DOI: 10.19783/j.cnki.pspc.211492

一种 DNP3 SAv5 的安全架构在配网终端的设计与应用

李 露，谢映宏，许永军，李蔚凡，华志强

（长园深瑞继保自动化有限公司，广东 深圳 518057）

摘要：为了解决配网终端日益突出的通信安全问题，针对配网终端通信系统的安全技术需求展开研究，设计出配网馈线远程自动化终端(FRTU)安全架构。该安全架构实现了分布式网络协议(DNP3)三层架构，突出应用层对象、变体、组别、安全数据应用分类。重点对 FRTU 的安全数据进行分类和建模，给出了 FRTU 数据到 DNP3 安全功能的映射。设计出一种符合安全认证一致性的协议模型，有效解决了 FRTU 协议安全的脆弱性问题。最后通过国际权威机构认证和安全测试，证明其安全认证(SAv5)符合认证和加密等一致性标准，为配网终端的安全接入提供参考依据。

关键词：DNP3 SAv5；FRTU；通信技术；信息安全；防御技术

Design and implementation of a DNP3 SAv5 secure architecture in a distribution network terminal

LI Lu, XIE Yinghong, XU Yongjun, LI Weifan, HUA Zhiqiang

(CYG SUNRI Co., Ltd., Shenzhen 518057, China)

Abstract: There are increasingly prominent communication security problems in distribution network terminals. Thus the security technology requirements of a feeder remote terminal communication system are studied, and the security architecture of a new feeder remote terminal unit (FRTU) is designed. It implements three-layer architecture of a distributed network protocol (DNP3), highlighting application layer objects, variants, groups and security data application classification. This paper focuses on the classification and modeling of FRTU security data, and gives the mapping from FRTU data to the DNP3 security function. A protocol model that conforms to security authentication consistency is designed to effectively solve the security vulnerability of the FRTU. Finally, through the authentication of an international authority and security test, it is proved that security authentication (SAv5) meets the consistency standards such as authentication and encryption. This provides a reference for the secure access of distribution network terminals.

This work is supported by the National Key Research and Development Program of China (No. 2018YFB0904900 and No. 2018YFB0904903).

Key words: DNP3 SAv5; FRTU; communication technology; information security; defense technology

0 引言

随着信息安全技术的发展，配网通信系统对信息安全技术需求越来越迫切。配电自动化以一次网架和设备为基础，以配电自动化系统为核心，综合利用多种通信方式，实现配网自动化系统的监测与控制。而馈线远程自动化终端(Feeder Remote Terminal Unit, FRTU)作为配电自动化系统的重要组成部分，承担故障检测、信息上送、安全认证、加密解密、控制命令接收和执行等功能。典型的配电自动化系统由配电主站、配电终端和通信通道三部分组成。其中，通信通道是配电自动化系统重要的组成部分，也是配网自动化系统正常运行、诊断、调度的基础。通信信道的安全问题，成为了配电自动化系统安全调度的迫切需求[1-2]。

目前电力系统协议有 IEC870-5-101、IEC870-5-104、SC1801、CDT、IEC61850 等，协议在设计之初都是封闭隔离的[3]，没有采用加密认证等安全手段，使得网络攻击者能够很容易地对数据进行监

基金项目：国家重点研发计划项目资助(2018YFB0904900, 2018YFB0904903)

听、篡改等，从而破坏了配电终端通信系统的稳定。近年来，相关公司虽对协议本身的安全功能进行改进，但有一定的局限性，未对安全协议模型进行可靠的形式化建模、认证、模糊测试分析[4-5]。采用的安全防护系统，基本上依赖系统级的纵深防御安全策略，无法抵抗协议本身因脆弱性所带来的安全威胁。

国内外专家关注了配电系统通信信道的协议安全，从协议内部进行广泛研究[6-18]。在经历“震网”事件后，各方将协议安全提到首要日程中。文献[19]提出了分布式网络协议安全(Distributed Network Protocol Security, DNP Sec)功能，对数据链路层进行了修改，引入了序列号、新报头、重要的应用层数据和认证数据。并利用了三重数据加密标准(Triple Data Encryption Standard, 3DES)作为数据加密算法，利用密钥哈希消息认证码(Key-Hash Message Authentication Code, HMAC)作为认证机制。但研究发现，3DES 加密算法缓慢、过时、不安全，加密和认证不同时，产生较高内存资源，在小型配网终端上不适用[20]。

文献[21]指出了数据采集与监视控制(Supervisory Control and Data Acquisition, SCADA)系统的协议脆弱性，通过添加安全套接字(Secure Sockets Layer, SSL)、互联网协议安全(Internet Protocol Security, IPSec)进行安全传输机制。该机制没有完全改变 DNP3 协议本身，没有从小型配网终端可实用性角度来进行加密和认证。

文献[22]介绍了 DNP3 所面临的脆弱性，并根据攻击目标和安全威胁对攻击类型进行分类，确定了 DNP3 所面临的安全威胁的范围。

文献[23]介绍了传统信息系统中通过增加安全机制的解决方案，如 IPSec 和传输层安全协议(Transport Layer Security, TLS)等，来保证 SCADA 系统通信安全。同样这种安全机制也没有从小型配网终端可用性角度出发，而是对协议进行封装保护，增加了传输负荷，对内存资源的需求较高。

针对上述问题，设计一种 DNP3 SAv5 的安全架构，基于 HMAC 应用层重要报文信息认证加密通信系统，有效解决欺骗、篡改、重放、窃听问题，并创新性地应用到配网终端 FRTU 中。安全架构可用于单播、广播、组播等，主要为配电终端和配电主站间的通信提供便利。

1　工程技术

SAv5 协议架构如图 1 所示，图中实线框部分的链路层、传输层、应用层为 DNP3 的三层架构。应用层位于性能加强结构(Enhanced Performance Architecture, EPA)和开放系统互连(Open System Interconnection, OSI)模型的顶层，主要处理用户数据并控制报文的上下流向和安全认证[24]。传输层实际为应用层的一个子层，能够为数据链路提供分块，最终完成单个应用层数据的传输层分块。链路层提供了传输层到物理层的接口，为数据链路传输最小单位。三层设计思想和特定对象的安全处理，能够提高配网自动化终端最大传输单元的数据处理能力。通过报文的重组和分用，提高应用层的报文传输能力。为解决 SAv5 安全架构的效率和安全问题，搭建了如图 1 所示的协议安全架构。

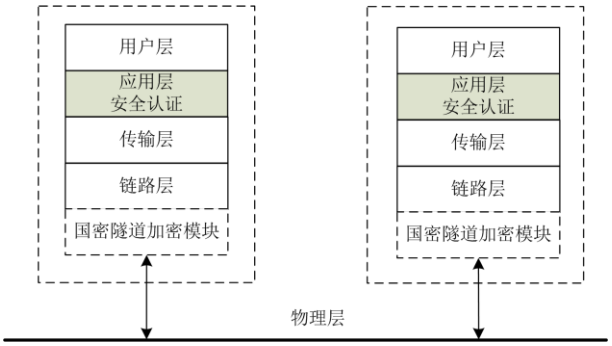

图 1 协议架构图

Fig. 1 Protocol architecture

1.1 消息认证

安全架构的设计，需通过消息认证的方式确保报文消息的完整性，防止篡改、欺骗。通信系统的发送方和接收方的认证，不允许第三方参与，当接收方接收到发送方的消息时，基于安全密钥的情况下，验证消息识别码的真实性。

