工业物联网中基于 PUFs 轻量级的密钥交换协议研究

夏艳东[1] 戚荣鑫[2] 季 赛[1,2]

[1](南京信息工程大学网络信息中心 江苏 南京 210044)

[2](南京信息工程大学计算机与软件学院 江苏 南京 210044)

摘 要 为了保障数据的安全性和隐私性,防止恶意用户访问传感器设备,针对工业物联网提出一种轻量级的认证与密钥交换协议。该协议采用物理不可克隆函数,模糊提取器保障传感器设备的安全。同时采用单向散列函数、异或操作和对称加解密等技术建立安全的会话通道。实验结果表明,相比于其他认证方案,该协议有效减少了密钥交换的通信和计算开销,所提出的协议适用于资源受限的传感器设备且能够抵抗现有多种已知攻击。

关键词 工业物联网 物理不可克隆函数 模糊提取器 密钥交换

中图分类号 TP309.7 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2022.03.050

PUFS-BASED LIGHTWEIGHT KEY EXCHANGE PROTOCOL IN IIOT

Xia Yandong[1] Qi Rongxin[2] Ji Sai[1,2]

[1](*Network Information Center*, *Nanjing University of Information Science and Technology*, *Nanjing 210044*, *Jiangsu*, *China*)

[2](*School of Computer and Software*, *Nanjing University of Information Science and Technology*, *Nanjing 210044*, *Jiangsu*, *China*)

Abstract To protect the security and privacy of data and prevent malicious users from accessing sensor devices, this paper proposes a lightweight authentication and key exchange protocol. The protocol adopted physical unclonable function and the fuzzy extractor to ensure the security of sensor equipment. Meanwhile, one-way hash function, bit-wise XOR operation and symmetric encryption/decryption were used to establish a secure session channel. The experimental results show that compared with other authentication schemes, the proposed protocol effectively reduces the communication and computing overhead of key exchange. It is suitable for resource constrained sensor devices and can resist a variety of known attacks.

Keywords IIoT Physical unclonable function(PUF) Fuzzy extractor Key exchange

0 引 言

1999 年,美国麻省理工学院(MIT)提出了物联网的雏形。2005 年,国际电信联盟(ITU)发布了《ITU Internet reports 2005——the Internet of Things》,该报告正式在全世界范围内提出了“物联网”的概念[1]。工业物联网就是将射频识别技术、传感网和智能分析等技术应用到工业领域中来,以更高效便捷的方式监控工业生产流程,实时收集生产数据,从而优化生产管理,降低生产成本,提高生产效率[2]。然而,工业物联网与传统物联网相比对数据传输的可靠性和实时性要求高[3]。因此,工业物联网需要满足时间同步精确、通信准确和适应性高等要求[4]。随着工业物联网技术的广泛应用,工业物联网中的安全问题成为其发展过程中所面临的重大挑战。工业生产中传感器节点采集的数据通常在公共信道进行传输,数据易遭受外部威胁和攻击[5]。此外,工业物联网中的设备资源有限无法支持复杂的计算操作,现有的认证方案大多数基于非对称密码体制。而基于非对称密码体制的方案需要大量计算、存储等资源,因此无法应用于工业物联网中。为了保障采集工业物联网中的数据安全和隐私,建立适

收稿日期:2020-01-13。国家自然科学基金项目(61672290)。**夏艳东**,硕士,主研领域:物联网,信息安全,大数据。**戚荣鑫**,硕士生。**季赛**,教授。

