文章编号：2095-4980(2021)02-0330-04

基于身份认证的智能电网安全防护技术

张志强[1]，王海宝[*2]，周文涛[1]，张晓晨[1]，高　阳[2]，綦　锐[2]

(1.国网北京市电力公司 朝阳供电公司，北京 100124；2.北京智芯微电子科技有限公司，北京 100192)

摘　要：为保障传感器安全接入信息内网，保障数据在传输、存储和使用过程中的机密性、完整性和可用性，本文在考虑设备性能和数字签名情况下提出了基于多因素的身份认证方案。随后利用椭圆曲线密码系统，提出了一种基于身份的新密钥建立协议。通过安全性能分析，与已有经典方案相比，本文所提方案在面对重播、模仿、中间人攻击(MITM)和去同步化攻击时更加安全，且计算时间开销更小。

关键词：传感器；状态监测终端；认证方案；密钥建立协议；智能电网

中图分类号：TN915.07；TP393.04　　**文献标志码：**A　　**doi：**10.11805/TKYDA2019496

Safety protection technology of smart grid based on identity

ZHANG Zhiqiang[1]，WANG Haibao[*2]，ZHOU Wentao[1]，ZHANG Xiaochen[1]，GAO Yang[2]，QI Rui[2]

(1. Beijing Chaoyang Electric Power Company of State Grid，Beijing 100124，China；
2. Beijing Smart Chip Microelectronics Technology Co., Ltd.，Beijing 100192，China)

Abstract：In order to ensure the security of sensor access to the information intranet and the confidentiality, integrity and availability of data in the process of transmission, storage and use, this paper proposes a multi parameter collaborative authentication scheme with joint consideration of the equipment performance and digital signature. Then a new identity based key establishment protocol is proposed by using elliptic curve cryptosystem. Through security performance analysis, compared with the existing classical schemes, the proposed scheme is more secure with less computing time consumption while facing the imitation attack, MITM(Man-In-The-Middle) attack and desynchronization attack.

Keywords：sensor；state monitoring terminal；authentication scheme；key establishment protocol；smart grid

智能电网是利用双向高速通信网络技术和基于计算机的自动化和分布式控制，满足 21 世纪用户需求的具有良好发展前景的平台，其为电力系统的可靠性、安全性、灵活性、效率和负载平衡/负载调整提供了实质性的改进[1−2]。智能电网采用了多种有线和无线技术实现通信网络，然而通信网络与电力系统的集成使其暴露出脆弱性，并对安全提出了挑战[3−4]。目前已有部分文献针对智能电网网络的安全性进行了相应研究。Tsai 和 Lo[5]提出了一种针对智能电网的匿名密钥分发方案，该方案利用基于身份的签名和基于身份的加密来进行相互认证，但它无法抵御短暂的秘密泄漏攻击。Jo 等[6]的协议旨在保护智能电网中的隐私。Saxena 等[7]提出了一种身份验证和授权方案，通过验证用户授权并在用户访问设备时一起执行用户身份验证来减轻智能电网中的外部和内部威胁。此外，目前还有学者开展了智能电网通信网络安全解决方案和基于 SM2 协议的相关工作。Yan 等[8]提出了一种基于哈希的智能电网消息认证码密钥协议解决方案，以确保通信安全。Chen 等[9]提出了一种基于计算 Diffie−Hellman 问题和双线性映射的智能电网密钥建立和匿名认证解决方案。然而，由于智能电网通信的轻量级和高效性要求，上述方案中使用的密码算法效率较低。此外，它们只能实现单向认证，无法避免虚假的智能控制中心攻击者对智能终端的恶意控制和操作。Yang 等人[10]使用基于不区分度的 Bellare−Rogaway 模型证明了 SM2 协议的安全性。然而，该方案在没有相互认证的情况下达成了密钥协议。在智能电网通信网络中，只有同

收稿日期：2019-11-27；**修回日期：**2019-12-26

基金项目：国网北京市电力公司科学技术资助项目(52020318003W)

作者简介：张志强(1976–)，男，本科，高级工程师，主要研究方向为智能电网。email:zhangzhiqiang12321@126.com

[*]**通信作者：**王海宝　email:wanghaibao12321@126.com

时实现双向身份认证和会话密钥生成，才能保证智能电网终端与智能电网控制中心之间的安全通信。

针对上述问题，本文首先提出了一种安全高效的基于多因素的身份认证方案，该方案基于数字签名和设备性能对传感器进行认证。随后利用椭圆曲线密码系统，针对模仿、中间人攻击(MITM)、去同步化攻击，进一步提出了适用于智能电网中传感器与状态监测终端的基于身份的密钥建立协议。

