An Information Security Control Method of Smart Substation

Jin Wang[1, a], Lei Su[1, b], Wei Li[1, c]

[1] STATE GRID Hubei Electric Power Research Institute, Wuhan, 430077, China

[a]email: syywangjin@qq.com, [b]email:sulei.sgcc@gmail.com, [c]email:89283643@qq.com

Keywords: Smart Substation; Evolution Ring; Message Security.

Abstract. The three layer equipment of IEC61850-compliant Smart Substation connecting directly to the Ethernet for the benefit of information transmission and sharing. However, it also brings certain information security risks. This paper proposes evolution ring based message security control scheme, which uses the high-speed hardware encryption core to ensure the security of GOOSE, SV and MMS messages. The result of time consuming analysis indicates that the proposed scheme can not only guarantee the security of messages, but also meet the message real-time transmission requirements of Smart Substation.

Introduction

With increasingly sophisticated Smart Substation related technologies, deployment of Smart Substation gradually enters the era of large-scale practical phase. [1] Power control system and information network have been applied in copious area, and their communication protocols have been standardized. These developments lead information communication more vulnerable to be hacked than ever before, which rise the new challenge in security and reliability of the power control system and its data network.

Smart Substation applies the international standard, IEC61850 protocol, as standard communication protocol to ensure that four telemetry signals which transmit in the network comply with communication specification, and intelligent control of Smart Substation can be accomplished.[2] In Smart Substation construction and operation stage, stability and reliability of network and accuracy of information communication among IEDs are vital to the success commissioning of Smart Substation. This requires Smart Substation not only capable of real-time analysis, monitoring, manage and forecast network operation status and communication among numerous IEDs, but also ensure integrity and accuracy of network transmission of signal. This is the urgent and necessary demand for Smart Substation operational security because power grid safeguard nations’ normal operation and civilians’ social life. Once there is a security exploit in smart grid, it may jeopardize the important facility in the network, or even worse, severe sabotage nation’s normal production that may cause the loss no less than the result of a war. The standardization and intelligent of network signals control make Smart Substation more vulnerable to be attacked than ever. Hence, how to manage the information security of Smart Substation is inevitably became a national level research issue that serves the country’s fundamental interests. [3]

Smart Substation Network Message Security Analysis

Smart Substation, a prominent node for smart grid, is responsible for electricity transmission and distribution. Whether the message transmit in the Smart Substation is safe and reliable is crucial to the stability and reliability of power system. At present, there are three types of message in Smart Substation,[4-5] GOOSE (Generic Object Oriented Substation Event) message, SV (Sampled Value) message and MMS (Manufacturing Message Specification) message, all have its security threats. Fig.1 illustrates how these three types of message are mapping and transmitting in IEC61850 protocol.

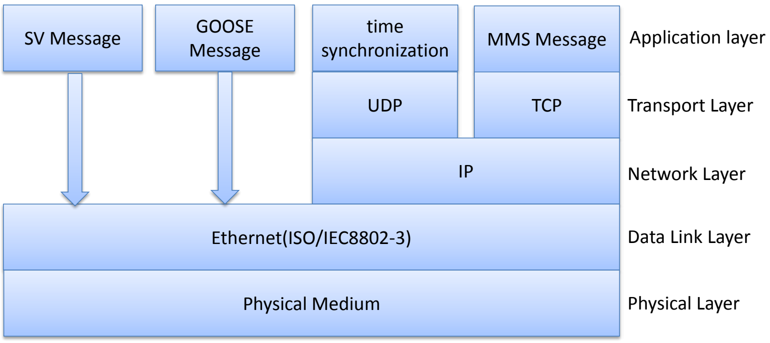

Fig.1 IEC 61850 Message Mapping

GOOSE applies to important protection message such as trip signal and it must reach the destination within a specific time frame, normally less than 4ms. In order to ensure real-time service, GOOSE message bypass network layer protocol and directly transmit through Ethernet link layer with priority Ethernet message forwarding method. SV message, which delivers data source for protection devices, is the foundation for protection devices to fulfill its function, hence the accuracy and speed of sample value is significant. Both SV and GOOSE are directly mapped to the Ethernet protocol stack. MMS, which serves as basis to ensure four telemetry signals, use a set of international message standard for real-time data exchanging and information monitoring among smart devices in heterogeneous network environment. As a message transits between substation internal and external network, MMS may be easily exploited by intruders, hence a high security level is demanded. As shown in Table 1, these three types of message need different levels of security clearance.

Table 1 Security criteria of messages

Security Requirement	GOOSE	SV	MMS
Identity Authorization	No	No	Yes
Encryption	Yes	No	Yes
Tamper Verification	Yes	Yes	Yes

Smart Substation Information Security Control Solution based on Evolution Ring

According to aforementioned analysis of message security requirements of Smart Substation network, this paper proposes an information security control solution based on evolution ring. As illustrated in Fig. 2, this method includes four major steps: VLAN division, base generation & action, message encryption and message decryption. VLAN division ensures that message only available within the specific ring to avoid unnecessary exposure from outside attack; Dynamic base key is generated by time window and voting mechanism; security control of message encryption and decryption are accordance with updated base key, and conduct timing status verification for the message simultaneously.