消息认证可概括为两个方面。首先，具有产生消息认证码的函数。其次，接收方同样采用该函数进行消息真实性的验证。消息认证由密钥协议和哈希函数两个流程组成。

1) 密钥协议

建立串口或网口通信链接后，首先由信任中心主站进行用户编码下发。然后，终端收到后设定加密算法、信息识别算法、随机数、信息识别码。最后，信任中心主站基于对称密钥或非对称密钥修改密钥，包括会话密钥(控制方向和监测方向)和升级密钥。

2) 哈希函数

哈希函数又称之为单向散列函数。数学模型为

$$h = H(M)$$

式中：M 是输入报文的信息；H 是哈希函数；h 是摘要消息，其长度固定并和输入的报文信息 M 无关。

主要的数学性质如下：

1) 给定 H 和 h，无法找到 M，也就是单向性；

2) 给定 H 和 M，找到不同的消息 $M1$，使得 $H(M)=H(M1)$，在计算上是不可行的，称为抗弱碰撞性；

3) 给定 H，产生不同的消息 $M1$ 和 $M2$，使得 $H(M1)=H(M2)$，在计算上是不可行的，称之为抗碰撞性。

上述数学性质，单向性最难求解，而碰撞性最弱。所以，哈希函数最大的安全性是抗碰撞能力。为解决哈希函数(Secure Hash Algorithm, SHA)抗差分攻击，对输出 MAC 按照 8 Byte 和 16 Byte 截取，隐藏输出结果。在没有安全密钥和完成 MAC 的情况下，攻击者是无法破解和伪造欺骗的，消息的完整性和不可篡改性也就得到保证。

1.2 HMAC

文献[25]对 SHA-1、SHA-256、SHA-384、SHA-512 算法进行测试。测试结果显示：相同情况下，无论是对长报文还是短报文进行哈希计算，SHA-256 的计算时间和 CPU 使用率与 SHA-1 相差无几。而 SHA-384、SHA-512 的计算时间则很长，而且 CPU 的占用率差异也较大，不太适合小型的嵌入式配网终端。因此对 SAv5 安全架构的通信报文最大为 255 Byte 时，在现有终端使用中，采用轻量级 SHA-256 算法在速度和安全方面较为合适。

SHA-256 算法输入最大长度为 2^{64} Bit，输出 256 Bit，输入被分成 512 bit 长的分组。而 HMAC 是一种基于密钥和哈希函数所生成的信息识别码，它能够解决消息完整性和身份认证真实性。

HMAC = H{(K XOR opad)||H[(K XOR ipad)||text]}

其中：K 为密钥，M 为消息，ipad=0x36 重复 b 次，opad = 0x5C 重复 b 次。处理过程如下[26]：

1) 在密钥 K 后面添加 0 来创建一个字长为 b 的字符串。

2) 将第 1)步生成的 b 字长的字符串与 ipad 做异或运算。

3) 将消息 M 的数据流填充至第 2)步的结果字符串中。

4) 用 H 作用于第 3)步生成的数据流。

5) 将第 1)步生成的 b 字长字符串与 opad 做异或运算。

6) 再将第 4)步的结果填充进第 5)步的结果中。

7) 用 H 作用于第 6)步生成的数据流，输出最终结果。

同时，HMAC 的安全性依赖于哈希函数本身和密钥的长度及随机性。SAv5 的安全架构通过设置密钥长度为 32 Byte 和频繁修改会话密钥的方式，对会话密钥进行保护。综上，在保证密钥安全的情况下，HMAC 认证是可靠的。

1.3 伪随机数生成器

为保证一次一密加密密钥的随机性，同时，在 HMAC 消息认证流程中，升级密钥和会话密钥是保证通信安全的重要属性，也要求密钥的随机性。在实际工作环境中，真随机数是很难产生的。该安全架构基于 FPPS 186-2 规则进行伪随机数生成，从而保证密钥和挑战信息的不可预测性，使得攻击者很难对密钥本身进行攻击，除非该密钥泄露。

伪随机数的生成通过单向 Hash 函数生成。利用 C 库函数的 SRAND()和 RAND()配合使用，产生伪随机初始序列。基于伪随机序列，构造 64 Byte 的随机种子，通过单向散列函数 SHA 计算哈希值并作 4 轮，每次 20 次计算。

1.4 加密技术

对称密码算法采用相同密钥，实现加密和解密过程。而非对称算法采用不同密钥，用来加密和解密。对称分组将明文数据分解为等长的明文分组，生成等长的密文分组。对称密码密钥分配方案中，有升级密钥(主密钥)和会话密钥(副密钥)。升级密钥保护会话密钥，会话密钥保护数据上行和下行通信。

非对称密码分配方案中，公钥保护密钥信息传输，私钥进行密钥信息解密。为保证数据不被篡改，信用中心主站通过私钥对挑战随机数、终端名称、更改序列号、密钥信息进行私钥签名。

信用主站基于协商机制，将证书相关信息通过 X.509 格式分发给终端用户并关联用户唯一编码。终端收到合法用户编码的升级密钥后，用此密钥进行密钥更新的加密和解密工作。具体过程如图 2 所示。

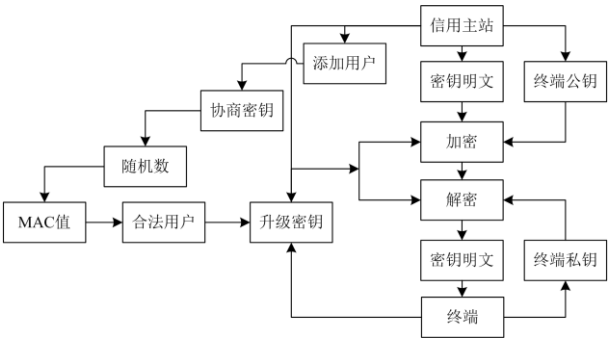

图 2 加密解密过程

Fig. 2 Encryption and decryption process

通过终端环境实测 AES 和常用的加密算法时间，并对实验数据进行比较，分析了 AES 和 RSA 算法的优良性能。实验中对一个 20 M 的文件进行加解密，其结果如表 1 所示。由表 1 可知，AES 和 RSA 加密时间分别为 250 ms 和 320 ms，解密时间分别为 225 ms 和 1000 ms。考虑到密钥的更新效率和安全性，AES 和 RSA 仍具有较好的性能。

表 1 加解密时间

Table 1 Encryption and decryption time

算法名称	加密时间/ms	解密时间/ms
AES	250	225
DES	310	320
3DES	750	755
RSA	320	1000

最后，DNP3 的出口数据由 FRTU 板载的国密加密模块进行出口加密，具备密钥加密和出口数据加密的双重属性。国密算法因 SM1 算法封闭，安全性非常高，由国家密码局授权的硬件模块调用，释放了 CPU 计算资源，提高了加解密效率。

2 终端安全建模

终端 FRTU 作为分站接入 DNP3 网络，最终实现 DNP3 SAv5，需要对 FRTU 的功能和数据进行抽象和分类，并将不同类型的数据内容映射到 DNP3 对象中。通过 DNP3 SAv5 安全架构的加密和认证，实现遥测、状态量变化(Change of State, COS)、时间顺序记录(Sequence of Event, SOE)、故障信息、校时、遥控等命令和参数的维护功能。

