International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.131-144
http://dx.doi.org/10.14257/ijsia.2016.10.8.11

Secure DNP3 Services Scheme in Smart Grid Link Layer Based on GCM-AES

Ye Lu[1], Tao Feng[1,2] and Guohua Ma[3]

[1] *College of Electrical Engineering and Information Engineering, Lanzhou University of Technology, Gansu Province, China*
[2] *(Corresponding Author) College of Computer and Communication, Lanzhou University of Technology, Gansu Province, China; 5241819@qq.com*
[3] *Force-Control Huacon Technology Co., Ltd. Beijing, China;*

Abstract

This paper defines a new DNP3 link layer frame structure based on the link layer packet characteristics of transmission time requirements and security requirements in substation automation system (SAS). The new frame structure can provide three different work modes: authentication, authorization-encryption, non-authenticated encryption. Then we propose a link-layer security service mechanism in substation automation system based on the GCM-AES, including the session key agreement protocol based on EKE, GMAC-based message authentication protocol, GCM-AES Authentication Encryption-based DNP3 protocol and GCM-AES-based message transform algorithm. Through experimental calculation and analysis, the results show that the new security mechanisms achieve the efficient and safety in substation packets transmission.

Keywords*: SAS, DNP3, GCM-AES, Real-time, Security*

1. Introduction

Modern intelligent electronic devices (IED) is installed in the substation automation system (SAS) to collect, monitor and analyze the data. In the smart grid, substation automation system improves the speed of the substation interactive information sharing, but face numerous threats to network security. Xiaming Ye *et. al.*, in [1] illustrates the basic form of across space communication of CPS information security risks. Which points out that the intelligent terminal equipment is the path for safety risk transmission, the depth fusion of Information system and energy system will cause serious information security problems. All the IED equipments in the SAS system connected by way of a peer. All equipment information sharing in the local area network (LAN). Once an IED is compromised and substation has not been effective safety protection, the stability of the SAS could be under threat, and even affect the safety of the smart grid.

For the safety of the smart grid, IEC62351-5 defines the security measures based on TCP / IP communications, including authentication, confidentiality and integrity [2]. The SAS system contains the RS485 interface, Ethernet-interface and CAN bus interface, supporting MODBUS, DNP3, TCP/IP communication protocols, It is important for construction of the smart grid to form a unified system and secure client-side interaction [3]. Shahzad Aamir in [4] studied the security of SCADA system and its protocols, more specifically, SCADA/DNP3 protocol security, to achieve the study goals, a SCADA simulation environment is designed for water pumping process through connectivity of intelligent sensors, and security is deployed inside DNP3 protocol stack. Guangchao Zhi *et. al.*, in [5] proposes a secure and coordinated communication interaction process based on BACnet/IP protocol for building SCADA systems, which can protect the building

ISSN: 1738-9976 IJSIA

intelligent system from network attacks to a certain extent. Xiang Lu *et. al.,* in [6] find that, current security solutions cannot be applied directly into the SAS due to insufficient performance considerations in response to application constraints, including limited device computation capabilities, stringent timing requirements and high data sampling rates. Moreover, intrinsic limitations of security schemes, such as complicated computations, shorter key valid time and limited key supplies, can easily be hijacked by malicious attackers, to undermine message deliveries, thus becoming security vulnerabilities. Amoah *et. al.,* in [7] presents a formal model for the behavioral analysis of DNP3-SA using Colored Petri Nets (CPN). This DNP3-SA CPN model is capable of testing and verifying various attack scenarios: modification, replay and spoofing, combined complex attack and mitigation strategies..

The DNP3 statute which widely used in the field of substation automation systems has proven to be unsafe. Samuel *et. al.,* in literature [8] already stated DNP3 protocol has vulnerability in the respective communication layer. They found and classified the attack occurred include: eavesdropping, data tampering and forgery data. David *et. al.,* in literature [9] through continuous sending unsolicited information to event buffer launched a denial of service attack to DNP3 protocol. [10] established a small test bed and simulation a series of attacks for DNP3 protocol experiments in SCADA systems. The results show that there are many security flaws in DNP3 protocol such as replay attack and middleman attacks. DNP statute also conducted a series of security improvements. Its two latest improved version was DNPsec and DNP3-SAv5.

The frame structure of DNPsec link layer encapsulates a new header, a new serial number and a data authentication section. Using a session key to encrypt and authenticate data frame. Update session key is determined by the serial number of frame and the session lifecycle. 3DES and HMAC-SHA1 algorithm was use to realize data encryption and authentication separately. However, security strength of 3DES and SHA-1 in the literature [11-12] has been determined not high and low operating efficiency. In addition, in the electric power SCADA system, many devices do not have enough storage space and computing speed to handle the encryption and authentication algorithms respectively.

