基于 PUF 的轻量级雾辅助物联网认证协议

郭奕旻[1] 张振峰[2] 熊 平[1] 郭亚军[3]

[1](中南财经政法大学信息与安全工程学院 武汉 430073)

[2](中国科学院软件研究所可信计算与信息保障实验室 北京 100190)

[3](华中师范大学计算机学院 武汉 430079)

摘 要 雾计算将云计算的功能扩展到网络边缘,是各类物联网应用的最佳解决方案.但是雾计算独特的特性给雾辅助的物联网也带来了新的安全性问题,特别是物联网设备与雾节点之间的认证问题.在雾辅助的物联网中,一些雾节点和物联网设备是部署在公共场所,这使得它们更容易受到各种攻击.因此,为雾辅助的物联网系统设计认证协议首先应确保安全性,即认证协议能够抵抗各种已知的攻击,特别是在雾节点不完全可信或者物联网设备被捕获时也应该是安全的.其次,认证协议应该是低延迟的,低延迟是雾计算的基本特征.最后,由于许多物联网设备资源受限,认证协议也应该是轻量级的.为了解决这些问题,本文提出了雾辅助物联网两个场景中的轻量级认证协议.两个协议都采用了物理不可克隆函数这一硬件安全原语,一种实现了物联网设备与雾节点之间的相互认证,另一种实现了远程用户通过雾节点安全访问物联网设备.协议中任何实体均不存储显式的挑战-响应对和其他敏感信息,具备显著安全优势.对两个协议的形式化安全、非形式化安全和性能分析表明,所提出的认证协议不仅在各种已知攻击下具有鲁棒性,且具有较少的计算和通信代价.

关键词 雾计算;物联网;物理不可克隆函数;认证;轻量级

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2022.01412

PUF-Based Lightweight Authentication Protocols for Fog Assisted IoT

GUO Yi-Min[1] ZHANG Zhen-Feng[2] XIONG Ping[1] GUO Ya-Jun[3]

[1](*School of Information and Safety Engineering, Zhongnan University of Economics and Law, Wuhan* 430073)

[2](*Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing* 100190)

[3](*School of Computer, Central China Normal University, Wuhan* 430079)

Abstract Fog computing is a new distributed computing paradigm that extends cloud computing services to the edge of the network, which has the characteristics of low latency, low bandwidth consumption, high reliability, high security, and high quality of experience. Therefore, fog computing is considered to be the most effective solution for supporting IoT applications. However, the unique characteristics of fog computing have also brought new security issues to the fog-assisted IoT, especially the authentication problem between IoT devices and fog nodes. Fog-enabled IoT is composed of the cloud layer, fog layer, and device layer. It is a decentralized distributed computing environment with multiple different trust domains. Among them, the cloud layer is trustworthy, but the fog layer and the device layer are not necessarily trustworthy. Fog nodes are usually deployed by different providers, and they can also automatically join or leave the network. Moreover, some fog nodes are deployed in public places and are easily destroyed. IoT devices belong to different owners and do not trust each other. In addition, IoT devices are usually deployed in places that are not

收稿日期:2021-03-01;在线发布日期:2021-08-23.本课题得到国家自然科学基金(62102453)和中南财经政法大学中央高校基本科研业务费专项资金(2722022BQ049)资助.**郭奕旻**,博士,讲师,主要研究方向为口令安全和身份认证.E-mail:yiminguo@zuel.edu.cn.**张振峰**,博士,研究员,主要研究领域为密码学和信息安全.**熊 平**,博士,教授,主要研究领域为信息安全、机器学习和数据挖掘.**郭亚军**,博士,教授,主要研究领域为信息安全和现代密码学.

strictly monitored and protected and are easy to be invaded, destroyed, or stolen by attackers. Therefore, the authentication protocol designed for the fog-assisted IoT system first ensures the security, that is, the authentication protocol can resist various known attacks, especially when the fog nodes are not completely trusted or the IoT devices are captured. Secondly, the authentication protocol should also be low-latency, which is the basic feature of fog computing. Finally, since many IoT devices are resource-constrained, the authentication protocol should also be lightweight. In order to solve these problems, this paper proposes two lightweight authentication protocols in two scenarios of fog-assisted IoT. Both protocols use the hardware security primitive of Physically Unclonable Functions (PUF). One implements mutual authentication between IoT devices and fog nodes, and the other implements remote users to securely access IoT devices through fog nodes. The two proposed protocols have the following advantages: (1) The two protocols can ensure the physical security of IoT devices and user devices, and can resist the compromised attack of fog nodes. (2) In the two protocols, no explicit challenge-response pairs (CRPs) are stored in any party participating in the authentication, thereby eliminating the security risk that CRPs must be stored in the "challenge-response" authentication mechanism using PUFs. (3) In the authentication process, the piggyback method is used to check the synchronization of the message, which can effectively prevent the desynchronization attack without adding any burden. (4) Both authentication protocols are lightweight. We employ the widely-accepted ROR model to perform formal security analysis on the two proposed protocols, and the results show that the two protocols are provably secure. We further use informal security analysis to find that the proposed scheme has robust security and can resist more known attacks than other existing schemes. Finally, we evaluate the performance of the two proposed protocols from the aspects of security features, communication cost, and computation cost. The results show that the proposed protocols outperform the existing protocols.

Keywords　fog computing; Internet of Things; physically unclonable function; authentication; lightweight

1　引　言

物联网的广泛应用促使了越来越多的物联网设备接入到网络中，这些互联设备将产生前所未有的数据量，将所有数据传输到云中集中式处理显然是不可取的，这是由于云虽然具有强大的计算、存储和高处理能力，但云与物联网物理距离较远，会导致数据处理延迟和网络拥塞，从而影响物联网应用的服务质量[1-2]. 为了解决物联网应用所需要的低延迟、低带宽消耗以及高可靠性、高安全性和高体验质量等需求，雾计算应运而生. 雾计算是将云计算的服务扩展到了网络边缘的一种新的分布式计算范式，它在网络边缘直接为物联网设备提供了计算、存储和网络等服务[3-4]. 雾计算具有位置感知、低延迟、移动性、实时交互、异构性、可扩展性、互操作性和大规模分布式控制等特性[5-7]. 但是，雾计算并不是替代了云计算[3]，而是对云计算进行了扩展. 雾计算是在两层架构的云与终端设备之间增加了靠近终端设备的雾层. 雾层由一个或者多个雾节点组成，雾节点由传统的网络组件构成，如路由器、交换机、基站、机顶盒等. 雾层负责接对物联网设备采集的数据进行计算、传输、临时存储和实时分析. 雾层与云层通信，可以借助云端强大的资源对数据进行永久存储和全局分析[8-10].