2.1 终端的应用数据分类

通过 DNP3 协议，需要将 FRTU 的各种应用数据映射到 DNP3 对象中。应用数据分类如表 2 所示。通过表 2 可知，应用数据分为 SOE 事件、遥测数据、遥信、故障信息、校时、遥控、加密、认证、安全事件防御。

2.2 数据映射

要想通过对象、变体、限定词对 DNP3 类型数据进行获取，需要通过 DNP3 访问 FRTU 终端的数据，仍需将 FRTU 终端数据分类，从而实现 DNP3 到 FRTU 数据的映射转换。以瞬时测量值为例，可将 FRTU 中的数据进行如表 3 所示的分类。由表 3 可知，遥测值对象定义为 30 和 32，不同种类变体不同。安全对象定义为 120，审计功能的对象定义为 121，不同种类变体不同。

为实现不同类型数据的打包上送，提高数据传输效率，可采用不同类型数据的组合式上送方式，包括遥测、遥信、SOE、故障量和静态数据。

通过上述方式数据的分类，可将 FRTU 终端不同类型的应用数据有效地映射到 DNP3 SAv5 对象中，便于配网终端安全架构的设计。

表 2 应用数据分类

Table 2 Application data classification

种类	级别	对象	变体
遥测	4	30	2
遥信	3	1	2
SOE	2	32	0
FLT	2	32	4
遥控	—	12	1
校时	—	50	3
挑战	—	120	1
应答	—	120	2
主动模式	—	120	3
密钥状态	—	120	4/5
密钥更改	—	120	5
用户状态更改	—	120	10
升级密钥请求	—	120	11
升级密钥应答	—	120	12
升级密钥确认	—	120	15
签名	—	120	14
安全事件防御	—	121	1

表 3 数据映射关系

Table 3 Data mapping relationship

种类	级别	对象	变体
A 相电压	4	30	2
B 相电压	4	30	2
C 相电压	4	30	2
频率	4	30	2
有功功率	4	30	2
无功功率	4	30	2
视在功率	4	30	2
功率因素	4	30	2
A 相电流	4	30	2
B 相电流	4	30	2
C 相电流	4	30	2
A 相故障电流	4	32	4
B 相故障电流	4	32	4
C 相故障电流	4	32	4
认证	—	120	1/2/3
加密	—	120	6/13
事件统计	—	121	1

3 安全架构设计

安全架构设计采用轮训和突发两种通信模式，主站可请求子站，终端确认信息；终端也可突发上送数据，主站确认信息，通信方式采用串口或网口。

安全架构在网络的应用层进行密钥加密和消息认证，最终通过国密隧道加密模块出口数据加密，保证数据传输的机密性、完整性及身份的合法性。

安全架构如图 3 所示，应用层主要包括认证、密钥加密、安全通信三个阶段。消息通信的密钥有两副：升级密钥和会话密钥，通过主站系统进行协商分配，进而保证通信系统的安全。

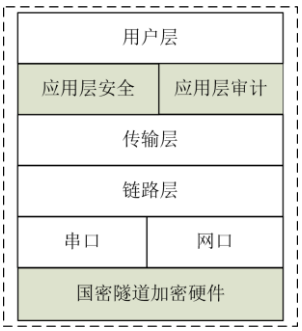

图 3 安全架构

Fig. 3 Security architecture

由图 3 可知，安全架构设计重点包括如下的安全属性。

1) 消息欺骗

DNP3 报文中通过源地址和目的地址的组合来区分报文信息的来源和目的，继而表明主站和终端身份。一旦身份地址被攻击者伪装成合法地址，并伪造了通信报文，从而导致欺骗。安全架构所添加的基于会话密钥的消息认证技术，能够明确确定正在与之授权的用户通信并提供服务，一旦恶意用户闯入，通过错误日志信息记录，便于审计和追溯。

2) 消息篡改

通信过程中，应用层每一次重要报文操作都基于会话密钥和 SHA256 函数进行摘要计算并作签名。攻击者恶意篡改报文，对端进行验签和 HMAC 验证时报错，并通过错误日志信息记录，便于审计。从而数据的完整性和不可抵赖性得到保障。

3) 窃听攻击

电网数据的重要性不言而喻，一旦电网数据被窃听，例如终端实时遥测数据、电能信息和控制，都可以用来进行行为分析，利用人工智能技术进行预测。DNP3 通信数据仍为明文传输，存在窃听的风险，但 SAv5 架构在保证不改变协议本身的条件下，通过国密隧道加密模块进行出口数据加密，因国密算法 SM1 未公开，很大程度上防止窃听，从而具备密钥加密和出口数据加密的双重属性。

4) 重放攻击

安全架构设计为防止攻击者发送一个目的主机曾接收过的数据包，在认证挑战数当中添加两个方向(控制和监测)的伪随机数、发送者名称和用户状态更改序列号来防止重放攻击。

5) 审计

审计能够快速分析事故的原因或故障范围，快速诊断和重现历史行为记录。在主站站点存在多个用户，目的是提供给每个用户一个独立认证或主站本身进行认证的方法。设计的目的是允许配电终端确定传输协议消息的内部用户，并记录用户访问信息系统的操作信息。

综上，SAv5 安全架构的设计可有效解决协议安全的脆弱性，其控制策略如表 4 所示。

表 4 脆弱性解决策略

Table 4 Vulnerability resolution strategy

脆弱性问题	欺骗	重放	篡改	窃听
采用策略	认证	挑战随机数	HMAC	AES/RSA1024/SM1

SAv5 安全架构涉及的安全通信流程如图 4 所示，操作方向包含控制和监测方向。重要操作包括写+HMAC、挑战、应答、密钥查询、密钥更改、证书下发等。为提高通信效率，在基于首次挑战和应答的双向认证后，后面可进行一次认证操作。

3.1 安全认证

基于 ICE/TS 62351-5 规范标准，馈线远程自动化终端可以用来明确地确定它正在与授权的用户通信并访问分站的服务。DNP3 主机可以用来明确地确定它正在与正确的分站通信[27]。

通过使用哈希函数和密钥，来计算给定消息的信息识别码[28]。在缺失密钥的情况下，无法生成有效的 MAC 码，并有效抵抗欺骗、修改、重放等攻击。

安全架构所设计的挑战和应答机制，就是 HMAC 的一个典型应用。该应用是 SAv5 安全架构保护的根本，主站和终端均可发起挑战。双方只需协商好需要进行验证的应用数据服务单元(Application Service Data Unit, ASDU)。使用指定的 HMAC 算法方便灵活地提供了一种单向认证机制，但运行在两种不同的模式下，通过 HMAC 算法进行一次单向认证和二次双向认证[29]。

