



智能变电站二次系统通信规约安全增强

汪晨,邵志鹏,黄秀丽

(国网智能电网研究院信息通信研究所,江苏 南京 210003)

摘要:随着 IEC6150 标准智能变电站和智能电网的广泛应用,变电站站内二次系统通信安全成为不容忽视的问题。结合 IEC62351 标准,以变电站站内为整体,从身份认证、加密通信、防重放攻击、密钥分配等方面研究变电站通信规约 MMS、GOOSE/SMV 的安全增强技术,并探讨加密后报文的分析技术,采用开源软件针对嵌入式系统定制改造,并结合试点装置运行情况,分析规约安全增强的设备通信性能。

关键词:智能变电站;二次系统;规约安全增强

中图分类号: TP309, TM769

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2015389

Protocol security enhancement on secondary system of smart substation

WANG Chen, SHAO Zhipeng, HUANG Xiuli

Institute of Information and Communication, State Grid Smart Grid Research Institute, Nanjing 210003, China

Abstract: With the wide application of smart substation communication protocol IEC6150 and Smart Grid, IEC61850 safety issue has become a problem can't be ignored. Combined with IEC62351, in the internal of substation as a whole, from authentication, encrypted communications, anti-replay attack, key distribution, the communication protocol security enhancement with in side of the substation which included MMS, GOOSE and SMV protocol was studied. Encrypted packet analysis technology was discussed. Combined with the test equipment run conditions, the performance caused by protocol security enhancement equipment was analyzed.

Key words: smart substation, secondary system, protocol security enhancement

1 引言

国内变电站主要有传统变电站和 IEC61850 标准^[1]的智能变电站,由于智能变电站设备能够进行互操作,且电网公司也在大力推广智能变电站,因此,智能变电站将是发展趋势^[2,3]。

随着智能电网^[4-6]的广泛应用,电力信息化开放程度越

来越高,信息安全受到重视^[7,8]。目前,变电站安全防护措施主要为变电站二次系统安全防护,它更像是个隔离防护设备,能够防护变电站内部系统与变电站外界的安全,而对于变电站内部的二次系统通信规约安全防护却无能为力。根据统计显示,80%的网络攻击源于内部网络。传统的直连方式安全问题并不突出,主要原因在于攻击者不易接入系统,且易被发现。而具备互操作的智能变电站,攻击者一

收稿日期:2015-09-20;修回日期:2015-12-10

基金项目:国家电网公司科技项目“电网智能化单元传输规约安全分析及增强技术”

Foundation Item: The Science and Technology Project of China State Grid Corporation “Smart Power Unit Transmission Protocol Safety Analysis and Enhance Technical Research”



且接入站内网络,即可展开攻击,且不易被发现。

基于 IEC61850 标准的智能变电站内部在通信规约设计上,并未进行安全设计。攻击者一旦接入站内网络,便可以随心所欲地进行破坏工作。为了弥补 IEC61850 的安全问题^[9,10],IEC62351 标准^[11-13]中给出了变电站通信规约安全的定义,参考文献[14-16]从不同角度研究和探讨 IEC62351 标准,但都有一个不足之处,对指导实际开发变电站安全设备还不具备足够的指导,如 IEC62351 标准中提出的 GOOSE/SMV 时间要求为 4 ms,而实际变电站环境中时间在微秒级才能够实时处理报文。

电力是国家重要的基础设施,安全稳定运行是最基本的要求。本文结合 IEC62351 标准与变电站实际运行情况,对智能变电站二次系统通信规约进行安全增强研究与设计开发,以指导变电站站内通信规约安全设备的开发。规约安全增强包括 MMS(manufacturing message specification,制造报文规范)规约的关联认证和防重放攻击、传输层加密通信、GOOSE(generic object oriented substation event,面向通用对象的变电站事件)/SMV(sampled measured value,采样测量值)规约的签名认证和防重放攻击、站内密钥分配、安全增强后的报文分析。最后,对增强的规约设备运行的时延或数据处理做简要分析。

2 通信规约安全增强

2.1 规约安全增强框架

变电站二次系统通信规约安全增强框架依据 IEC62351 标准,结合变电站实际,对 IEC61850 标准智能变电站站内通信规约 MMS 和 GOOSE/SMV 进行安全增

强,如图 1 所示。

(1)MMS 规约安全增强

MMS 规约安全增强体现为应用层的应用认证和传输层的通信加密。应用层在 MMS 关联过程对 MMS 客户与服务进行双向签名认证和防重放攻击,传输层在 TCP 基础上,引入 SSL/TLS 协议进行通道加密。