DNP3-SAv5 did not provide data encryption and authentication algorithms in detail. However, it proposed a multi-user authentication policy. Currently, there are some new possible authentication schemes proposed by researchers. [13] proposed public key authentication scheme based on ECC According to the characteristics and structure of the SAS System DNP3 protocol, which can provide lightweight, high real-time, multi-user authentication service. DNP3-SAv5 protocol did not specification defines the data is not encrypted, DNP3-SAv5 protocol does not define the data encryption standard, vulnerable to eavesdropping attacks. Because the DNP3-SAv5 protocol does not encrypt the data, Similar to the Stuxnet can collect sensitive data, which leads to information leakage [14].

According to the characteristics of different message types in substation automation system (SAS), the paper designs the frame structure of DNP3 protocol, which is based on the characteristics of transmission time requirement and security requirement. The new frame structure can provide authentication, authentication-encryption and Non-authenticated-Non-encrypted by three different modes of operation. Based on the new frame structure of DNP3 protocol, this paper proposes the interactive process and encryption process of DNP3 protocol based on GCM-AES. GCM-AES is a kind of efficient and safe encryption algorithm which can be realized by software and hardware, and already be proved secure and has no patent. It is especially suitable for the environment with strict requirement of network transmission delay. GCM (Galois / Counter Mode) compared to other authentication encryption algorithm is fast and the low hardware cost [15]. Based on the experimental analysis and calculation, the new protocol has been implemented to achieve high efficiency and secure transmission.

2. SAS Link Layer Frame Classification

2.1. Classification by Transmission Time Characteristics

In the SAS system, the packet is divided into 7 kinds according to the transmission time characteristic: ①Fast speed packet, ②trip message, ③medium speed message, ④low speed packet, ⑤original data packets, ⑥file transfer message, ⑦time synchronization packets. Figure 1 shows the mapping of the various types of packets in the network structure. SMV: sampling survey value, GOOSE: substation event, Time-syn: time synchronization, MMS: manufacturing message specification.

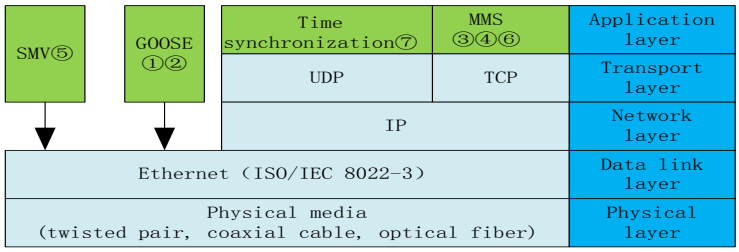

Figure 1. DNP3 Packet Classification

The①②⑤ packets are non routing multicast data, which transform through the internal network of substation, These messages require high real-time and short transmission time. In particular, the class①②messages transmission time is less than 4ms[16]. Other③④⑥ ⑦class of message are some service message, which across the network of multiple levels, real time is low.

Table 1. Classification based on the Transmission Time Characteristic

Category	PDU size	Transport type	Transport requirements	Real time
GOOSE①②	1500B	Multicast	<4ms	high
SMV⑤	1500B	Multicast	Based on the stream	high
MMS③④⑥⑦	>3000B	Connection-oriented	No demand	low

2.2. Classification by Transmission Safety Characteristics

Taking into account the real-time of SAS System, we need to take appropriate cryptographic authentication scheme according to the different time characteristics of packets to ensure the real-time and safety of system. Secure transmission requirements for different data packets is showed in Table 2.

Table 2. Classification based on Transport Security Features

Category	Certificate	Confident	Tamper detection	Mode
GOOSE①	Do not need	Need	need	NULL
GOOSE②SMV⑤	Do not need	Need	need	GCM
MMS③④⑥⑦	need	Not need	need	GMAC

GOOSE message is mainly to protect the control class data, efficiency improvement method of generating verification code is proposed in the paper [17], which move the content of the GOOSE message to the end part and reduce most of the computation time in the HMAC method. The GOOSE message is divided into two categories, one is the high security requirements of tripping command message, which only check the message integrity and reliability of the source, in order to improve the efficiency of data transmission with highest integrity and timeliness requirements and use GMAC authentication mode. Another type of message that does not require security protection, they are transported directly with non encrypted authentication to reduce network traffic.

SMV messages are power quality measurement and data packets, which packets flow is high. To send and receive information on both sides of the identity authentication also need to use the GMAC model.

MMS messages within and outside the substation are interaction packets. The security requirements of the message is highest, and real-time is relatively low, easy to be invaded by the external network. We should adopt GCM encryption authentication mode with the double protection of the authentication and encryption. MMS packets through the power dispatching network to the substation layer, process layer, equipment layer, Cross the application layer, network layer should also be combined with the network layer of IPsec, transmission layer of TLS, application layer of SSL and other technologies to further improve the security of information transmission.

