DOI: 10.19783/j.cnki.pspc.200240

智能变电站网络安全防护应用研究

俞 华[1]，穆广祺[2]，牛津文[3]，原 辉[4]，姜 敏[5]，谷永刚[6]

(1. 国网山西省电力公司电力科学研究院，山西 太原 030000；2. 国网山西省电力公司，山西 太原 030000；
3. 许继集团有限公司，河南 许昌 461000；4. 国网山西省电力公司电力科学研究院，山西 太原 030000；
5. 国网山西省电力公司，山西 太原 030000；6. 国网陕西省电力公司，陕西 西安 710000)

摘要：近年来，随着乌克兰电网遭受网络攻击等一系列事件的发生，变电站网络安全面临着一系列新挑战。目前变电站智能设备种类繁多，面临越趋严峻的非法访问、操作越权及数据篡改等内部网络威胁。因此，提出变电站智能设备的多维度网络安全防护机制，引入多级身份认证、分布式权限验、逆向矩阵等网络加固机制，解决常见的网络攻击问题。在不影响传输效率及性能的基础上确保智能设备网络访问与控制的安全性、可靠性及健壮性。

关键词：PAXOS 算法；分布式权限验证；多级身份认证；逆向矩阵；网络加固

Application research on network security protection of an intelligent substation

YU Hua[1], MU Guangqi[2], NIU Jinwen[3], YUAN Hui[4], JIANG Min[5], GU Yonggang[6]

(1. Electric Power Research Institute of State Grid Shanxi Electric Power Company, Taiyuan 030000, China; 2. State Grid Shanxi Electric Power Company, Taiyuan 030000, China; 3. XJ Group Corporation, Xuchang 461000, China; 4. Electric Power Research Institute of State Grid Shanxi Electric Power Company, Taiyuan 030000, China; 5. State Grid Shanxi Electric Power Company, Taiyuan 030000, China; 6. State Grid Shaanxi Electric Power Company, Xi'an 710000, China)

Abstract: In recent years, with the occurrence of a series of incidents such as network attacks on Ukraine's power grid, the network security of substations is facing a series of new challenges. At present, there are many kinds of intelligent equipment in a substation, and they face increasingly severe internal cyber threats such as unauthorized access, unauthorized operation and data modification. Therefore, a multi-dimensional network security protection mechanism for substation intelligent equipment is proposed, and the network reinforcement mechanisms such as multi-level identity authentication, distributed authority verification and reverse matrix are introduced to solve the common network attack problems. In order not to affect transmission efficiency and performance, the security, reliability and robustness of network access and control of intelligent equipment are ensured.

This work is supported by Science and Technology Project of the Headquarters of State Grid Corporation of China "Research on the Auxiliary System of the Third Generation Intelligent Substation" (No. 520530180015).

Key words: PAXOS algorithm; distributed authority authentication; multi-level identity authentication; reverse matrix; network reinforcemen

0 引言

随着智能电网建设的飞速发展，变电站智能设备数量呈持续增长态势，这些设备均广泛应用了网络通信技术，网络是恶意攻击者的主要入侵渠道，随之而来的网络信息安全形势越趋严峻。

目前防范变电站外部网络安全威胁所采用的策略主要包括纵向加密、横向隔离及安全分区。变电站外部边界的网络安全防护技术也已非常成熟，主要包括屏蔽非授权访问的防火墙技术；隐藏内网主机真实 IP 地址的 NAT 技术[1]；主动防御攻击的 IDS 入侵检测系统[2]；专网网络点对点加密传输的虚拟网(VPN)技术[3]。

防范内部网络安全威胁方面，目前仅限于第三方安全监视技术的研究及应用，如：网络安全监测

基金项目：国家电网有限公司总部科技项目资助(520530180015)“第三代智能变电站辅助系统研究”

技术[4]。智能设备的本体网络安全威胁主要包括非法访问、操作越权以及数据篡改等。非法访问主要指未经身份授权的访问，如：现有智能设备大多未对运维终端进行严格身份认证，导致任意运维终端单一密码认证即可登录并进行各种控制操作；操作越权主要指对数据进行超越权限的访问，如：操作员通过权限提升以管理员权限修改智能设备关键配置信息，引起设备通信故障；数据篡改主要指入侵者通过报文重放、链路劫持等手段篡改通信数据引起错误操作，或通过修改数据库及配置文件的敏感数据引起定值错误，如：变电站内通信报文基本仍采用明文传输，极易发生报文重放及链路劫持攻击。若不能对上述网络安全漏洞进行有效防护，有可能造成继电保护系统和开关设备的误动、拒动，进而严重威胁电网的安全稳定运行。

本文针对目前变电站智能设备普遍存在的网络安全问题，提出了多维度的网络访问安全防护机制，通过引入多级认证来解决身份认证环节问题；引入 PAXOS 算法解决安全配置信息不统一问题，并对权限进行分布式[5]验证，防范操作越权；引入逆向矩阵、网络加固来解决敏感数据的明文传输与存储的问题。从而有效地防范变电站内部网络安全威胁，实现变电站智能设备安全可靠的稳定运行。

1 变电站智能设备网络架构介绍

变电站智能设备网络架构图如图 1 所示，为防范外部网络威胁，变电站划分为安全 I 区、II 区、III 区。I/II 区之间通过防火墙技术实现安全访问控制；II/III 区之间则采用横向隔离技术实现物理网络隔离；变电站与调度数据网之间采用纵向加密技术实现数据密通。按网络结构划分，变电站智能设备包括站控层、间隔层和过程层智能设备。站控层智能设备主要包含数据通信网关机、网络安全监测装置及一体化监控等；间隔层智能设备主要包括保护测控装置、在线监测装置等；过程层设备主要包括智能终端、合并单元等。

