一种支持工业物联网故障检测的混合互认证方案*

沈宫新,宋楚平
(南京科技职业学院 信息工程学院,江苏 南京 210048)

摘　要:在工业物联网(IIoT)中,工业机器人和员工在制造过程中扮演着非常重要的角色。一个安全、高效的工业机器人和员工认证方案一直是研究热点,并面临诸多挑战。例如,工业机器人和员工在身份验证阶段容易受到模拟和去同步攻击。同时,控制中心很难找到不受控制的工业机器人。针对上述情况,提出了一种支持工业物联网故障检测的混合互认证方案。分别为员工和工业机器人(IR)设计了基于椭圆曲线加密(ECC)的认证和基于物理不可克隆函数(PUF)的认证。使用了基于阈值的故障检测,添加了禁用表以防止无授权员工访问监控和数据采集中心(SCDAC)。最后,分析论证了该方案的可行性和高效性。

关键词:工业物联网;ECC 认证;PUF 认证;阈值检测
中图分类号:TP393　　**文献标识码**:A　　DOI: 10.19358/j.issn.2096-5133.2020.01.005
引用格式:沈宫新,宋楚平. 一种支持工业物联网故障检测的混合互认证方案[J]. 信息技术与网络安全,2020,39(1):24-30.

A mixed mutual authentication scheme supporting fault-detection in industrial Internet of Things

Shen Gongxin, Song Chuping
(School of Information Engineering, Nanjing Polytechnic Institute, Nanjing 210048, China)

Abstract: In the industrial Internet of Things (IIoT), industrial robots and employees play a very important role in the manufacturing process. A safe and efficient industrial robot and employee certification program has always been a research hotspot and faces many challenges. For example, industrial robots and employees are vulnerable to simulation and desynchronization attacks during the authentication phase. At the same time, it is difficult for the control center to find uncontrolled industrial robots. Aiming at the above situation, a hybrid mutual authentication scheme supporting industrial IoT fault detection is proposed. Elliptic Curve Cryptography (ECC)-based authentication and physical unclonable function (PUF)-based authentication are designed for employees and industrial robots, respectively. Threshold-based fault detection is used, and a disable table is added to prevent unauthorized employees from accessing the Supervison Control and Data Acquisition Center (SCDAC). Finally, the analysis demonstrates the feasibility and efficiency of the program.

Key words: industrial Internet of Things; ECC certification; PUF certification; hreshold detection

0　引言

制造业的信息化,网络和物联网相关技术的快速发展在工业生产系统的各个领域得到越来越广泛的应用,极大地提高了生产率和经济效益。考虑到制造业的特征(例如:封闭性、高价值数据、分散化),利用病毒、网络协议的漏洞等,恶意攻击者可以窃听或破坏有价值的制造数据[1-3]。无休止的攻击可能导致灾难性的后果,如工业核心技术的泄漏或网络终端的非法操纵,这将造成巨大的生命和财产损失[4-6]。此外,威胁不仅来自外部黑客或恶意竞争对手,还来自潜在的内部攻击者,包括可能有权访问控制中心的前雇员。通过各种不同的攻击方式,正常的生产活动将遭受破坏,机密的数据被泄露,甚至制药和化学配方和工艺遭到恶意修改。

目前,对物联网认证的研究主要集中在以下三个方面。

(1)基于公共密码学系统的方案,主要依赖于

* 基金项目:南京科技职业学院科研项目(NHKY-2017-16)

RSA、椭圆曲线密码技术(Elliptic Curves Cryptography, ECC)[7-8]。2004 年以来,LAUTER K[9] 声称 ECC 可以应用于资源受限的设备中,研究将 ECC 应用于物联网认证。2015 年,VANGA 提出了一项支持多服务器和生物特征认证的框架[10],能够抵抗已知会话的临时信息攻击和设备丢失攻击,但是存在离线密码猜测攻击漏洞。AMIN R 在 2018 年提出了分布式云计算环境中 IoT 设备的轻量级身份验证协议方案[11],解决了上述安全漏洞,但没有保护模拟攻击和特权内部攻击。