3. New DNP3 Link Layer Frame Structure

The DNPsec protocol link layer frame format is used to achieve authentication and encryption. The frame format is shown in Figure 2.

New Header				Key sequence Number	Original LH Header					Payload Data		Authentication Data
Dest Add	MK	SK	Reserved	4bytes	sync	len	Link control	Dest Add	Source Add	TPDU	Pad data	ICV

Figure 2. DNPsec Link Layer Protocol Packet Format

In this paper, we combine the IEC62351 standard and the advantages of the link layer message in the DNP3sec standard, redefines the DNP link layer frame structure based on the GCM encryption authentication scheme. Its frame structure is shown in Figure 3.

New Header						Key sequence Number	Original LH Header					Payload Data		Authentication Data	
Dest Add	MK	SK	a	b	Function code	4bytes	sync	len	Link control	Dest Add	Source Add	TPDU 17-144	Pad data	Seqnum 4bytes	ICV

Figure 3. Improved DNPsec Link Layer Packet Format

20 bytes of the authentication field is divided into two fields: 4 byte sequence number field and 16 bytes of MAC field. Sequence number field SN was corresponding to the SN field of GOOSE message in IEC61850 standard. In the first new fields we redefined the third bit and fourth bit of third byte as a, b in original part, and define the Reserved field to Function field, the field of meaning as shown in Table 3.

Table 3. Function Code Definitions

Null Request	GCM Request	GMAC request	NULL Response	GCM Response	GMAC Response
00	2F	30	80	8F	90

Other fields are in agreement with the original DNPsec protocol. The ‘a’ indicates whether to use the encryption scheme, The ‘a’ represents the encryption mode. Table 4 describes the encryption mode for the different combinations of the two. The original DNPsec message is set by ‘a’ is 0 and ‘b’ is any, which is non encrypted-non authentication scheme, the message was send as Plaintext, as NULL model. The GCM mode is set by a=1 and b=1 which is the encryption authentication mode. The GMAC mode is set by a=1 and b=0 which only use certification.

Table 4. The New Header a, b Field Packet Encryption Mode

Mode	a	b	Encryption Authentication	Message Type
NULL	0	Any	no need	GOOSE①
GCM	1	1	need	GOOSE②、SMV⑤
GMAC	1	0	only certification	MMS③④⑥⑦

4. New Link Layer Security Service Mechanism

4.1. Message Communication Protocol with No Safety Protection

Under the NULL model, GOOSE① message is sent directly without safety protection for reducing network traffic. The interaction process is shown in Figure 4. 80 (see Table 3) is message response function code of the Null mode.

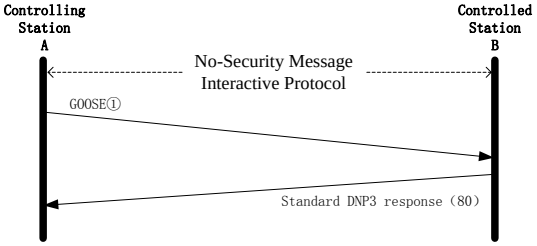

Figure 4. No-Security Message Interactive Protocol

4.2. Link Layer Session Key Agreement Protocol

The mode of GCM and GMAC need a session key. In the initial stage, the protocol interacts with the request response mode. The current session key is determined by the update key state and session key security period. When the session is established, by the type of transmission data, the protocol uses different GCM encryption authentication algorithm to achieve the synchronous transmission and encryption of data and realize the corresponding function processing in the controlled end. By the end of the session or the end of the session key security period, the session key will be updated to achieve the continuous transmission of data. The security period of session key can be dynamically set by the frequency of the data exchange. This scheme using enhanced EKE protocol as the authentication key exchange protocol, which is divided into the following six steps.

Step 1.A→B: A generates a random key K_A. Use the symmetric algorithm and the premaster shared key P_{AB} to encrypt K_A . Send the result $E(P_{AB,}K_A)$ to B.

Step 2.B→A: B decrypts the message with a premaster shared key P_{AB} to get K_A, Then generate a random key K_B, using the random key K_A and P_{AB} to encrypt K_B and send the result $E(P_{AB} ,(E(K_A,K_B)))$ to A.

Step 3. A→B: A decrypt the message $E(P_{AB},(E(K_A,K_B)))$ to get K_B and generate a random number R_A and S_A with K_B encryption. Send the result $E(K_B,R_A||S_A)$ to B.

Step 4. B→A: B decrypt the message $E(K_B,R_A||S_A)$ to get R_A and S_A, and generates a random number R_B and S_B, then encrypt R_A, R_B and S_B by K_B and sent the result $E(K_{B,}R_A||R_B||S_B)$ to A.