用于工业物联网的安全且轻量的认证与密钥交换协议是当前研究的热点方向。Chang 等[6]设计了一种基于智能卡的移动无线传感网认证协议,该协议能够提供完美前向安全性,但 Li 等[19]分析认为 Chang 等人的协议存在缺乏正确的双向认证且无法抵抗智能卡丢失攻击等问题。为了提高用户身份验证的安全性,生物特征凭借唯一性、不易复制性等特性[7-8]而得到广泛应用[9,11]。Li 等[19]基于椭圆曲线密码体制,提出了一种基于生物特征的无线传感网认证协议,该协议解决了 Chang 等的协议安全威胁,且能够抵抗大多数常见攻击并提供一些理想的安全属性。何炎祥等[10]梳理了无线传感器网络中公钥密码机制研究现状,指出无线传感器网络对外部用户的认证应该集中于基于口令、智能卡、生物特征等多因素访问控制方法的研究。Srinivas 等[9]提出了一种基于智能卡,生物特征和密码的三因素用户认证密钥协商方案,该方案支持智能卡撤销以及密码和生物密钥更新。Li 等[11]提出了一种基于密码,切比雪夫混沌映射和二次剩余定理的三方认证密钥协商方案,该方案提供了用户匿名属性。Esfahani 等[13]提出一种适用于工业物联网中机器对机器(M2M)通信的轻量级认证机制,该机制仅使用哈希函数和异或操作,尽管该协议适用于资源有限的 M2M 设备,但是未考虑网关节点(GWN)与 M2M 设备之间的认证。

针对上述研究中仍存在的问题,本文利用基于物理不可克隆函数(PUFs)与模糊提取器,提出了一种轻质的用户认证与密钥交换协议,所提出的协议利用模糊提取器提取生物特征信息进行用户认证,并结合物理不可克隆函数提取传感器设备物理特征。本协议仅使用单向函数,异或操作和对称加/解密技术实现工业物联网中用户,GWN 和传感器设备的三重双向认证并建立用户与传感器设备间的安全会话密钥,能够有效减少通信与计算开销。实验结果与分析表明,所提出的协议适用于资源有限的传感器设备,能够抵抗重放攻击、伪装攻击、特权内部攻击、中间人攻击和物理设备窃取等多种攻击。

1　预备知识

1.1　物理不可克隆函数

物理不可克隆函数[12,14]是基于难以处理的复杂的物理系统将一组挑战映射到一组响应中的函数。PUF 表示物理不可克隆函数,PUF 的输入一般称为挑战,用 $c \in C$ 表示,输出一般被称为响应,用 $r \in R$ 表示。挑战及其对应的响应被称为挑战-响应对(Challenge Response Pair,CRP),用 $CRP(c,r)$ 表示。存在一个映射关系 $PUF: C \rightarrow R$ 使得 $PUF(C) = R$,对于每一个物理不可克隆函数 PUF,挑战响应对是唯一的。物理不可克隆函数 PUF 具有以下属性:

(1) PUF 函数的输出必须取决于硬件的物理微结构,对于任意 PUF 函数,使用相同的挑战 c 作为 PUF 函数输入时,在误差允许的范围内,该函数总是输出相同的响应值 $r = PUF(c)$。

(2) PUF 函数的输出是不可预测的:给定挑战响应对集合 $Q = \{(c_i, r_i = PUF(c_i)) \mid i = 1,2,\cdots,n\}$,在一定误差范围内,敌手预测响应值 $PUF(c_t)$ 是困难的。其中 c_t 是一个挑战且满足条件 $(c_t, r_t = PUF(c_t)) \notin Q$。

(3) 函数 PUF 易于实现:给定函数 PUF 和输入 c,在多项式时间内计算出 $PUF(c)$ 是可行的。

(4) 函数 PUF 具有不可克隆性:从物理层面,给定一个实体的物理不可克隆函数 PUF,构造一个物理实体使得该实体包含的物理不可克隆函数 PUF' 对于任意一个输入 $c \in C$ 在很小的误差范围内满足 $PUF'(c) = PUF(c)$ 是困难的。从数学层面,给定一个物理不可克隆函数,构造一个函数 F 使得对于任意一个输入 $c \in C$ 在很小误差范围内满足 $F(c) = PUF(c)$ 是困难的。因此,函数 PUF 是物理不可克隆的。

1.2　模糊提取器

近年来,模糊提取器(Fuzzy Extractor, FE)[15,17]广泛应用于用户生物特征信息验证,模糊提取器通常定义为一个三元组 (M,l,t),主要由以下密钥生成算法和密钥重构算法组成。