雾计算的这些特性能够较好地支持各种物联网应用[11]. 目前已经提出了许多雾辅助的物联网应用范例[9,12]，包括智能家居[13-15]、医疗保健[12,16-18]、智慧城市[19-22]、车联网[23-26]等. 但是，雾计算与物联网结合后会出现一些新的安全性问题，特别是雾计算中的认证问题面临更大的挑战. 这主要有多个方面的原因：首先，雾计算的分散基础构架引入了云、雾服务提供商和用户等多个不同的信任域，在多个信任域中，云节点被认为是可信的，但雾节点和雾设备

不被认为是完全可信的,这是由于一些雾节点和物联网设备是部署在公开的场所,很容易被攻击者入侵,破坏或被盗;其次,雾计算的认证过程不应该由云参与.云的参与增加了认证延迟,这与雾计算的引入目的相违背.也就是说,雾计算环境中的认证应该在雾节点和物联网设备之间进行,并且这两个实体不一定完全可信;再次,一些物联网设备是资源受限的,雾计算环境中的认证协议也应该是轻量级的.最后,雾计算环境中的认证协议应具有较好的安全特性(如匿名性),并能够抵抗各种已知的攻击.

目前已经为物联网系统设计了许多有效的云辅助和网关辅助的认证协议[27-32].在云辅助的物联网认证协议中,必须借助远程的云来执行认证过程.在网关辅助的物联网认证协议中,靠近物联网设备的网关被假设为完全可信,这种假设不总是成立的.现有的这些认证协议不适合应用于雾辅助的物联网系统主要有下面几个原因:首先,在这些安全协议中需要有一个完全可信方.为了能够对物联网设备实施认证,一些秘密信息必须存储在可信方中.虽然云可以被认为是完全可信的,但是由云参与会增加认证延迟,这不符合雾计算的特征;第二,一些认证协议也默认物联网设备是物理安全的,所以将认证所需要的秘密信息存储在物联网设备中.实际上许多物联网设备是部署在公共场所,它们很容易被捕获;第三,许多为物联网系统设计的认证协议采用了计算量大的密码原语,因而不适合资源受限的物联网设备参与认证.针对物联网设备的物理安全问题,比较可取的方法是采用物理不可克隆函数(Physically Unclonable Functions,PUF)的硬件安全原语.但是现有的基于 PUF 的物联网认证协议也存在许多问题,例如,这些协议更容易被执行各种攻击[33],另外,基于 PUF 的物联网认证协议通常是由验证方来存储物联网设备的"挑战-响应"对(Challenge-Response Pair,CRP),当验证方中的 CRPs 被泄漏,认证协议将是不安全的[34-36].Chatterjee 等人[37]将 CRPs 转移存储到另外一个安全数据库中,但这增加了认证的复杂性.目前也存在一些专门为雾计算环境设计的认证协议[38-40],但是这些协议不能满足雾计算安全认证协议必备的三个条件[41].针对上述问题,本文提出了轻量级安全的雾辅助物联网系统认证协议.该协议使用 PUFs 实现了雾计算环境中预期的安全性和效率要求.本文的主要贡献如下:

(1)设计了一种基于 PUFs 的轻量级雾辅助物联网认证协议,该协议在没有可信的云或者其他第三方参与下,实现了物联网设备、雾节点和用户之间的相互认证.

(2)该协议在雾节点被破坏或者被捕获情况下,也不泄漏用户和物联网设备的秘密信息.

(3)该协议在参与认证的任何一方中不存储显式的 CRPs,从而消除使用 PUFs 的"挑战-响应"认证机制中必须存储 CRPs 而带来的安全风险.

(4)该协议在认证过程中使用捎带的方式检验消息的同步性,能够在不增加任何负担情况下有效地防止去同步攻击.

(5)用 Real-Or-Random(ROR)安全模型形式化分析发现,提出的协议是可证明安全的.进一步用非形式化安全分析发现提出的协议能够抵抗各种已知攻击.

(6)通过详细的性能分析和与现有的认证协议比较表明,提出的认证协议兼顾了安全性和效率,更适合应用于雾辅助的物联网环境.

本文第 2 节介绍相关工作;第 3 节介绍预备知识和系统模型;第 4 节提出雾辅助物联网的认证协议;第 5 节对提出的协议进行形式化安全证明和非形式化安全分析;第 6 节是对认证协议的性能分析;第 7 节是本文的总结.

2 相关工作

近几年已经为物联网系统提出了许多认证协议.按照物联网系统的支撑方式不同,这些认证协议大致可以分为云辅助物联网认证协议、网关辅助物联网认证协议和雾辅助的物联网认证协议.在每一类认证协议中,采用不同的密码原语设计的认证协议也存在不同的性能.

云辅助物联网认证协议的基本特征是由可信云参与认证,在云端存储认证所需要的秘密信息.例如,Wu 等人[42]为可穿戴设备设计了一种由云服务器辅助的轻量级的认证协议.该协议只使用密码学中的哈希运算,因而有较高的效率,但是 Wu 等人的协议中,云服务器、可穿戴设备和用户手机都存储了秘密信息,因而该协议不支持匿名性和可跟踪性,也不能抵抗可穿戴设备和手机被盗攻击.Srinivas 等人[31]为可穿戴监控系统提出了一种基于云的认证方案.该协议使用了模幂、中国剩余定理和密码学哈希函数等密码原语操作.物联网注册时在云中存储

了物联网设备的身份标识和秘密证书，远程用户在云的辅助下实现了与可穿戴设备之间的相互认证. Jiang 等人[43]为自动驾驶汽车安全设计了云中心的三因子认证协议，云中存储了自动汽车和用户的秘密信息. 该协议主要采用公钥加密技术，存在计算量大的问题. Guo 等人[44]则为可穿戴计算环境设计了一种有效的匿名认证协议和群证明协议. 实现了穿戴设备与用户之间，以及用户和云服务器之间的相互认证，并为用一个用户的多个可穿戴设备生成一个群证明. Guo 等人的协议在云服务器主要存储可穿戴设备和用户设备的临时身份和哈希处理后的密文，并且协议只使用密码学中的哈希函数，具有较好的性能.

网关辅助物联网认证协议的基本特征是网关参与认证，并且假设网关是完全可信的，认证的秘密信息通常存储在网关中. 在采用对称密码和哈希函数等轻量级密码原语的认证协议中，通常事先在物联网设备和网关之间共享密钥. 例如，Wazid 等人[45]为物联网网络设计了一个轻量级的认证与密钥交换协议. 该协议的网关中存储了物联网设备和用户的秘密信息. 物联网设备设置时存储了一个秘密证书，作为与网关的共享密钥. 显然该协议不能抵抗物联网设备被捕获攻击. 这一类的认证方案还常常不具备匿名性，例如，在 Wu 等人[29]提出的认证方案中，网关不仅负责对传感器和用户进行注册，也参与了对用户的认证，由于用户和传感器的身份可以被跟踪，该认证方案不能抵抗传感器被捕获攻击，也不支持用户匿名性. 同样，Darbandeh 等人[46]、Ali 等人[47]、Sureshkumar 等人[48]、Poh 等人[49]设计的轻量级认证方案也存在类似的安全问题. 为了增强物联网系统的安全性，一些学者采用公钥密码技术设计网关辅助的认证协议[50-53]，例如，Naoui 等人[54]使用椭圆曲线密码技术为智能家居提出了一个认证协议，该协议支持用户匿名性，不过，由于在网关和物联网设备之间存在预共享密钥，因此不能抵抗物联网设备被捕获攻击. 在 Shuai 等人[55]提出的认证协议中，双方交换的消息时没有使用时间戳，因此不能检验消息的新鲜性. Li 等人[56]设计的认证方案具有匿名性，但不能抵抗假冒攻击. 总的来说，基于公钥密码原语设计的认证协议虽然在安全性方面有优势，但它们的操作是复杂和耗时的，不适合资源受限的物联网设备.

