



电力移动巡检中基于区域划分的 无线传感器安全通信及防泄露定位技术

徐敏, 彭林, 韩海韵, 李尼格, 侯战胜

(国网智能电网研究院, 江苏 南京 210003)

摘要:为了解决电网传感器传输效率低及安全问题,保障电网的正常运行,以降低网络负担、提高系统接入安全度为目标,设计了一种基于区域划分的采用时间同步校验技术进行身份认证的无线传感器安全通信及防泄露私钥定位技术,将电力传输网中海量的传感器分区域划分,有效提高了电网数据传输的效率。通过防泄露私钥定位技术,防范了坐标映射表的泄露给电网数据信息带来的风险。通过私钥及时间戳交叉认证技术,有效地增加了系统通信的安全等级。

关键词:私钥及时间戳交叉认证;高强度加密算法套件;防泄露私钥

中图分类号:TP393

文献标识码:A

doi: 10.11959/j.issn.1000-0801.2016065

Wireless sensor security communication and anti-leak locating technology based on region partition in power mobile inspection

XU Min, PENG Lin, HAN Haiyun, LI Nige, HOU Zhansheng

State Grid Smart Grid Research Institute, Nanjing 210003, China

Abstract: In order to solve the problem of low transmission efficiency and security of the grid, ensure the normal operation of power network, reduce network burden and improve the security of system access, a secure communication and private key location technology of wireless sensor based on region partition was designed by using the technology of time synchronization verification. The power transmission network in the vast amount of sensor partition effectively improved the efficiency of power grid data transmission. The risk of leakage of the coordinate mapping table to the grid data information was prevented by the leakage of the private key location technology. Through the private key and the time stamp authentication technology, the security level of the system communication was effectively increased.

Key words: private key and timestamp cross certification, high strength encryption algorithm suite, leak proof private key

1 引言

随着计算机网络技术、通信技术、嵌入式技术和传感

器技术的飞速发展和日益成熟,具有感知能力、计算能力和通信能力的微型传感器及其构成的无线传感器网络(wireless sensor network, WSN)引起了人们的极大关注。



(2)中心节点接收到来自传感器的信息后,解析该信息。识别出其所属区域的节点识别码后进行判断分析,只有节点标识码与自己的节点匹配后,方才进行数据的汇入;否则,视为无效信息进行丢弃处理。中心节点接收完所属区域所有传感器的数据信息后,进行数据特征提取,获得每个传感器的特征向量,将各种传感器的数据分成有意义的群组,并对不同传感器的冗余信息进行加权,利用最小二乘估计算法^[2]计算加权平均值,最后融合这些传感器的特征向量获得联合特征向量。

(3)中心节点将传感器数据融合后,利用时间同步模块发出指令,与服务器进行时间同步,调用硬件加密卡接口的摘要算法——SM3 散列运算进行预处理,并与系统时间戳再次进行 SM3 散列运算验证,最终利用中心节点的私钥进行 SM2 签名运算^[3],具体处理过程如下。

步骤 1 对中心节点的节点标识码和中心节点证书的公钥进行 SM3 散列运算得到 Z 值,运算式为: $Z=SM3(ENTL+NodeCode+a+b+xG+yG+xA+yA)$,其中,ENTL 是由 2 byte 表示的 NodeCode 的比特长度;NodeCode 为节点标识码; a 、 b 为系统曲线参数; xG 、 yG 为基点; xA 、 yA 为用户的公钥^[4,5]。

步骤 2 使用 Z 值和待签名消息 M ,通过 SM3 杂凑运算得到摘要值 H 。摘要值 H 用于 SM2 数字签名。运算式为: $H=SM3(Z+M)$ 。

步骤 3 获取中心节点系统时间戳 T 作为待签名信息,再次使用 Z 值,通过 SM3 杂凑运算得到摘要值 Y 。摘要值 Y 用于 SM2 数字签名。运算式为: $Y=SM3(Z+T)$ 。

步骤 4 使用终端的证书私钥,对经过 SM3 散列预处理后的信息 H 和 Y 进行 SM2 签名运算得到签名值结果 S , $S=SM2(H+Y)$,加入节点标识码信息后,将 S 传递给服务器,具体传输数据格式如图 3 所示。

(4)服务器接收到来自中心节点的信息后,将信息分组分解,读取加密套件标志位,选择指定的加密算法,调用硬件加密卡接口使用 SM3 摘要算法,将本地证书在预处理后进行散列,之后用 SM2 算法进行信息的验证。具体处理过程如下。