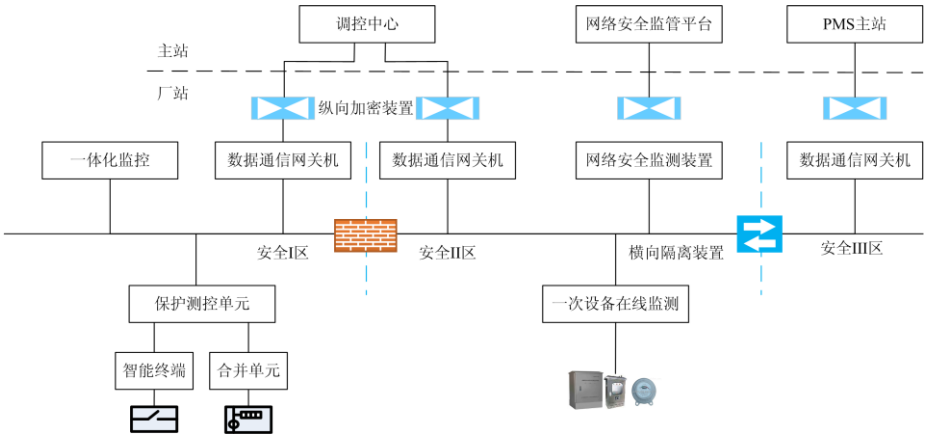

图 1 变电站智能设备网络架构图

Fig. 1 Network architecture of substation intelligent equipment

变电站智能设备包含人机接口和运维终端、采集及上传等网络接口。人机接口主要面临运维终端的非法访问及操作越权威胁，此两种安全威胁可采用与网络接口类似的安全防护机制。故本文重点针对网络接口面临的三种本体安全漏洞及威胁，以数据通信网关机[6](以下简称网关机)为例在身份认证、权限校验、数据传输及存储等多个方面对变电站智能设备进行网络安全防护。

2 多级身份认证

网关机目前针对运维终端访问的身份认证机制大多仅限于用户名密码、设置密码有效期、限制访问连接数等常用手段，缺乏一套完善的身份认证[7]机制抵御非法访问。

本节提出多级身份认证概念，即在验证用户名密码之前，网关机首先采用“数字证书+数字签名”的方式进行第一级的身份认证以确认运维终端的访问合法性；物理认证采用 UKey[8]识别码进行第二级的身份认证。除 UKey 外，指纹、虹膜等均可作为物理认证方式。

2.1 虚拟身份认证

虚拟身份认证基于国密算法[9]，尤其是在智能电网系统[10]中，采用非对称加密算法 SM2 生成数字签名、SM3 算法生成秘钥 Key，对称加密算法 SM4 进行随机数加密。其中，运维终端与网关机分别存放自身私钥与对方公钥，用于验证签名与网络数据

的加解密。虚拟身份认证方式流程图如图 2 所示。

图 2 虚拟身份认证流程图

Fig. 2 Flow chart of virtual identity authentication

虚拟身份认证请求由运维终端发起，首先使用秘钥 Key(SM3 算法生成)加密随机数[11]*S*(取值 0-65535)、运维终端私钥生成数字签名、网关机公钥加密网络数据发送给网关机。

网关机收到数据后，使用自身私钥进行解密；保存加密随机数 *S* 至本地；使用运维终端公钥验证数字签名；自身私钥加密生成数字签名，运维终端公钥加密发送给运维终端。

运维终端收到数据后用自身私钥解密，使用网关机公钥验证数字签名，如验证签名通过则表示双方双向验证签名成功。

最后，运维终端使用自身私钥对秘钥[12] Key 生成数字签名，使用网关机公钥加密发送给网关机，网关机收到后使用自身私钥解密数据，并验证对称秘钥 Key 的数字签名，验证签名通过后使用秘钥 Key 解密得到随机值 *S*。

通过以上步骤，双方虚拟身份认证流程结束，数据交互由随机值 *S* 参与首次通信报文 CRC 校验码的计算，以确保通信的抗抵赖性[13]。

2.2 物理身份认证

物理身份认证始于虚拟身份认证之后，采用插入网关机 USB 接口的 UKey 并对外部输入的识别码(或指纹[14]、虹膜[15])等信息进行身份识别，作为身份认证的第二道屏障保证运维终端使用者身份的合法性，具体认证流程如图 3 所示。

图 3 物理身份认证流程图

Fig. 3 Flow chart of physical identity authentication

虚拟身份认证结束后，网关机提示运维终端插入 UKey，并输入用户识别码；并将 UKey 内置的识别码与输入的识别码进行比对，以验证用户身份。

物理身份认证具有灵活性与可扩展性等特点，即所有即插即用设备均可通过接入网关机的 USB 接口使用，操作便捷，无需额外配置；另外，UKey 具备小巧、便于携带的优势，实际工程应用中被广泛使用。

2.3 身份认证体系扩展应用及优化

随着变电站信息安全等级的提升，运维终端作为网关机及其他智能设备的重要网络访问入口。与运维终端交互的身份数据作为关键信息也同样需要安全防护，因此采用加密芯片[16]的方式将身份信息及认证代码安全地植入到芯片中加以保护，可极大程度上保证整个认证体系的安全稳定。

另外，目前基于 IEC 61850 通信标准的 GOOSE、SV 报文由于缺乏有效的安全认证体系，同样需要加入安全认证机制，即使用报文中的保留字段及扩展字段，将数字签名、数字摘要、随机数等信息加入其中与原始报文一起发送(其中的保留及扩展字段的变换不仅满足 ASN.1 基本编码规则的 TLV 转换语法，还使得原始报文和认证报文能够在变电站自动化通信系统中兼容，符合 IEC 62351 标准)，最终实现变电站过程层通信双方 GOOSE、SV 报文安全通信的目的。