$Gen(\cdot)$:密钥生成算法是一个概率性算法。用户以个人生物信息 BIO_i 作为算法输入,其中 BIO_i 取自给定的度量空间 M,输出一个对应的长度为 l 比特的生物密钥 $\sigma_i \in \{0,1\}^l$ 和一个公共重构参数 τ_i,算法满足 $Gen(BIO_i) = (\sigma_i, \tau_i)$。其中,用户对于生物密钥 σ_i 保密,公共重构参数 τ_i 用于帮助重构出初始生物密钥 σ_i。

$Rep(\cdot)$:密钥重构算法是一个确定性算法。该算法以一个含噪声的用户生物信息 $BIO'_i \in M$ 以及和原生物信息 BIO_i 相关公共参数 τ_i 与 t 作为输入,输出为初始的生物密钥 σ_i,算法满足 $Rep(BIO'_i, \tau_i) = \sigma_i$。其中 t 为预定的误差容限阈值,当生物信息 BIO_i 与 BIO'_i 之间的汉明距离小于 t 值时,用户能够通过生物信息 BIO'_i 恢复出初始生物密钥 σ_i。

2 密钥交换方案构造

本文基于用户生物特征和传感器设备物理特征，提出了一种适用于工业物联网环境的轻量的用户认证与密钥交换协议。该协议包含 6 个步骤：传感器设备注册，用户注册，网关节点注册，登录，身份认证与密钥交换，生物密钥和密码更新。用户、网关节点和传感器设备分别在注册中心注册，注册中心作为一个可信第三方为用户，网关节点和传感器设备生成认证所需的身份标识和密钥，具体的注册流程如图 1 所示。

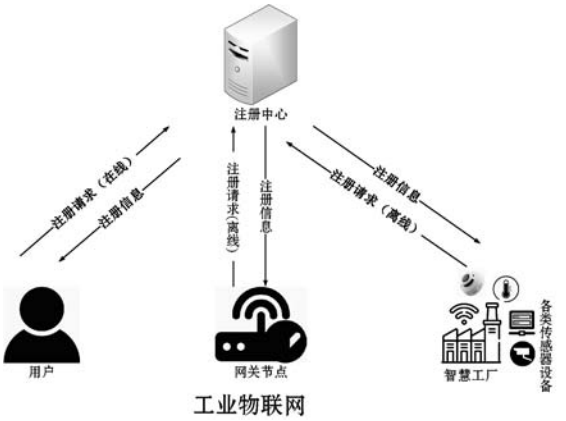

图 1 工业物联网初始化注册阶段

2.1 传感器设备注册阶段

传感器设备 SD_j 以离线的方式执行以下步骤完成注册，具体的注册步骤如下：

（1）传感器设备 SD_j 输入挑战 c_j，经过函数 PUF 得到响应值 r_j，然后利用模糊提取器提取传感器设备的物理特征 $Gen(r_j)=(\sigma_{r_j},\tau_{r_j})$ 得到 σ_{r_j}，并在安全的信道上发送注册请求和 σ_{r_j} 给注册中心（Register Center，RC）。

（2）在接收到传感器设备 SD_j 的注册请求后，RC 生成一个长度为 1 024 比特的密钥 key_{ISD_j-GWN} 并为每个传感器设备生成长度为 128 比特的身份标识 ISD_j。同时，为了保护密钥 key_{ISD_j-GWN} 的安全，RC 计算 $E_j=h(key_{ISD_j-GWN}\|ISD_j)\oplus\sigma_{r_j}$，然后将 ISD_j 和 E_j 发送给传感器设备。

（3）传感器设备 SD_j 计算 $E_j\oplus\sigma_{r_j}$ 并将 ISD_j 和 $E_j\oplus\sigma_{r_j}$ 保存在存储器中。

2.2 用户注册阶段

用户 U_i 在一个安全的信道上执行以下步骤完成注册，具体注册步骤如下：

（1）用户 U_i 选择一个 128 比特长的身份标识 ID_i 和一个 64 比特长的高熵密码 PW_i，通过指纹提取传感器取得用户生物特征信息 BIO_i，并依据密钥生成算法计算生物密钥 σ_i。然后，选择一个随机数 a 并计算 $RPW_i=h(PW_i\|\sigma_i\|a)$，将消息〈$ID_i$，$RPW_i$〉发送给 RC。