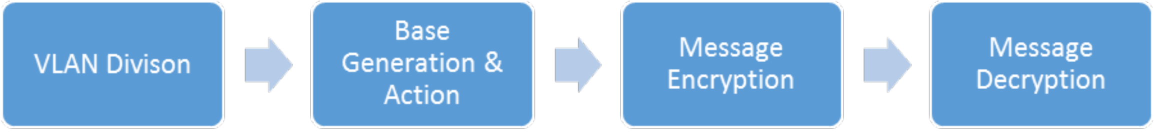

Fig. 2 Framework of security control method in Smart Substation based on evolution ring

VLAN in Evolution Ring.

VLAN (Virtual Local Area Network) technology can separate a physical LAN into several logical VLAN. Each VLAN is comprised of a group of identical demand computer workstations. As shown in Fig. 3, the internal broadcasting and unicast streaming in a VLAN will not forward to other VLANs, which helps to control network traffic and partially reduces the scope of vulnerable message to an acceptable range, thus intensifies the network security. In order to have sufficient protection in grid security, it is necessary to encrypt the sensitive message before transmission.

VLAN is divided on account of different voltage levels in Smart Substation, and segregates the

Smart Substation network into different rings served as the basic component for information control.

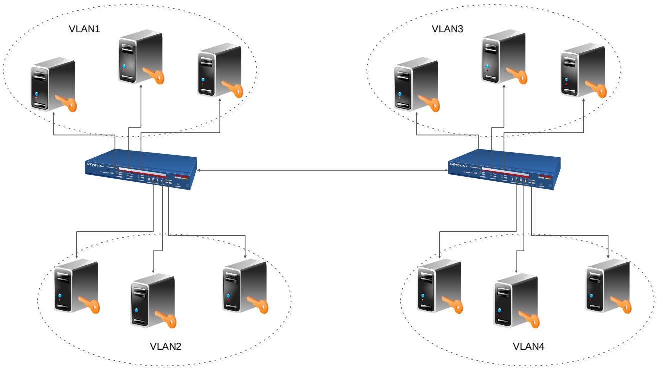

Fig. 3 Illustration of VLAN

Base Generation & Action.

The process of base generation and base action (Fig. 4) includes following steps:

Step 1: Divide VLAN on account of different voltage levels in Smart Substation, and segregates the Smart Substation network into different rings $R_i,\ i=1,\ 2,\ldots,S$, here S represents the number of ring.

Step 2: Assume each ring R_i has several nodes $N_{i,k},\ k=1,\ 2,\ldots,M$, here M represents the number of nodes in ring R_i, set variable time window as W_i.

Step 3: For ring R_i, at interval W_i, each node $N_{i,k}$ in the ring vote one node as base B_i of the ring R_i according to the default voting mechanism.

Step 4: Base B_i generate base key BK_i by base key evolutionary algorithm BA_i , send base key BK_i to message encryption end and decryption end in ring R_i simultaneously.

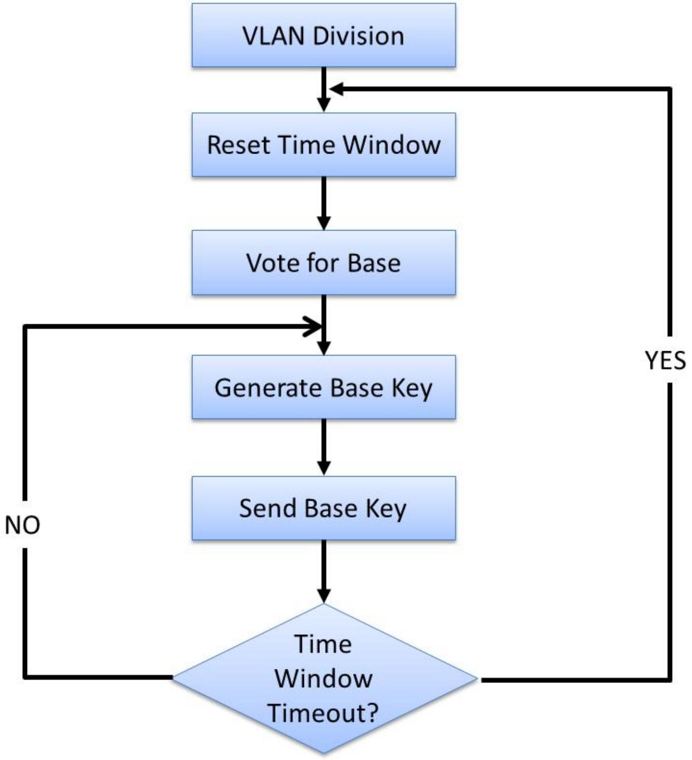

Fig. 4 Flowchart of base generation and action.

Message Encryption & Decryption Algorithm

For ring R_i, message encryption process (Fig. 5) is as below:

Step 1: Message signature end receives base key BK_i and random signature factor α_i, signed user use base key BK_i and signed user key evolutionary algorithm SA_i to generate signed user key SK_i.