终端收到受保护的 ASDU，需要挑战和应答身份认证，流程如图 5 所示，细节如下：

1) 终端向主站发出挑战请求，报文包括挑战序列号、MAC 算法、挑战随机数。

2) 主站进行应答，报文包含挑战序列号、信息识别码。

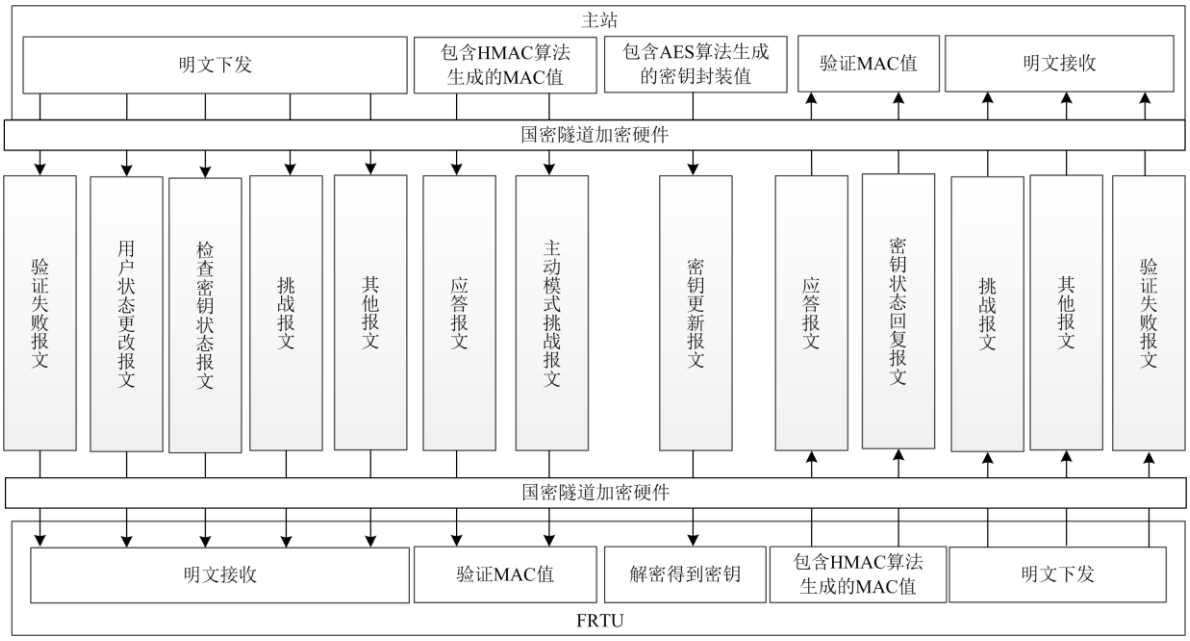

图 4 通信流程

Fig. 4 Communication flow

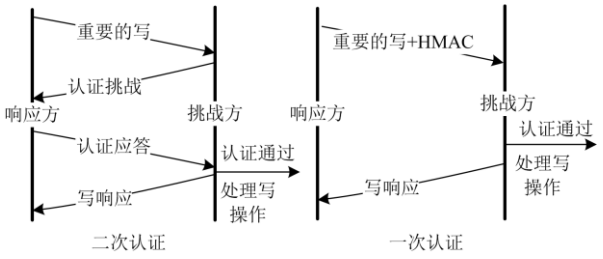

图 5 安全认证流程

Fig. 5 Safety authentication flow

3) 终端收到应答后，将存储的 ASDU、挑战对象信息、密钥进行 HMAC 运算，如果主站的 MAC 和分站的 MAC 一致，认证成功。

通过图 5 可知，认证可采用一次单向认证和二次双向认证。一次单向认证，主动模式下直接生成 HMAC，能够减少协议通信开销。至少发生一次挑战-应答，主要是利用操作中的消息序列号和随机挑战数，避免受到重放攻击。

二次双向认证，响应方发送重要的写操作，挑战方判断重要操作立即发起挑战，响应方随即发起挑战，挑战方通过 HMAC 认证，通过执行写操作并写响应[30]。通过单向认证、双向认证和非对称密钥相互认证，避免了欺骗攻击。

篡改攻击，通过挑战者受保护的 ASDU 单元加入到 MAC 中计算，防止攻击者修改 ASDU。双方协商 MAC 算法后，输入挑战报文(包括随机数、序列号)、ASDU 报文后，在密钥协助下输出 MAC 码。

3.2 审计

审计的目标是发现和定位安全问题，快速找出安全事故的原因，快速重现历史状态信息，为后续安全规则的制定提供参考依据。应用层采用多用户、多密钥的管理机制，任何一个用户的离去都不影响其他用户的通信。像非法用户、用户失效、非法地址、认证失败、解密失败、密钥更改超限、统计阈值超限等安全事件记录也是 SAv5 安全架构的一个重要部分。

安全架构将创建审计跟踪定义为“谁访问了信息技术系统以及用户在给定时间内执行了哪些操作的记录”。此种原则有区块链通信思想，目的就是给访问操作打上指纹信息，为安全事故提供追溯和分析。

3.2.1 安全密钥管理

密钥管理流程如图 6 所示。通过图 6 可知，密钥管理的重点是 2 把密钥，主密钥(升级密钥)和副密钥(会话密钥)。升级密钥保护会话密钥的安全，会话密钥为日常通信会话交流所用。通信建立后，主站可初始化会话密钥和升级密钥。安全统计阈值达到设定值或密钥存活期失效，需要修改会话密钥或升级密钥，保证密钥安全分发。

密钥的对应关系如表 5 所示。从表 5 可知，对称密钥通过主站和分站共享初始态的升级密钥。一旦终端接入，按照密钥管理流程，将初始态升级密

钥切换至正式态升级密钥，监控和控制方向的会话密钥相互独立，一方泄密不影响另一方。非对称密钥通过信用主站将公钥信息按照 X.509 格式进行远程暴露，私钥各自持有。

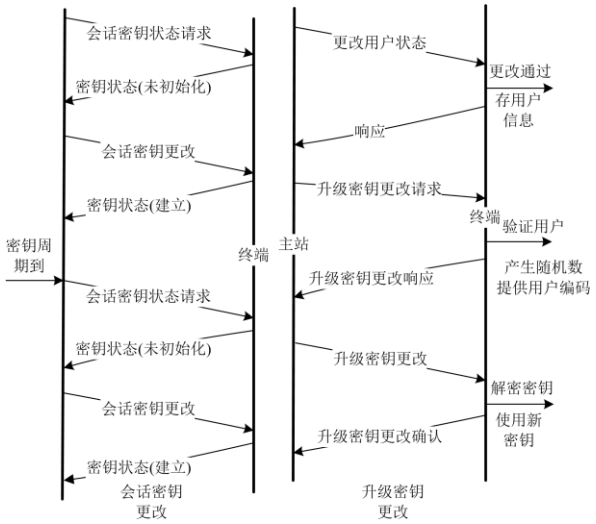

图 6 密钥管理流程

Fig. 6 Key management flow

表 5 密钥对应关系

Table 5 Key corresponding relationship

非对称密钥	说明	对称密钥	说明
用户私钥	签名密钥	监控方向会话密钥	认证监控方向报文
用户公钥	验签密钥	控制方向会话密钥	认证控制方向报文
分站私钥	解密密钥	升级密钥	会话密钥加密/解密
分站公钥	加密密钥	—	—

密钥管理数据结构设计如下：

```
typedef struct
{
    BYTE        byKeyStatus;
    BYTE        byMDSKey[32];
    WORD        wLength_MDSK;
    BYTE        byCDSKey[32];
    WORD        wLength_CDSK;
    BYTE        byGetUKey;
    BYTE        byUKey16[16];
    BYTE        byUKey32[32];
    WORD        wLength_UK;
    WORD        wLenSymmetricKey;
    BYTE        bySymmetricKey[32];
    BYTE        byAuthorityPrivateKey[32];
    WORD        wLenAuthorityPrivateKey;
    BYTE        byAuthorityPublicKey[32];
    WORD        wLenAuthorityPublicKey;
    BYTE        byUserPrivateKey[32];
    WORD        wLenUserPrivateKey;
    BYTE        byUserPublicKey[32];
    WORD        wLenUserPublicKey;
    BYTE        byOutstationPrivateKey[32];
    WORD        wLenOutstationPrivateKey;
    BYTE        byOutstationPublicKey[32];
    WORD        wLenOutstationPublicKey;
    tagDnpAuth_Statistic
    SecurityStatistic[ENUM_DNP_STATIC_MAX_NUM];
}tagDnpAuth_Key, *tagPDnpAuth_Key;
```