3 分布式权限校验

3.1 分布式权限校验机制

针对运维终端获取白名单参数、修改四遥信息及远程控制等关键操作的越权访问，采用权限校验机制可有效地避免此类安全威胁。常用的权限校验方

式有客户端-服务端模式和集中式权限校验模式[17]。现行验证方式为客户端-服务端模式，该模式服务端权限数据单机存储，缺少验证数据有效性的参照系。集中式权限校验模式将权限校验请求发往权限服务主机进行验证，采用此模式即使最理想情况下也需一次网络传输应答时间，若发生请求丢失和网络阻塞等情形，还需重复发送验证请求以获得理想的结果。

本文基于 PAXOS 算法[18]提出一种分布式权限校验机制，PAXOS 算法是图灵奖获得者 Leslie Lamport 提出的采用消息传递方式解决分布式领域中一致性问题的算法。采用该算法使变电站网络中的设备获得相同的操作序列，保证设备间权限数据一致。在原有 PAXOS 算法基础上添加镜像状态机[19]，可在本机建立对比参照系，在初始数据、操作序列相同情况下，获得相同的数据状态。当客户端进行权限校验时，对两个状态机中的数据进行 CRC 校验，一致的情况下则认为数据是可信的，直接在本机校验即可，若 CRC 校验不通过，则通过 PAXOS 算法进行分布式权限校验。

数据状态转移流程如图 4 所示。

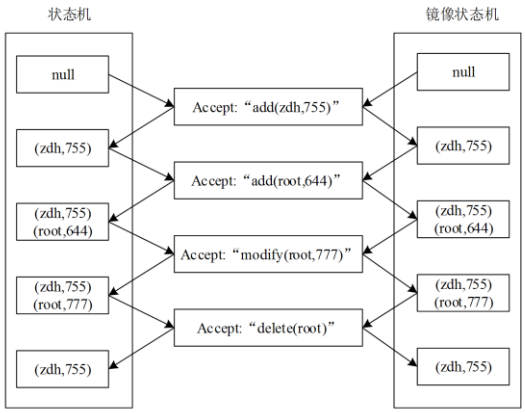

图 4 数据状态转移流程

Fig. 4 Data state transition process

3.2 分布式权限校验执行流程

在 PAXOS 算法中，有三种不同的角色，Proposer，Acceptor 和 Learner[20]，其中 Proposer 负责发起提案，Acceptor 针对提案共同确认一个值，Learner 学习已经通过的提案。

PAXOS 算法投票流程如图 5 所示。通过图 5 算法流程可知，Accept 阶段，Acceptor 根据提案编号 b 和它响应的所有 prepare 请求编号的最大值 pb 来决定是否接受提案 v。在提案 v 为错误的情况下，该提案一样会被接受并记录为 av，在随后的 PAXOS 流程中，当 Proproser 提出新的提案，若投票集合包含此 Acceptor，则此 Acceptor 会将错误的提案 av

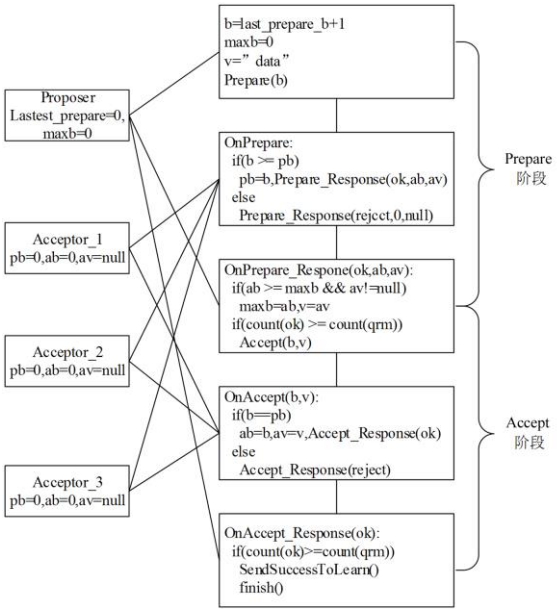

图 5 PAXOS 算法投票流程

Fig. 5 PAXOS algorithm voting process

返回给 Proproser，导致新一轮提案失败[21]。所以分布式权限校验在 PAXOS 算法基础上添加约束条件，在 Acceptor 收到编号为 b 的 prepare 请求后，不仅验证提案编号，还验证用户权限，只有大多数 Acceptor 验证用户权限正确，才能够进入到 Accept 阶段。以网关机越权操作为例，非法修改网关机数据，然后使用客户端操作，此时数据 CRC 校验不一致，进入分布式权限验证流程，如图 6 所示。

第一轮投票网关机作为 Proposer_1，向监控主机、保信子站等作为 Acceptor 的设备发起 Prepare 请求，将允许(zdh,007)授权作为提案。一半以上的设备因与自身权限信息(zdh,755)不一致拒绝该请求，故不再进行 Accept 阶段。第二轮拒绝请求的设备作为 Proposer_2，将不允许(zdh,007)授权作为提案发起 prepare 请求，经半数以上 Acceptor 响应后进入 Accept 阶段。假设由于网络等原因，没有一半以上的设备记录该提案，则进入第三轮投票，最坏情况下仍由网关机发起 Prepare 请求，由于存在设备记录过不允许(zdh,007)授权，故该设备该提案返回，第三轮进入 Accept 阶段的提案仍为不允许(zdh,007)授权，此时超过半数设备记录该提案，投票流程完成。最终的结果为不允许(zdh,007)授权，权限验证不通过。

