# 基于 IBE 策略的物联网终端设备间的身份认证方案*

李秋月[1],赵　艳[2],李世明[1,3],於家伟[1],高胜花[1]

(1.哈尔滨师范大学 计算机科学与信息工程学院,黑龙江 哈尔滨 150025;
2.洛阳师范学院 物理与电子信息学院,河南 洛阳 471022;
3.上海市信息安全综合管理技术研究重点实验室,上海 200240)

**摘　要**:随着物联网终端设备间直接通信的需求不断增大,为解决物联网终端设备间安全通信和隐私保护问题,终端设备间认证技术成为人们关注的一个热点,业界诸多学者已经对此展开相关研究并提出多种物联网终端设备间的认证机制。但是,上述机制在安全强度及抵抗攻击效果方面尚存在不足。为解决此问题,该文提出一种基于 IBE 策略的物联网终端设备身份认证方案,实现终端设备之间匿名双向认证,同时使用椭圆曲线加密算法保证认证过程中信息传输的安全性。通过安全性理论分析和性能分析表明,该方案可很好地抵抗重放攻击、中间人攻击和篡改攻击等已知攻击且具有较低的计算开销。

**关键词**:物联网安全;物联网终端设备认证;IBE 策略;双向认证

**中图分类号**:TP309.1　　**文献标识码**:A　　DOI:10.19358/j.issn.2096-5133.2020.03.002

**引用格式**:李秋月,李世明,於家伟,等.基于 IBE 策略的物联网终端设备间的身份认证方案[J].信息技术与网络安全,2020,39(3):6-9,22.

## IBE-based authentication scheme for Internet of Things terminal devices

Li Qiuyue[1],Zhao Yan[2], Li Shiming[1,3],Yu Jiawei[1],Gao Shenghua[1]

(1. College of Computer Science and Information Engineering,Harbin Normal University,Harbin 150025,China;
2. School of Physics and Electronic Information, Luoyang Normal University, Luoyang 471022, China;
3. Shanghai Key Laboratory of Information Security Management Technology Research,Shanghai 200240,China)

**Abstract**:Along with qrowing demand of direat communicootion between the Internet of Things terminal equipments,in order to solve the Internet of Things secure communication between terminal equipment and privacy problem,authentication techniques between terminal equipments become a hot spot of people,many scholars have a related industry research and put forward a variety of IoT authentication mechanism between the terminal equipment. However,the above mechanism is still insufficient in terms of security intensity and anti-attack effect. In order to solve this problem,this paper proposes an authentication scheme of Internet of Things terminal devices based on IBE strategy,which realizes anonymous two-way authentication between terminal devices,and uses elliptic curve encryption algorithm to ensure the security of information transmission during authentication. The analysis of security theory and performance shows that the scheme can resist replay attack,man-in-the-middle attack,tamper attack and other known attacks.

**Key words**: Internet of Things security;IoT trust ID;identity-based encryption strategy;two-way authentication

## 0　引言

互联网的开放性有利于物联网设备的接入,却也给物联网设备带来了不可预知的风险,攻击者可能通过身份假冒等手段达到攻击或破坏的目的,从而威胁或破坏物联网系统的安全[1]。为此,国内外学者提出了许多物联网设备的接入认证方案[2-5],但随着物联网终端设备直接通信的需求日益增长,终端设备间的认证技术引起了人们的关注并对此做出了相关研究,如:CHEN D 等人提出一种基于声学指纹的轻量级无线设备认证协议[6];SOWJANYA K 等人为克服 LI X 等人的方案[7]存在的漏洞提出了一种基于 ECC 端到端认证协议[8];SHIVRAJ VL 等人提出了基于 Lamport OTP 的物联网端到端身份

*基金项目:上海市信息安全管理技术研究重点实验室开放课题(AGK2015003)

验证协议[9];WILSON P 提出了一种基于非对称密码的 IoT 设备间相互认证协议,并提供了共享的秘密会话密钥[10]。但是上述方案仍存在不足,如:文献[6]存在采用硬件指纹技术成本较高、操作不方便的问题;文献[7]不支持完全正向保密、易出现时钟同步问题;文献[9]安全级别较高,OTP 生成策略的难度等同于解决 Diffie-Hellman 计算问题,但是交互次数较多,需要大量的通信开销。