3.2.2 多用户管理

多用户模型如图 7 所示，用户管理可支持默认用户或其他用户。从图 7 可知，每个用户拥有唯一用户编码并关联自身密钥，能够动态实现用户的添加、删除、改变。并提供一种分别对每个用户和主站身份认证的方法，最终确定传输任何协议消息的单个用户。根据用户的个人身份或用户执行的角色限制对某些功能进行访问。

用户角色管理数据结构设计如下：

```
typedef struct
{
    BYTE        byUserName[50];
    WORD        wUserNameLen;
    WORD        wUserRoleExpiryInteval;,
    WORD        wUserRole;
    BYTE        byOperation;
    DWORD       dwStatusChangeSequenceNum;
    WORD        wUserNumber;
    BYTE        byUserEdit;
    BYTE        byUserValid;
}tagDnpAuth_UserStatus, *tagPDnpAuth_UserStatus;
```

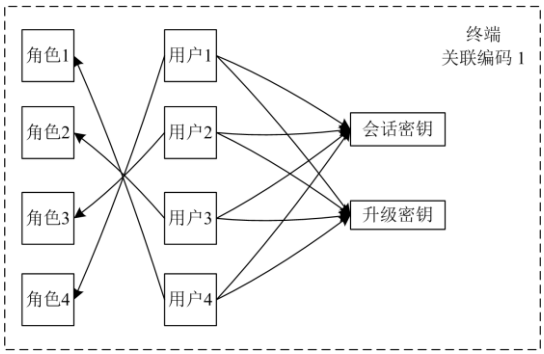

图 7 多用户模型

Fig. 7 Multiple users model

3.2.3 安全事件统计

安全事件统计作为协议内部被动防护技术的

一种重要手段[31-33]，能够实时监测异常数据。在协议的安全分析中，作为一种主动监测方案。通过特征字的识别技术或者行为识别，能够有效建立不同的安全防御策略[34-35]。下面的数据结构定义了事件统计的个数、关联 ID、事件时间，目的是进行安全分析和策略调整。

数据结构设计如下：

```
typedef struct
{
    DWORD       dwNewCountValue;
    DWORD       dwLastCountValue;
    WORD        wAssoID;
    BYTE        byEventTime[8];
}tagDnpAuth_Statistic, *tagPDnpAuth_Statist;
```

4　测试验证

根据上述所设计的安全架构，搭建如图 8、图 9 所示的 DNP3 SAv5 测试环境，验证分析安全架构的一致性和安全性。图 8 为测试终端，图 9 为测试环境。通过图 8、图 9 可知，测试硬件使用 FRTU 终端、交换机、集成加密和认证的 PC2、集成模糊测试脚本的 PC1。交换机可用作端口镜像映射，方便流量监视，便于进行欺骗、修改、重放、窃听 4 种安全威胁。

图 8　FRTU 配网终端

Fig. 8 FRTU distribution network terminal

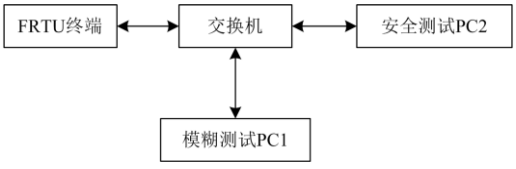

图 9　通信测试环境

Fig. 9 Communication test environment

4.1　一致性测试

基于上述测试环境，通过安全测试 PC2，安全测试策略围绕三个方面：密钥管理、用户管理和认证管理。

密钥管理，终端上电后，建立长链接并完成密钥的初始化。包括升级密钥和会话密钥。具体交互报文流程如图 10 所示。

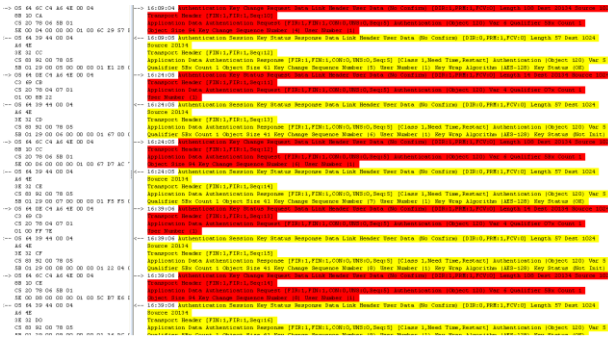

图 10　密钥交互流程

Fig. 10 Key interaction flow

认证管理，接收到重要写操作后，配网终端进行双向认证。具体交互报文流程如图 11 所示。

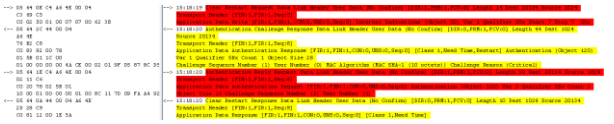

图 11　二次认证流程

Fig. 11 Secondary authentication flow

基于二次认证后，再进行重要写操作，可同时下发一次认证，减少网络带宽，提高通信效率。

用户管理，能够动态实现用户的添加、删除和改变。通过每个用户的唯一编码，关联会话密钥和升级密钥，提高安全管理策略。交互报文流程如图 12 所示。

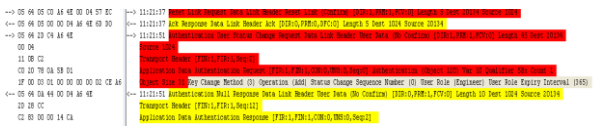

图 12　用户管理流程

Fig. 12 User management flow

基于上述的流程测试，配网终端 FRTU 在国际权威机构 ASE 进行了认证测试，最终顺利通过。认证报告如图 13 所示。

4.2　模糊测试

为验证 SAv5 安全架构的脆弱性对配网终端所造成的伤害，采用基于 Sulley 的 Peach 模糊测试工具。通过构造畸形输入数据使得 SAv5 安全架构出现潜在漏洞，并监控输出中的异常。该测试具有可充分遍历所有输入数据、代码覆盖广、测试自动化、快速发现软件中存在的漏洞问题等优点。

图 13 认证报告

Fig. 13 Certification report

基于安全协议的模糊测试理论和方法，输出如图 14 所示的测试流程。通过图 14 可知，首先确定测试对象，其次进行安全规则解析，然后构造测试用例，最后执行测试用例。

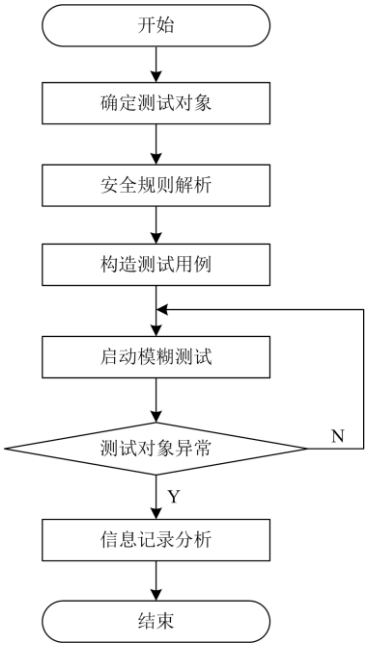

图 14 测试流程

Fig. 14 Test process

1) 确定测试对象

测试对象采用图 9 所示的模糊测试 PC1，设定好 DNP3 SAv5 主站和分站链路地址及配网终端 IP。

2) 安全规则解析

通过 DNP3 SAv5 的样本获取，结合 wireshark 抓包工具，设置源 IP 和目的 IP 过滤条件，截获测试样本报文，进行安全规则解析。样本报文获取如图 15 所示。