Step 5. A→B: A decrypt the message $E(K_{B,}R_A||R_B||S_B)$ to get R_A, R_B and S_B, assuming that the R_A obtained by A was the same to the R_A sent to the B in step3, then A encrypt R_B and S_B by K_B and sent the result $E(K_{B,}R_B||S_B)$ to B.

Step 6. B: B decrypt the message $E(K_{B,}R_B||S_B)$ to get the R_B, if the R_B was same as the step 4 sent to the A. Then this Agreement establishes the session key. Now the two sides use Ks=SA⊕SB as the session key.

Each node has the number of n-1 master keys at most, as much as the desired session keys. The time of using the master key is very short, so it is difficult to analyze the key.

The session key is used to protect the message within a limited time, and the session key is updated at the end of the survival period. Session key agreement protocol based on EKE as shown in Figure 5.

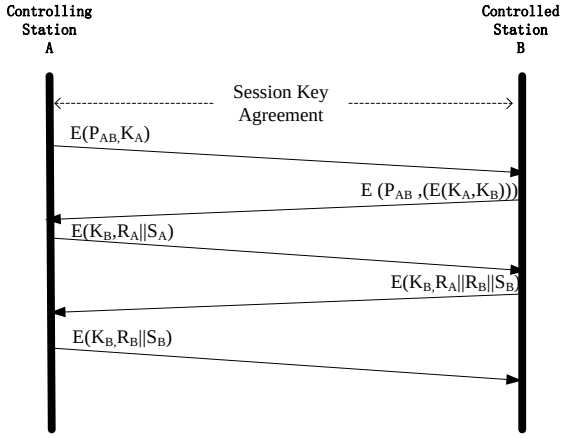

Figure 5. Session Key Agreement

4.3. Link Layer Authentication Protocol

SMV⑤ message are some measurement data message with large amount of data, Transmission adopts the GMAC message authentication protocol to meet the real-time requirements. GMAC algorithm use the session key K_S generated in the section 3.2 to authenticate message and generat message authentication codes T. The SMV⑤ message is divided into a number of unit m_i,which length is 128 bits. Message $M=(m_1,m_2,\ldots,m_n)$, $0<n<239-256$, K1 is a constant number, can be R_b or R_{b+1}. $MSB_{Tlen}(X)$ means the left Tlen bits of X. GMAC (K_s,M, K_1) is Calculated as follows:

$$C_1=E(K_S,m_1)$$
$$C_2=E(K_S,m_2 \oplus C_1)$$
$$C_2=E(K_S,m_3 \oplus C_2)$$
$$\ldots$$
$$C_n=E(K_S,m_n \oplus C_{n-1} \oplus K_1)$$
$$T=MSB_{Tlen}(C_n)$$

Message authentication protocol is shown in Figure 6, which is divided into the following three steps:

Step 1. A→B: A generates a random number R_b. Use GMAC algorithm to generate T= GMAC (K_s,M,R_b) and Send the result M||R_b||T to B.

Step 2. B→A: B recieve the message M||R_b||T. Use GMAC algorithm to generate T′= GMAC (K_s,M,R_b), if the T=T′, then R_b+1, B send the result T′=GMAC (K_s,R_b+1,90) to A.

Step 3. A: A calculate GMAC(K_s,R_b+1,90) to get T′ ,if the T′ transform in 2 times is the same, it means B received the message M.

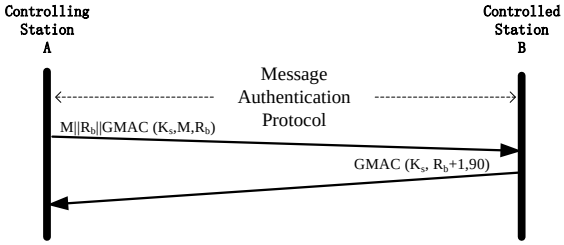

Figure 6. Message Authentication Protocol

4.4. Link Layer Authentication-encryption Protocols

A high speed hardware structure based on GCM is studied in the [18]. The throughput rate of the algorithm is reach to 97.9Gbit/s. At present, the throughput rate of the GCM algorithm has reached 162.56Gbit/s [19]. GCM used counter mode to realize encryption and use the norm Hash function in Galois field to realize authentication service at the same time, which can provide data confidentiality, integrity and authenticity. The program uses AES for data encryption and decryption, and use GHASH for authentication, which is more secure, reliable and suitable for the industrial network. The scheme was accepted by NIST as the main algorithm of industrial network security[20] for the low operation rate and less storage space of data link layer encryption. The [21] gives a definition of the data and function of GCM algorithm.

Definition of GCM algorithm:

Encryption function: $GCM(P,A,K_s,M)\rightarrow(M`,T)$

Decryption function: $GCM(P,A,K_s,M`,T)\rightarrow M$

Vector $P=(P_1,P_2,\ldots P_n)$, $1<n<264$, P is the initial vector, for a fixed key, the initial vector must be unique. The message sequence number is used as the initial vector of the algorithm.