目前也提出了一些雾辅助物联网的认证协议，大部分认证协议是从基于云或者基于网关认证协议移植而来，不适合应用在雾计算环境中. 例如，Ibrahim 等人[38]最早提出了雾计算的认证方案，但该方案中暗含雾服务器是可信的，在注册阶段，雾服务器存储了雾用户的密钥，因此该方案不能抵抗雾服务器被破坏攻击. Gope[57]为雾计算场景设计了三种有效的轻量级匿名认证协议，其中第一个认证协议是在云协助下完成，这会存在认证延迟问题. 另外物联网设备在注册时，存储了许多敏感信息. 因此这些协议不能抵抗物联网设备被捕获攻击. Jia 等人[40]提出的认证方案也是在云服务器的帮助下完成. 在 Wazid 等人[39]设计的雾计算认证方案中，雾服务器存储了注册用户的伪身份，注册用户存储了某个雾服务器的临时身份和秘密参数，所以当该雾服务器失效或者离开雾，用户必须重新注册. Guo 等人[41]为雾计算环境设计了一个有效的认证协议，该协议由雾节点协助认证，并且在雾节点被破坏情况下，认证协议也是安全的.

在物联网应用中还有一类认证协议除使用密码原语外，还采用了硬件安全原语物理不可克隆函数(PUF). 这一类物联网认证协议最大的优势是轻量级的，并能够保证嵌入 PUFs 设备的物理安全性. 目前已经提出了许多基于 PUF 的物联网认证协议[37,58-59]. 但是这些认证协议存在一些安全问题. 引起这些安全问题的原因主要有两种：一种是由于设计方法缺陷而导致的漏洞，例如，不支持匿名性[59-60]、存在去同步攻击[61-62]、拒绝服务攻击[58,63-64]、假冒攻击[60,65-66]等等. 另一种是在某一参与认证方中存储了认证设备的“挑战-响应”对(CRP)而引起的安全问题. Frikken 等人[58]采用零知识证明来隐藏 PUF 的输出响应，但是每次需要用户输入口令. 另外，由于设计过于简单，Frikken 等人的认证协议还遭受多种攻击. Chatterjee 等人[37]指出了在验证方不应该显式地存储“挑战-响应”对这一挑战性问题，并结合身份的加密、PUFs 和密码学中的哈希函数设计了一个认证协议，但是，Chatterjee 等人的协议另外增加一个安全数据库来存储“挑战-响应”对，这增加了认证的复杂性.

3　预备知识与系统模型

3.1　密码哈希函数

密码哈希函数 $h:\{0,1\}^* \rightarrow \{0,1\}^n$ 是一个确定

性函数,它的输入是任意长度的二进制字符 x(称为消息),输出是一个固定长度为 n 的二进制字符串 $h(x)$(称为消息摘要).抗冲突的单向哈希函数形式化定义如下[67-68]:

定义 1. 抗冲突的哈希函数.假设 $Adv_{\mathcal{A}}^{\text{Hash}}(t)$ 表示一个敌手 $\mathcal{A}$ 在多项式时间 t 内发现一个哈希冲突的优势,那么

$$Adv_{\mathcal{A}}^{\text{Hash}}(t)=Pr[(x_1,x_2)\in R\leftarrow\mathcal{A}:x_1\neq x_2,h(x_1)=h(x_2)],$$

其中 $Pr[X]$ 表示随机事件 X 的概率,$(x_1,x_2)\in R\leftarrow\mathcal{A}$ 表示由 $\mathcal{A}$ 随机选择的输入字符串 x_1 和 x_2.一个 (θ,t) 的敌手 $\mathcal{A}$ 攻击哈希函数 $h(\cdot)$ 的抗碰撞性意味着 $\mathcal{A}$ 的执行时间最多为 t,并且 $Adv_{\mathcal{A}}^{\text{Hash}}(t)\leq\theta$.

3.2 物理不可克隆函数

物理不可克隆函数 PUF 是一种不可复制的单向函数,它根据设备独特的物理微结构将一组挑战映射为一组响应.挑战-响应对 CRP 常用来描述 PUF.PUF 中挑战(C)和响应(R)之间的关系为:$R=PUF(C)$.PUF 易于构造和评估,具有可再现性、唯一性、可标识性,物理不可克隆性和不可预测性[61].安全 PUF 形式化定义如下[58,69]:

定义 2. 安全 PUF 函数.一个安全的物理不可克隆函数 $PUF:\{0,1\}^{k_1}\rightarrow\{0,1\}^{k_2}$ 具有以下的属性:

(1)对于任何概率多项式时间的敌手 $\mathcal{A}$,预测 PUF 的输出是不可行的,也就是说,敌手在下面游戏中的优势 $Adv_{\mathcal{A}}^{\text{PUF}}(k_2)$ 是忽略不计的.

(阶段 1).敌手 $\mathcal{A}$ 选择任意的 r_i,能够得到的响应 $PUF(r_i)$.

(挑战).$\mathcal{A}$ 选择在阶段 1 尚未查询的挑战 c.

(阶段 2).允许 $\mathcal{A}$ 向 PUF 查询除挑战 c 以外的其他挑战,并且能够得到阶段 1 中的响应结果.

(响应).$\mathcal{A}$ 最后返回针对 $r=PUF(c)$ 的猜测值 r',如果 $r=r'$,则 $\mathcal{A}$ 获胜.$\mathcal{A}$ 获胜的概率表示为 $Adv_{\mathcal{A}}^{\text{PUF}}(k_2)=Pr[r=r']$.

(2)对同一个挑战 x,两个 PUF_D 输出的最大距离为 t(t 为汉明距离),也就是,存在一个可忽略的 ε_1,使得 $Pr[dist(y,z)>t|x\leftarrow\{0,1\}^{k_1},y\leftarrow PUF_D(x),z\leftarrow PUF_D(x)]\leq\varepsilon_1$.

(3)对同一个挑战 x,来自不同设备 A,B 的两个输出 $PUF_A(x),PUF_B(x)$ 之间的距离至少为 t,也就是存在一个可忽略的 ε_2,使得 $Pr[dist(y,z)<t|x\leftarrow\{0,1\}^{k_1},y\leftarrow PUF_A(x),z\leftarrow PUF_B(x)]\leq\varepsilon_2$.