(2)GOOSE/SMV 规约安全增强

GOOSE/SMV 规约安全增强对报头进行 CRC 检验,对报文进行签名认证,对报文进行重放攻击。

(3)密钥分配

对(1)和(2)中的签名认证和通信加密涉及的密钥进行分配以及规约增强后报文分析设备的密钥分配。

本文还将对签名认证算法在 GOOSE/SMV 运行的实时嵌入系统中运行的时间参数进行分析。

2.2 MMS 通信规约安全增强

MMS 规约安全增强一是在应用层增加 MMS 关联认证和防重放攻击功能,二是在传输层之上使用定制的 SSL/TLS 协议,如图 2 所示。

MMS 规约在应用层上使用 ACSE (association control service element,关联控制服务元素),ACSE 的关联请求单元(AARQ)和关联响应单元(AARE)声明了认证功能单元的描述,但未有实现内容,且默认情况下认证功能单元不启用。在传输层上仅使用传统的 TCP。

本文在具备认证功能单元的 ACSE 基础上,启用 ACSE 的认证功能单元,设计认证功能单元数据结构,设计认证过程。在认证过程同时,引入防重放攻击功能,使得 MMS 应用层同时具备认证与防重放攻击功能。在传输层

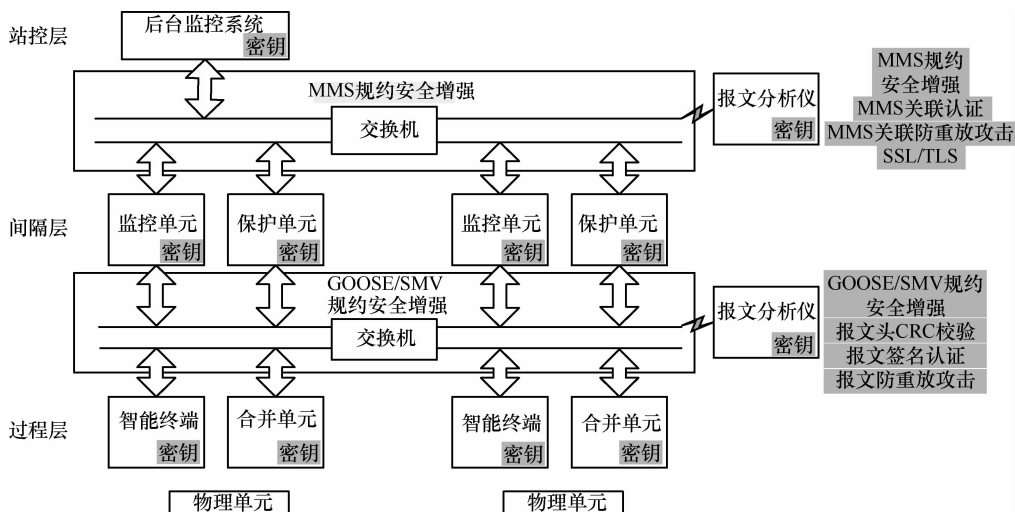


图 1 规约安全增强框架

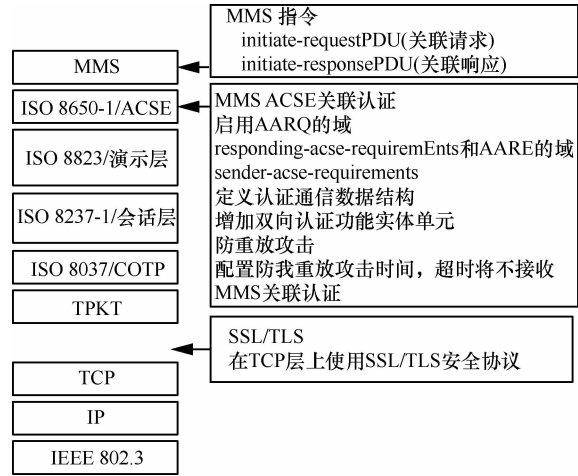


图2 MMS 规约安全增强

引入定制 SSL/TLS 协议。

图3是增强的MMS交互过程,其中阴影部分为安全增强部分,相较于普通的MMS,增强了传输层的加密通道功能和应用层的认证及防重放攻击功能。

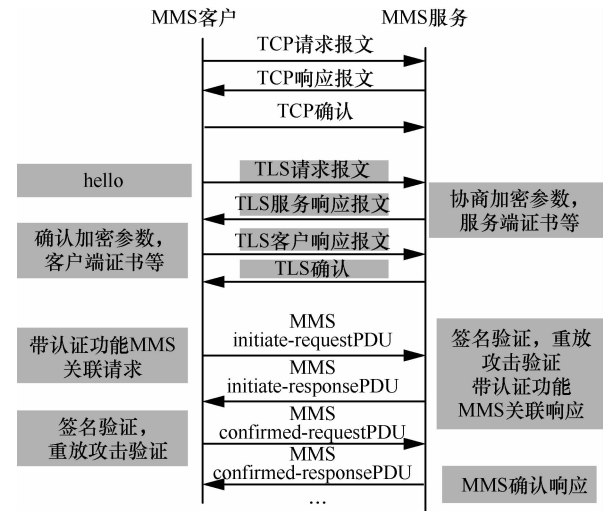


图3 MMS 规约安全增强通信过程

2.2.1 MMS 关联认证及防重放攻击

为了能够兼容之前的MMS规约,通过以下3个步骤完成MMS规约的关联认证:

- 启用ACSE的认证功能单元;
- 设计认证数据结构;
- 设计双方认证流程。

ACSE认证功能单元如图4所示,AARQ-apdu和AARE-apdu分别对应ACSE的关联请求与关联响应数据结构。认证功能单元启用标识未启用时,认证机制和认证结构同时不被使用。ACSE默认情况下不启用认证功能单元启用标识,认证机制名为双方选定,认证数据结构默认仅为一个声明。

安全增强的MMS关联认证功首先启用 sender-acse-requirements 和 responder-acse-requirements 两个域值,且值为 authentication(0);然后定义认证数据结构,并将认证数据结构的标识符作为认证机制值。认证数据结构定义如图5所示。

图5(a)为认证数据结构的抽象接口,图5(b)为定义的认证数据结构。认证数据结构主要有以下3项内容。

(1)SignatureCertificate:签名验证证书

SignatureCertificate ::= OCTET STRING(size(0..8192))

SignatureCertificate最大可携带8192byte内容。在关联认证过程,签名方发送签名时间时,主动将验证签名的证书通过域SignatureCertificate发送给验证方。SignatureCertificate内容应按照基本编码规则编码的X.509证书。

(2)SignedValue:签名值

SignedValue ::= OCTET STRING(size(0..256))

SignedValue为发送方用自己的私钥对时间值摘要的签名。

(3)Time:认证值创建时间

Time为开始创建认证值的时间,用GeneralizedTime

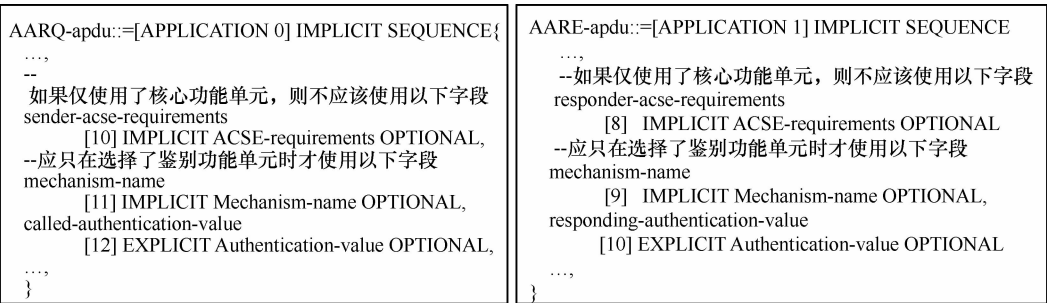


图4 AARQ 和 AARE 认证功能单元



```

Authentication-value ::= CHOICE {
    charstring [0] IMPLICIT GraphicString,
    bitstring [1] IMPLICIT BIT STRING,
    external [2] IMPLICIT EXTERNAL,
    other [3] IMPLICIT SEQUENCE {
        other-mechanism-name
            MECHANISM-NAME.&id({ObjectSet})
        other-mechanism-value
            MECHANISM-NAME.&Type
    }
}

```

```

STASE-MMS-Authentication-value {iso member-body usa(840) ansi-t1-259-
1997(0)stase(1) stase-authentication-value(0) abstractSyntax(1) version1(1)}
DEFINITIONS IMPLICIT TAGS ::= BEGIN
    -- EXPORTS everything
    IMPORTS
        SenderId, ReceiverId, Signature, SignatureCertificate
    FROM ST-CMIP-PCI {iso member-body usa (840) ansi-t1-259-1997 (0)
    stase(1) stasepci(1) abstractSyntax(4) version1(1)};
    MMS_Authentication-value ::= CHOICE {
        certificate-based [0] IMPLICIT SEQUENCE {
            authentication-Certificate [0] IMPLICIT &SignatureCertificate,
            time [1] IMPLICIT GENERALIZEDTIME,
            signature [2] IMPLICIT &SignedValue
        },
        ...
    }
END