为此,本文针对物联网应用环境特点及物联网终端设备认证的安全需求,提出一种基于身份加密(Identity-Based Encryption,IBE)策略的物联网设备间的身份认证方案,以达到更高的安全强度和更好的抵抗攻击的效果。

## 1 基于 IBE 策略的终端设备间的认证方案

本文所提出的认证方案是基于物联网环境下的物联网终端设备之间进行身份合法性识别的一种认证机制。本方案是基于以下安全需求而研究的:

(1)在不泄露通信双方终端设备身份标识信息的情况下完成双向认证。

(2)本认证方案的安全性不会因终端设备的恶意丢失而下降。

(3)传输的数据在机密性、完整性等方面具有较高的安全性,即使遭到窃听也不会被破译、篡改。

(4)各终端设备具有同步时钟的功能,保证终端设备本地时钟偏差较小,甚至可忽略不计。

(5)可信中心与各终端设备之间有安全的传输信道。

### 1.1 认证方案策略

鉴于 ECC 在相同安全强度下密钥尺寸更小、运行速度更快、抗攻击性强的特点[11],本方案采用的 ECC 加密算法基于 IBE 策略,由可信中心生成系统参数,并结合物联网终端设备的身份信息生成该终端设备的密钥对,帮助终端设备完成注册,不参与终端设备间的认证过程。当终端设备双方需要通信时,终端设备利用公开的系统参数和私有信息经过三轮信息交互,在匿名的情况下完成终端设备身份的双向认证。

### 1.2 定义及符号说明

**定义 1** 物联网应用系统中具有接入与数据处理功能的设备称为物联网终端设备[12],记作 $D_i$;所有终端设备的集合称为终端设备集,记作 $D$,$D=\{D_1,D_2,\cdots,D_i,\cdots,D_n\}$,$i,n\in Z^+$。

**定义 2** 能够唯一代表或识别终端设备 $D_i$ 的信息称为身份标识,记作 $ID_i$,$D$ 的所有身份标识记作 $ID=\{ID_1,ID_2,\cdots ID_i\cdots ID_n\}$,$i,n\in Z^+$。

**定义 3** 对于任意 $D_j$ 通过某种计算过程后使得 $D_i$ 信任 $D_j$,记作 $D_i\succ D_j$,其中 $\succ$ 称为信任关系;若同时存在 $D_j\succ D_i$,则称为双向信任,记作 $D_i\succ\prec D_j$。

**定义 4** 对于任意的 $D_i$ 与 $D_j$,在构建 $D_i\succ D_j$ 或 $D_j\succ D_i$ 的过程称为设备认证,记作 Ж。

**定义 5** 在执行 Ж 前受 $D_i$ 信赖的可靠第三方称为可信中心,记作 TC。

本文研究中所涉及的符号说明如表 1 所示。

表 1 符号含义说明

| 符号 | 含义 | 符号 | 含义 |
|---|---|---|---|
| $p$ | 一个大于 3 的大素数 | $PK_i$ | $D_i$ 的公钥 |
| $E_p$ | 有限域上的椭圆曲线 | $SK_i$ | $D_i$ 的私钥 |
| $G$ | 阶为 $n$ 的加法循环群 | $\Delta t$ | 有效时间值 |
| $P$ | 是 $G$ 的一个生成元 | $h_i$ | 哈希函数 |
| $D_i$ | 终端设备 $i$ | $\oplus$ | 异或操作 |
| TC | 可信中心 | $Enc_j$ | 密钥为 $j$ 的加密函数 |
| $ID_i$ | $D_i$ 的身份 ID | $Dec_j$ | 密钥为 $j$ 的解密函数 |
| $T_i$ | TC 的时间戳 | $V_i$ | 终端设备 $i$ 的认证信息 |
| $T_{ij}$ | $D_i$ 生成的时间戳,用于 $D_j$ 重放攻击检测 | $DT_{xor}$ | 异或运算所需时间 |
| $t_i$ | $D_i$ 收到消息时的时间 | $DT_{hash}$ | 哈希运算所需时间 |
| $SK_{TC}$ | TC 的私钥 | $DT_{mul}$ | 点乘运算所需时间 |
| $PK_{TC}$ | TC 的公钥 | $DT_{pair}$ | 映射运算所需时间 |