3.3 分布式权限校验时间性能

变电站设备运行正常情况下权限验证时间性能如图 7 所示；网关机数据异常情况下权限验证时间性能如图 8 所示。

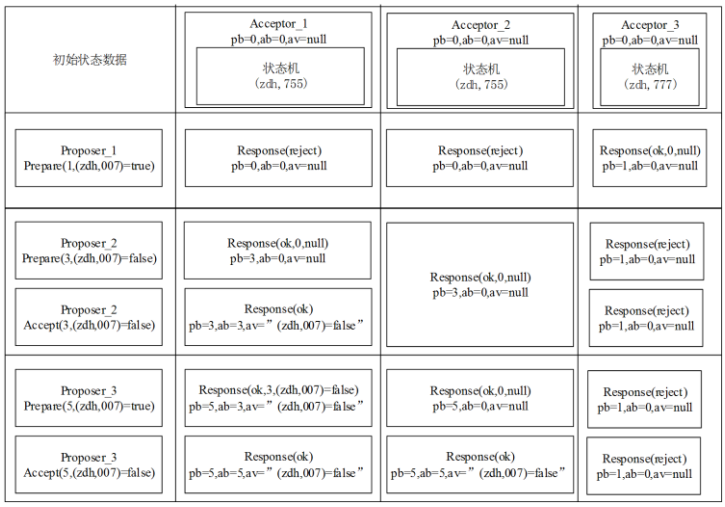

图 6 分布式权限校验流程

Fig. 6 Distributed authority verification process

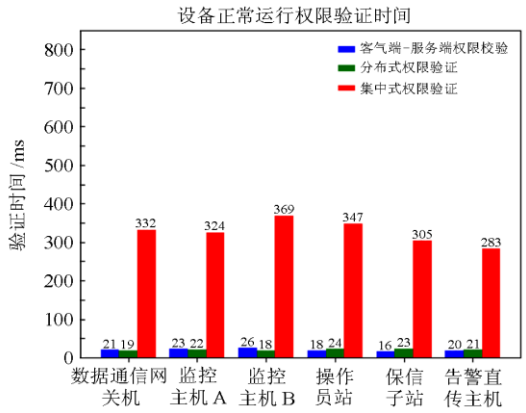

图 7 设备正常运行权限验证时间

Fig. 7 Device normal operation permission verification time

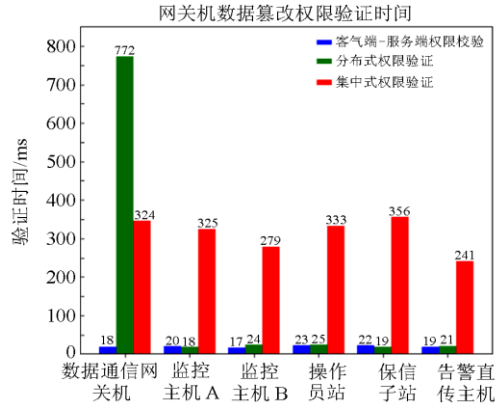

图 8 网关机数据异常权限验证时间

Fig. 8 Gateway abnormal permission verification time

从上图可知在设备正常运行情况下，采用分布式权限校验方案时间性能和客户端-服务端模式一致。在网关机数据异常情况下，监控主机、保信子站等设备不受影响，网关机权限校验耗时增加，但是有效地阻止了越权操作。

4 逆向矩阵

4.1 逆向矩阵原理

网关机数据库及配置文件中的敏感数据(如转发表、密码、通信参数等)采用加密存储，虽然在很大程度上实现了数据的保密性，但考虑到解密技术不断发展及秘钥不慎泄露的风险，加密数据很可能变得不再安全。

因此本文提出一种针对明文数据的逆向矩阵算法，将原始数据矩阵化、颗粒化、散列化，再通过 SM4 加密算法进行加密存储，这样即使密文被破解，也无法得知数据的真实含义，进一步保证了敏感数据的安全性。

4.2 逆向矩阵散列算法

逆向加密算法首先将原始数据矩阵化，每一个字节代表矩阵的一个元素，生成由 $m\times n$ 个元素排列的矩阵 $\boldsymbol{A}$，如式(1)所示。

$$\boldsymbol{A}=\begin{bmatrix}\alpha_{11} & \alpha_{12} & \alpha_{13} & \cdots & \alpha_{1n}\\ \alpha_{21} & \alpha_{22} & \alpha_{23} & \cdots & \alpha_{2n}\\ \alpha_{31} & \alpha_{32} & \alpha_{33} & \cdots & \alpha_{3n}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \alpha_{m1} & \alpha_{m2} & \alpha_{m3} & \cdots & \alpha_{mn}\end{bmatrix} \tag{1}$$

将矩阵 $\boldsymbol{A}$ 进行转置操作 $(\boldsymbol{A})^{\mathrm{T}}$ 生成矩阵 $\boldsymbol{B}$，如式(2)所示。

$$\boldsymbol{B}=\begin{bmatrix}\alpha_{11} & \alpha_{12} & \alpha_{13} & \cdots & \alpha_{m1}\\ \alpha_{12} & \alpha_{22} & \alpha_{23} & \cdots & \alpha_{m2}\\ \alpha_{13} & \alpha_{32} & \alpha_{33} & \cdots & \alpha_{m3}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \alpha_{1n} & \alpha_{2n} & \alpha_{3n} & \cdots & \alpha_{mn}\end{bmatrix} \tag{2}$$

然后，将矩阵 $\boldsymbol{B}$ 通过逆向算法生成矩阵 $\boldsymbol{C}$，以达到无法识别原始数据的目的，具体步骤如下：

1) 矩阵 $\boldsymbol{B}$ 每一行的第 i 个元素($i\geqslant 1$)依次与 $m-i-1(m>i)$ 个元素进行位置互换，生成矩阵 $\boldsymbol{B}_1$。

2) 将矩阵 $\boldsymbol{B}_1$ 每一列的第 j($j\geqslant 1$)个元素依次与 $n-i-1(n>j)$ 的元素进行位置互换，生成 $\boldsymbol{B}_2$。

3) 将矩阵 $\boldsymbol{B}_2$ 中第 $i=j$ 的元素依次与第 $m-i-1=n-j-1$ 的元素进行位置互换，生成矩阵 $\boldsymbol{C}$。