步骤 1 对中心节点的节点标识码和中心节点证书的公钥进行 SM3 散列运算得到 Z 值,运算式为: $Z=SM3$

$(ENTL+NodeCode+a+b+xG+yG+xA+yA)$ 。

步骤 2 使用 Z 值和待签名消息 M ,通过 SM3 散列运算得到摘要值 H 。摘要值 H 用于 SM2 数字签名。运算式为: $H=SM3(Z+M)$ 。

步骤 3 获取服务器系统时间戳 T 作为待签名信息,再次使用 Z 值,通过 SM3 杂凑运算得到摘要值 Y 。摘要值 Y 用于 SM2 数字签名。运算式为: $Y=SM3(Z+T)$ 。

步骤 4 使用网关服务器的公钥,对经过 SM3 散列预处理后的信息 H 和 Y 进行拼接组合,并和中心节点传来的签名值 S 进行 SM2 验签运算,得到结果 $Q=SM2(H+Y+S)$,并判断 Q 值是否为真,若为真,则说明中心节点的证书合法,验证通过;否则,说明中心节点的证书非法,中断与中心节点的连接。

步骤 5 在验证通过后,中心节点将所属传感器的信息发送至后台的身份认证服务器上。

(5)处于工作内网的服务器接收到中心节点的认证信息后,建立数据连接,利用加密套件标志位指定的对称加密算法——SM1 算法,对中心节点传来的加密信息进行解密运算后,最终获取现场传感器经中心节点融合处理过后的监测数据。

3 基于私钥定位的无线传感器防泄密定位技术

电力移动巡检中,巡检人员通过移动终端发现输电线路故障后,最重要的是准确获知发生故障的线路节点,以便用最快的速度赶去现场进行检修工作,因此无线传感器定位技术便成了其中的重要研究方向。最简单的方法是在传感器上安装 GPS(global positioning system,全球定位系统)装置,获取传感器的位置信息,但由于电力传输网的传感器具有数量巨大且安装后位置变化不明显等特点,给每个传感器安装 GPS 模块会耗费巨大的成本,且后续的维护工作也将异常繁琐,因此必须设计一套行之有效的办法,既能节约成本又能准确获知传感器的位置,并且能阻止黑客等从外部获取传感器位置信息,防止电网关键数据泄露。

针对电网传感器的数量大且位置较为固定等特点,可以采用基于私钥定位的无线传感器防泄密定位技术,满足电网对传感器定位及防泄密的需求。对于数量较少且分布

服务器地址 (8 bit)	分组长度 (4 bit)	节点编码 (2 bit)	签名值(S) (32 bit)	加密套件 (2 bit)	私钥散列值 (256 bit)	传感器位置 (8 bit)	数据
------------------	-----------------	-----------------	--------------------	-----------------	--------------------	------------------	----

图 3 中心节点数据传输格式

较为集中的中心节点服务器,在安装服务器的过程中,利用 GPS 模块进行位置的测量并进行记录,与每个中心节点独一无二的私钥证书散列码进行关联,生成中心节点分布图,对于数量大且分布随机的无线传感器,利用 APIT 算法^[6]测量各传感器相对于中心节点的位置,经过中心节点分布图的加权计算,便可得知该无线传感器的准确位置信息。

APIT 算法属于距离无关、区域相关的定位策略。其实现简单,定位成本低,传感器节点功耗小,定位精度高,因而得到广泛应用。如图 4 所示,它的基本算法是从待定位节点周围的锚节点中任意选取 3 个,组合成一个三角形,判断该点是否位于该三角形内。如果在三角形内,则将其标记,依次对待定位节点周围的锚节点进行各种不同组合并检测,最终找出所有满足要求的三角形重叠区域,求其质心位置以替代待定位节点在网络中的具体位置坐标。

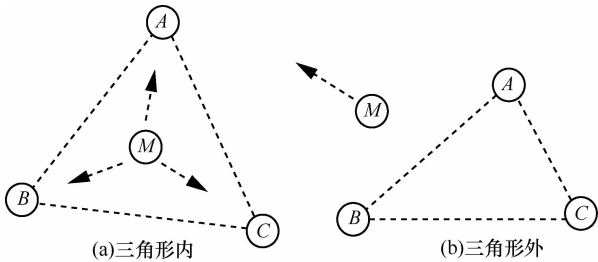


图 4 APIT 算法原理

具体定位步骤如下。

(1)设备安装人员将无线传感器安装到对应的节点位置,并设置其对应的中心节点区域。

(2)安装人员安装中心节点服务器时,利用 GPS 模块获取该服务器的坐标信息 G ,上传至服务器,中心节点自动利用其对应的私钥签名值 S 进行散列运算,得到摘要值 H ,运算式为: $H=SM3(S)$,并将摘要值 H 发送至服务器。