（2）RC 接收到用户注册请求后，生成一个 1 024 比特长的密钥 key_{U_i-GWN} 和对应于 ID_i 的临时身份标识 TID_i，计算 $B_i=h(ID_i\|key_{U_i-GWN})\oplus RPW_i$；然后，RC 通过安全信道将消息〈$TID_i$，$B_i$〉返回给用户。

（3）用户 U_i 接收到 RC 返回的消息后，为防止特权内部攻击，计算 $B'_i=B_i\oplus RPW_i\oplus h(ID_ib\|\sigma_i)$，$A_i=h(ID_i\|\sigma_i)\oplus a$。为了能够在发送访问请求前验证用户身份以避免不必要的通信开销，计算 $D_i=h(ID_i\|RPW_i\|A_i)$ 以进行本地化的身份验证；然后，用户将参数 A_i、B'_i、D_i、TID_i、$h(\cdot)$、$Gen(\cdot)$、$Rep(\cdot)$、τ_i 和 t 保存到用户设备中。

2.3 网关节点注册阶段

网关节点（$IGWN$）以离线的方式执行以下步骤完成注册：

（1）网关节点 $IGWN$ 发送注册请求给 RC。

（2）RC 接收到网关节点 $IGWN$ 的注册请求后，为网关节点生成一个 128 比特长的身份标识 $IGWN$；然后将用户信息$\{TID_i,ID_i,key_{U_i-GWN}\mid i=1,2,\cdots,n\}$ 和传感器信息$\{ISD_j,key_{ISD_j-GWN}\mid j=1,2,\cdots,n\}$ 安全地保存到网关节点中。

2.4 登录阶段

在登录过程中，用户 U_i 发送请求访问传感器设备，为了减少资源开销，在发送请求前需要先进行本地化身份验证，具体的步骤如下：

（1）用户 U_i 输入 ID_i 和 PW_i，通过指纹提取器提取生物特征信息 BIO_i；然后用户设备利用密钥重构算法重构生物密钥 $\sigma_i^*=Rep(BIO_i^*,\tau_i)$ 并分别计算 $a^*=A_i\oplus h(ID_i\|\sigma_i^*)$，$RPW^*=h(PW_i\|\sigma_i^*\|a^*)$ 和 $D_i^*=h(ID_i\|RPW^*\|A_i)$；最后验证 D_i^* 与 D_i 是否相等。若相等，则本地化身份验证成功，继续执行协议，反之，中止会话请求。

（2）用户 U_i 利用智能设备生成一个随机整数 r_{U_i} 和一个时间戳 TS_1，并计算 $B_i^*=B'_i\oplus h(ID_i\|\sigma_i^*)$。然后，为了向网关节点和目标设备 SD_j 安全地传递参数 r_{U_i}，分别计算消息 $M_1=r_{U_i}\oplus h(B_i^*\|TS_1)$ 与 $M_2=ISD_j\oplus B_i^*\oplus h(ID_i\|r_{U_i})$，并将 M_1、M_2、r_{U_i} 等参数作为哈希函数的输入计算 M_3，消息 M_3 用于辅助网关节点验证用户身份。

（3）用户 U_i 通过公共信道发送消息请求 TID_i、M_1、M_2、M_3 和 TS_1 给网关节点 $IGWN$。

2.5　密钥交换阶段

当用户 U_i 完成本地化身份验证并发送认证请求给目标传感器设备,认证与密钥交换的过程如图 2 所示。该步骤是为了通过网关节点 *IGWN* 与目标访问传感器设备进行双向认证并建立安全会话密钥。该步骤包含用户与网关节点、网关节点与目标传感器设备、传感器设备与用户之间的双向认证。因为本方案采用时钟同步机制,采用随机数与时间戳相结合的方式防止重放攻击,具体的认证与密钥交换过程如下。