### 1.3 初始阶段

(1)系统初始化:可信中心 TC 在椭圆曲线 $E_p$ 上生成一个阶为 $n$ 的加法循环群 $G$,$P$ 是 $G$ 的一个生成元,随机选取 $SK_{TC}\in Z_p^*$ 作为系统私钥,生成系统公钥 $PK_{TC}=SK_{TC}P$,保存系统私钥 $SK_{TC}$,公开参数 $\{G,P,PK_{TC},h_1,h_2\}$。TC 选择 2 个单向哈希函数:$h_1:\{0,1\}^*\times G^2\rightarrow Z_p^*$,$h_2:\{0,1\}^*\rightarrow Z_p^*$。其中 $h_1$ 的构造方法为先将椭圆曲线上的 2 个点做点加运算,再做点乘运算,接着将运算结果的两个坐标值相加后做模 $p$ 运算,用于计算能力较强的 TC。$h_2$ 的构造方法是做模 $p$ 运算,用于计算能力较弱的终端设备 $D_i$。

(2)设备注册:$D_i$ 将固化在网卡信息中的 MAC 地址作为自己的身份标识 $ID_i$ 发送给 TC,TC 收到消息后,生成时间戳 $T_i$,计算 $SK_i = SK_{TC} + h_1(ID_i \oplus T_i) \bmod(p)$、$PK_i = SK_i P$,然后公开公钥 $PK_i$,发送 $\{SK_i, T_i\}$ 到 $D_i$。$D_i$ 接收到 $\{SK_i, T_i\}$ 后计算 $SK_i P = PK_{TC} + h_1(ID_i \oplus T_i)$ 是否成立,若成立,则保存私钥 $SK_i$。否则,终端设备注册失败。

### 1.4 认证阶段

在终端设备认证阶段,终端设备 $D_i$ 的密钥对为 $(SK_i, PK_i)$,终端设备 $D_j$ 的密钥对为 $(SK_j, PK_j)$,认证过程如图 1 所示。

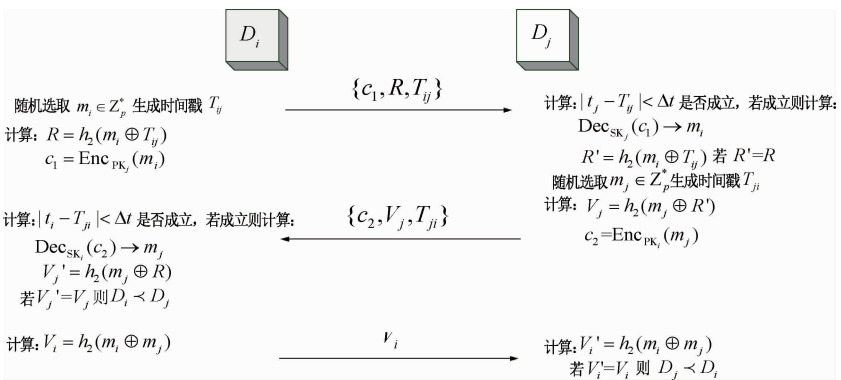


图 1 终端设备认证过程

过程描述如下:

(1)$D_i$ 随机选取 $m_i \in Z_p^*$,生成时间戳 $T_{ij}$ 计算:$R = h_2(m_i \oplus T_{ij})$、$c_1 = \mathrm{Enc}_{PK_j}(m_i)$,然后把 $\{c_1, R, T_{ij}\}$ 发送给 $D_j$。