(2)对称密码系统轻量认证方案,特别是基于哈希的[12-13]或基于 PUF 的[14-15]方案在最近的研究中得到了越来越广泛的应用。GODOR G 提出了一个 SLAP(最简单的轻量级身份验证协议)[16],通过理论分析可以抵御众所周知的攻击。然而,AKGUN M[17] 指出了对其协议的模拟攻击,并在不增加任何额外计算和内存成本的情况下解决了该问题。上述每个基于哈希的方案都有一个固有的缺陷,即容易受到物理攻击。因此,基于具有明显防止篡改特性的 PUF 的方案得到了越来越多的关注。BRINGER J[18] 首次提出了一种基于树的相互认证协议,该协议使用 PUF 提高了安全性。但是该协议容易遭受 DoS 攻击和模拟攻击[19]。最近,AKGUN M[20] 提出了一种可扩展的基于 PUF 的认证协议,该协议不能满足 RFID 系统中的高等级隐私和可扩展性要求,GOPE P[21] 断言该方案在执行穷举搜索以识别标签时是不切实际的。

(3)超轻量身份验证协议基本上是简单的逻辑操作,比如 AND、OR 和 XOR。目前对于工业物联网来说,还没有一个完善的标准安全协议。

本文针对工业物联网(IIoT)的应用情境,提出了一种支持工业物联网故障检测的混合互认证方案。分别为员工和工业机器人(IR)设计了基于椭圆曲线加密(ECC)的认证和基于物理不可克隆函数(PUF)的认证,IR 通过 SCDAC 进行身份验证,操作精细的加工和制造,并在成功进行身份验证后将机密技术数据传输到 SCDAC。同时,合法员工有权访问 SCDAC 以进行生产过程中的监控或管理。

1 问题定义

1.1 符号定义

本文的系统分析中,使用的符号和描述如表 1 所示。

表 1 本文中使用的符号表

定义	说明
G_1, G_2	G 的乘法子群
$\|\|$	连接操作
XOR	异或运算
P_s, m_s	SCDAC 的公钥和私钥
P_u, PW	员工的 verifer 值和密码
$h(*)$	单向散列函数$\{0,1\}^* \rightarrow \{0,1\}^K$.
PID_i, TID_i	伪标识符和临时 ID
C_i, R_i	呼叫,应答
K_i, N'	分别由 SCDAC 和 IR 生成的随机数
SK_1, SK_2	由员工计算的验证者值

1.2 定理描述

(1)椭圆曲线加密(ECC)

在有限域 F_p 中,存在非奇异椭圆曲线 $y^2 = x^3 + ax + b$,其中对于任何常数满足 $4a^3 + 27b^3$ 不等于 0,连同所有仿射坐标对 $(x, y) \in F_p$ 和一个叫做无穷远点的特殊点 O,椭圆曲线上的一组点形成一个以 O 为附加同一性的阿贝尔群[22-23]。

定义 1 椭圆曲线离散对数问题(ECDLP)的难度:在椭圆曲线上,$\{0, G, 2G, 3G\cdots\}$ 必须是任意点 G 的循环组。计算 $k \times G$ 很容易,其中 k 是一个称为标量乘法的整数。然而,从 $k \times G$ 的结果反向找到 k 是不可行的,这称为椭圆曲线离散对数问题(ECDLP)。

(2)双线性配对(Bilinear Pairing)

定义三个素数 p 阶乘法循环群 G_1, G_2 和 G_t。定义映射 $e: G_1 \times G_2 \rightarrow G_t$ 满足以下属性,则该映射称为双线性映射。

①双线性:对于所有 $W, Q, Z \in G_1$,有 $e(W, Q + Z) = e(W, Q)e(W, Z)$。对于任何 $x, y \in Z_{p*}$,得到 $e(xW, yQ) = e(W, Q)^{xy} = e(yW, xQ)$。

②可计算性:对于任意的 $W, Q \in G_1$,存在一种有效的算法计算 $e(W, Q)$。

③非退化性:对于所有 $P \in G_1$,$e(P, P) \neq 1_{G2}$,其中 1_{G2} 是 G_2 的生成元。

本文中使用的是 $G_1 = G_2$ 双线性配对。既即 $G_1 \times G_1 \rightarrow G_t$

(3)物理不可克隆功能(PUF)

