.P., Yang, B.B. and Shang, S. (2018) A Grid Resource Data Collection Scheme Based on Smart Terminal. *Electroacoustic Technology*, **42**, 58-60+82.

[8] Sun, N., He, Y.S. and Liu, J.X. (2015) Concentrator Communication Security Protection Technology Based on DLMS/COSEM Protocol. *Power Information and Communication Technology*, **13**, 120-127.

[9] Lu, B.H. and Ma, Y.H. (2013) Research on Smart Grid AMI Communication System and Its Data Security Strategy. *Power System Technology*, **37**, 2244-2249.