最后将矩阵 $\boldsymbol{C}$ 序列化为字符串，使用 SM4 算法将字符串进行加密为密文存储到本地。

对于矩阵规模的选择，m 与 n 的值根据明文数据长度 len 及公式 $m\times n\geqslant len$；$m=n$ 计算得出；如需获得明文数据，对逆向加密流程反向操作即可。

4.3 逆向矩阵测试实验

网关机作为变电站主厂站协同互动的关键设备，存储大量敏感信息，如用户数据、转发表 RCD 文件[22]、通信参数等。这些信息在加密存储之前进行矩阵逆向操作，确保运维终端网络访问网关机并获取配置信息时，即使信息泄露也无法取得真实数据。本节以存储四遥信息的 RCD 文件为例，验证网关机配置文件矩阵逆向后的安全性与保密性。

RCD 配置文件记录网关机标准化的四遥数据信息，如图 9 所示。

```
<!Entity=RCD Version=1.0 Code=UTF-8 data=1.0 time='2018-05-06 09:41:24'!>
<E>
<变电站 name="国家电网.公司名称.500kV沭阳变" link="省调">
<版本信息>
@    sn    model_type    version    manufacturer
//    序号    模型类型    版本号    制造厂商
#    1    SCD    V3.6    COMPANY
#    2    RCD    V1.0    COMPANY
</版本信息>
<合并计算参与量信息>
@    sn    reference    des    alias
//    序号    IEC61850路径名    中文描述    别名
# 1 CB5043CTRL/BinInGGIO2$ST$Ind2$stVal 智能终端开关压力低禁止重合闸 OP1
</合并计算参与量信息>
<合并计算生成量>
@    sn    merge_des    data_id    alias    expression    type    private
//    序号    中文描述    本地标识    别名    表达式    类型    私有信息
#    1    开关油压低重合闸    DST10    ALIAS1    OP1|OP2    YX    NULL
</合并计算生成量>
<遥信转发信息>
@ sn yx_no ref des alias type negative timeTag private
// 序号 点号 路径名 中文描述 别名 类型 极性 是否带时标 私有信息
# 1 2 GGIO7$ST$DPCSO1$stVal 5042开关 SinglePoint Positive true NULL
</遥信转发信息>
<遥测转发信息>
@ sn yc_no ref des alias type timeTag factor offset threshold private
// 序号 点号 路径名 中文描述 别名 类型 时标 系数 基准值 死区 私有信息
# 1 2 phsA$cVal$mag$f 断路器Ia NULL FloatValue false 1.0 0.0 0.0 NULL
</遥测转发信息>
<遥控转发信息>
@ sn yk_no ref des type overtime controlMode LockPoint LockSate private
// 序号 点号 路径名 中文描述 类型 超时 模式 关联遥信 关联状态 私有信息
# 1 2 CBSynCSWI1$CO$Pos 5042开关 DPoint 60000 SControl NULL none NULL
</遥控转发信息>
</变电站>
</E>
```

图 9 网关机 RCD 文件

Fig. 9 Gateway RCD file

通过对 RCD 配置文件进行矩阵化、转置、散列操作，生成逆序的新矩阵，如图 10 所示。

从图 10 中可以看出，RCD 配置文件矩阵化之后通过逆向算法生成新的矩阵即使没有进行加密，也无法从中识别出真实信息。

4.4 逆向矩阵实验结果分析

当运维终端在线获取网关机配置文件时，即使发生数据与秘钥泄露，也无法通过解密获取到真实的明文数据，这就保证了原始数据的隐私安全。

图 10 RCD 文件矩阵逆向化

Fig. 10 RCD file matrix reverse

实验中，网关机敏感数据均采用逆向矩阵存储，因此运维终端读取相关信息时需将逆向矩阵反向还原后展示，并且当运维终端修改数据后，仍然需要将数据进行矩阵逆向后发送给网关机。随着数据容量的增加，读写效率与用户体验会在一定程度上受到影响，以下针对某变电站现场实际工程项目对网关机的读写效率进行对比。

如图 11、图 12 所示，由于网关机数据库与单个配置文件容量大小在 1 MB 左右，因此实际应用过程中读写效率的差异在可控范围内，不会影响使用效率与用户体验。

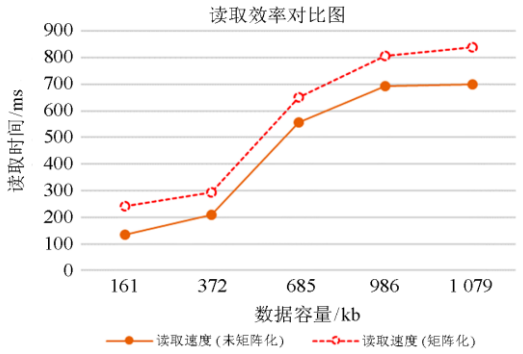

图 11 矩阵化读取效率对比图

Fig. 11 Matrix reading efficiency comparison chart

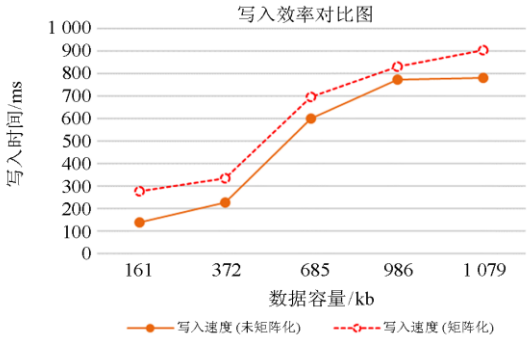

图 12 矩阵化写入效率对比图

Fig. 12 Matrix write efficiency comparison chart

4.5 优势与不足

本次测试数据包含网关机的数据库与配置文件，测试结果显示，在保证信息安全的情况下，运维终端对网关机的所有操作均正常运行。

网关机内逆向存储的数据库及配置文件均为私有数据，不允许除定制运维终端外的任意工具及任意方式的读写操作，因此最大程度上保证了敏感数据的隐私性与保密性。

针对基于 IEC 61850 标准的公共配置文件(如 SCD 等)采用非矩阵密文的方式存储在网关机内，具备管理员权限的用户均可登录运维终端将 61850 配置文件以明文形式导出至本地或导入网关机，便于不同厂家之间、主厂站之间完成互操作。