3.3 网络模型

本文所使用的网络模型是一个典型的雾计算模型(如图 1 所示),它由云层、雾层和物联网设备层组成,其中云层不参与认证.我们的网络模型中主要包括四类实体:注册权威、雾节点、物联网设备和用户.其中注册权威是可信的服务器,它负责以离线的方式安全地为不同的实体注册.其他实体在使用前需要向注册权威进行登记或注册.我们考虑该网络模型中的两种场景,第一个场景是当一个物联网设备接入或者雾节点接入时,雾节点需要与雾节点覆盖下的物联网设备进行相互认证,以便检验双方的合法性,并将物联网设备采集的数据安全传送到雾节点进行临时处理.这是雾计算环境中比较常见的场景,例如,传感器节点采集数据需要安全地传送给附近的网关节点.第二个场景是远程用户需要访问某个雾节点下的物联网设备,这时用户、雾节点和物联网设备之间应进行相互认证,以便验证实体的合法性和数据的真实性.例如,在雾辅助的智能家居应用中,远程用户实时监控自己的智能家居;或者远程的医生直接访问智能家居中传感器采集患者的医疗数据.

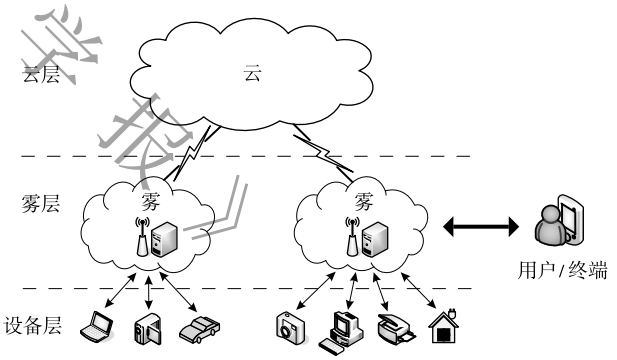


图 1 雾辅助物联网的网络模型

3.4 威胁模型

针对本文使用的网络模型,对敌手的能力作如下假设:

(1)根据 Dolev-Yao 威胁模型[70],我们假设敌手能够完全控制公共通信信道,即敌手能窃听、伪造、重放、延迟和删除消息.

(2)由于物联网设备可能部署在开放环境中,因此我们假设物联网设备不是可信实体,它可能被破坏或受到克隆攻击.

(3)根据雾计算的特征,雾节点可以自由地接入环境中,并且雾节点也可能部署在开放环境中,因

此我们假设雾节点不是完全可信的[41].

(4)用户的移动设备可能被盗或者丢失,因此移动设备也不认为是可信实体.当敌手得到了某个设备,我们假设他会采用某种分析方法(例如功率分析攻击[71-72]、边信道攻击[73])提取存储在被捕获设备中的敏感信息.

(5)我们假设注册权威是完全可信的,它不能被敌手破坏.

(6)在认证协议中,存在两类通信信道,一类是用于实体注册的安全通道;另一类是用于实体之间认证的公共通道.$\mathcal{A}$只能控制在公共信道上传输的消息,但不能截获在安全信道上传输的消息[29].

4　提出的认证协议

在第 4 节我们分别为雾辅助物联网的两个场景提出轻量级安全认证协议.协议一是物联网设备和雾节点之间建立连接的相互认证协议(FD-AKE);协议二则是远程用户通过雾节点访问某个物联网设备的认证协议(UFD-AKE).下面先介绍物联网设备和用户注册过程,然后分别介绍协议 FD-AKE 和协议 UFD-AKE.表 1 列出了提出的协议中所使用的符号和它们的含义.

表 1　符号及其定义

符号	定义
FN_t,S_d	雾节点和物联网设备
U_i,MD_i	用户和用户的移动设备
ID_i,ID_d	用户和物联网设备的身份
PID_i,PID_d	用户和物联网设备的伪身份
TID_i,TID_d	用户和物联网设备的临时身份
Req_i	用户的注册请求
$PUF(\cdot)$	物理不可克隆函数
C,R	PUF 的输入挑战和输出响应
PW_i,α_i	用户的口令和指纹
RA	注册权威
K	注册权威的秘密参数
T_i,ΔT_i	时间戳和最大允许的传输延迟
r_i,n_i	随机数
SK	会话钥
$h(\cdot)$	密码哈希函数
$\|$,$\oplus$	连接符和异或运算

4.1　注　册

注册权威负责安全地为每个物联网设备和用户进行注册.

4.1.1　物联网设备注册

当部署一个新的物联网设备时,它需要由注册权威 RA 进行注册,注册过程如下:

步骤 1. 注册权威 RA 为物联网设备 S_d 选择一个唯一身份 ID_d,产生一个随机挑战 C_d,通过安全信道将(ID_d, C_d)传送给物联网设备.

步骤 2. 物联网设备根据接收到 C_d 后,利用其嵌入的 PUF 计算 C_d 对应的响应 R_d,即 $R_d = PUF_{S_d}(C_d)$,并将通过安全信道传送给注册权威.

步骤 3. 注册权威在接收到 R_d 后,先为物联网设备选择一个临时身份 TID_d,并计算一个伪身份 $PID_d = h(ID_d \| K)$,其中 K 是注册权威的一个秘密参数,并计算 $h(R_d)$.注册权威将物联网设备 S_d 的参数$\{TID_d, PID_d, C_d, h(R_d)\}$通过安全信道传送给其对应的雾节点 FN_t 存储.将$\{TID_d\}$安全地传送给物联网设备.

步骤 4. 物联网设备接收到消息后存储$\{TID_d^{\text{old}} = \text{null}, TID_d^{\text{new}} = TID_i\}$,存储新旧临时身份目的是防止协议不同步或者阻止去同步攻击.

评注 1. 物联网设备注册后,注册权威没有在雾节点中显式地存储 PUF 的 CRPs.这与现有的基于 PUF 认证协议不同,基于 PUF 认证协议常常在验证方或者其他数据库中存储$\{C_d, R_d\}$.但是直接存储 CRPs 可能会招致多种攻击[35,74],攻击者只需较少的 CRPs 就能够取得较好的攻击效果[36].我们在雾节点处存储的是 R_d 的哈希值 $h(R_d)$,攻击者即使捕获了雾节点,也不能根据哈希值 $h(R_d)$ 反向猜出 R_d.假设 R_d 为 128 位随机数,攻击者最优猜测顺序是按照概率降序方式猜测.但是猜测 R_d 每一种可能的 128 位是等概率的,攻击者只能每选择一个 128 位随机数,再计算该随机数的哈希值,并与 $h(R_d)$ 比较以判断是否正确猜出.从文献[75]分析可以看出,8 位随机数的部分猜测熵就能够抵抗人类的猜测.128 位随机数穷举猜测时间大约为 10^{18} 年的数量级.另外,在雾计算环境中,雾节点之间能够以安全方式进行通信[76-77],因而物联网设备的注册信息只需存储在最近的雾节点中.

4.1.2　用户注册

用户通过自己的移动设备 MD_i 进行注册,注册过程如下:

步骤 1. 用户选择一个身份 ID_i,移动设备向注册权威 RA 发送注册请求消息$\{Req_i\}$.

步骤 2. 注册权威在接收到用户的注册请求后,产生一个随机挑战 C_i,并将 C_i 通过安全信道传送给用户.

步骤 3. 用户接收到 C_i 后,利用移动设备嵌入

的 PUF 计算 $R_i=PUF_{U_i}(C_i)$，并将 R_i 通过安全信道传送给注册权威.

