Reinforced Protection Design for Replay Attack of Intelligent Substation GOOSE/SMV Based on IEC62351

Huang Xiuli
Research Institute of Information Technology & Communication
State Grid Smart Grid Research Institute
Nanjing, China.
e-mail: huangxiuli@sgri.sgcc.com.cn

Wang Chen
Research Institute of Information Technology & Communication
State Grid Smart Grid Research Institute
Nanjing, China.
e-mail: wangchen@sgri.sgcc.com.cn

Zhang Tao
Research Institute of Information Technology & Communication
State Grid Smart Grid Research Institute
Nanjing, China.
e-mail: zhangtao@sgri.sgcc.com.cn

Hua Ye
Research Institute of Information Technology & Communication
State Grid Smart Grid Research Institute
Nanjing, China.
e-mail: huaye@sgri.sgcc.com.cn

Ma Yuanyuan
Research Institute of Information Technology & Communication
State Grid Smart Grid Research Institute
Nanjing, China.
e-mail: mayuanyuan@sgri.sgcc.com.cn

Guan Xiaojuan
Research Institute of Information Technology & Communication
State Grid Smart Grid Research Institute
Nanjing, China.
e-mail: guanxiaojuan@sgri.sgcc.com.cn

Abstract: In the smart substation security area, the IEC 62351 standard defines clearly security measures, provides security guarantees for substation communication system and network security. This paper analysises the part of IEC 62351 standard of GOOSE/SMV protocol security, finds out the shortcomings of the design of the protocol in the replay attack. According to the defects of its security design, this paper enhances the design of the GOOSE/SMV protocol in replay attack, and defines the related data structures.

Keywords: IEC 62351, Smart Substation, Electrical secondary system, GOOSE/SMV protocol, Communication security

I INTRODUCTION

Compared with traditional substation, the way of using and scope of getting for intelligent substation information have many new changes. There are much data can be obtained through the station network such as analog station data and status data of primary device , and process information and operation information on the process layer and the spacer layer devices, etc. intelligent substation is more easier to exchange information with scheduling and control centers, substations or other users by information sharing mechanism to achieve system-level integrated application[1]. Communication protocol is one of the most critical parts of the power system operation, which is responsible for retrieving information from the field device and sending control commands to field devices.

Although the protocol is a key role, but under the security lack of protocol, an attacker will go directly to the dispatch center or inside the substation once bypassing the peripheral physical protection measures , then the attacker can directly control equipment on-site via the communication protocol. Safety, security and reliability of the electric power industry are always the important issues in the design and operation of the system[2].

In the aspect of smart substation security protection, IEC 62351 standard defines specific security measures. Security of end to end communications is a clear goal in IEC-62351 standard, the standard includes a number of sub-standard in different completion status. The goal of procedures, protocol enhancements and related algorithms specified in IEC 62351 is to enhance the messaging security through GOOSE/SMV[3]. Objective of this paper is to make the strengthen design for GOOSE/SMV at the application layer based on IEC62351 to meet smart substation development needs and improve substation secondary system security defense capabilities

II GOOSE/SMV SECURITY INSTRUCTION

IEC62351 standard is the standard for computer communication networks and systems in substation automation system based on IEC 61850 standard[4], which uses a variety of new technologies including hierarchical, object-oriented modeling etc.. GOOSE/SMV messages is directly mapped to the link layer and physical layer via presentation layer[5], using Ethernet technology to ensure packet transmission real-time, which transmits the input and output data values between multiple physical devices, mainly for real-time signal such as protection trip , lock, circuit breaker position etc. , the application of GOOSE / SMV in the power system is more widely.

Currently, one of the main risks GOOSE / SMV faced[6] is the replay attacks. Replay attack is also known as freshness attacks which means the attacker sends the package that a destination host has received to achieve the purpose of deceiving the system, it mainly used for undermining the validity of certification in authentication process. It is a type of attack, this attack will continue to maliciously or fraudulently repeate an efficient data transmission, and a replay attack can be made by the initiator or by the enemy. Attacker steals authentication credentials using network monitoring or other means, and then re-sent it to the authentication server. Encryption can effectively prevent session hijacking, but fail to prevent replay attacks. Replay attack can happen in any network communication process , it is one of attack usually used by hackers in the computer world.

III SECURITY ENHANCED GOAL OF GOOSE/SMV

GOOSE/SMV security protection design in this article is based on IEC62351[7-8] by the certification of the time validity to enhance GOOSE / SMV protection against replay attacks.

GOOSE message contains time information,but SMV message doesn't contains time information and need to add time information, so treatment methods between the two messages is similar and the process is not exactly same:

1)GOOSE: to directly use the time information in packets；

2)SMV: to extend the time information on the basis of the original data structure.