```

图5 MMS 关联认证数据结构定义

格式表示的格林威治时间(GMT)值。Time 同时可以防重放攻击使用。

防重放攻击使用关联认证的时间值,在签名验证通过后,使用最近一次的历史时间值与 Time 做差比较,超过阈值,则拒绝接收对方的请求或响应。只在允许的时间范围内方可接收对方的请求或响应。

认证与防重放攻击过程如图 6 所示。

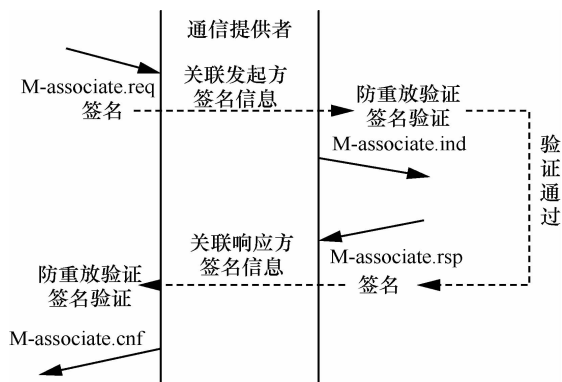


图6 MMS 关联认证与防重放过程

详细步骤如下。

(1) 关联请求发起者

步骤 1 设置 sender-acse-requirements 为 authentication (0)、认证机制值为认证数据结构 ID。

步骤 2 获取系统时间 Time, 使用散列算法对 Time 进行摘要运算, $HTime = Hash(Time)$ 。

步骤 3 加载私钥 Key 和证书 (带 CA 签名的公钥) Cert, 并使用私钥对 HTime 进行签名, $SignedValue = Encrypt(Key, HTime)$, 其中, Encrypt 表示通过密钥给值 HTime 进行加密。

步骤 4 先将证书 Cert、Time 和 SignedValue 封装成认证数据结构; 再将认证数据结构赋给 called-authentication-

value, 完成 AARQ-apdu 其他域的操作, 并将 AARQ-apdu 发送至接收者。

(2) 关联响应者

步骤 1 提取关联请求者的 AARQ-apdu。

步骤 2 判定是否存 sender-acse-requirements, 且值为 authentication(0), 若不存在, 或是值不为 authentication(0), 则报关联功能未启用错误, 拒绝关联。

步骤 3 提取认证机制值, 若不存在且不等于认证数据结构 ID 值, 则报关联认证机制不一致错误, 拒绝关联。

步骤 4 分别提取认证数据结构值的证书 Cert、时间值 Time、签名值 SignedValue。

步骤 5 加载 CA 证书, 使用 CA 证书验证关联请求者的证书 Cert 是否有效, 若无效, 报证书无效错误, 并拒绝关联。

步骤 6 先使用证书 Cert 解密签名值 SignedValue, $HTime' = Decrypt(Cert, SignedValue)$, 再使用散列算法对时间 Time 进行运算, $HTime'' = Hash(Time)$; 比较 $HTime'$ 和 $HTime''$, 若不相等, 则报签名不正确错误, 拒绝关联; 此步骤中的 Decrypt 表示使用 Cert 对 SignedValue 进行解密操作。

步骤 7 提取防重放攻击阈值 T, 最近关联时间 LTime; 其中, T 可配置且参考值为 10 min, LTime 初始值为 0, 表示无历史关联时间。

步骤 8 计算 LTime 和 Time 差值是否在阈值范围内, 若是, 报重放攻击错误, 拒绝关联。

步骤 9 关联成功。

关联成功后, 关响应者同样会发起关联认证, 然后关联请求者接收关联认证, 此过程上述步骤类似, 区别在于 sender-acse-requirements 被 responder-acse-requirements 替代, called-authentication-value 被 responding-authentication-value 替代以及时间、公钥与证书内容不相同等, 在此不再描述。

(2)传输层 SSL/TLS 增强

传输层 TCP 之上使用 SSL/TLS 协议实现安全加密隧道,由于变电站内部环境的特殊性,对 SSL/TLS 有以下要求:

- 加密套件不能为 null;
- SSL/TLS 版本需要为 SSL3.1 之上;
- 启用密码重协商机制,且重协商值可配置;
- 支持多证书机构,证书长度建议不要超过 8 192 byte,证书撤销和取消过程中,不应该导致已有连接终止;
- 为了统一通信,端口设定为 3782。

本文不讨论 SSL/TLS 具体内容,详见 RFC2246^[17]。

2.3 GOOSE/SMV 通信规约安全增强

GOOSE/SMV 规约使用在实时性要求非常高的合并单元和智能终端上,虽然 IEC62351 标准提出小于 4 ms,但在实际过程中,要远远小于此值。如合并单元的 SMV 报文以周期 80 次采样为例,则 1 s 要处理 4 000 帧,1 帧仅 250 μs。因此,GOOSE/SMV 暂不采用加密,仅采用签名和防重放攻击增强。