Step 2: For GOOSE/SV message, obtain message ASDU (Application Service Data Unit) data set A; for MMS message, obtain message ItemName data set I and UTC field timing status U; use fingerprint function F to generate information abstract DA or DI for A or I.

Step 3: For GOOSE/SV message, according to random signature factor α_i, obtain information abstract DA subset $PGS \in DA$; for MMS message, according to random signature factor α_i, obtain information abstract DI subset $PMMS \in DI$.

Step 4: For GOOSE/SV message, use signed user key SK_i and message timing status T to sign digitally in information abstract PGS and generate evolutionary ring signature information DSMGS; for MMS message, use signed user key SK_i and UTC field timing status U to sign digitally in information abstract PMMS and generate evolutionary ring signature information DSMMMS.

Step 5: For GOOSE/SV message, insert evolutionary ring signature information DSMGS into IEC 61850 message reserved1 and reserved2 field; for MMS message, insert evolutionary ring signature information DSMMMS into Ostring field.

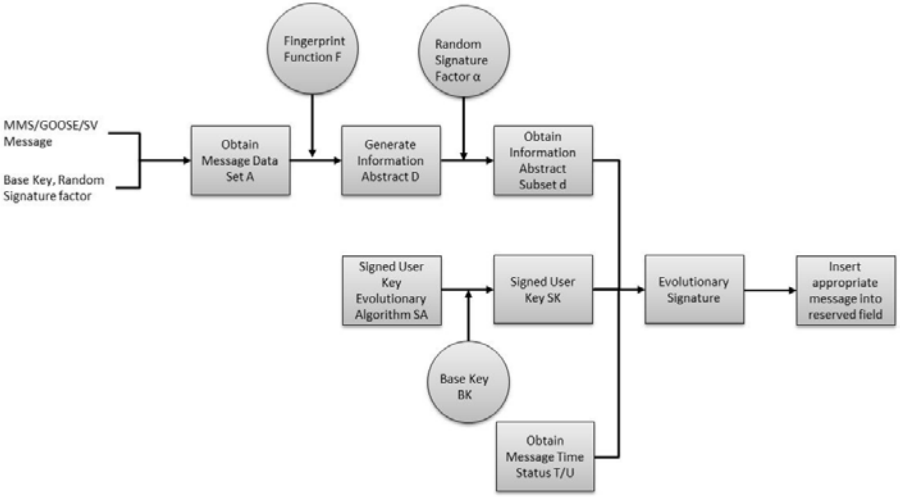
Fingerprint Function F
Random Signature Factor α
MMS/GOOSE/SV Message
Base Key, Random Signature factor
Obtain Message Data Set A
Generate Information Abstract D
Obtain Information Abstract Subset d
Signed User Key Evolutionary Algorithm SA
Signed User Key SK
Evolutionary Signature
Insert appropriate message into reserved field
Base Key BK
Obtain Message Time Status T/U

Fig. 5 Flowchart of encryption algorithm.

Performance Analysis of the Method

The current standard Ethernet message size is 64-1522B. Calculating with throughput of present AES high speed hardware encryption core, 51.2Gbps, the maximum single encryption time is:

$$t_2 = \frac{1522B}{51.2Gbps} < 0.24\mu s \tag{1}$$

However, the ratio of maximum GOOSE/MMS message encryption and decryption time and maximum allowed transmission time is:

$$p_2 = \frac{t_2 \times 2}{4ms} < 0.012\% \tag{2}$$

According to time ratio in formula (1) and (2), the encryption and decryption time only cost a fraction of message transmission time in Smart Substation, which can be ignored. As a result, the information security control method based on evolution ring of Smart Substation can satisfy the requirement of real-time message transmission.

Conclusion

Focus on current information security issue of three layer equipment in Smart Substation which directly connect to Ethernet, this paper analyzes the security methods of Smart Substation message, introduces the information security control method based on VLAN division and evolution ring. The method uses high speed hardware encryption core to secure GOOSE, SV and MMS message transmitted in Smart Substation network. By calculating the time cost of proposed method, the result indicates that encryption and decryption time only cost a tiny portion of maximum allowed transmission time in smart grid which can satisfy both the requirement of real-time message delivery and ensure information security.

References

[1] Digitization of substation applied technology [M]. 2008, Beijing: China Electric Power Press.

[2] Li Mengchao, W.Y., Li Xianwei, Smart Substation and its technological feature analysis [J] Power system protection and control, 2010. 38(5): p. 59-62.

[3] Cao Nan, L.G., Wang Dongqing, Review of key technology in Smart Substation and itsstructual method [J]. Power system protection and control, 2011. 39(5): p. 63-68.

[4] Song Lijun, W.R., Di Junfeng, GOOSE mechanism analyzation implementation and its application in substation digitalization. 37, 2009. 14(31-35).

[5] IEC61850-5, Communication networks and systems in substations - Part 5. Communication requirements for functions and device models[S], 2004.