但是逆向矩阵模式仅支持运维终端在线网络安全访问机制，并未涉及离线配置，有待进一步提升优化。

5 网络加固

5.1 网络加固机制介绍

为抵御运维终端与网关机数据交互过程中的重放攻击、中间人攻击等网络攻击手段，简单粗暴的交互流程由于缺乏相应的网络防护机制已不再适应当前的网络环境。因此，需要引入防劫持保护机制，即对交互的数据加入发送/接收序号、CRC 校验[23]、密文传输等保护手段；并对网关机进行访问的 IP 地址、端口号进行可信认证及连接数限制，以确保数据交互的安全性、可靠性[18]、一致性、不可逆性。交互数据帧格式如表 1 所示。

表 1 网络数据帧格式

Table 1 Network data frame format

报文内容		长度	说明
起始报文		1 字节	自定义
数据内容长度		2 字节	网络字节序
结束报文		1 字节	自定义
发送/接收序号		1 字节	网络字节序
数据内容	数据	*N* 字节	通信双方交互内容
	随机数	8 字节	由发送方生成
	时间戳	4 字节	本地时间转换 UTC 时间后相对于 UTC 时间 1970-01-01 00:00:00 00:00 所经历的秒数。网络字节序
	签名值	64 字节	SM2 签名
CRC 校验和		1 子节	数据内容校验和

由表 1 可以看出发送序号为发送端对发送报文的累加，依次加 1，接收序号为接收端接收报文的累加，依次加 1。收到报文的一方将发送/接收序号与自身存储的上一帧发送/接收序号进行比对，来判断是否为将要接收的正确报文，对于序号错误的数据帧进行丢弃处理。发送/接收序号初始值由运维终端随机生成。通过对发送/接收序号的判断可以有效防止重放攻击[24]。与传统 TCP 协议中 SEQ/ACK 不同的是，初始发送/接收序号由系统随机生成，而不是从 0 开始计数，并且 TCP 协议的 SEQ/ACK 主要应用于传输层数据丢包时的处理，而本文提出的发送/接收序号则用于防止应用层数据被第三方恶意

截获并发起重放攻击，因此应用层的发送/接收序号适用于所有应用系统的网络数据传输安全功能。

数据内容在身份认证阶段由对方公钥加密传输，身份认证结束后由对称加密算法 SM4[25]进行加密传输。

时间戳为当前时间相对于 1970-01-01 00:00:00 00:00 所经历的秒数，网关机收到运维终端的重要操作(如程序升级、配置变更等)时，将本地时间与报文中的时间戳进行比较，当时间差值超过一定范围(如 30 s，可配置)则直接丢弃此数据帧。

签名值使用私钥通过 SM2 算法对数据内容(签名值除外)加入 64 字节的数字签名，接收端解密后首先进行验证签名，如果验签出错则直接丢弃此帧报文。

CRC 校验和在身份认证阶段由数据内容计算得出，身份认证结束后由数据内容与对方随机数共同计算得出，网关机收到报文后首先验证 CRC 是否正确，如果验证错误则直接丢弃此帧，以防止中间人攻击[26]。

5.2 重放攻击攻防实验

重放攻击是指攻击者发送一个目标主机已接收过的数据包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。

假设运维终端与网关机在身份认证阶段，攻击者利用网络监听或者其他方式盗取认证凭据请求，之后再把它重新发给认证网关机，达到获取认证凭证的目的。

重放攻击身份认证流程如图 13 所示。

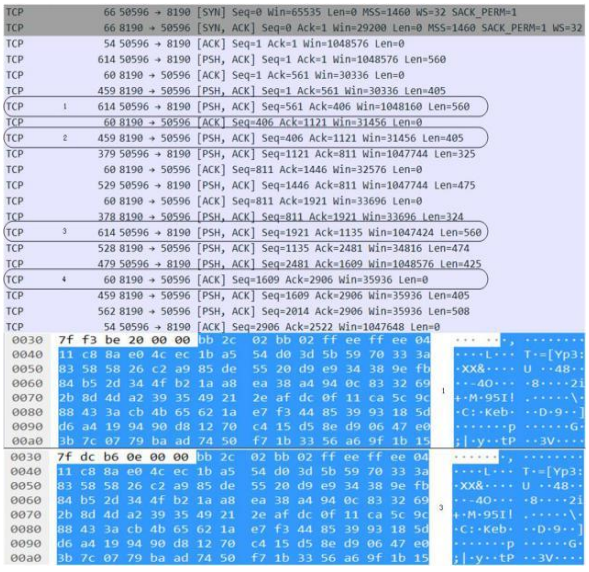

图 13 身份认证重放攻击网络数据

Fig. 13 Identity authentication replay attack network data

从图 13 中可以看出，运维终端发送身份认证凭证请求(框体 1)，网关机回复身份认证凭证确认(框体 2)。此时，当攻击者截获此帧报文并伪造运维终端 IP 地址及端口号并重复发送给网关机企图再次获取身份认证凭证时(框体 3)，由于未加入重放攻击防御机制，因此网关机再次回复身份认证凭证确认帧(框体 4)。