(1) 网关节点 *IGWN* 接收到用户认证请求后,验证发送与接收的时间差值是否小于最大允许的通信时间延迟 ΔT,若差值小于 ΔT,则继续认证过程,反之,中止会话。然后检索网关节点 *IGWN* 数据库中存储的与 TID_i 对应的用户身份 ID_i 以及用户与网关节点间的对称密钥 key_{U_i-GWN},若存在,则继续认证,反之,中止会话。然后,网关节点 *IGWN* 通过已知参数获取对称密钥 $M_4=h(ID_i \parallel key_{U_i-GWN})$、$r_{U_i}^*$ 和 ISD_j,并计算 M_5 以验证 M_5 与 M_3 是否相等。若相等,则用户 U_i 身份验证成功,反之,则中止会话。然后,网关节点 *IGWN* 生成一个随机整数 r_g 和当前时间戳 TS_2,采用 AES-128 对称密码加密隐私参数 ID_i、$IGWN$、r_g,$r_{U_i}^*$、$h(M_4 \parallel TS_2)$,并将这些参数与 E_j、TS_2 一起置入哈希函数运算中得到消息 M_7 以帮助传感器验证网关节点身份;最后,将认证消息 M_6、M_7 和 TS_2 发送给目标传感器设备 SD_j。

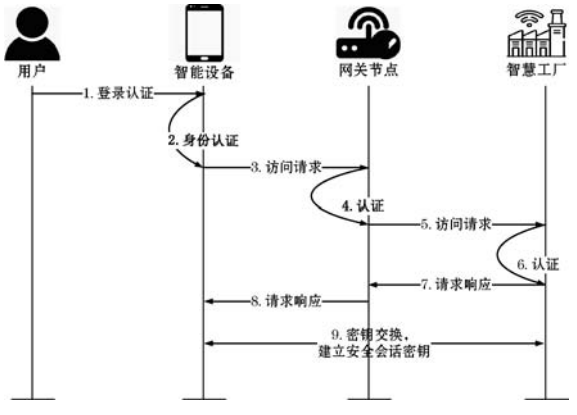

图 2　用户认证与密钥交换过程

(2) 目标传感器设备 SD_j 接收到网关请求后,验证发送与接收的时间差值是否小于最大允许的通信时间延迟 ΔT,若差值小于 ΔT,则继续认证过程,反之,中止会话。传感器设备利用不可克隆函数计算 $r_j^*=PUF(c_j)$ 并利用模糊提取器重构算法获取物理密钥 $\sigma_{r_j}^*=Rep(r_j^*,\tau_{r_j})$。计算对称密钥 $M_8=h(ISD_j \parallel key_{ISD_j-GWN}) \oplus \sigma_{r_j}^*$ 解密消息 M_6 得到私密参数 ID_i、$IGWN^*$、r_g、$r_{U_i}^*$ 和 $h(M_4 \parallel TS_2)$。然后,为验证网关节点的身份利用获取的参数计算消息 M_9,若 M_9 与 M_7 相等,则成功验证网关节点身份,继续会话,反之,中止会话。认证成功后,传感器设备 SD_j 生成一个随机整数 r_{SD_j} 和当前时间戳 TS_3、并将参数 ID_i、$IGWN^*$、ISD_j、r_g、$r_{U_i}^*$、r_{SD_j}、$h(M_8 \parallel TS_3)$,TS_3 和 $h(M_4 \parallel TS_2)$ 作为哈希函数的输入计算会话密钥 SK_{ij}。同时,为帮助用户与网关节点验证传感器设备 SD_j 的身份,计算 $M_{10}=r_{SD_j} \oplus h(M_4 \parallel TS_2)$ 以安全传输参数 r_{SD_j}。以参数 r_{SD_j}、r_g、ISD_j、$IGWN^*$、M_{10} 和 TS_3 作为哈希函数的输入计算消息 M_{11} 帮助网关节点验证传感器设备身份,以参数 SK_{ij}、r_{SD_j}、$r_{U_i}^*$ 和 TS_3 作为哈希函数的输出计算消息 M_{12} 帮助用户验证传感器设备身份。最后,传感器设备将消息 M_{10}、M_{11}、M_{12} 和 TS_3 发送给网关节点 *IGWN*。