GOOSE/SMV 签名安全增强如图 7 所示,它包含两个部分:一是对报文头部进行 CRC 校验,二是对报文进行签名。CRC 校验防护报文头部被篡改,签名验证确保报文内容不被篡改,且能够确认报文的可信来源。签名内容包含 CRC 校验值,同时保护报文头部。

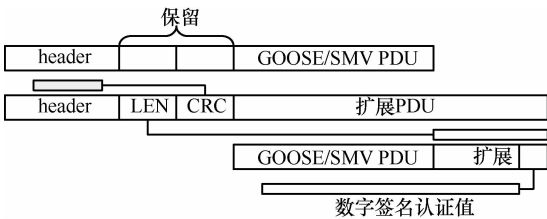
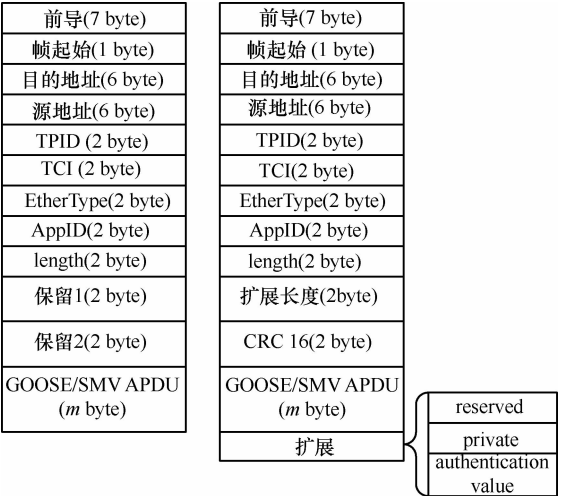


图 7 GOOSE/SMV 安全增强方法

GOOSE/SMV 签名安全增强内容如图 8 所示,图 8(a)为 IEC61850 标准的报文结构,图 8(b)为安全增强的报文结构,安全增强体现在以下几个方面。

- 使用标准报文的保留 2 字段,存放 CRC 校验值,CRC 校验内容为 TPID、TCI、EtherType 和 APPID 域的 8 byte 内容。CRC 校验采用 CRC16 算法。
- 保留 1 字段保存扩展部分的长度,扩展部分包含有签名值。
- 扩展部分主要包含签名值,此外,扩展部分还包含了一个保留域和商家私有信息域。本文不仅考虑签名值,将忽略保留域和商家私有信息的处理。

扩展的定义数据结构如图 9 所示,reserved 和 private



(a)IEC61850报文结构 (b)安全增强报文结构
图 8 GOOSE/SMV 报文结构

暂仅提供声明,signature 为签名值,长度最大可以支持 2 048 bit 的签名长度。

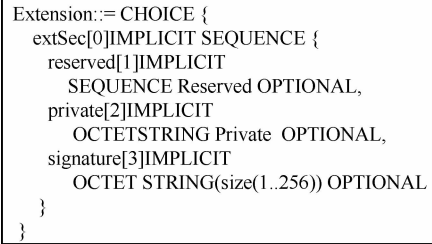


图 9 扩展数据结构定义

签名算法可采用 RSA 算法与 HMAC 算法,但由于 RSA 算法的实时性太差(加解密时间为毫秒量级),因此在硬件未升级前提下建议使用 HMAC,以保证实时性要求,确保在不影响业务前提下,尽量保证安全。

防重放防护 GOOSE/SMV 装置被重放攻击同样必要。单帧故障重放攻击会对 GOOSE 报文产生非常严重的影响,因为 GOOSE 报文为动作报文;而连续多帧的重放攻击对 SMV 具备同样严重的影响,因为接收的数据不足以反映正常的设备状态。

GOOSE 报文中具有时间参数,可以直接使用;而 SMV 报文中没有时间参数,需要首先添加时间结构,才能使用。SMV 时间结构如图 10 所示,security 域为 SAV 报文结构中的保留域,为了兼容性,在 security 域上添加时间域。

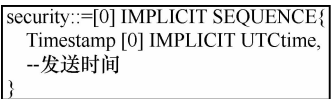


图 10 SMV 时间添加的结构



包含签名与防重放的 GOOSE/SMV 规约安全增强的交互流程如图 11 所示,图 11(a)为普通过程,图 11(b)为安全增强过程,其中阴影部分为安全增强功能。

详细步骤如下。

(1)发送端

步骤 1 构造 APDU。

步骤 2 构造报文扩展(extension)的 TLV 结构。扩展结构主要为认证(authentication)的 TLV 结构,其中 T 为标签,L 表示值 V 的长度,V 表示值;构造 TLV 结构时,V 的长度依据签名算法输出值长度确定,且初始值预设为 0。