工业机器人芯片由微处理器和 PUF 组成,PUF 为机器人的唯一标识,取决于内部物理特性,并且无论温度、电压、时间等,都将输出唯一的值。任何

检测或观察 PUF 操作的尝试都将改变基础电路特性。PUF 作为挑战响应微观结构,其定义为 $R = PUF_T(C)$,实际上不可能预测响应。

2 常规模型和分析

2.1 常规模型认证分析

IIoT 中的认证模型如图 1 所示,系统模型中有三个实体,包括工业机器人(IR)、监督控制和数据采集中心(SCDAC)、员工。在此模型下,IR 和员工将与 SCDAC 相互认证,成功验证后,IR 会定期将生产数据传输给 SCDAC,员工将上传工作数据并将指令发送给 IR,并应定期更改 IR 的密码。同时,为了避免恶意员工的攻击,SCDAC 将维护一个禁止列表以防恶意员工的访问。在 IR 和 SCDAC 之间的认证阶段,IR 应该考虑计算和存储设备是资源受限的设备,而在员工与 SCDAC 之间进行身份验证时,安全性应该比计算成本和内存开销更受关注。

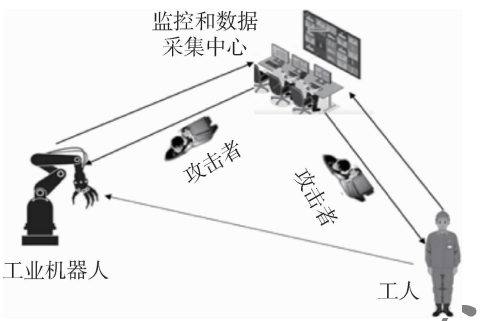

图 1 工业物联网认证模型

2.2 模型攻击分析

在认证模型下,假设 SCDAC 是完全可信的,IR 是可信的,在实际中容易被信道攻击。员工是半信任的,可能发送错误指令甚至尝试窃取机密数据或者破坏正常的生产活动。攻击者不仅可以在认证阶段窃听开放信道之间的秘密信息,还可以检索存储在 IR 存储器中的信息。同时攻击者可以阻止来自 SCDAC 的下达信息,也可以阻止来自 IR 的上传信息。

3 安全模型构建和分析

提出一种安全的混合互验证模型方案,该方案分为四个阶段,包括设置和注册、身份验证、通信、密码更改和用户驱逐。一般来说,身份验证协议分别基于 ECC 和 PUF,适用于员工和 IR。此外,协议具有错误检测和纠正机制,可以找到损坏的 IR 并驱逐权限已过期的员工。本文提出的混合相互认证方案如图 2 所示。

3.1 设置和注册

(1)SCDAC 在有限域 F_p 上选择非奇异椭圆曲线 E_p,其中具有阶数 n 的 G 是基点,使得 $nG = 0, n \in Z_{p*}$。SCDAC 选择 $m_s \in Z_{p*}$ 作为主密钥,$G, Z \in G_1$ 并计算 $P_s = m_s \times G$。之后,SCDAC 选择一个防冲突哈希函数 $h(*)$ 到 Z_{p*} 并释放参数 $\{E_p, F_p, G, Z, n, P_s, h(*)\}$。