(3) 当网关节点 *IGWN* 接收到传感器传回的消息后,验证发送与接收的时间差值是否小于最大允许的通信时间延迟 ΔT,若差值小于 ΔT,则继续认证过程,反之,中止会话。网关节点 *IGWN* 计算 $r_{SD_j}^*$ 和 M_{13},并验证 M_{13} 与 M_{11} 是否相等。若相等,则验证传感器设备成功继续会话,反之,中止会话。然后,网关节点生成当前时间戳 TS_4,计算与用户间的对称密钥 $M_{14}=h(M_4 \parallel TS_4)$ 用于将参数 $r_{U_i}^*$、r_g、$r_{SD_j}^*$、$IGWN$、$h(M_8 \parallel TS_3)$ 和 TS_2 加密发送给用户以帮助生成会话密钥。此外,计算 $M_{16}=M_{14} \oplus TID_i^{new}$ 以更新用户 U_i 的临时身份标识 TID_i。最后,网关节点 *IGWN* 将消息 M_{12}、M_{15}、M_{16},TS_3 和 TS_4 转发给用户 U_i。

(4) 用户 U_i 接收到网关节点转发的消息后,验证发送与接收的时间差值是否小于最大允许的通信时间延迟 ΔT,若差值小于 ΔT,则继续认证,反之,中止会话。用户 U_i 计算 $h(B_i^* \parallel TS_4)$ 以解密获取参数 $r_{U_i}^*$、r_g、$r_{SD_j}^*$、$IGWN$、$h(M_8 \parallel TS_3)$ 和 TS_2;然后验证 $r_{U_i}^*$ 与 r_{U_i} 是否相等,若不相等,表示会话不一致,则中止会话,反之,继续会话,将参数 ID_i、$IGWN^*$、ISD_j、r_g、$r_{U_i}^*$、$r_{SD_j}^*$、$h(M_8 \parallel TS_3)$、TS_3 和 $h(M_4 \parallel TS_2)$ 作为哈希函数的输入计算会话密钥 SK_{ij}^*。为了验证用户 U_i 计算的会话密钥是否与传感器设备 SD_j 计算的会话密钥相等,用户 U_i 计算 $M_{17}=h(SK_{ij}^* \parallel r_{U_i} \parallel r_{SD_j}^* \parallel TS_3)$,若 M_{17} 与 M_{12} 相等,则会话密钥建立成功,反之,中止会话。最后,用户 U_i 计算临时身份标识 $TID_i^{new}=h(B_i^* \parallel TS_4) \oplus M_{16}$ 代替旧的临时身份标识。

2.6　生物密钥与密码更新阶段

该步骤进行本地化的生物密钥与密码更新,不需要 RC 的参与,具体的更新过程如下:

(1) 用户 U_i 输入 ID_i、PW_i^* 和 BIO_i^* 到用户设备进行本地化身份验证,用户设备通过模糊提取器密钥生

成算法计算 $Gen(BIO_i^*)=(\sigma_i^*,\tau_i^*)$，并结合本地存储的 A_i 提取出私密参数 $a'=h(ID_i \| \sigma_i^*) \oplus A_i$，计算 $RPW_i^*=h(PW_i^* \| \sigma_i^* \| a')$；用户设备计算 $D_i^*=h(ID_i \| RPW_i^* \| A_i)$ 与本地存储的 D_i 进行验证，若两者不相等，则中止更新，反之，继续更新过程，提示用户输入新的密码和生物信息。

（2）用户 U_i 输入新的密码 PW_i^{new} 和生物信息 BIO_i^{new} 后，利用模糊提取器提取新的生物密钥 $Gen(BIO_i^{new})=(\sigma_i^{new},\tau_i^{new})$，计算 A_i^{new} 和 RPW_i^{new}；结合用户设备存储 B'_i 计算 $B_i^{new'}$ 和 D_i^{new}；最终，用户设备以 A_i^{new}、$B_i^{new'}$、D_i^{new} 和 τ_i^{new} 替换存储的 A_i、B'_i、D_i 和 τ_i 完成更新操作。