(2)$D_j$ 计算 $|t_j - T_{ij}| < \Delta t$ 是否成立,若不成立,则拒绝此次认证请求。否则,计算 $\mathrm{Dec}_{SK_j}(c_1)$ 获得 $m_i$,再计算 $R' = h_2(m_i \oplus T_{ij})$,比较 $R'$ 与 $R$,若不相同则拒绝此次认证请求。否则,$D_j$ 随机选取 $m_j \in Z_p^*$,生成时间戳 $T_{ji}$,计算:$V_j = h_2(m_j \oplus R')$、$c_2 = \mathrm{Enc}_{PK_i}(m_j)$,然后把 $\{c_2, V_j, T_{ji}\}$ 发送给 $D_i$。

(3)$D_i$ 计算 $|t_i - T_{ji}| < \Delta t$ 是否成立,若不成立,则拒绝此次认证请求。否则,计算 $\mathrm{Dec}_{SK_i}(c_2)$ 获得 $m_j$,再计算 $V_j' = h_2(m_j \oplus R)$,比较 $V_j'$ 与 $V_j$,若不相同则拒绝此次认证请求。否则,$D_i \prec D_j$。$D_i$ 计算 $V_i = h_2(m_i \oplus m_j)$ 并把 $V_i$ 发送给 $D_j$。

(4)$D_j$ 接收到 $V_i$,计算 $V_i' = h_2(m_i \oplus m_j)$,比较 $V_i'$ 与 $V_i$,若不相同则拒绝此次认证请求。否则,$D_j \prec D_i$。

(5)当 $D_i \succ\prec D_j$ 时,本次认证成功,否则,本次认证失败。

## 2 安全性分析

### 2.1 抵抗重放攻击

攻击者通过重复利用监听到的历史消息来冒充合法用户进行重放攻击。本方案在生成的密钥中加入了时间戳 $T_i$ 作为密钥的新鲜因子,因此用此密钥加密生成的密文也具有新鲜性。在认证过程中也加入时间戳 $T_{ij}$,当攻击者拦截到具有时间戳 $T_{ij}$ 的密文,并利用所拦截到的消息进行重放攻击时,终端设备 $D_j$ 会验证时间戳 $T_i$ 是否满足不等式 $|t_j - T_{ij}| < \Delta t$,因为 $T_{ij}$ 是旧的时间戳,两条消息之间的时间差超出有效时间,不等式验证失败,从而本方案能够抵抗重放攻击。

### 2.2 防假冒攻击

在终端设备 $D_i$ 与 $D_j$ 之间进行身份认证的过程中,双方终端设备彼此发送的消息中 $m_i$、$m_j \in Z_p^*$ 是随机数以密文 $c_i$ 的形式发送,$T_{ij}$、$T_{ji}$ 是时间戳,$R = h_2(m_i \oplus T_{ij})$、$V_j = h_2(m_j \oplus R')$、$V_i = h_2(m_i \oplus m_j)$,没有发送彼此的身份信息 $ID_i$ 和 $ID_j$。攻击者若试图通过分析密文来获得 $D_i$ 与 $D_j$ 的密钥对 $(SK_i, PK_i)$ 和 $(SK_j, PK_j)$ 进而获取终端设备的身份信息,这是一个椭圆曲线上的离散对数问题,显然是十分困难的,故本认证方案可以有效对抗假冒攻击。

### 2.3 防中间人攻击

假设攻击者截获 $D_j$ 与 $D_i$ 的通信消息 $\{c_2, V_j, T_{ji}\}$,并认证消息 $V_j$ 进行篡改后发送给 $D_i$,$D_i$ 接收到消息后计算 $V_j' = h_2(m_j \oplus R)$ 与 $V_j$ 进行比较,若 $V_j' = V_j$ 则验证成功,但是由于 $V_j$ 是经过哈希函数 $h_2$ 运算得到的散列值,具有单向不可逆性,攻击者无法对其进行篡改进而实施中间人攻击。若攻击者截获 $D_i$ 发送给 $D_j$ 的认证消息 $V_i$,攻击者也无法