步骤 3 extension 长度计算。计算 extension 的 TLV 结构的长度,并填充至保留 1 字段。

步骤 4 填充 EtherType 和 APPID 字段;填充链路信息,即源 MAC 地址、目的 MAC 地址、TPID、TCI。

步骤 5 CRC 计算。

步骤 6 签名值计算。

步骤 7 发送报文。

(2)接收端

步骤 1 接收报文,并解析报文结构。

步骤 2 验证签名。

步骤 3 验证 CRC。

步骤 4 防重放攻击验证。

2.4 密钥分配

在通信规约安全增强中,提供了两种形式的加密算法:非对称加密算法和对称加密算法。非对称加密算法应用于 MMS 身份认证和 GOOSE/SMV 签名认证;加密算法应用于 MMS 隧道建立后的加密过程以及 GOOSE/SMV 采用 HMAC 方式的签名认证。变电站中,除设备通信外,还有网络分析设备,还需要考虑这些网络设备的处理问题。

(1)通信设备密钥分配

现代加密多采用算法可公开,密钥不公开。对于非对称加密,公钥可公开,私钥不公开。在规约安全增强过程中,涉及 MMS 关联认证和加密通道、GOOSE/SMV 签名认证。

MMS 关联认证、SSL/TLS 隧道,使用非对称的加密算法,且对实时性要求不是特别紧急,可采用私钥自己保留,

公开由 CA 统一签发证书。私钥可采用硬件或软件保存,建议采用硬件保存;公钥通过 CA 签名后,公开给对端。

GOOSE/SMV 签名认证由于非对称算法目前不能够满足实时性要求,可采用 HMAC 算法,使用对称密钥。对称密钥分配是关键,而对于变电站实际设备,频繁更新密钥并不实际,可采取预设密钥,且密钥以加密形式保存在装置中。待设备性能满足使用非对称算法时,可采用非对称的密钥分配。

(2)报文分析设备处理

在没有安全增强的变电站中,报文分析设备可以直接分析报文,但在安全增强的变电站中,报文分析设备需要有密钥才可以分析报文。

①MMS 关联认证与加密通信

MMS 关联认证与加密通信,使用非对称的加密算法,对于需要有私钥进行验证签名的方式 MMS 关联认证,并无可取办法,因为只有私钥才可以认证签名,提供私钥给报文分析设备,显示不符合非对称加密的安全原则。可采取离线分析方法,并辅以管理方式将私钥备份集中于统一安全设备中,安全设备提供接口,接口能够直接对报文进行签名验证,返回验证结果,而密钥对报文分析请求者是透明的存在。

MMS 加密通信采用的是 SSL/TLS 方式,实际加密密钥是 SSL/TLS 在构建通道时协商的一次性共享密钥。本文简要介绍一种临时密钥分发方式来解决在 SSL/TLS 通信过程中,通信密钥至报文分析设备的分配过程,其可达到准实时分析,如图 12 所示。

通信双方通过 SSL/TLS 构建加密通道时,协商好通信密钥后,服务端将协商的密钥和链接信息发送至临时密钥管理中心;临时密钥管理中心保存有不同时段、不同链路

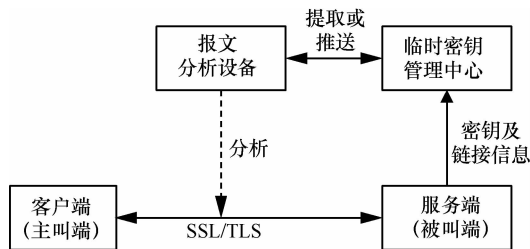


图 12 临时密钥分发过程

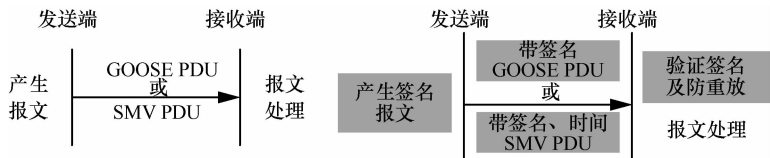


图 11 GOOSE/SMV 安全增强交互过程

的临时密钥信息以及报文分析设备所在链路信息,并实时将关联的链路密钥推送至报文分析设备;报文分析设备本地缓存临时密钥,当采集到数据后,先依据时间与链路从本地查询密钥,若未找到,则再向临时密钥管理中心请求最新密钥。临时密钥缓存中保存有推送密钥和请求密钥。