图 15 样本报文获取

Fig. 15 Sample message acquisition

3) 构造测试用例

基于安全规则解析，快速生成测试系统可识别的数据包，通过变异自动编造数据，生成变异用例，为测试执行做准备。

构造数据时，Sulley 具有一些常用的数据，如 s_static()、s_binary()、s_random()、s_byte()、s_int()、s_word() 和 s_string() 等。通过 s_block_start() 和 s_block_end()可开始和结束用例流程。

4) 执行测试用例

执行变异测试用例，侧面反映了协议形式化描述的有效性及测试用例生成算法的可靠性。通过 Sulley 数据构造产生一系列的请求，并将相关请求连接成有向图，形成一次完整的测试路径。

Sulley 从根节点开始到叶子节点结束，先进行会话初始化 sessions.session()，其次会话 sessions.connect()，最后 sessions.fuzz()。

5) 启动模糊测试

开启 Sulley 流量监控嗅探进程，并作进程监视，如图 16 所示。监视 Fuzzing 测试运行过程中的异常，异常存储方式为 Log 形式，便于测试分析和用例执行验证。

图 16 嗅探进程

Fig. 16 Sniffer process

将 DNP3fuzz.ph 测试用例放入到模糊测试主机 PC1 sulley-master 目录中，执行脚本对 2000 端口进行 dnp 服务模糊，如图 17 所示。

6) 信息记录分析

Fuzzing 测试开始时，Sulley 发送会话请求，同时 Sulley 的网络监控器代理监视双方的通信数据流，并将监视到的测试用例保存到 PCAP 路径下。一旦进程监视器监视到被测对象异常，自动输出报告，允许事后分析，从而找出引起错误的测试路径，也就是漏洞位置。

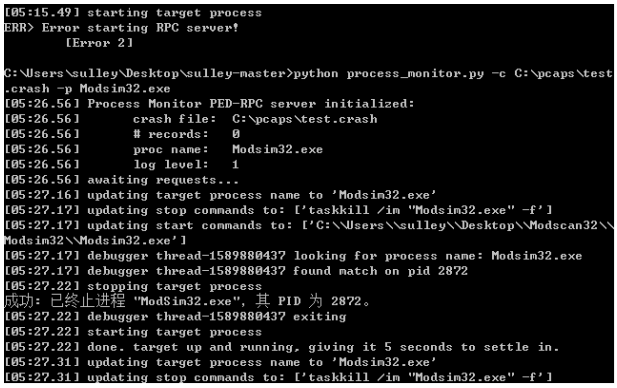

图 17 执行脚本

Fig. 17 Execute script

模糊测试主机 PC1 web 可以成功看到 fuzzy 进程和结果情况，具体如图 18 所示。本次 fuzzy 进程未发生崩溃报告输出。

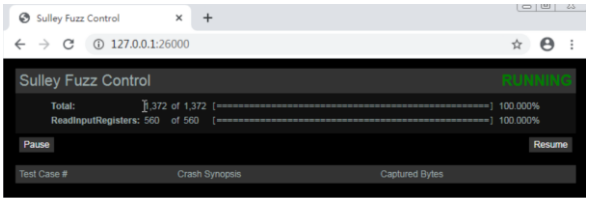

图 18 测试结果

Fig. 18 Test report

表 6 所示的模糊测试统计结果，用于定量分析测试用例的变异情况。

正常用例：协议报文格式正确，协议字段取值符合标准。

异常用例：协议报文格式错误，协议字段取值不符合标准。

变异率：异常用例数在用例总数中的比例。变异率的大小虽不能直接体现用例变异情况的好坏，但变异率数据的稳定可以直接反映用例的随机性和针对性。

表 6 测试结果统计表

Table 6 Statistical table of test results

功能码	用例总数	正常用例	异常用例	变异率/%
G120V1	200	101	99	49.5
G120V2	200	101	99	49.5
G120V3	200	101	99	49.5
G120V4	200	101	99	49.5
G120V5	200	102	98	49.5
G120V11	200	102	98	49.5
G120V14	200	102	98	49.5
G50V3	200	102	98	49.5

4.3 特性测试

基于一致性和模糊测试后，对 SAv5 安全架构的安全属性进行测试分析，并对同类的安全方案进行比较和总结。

4.3.1 功能测试

在确保 SAv5 安全架构拥有完整性和保密性的前提下，进行加密和认证测试，并能够抵御相关攻击。

1) 正常测试

通过 PC2 建立链接，并发送写命令于终端 FRTU，从图 19 可知，FRTU 收到命令后，发送唯一用户编码、挑战序列号和伪随机数挑战给 PC2。接着 PC2 进行挑战应答于 FRTU，终端认证成功后执行写响应。具体流程见图 19 中 1->2->3->4。

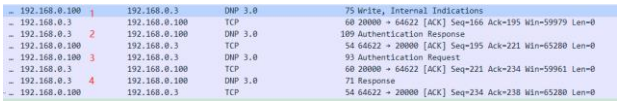

图 19 认证报文

Fig. 19 Authentication network message

2) 重放攻击

攻击者通过交换机截获已认证过的报文进行重放攻击，FRTU 接收到上述报文后，由于序列号和伪随机数均相同，因此 FRTU 返回错误 Error。通过图 20 可知，FRTU 返回 Error 并记录日志，达到阈值后不再响应。

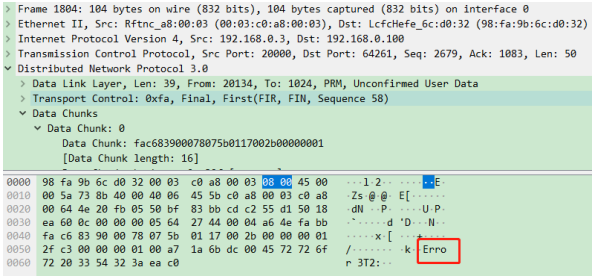

图 20 重放攻击报文

Fig. 20 Replay attack network message

3) 篡改攻击

攻击者通过交换机截获上述未认证过的报文进行 ASDU 篡改，FRTU 接收到篡改报文后，由于攻击者无法获取会话密钥，产生了错误的 MAC。FRTU 接收到篡改攻击报文后，通过会话密钥验证 MAC 出错，因此 FRTU 错误认证错误 Error。如图 21 所示。