步骤 4. 注册权威在接收到用户传送的消息 R_i 后，为用户选择一个临时身份 TID_i，并计算 $h(R_i)$，将 $\{TID_i,C_i,h(R_i)\}$ 传送给雾节点进行存储，并将 $\{TID_i\}$ 通过安全信道传送给用户.

步骤 5. 移动设备接收到消息后，要求用户选择一个口令 PW_i，并在移动设备上按下指纹 α_i，计算 $\beta_i=PUF_{U_i}(\alpha_i)$. 移动设备产生一个随机数 r_i，为用户计算一个伪身份 $PID_i=h(ID_i\|r_i)$. 移动设备利用口令和指纹信息隐藏一些秘密信息：$HPW_i=h(PW_i\|\beta_i\|r_i)$，$Y_i=r_i\oplus h(ID_i\|PW_i\|\beta_i)$，$PID_i^*=PID_i\oplus HPW_i$. 计算一个认证消息 $Auth_i=h(PID_i\|r_i\|HPW_i)$. 最后在移动设备中存储 $\{TID_i^{\text{old}}=\text{null},TID_i^{\text{new}}=TID_i,Y_i,PID_i^*,Auth_i\}$，其中 TID_i^{new} 和 TID_i^{old} 表示用户新旧连续两个临时身份，其目的是防止协议不同步或者阻止去同步攻击. 用户注册过程如图 2 所示.

用户 U_i /移动设备 MD_i	注册权威 RA
步骤 1. 选择身份 ID_i，发送注册请求. $\{Req_i\}$ → (安全信道)	
	步骤 2. 产生 C_i. $\{C_i\}$ ← (安全信道)
步骤 3. 计算 $R_i=PUF_{U_i}(C_i)$. $\{R_i\}$ → (安全信道)	
	步骤 4. 产生 TID_i，计算 $h(R_i)$. 将 $\{TID_i,C_i,h(R_i)\}$ 传给雾节点存储. $\{TID_i\}$ ← (安全信道)
步骤 5. 选择口令 PW_i，按下指纹 α_i，计算 $\beta_i=PUF_{U_i}(\alpha_i)$. 产生随机数 r_i，计算 $PID_i=h(ID_i\|r_i)$， $HPW_i=h(PW_i\|\beta_i\|r_i)$， $Y_i=r_i\oplus h(ID_i\|PW_i\|\beta_i)$， $PID_i^*=PID_i\oplus HPW_i$， $Auth_i=h(PID_i\|r_i\|HPW_i)$. 存储 $\{TID_i^{\text{old}}=\text{null},TID_i^{\text{new}}=TID_i,Y_i,PID_i^*,Auth_i\}$.	

图 2 用户注册过程

用户如果需要更新口令和指纹，只需要在本地进行，更新过程如下：

口令更新步骤 1. 移动设备 MD_i 要求用户 U_i 输入身份 ID_i 和旧口令 PW_i^{old}，并按下旧指纹信息 α_i^{old}.

口令更新步骤 2. MD_i 计算 $\beta_i=PUF_{U_i}(\alpha_i)$，$r_i=Y_i\oplus h(ID_i\|PW_i\|\beta_i)$，$HPW_i=h(PW_i\|\beta_i\|r_i)$，$PID_i=PID_i^*\oplus HPW_i$，计算认证消息 $Auth_i^*=h(PID_i\|r_i\|HPW_i)$，检查 $Auth_i^*$ 是否等于 $Auth_i$，如果相等，则继续，否则终止口令更新请求.

口令更新步骤 3. 当用户选择一个新口令 PW_i^{new}，按下新指纹 α_i^{new} 后，MD_i 计算 $\beta_i^{\text{new}}=PUF_{U_i}(\alpha_i^{\text{new}})$，$HPW_i^{\text{new}}=h(PW_i^{\text{new}}\|\beta_i^{\text{new}}\|r_i)$，$Y_i^{\text{new}}=r_i\oplus h(ID_i\|PW_i^{\text{new}}\|\beta_i^{\text{new}})$，$PID_i^{\text{new}}=PID_i\oplus HPW_i^{\text{new}}$ 和 $Auth_i^{\text{new}}=h(PID_i^{\text{new}}\|r_i\|HPW_i^{\text{new}})$. 最后，移动设备存储更新后的信息 $\{TID_i^{\text{old}}=\text{null},TID_i^{\text{new}}=TID_i,Y_i^{\text{new}},PID_i^{\text{new}},Auth_i^{\text{new}}\}$.

4.2 FD-AKE 协议

物联网设备与雾节点之间执行 FD-AKE 协议，完成相互认证并生成一个共享的会话钥，FD-AKE 协议认证过程如下：

步骤 1. 物联网设备 S_d 产生一个临时交互号 n_1 和当前时间戳 T_1，将 $\{TID_d,n_1,T_1\}$ 传给雾节点 FN_t.

步骤 2. 雾节点接收到消息后，首先检验该消息的新鲜性，也即是判断 $|T_1^*-T_1|\leq\Delta T_1$ 是否成立，其中 T_1^* 是接收消息的时间，ΔT_1 表示物联网设备和雾节点之间最大允许传输延迟. 如果消息是新鲜的，雾节点根据 TID_d 查找对应的 C_d，并产生一个随机新的挑战 C_d^{new}，一个新的临时身份 TID_d^{new} 和一个临时交互号 n_2 和当前时间戳 T_2，计算 $A_1=n_2\oplus h(TID_d\|h(R_d)\|n_1\|T_1\|T_2)$，$A_2=C_d^{\text{new}}\oplus h(R_d)\oplus n_1\oplus n_2\oplus T_2$，$A_3=TID_d^{\text{new}}\oplus h(TID_d\|h(R_d)\|C_d^{\text{new}}\|n_2\|T_2)$，$M_1=h(TID_d^{\text{new}}\|h(R_d)\|n_1\|n_2\|T_2)$. 之后将 $\{A_1,A_2,A_3,M_1,C_d,T_2\}$ 通过开放信道传给物联网设备 S_d.

步骤 3. 物联网设备接收到消息后，检验 $|T_2^*-T_2|\leq\Delta T_1$ 是否成立，其中 T_2^* 是接收消息的时间. 如果成立，物联网设备利用 C_d 计算 PUF 的输出 $R_d=PUF_{S_d}(C_d)$，根据得到的 R_d，物联网设备进一步计算 $n_2=A_1\oplus h(TID_d\|h(R_d)\|n_1\|T_1\|T_2)$，$C_d^{\text{new}}=A_2\oplus h(R_d)\oplus n_1\oplus n_2\oplus T_2$，$TID_d^{\text{new}}=A_3\oplus h(TID_d\|h(R_d)\|C_d^{\text{new}}\|n_2\|T_2)$，最后计算 $M_1^*=h(TID_d^{\text{new}}\|h(R_d)\|n_1\|n_2\|T_2)$，并与接收到的 M_1 进行比较，如果两者相等，表示物联网设备成功认证雾节点. 物联网设备根据新的挑战 C_d^{new} 计算新的响应 R_d^{new}，并存储新的临时身份 TID_d^{new}. 物联网设备产生一个临时交互号 n_3 和当前时间戳 T_3，$A_4=n_3\oplus h(TID_d^{\text{new}}\|C_d^{\text{new}}\|h(R_d)\|n_2\|T_2\|T_3)$，$A_5=n_3\oplus R_d^{\text{new}}$，$M_2=h(TID_d^{\text{new}}\|R_d^{\text{new}}\|n_2\|n_3\|T_3)$，$SK=h(TID_d\|TID_d^{\text{new}}\|R_d^{\text{new}}\|h(R_d)\|n_2\|n_3\|T_3)$. 最后，

物联网设备将$\{A_4, A_5, M_2, T_3\}$传给雾节点.