1　总体方案思路

用于配电站室设备/环境状态监测的无线传感器节点众多，分布范围广，不可控因素多，在感知层、网络层、应用层存在众多信息安全风险。传感器(包括环境状态监测传感器、抓拍摄像头和设备状态监测传感器)与状态监测终端之间的安全防护方案如图 1 所示。其中，传感器内嵌低功耗安全芯片，状态监测终端内嵌适用于终端的高性能终端安全芯片。状态监测终端与传感器之间通过相应算法进行数据加解密和身份认证。针对传感器和状态监测终端之间的安全防护方案主要有两个待解决的问题，一个是双向身份认证的设计，另一个是密钥管理技术。从安全的角度来看，需要解决的重要问题是认证机制，它必须是安全的，不受不同类型的攻击，并且易于实现，因此本文在第二节提出了多因素认证的认证方案，在第三节进一步提出了基于身份的密钥建立协议，在第四节进行性能分析。

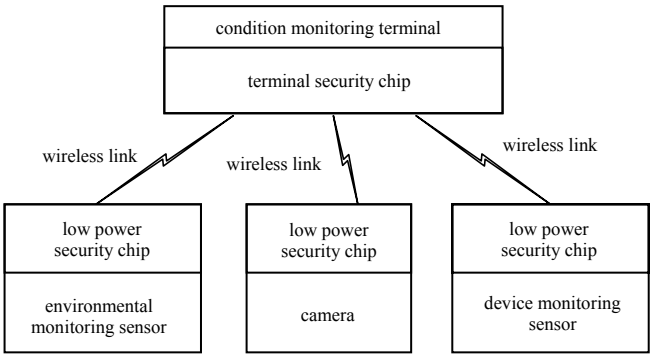

Fig.1 Safety protection scheme between sensors and status monitoring terminals
图 1 传感器和状态监测终端之间的安全防护方案

2　基于多因素的认证方案

在基于多因素的身份认证方案中，只有通过多因素身份验证成功的设备才算认证成功，否则身份验证过程失败，整个身份验证过程将重新启动。该方案在一个安全信道上，使用传感器与状态监测终端的公钥和私钥进行身份验证。传感器将对一个只被使用一次的任意或非重复的随机数值执行功能操作，该随机数值将作为身份验证的第二个因素。从功能操作的响应中，传感器将验证其是否是它所声明的设备。在安全通道上，当传感器向状态监测终端发送连接请求时，状态监测终端向传感器发送带私钥签名的一个只被使用一次的任意或非重复的随机数值 N 和一个时间戳。该传感器首先产生签名，然后通过函数运算传递随机数。该传感器发送使用其私钥签名的函数运算响应之前的随机数和时间戳。函数运算可以是一个密码谜题，也可以是设备执行某些功能的能力。状态监测终端检查响应并验证传感器的签名。一旦函数运算响应和签名被验证，传感器将被验证。

本节所提方案不仅通过签名验证传感器，而且通过签名验证状态监测终端。此外，该方案包含时间戳，以防止重播攻击。传感器和状态监测终端将有一个 5 s 的窗口来响应它们收到的请求，且设置了会话超时，若超时，所有步骤将再次重复。

3　基于身份的密钥建立协议

本文利用椭圆曲线密码系统提出一种基于身份的密钥建立协议，它由 3 个步骤组成：参数生成、初始化和密钥协议。

1) 参数生成

给定一个值 k 作为系统参数，信任机构(Trusted Authority，TA)首先会选择一个 k 比特的素数 q，并构造 $\{F_q,E/F_q,G_q,P\}$，其中，F_q 表示 q 个元素的有限域，E/F_q 是包含 F_q 的子集，G_q 是一个在 E/F_q 的点集，P 是椭圆曲线上一点。随后选择主密钥 $x\in Z_q^*$，并计算系统公钥 $P_{\text{pub}}=xP\in E/F_q$。最后选择哈希函数 $H_1:\{0,1\}^*\times G_q\to G_q$ 和 $H_2:\{0,1\}^*\times G_q\to Z_q^*$，并发布 $\{F_q,E/F_q,G_q,P,P_{\text{pub}},H_1,H_2\}$ 作为系统参数，且保密主密钥 x。

2) 初始化

初始化时，TA 将系统参数和主密钥 x 作为输入，并发送传感器和状态监测终端其私有密钥的份额。首先，TA 使用标识符 ID_s 为每个传感器执行以下过程。传感器选择随机数 $r_s\in Z_q^*$，计算 $R_s=r_sP$，并通过一个安全