对其进行篡改后转发,不能实现中间人攻击。

### 2.4 防篡改攻击

由于本方案的加密算法是基于椭圆曲线上的离散对数问题,攻击者想通过将密文解密是十分困难的,并且本方案中的认证信息 $V_i$ 是经过哈希函数 $h_2$ 运算得到的散列值,具有单向不可逆性,攻击者无法对其进行篡改。故而本认证方案具有消息正确性和消息完整性的安全属性,能够防篡改攻击。

### 2.5 抵抗恶意 TC 攻击

假设 TC 没有被攻击,无隐私信息泄露,由上述分析可知本方案是安全的。若 TC 已被攻击者攻击,攻击者将会利用获取的设备 $D_i$ 的密钥对发动已知会话密钥攻击。由于本方案的 $\mathcal{K}$ 过程中,每次会话都有随机数 $m_i \in Z_p^*$ 或时间戳 $T_{ij}$ 的参与,因此攻击者无法通过身份验证,故本方案能抵抗恶意 TC 攻击。

## 3 性能分析

本方案提出 IBE 策略的目的是为了减少证书和其管理的开销,消除证书的影响。一般在 32 位 3 GHz 奔腾处理器上各种运算所需时间如表 2 所示[13]。本方案计算开销与其他使用 ECC 加密算法的认证方案计算开销的比较如表 3 所示。本方案未进行复杂的映射运算,增加了运算时间小于点乘运算的异或运算,分析表 2、表 3 可知,本方案计算开销较小。

表 2 各种运算所需时间 (ms)

| 运算方法 | 所需时间 |
|---|---|
| $DT_{mul}$ | 0.6 |
| $DT_{hash}$ | 0.6 |
| $DT_{pair}$ | 4.5 |

表 3 计算开销比较

| 方案 | 计算开销 |
|---|---|
| 文献[8] | $9DT_{mul}+4DT_{hash}$ |
| 文献[13] | $4DT_{mul}+4DT_{hash}+4DT_{pair}$ |
| 本方案 | $6DT_{mul}+6DT_{hash}+6DT_{xor}$ |

## 4 结论

为解决物联网终端设备间安全通信和隐私保护问题,本文提出于一种基于 IBE 策略的物联网终端设备间的身份认证方案。该方案中可信中心生成系统信息并完成设备注册,但是不参与终端设备间认证过程,终端设备间进行三轮交互,完成匿名双向认证过程;此外,通过安全性分析和性能分析,本方案可以防重放、假冒、中间人和篡改等攻击,具有认证性、匿名性、机密性、消息正确性和完整性等安全属性和较小的计算开销。

## 参考文献


[1] 张玉清,周威,彭安妮. 物联网安全综述[J]. 计算机研究与发展,2017,54(10):2130-2143.

[2] KUMAR P,GURTOV A,IINATTI J,et al. Lightweight and secure session-key establishment scheme in smart home environments [J]. IEEE Sensors Journal, 2016, 16 (1): 254-264.

[3] LI N,LIU D,NEPAL S. Lightweight mutual authentication for IoT and its applications [J]. IEEE Transactions on Sustainable Computing,2017,2(4):359-370.

[4] TEWARI A,GUPTA B B. A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices [J]. Advanced Intelligence Paradigms,2017,9(2/3):111-121.

[5] KIM K W,HAN Y H,MIN S G. An authentication and key management mechanism for resource constrained devices in IEEE 802. 11-based IoT access networks [J]. Sensors, 2017,17(10):2170-2083.

[6] CHEN D,ZHANG N,QIN Z,et al. S2M:a lightweight acoustic fingerprints-based wireless device authentication protocol [J]. IEEE Internet of Things Journal, 2017, 4 (1):88-100.

[7] LI X,PENG J,KUMARI S,et al. An enhanced 1-round authentication protocol for wireless body area networks with user anonymity [J]. Computers & Electrical Engineering, 2017,61:238-249.

[8] SOWJANYA K,DASGUPTA M,RAY S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems[J]. International Journal of Information Security,2019,19:129-146.

[9] SHIVRAJ VL, RAJAN MA, MEENA S, et al. One time password authentication scheme based on elliptic curves for internet of things (IoT) [C]. Proceedings of 2015 5th National Symposium on Information Technology:Towards New Smart World (NSITNSW), Riyadh, Saudi Arabia, 2015: 1-6.