步骤 4. 雾节点收到消息后，检验$|T_3^* - T_3| \leq \Delta T_1$是否成立，其中$T_3^*$是接收消息的时间. 如果该等式成立，雾节点计算$n_3 = A_4 \oplus h(TID_d^{new} \| C_d^{new} \| h(R_d) \| n_2 \| T_2 \| T_3)$，$R_d^{new} = n_3 \oplus A_5$，$M_2^* = h(TID_d^{new} \| R_d^{new} \| n_2 \| n_3 \| T_3)$，并与接收到的$M_2$进行比较，如果相等，表示雾节点认证了物联网设备，也验证了雾节点与物联网设备之间是同步的. 雾节点随后计算$SK = h(TID_d \| TID_d^{new} \| R_d^{new} \| h(R_d) \| n_2 \| n_3 \| T_3)$，同时为物联网设备存储新旧值$\{TID_d, PID_d, C_d, h(R_d)\}$和$\{TID_d^{new}, PID_d, C_d^{new}, h(R_d^{new})\}$. 图 3 是 FD-AKE 协议简图.

物联网设备 S_d	雾节点 FN_t
步骤 1.	
产生 n_1 和 T_1.	
$\{TID_d, n_1, T_1\}$ →	
（开放信道）	
	步骤 2.
	判断$\|T_1^* - T_1\| \leq \Delta T_1$？
	根据 TID_d 查找 C_d，产生 $C_d^{new}, TID_d^{new}, n_2, T_2$.
	计算
步骤 3.	$A_1 = n_2 \oplus h(TID_d \| h(R_d) \| n_1 \| T_1 \| T_2)$，
判断$\|T_2^* - T_2\| \leq \Delta T_1$？	$A_2 = C_d^{new} \oplus h(R_d) \oplus n_1 \oplus n_2 \oplus T_2$，
计算 $R_d = PUF_{S_d}(C_d)$，	$A_3 = TID_d^{new} \oplus h(TID_d \| h(R_d) \| C_d^{new} \| n_2 \| T_2)$，
$n_2 = A_1 \oplus h(TID_d \| h(R_d) \| n_1 \| T_1 \| T_2)$，	$M_1 = h(TID_d^{new} \| h(R_d) \| n_1 \| n_2 \| T_2)$.
$C_d^{new} = A_2 \oplus h(R_d) \oplus n_1 \oplus n_2 \oplus T_2$，	$\{A_1, A_2, A_3, M_1, C_d, T_2\}$ ←
$TID_d^{new} = A_3 \oplus h(TID_d \| h(R_d) \| C_d^{new} \| n_2 \| T_2)$，	（开放信道）
$M_1^* = h(TID_d^{new} \| h(R_d) \| n_1 \| n_2 \| T_2)$.	
检验 $M_1^* = M_1$？如果相等，则根据 C_d^{new}	步骤 4.
计算 R_d^{new}，存储 TID_d^{new}，产生 n_3 和 T_3，	判断$\|T_3^* - T_3\| \leq \Delta T_1$？
$A_4 = n_3 \oplus h(TID_d^{new} \| C_d^{new} \| h(R_d) \| n_2 \| T_2 \| T_3)$，	计算
$A_5 = n_3 \oplus R_d^{new}$，	$n_3 = A_4 \oplus h(TID_d^{new} \| C_d^{new} \| h(R_d) \| n_2 \| T_2 \| T_3)$，
$M_2 = h(TID_d^{new} \| R_d^{new} \| n_2 \| n_3 \| T_3)$，	$R_d^{new} = n_3 \oplus A_5$，
$SK = h(TID_d \| TID_d^{new} \| R_d^{new} \| h(R_d) \| n_2 \| n_3 \| T_3)$.	$M_2^* = h(TID_d^{new} \| R_d^{new} \| n_2 \| n_3 \| T_3)$，
$\{A_4, A_5, M_2, T_3\}$ →	检验 $M_2^* = M_2$？如果相等，计算
（开放信道）	$SK = h(TID_d \| TID_d^{new} \| R_d^{new} \| h(R_d) \| n_2 \| n_3 \| T_3)$，
	存储新旧值$\{TID_d, PID_d, C_d, h(R_d)\}$和
	$\{TID_d^{new}, PID_d, C_d^{new}, h(R_d^{new})\}$.

图 3　FD-AKE 协议简图

评注 2. 认证协议常常由于某种原因失去同步而不能认证，也就是在雾节点的数据库中找不到物联网设备的临时身份 TID_d. 现有的基于 PUF 认证协议要么没有安全机制抵抗去同步攻击[59]，要么会在注册时额外产生多组 CRPs[78]. 当找不到设备的临时身份时，验证方要求设备选择一组未使用的 CRP 来验证身份. 这种同步方法明显增加了存储和认证的负担. 我们的解决思路是采用认证捎带的方式验证协议的同步性. 例如在 FD-AKE 协议中，认证消息 M_1 和 M_2 中都包含了更新信息 TID_d^{new}，这样在认证过程中也验证了双方是否同步. 另外，双方都存储了新旧两个临时身份，即使攻击者实施了去同步攻击，在下一次认证过程中依然可以在验证方中找到临时身份.

4.3　UFD-AKE 协议

在 UFD-AKE 协议中，远程用户首先在移动设备上登陆，登陆成功后，移动设备与雾节点和物联网设备之间执行相互认证，最后生成一个用于保密它们之间后续通信的会话钥. UFD-AKE 协议过程如下：

步骤 1. 用户在移动设备中输入身份和口令，并在移动设备显示屏上按压指纹. 移动设备计算$\beta_i = PUF_{U_i}(\alpha_i)$，$r_i = Y_i \oplus h(ID_i \| PW_i \| \beta_i)$，计算$HPW_i = h(PW_i \| \beta_i \| r_i)$，$PID_i = PID_i^* \oplus HPW_i$，接着计算认证消息$Auth_i' = h(PID_i \| r_i \| HPW_i)$，与移动设备中存储的$Auth_i$进行比较，如果两者相等，则用户登录成功. 接着移动设备发起认证过程. 移动设备产生一个 n_1 和当前时间戳 T_1，选择一个需要访问的物联网设备 PID_d，将$\{TID_i, PID_d, n_1, T_1\}$传给雾节点.