防御重放攻击机制身份认证流程如图 14 所示。

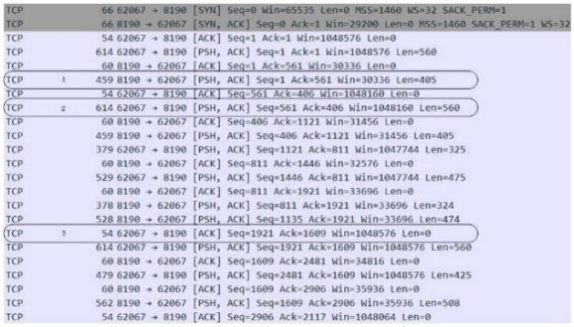

图 14 身份认证重放攻击防御网络数据

Fig. 14 Authentication back to attack defense network data

从图 14 中可以看出，当攻击者截获身份认证凭证报文(框体 1)并伪造运维终端 IP 地址及端口号重新将报文(框体 3)发送给网关机企图再次获取身份认证凭证时，由于数据帧发送/接收序号、随机数均相同，因此网关机在不影响正常通信流程的基础上丢弃此数据帧以达到防御重放攻击的目的(网关机未回复框体 3 的身份认证凭证请求)。

另外，如果重放攻击时间间隔过长，导致时间戳与本地时间差超阈值也会被认定为非法数据帧进行丢弃处理。

5.3 网络加固机制扩展应用

网络加固机制作为基于 TCP/IP 协议的安全通信手段主要应用于变电站站控层智能设备；但是作为智能变电站间隔层、过程层的 GOOSE、SV 电力报文有可能跨区域、跨电网传输，使得其更可能遭受窃听、攻击、篡改等入侵事件，其在电力信息安全方面的重要性愈发突出，因此针对 GOOSE、SV 报文引入网络安全加固机制实现网络数据的完整性和保密性成为了问题的关键。

首先提取 GOOSE、SV 报文中的关键信息并计算其长度，使用通信双方公钥对关键信息及随机数进行加密，并使用身份认证阶段存储的对端随机数与数据内容计算 CRC，最后将发送/接收序号加入到保留字段完成网络安全加固，实现智能变电站间隔层、过程层网络数据的完整性、保密性传输。

6 结论

本文提出的一套网络安全防护应用机制从访问、权限、数据传输及存储等四个方面解决变电站智能设备内部网络安全威胁，针对用户网络访问的身份识别引入多级认证机制，即对用户的身份进行虚拟与物理的多因子认证，从而实现双重抗抵赖。采用 PAXOS 算法，解决了安全配置数据及权限信息不统一的问题，并进行分布式权限验证。针对敏感数据的保护引入逆向矩阵机制，即将明文数据矩阵化，并通过逆向矩阵算法使之散列无序排列，最后使用 SM4 算法加密存储，达到双重保护的目的。针对网络数据交互过程中可能出现的重放攻击、中间人攻击等常用攻击手段，引入防劫持保护机制，对网络数据加入发送/接收序号、CRC 校验、时间戳比较、密文传输等机制，确保数据的安全性、一致性、不可逆性。

本防护方案可部署于一体化监控服务器、I/II 区数据通信网关机等智能设备中，有效提升了变电站智能设备内部网络安全，规避了非法访问、越权操作及数据篡改的网络风险。

参考文献

[1] 孟卿卿, 王建勇. GB/T28181 协议 NAT 穿越方案研究[J]. 信息技术, 2020, 44(3): 148-152.
MENG Qingqing, WANG Jianyong. Study on NAT crossing scheme of GB/T28181 protocol[J]. Information Technology, 2020, 44(3): 148-152.

[2] 张立静, 盛戈皞, 江秀臣. 泛在电力物联网在变电站的应用分析与研究展望[J]. 高压电器, 2020, 56(9): 1-10.
ZHANG Lijing, SHENG Gehao, JIANG Xiuchen. Application analysis and research prospects of ubiquitous power internet of things in substation[J]. High Voltage Apparatus, 2020, 56(9): 1-10.

[3] 蒋斌. VPN 下的电网调度数据网网络安全策略[J]. 通讯世界, 2019, 26(12): 230-231.
JIANG Bin. Network security strategy of grid dispatching data network under VPN[J]. Communication World, 2019, 26(12): 230-231.

[4] 赵隆, 张甜, 黄新波, 等. 智慧输电线路接续管状态实时感知技术研究[J]. 高压电器, 2020, 56(9): 114-121, 128.
ZHAO Long, ZHANG Tian, HUANG Xinbo, et al. Research on the state-aware technology of smart transmission line tension splice connector[J]. High Voltage Apparatus, 2020, 56(9): 114-121, 128.

[5] CHEN Haoyong, WANG Xiaojuan, LI Zhihao, et al. Distributed sensing and cooperativeestimation/detection of ubiquitous powerinternet of things[J]. Protection and Control of Modern Power Systems, 2019, 4(2): 151-158. DOI: 10.1186/s41601-019-0128-2.

[6] 彭志强, 徐春雷, 张琦兵, 等. 电力系统通用服务协议一致性测试技术[J]. 电力系统保护与控制, 2020, 48(3): 84-91.
PENG Zhiqiang, XU Chunlei, ZHANG Qibing, et al. Conformance testing technology of power system general service agreement[J]. Power System Protection and Control, 2020, 48(3): 84-91.

[7] 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.

[8] 朱智强, 林韧昊, 胡翠云. 基于数字证书的 openstack 身份认证协议[J]. 通信学报, 2019, 40(2): 188-196.
ZHU Zhiqiang, LIN Renhao, HU Cuiyun. Openstack authentication protocol based on digital certificate[J]. Journal of Communications, 2019, 40(2): 188-196.

[9] 卢希. 国产密码算法的安全/可信之路[J]. 智能建筑与智慧城市, 2019(3): 11-12.
LU Xi. The way of security and credibility of domestic cryptographic algorithms[J]. Intelligent Building and Smart City, 2019(3): 11-12.

[10] KUMAR D S, SAVIER J S, BIJU S S. Micro-synchrophasor based special protection scheme for distribution system automation in a smart city[J]. Protection and Control of Modern Power Systems, 2020, 5(1): 97-110. DOI: 10.1186/s41601-020-0153-1.