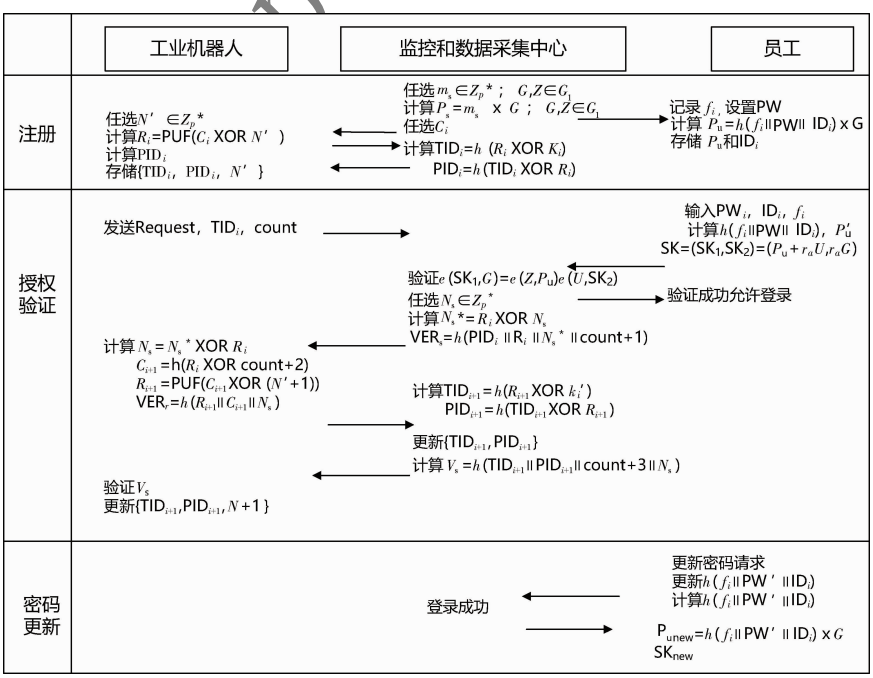

图 2 混合互验证模型

(2)员工将注册一个账户以访问 SCDAC 并向 IR 发送指令。员工 U_i 注册来自 SCDAC 的 ID_i 和员工的生物信息,如指纹信息 f_i 和计算机 $P_u = h(f_i || PW || ID_i) \times G$。然后 SCDAC 将 P_u 和相应的 ID_i 存储到数据库中,并标记为 1,表示它是一个活跃的账户;标记为 0,表示这是一个未激活的账户,如表 2 所示。

表 2 SCDAC 中的认证表

标识	密码和认证	状态位
ID_1	$P_{u1} = h(f_1 \| \| PW \| \| ID_1) \times G$	0/1
ID_2	$P_{u2} = h(f_2 \| \| PW \| \| ID_2) \times G$	0/1
ID_3	$P_{u3} = h(f_3 \| \| PW \| \| ID_3) \times G$	0/1

(3)每个 IR 都将注册到 SCDAC。首先,SCDAC 随机生成呼叫 C_i 到 IR_i。之后,IR_i 随机生成数并计算 $R_i = PUF(C_i XOR N)$。SCDAC 从 IR_i 接收 R_i 并计算临时标识符 $TID_i = h(R_i XOR K_i)$ 和伪标识 $PID_i = h(TID_i XOR R_i)$,其中 K_i 由 SCDAC 随机选择。同时,SCDAC 将 $\{TID_i, PID_i\}$ 存储到内存中,并将 TID_i 发送到 IR_i。最后,IR_i 计算 PID_i 并将 $\{TID_i, PID_i, N'\}$ 存储在存储器中。

3.2 认证和报告

(1)当 U_i 想要登录 SCDAC 时,U_i 会将 PW,ID_i 和 f_i 输入终端设备,如计算机或 Pad。终端将选择随机 $r_a \in Z_{p*}$,并进行计算 $P_{u'} = h(f_i || PW || ID_i) \times Z$,接下来,$U_i$ 随机选择 $r \in Z_{p*}$ 并计算 $SK = (SK_1, SK_2) = (h(f_i || PW || ID_i) \times Z + r \times U, r_a \times G)$。最后,终端设备将 SK 发送到 SCDAC。

(2)SCDAC 通过检查以下等式是否成立来验证用户身份的合法性。

$$e(SK_1, G) = e(Z, P_u) e(U, SK_2)$$

(3)如果 U_i 通过验证,员工可以访问 SCDAC 并检查生产过程。之后,IR_i 尝试在开始生产之前对服务器进行身份验证。IR_i 向 SCDAC 发送认证请求,TID_i 和计数。SCDAC 检查 TID_i 是否在数据库中。如果是,则 SCDAC 生成随机数 N_s,并计算 $N_s^* = R_i XOR N_s$,并将 C_i, N_s^* 连同 $VER_s = h(PID_i || R_i || N_s^* || count + 1)$ 发送到 IR_i。此后,IR_i 验证 VER_s 的正确性以检查 SCDAC 的身份。

(4)如果 SCDAC 被认证为合法,则 IR_i 会计算,$N_s = N_s^* XOR R_i, C_{i+1} = h(R_i XOR count + 2), R_{i+1} = PUF(C_{i+1} XOR (N' + 1))$ 和 $VER_r = h(R_{i+1} || C_{i+1} || N_s)$,并发送 $\{C_{i+1}, R_{i+1}, VER_r\}$ 到 SCDAC。随后,SCDAC 将检查 VER_r 以验证 IR_i 的身份,因为只有有效的 IR_i 才能获得正确的 N_s。随后,SCDAC 计算 $TID_{i+1} = h(TID_{i+1} XOR R_{i+1})$ 并更新 $\{TID_{i+1}, PID_{i+1}\}$。同时,SCDAC 计算 $V_s = h(TID_{i+1} || PID_{i+1} || count + 3 || N_s)$ 并将 $\{TID_{i+1}, PID_{i+1}, V_s\}$ 发送给 IR_i。最后,如果 V_s 被正确验证,IR_i 将更新内存中的 $\{TID_{i+1}, PID_{i+1}, N' + 1\}$