信道将其与 ID_s 一起发送给 TA。TA 将计算 $y_s = H_1(ID_s, R_s).x$ 并发送回传感器。在该步骤，TA 会对带有标识符的状态监测终端 ID_m 进行以下操作：首先状态监测终端 m 选择一个随机数 $r_m \in Z_q^*$，计算 $R_m = r_m P$，并将 ID_m 一起发送给 TA。TA 将计算 $y_m = H_2(ID_m, y_s).x$ 并发送回状态监测终端。终端 m 计算 $S_m = r_m + y_m$，并考虑 S_m 和 r_m 分别作为私钥和公钥。

3) 密钥协议建立

建立密钥协议时，在传感器和状态监测终端之间，通过三条消息建立一个经过身份验证的会话密钥。首先，状态监测终端会选择一个随机数 $a \in Z_q^*$，并计算 $T_M = aP$。然后将元组 (T_M, ID_M, R_M) 发送给传感器。当传感器收到来自状态监测终端的启动信息之后，会选择一个随机数 $b \in Z_q^*$，并计算以下数值：$T_x = b + r_s$，$T_s = T_x P$，$k_{s \to M} = T_x(R_M + H_2(ID_M, y_s)P_{\text{pub}} + T_M)$ 和 $M_1 = H_1(0, k_{s \to M})$。并发送 T_s, ID_s 和 M_1 给状态监测终端。随后，状态监测终端将计算 $k_{M \to s} = (S_M + a)T_s$ 和 $M_1' = H_1(0, k_{M \to s})$。然后，其将会检查是否满足等式 $M_1' = M_1$。若相等，那么状态监测终端将会认为传感器验证通过，并设 K 为会话密钥，其中 $K = H_1(ID_M \| ID_s, k_{M \to s})$。此外 $H_2(\cdot)$ 也可用来进行密钥设定。最后，状态监测终端会计算 $M_2 = H_1(1, k_{M \to s})$ 并发送给传感器。待接收到 M_2 后，传感器将计算 $M_2' = H_1(1, k_{s \to M})$，并验证是否满足 $M_2' = M_2$。若满足，则验证通过并设定 $K = H_1(ID_M \| ID_s, k_{s \to M})$ 为会话密钥。

4 安全性和性能分析

在本节中，首先分析了多因素认证的认证方案的性能，随后分析了本文所提出的基于身份的密钥建立协议的安全性，并与其他协议的性能进行了比较。在分析中，本文假定主动攻击者能够窃听、修改和注入消息。

针对基于身份的密钥建立协议，就安全而言，本文从重播、模仿、中间人攻击(MITM)和去同步化攻击四方面进行分析，并就安全性能与文献[11−12]所提方案分别进行对比，对比结果如表 1 所示。

在重播攻击中，攻击者窃听交换的消息。然后，他可以根据自己的判断重新发送。在本文所提出的协议中，双方都在挑战对方。状态监测终端生成一个新的只被使用一次的任意或非重复的随机数值 a，并期望在第二个消息中返回一些内容，这些内容与基于该消息生成的机密密钥的期望相匹配。因此，任何试图说服任一方接受基于旧的随机数值构建的旧消息的尝试都是失败的。

针对模仿攻击，如果攻击者能够作为经过身份验证的一方与另一方通信，那么他就能够进行模仿攻击。在本文所提的协议中，传感器和状态监测终端通过不对称的预先共享的密钥来相互认证，由于他们各自没有对方的正确密钥，因此无法冒充，从而避免了模仿攻击。

在 MITM 攻击中，攻击者秘密地成为通信的中继并可能改变双方之间正确的通信，使双方相信他们在直接交谈，而实际上他们是通过攻击者交谈的。通过判断是否满足 $M_1' = M_1$ 和 $M_2' = M_2$，进行相互消息身份验证可以阻止 MITM 攻击。

在去同步化攻击中，攻击者可以阻止传感器和状态监测终端之间传输的消息，使它们永久地失去同步密钥，而导致传感器和状态监测终端之间将不再能够相互沟通。在所提的协议中，会话密钥是基于主秘密和新生成的随机数构造的，新生成的密钥和以前的会话密钥之间没有建立任何连接，因此无法被攻击者去同步化。

表 1 各方案面对不同攻击的弹性

Table1 Resilience of schemes to attacks

attack type	program		
	literature[11]	literature[12]	this article
replay attack	✓	✓	✓
imitation attack	×	✓	✓
MITM attack	✓	×	✓
desynchronization attack	✓	×	✓