(3)安装人员安装完毕全部中心节点后,服务器汇聚所有上传的中心节点私钥散列值数组 $\{H_n\}$ 及安装人员上传的坐标信息数组 $\{G_n\}$,将私钥散列值与坐标信息进行关联,自动生成坐标映射表,如图 5 所示。

(4)中心节点收到所属区域传感器传来的数据信息后,进行数据融合分析,对监测数据超出预警的传感器数值进行标记,利用 APIT 算法计算出报警传感器相对于中心节点的传感器相对位置信息 A 。

(5)如图 3 所示,中心节点在与服务器通信过程中,除了发送自身节点标识码、签名信息、加密套件标识码之外,

$$\begin{Bmatrix} SM3(S_1) & \cdots & SM3(S_j) \\ \vdots & \ddots & \vdots \\ SM3(S_j) & \cdots & SM3(S_n) \end{Bmatrix} \times \begin{Bmatrix} G_1 & \cdots & G_i \\ \vdots & \ddots & \vdots \\ G_j & \cdots & G_n \end{Bmatrix}$$

私钥散列值	坐标位置
BH4D1DSCD2QWDEW...	(118.543,32.043)
XSACSCSD324R4F4...	(118.214,32.333)
E32ETVFD34RF43G...	(118.346,32.543)
D34G54G45G54G34...	(118.814,32.313)
...	...

图 5 坐标映射关系

还附加了自身私钥 256 bit 的散列值及 8 bit 传感器相对位置信息,服务器收到该散列值后,自动匹配坐标映射表,从而获取该中心节点的位置信息 Z ,并根据传感器相对位置信息进行加权系数 J 调整计算,从而获知报警传感器的准确位置信息 $P=Z+J \times A$ 。

(6)根据系统设定,定期进行中心节点的私钥自动更新操作,因此即使内部坐标映射表信息泄露,一旦私钥更新完毕,根据旧的映射表仍然无法获知报警的中心节点及传感器详细位置信息,有效地保障了电力传输信息的安全可靠程度。

传统的中心节点依靠设备编号进行区分识别定位,但是其安全性往往遭到质疑。中心节点的设备编号是固定的,通过特定程序便可读取设备编号,一旦中心节点分布图遭到泄露,中心节点以及传感器的位置信息就会泄露,且后续无法修改,除非更换中心节点硬件设备。采用私钥技术定位中心节点是动态的,每个中心节点有唯一的私钥和共用的公钥,私钥可以用来加解密运算,也能进行定位关联,且可以定期自动更新私钥,即使中心节点分布信息泄露,一旦私钥启动更新,旧的分布信息也没有用处,泄露者无法根据旧的定位信息了解目前中心节点的位置状态。利用 APIT 算法对中心节点所属区域的传感器进行无线定位,计算传感器相对中心节点的位移,从而计算出报警传感器的准确位置,窃听者即使获知传感器的位移信息,由于其无法知晓中心节点的位置,依然无法获取报警传感器的准确位置,从而保障了传感器数据通信的安全。

4 性能分析与验证

4.1 安全性分析

本文采用基于椭圆曲线的国家商用密码管理办公室



(以下简称国密局)安全认证体制,其安全性是国际上公认的安全实用的密码体制。目前,椭圆曲线的离散对数问题的计算复杂度是完全指数级,攻击者想通过公钥破译私钥是不可行的,可以满足无线传感器网络的安全要求。本文提出的时间同步身份验证技术进一步增加了国密局身份认证的安全性,在离散对数的计算基础上加入了时间验证因素,使攻击者更加难以突破安全防线。

4.2 计算开销

本文采用区域划分传感器的方法,利用中心节点对数据融合的处理,大量消除了传感器的冗余数据,并用私钥绑定映射坐标表,配合 APIT 算法计算传感器的具体位置,提高了整个系统的抗风险能力和处理效率。经过计算机模拟江苏省电力传输网大量传感器接入服务器的数据,计算结果如图 6 所示,区域划分后的传感器系统对后台服务器的单周计算开销要远远小于未进行区域划分的传感器系统。

5 结束语

本文提出了一种基于区域划分的采用国密局加密算法及时间同步校验技术进行身份认证的无线传感器安全通信及防泄密私钥定位技术。将电力传输网中海量的传感器分区域划分,利用中心节点进行传感器数据的融合,消除冗余数据,有效提高了电网数据传输的效率,降低了冗余检测数据对带宽的占用程度。通过对国密局加密算法套件的运用,创新地将时间同步验证技术添加到身份认证签名算法中,有效地增加了系统通信的安全等级,防止外部黑客侵入网络获取电网重要信息。通过对私钥散列值与位