3 实验分析

本协议采用模糊提取器提取用户生物特征并结合物理不可克隆函数提取传感器设备物理特征。在保证协议安全性的前提下提出了一个适用于工业物联网环境更轻量的认证与密钥交换协议。协议中，我们仅采用对称加/解密操作、哈希操作、异或操作来实现三重双向身份并建立用户与传感器设备的会话密钥。由于异或操作所需要的计算开销远小于其他操作，我们只考虑模糊提取操作、哈希操作、对称加/解密操作和群 G_1 上的标量乘法操作。我们以符号 T_{fe}、T_h、T_e 和 T_m 分别表示进行模糊提取操作、哈希操作、对称加/解密操作和群 G_1 上的标量乘法操作所需要计算开销。各操作所需的计算开销如表 1 所示。

表 1 各操作计算开销

名称	描述	计算时间/ms
T_{fe}	模糊提取器	17.1
T_h	哈希函数	0.32
T_e	对称加/解密	5.6
T_m	使用 ECC 的标量乘法	19.2

在认证与密钥交换阶段，Li 等[19]的协议需要的计算总开销为 $1T_{fe}+19T_h+6T_m$，Li 等[20]的协议需要的计算总开销为 $1T_{fe}+19T_h+3T_m+8T_e$，Wang 等[21]的协议需要的计算总开销为 $26T_h+4T_m+4T_e$，本文协议需要的计算总开销为 $2T_{fe}+19T_h+4T_e$。同时，Li 等[19]、Li 等[20]、Wang 等[21]以及本文协议中实体间通信所需的通信开销分别为 2 720 比特、2 688 比特、3 200 比特和 3 040 比特。本文协议在保证安全的前提下提高了协议运行的效率。本文协议和其他协议在认证与密钥交换阶段的计算开销和通信开销如表 2 所示。表 3 为各文献安全属性对比。可以看出，本文协议的计算总开销与通信总开销远小于文献[19]、文献[20]和文献[21]，同时能够抵抗多种安全威胁。本文协议与其他协议相比，支持更多如用户匿名、不可追踪等安全属性，并提升安全性，降低了计算开销，更适合于资源受限的工业物联网中的传感器设备。

表 2 各方案性能对比

开销	协议			
	文献[19]	文献[20]	文献[21]	本文
U_i 端开销	$1T_{fe}+8T_h+3T_m$	$1T_{fe}+7T_h+2T_m+2T_e$	$12T_h+2T_m+1T_e$	$1T_{fe}+8T_h+1T_e$
IGWN 端开销	$7T_h+1T_m$	$8T_h+1T_m+4T_e$	$10T_h+2T_e$	$7T_h+2T_e$
SD_j 端开销	$4T_h+2T_m$	$4T_h+2T_e$	$4T_h+2T_m+1T_e$	$1T_{fe}+4T_h+1T_e$
计算开销/ms	$1T_{fe}+19T_h+6T_m \approx 138.38$	$1T_{fe}+19T_h+3T_m+8T_e \approx 125.58$	$26T_h+4T_m+4T_e \approx 107.52$	$2T_{fe}+19T_h+4T_e \approx 62.68$
通信开销/比特	2 720	2 688	3 200	3 040

表 3 安全属性对比

安全属性	协议			
	文献[19]	文献[20]	文献[21]	本文
抵抗用户设备窃取攻击	是	是	是	是
抵抗用户伪装攻击	是	是	是	是
抵抗传感器设备窃取攻击	是	–	是	是
抵抗传感器设备伪装攻击	是	是	–	是
抵抗特权内部攻击	否	否	否	是
抵抗重放攻击	是	是	是	是
抵抗离线字典攻击	–	–	–	是
生物特征保护	是	是	否	是
用户匿名性	是	是	是	是
不可追踪性	是	是	是	是
双向身份验证	是	是	是	是
会话密钥安全	是	是	是	是

4 结　语

本文利用物理不可克隆函数与模糊提取器,提出了一种用于工业物联网的身份认证与密钥交换协议,该协议使用模糊提取器实现了用户生物特征与传感器设备物理特征模式匹配,有效保证了用户设备与传感器设备的安全。实验结果表明本文协议能够抵抗多种攻击且满足众多安全需求,有效提高了协议执行的效率。与其他现有的方案相比,本文协议更适用于资源有限的工业物联网环境。

参 考 文 献

[1] 康世龙,杜中一,雷咏梅,等. 工业物联网研究概述[J]. 物联网技术,2013,3(6):80 - 82,85.