(5)如果所有机器人都通过了认证,那么工业机器人将生成实时生产数据以传输给 SCDAC。

3.3 密码更新

(1)当员工 U_i 想要将旧密码 PW 更改为新密码 PW′时。在登录 SCDAC 后,U_i 会将 $h(f_i || PW || ID_i)$ 更新为新的 $h(f_i || PW' || ID_i)$。U_i 利用旧密码 PW 登录 SCDAC 并发送密码更新请求。

(2)U_i 计算 $h(f_i || PW' || ID_i)$,$P_{unew} = h(f_i || PW' || ID_i) \times G$ 和 SK_{new} 由 PW′计算。

3.4 基于阈值的故障检测

在特定时间段 t_i 内,产品的缺陷率 d' 必须不高于 SCDAC 的指令 d。如果某段时间内,缺陷率不高于 d,则不会调用生产日志进行检查。相反,如果缺陷率异常高于指令 d,则存在工业机器人生产参数被对手或内部员工修改的可能。因此,SCDAC 在该时间段内调用生产日志并检测故障。

(1)SCDAC 将定义指令 d 并将其广播给所有员工。首先,SCDAC 选择随机值 $p_1 \in Z_{p*}$ 并计算 $W = p_1 \times G, f = H(d || W || t)$ 和 $s_1 = p_1 - f \times m_s$。此后,SCDAC 向所有员工广播元组 $\{d, s_1, f, t\}$。

(2)员工使用元组 $\{d, s_1, f, t\}$ 中的元素检查指令 d 的有效性。员工首先计算 $W' = f \times p_s + s_1 \times G$ 并检查方程 $f = H(d || W' || t)$ 的有效性。如果等式成立,员工将在一个特定时间段 t_i 内将缺陷率 d' 与指令 d 进行比较。如果 d' 明显高于 d,则员工将向 SCDAC 发送警告 $u = d' || t_i$,其中 d' 是期间 t_i 内的缺陷率,否则忽略它。

(3)在收到员工的警告信息后,SCDAC 将在时段 t_i 内调用生产日志并修复故障源,以确定行业机器人是否已被对手破坏。

3.5 用户禁用

(1)为了防止来自恶意员工的攻击,SCDAC 将维护一个禁用表,禁止他们访问 SCDAC。如果员工向工业机器人发送错误指令,SCDAC 将删除验证者

表中的账户,并将员工的账户移至禁用表。

(2)员工使用元组$\{d,s_1,f,t\}$中的元素检查指令d的有效性。员工首先计算$W'=f\times p_s+s_1\times G$并检查方程$f=H(d\ ||\ W'||\ t)$的有效性。如果等式成立,员工将在一个特定时间段$t_i$内将缺陷率$d'$与指令$d$进行比较。如果$d'$明显高于$d$,员工将向 SCDAC 发送警告报告$u=\{d'||t_i\}$,其中$d'$是期间$t_i$内的实际缺陷率。

4 安全模型攻击验证

4.1 抵抗模仿攻击

在方案中,攻击者将尝试模拟有效的员工或行业机器人登录 SCDAC。首先,对手试图伪造新的$\{h(f_i||\ \mathrm{PW}\ ||\ \mathrm{ID}_i)_{\mathrm{guess}}\times Z+r_a\times U,r_a\times G\}$来冒充员工登录 SCDAC 进行身份验证,由于哈希碰撞抵抗假设和椭圆曲线离散对数问题(ECDLP)的难度,伪造正确是不可能的。更具体地说,对手难以计算$P_u=h(f_i||\ \mathrm{PW}\ ||\ \mathrm{ID}_i)\times G$,因此对手无法模仿员工未通过身份验证。可以确保 SCDAC 和 IR 之间的认证以防止冒充攻击。