置信息的捆绑,消除了传统方式将设备编号与坐标绑定而带来的后续坐标映射表泄露的隐患,通过私钥更新防止了坐标映射表的泄露给电网数据信息带来的损失。通过对 APIT 算法的运用,计算出分布较散的传感器与其所属区域中心节点的相对位移,结合中心节点坐标计算出报警传感器的具体位置,有效降低了无线传感器定位的成本,大幅提高了电网数据的抗窃听能力。

参考文献:

- [1] 国家商用密码管理办公室.证书认证系统密码及其相关安全技术规范 [EB/OL].(2005-04-01)[2011-05-09].<http://www.docin.com/p-199938579.html>.
State Cryptography Administration Office of Security Commercial Code Administration. Specifications of cryptography and related security technology for certificate authentication system[EB/OL]. (2005-04-01) [2011-05-09].<http://www.docin.com/p-199938579.html>.
- [2] 王建国,王福豹,段渭军.加权最小二乘估计在无线传感器网络定位中的应用[J].计算机应用研究,2006(9):41-43.
WANG J G, WANG F B, DUAN W J. Application of weighted least square estimates on wireless sensor network node localization [J]. Application Research of Computers, 2006 (9): 41-43.
- [3] State Encryption Administration. SM2 elliptic curve public key cryptography algorithm recommends curve parameters [EB/OL]. [2010-12-22]. <http://www.oscca.gov.cn/UpFile/2010122214836668.pdf>.
- [4] LIANG W Q. Research on public key cryptography and its applications based on elliptic curve [J]. Journal of Anhui Radio & TV University, 2011(1):122-125.

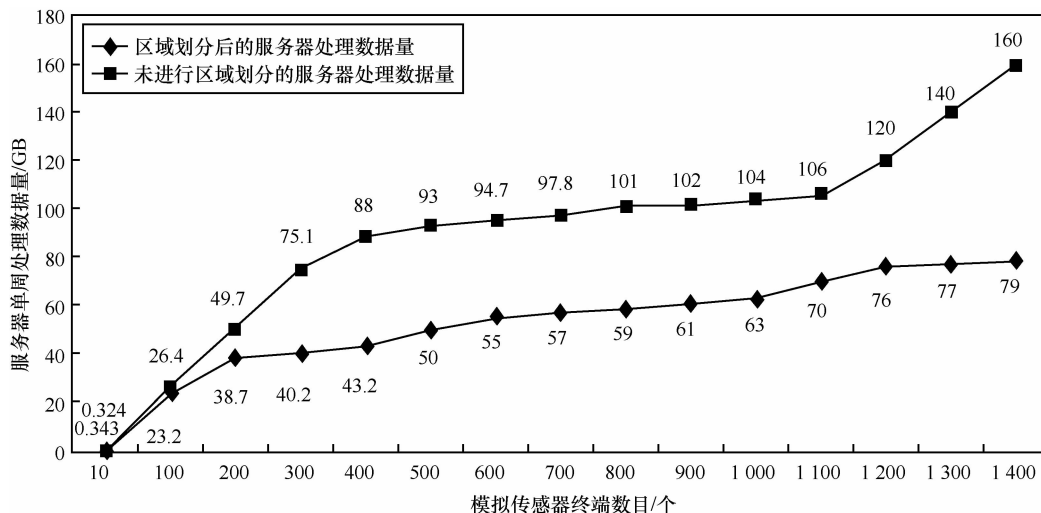
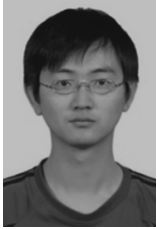


图6 服务器单日计算开销对比

- [5] HANKERSON D, MENEZES A, VANSTONE S. Guide to Elliptic Curve Cryptography[M]. New York: Springer-Verlag, 2004: 75-152.
- [6] WANG Q, REN K, YU S C, et al. Dependable and secure sensor data storage with dynamic integrity assurance[J]. ACM Transactions on Sensor Networks, 2011, 8(1): 1-24.

[作者简介]



徐敏(1984-),男,国网智能电网研究院工程师,主要研究方向为电力移动可穿戴设备及终端安全通信技术。



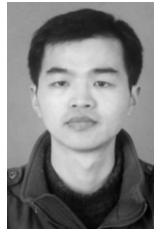
彭林(1978-),男,国网智能电网研究院主任、工程师,主要研究方向为电力移动互联网及电力云计算技术。



韩海韵(1980-),男,国网智能电网研究院主任工程师,主要研究方向为电力移动互联网及电力云计算技术。



李尼格(1985-),女,国网智能电网研究院工程师,主要研究方向为电力大数据分析及安全测评技术。



侯战胜(1983-),男,国网智能电网研究院工程师,主要研究方向为电力移动可穿戴设备及电力情景计算技术。