IV GOOSE/SMV PROTECTION REINFORCED DESIGN FOR REPLAY ATTACK

A. GOOSE protection process

GOOSE replay attack[9] protection will be implemented by the following some rules:1)GOOSE messages generated time will be compared to messages received time, if time difference is more than two minutes then the packet will be discarded; 2)state number of messages received will be compared to state number of the history messages , if the new state number is less than the older one, and the historical state number isn't maximum limit, then the packet will be discarded;3) if the packet generation time expires, packets will be discarded.

After Authentication[10] Value is certificated, the event time will be get by t field in GOOSE message, then the following steps will be executed to prevent replay attacks:

1)To Certificate Authentication Value;

2)Client read t value in GOOSE message and cur value in system and compare them,if the time different is more than 2 min (cur> t + 2, this time period is minute),then give up GOOSE packet.

3)Client records and tracks the received Stnum from Publisher. If a smaller Stnum value is received , and it has not exceeded the maximum state number or timeallowedtoLive (time to allow to live) expires, then the message should be discarded;

4)If the message is timeout, then reset Stnum ;

5)If Stnum has exceeded the maximum state number, then reset Stnum;

6)When initializated or powed, Stnum should be initialized to 0.

Deviation time here (skew period) requirements should be configurable and should support that the minimum value should not be greater than 10s(maximum-minimum).

B. GOOSE protection steps for replay attack

GOOSE protection steps are shown below:

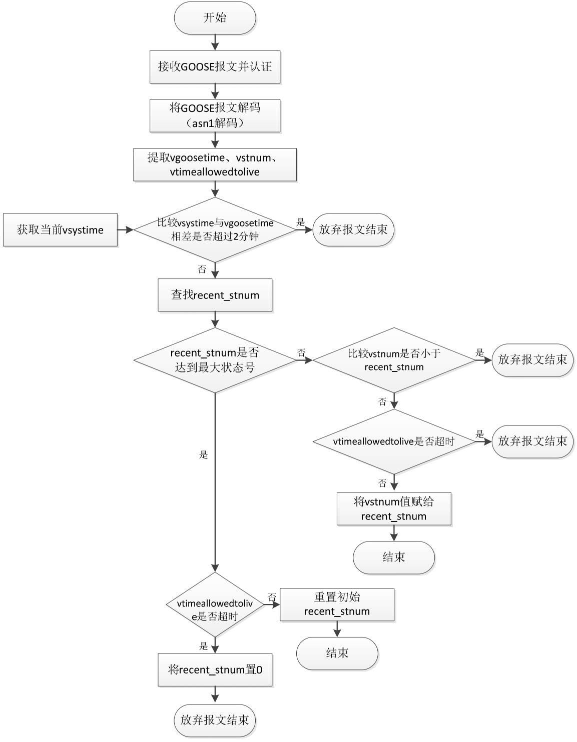

开始
接收GOOSE报文并认证
将GOOSE报文解码（asn1解码）
提取vgoosetime、vstnum、vtimeallowedtolive
获取当前vsystime
比较vsystime与vgoosetime相差是否超过2分钟
是
放弃报文结束
否
查找recent_stnum
recent_stnum是否达到最大状态号
否
比较vstnum是否小于recent_stnum
是
放弃报文结束
否
vtimeallowedtolive是否超时
是
放弃报文结束
否
将vstnum值赋给recent_stnum
结束
是
vtimeallowedtolive是否超时
否
重置初始recent_stnum
结束
是
将recent_stnum置0
放弃报文结束

Figure 1 GOOSE protection steps

Protection steps in the figure above are described below:

Add the location: The client receives a GOOSE message and has certificated it.

Step1: The GOOSE message decoding (asn1 decoding);

Step2: Extracte "t" ,"stNum" and "vgoosetime, vstnum, vtimeallowedtolive" from timeAllowedtoLive field in decoded GOOSE packet;

Step3: Get the current system time "vsystime" ;

Step4: Compare the current system time "vsystime" and message time "vgoosetime", if time difference is more than two minutes, the packet is discarded, it is to end;

Step5: Find the recently received the state number "recent_stnum" from history records, if history record does not resist, then take the minimum state number, and writes the current state number to history records.