4) 欺骗攻击

攻击者通过未授权的非法用户编码进行欺骗认证，FRTU 接收到欺骗报文后，判定用户未启用并无权限，认证失败，如图 22 所示。

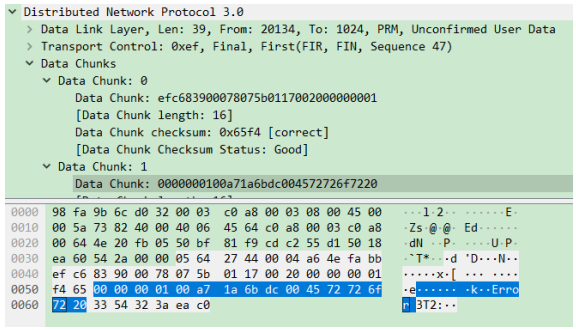

图 21　篡改攻击报文

Fig. 21 Modification attack network message

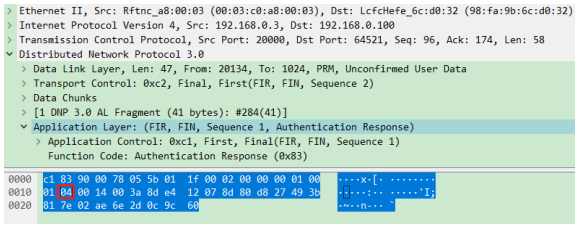

图 22　欺骗攻击报文

Fig. 22 Spoofing attack network message

5) 窃听攻击

DNP 出口报文，通过板载国密隧道加密模块进行加密和解密，有效防止窃听，具备密钥加密和出口数据加密的双重属性。出口加密报文如图 23 所示。

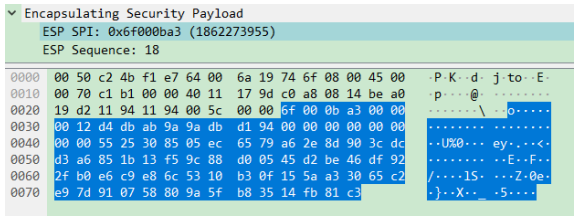

图 23　加密网络报文

Fig. 23 Encrypted network message

4.3.2 方案比较分析

为保证配网终端 FRTU 的通信效率，对比测试文献[21]SSL、文献[23]IPSec 的总传输耗时，如表 7 所示。通过表 7 可知，DNP SAv5 传输耗时较短，而 SSL 和 IPSec 传输耗时较长，因其协议耗用资源大，小型 FRTU 终端很难发挥复杂协议处理优势。

表 7　传输时间比较

Table 7 Comparison of transmission time

安全方案	主站处理耗时/ms	终端处理耗时/ms	总传输耗时/ms
DNP SAv5	25	70	421
DNP SSL	151	310	530
DNP IPSec	160	290	560

为分析 SAv5 总体安全性能，对比了文献[21]SSL、文献[23]IPSec 安全方案，如表 8 所示。文献[21]SSL 对传输层进行协议封装，协议开销较大。而配网 FRTU 终端内存资源小，SSL 协议性能很难发挥。文献[23]IPSec 为因特网协议安全，但算法标准为开源，增加了算法被破解的风险。SAv5 国密算法模块，因 SM1 算法封闭，安全性非常高。通过国家密码局授权的硬件模块调用，释放了 CPU 计算资源，提高了加解密效率。

表 8　安全方案比较

Table 8 Comparison of security schemes

安全方案	完整性	保密性	不可抵赖	可实用性	可靠性
DNP SAv5	较好	较好	较好	较好	好
DNP SSL	好	中	好	中	好
DNP IPSec	中	好	中	好	好

4.4 测试总结

综上，分别采用了 3 种不同的测试策略，验证 DNP3 SAv5 安全架构所具备的安全认证传输机制保证了配网终端安全性。通过一次认证机制，通信效率可快速提高，保证了电网系统通信的实时性。

5　结语

集成 DNP3 SAv5 安全架构的馈线远程终端在泰国 PEA 和 MEA 两大电力用户得到应用，使用效果较好，稳定性较高，满足客户需求。对于认证和加密部分，很好地解决了协议安全本身的脆弱性，并创新地引入到配网终端 FRTU 中。通过相关测试加以佐证，证明 DNP3 SAv5 安全架构具有较高的安全性，能够满足电力系统的要求。

参考文献

[1] 苏莎莎, 赵一鸣, 谢炯, 等. 电网调度数据网 SM 算法优化方案[J]. 电力信息与通信技术, 2020, 18(11): 15-21.
SU Shasha, ZHAO Yiming, XIE Jiong, et al. Optimization scheme of SM algorithm in power grid dispatching data network[J]. Electric Power Information and Communication Technology, 2020, 18(11): 15-21.

[2] 廖会敏, 王栋. 基于 SM2 算法的电力无介质数字认证技术研究[J]. 供用电, 2020, 37(4): 46-51.
LIAO Huimin, WANG Dong. Research on digital authentication technology of electric power no-medium based on SM2 algorithm[J]. Distribution & Utilization, 2020, 37(4): 46-51.

[3] 陶耀东, 李宁, 曾广圣. 工业控制系统安全综述[J]. 计算机工程与应用, 2016, 52(13): 8-18.
TAO Yaodong, LI Ning, ZENG Guangsheng. Review of

industrial control systems security[J]. Computer Engineering and Application, 2016, 52(13): 8-18.

[4] FOVINO I N, CARCANO A, DE LACHEZE M T, et al. Modbus/DNP3 state-based intrusion detection system[C] // 2010 24th IEEE International Conference on Advanced Information Networking and Applications, April 20-23, 2010, Perth, WA, Australia: 729-736.

[5] 雷煜卿, 李建岐, 侯宝素. 面向智能电网的配用电通信网络研究[J]. 电网技术, 2011, 35(12): 14-18.
LEI Yuqing, LI Jianqi, HOU Baosu. Power distribution and utilization communication network for smart grid[J]. Power System Technology, 2011, 35(12): 14-18.

[6] 常方圆, 李二霞, 亢超群, 等. 配电终端可信安全防护方案研究[J]. 计算机应用研究, 2020, 37(增刊 2): 256-258.
CHANG Fangyuan, LI Erxia, KANG Chaoqun, et al. Research on trusted security protection scheme of distribution terminal[J]. Application Research of Computers, 2020, 37(S2): 256-258.

[7] 俞华, 穆广祺, 牛津文, 等. 智能变电站网络安全防护应用研究[J]. 电力系统保护与控制, 2021, 49(1): 116-118.
YU Hua, MU Guangqi, NIU Jinwen, et al. Application research on network security protection of an intelligent substation[J]. Power System Protection and Control, 2021, 49(1): 116-118.

[8] 何金栋, 王宇, 赵志超, 等. 智能变电站嵌入式终端的网络攻击类型研究及验证[J]. 中国电力, 2020, 53(1): 81-91.
HE Jindong, WANG Yu, ZHAO Zhichao, et al. Type and verification of network attacks on embedded terminals of intelligent substation[J]. Electric Power, 2020, 53(1): 81-91.

[9] 黄虹, 文康珍, 刘璇, 等. 泛在电力物联网背景下基于联盟区块链的电力交易方法[J]. 电力系统保护与控制, 2020, 48(3): 22-25.
HUANG Hong, WEN Kangzhen, LIU Xuan, et al. Power trading method based on consortium blockchain under ubiquitous power internet of things[J]. Power System Protection and Control, 2020, 48(3): 22-25.

[10] 李福阳, 李俊娥, 刘林彬, 等. 智能变电站嵌入式终端安全测试方法研究[J]. 电力建设, 2021, 42(2): 126-136.
LI Fuyang, LI Jun'e, LIU Linbin, et al. Research on security testing technologies for embedded terminals in intelligent substation[J]. Electric Power Construction, 2021, 42(2): 126-136.

[11] XU Yan. A review of cyber security risks of power systems: from static to dynamic false data attacks[J]. Protection and Control of Modern Power Systems, 2020, 5(3): 190-201.