4.2 抵抗去同步攻击

资源受限的设备容易受到去同步攻击。因此,只考虑对工业机器人的反去同步攻击的安全性。在 IIoT 系统中,同步对于双方通信至关重要。在方案中,攻击者可以篡改阻止消息$\{\mathrm{TID}_i+1,\mathrm{PID}_i+1,V_s\}$以打破 SCDAC 到 IR 之间的同步。然而,SCDAC 已经得到C_i+1和R_i+1,因此 SCDAC 可以计算伪身份$\mathrm{PID}_i+1=h(\mathrm{TID}_i+1\mathrm{XOR}R_i+1)$。此后,SCDAC 和 IR 共享相同的更新伪标识PID_i+1,以便它们可以在下一次认证中成功认证。

4.3 抵抗窃听攻击

如果攻击者在身份验证阶段和数据报告阶段执行窃听攻击以获取机密信息。在提出的方案中,对手可以在员工和 SCDAC 之间获得 SK、P_u。但是,由于 ECDLP 不可行,对手无法通过身份验证,因此攻击者无法找出正确的密码 PW。SCDAC 和 IR 之间的身份验证,攻击者可能会窃取TID_i和PID_i但没有R_i,因此,攻击者无法冒充有效的 IR 来通过 SCDAC 进行身份验证。在数据报告阶段,提出的协议可以实现强大的匿名性并防止报告数据的泄漏。因此,该方案可以抵御窃听攻击。

4.4 抵抗回复攻击

如果攻击者可以在下一个会话中拦截并重新发送认证数据,则临时标识符 TID、伪身份 PID、计数器计数和随机数N'在每个会话中将是不同的。同时,呼叫C_i和响应R_i将更新为$C_i+1=h(R_i\ \mathrm{XOR}\ \mathrm{count}+2)$,$R_i+1=\mathrm{PUF}(C_i+1\ \mathrm{XOR}\ (N'+1))$。显然,攻击者无法使用上一个身份验证消息在下一个会话中执行回复攻击。

4.5 抵抗内部攻击

在安全模型中,假设内部恶意员工可能有权访问 SCDAC 并发送错误的推荐。首先,如果检测到异常缺陷率,SCDAC 将从工业机器人调用生产日志,并指出一名员工U_i已更改生产参数。SCDAC 将确定员工ID_i的身份并将其加入禁用表以防止U_i再次访问服务器。此外,通过设置员工的生命周期,从而防止以前的内部人员攻击。

从上述安全性分析可以看出,本文提出的方案可以承受第 1 节中提到的所有安全威胁和攻击。为了表明该方案在安全特征方面的优越性,将提出的认证方案与一些相关的和最先进的工作进行了比较[24-27],比较结果如表 2 所示。分析可知,虽然 A 的方案可以实现限制性匿名,但它和 C 方案一样不能识别损坏的标签。此外,除了本文的方案和文献[24]之外,其他方案不能抵御来自内部的攻击。因此,本文提出的方案在安全性方面优于其他相关方案。

表 3 安全性对比表

攻击类型	文献[24]	文献[25]	文献[26]	文献[27]	本文
模仿攻击	√	√	√	√	√
去同步攻击	√	√	√	×	√
窃听攻击	×	√	√	√	√
回复攻击	×	√	√	√	√
内部攻击	√	×	×	×	√
限制性名	√	×	×	√	√

5 安全模型性能分析

在本节中,将通过理论分析提出通信成本和计算开销。此后,通过实验模拟本文认证方案的运行时间。

5.1 通信成本比较

首先,临时伪TID_i的长度、安全散列 PUF 的输出长度、随机呼叫数C_i的长度以及随机值K_i分别是 32 位、128 位、120 位和 128 位。此外,该比较的

三个阶段,包括 IR 设置阶段、SCDAC 设置阶段和 IR 与 SCDAC 之间的认证阶段。在设置阶段,SCDAC 将挑战 C_i 和临时身份 TID_i 发送到 IR,而 IR 将 R_i 发送到 SCDAC。因此,在设置阶段,通信成本为 SCDAC 为 152 位,IR 为 128 位。至于认证阶段,总共有四种消息 $\{request, TID_i, count\}$,$\{C_i, N_s^*, VER_s\}$,$\{C_i+1, R_i+1, VER_r\}$,$\{TID_i+1, PID_i+1, V_s\}$,大小为 32 + 32 + 32 + 120 + 120 + 128 + 120 + 120 + 128 + 32 + 32 + 128 = 1 024 bit。