Step6: Compare GOOSE messages state number "vstnum" with recent state number "recent_stnum", (i)If "recent_stnum" has not reached the state maximum number and "vstnum" is smaller than "recent_stnum", then discard the message;

(ii)If "recent_stnum" has not reached the maximum state number and the survival time allowed "vtimeallowedtolive" is overtime, then discard the message;

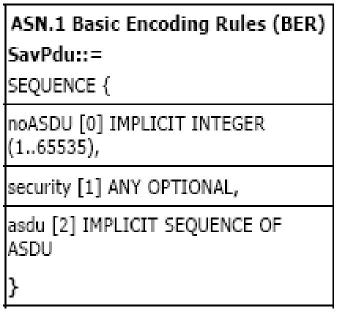
Step7: If "recent_stnum" has reached the maximum value, then set "recent_stnum" with 0;

Step8: If a timeout exists, then replace "recent_stnum" with 0;

C. *SMV protection process for replay attack*

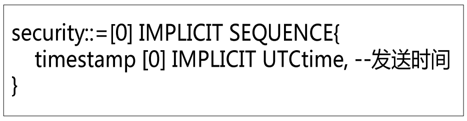
SMV replay attack protection will be implemented by adding the message generated time field in SMV data structure and complying the following some rules:1)SMV messages generated time will be compared to messages received time, if time difference is more than two minutes then the packet will be discarded; 2)state number of messages received will be compared to state number of the history messages , if the new state number is less than the older one, and the historical state number isn't maximum limit, then the packet will be discarded;3) if the packet generation time expires, packets will be discarded.

In order to prevent SMV replay attack, it is need to achieve the time field in security field in SMV.



```
ASN.1 Basic Encoding Rules (BER)
SavPdu::=
SEQUENCE {
noASDU [0] IMPLICIT INTEGER
(1..65535),
security [1] ANY OPTIONAL,
asdu [2] IMPLICIT SEQUENCE OF
ASDU
}
```

Figure 2 type of security field declaration



```
security::=[0] IMPLICIT SEQUENCE{
    timestamp [0] IMPLICIT UTCtime, --发送时间
}
```

Figure 3 Securty field definition

Timestamp presents SMV generation time , and after Authentication Value is certificated, the event time will be get by timestamp field in SMV message, then the following steps will be executed to prevent replay attacks:

1)To Certificate Authentication Value;

2)Client read timestamp value in SMV message and cur value in system and compare them,if the time different is more than 2 min (cur> timestamp + 2, this time period is minute),then give up SMV packet.

3)Client records and tracks the received smpCnt from Publisher. If a smaller smpCnt value is received , and it has not exceeded the maximum state number. then the message should be discarded;

4)If the message is timeout, then reset smpCnt;

5)If smpCnt has exceeded the maximum state number, then reset smpCnt;

6)When initializated or powed, smpCnt should be initialized to 0.

D. *SMV protection steps for replay attack*

Because time information in SMV is customized, it is need to add time information to the SMV packet in sender end.

(1)Sender end protection steps are shown below:

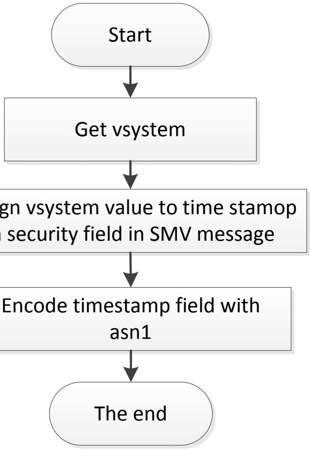

Start
Get vsystem
Assign vsystem value to time stamop in security field in SMV message
Encode timestamp field with asn1
The end

Figure 4 SMV sender end protection steps

Protection steps in the figure above are described below:

Add a location: construct SMV message.

Step1: Get the current system time "vsystime" ;

Step2: Assign system time to "timestamp" in the security field in SMV message;

Step3: Make Asn1 encoding for timestamp fields;

(2)Receiving end protection steps are shown below:

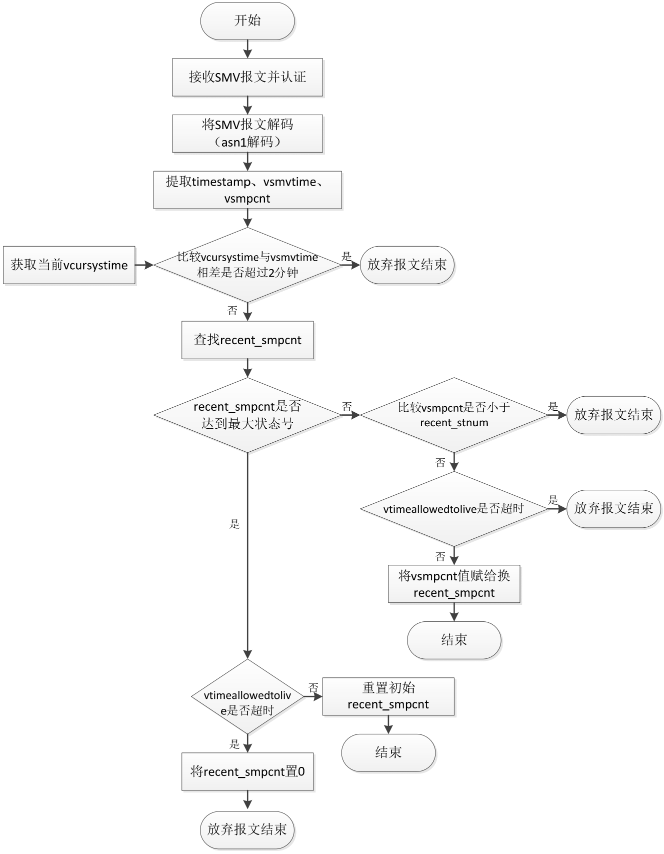

开始
接收SMV报文并认证
将SMV报文解码（asn1解码）
提取timestamp、vsmvtime、vsmpcnt
获取当前vcursystime
比较vcursystime与vsmvtime相差是否超过2分钟
是
放弃报文结束
否
查找recent_smpcnt
recent_smpcnt是否达到最大状态号
否
比较vsmpcnt是否小于recent_stnum
是
放弃报文结束
否
vtimeallowedtolive是否超时
是
放弃报文结束
否
将vsmpcnt值赋给换recent_smpcnt
结束
是
vtimeallowedtolive是否超时
否
重置初始recent_smpcnt
结束
是
将recent_smpcnt置0
放弃报文结束

Figure 5 SMV receiving end protection steps

Protection steps in the figure above are described below:

Add the location: The client receives a SMV message and has certificated it.

Step1: The SMV message decoding (asn1 decoding);

Step2: Extracte "timestamp" and "vsmvtime, vsmpcnt" from smpCnt field in decoded SMV packet;

Step3: Get the current system time "vcursystime" ;

Step4: Compare the current system time "vcursystime" and message time "vsmvtime", if time difference is more than two minutes, the packet is discarded, it is to end;

Step5: Find the recently sampled number "recent_smpcnt" from history records, if history record does not resist, then take the minimum sampling number, and writes the current sampling number to history records.

Step6: Compare SMV messages sampling number "vsmpcnt" with recent sampling number "recent_smpcnt", if "recent_smpcnt" value has not reached the maximum sampling value and "vsmpcnt" is smaller than "recent_smpcnt", then discard the message；

Step7: If "recent_smpcnt" has reached the maximum value, then replace "recent_smpcnt" with 0;

Step8: If a timeout exists, then replace "recent_smpcnt" with 0;

V Summary and Outlook

Combined with IEC 62351 standard, this paper makes a brief analysis for intelligence substation communication security. Focus on studying GOOSE / SMV security in the IEC 62351 standard , this paper analysed its lack in replay attacks protection design, and proposed to the improved design in the time parameters, and also extended the related data structures design. By the above method, it can resist attacks against smart substation communication process, and reduce the risk of intelligent substation equipment controlled or malicious misused, at same time it also prevent critical business tampered or stolen, which ensures that no grid and blackouts accidents occur due to information security .

References

[1] Chen Shuyong, Song Shufang, Li Lanxin, etal. Survey on smart grid technology[J]. Power System Technology, 2009, 33(8): 1-7(in Chinese).

[2] Steffen Fries, Hans Joachim Hof, Maik Seewald. Enhancing IEC 6235 1 to Improve Security for Energy Automation in Smart Grid Environments[C].2010 Fifth International Conference on Intemet and Web Applications and Services, 135-142.

[3] DUAN Jiquan, DUAN Bin. Real-time processing of GOOSE message in substation. Automation of Electric Power Systems,2007,31(11):65-69.

[4] Lu Qiang. Digital Power System(DPS)[J]. Automation of Electric Power Systems, 2000, 24(9) : 1-4.

[5] GONG Jian,LU Cheng,WANG Qian. Introduction to Computer Network SecurityNanjing: Southeast University Press,2000.

[6] Xin Yaozhong. Four issues of network information security[C].China Information Association Information Security Committee Annual Meeting Proceedings.2004:150-157.

[7] DING Jie, XI Houwei. Research on substation automation system based on IEC 62351 security standards. Power SystemTechnology,2006,30(Sup):345-348.

[8] IEC. IEC 6235l, Power systems management and associated information exchange-Data and communications security [S].2007.

[9] DUAN Jiquan,DUAN Bin. Real-time processing of GOOSE message in substaion. Automation of Electirc Power Systems, 2007,31(11):65-69.

[10] YANG Yang,HUANG Xiaoqing,Cao Yijia. Substation communication messages safety certification and real-time simulation[J]. Automation of Electirc Power Systems, 2011,35(13):77-82.