②GOOSE/SMV 签名认证

GOOSE/SMV 可采用非对称(如 RSA)和 HMAC 两种方式进行签名认证,但由于硬件限制,非对称签名认证实时性不能满足要求。将来若实时性满足要求,可采取 MMS 关联认证离线分析方式。HMAC 认证签名方式使用共享密钥,可采取提供接口及加密的共享密钥打包提供给报文分析设备,报文分析设备通过接口来验证签名而不能直接访问密钥。

2.5 嵌入式安全增强算法性能分析

采用 SSL/TLS 开源算法,并针对嵌入式系统 RP1001 (CPU 为 mpc8321,主频 333 MHz,内存 256 MB)对 MMS 进行规约安全定制开发,改造后提供 MMS 应用层的关联认证接口(签名和身份认证)以及传输层 TLS 加密隧道功能。MMS 关联的认证只在关联时判别,对运行中的性能没有影响。表 1 为规约改造前后的读取动态数据测试的 3 组结果。

表 1 MMS 传输层改造前后时延分析

耗时	改造前/ μ s	改造后/ μ s
发送接口最大耗时	1 563, 1 618, 1 495	3 391, 3 574, 3 508
接收接口最大耗时	786, 805, 729	152 368, 158 201, 173 001

从表 1 中可以看出,接收接口的耗时增加很多,单装置运行中主要用到发送报告服务,不会召唤动态模型,且 MMS 通信在系统中是相对慢速任务,因此 MMS 的安全改造对装置的运行总体影响不大,特别是对发送的影响,但对于接收,还需要继续优化处理,减少接收时延。

采用 PolarSSL 开源算法^[24],在嵌入式 PowerPC 系统中对 RSA、HMAC、SHA-1 和 SHA-256 进行改进,以满足 GOOSE/SMV 签名使用。表 2 和表 3 为使用 SHA-1 和 SHA-256 做摘要的 RSA、HMAC 算法在 RP1202 板(GOOSE 和 SMV 发送,中断周期为 833 μ s)和 RP1204 板(SMV 接收,中断周期为 250 μ s)中的测试时间均值。

从表 2、表 3 中可知,RSA 算法为毫秒级,明显不能满足实时要求(时间远远超过一个中断)。对于 HMAC 算法,时间在几十微秒至一百多微秒。

对于 GOOSE 报文,一般使用 3~4 个控制块,标准情况下发送约为 200 μ s,接收约为 150 μ s,产生耗时 200 μ s,加

表 2 HMAC 算法

密钥长度/bit	HMAC_SHA256/ μ s		HMAC_SHA1/ μ s	
	签名	解签	签名	解签
80	111	54	57	26
800	128	68	65	33

表 3 RSA 算法

密钥长度/bit	RSA-SHA256/ms		RSA-SHA1/ms	
	签名	解签	签名	解签
1 024	28	14	22	9
2 048	36	18	29	15

上签名时间,未达到 833 μ s 的中断周期,能够满足要求。

对于 SMV 报文,标准报文处理大约需要 120 μ s,833 μ s 中断周期的 RP1202 板时,HMAC-SHA256 能够满足要求,但 250 μ s 中断周期的 RP1204 板时,若采用 HMAC-SHA256 时,将有可能产生分组丢失现象。因为 HMAC-SHA256 情况下签名需要 128 μ s 时,时间相加后在 230 μ s (128 μ s+120 μ s),接近 250 μ s。而 128 μ s 给定的是平均时间,在峰值时将会导致丢帧。

3 结束语

本文通过参考 IEC62351 标准,并与实际变电站设备相结合,研究变电站 MMS 规约的关联认证以及关联防重放攻击和为传输层构建加密隧道、GOOSE/SMV 规约的签名认证和防重放攻击、站内密钥分配和加密报文在线或离线分析方法。从报文的完整性、机密性、不可抵赖性和防重放安全特性上,对变电站规约进行安全防护,增强变电站内部规约通信安全。同时,探讨并验证对实时性要求非常高的 GOOSE/SMV 报文签名认证在现有条件下可采用的签名算法。

本文的研究成果虽然在安全算法、嵌入式硬件以及性能分析的选择不够全面,但研究成果在实验条件和试点环境已具备基本的变电站安全功能,可为变电站安全工程实践推进做参考。要实践变电站安全的工程应用,还需要很长的路要走。变电站二次系统的稳定运行是基本条件,要想将变电站安全工程应用化,基本前提就是安全功能在实时性上不能影响业务的运行。目前的变电站规约安全研究与应用,在算法和稳定性上不能完全满足工程应用要求。为了能够落地变电站规约安全应用,有必要对规约安全功能进行优化,减少安全功能带来的时间影响;有必要深入研究嵌入式系统密钥如何分配及管理;同时,嵌入式系统