5.2 计算成本分析

比较认证阶段加密操作的计算花费时间。计算机硬件配置为 IntelCorei3-3120CPU 和 4 GB 内存,操作系统为 Ubuntu 16.04,不考虑运行时间极短的 XOR 操作和随机数生成操作。仿真实验由 C 语言和基于配对的密码学(PBC)库执行。定义符号如下:

T_{Hash}:表示单向哈希操作的时间

T_{PUF}:表示一次 PUF 操作的时间

T_{XOR}:表示 XOR 操作的时间

T_{RAN}:表示随机数生成的时间

$T_{Sys-e/d}$:表示对称加密和解密的时间

通过表 4,可以清楚地看到,本文提出的方案的计算开销比认证阶段的其他方案工作要少,即 SCDAC 的 $4T_{Hash} + 3T_{XOR} + T_{PUF}$,以及 IR 的 $3T_{Hash} + 3T_{XOR} + T_{PUF}$。同时,单向安全散列的运行时间为 0.000 48 s,近似等于一个 PUF 操作。综上所述,IR 和 SCDAC 的总运行时间约为 0.004 32 s,与表 4 的其他方案工作相比,其运行时间最少。

表 4 计算耗时对比表

对比方案	用户端	服务端
文献[7]	$4T_{Hash} + 3T_{PUF} + T_{RAN}$	$4T_{Hash} + 2T_{RAN}$
文献[18]	$3T_{Sys-e/d} + 12T_{Hash}$	$3T_{Sys-e/d} + 12T_{Hash}$
文献[25]	$4T_{Hash} + 2T_{PUF} + T_{RAN}$	$4T_{Hash} + 2T_{RAN}$
本文	$3T_{Hash} + 3T_{XOR} + T_{PUF}$	$4T_{Hash} + 3T_{XOR} + T_{PUF}$

6 结论

本文首先分析了工业物联网中不同的角色,对比了主要的身份验证方案及其优缺点,提出了一种混合认证方案来更好地解决工业物联网安全问题。根据不同的安全威胁,分别为员工和工业机器人设计了基于 ECC 的认证和基于 PUF 的认证。设计了一种基于阈值的故障检测方案,通过向员工广播缺陷率来检测机器人是否受到攻击。对于恶意员工,添加了禁止表以防止访问 SCDAC。此外,通过对模拟攻击、去同步攻击、窃听攻击和内部攻击等的安全性分析,确保提出的方案优于其他相关方案。最后,证明此方案在通信和计算开销方面是高效的。在未来的工作中,将尝试使用区块链在物联网设备之间设计更高效和安全的认证方案。

参考文献

[1] GRAMMATIKIS P I R, SARIGIANNIDIS P G, MOSCHOLIOS I D. Securing the internet of things: challenges, threats solutions[C]. Internet of Things, 2018.

[2] DEOGIRIKAR J, VIDHATE A. Security attacks in IoT: a survey[C]. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE, 2017: 32-37.

[3] ABDUL-GHANI H A, KONSTANTAS D. A comprehensive study of security privacy guidelines, threats, and countermeasures: an IoT perspective[J]. Sensor Actuator Networks, 2019,8(2):22.

[4] CHEN D, CHANG G, SUN D, et al. TRM-IoT: a trust management model based on fuzzy reputation for internet of things[J] Computer Science and Information Systems, 2011, 8(4):1207-1228.

[5] JABBAR W A, SHANG H K, HAMID S N I S, et al. IoT-bbms: Internet of Things-based baby monitoring system for smart cradle[J]. IEEE Access, 2019: 1-1.

[6] PATA S D, MILICI D L, POIENAR M, et al. Management system for the control of the forklifts activity in a factory[C]. 2019 8th International Conference on Modern Power Systems (MPS), May 2019:1-4.

[7] LOHACHAB A, KARAMBIR. ECC based inter-device authentication authorization scheme using MQTT for IoT networks[J]. Information Security Applications, 2019, 46: 1-12.

[8] LIAO Y P, HSIAO C M. A secure ECC-based rfid authentication scheme integrated with id-verifier transfer protocol[J]. Ad Hoc Networks, 2014,18:133-146.