Additional authentication data: $A=(a_1,a_2,\ldots a_3)$, $0<n<2^{64}$. Using LH Header Original as an additional authentication data, the part can only be certified and can not be encrypted
。

Message $M=(m_1,m_2,\ldots,m_n)$, $0<n<2^{39}-256$. M is IED ready to send the GOOSE type data. Where each M is 128 bits, the deficiency is zero.

GCM encryption and decryption algorithm mainly consists of two operations: CTR encryption-decryption and norm hash authentication, The CTR encryption and decryption using XOR operation of the initial vector P and M plaintext, HASH certification was realized by GHASH function.

The authentication and encryption algorithm of data link layer does not encrypt the header field of the message. The purpose is to protect the communication between the two sides from affecting by the impact of encryption and to use VLAN in the future.

According to the data type of the goose, the sender first send the package to the data link layer, Encryption mode was set by Set_Reserved (a, b) function, the GOOSE message number was set to SN by Get_seqnum () function. Before the authentication and encryption, the additional authentication data A is calculated by the function Value (Original LH Header), then the encryption function is called to encrypt the message. Figure 7 shows the flow chart for the GOOSE message when it is sent.

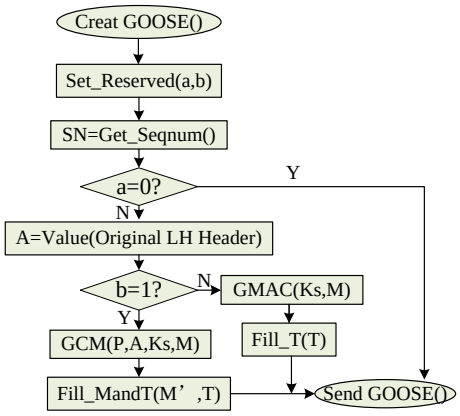

Figure 7. GOOSE② Message Conversion Algorithm

Encryption function GCM (P,A,K_s,M) was set according to the following 7 steps, the output is the 128 bit of cipher text M' and 16 bytes of verification code T.

step1: M=$m_1||m_2||\ldots||m_n$; Dividing the message M every 128 bits for a APDU, and the rest bit zero.

step2: H=E(K_s,M);

step3: P=GHASH(H,A,SN); Initialization vector P.

step4: for i=1 to r, do y_i=yi-1++,m_i'=$m_i \oplus E(K_s,y_i)$; m'_i was calculated by the encrypted P_i XOR plain text m_i.

step5: $m_n'=m_n \oplus MSB_{|mn|}(E(K_s(y_n)))$, Calculate the last paragraph of the cipher text.

step6: $M'=m_1'||m_2'||\ldots||m_n'$; Connect each cipher text and output.

step7: T=MSB16(GHASH(Ks,H,A,M′)⊕E(Ks,P0)); Calculating the output of 16 bit verification code. Authentication encryption algorithm as shown in Figure 8.

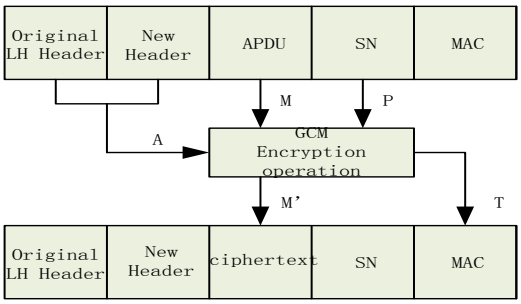

Figure 8. Message Authentication-Encryption Algorithm

Authentication-Encryption protocol will be divided into the following three steps shown in Figure 9:

Step 1. A→B: A use GCM algorithm and K_s to encrypt P,A,M by function GCM(K_s,P,A,M). Then Send the result P||A||M′||T to B.

Step 2. B→A: B decrypt the message M′ to get M, then calculate Authentication codes T′, if the T=T′,B encrypt 8F and send the result E(K_s,8F) to A.

Step 3. A: A decrypt the message to get 8F, The communication finish.

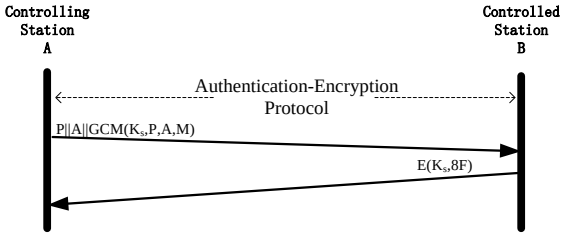

Figure 9. Authentication-Encryption Protocol

5. Security Analysis

In this paper, the security transmission method proposed by SAS system is able to verify the authenticity and integrity of the original data packet, and ensure the consistency of the data packet from the sender to the receiver. The network protocol security framework based on AES encryption algorithm and dynamic session key update scheme can hide data frame source address and prevent data from being tapped.