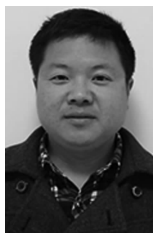


硬件性能的提升也将大大推进变电站规约的安全应用。

参考文献:

- [1] IEC61850. Communication Networks and Systems in Substation[S]. 2004.
- [2] 辛耀中,王永福,任雁铭.中国 IEC 61850 研发及互操作试验情况综述[J].电力系统自动化,2007,31(12):1-6.
XIN Y Z, WANG Y F, REN Y M. Survey on research, development and interoperability test of IEC 61850 in China[J]. Automation of Electric Power Systems, 2007, 31(12):1-6.
- [3] 熊浩清,杨红旗,李会涛.智能变电站发展前景分析[J].河南电力,2011(3).
XIONG H Q, YANG H Q, LI H T. Analysis of development future of smart substation[J]. Henan Power, 2001(3).
- [4] 刘振亚.建设坚强智能电网支撑又好又快发展[J].电网与清洁能源,2009,25(9):1-3.
LIU Z Y. Build strong smart grid as pillar of sound and rapid development[J]. Power System and Clean Energy, 2009, 25(9):1-3.
- [5] 肖世杰.构建中国智能电网技术思考[J].电力系统自动化,2009,33(9):1-4.
XIAO S J. Consideration of technology for constructing Chinese smart grid [J]. Automation of Electric Power Systems, 2009, 33(9):1-4.
- [6] 余贻鑫,栾文鹏.智能电网[J].电网与清洁能源,2009,25(1):7-11.
YU Y X, LUAN W P. Smart grid [J]. Power System and Clean Energy, 2009, 25(1):7-11.
- [7] 陈来军,梅生伟,陈颖.智能电网信息安全及其对电力系统生存性的影响[J].控制理论与应用,2012,29(2):240-244.
CHEN L J, MEI S W, CHEN Y. Smart grid information security and its influence on power system survivability [J]. Control Theory & Applications, 2012, 29(2):240-244.
- [8] 陈涛,王旭.智能电网信息安全风险分析与思考[J].电力信息与通信技术,2012,10(12):97-100.
CHEN T, WANG X. Smart grid information security risk analysis and reflection [J]. Electric Power Information Technology, 2012, 10(12):97-100.
- [9] 莫峻,谭建成.基于IEC61850的变电站网络安全分析[J].电力系统通信,2009,30(198):12-16.
MO J, TAN J C. Research on network security in substations based on IEC 61850 [J]. Telecommunications for Electric Power System, 2009, 30(198):12-16.
- [10] 盛兆勇. IEC61850 安全性分析及解决方案研究[D]. 青岛:中国海洋大学,2013.
SHENG Z Y. Research on security and solutions of IEC 61850[D]. Qingdao: Ocean University of China, 2003.
- [11] IEC 62351: data and cCommunication security[S]. 2005.
- [12] IEC 62351-6: Security for IEC 61850[S]. 2005.
- [13] IEC TC57 security standards for the power system's information infrastructure-beyond simple encryption [EB/OL]. [2015-09-10]. http://www.pcsforum.org/library/files/1129579675White_Paper_on_Security_Standards_in_IEC_TC57_ver_5.pdf.
- [14] 梁峰,丁杰.基于IEC62351的变电站通信安全技术的研究[J].电力系统自动化,2007,31(增刊):157-261.
LIANG F, DING J. Research on substation communication secure technologies based on IEC 62351 standard [J]. Automation of Electric Power Systems, 2007, 31(Sup):157-261.
- [15] 丁杰,奚后玮,陈爱民,等.基于IEC62351安全体系的变电站自动化系统[J].电网技术,2006,30(增刊):345-348.
DING J, XI H W, CHEN A L, et al. Research on substation automation system based on IEC 62351 security standards [J]. Power System Technology, 2006, 30(Sup):345-348.
- [16] 龙林德,李晶,刘莉莉.基于IEC 62351的变电站自动化系统通信安全的研究[J].长沙通信职业技术学院学报,2010,9(3):1-6.
LONG L D, LI J, LIU L L. Research on communication security of substation automation system based on IEC 62351[J]. Journal of Changsha Telecommunications and Technology Vocational College, 2010, 9(3):1-6.
- [17] RFC2246[S/OL]. [2015-09-20]. <http://tools.ietf.org/html/rfc2246>

作者简介



汪晨(1982-),男,国网智能电网研究院工程师,主要研究方向为电力信息安全。



邵志鹏(1984-),男,国网智能电网研究院工程师、项目经理,主要研究方向为信息安全技术及其在电力系统中的应用。



黄秀丽(1979-),女,国网智能电网研究院工程师,主要研究方向为电力信息安全。