[9] LAUTER K, The advantages of elliptic curve cryptography for wireless security[J]. IEEE Wireless communications, 2004,11(1): 62-67.

[10] ODELU V, DAS A K, GOSWAMI A. A secure biometrics-based multi-server authentication protocol using smart cards[J]. IEEE Transactions on Information Forensics Security ,2015,10(9):1-1.

[11] AMIN R, KUMAR N, BISWAS G, et al. A light weight authentication protocol for IoT-enabled devices in distributed cloud computing environment[J]. Future Generation Computer Systems, 2018,78:1005-1019.

[12] KAVUN E B, YALCIN T. A lightweight implementation of keccak hash function for radio-frequency identification applications[C]. International Workshop on Radio Frequency Identification: Security Privacy Issues. Springer, 2010:258-269.

[13] AHMADIAN Z, SALMASIZADEH M, AREF M R. Desynchronization attack on rapp ultralightweight authentication protocol[J]. Information Processing Letters, 2013, 113(7):205-209.

[14] CHATTERJEE U, CHAKRABORTY R S, MUKHOPADHYAY D. A PUF-based secure communication protocol for IoT[J]. ACM Transactions on Embedded Computing Systems (TECS), 2017,16(3):67.

[15] CHATTERJEE U, GOVINDAN V, SADHUKHAN R, et al. Building PUF-based authentication key exchange protocol for IoT without explicit crps in verifier database[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 16(3): 424-437.

[16] GODOR G, ANTAL M, IMRE S. Mutual authentication protocol for low computational capacity rfid systems[C]. in IEEE GLOBECOM 2008 IEEE Global Telecommunications Conference, IEEE, 2008:1-5.

[17] AKGUN M, CAGLAYAN M U. Server impersonation attacks revisions to slap, rfid lightweight mutual authentication protocol[C]. 2010 Fifth International Conference on Systems and Networks Communications. IEEE, 2010 : 148-153.

[18] BRINGER J, CHABANNE H, ICART T. Improved privacy of the treebased hash protocols using physically unclonable function[C]. International Conference on Security Cryptography for Networks. Springer, 2008:77-91.

[19] KARDAS S, ELIK S C, YILDIZ M, et al. Puf-enhanced offline rfid security and privacy[J]. Network and Computer Applications, 2012,35(6): 2059-2067.

[20] AKGUN M, CAGLAYAN M U. Server impersonation attacks revisions to slap, rfid lightweight mutual authentication protocol[C]. 2010 Fifth International Conference on Systems and Networks Communications. IEEE, 2010:148-153.

[21] GOPE P, LEE J, QUEK T Q. Lightweight practical anonymous authentication protocol for rfid systems using physically unclonable functions[J]. IEEE Transactions on Information Forensics Security, 2018,13(11): 2831-2843.

[22] HANKERSON D, MENEZES A, VANSTONE S. Guide to elliptic curve cryptography springer[Z]. ISBN: 0-387-95273-X; 332 pages web, 2003.

[23] STALLINGS W. Cryptography network security: principles practice [Z]. Pearson Upper Saddle River, 2017.

[24] SUI Z, NIEDERMEIER M, DE MEER H. TAI: a threshold-based anonymous identification scheme for demand-response in smart grids[J]. IEEE Transactions on Smart Grid, 2016,9(4): 3496-3506.

[25] FAN K, JIANG W, LI H, et al. Lightweight rfid protocol for medical privacy protection in IoT[J]. IEEE Transactions on Industrial Informatics, 2018,14(4): 1656-1665.

[26] AGHILI S F, ASHOURI-TALOUKI M, MALA H. Dos, impersonation and de-synchronization attacks against an ultralightweight rfid mutual authentication protocol for IoT[J]. Supercomputing, 2018,74(1): 509-525.

[27] LI X, NIU J, KUMARI S, et al. A robust biometrics based three-factor authentication scheme for global mobility networks in smart city[J]. Future Generation Computer Systems, 2018,83: 607-618.

(收稿日期:2019-11-02)

作者简介:

沈宫新(1975 -),通信作者,男,硕士,讲师,主要研究方向:软件工程、信息安全。E-mail:sgx0554@163.com。

宋楚平(1972 -),男,硕士,教授,主要研究方向:数据挖掘、网络安全。

版权声明