[2] 王飞跃,张军,张俊,等. 工业智联网:基本概念,关键技术与核心应用[J]. 自动化学报,2018,44(9):1606 - 1617.

[3] 于洪飞. 工业物联网技术的应用及发展[J]. 电子技术与软件工程,2019(8):20.

[4] 李士宁,罗国佳. 工业物联网技术及应用概述[J]. 电信网技术,2014(3):26 - 31.

[5] 杨威,王宇建,吴永强. 物联网设备身份认证安全性分析[J]. 信息安全研究,2019,5(10):918 - 923.

[6] Chang C, Le H. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks [J]. IEEE Transactions on Wireless Communications,2016, 15(1):357 - 366.

[7] 胡彬. 生物识别技术与安全浅析[J]. 网络安全技术与应用,2017(5):137 - 138.

[8] 王丹娜. 生物识别:传统信息安全在新技术环境的创新应用[J]. 中国信息安全,2019(2):60 - 64.

[9] Srinivas J, Das A K, Wazid M, et al. Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things[J]. IEEE Transactions on Dependable and Secure Computing, 2018,17(6):1133 - 1146.

[10] 何炎祥,孙发军,李清安,等. 无线传感器网络中公钥机制研究综述[J]. 计算机学报,2019,43(3):381 - 408.

[11] Li C T, Chen C L, Lee C C, et al. A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps[J]. Soft Computing, 2018,22(8):2495 - 2506.

[12] Suh G E, Devadas S. Physical unclonable functions for device authentication and secret key generation[C]//Proceedings of the 44th annual Design Automation Conference. ACM, 2007: 9 - 14.

[13] Esfahani A, Mantas G, Matischek R, et al. A lightweight authentication mechanism for M2M communications in Industrial IoT environment[J]. IEEE Internet of Things Journal, 2019, 6(1): 288 - 296.

[14] 张紫楠,郭渊博. 物理不可克隆函数综述[J]. 计算机应用,2012,32(11):3115 - 3120.

[15] Odelu V, Das A K, Goswami A. A secure biometrics-based multi-server authentication protocol using smart cards[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1953 - 1966.

[16] Palash S. A simple and generic construction of authenticated encryption with associated data[J]. ACM Transactions on Information and System Security, 2010,13(4):1 - 16.

[17] 杜俊雄,陈伟,李雪妍. 基于物联网设备指纹的情境认证方法[J]. 计算机应用,2019,39(2):464 - 469.

[18] Choo K R. Key establishment: Proofs and refutations[D]. Brisbane :Queensland University of Technology, 2006.

[19] Li X, Niu J, Bhuiyan M, et al. A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3599 - 3609.

[20] Li X, Peng J, Niu J, et al. A robust and energy efficient authentication protocol for Industrial Internet of Things[J]. IEEE Internet of Things Journal,2018,5(3):1606 - 1615.

[21] Wang D, Li W, Wang P. Measuring two-factor authentication schemes for real-time data access in Industrial wireless sensor Networks[J]. IEEE Transactions on Industrial Informatics, 2018, 14(9): 4081 - 4092.

(上接第 212 页)

[12] Guan J, Ou J, Lai Z, et al. Medical image enhancement method based on the fractional order derivative and the directional derivative[J]. International Journal of Pattern Recognition and Artificial Intelligence,2018,32(3):1 - 22.

[13] Muslim H S M, Khan S A, Hussain S, et al. A knowledge-based image enhancement and denoising approach[J]. Computational and Mathematical Organization Theory, 2019, 25(2): 108 - 121.

[14] Ahmed I T, Der C S, Jamil N, et al. Analysis of global spatial statistics features in existing contrast image quality assessment algorithm[C]//2019 7th International Conference on Information and Communication Technology (ICoICT), 2019.

[15] Dou H, Chen C, Hu X, et al. Asymmetric cyclegan for unpaired NIR-to-RGB face image translation[C]//2019 IEEE International Conference on Acoustics, Speech and Signal Processing(ICASSP). IEEE,2019:1757 - 1761.