We set up a small protocol test bed, including a master station, an outstation and an attacker, which use the OpenDNP3 Library, GCM GSL 1.16 (GNU Scientific Library) and OPENSSL based on Visual Studio2015 Lib. We simulate two kinds of attacks: eavesdropping attacks and camouflage attacks, and analyzes the other three types of attacks.

Anti-eavesdropping attack: figure 10 shows the use of Wire-shark to monitor object data DNP3, Although we sniff the protocol packet. However, we could not parse the protocol of real data, because we cannot obtain the session key, and crack AES encryption algorithm. Among them, code function is 0x90, which is the authentication response function code.

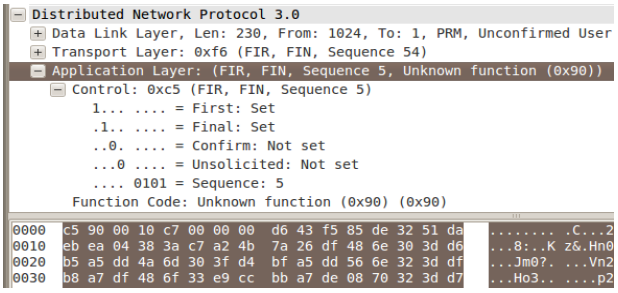

Figure 10. Wire-shark Sniffing DNP3 Object Data

Anti-camouflage and middle attack: If an attacker pretends to be a local user, he needs to obtain a session key, a password and a certificate to calculate the correct response data. Because the security of AES algorithm and Non reversible of GHASH algorithm, obtaining keys, certificates and user passwords seems to be unrealized. Figure 11 shows the authorization certificate does not match, the external substation refused the connection request of non certified master station. When the master station change to the correct authorization certificate, connection is established rapidly.

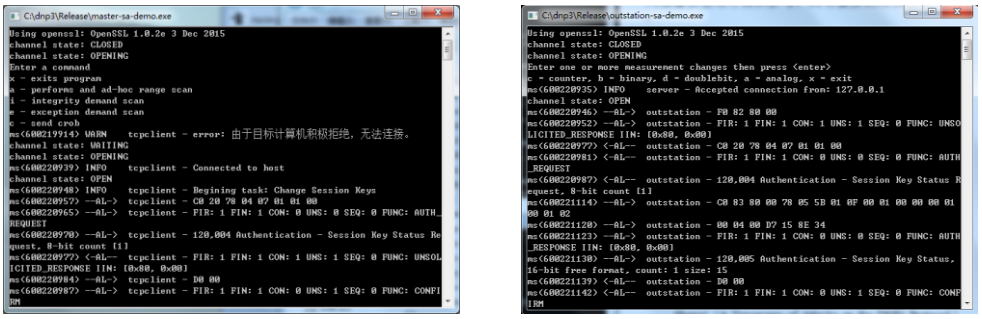

Figure 11. Master Station and Out Station Connection

Anti replay attack: as the time stamp of the replay attack is far away from the current time of the system, and the sequence number for the message has been used, the current receiver uses the session key cannot verified replay packet of GHASA authentication code. If the attacker wants to implement replay attack, it must obtain the initial key of data packet to calculate the session key. Since the initial key is configured before the transmission, the attacker can not obtain or calculate it, thus the receiving end can not match the appropriate session key, which directly discard the replay attack packets.

Anti-traffic attack: because the message is encrypted in each of the intermediate transmission nodes, so all the data in the link, including the routing information, appear in the form of the cipher text. In this way, the link encryption covers the source and destination of the transmitted message. Due to the filling technology and the fill character can be encrypted without the need for transmission, which makes message frequency and length characteristics to be covered up, so as to prevent the analysis of business communication.

Anti-internal attacks and denial of service attacks: When applying a multi factor authentication and attribute based authorization scheme in the application layer, Protocol can resist insider attacks to some extent. Because only authorized users have access to the IED, it can also defend DOS attacks in a certain extent.

6. Time Analysis

We use the GOOSE information exchange as an example, the GCM authentication encryption algorithm is used in data link layer, Make the Δ as maximum time of single message processing overhead. The entire transmission time overhead of the message is shown in Figure 12.

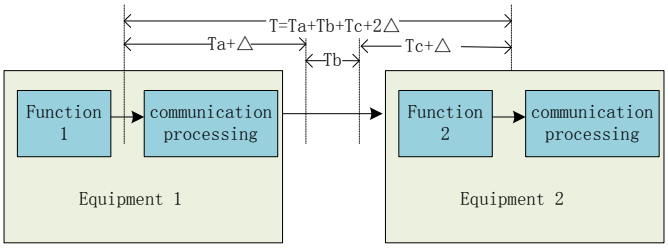

Figure 12. GCM-AES Algorithms Packet Time Overhead

Definition: The total end-to-end delay $T=T_a+T_b+T_c+2\Delta$

1. T_a and T_b is the packing time of node protocol package.

2. Δ is the GCM algorithm encryption authentication time overhead, $\Delta \geqq 0$.