步骤 2. 雾节点接收到消息后，首先检验$|T_1^*-T_1|\leq\Delta T_1$是否成立，其中$T_1^*$是接收消息的时间，$\Delta T_1$表示用户和雾节点之间最大允许传输延迟. 如果该条件成立，雾节点根据PID_d知道用户要访问的物联网设备S_d，根据PID_d，查找物联网设备存储在雾节点中的信息$\{TID_d,PID_d,C_d,h(h_d)\}$. 雾节点产生一个临时交互号$n_2$和当前时间戳$T_2$，并为物联网设备产生一个随机新的挑战$C_d^{new}$，一个新的临时身份$TID_d^{new}$以及为用户和传感器产生一个共享的会话钥$SK$. 计算$A_1=n_2\oplus h(TID_d\|h(R_d)\|n_1\|T_1\|T_2)$，$A_2=C_d^{new}\oplus h(R_d)\oplus n_1\oplus n_2\oplus T_2$，$A_3=TID_d^{new}\oplus h(TID_d\|h(R_d)\|C_d^{new}\|n_2\|T_2)$，$M_1=h(TID_d^{new}\|h(R_d)\|n_1\|n_2\|T_1\|T_2)$，$SK^*=SK\oplus h(TID_d^{new}\|TID_i\|h(R_d)\|n_2\|T_2)$. 最后雾节点将$\{TID_i,A_1,A_2,A_3,M_1,C_d,T_2,SK^*\}$通过开放信道传给物联网设备$S_d$.

步骤 3. 物联网设备接收到消息后，检验$|T_2^*-T_2|\leq\Delta T_2$是否成立，其中$T_2^*$是接收消息的时间，$\Delta T_2$是物联网设备和雾节点之间最大允许传输延迟. 如果消息新鲜性条件成立，物联网设备利用C_d计算PUF的输出$R_d=PUF_{S_d}(C_d)$，根据得到的R_d，物联网设备进一步计算$n_2=A_1\oplus h(TID_d\|h(R_d)\|n_1\|T_1\|T_2)$，$C_d^{new}=A_2\oplus h(R_d)\oplus n_1\oplus n_2\oplus T_2$，$TID_d^{new}=A_3\oplus h(TID_d\|h(R_d)\|C_d^{new}\|n_2\|T_2)$，最后计算$M_1^*=h(TID_d^{new}\|h(R_d)\|n_1\|n_2\|T_1\|T_2)$，并与接收到的$M_1$进行比较，如果两者相等，表示物联网设备成功认证雾节点. 物联网设备根据新的挑战C_d^{new}计算新的响应$R_d^{new}=PUF_{S_d}(C_d^{new})$，并存储新旧临时身份$TID_d$和$TID_d^{new}$，计算会话钥$SK=SK^*\oplus h(TID_d^{new}\|TID_i\|h(R_d)\|n_2\|T_2)$. 物联网设备产生一个临时交互号$n_3$和当前时间戳$T_3$，计算$A_4=n_3\oplus h(TID_d^{new}\|C_d^{new}\|h(R_d)\|n_2\|T_2\|T_3)$，$A_5=n_3\oplus C_d^{new}\oplus R_d^{new}$，$M_2=h(TID_d^{new}\|R_d^{new}\|TID_i\|n_2\|n_3\|T_3)$. 最后，物联网设备将$\{A_4,A_5,M_2,T_3\}$传给雾节点.

步骤 4. 雾节点收到消息后，检验$|T_3^*-T_3|\leq\Delta T_2$是否成立，其中$T_3^*$是接收消息的时间. 如果该等式成立，雾节点计算$n_3=A_4\oplus h(TID_d^{new}\|C_d^{new}\|h(R_d)\|n_2\|T_2\|T_3)$，$R_d^{new}=n_3\oplus A_5\oplus C_d^{new}$，$M_2^*=h(TID_d^{new}\|R_d^{new}\|TID_i\|n_2\|n_3\|T_3)$，并与接收到的$M_2$进行比较，如果相等，表示雾节点认证了物联网设备，也验证了雾节点与物联网设备之间是同步的. 雾节点随后临时存储物联网设备的新旧值$\{TID_d,PID_d,C_d,h(R_d)\}$和$\{TID_d^{new},PID_d,C_d^{new},h(R_d^{new})\}$. 雾节点产生一个临时交互号$n_4$和当前时间戳$T_4$，并为用户产生一个新的临时身份$TID_i^{new}$和一个新的挑战$C_i^{new}$. 随后计算$A_6=n_4\oplus h(TID_i\|h(R_i)\|n_1\|T_1\|T_4)$，$A_7=C_i^{new}\oplus h(R_i)\oplus n_1\oplus n_4\oplus T_4$，$A_8=TID_i^{new}\oplus h(TID_i\|h(R_i)\|C_i^{new}\|n_4\|T_4)$，$M_3=h(TID_i^{new}\|PID_d\|h(R_i)\|n_1\|n_4\|T_1\|T_4)$，$SK'=SK\oplus h(TID_i^{new}\|PID_d\|h(R_i)\|n_4\|T_4)$. 最后雾节点将$\{A_6,A_7,A_8,M_3,C_i,T_4,SK'\}$通过开放信道传给用户.

步骤 5. 用户接收到消息后，首先检验$|T_4^*-T_4|\leq\Delta T_1$是否成立，其中$T_1^*$是接收消息的时间，$\Delta T_1$表示用户和雾节点之间最大允许传输延迟. 如果该条件成立，用户根据C_i计算PUF的输出$R_i=PUF_{U_i}(C_i)$，$n_4=A_6\oplus h(TID_i\|h(R_i)\|n_1\|T_1\|T_4)$，$C_i^{new}=A_7\oplus h(R_i)\oplus n_1\oplus n_4\oplus T_4$，$TID_i^{new}=A_8\oplus h(TID_i\|h(R_i)\|C_i^{new}\|n_4\|T_4)$，$M_3^*=h(TID_i^{new}\|PID_d\|h(R_i)\|n_1\|n_4\|T_1\|T_4)$，并与接收到的$M_3$进行对比，如果两者相等，则表示用户认证了雾节点. 用户计算会话钥$SK=SK'\oplus h(TID_i^{new}\|PID_d\|h(R_i)\|n_4\|T_4)$，并更新临时身份为$TID_i^{new}$，计算$R_i^{new}=PUF_{U_i}(C_i^{new})$. 用户产生一个临时交互号$n_5$和当前时间戳$T_5$，计算$A_9=n_5\oplus h(TID_i^{new}\|SK\|n_4\|n_5\|T_5)$，$A_{10}=n_5\oplus C_i^{new}\oplus R_i^{new}$，$M_4=h(TID_i^{new}\|TID_d^{new}\|R_i^{new}\|n_4\|n_5\|T_4\|T_5)$，将$\{A_9,A_{10},M_4,T_5\}$传给雾节点.

步骤 6. 雾节点收到消息后，检验$|T_5^*-T_5|\leq\Delta T_1$是否成立，其中$T_4^*$是接收消息的时间. 如果条件成立，雾节点计算$n_5=A_9\oplus h(TID_i^{new}\|SK\|n_4\|n_5\|T_5)$，$R_i^{new}=A_{10}\oplus n_5\oplus C_i^{new}$，$M_4^*=h(TID_i^{new}\|TID_d^{new}\|R_i^{new}\|n_4\|n_5\|T_4\|T_5)$，并与接收到的$M_4$进行比较，如果两者相等，表示雾节点认证了用户，同时表示整个认证过程是同步的. 雾节点最后更新用户和物联网设备所对应的存储信息. 图 4 是 UFD-AKE 协议的认证过程概括.