[12] 康文洋, 汤鹏志, 左黎明, 等. 基于 NB-IOT 的孤岛式微电网密钥协商协议研究[J]. 电力系统保护与控制, 2020, 48(5): 119-126.
KANG Wenyang, TANG Pengzhi, ZUO Liming, et al. Research on key agreement protocol for isolated microgrid based on NB-IOT[J]. Power System Protection and Control, 2020, 48(5): 119-126.

[13] 王雷, 李乐为, 史金伟, 等. EMS 与 DMS 间数据交互的数据传输与安全控制操作方法研究[J]. 电力系统保护与控制, 2018, 46(10): 76-79.
WANG Lei, LI Lewei, SHI Jinwei, et al. Research on data transmission and security control operation method of data interaction between EMS and DMS[J]. Power System Protection and Control, 2018, 46(10): 76-79.

[14] 李大虎, 袁志军, 黄文涛, 等. 电网安全风险闭环管控体系构建方法设计[J]. 电力系统保护与控制, 2021, 49(22): 162-164.
LI Dahu, YUAN Zhijun, HUANG Wentao, et al. Construction method design of a power grid security risk closed-loop management and control system[J]. Power System Protection and Control, 2021, 49(22): 162-164.

[15] 冯涛, 鲁晔, 方君丽. 工业以太网协议脆弱性与安全防护技术综述[J]. 通信学报, 2017, 38(增刊 2): 186-188.
FENG Tao, LU Ye, FANG Junli. Research on vulnerability and security technology of industrial Ethernet protocol[J]. Journal on Communications, 2017, 38(S2): 186-188.

[16] 张文亮, 刘壮志, 王明俊, 等. 智能电网的研究进展及发展趋势[J]. 电网技术, 2009, 33(13): 1-11.
ZHANG Wenliang, LIU Zhuangzhi, WANG Mingjun, et al. Research status and development trend of smart grid[J]. Power System Technology, 2009, 33(13): 1-1l.

[17] AMOAH R, CAMTEPE S, FOO E. Formal modelling and analysis of DNP3 secure authentication[J]. Journal of Network & Computer applications, 2016, 59: 345-360.

[18] AMOAH R, CAMTEPE S, FOO E. Securing DNP3 broadcast communications in SCADA systems[J]. IEEE Transactions on Industrial Informatics, 2016, 12(4): 1474-1485.

[19] MAJDALAWICH M, PARISI-PRESICCE F, WIJESEKERA D. DNPSec: distributed network protocol version 3 (DNP3) security framework[M] // Advances in Computer, Information, and Systems Sciences, and Engineering, Netherlands: Springer, 2007: 227-234.

[20] 张尧, 叶玲. 基于 AES 的 WSN 加密算法[J]. 计算机工程与设计, 2015, 36(3): 619-623.
ZHANG Yao, YE Ling. Encryption algorithms for wireless sensor networks based on AES[J]. Computer Engineering and Design, 2015, 36(3): 619-623.

[21] SHAHZAD A, MUSA S. Cryptography and authentication

placement to provide secure channel for SCADA communication[J]. International Journal of Security, 2012, 6: 28-44.

[22] EAST S, BUTTS J, PAPA M, et al. A taxonomy of attacks on the DNP3 protocol[C] // International Conference on Critical Infrastructure Protection, 2009, Springer, Berlin Heidelberg, 67-85.

[23] NICHOLSON A, WEBBER S, DYER S, et al. SCADA security in the light of cyber-warfare[J]. Computers & Security, 2012, 31(4): 418-436.

[24] CRAIN J A, BRATUS S. Bolt-on security extensions for industrial control system protocols: a case study of DNP3 SAv5[J]. IEEE Security & Privacy, 2015, 13(3): 74-79.

[25] CREMERS C, DEHNEL-WILD M, MIINER K, et al. Secure authentication in the grid: a formal analysis of DNP3: SAv5[C] // 22nd European Symposium on Research in Computer Security, September 11-15, 2017, Oslo, Norway: 389-407.

[26] 闫爽. 智能电网 DNP3 协议安全机制研究与实现[D]. 长沙: 国防科学技术大学, 2016.
YAN Shuang. The research and implementation of security mechanism for smart grid DNP3[D]. Changsha: University of Defense Technology, 2016.

[27] 刘茜. 面向 SCADA 系统安全分布式网络协议的设计与实现[D]. 西安: 西安电子科技大学, 2017.
LIU Qian. Design and implementation of secure distributed network protocol for SCADA system[D]. Xi'an: Xidian University, 2017.

[28] 李丹枫, 王飞, 赵国鸿. 一种大流量报文 HMAC-SM3 认证实时加速引擎[J]. 计算机工程与科学, 2021, 43(1): 82-85.
LI Danfeng, WANG Fei, ZHAO Guohong. A real-time HMAC-SM3 acceleration engine for large network traffic[J]. Computer Engineering & Science, 2021, 43(1): 82-85.

[29] 冯峰, 周清雷, 李斌. 基于多核 FPGA 的 HMAC-SHA1 口令恢复[J]. 计算机工程与科学, 2020, 42(10): 1860-1862.
FENG Feng, ZHOU Qinglei, LI Bin. HMAC-SHA1 password recovery based on multi-core FPGA[J]. Computer Engineering & Science, 2020, 42(10): 1860-1862.

[30] LU Ye, FENG Tao. Research on trusted DNP3-BAE protocol based on Hash chain[J]. EURASIP Journal on Wireless Communications and Networking, 2018: 108-118.

[31] 琚安康, 郭渊博, 朱泰铭, 等. 网络安全事件关联分析技术与工具研究[J]. 计算机科学, 2017, 44(2): 38-40.
JU Ankang, GUO Yuanbo, ZHU Taiming, et al. Survey on network security event correlation analysis methods and tools[J]. Computer Science, 2017, 44(2): 38-40.

[32] 侯连全, 章坚民, 金乃正, 等. 变电站过程层与 SMV 安全传输的网络攻击检测与取证设计[J]. 电力系统自动化, 2016, 40(17): 87-92.
HOU Lianquan, ZHANG Jianmin, JIN Naizheng, et al. Design of cyber-attack detection and evidence taking of substation process layer and SMV secure transmission[J]. Automation of Electric Power Systems, 2016, 40(17): 87-92.

[33] 傅戈, 周年荣, 文红. 智能电网工业系统通信控制协议的安全研究[J]. 信息安全与技术, 2014, 5(1): 36-38.
FU Ge, ZHOU Nianrong, WEN Hong. The study of security issues for the industrial control system communication protocols in smart grid system[J]. Information Security and Technology, 2014, 5(1): 36-38.

[34] JI C, KIM J, LEE JY, et al. Review of one-time signatures for multicast authentication in smart grid[C] // 2015 12th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT), October 19-20, 2015, Melville, NY, USA: 1-4.

[35] CHIM T W, YIU S M, LI V O, et al. PRGA: privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid[J]. IEEE Transactions on Dependable and Secure Computing, 2014, 12(1): 85-97.

收稿日期：2021-11-03；　　修回日期：2022-01-17

作者简介：

李　露(1988—)，男，硕士，工程师，从事配网终端嵌入式设计；E-mail: lilu502@163.com

谢映宏(1986—)，男，工程师，从事配网终端设计；

许永军(1977—)，男，高级工程师，从事配网终端设计。

(编辑　魏小丽)