3. T_b is the transmission time, which depends on the network bandwidth and the type of Ethernet.

GCM algorithm encryption speed in Literature [19] is 100Gbits/s.The maximum time of single encryption is 0.015us.So 0≦Δ≦0.015us. Total time to encrypt and decrypt is 2Δ=0.03us. Its ratio between encryption-decryption time and the maximum transmission time is $2\frac{\Delta}{4\text{ms}} = 7\times10^{-6}$。The ratio is very small, and with the speed of the GCM-AES algorithm is more and more fast, encryption and decryption time can be ignored.

We use Visual Studio2015 to write a console application of GCM authentication encryption algorithm by c++, verified the time consumption by calculating the single encryption-decryption. By using the method of 1000 times of cyclic encryption-decryption. Initial key KEY:16bit using 1111111111111111, initial vector SN: 4bit using 2222, additional authentication data A: 26bit, Plaintext M: 1152bit. Adata Input and Pdata Input: input 1 means to automatically add 26bit and 1152bit random data. Echo 0 indicates that the loop do not displayed the encryption-decryption process. Figure 13 shows the experimental result.

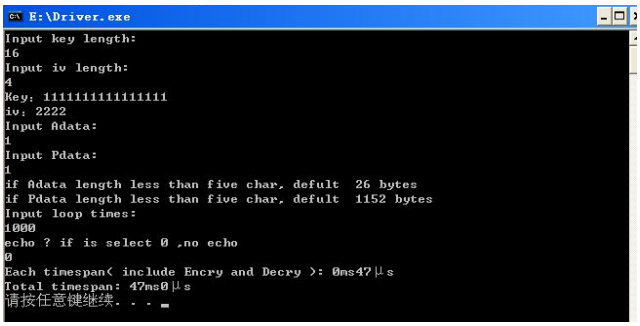

Figure 13. Timeliness Verify Results

Finally, the total time of the encryption-decryption time is 47ms, a single time of encryption-decryption calculated is 47us. Which is far less than the maximum transmission time 4ms of the GOOSE message allowed, the ratio is 47us/4ms=11.75/1000, considering the influence of the system load to performance of CPU in common PC, the results of value is bigger than theoretical calculation. If we choose a faster computer, the ratio of time overhead of encryption-decryption for maximum transmission time 4ms of GOOSE packets can be made lower and lower, so GCM algorithm can be used for GOOSE message security transmission of encryption-decryption. In this paper, we further compare three kinds of encryption-decryption algorithms, time overhead is shown in Figure 11, the results show that the time overhead of the GCM-AES encryption scheme is the minimum.

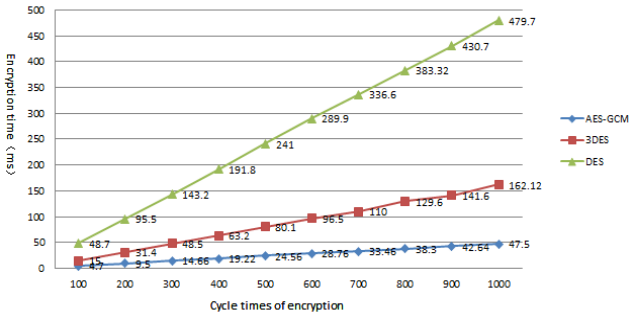

Figure 14. Time Cost Comparison Results

7. Conclusion

The paper combines the advantages of the link layer packet IEC62351 standard and DNPsec standard, defined DNPsec link layer frame structure based on GCM-AES encryption authentication scheme, realize secure transmission of link layer in SAS system by three modes of encryption-authentication algorithm, analysis the maximum transmission delay. The scheme can match the real-time requirements of all kinds messages in IEC61850 power communication protocol. However in view of the high security requirements of MMS, the next step of research work still need to use application layer SSL, transport layer of TLS and network layer IPSec technology to achieve interactive message transmission safely between internal and external network. In addition, multi factor authentication and access control based on role should be considered in the remote substation control system. The link layer encryption authentication scheme proposed in this paper can provide reference for the safe operation of power grid.