此外，本文在实验中选取不同的密钥和明文，计算上述三种算法的运行时间，即从调用到运行整个过程所花费的时长，如图 2 所示。可以看出，文献[11]与文献[12]所提算法的时间开销皆随明文长度的增加而增长，而本文所提算法在不同明文长度下时间开销最小，并且稳定在 0.16 s 和 0.28 s 之间。

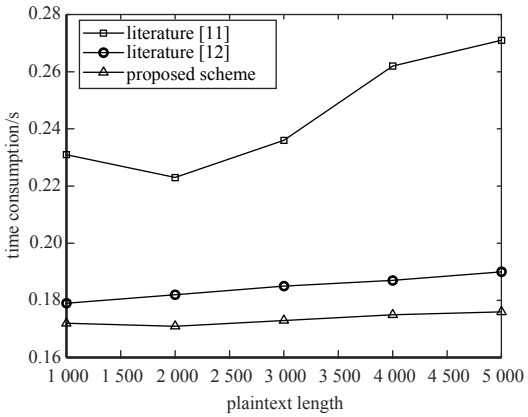

Fig.2 Time cost of the various schemes

图 2 时间开销

5　结论

为实现传感器和状态监测终端间的身份鉴别及业务数据的加密，确保数据完整性和机密性，本文首先提出一种基于多因素的身份认证方案，具有较高的安全性和有效性。随后利用椭圆曲线密码系统，提出了一种安全、轻量级的基于身份的新密钥建立协议。分析显示，本文所提方案在面对不同攻击时弹性最大，可防御或避免的攻击种类最多，且计算时间开销最低。

参考文献：

[1] WANG W,LU Z. Cyber security in the smart grid: survey and challenges[J]. Computer Networks, 2013,57(5):1344-1371.

[2] KHAN R,MCLAUGHLIN K,LAVERTY D,et al. Design and implementation of security gateway for synchrophasor based real-time control and monitoring in smart grid[J]. IEEE Access, 2017,5:11626-11644.

[3] 白煜,滕建辅,张立毅,等. 基于零知识证明的多实体 RFID 认证协议[J]. 太赫兹科学与电子信息学报, 2017,15(1):104-109. (BAI Yu,TENG Jianfu,ZHANG Liyi,et al. Multiple entities RFID authentication protocol based on zero-knowledge proof[J]. Journal of Terahertz Science and Electronic Information Technology, 2017,15(1):104-109.)

[4] 苏耀鑫,高秀峰. 基于矩阵的无线传感器网络 SNEP 改进[J]. 太赫兹科学与电子信息学报, 2018,16(6):1072-1079. SU Yaoxin,GAO Xiufeng. Research on improvement of SNEP protocol based on matrix[J]. Journal of Terahertz Science and Electronic Information Technology, 2018,16(6):1072-1079.)

[5] TSAI J L,LO N W. Secure anonymous key distribution scheme for smart grid[J]. IEEE Transactions on Smart Grid, 2015, 7(2):906-914.

[6] JO H J,KIM I S,LEE D H. Efficient and privacy-preserving metering protocols for smart grid systems[J]. IEEE Transactions on Smart Grid, 2015,7(3):1732-1742.

[7] SAXENA N,CHOI B J,LU R. Authentication and authorization scheme for various user roles and devices in smart grid[J]. IEEE Transactions on Information Forensics and Security, 2015,11(5):907-921.

[8] YAN Lili,CHANG Yan,ZHANG Shibin. A lightweight authentication and key agreement scheme for smart grid[J]. International Journal of Distributed Sensor Networks, 2017,13(2):1-7.

[9] CHEN Y,MARTÍNEZ J F,CASTILLEJO P,et al. An anonymous authentication and key establish scheme for smart grid: FAuth[J]. Energies, 2017,10(9):1354-1-23.

[10] YANG A,NAM J,KIM M,et al. Provably-secure(Chinese government) SM2 and simplified SM2 key exchange protocols[J]. The Scientific World Journal, 2014:1-8.

[11] NICANFAR H,JOKAR P,LEUNG V C M. Smart grid authentication and key management for unicast and multicast communications[C]// 2011 IEEE PES Innovative Smart Grid Technologies. Perth,WA,Australia:IEEE, 2011:1-8.

[12] KAMTO J,QIAN L,FULLER J,et al. Light-weight key distribution and management for advanced metering infrastructure[C]// 2011 IEEE GLOBECOM Workshops(GC Wkshps). Houston,TX,USA:IEEE, 2011:1216-1220.