[11] 刘芹, 彭在兴, 王颂, 等. 基于随机森林算法的断路器分合闸线圈故障电流曲线识别[J]. 高压电器, 2019, 55(7): 93-100.
LIU Qin, PENG Zaixing, WANG Song, et al. Fault current curves identification of circuit breaker opening/closing coil based on random forest algorithm[J]. High Voltage Apparatus, 2019, 55(7): 93-100.

[12] 黄宇鹏, 余涛, 应志玮, 等. 基于混合加密安全传输信息的虚拟电厂交易系统[J]. 信息技术与信息化, 2020(3): 88-91.
HUANG Yupeng, YU Tao, YING Zhiwei, et al. Virtual power plant transaction system based on mixed encryption and secure transmission of information[J]. Information

Technology and Informatization, 2020(3): 88-91.

[13] 景泉, 李晓东, 金鑫, 等. 抗双方泄漏抵赖的云端数据托管协议[J]. 计算机应用与软件, 2018, 35(9): 281-287.
JING Quan, LI Xiaodong, JIN Xin, et al. Cloud data escrow Protocol against both sides' disclosure and repudiation[J]. Computer Application and Software, 2018, 35(9): 281-287.

[14] 田纯青. 身份认证技术在电力行业移动应用中的应用[J]. 现代信息科技, 2019, 3(10): 160-161.
TIAN Chunqing. Application of identity authentication technology in mobile application of power industry[J]. Modern Information Technology, 2019, 3(10): 160-161.

[15] 郑杰生, 温柏坚, 吴广财. 移动网络环境下实现电力移动终端的安全通信[J]. 信息技术, 2019, 43(4): 57-61.
ZHENG Jiesheng, WEN Baijian, WU Guangcai. Secure communication of electric power mobile terminal in mobile network environment[J]. Information Technology, 2019, 43(4): 57-61.

[16] 何安平, 郭慧波, 冯志华, 等. 基于异步电路设计的RSA 算法加密芯片[J]. 计算机工程与设计, 2019, 40(4): 906-913.
HE Anping, GUO Huibo, FENG Zhihua, et al. RSA algorithm encryption chip based on asynchronous circuit design[J]. Computer Engineering and Design, 2019, 40(4): 906-913.

[17] 任伟, 徐子立, 宋晓林, 等. 基于数据挖掘的配网数字化计量系统运行特性监测和评价方法研究[J]. 高压电器, 2020, 56(8): 183-191.
REN Wei, XU Zili, SONG Xiaolin, et al. On-site monitoring and evaluation method of operation characteristics of mv distribution digital metering system based on data mining technique[J]. High Voltage Apparatus, 2020, 56(8): 183-191.

[18] LAMPORT L. The part-time parliament[J]. ACM Transactions on Computer Systems, 1998, 16(2): 133-169.

[19] 王江, 章明星, 武永卫, 等. 类 Paxos 共识算法研究进展[J]. 计算机研究与发展, 2019, 56(4): 692-707.
WANG Jiang, ZHANG Mingxing, WU Yongwei, et al. Research progress of Paxos-like consensus algorithm[J]. Journal of Computer Research and Development, 2019, 56(4): 692-707.

[20] 杨革, 徐虹. Paxos 算法的研究与改进[J]. 科技创新与应用, 2017(7): 25-26.
YANG Ge, XU Hong. Research and improvement of paxos algorithm[J]. Technology Innovation and Application, 2017(7): 25-26.

[21] 常小强, 宋政湘, 王建华. 基于蒙特卡罗算法的电动汽车充电负荷预测及系统开发[J]. 高压电器, 2020, 56(8): 1-5.
CHANG Xiaoqiang, SONG Zhengxiang, WANG Jianhua. Electric vehicle charging load prediction and system development based on Monte Carlo algorithm[J]. High Voltage Apparatus, 2020, 56(8): 1-5.

[22] 彭志强, 刘翌, 罗俊, 等. 智能变电站监控信息自动验收体系架构及关键技术[J]. 电力系统保护与控制, 2020, 48(7): 174-181.
PENG Zhiqiang, LIU Yi, LUO Jun, et al. Architecture and key technologies of automatic acceptance system for monitoring information of intelligent substation[J]. Power System Protection and Control, 2020, 48(7): 174-181.

[23] 叶远波, 陈晓东, 项忠华, 等. 基于间隔 CRC 校验码的智能变电站改扩建配置文件定位研究[J]. 电力系统保护与控制, 2020, 48(6): 173-179.
YE Yuanbo, CHEN Xiaodong, XIANG Zhonghua, et al. Research on the location of configuration file for the reconstruction and expansion of intelligent substation based on interval CRC check code[J]. Power System Protection and Control, 2020, 48(6): 173-179.

[24] XIONG Li, NIU Jianwei, KUMARI S, et al. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments[J]. Journal of Network and Computer Applications, 2018, 103(1): 194-204.

[25] 蒋炯炜, 洪泽, 陈振娇. SM4 加密算法在车联网上的应用[J]. 计算机与网络, 2020, 46(3): 58-60.
JIANG Jiongwei, HONG Ze, CHEN Zhenjiao. Application of SM4 encryption algorithm in the internet of vehicles[J]. Computer and Network, 2020, 46(3): 58-60.

[26] SAQIB N. Key exchange protocol for WSN resilient against man in the middle attack[C] // 2016 IEEE International Conference on Advances in Computer Applications, October 24-25, 2016, Coimbatore, India: 265-269.

收稿日期：2020-04-10； 修回日期：2020-10-01

作者简介：

俞 华(1980—)，男，硕士，正高级工程师，从事高压设备状态评价技术研究工作；E-mail: yuhuadky@sx.sgcc.com.cn

穆广祺(1963—)，男，硕士，正高级工程师，从事变电运行检修管理工作；E-mail: muguangqi@sx.sgcc.com.cn

牛津文(1984—)，男，通信作者，硕士，工程师，从事电力系统自动化产品、计算机网络通信研究工作。E-mail: niujinwen@xjgc.sgcc.com.cn

（编辑 姜新丽）