Acknowledgements

Thanks are due to Xian Guo for assistance with the experiments and to Jing Wang for valuable discussion. We are deeply indebted to all the other tutors and teachers in Translation Studies for their direct and indirect help to me. This work was supported by the National Natural Science Foundation of China (NSFC 61461027, 61462060)

References

[1] X. Ye, F. Wen and J. Shang, "Propagation Mechanism of Cyber Physical Security Risks in Power Systems", The Journal of Power System Technology, no. 39, **(2015)**, pp. 3072-3079.
[2] IEC/TS 62351-1: Power systems management and associated information exchange-data and communications security: part 1 communication network and system security-introduction to security issues, **(2007)**.
[3] W. Qiu, D. Guo, C. Zhang, Y. X. Xu and G. Wang, "A Smart Grid Client-side Testing Platform for Monitoring", Mathematical Modeling of Engineering Problems, no. 2, **(2015)**, pp. 17-20.
[4] A. Shahzad, K. P. Udagepola, Y.-K. Lee, S. Park and M. Lee, "The sensors connectivity within SCADA automation environment and new trends for security development during multicasting routing transmission", International Journal of Distributed Sensor Networks, no. 36, **(2015)**, pp. 2244-2249.
[5] G. Zhi, F. Zeng, H. Liu and F. Kuang, "Realization of The Communication Between Devices of BACnet/IP and Real-time Database", Review of Computer Engineering Studies, no. 1, **(2014)**, pp. 17-22.
[6] X. Lu, W. Wang and J. Ma, "Authentication and Integrity in the Smart Grid: An Empirical Study in Substation Automation Systems", International Journal of Distributed Sensor Networks, no. 27, **(2012)**, pp. 279-292.
[7] A. Raphael, C. Seyit and F. Ernest, "Formal modeling and analysis of DNP3 secure authentication", Journal of Network and Computer Applications, no. 59, **(2016)**, pp. 345-360.
[8] S. East, J. Butts, M. Papa and S. Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol", Critical Infrastructure Protection III, Springer Berlin Heidelberg, no. 44, **(2009)**, pp. 67-78.
[9] D. M. Nicol, D. Jin and G. Yan, "An event buffer flooding attack in DNP3 controlled SCADA systems", Proceedings of the 2011 Winter Simulation Conference, Winter Simulation Conference, **(2011)**, pp. 2614-2626.
[10] D. Lee, HajJu Kim and K. Kim, "Simulated Attack on DNP3 Protocol in SCADA System. The Institute of Electronic", Information and Communication Engineer, no. 17, **(2014)**, pp. 21-27.
[11] T. Radu and S. Mircea, "Evaluation of DES, 3 DES and AES on Windows and UNIX platforms", International Joint Conferences on Computational Cybernetics and Technical Informatics, Proceedings, **(2010)**, pp. 119-123.
[12] M. Stéphane, "Classification and generation of disturbance vectors for collision attacks against SHA-1, Designs, Codes and Cryptography", no. 59, **(2011)**, pp. 247-263.
[13] B. Vaidya, D. Makrakis and H. T. Mouftah, "Authentication and authorization mechanisms for substation automation in smart grid network", IEEE Network, no. 27, **(2013)**, pp. 5-11.
[14] M. Naiara, M. Elías, L. Jesús, J. Eduardo, A. Astarloa, "Cyber-security in substation automation systems", Renewable and Sustainable Energy Reviews, no. 54, **(2016)**, pp. 1552-1562.
[15] D. McGrew and J. Viega, "The Galois/Counter mode of operation (GCM) Submission to NIST", **(2004)**.

[16] J. Ding, H. Xi and A. Chen, "Research on Substation Automation System Based on IEC62351 Security Standards", Power System Technology, no. 30, **(2006)**, pp. 345-348.
[17] Z. Wang, G. Wang and Z. Xu, "An HMAC Based Authenticated Method for GOOSE Packets", Power System Technology, no. 39, **(2015)**, pp. 3628-3633.
[18] J. Zhao, L. Li and H. Pan, "High-Speed Hardware Implementation for GCM in IEEE802.1AE", Journal of Electronics & Information Technology, no. 32, **(2010)**, pp. 1515-1519.
[19] Satoh A., "High-speed parallel hardware architecture for Galois counter mode", Proceedings of IEEE International Symposium on Circuits and Systems, New Orleans, USA, **(2007)** May 27-30, pp. 1863-1866.
[20] Encryption modes development. Submission to NIST, Accessed: **(2013)** November 21st.
[21] W. Stalling, Editor, Cryptography and Network Security. Prentice Hall Publishers, New Jersey, **(2003)**.

Authors

Ye Lu, male, doctoral student. He received the Master's degree from the Lanzhou University of Technology. His research interests include Industrial system communication security and cryptographic.

Feng Tao, male, researcher, doctoral tutor. He received the Doctor's degree from the Xidian University, Native of Vice president of computer and communication, Lanzhou University of Technology. A senior member of China computer society, a member of China cryptography society. His research interests include Network Information Security and cryptographic.

Guohua Ma, male, senior engineer, the main research directions: industrial automation and security.