[10] WILSON P. Inter-device authentication protocol for the internet of things[D]. MSc Thesis,Department of Electrical and Computer Engineering, University of Victoria, BC, Canada,2017.


(下转第 22 页)

的监测结果进行宏观分析和展示,根据内置的数据模型能够对系列安全事件进行智能化分析,包括事件聚类分析、样本聚类分析、时间序列历程分析、时间序列相关分析等。展示内容包括攻击来源、攻击目标、攻击类型、攻击时间等详细的事件记录信息。

### 3.3.5 管理配置模块

管理配置模块能够对数据探针的工业协议库、协议解析参数、攻击信息库、行为模型库、用户权限和行为范围等进行管理和配置。该模块能够自动监控所在网络的接入设备,根据设备的通信特征识别各种类型的控制器、服务器,自动生成网络拓扑。

## 4 结论

本文通过对电力行业的工控网络架构、安全风险、防护现状等网络安全问题进行研究分析,按照电力系统的安全防护总体原则及相关标准规范,针对电力生产分区的特点及网络要求,提出了以数据探针为组成单元的能够覆盖电厂工控网络各个层级并配置监测中心服务器的安全防护架构,能够解析多种工控协议,对已知和未知危险流量进行识别和学习,并将宏观网络态势以可视化的方式展示出来。安全防护架构具有多层次、立体化、智能化的显著特点,能够深度有效的保护电厂生产网络系统。

## 参考文献

[1] 陈连栋. 电力行业网络安全态势感知研究[D]. 北京:华北电力大学,2015.

[2] 魏钦志. 工业控制系统安全现状及安全策略分析[J]. 信息安全与技术,2013(2):25-28.

[3] 吴莹辉. 网络安全态势感知框架中态势评估与态势预测模型研究[D]. 北京:华北电力大学,2015.

[4] 朱明露. 功能安全标准在电厂安全系统中的应用研究[J]. 中国仪器仪表,2015(9):29-31.

[5] 谭小彬,张勇,钟力. 基于多层次多角度分析的网络安全态势感知[C]. 全国计算机安全学术交流会论文集(第二十三卷)[A],2008.

[6] 崔艳娜,张红金,李继安. 工业控制系统漏洞的统计及其分析研究[J]. 电子产品可靠性与环境试验,2018(6):41-46.

[7] 龚正虎,卓莹. 网络态势感知研究[J]. 软件学报,2010年07期

[8] 王娟. 大规模网络安全态势感知关键技术研究[D]. 成都:电子科技大学,2010.

[9] 胡威. 网络安全态势感知若干关键性问题研究[D]. 上海:上海交通大学,2007.

[10] 陶耀东,贾新桐. 工业控制系统网络安全态势感知框架研究[J]. 信息技术与网络安全,2018(5):3-6.

[11] 白雪原. 工控系统安全威胁及防护应用探讨[J]. 中国信息化,2018(5):70-71.

(收稿日期:2019-11-01)

**作者简介:**

张大松(1985 - ),男,博士,高级工程师,主要研究方向:信息安全、工控安全、机器学习、智能控制。

(上接第 9 页)

[11] 顾兆军,刘东楠. 一种面向廊桥 AP 的 ECC 身份认证方案[J]. 小型微型计算机系统,2019,40(1):98-103.

[12] KA A K. RMAC-A lightweight authentication protocol for highly constrained IoT devices [J]. International Journal on Cryptography and Information Security (IJCIS),2018,8(3):1-14.

[13] 张刚,石润华,仲红. 车载自组织网络中基于身份的匿名认证方案[J]. 计算机工程与应用,2016,52(17):101-106,122.

(收稿日期:2020-01-12)

**作者简介:**

李秋月(1992 - ),女,硕士研究生,主要研究方向:网络与信息安全。

赵艳(1980 - ),女,博士,主要研究方向:信息安全。

李世明(1976 - ),男,硕士,副教授,主要研究方向:网络与信息安全、物联网技术、数据挖掘。

# 版权声明