用户 U_i/ 移动设备 MD_i	雾节点 FN_t	物联网设备 S_d
步骤 1.	步骤 2.	
输入 ID_i，PW_i 和 α_i.	检验 $\lvert T_1^* - T_1 \rvert \le \Delta T_1$？如果成立，	
计算 $\beta_i = PUF_{U_i}(\alpha_i)$，	根据 PID_d 查找 TID_d，PID_d，C_d，$h(R_d)$，	
$r_i = Y_i \oplus h(ID_i \Vert PW_i \Vert \beta_i)$，	产生 n_2，T_2，C_d^{new}，TID_d^{new} 和 SK.	步骤 3.
$HPW_i = h(PW_i \Vert \beta_i \Vert r_i)$，	计算 $A_1 = n_2 \oplus h(TID_d \Vert h(R_d) \Vert n_1 \Vert T_1 \Vert T_2)$，	检验 $\lvert T_2^* - T_2 \rvert \le \Delta T_2$？如果成立，
$PID_i = PID_i^* \oplus HPW_i$，	$A_2 = C_d^{\text{new}} \oplus h(R_d) \oplus n_1 \oplus n_2 \oplus T_2$，	计算 $R_d = PUF_{S_d}(C_d)$，
$Auth_i' = h(PID_i \Vert r_i \Vert HPW_i)$.	$A_3 = TID_d^{\text{new}} \oplus h(TID_d \Vert h(R_d) \Vert C_d^{\text{new}} \Vert n_2 \Vert T_2)$，	$n_2 = A_1 \oplus h(TID_d \Vert h(R_d) \Vert n_1 \Vert T_1 \Vert T_2)$，
检验 $Auth_i' = Auth_i$？，如果相等，	$M_1 = h(TID_d^{\text{new}} \Vert h(R_d) \Vert n_1 \Vert n_2 \Vert T_1 \Vert T_2)$，	$C_d^{\text{new}} = A_2 \oplus h(R_d) \oplus n_1 \oplus n_2 \oplus T_2$，
产生 n_1，T_1，选择 PID_d.	$SK^* = SK \oplus h(TID_d^{\text{new}} \Vert TID_i \Vert h(R_d) \Vert n_2 \Vert T_2)$.	$TID_d^{\text{new}} = A_3 \oplus h(TID_d \Vert h(R_d)$
$\{TID_i, PID_d, n_1, T_1\}$	$\{TID_i, A_1, A_2, A_3, M_1, C_d, T_2, SK^*\}$	$\Vert C_d^{\text{new}} \Vert n_2 \Vert T_2)$，
$\xrightarrow{}$	$\xrightarrow{}$	$M_1^* = h(TID_d^{\text{new}} \Vert h(R_d) \Vert n_1 \Vert n_2 \Vert T_1 \Vert T_2)$.
$(U_i \rightarrow FN_t$，通过开放信道)	$(FN_t \rightarrow S_d$，通过开放信道)	检验 $M_1^* = M_1$？如果成立，
		计算 $R_d^{\text{new}} = PUF_{S_d}(C_d^{\text{new}})$，
	步骤 4.	$SK = SK^* \oplus h(TID_d^{\text{new}} \Vert TID_i \Vert$
	检验 $\lvert T_3^* - T_3 \rvert \le \Delta T_2$？如果成立，	$h(R_d) \Vert n_2 \Vert T_2)$.
	计算	存储新旧临时身份 TID_d 和 TID_d^{new}.
	$n_3 = A_4 \oplus h(TID_d^{\text{new}} \Vert C_d^{\text{new}} \Vert h(R_d) \Vert n_2 \Vert T_2 \Vert T_3)$，	产生 n_3 和 T_3，
步骤 5.	$R_d^{\text{new}} = n_3 \oplus A_5 \oplus C_d^{\text{new}}$，	计算 $A_4 = n_3 \oplus h(TID_d^{\text{new}} \Vert C_d^{\text{new}} \Vert$
检验 $\lvert T_4^* - T_4 \rvert \le \Delta T_2$？如果成立，	$M_2^* = h(TID_d^{\text{new}} \Vert R_d^{\text{new}} \Vert TID_i \Vert n_2 \Vert n_3 \Vert T_3)$，	$h(R_d) \Vert n_2 \Vert T_2 \Vert T_3)$，
计算 $R_i = PUF_{U_i}(C_i)$，	检验 $M_2^* = M_2$？如果成立，	$A_5 = n_3 \oplus C_d^{\text{new}} \oplus R_d^{\text{new}}$，
$n_4 = A_6 \oplus h(TID_i \Vert h(R_i) \Vert n_1 \Vert T_1 \Vert T_4)$，	临时存储新旧值 $\{TID_d, PID_d, C_d, h(R_d)\}$ 和	$M_2 = h(TID_d^{\text{new}} \Vert R_d^{\text{new}} \Vert TID_i \Vert n_2 \Vert n_3 \Vert T_3)$.
$C_i^{\text{new}} = A_7 \oplus h(R_i) \oplus n_1 \oplus n_4 \oplus T_4$，	$\{TID_d^{\text{new}}, PID_d, C_d^{\text{new}}, h(R_d^{\text{new}})\}$.	$\{A_4, A_5, M_2, T_3\}$
$TID_i^{\text{new}} = A_8 \oplus h(TID_i \Vert h(R_i) \Vert$	产生 n_4，T_4，TID_i^{new} 和 C_i^{new}.	$\xleftarrow{}$
$C_i^{\text{new}} \Vert n_4 \Vert T_4)$，	计算	$(FN_t \leftarrow S_d$，通过开放信道)
$M_3^* = h(TID_i^{\text{new}} \Vert PID_d \Vert h(R_i) \Vert$	$A_6 = n_4 \oplus h(TID_i \Vert h(R_i) \Vert n_1 \Vert T_1 \Vert T_4)$，	
$n_1 \Vert n_4 \Vert T_1 \Vert T_4)$.	$A_7 = C_i^{\text{new}} \oplus h(R_i) \oplus n_1 \oplus n_4 \oplus T_4$，	
检验 $M_3^* = M_3$？如果成立，计算	$A_8 = TID_i^{\text{new}} \oplus h(TID_i \Vert h(R_i) \Vert C_i^{\text{new}} \Vert n_4 \Vert T_4)$，	
$SK = SK' \oplus h(TID_i^{\text{new}} \Vert PID_d \Vert$	$M_3 = h(TID_i^{\text{new}} \Vert PID_d \Vert h(R_i) \Vert n_1 \Vert n_4 \Vert T_1 \Vert T_4)$，	
$h(R_i) \Vert n_4 \Vert T_4)$，	$SK' = SK \oplus h(TID_i^{\text{new}} \Vert PID_d \Vert h(R_i) \Vert n_1 \Vert T_4)$.	
更新临时身份 TID_i^{new}，	$\{A_6, A_7, A_8, M_3, C_i, T_4, SK'\}$	
计算 $R_i^{\text{new}} = PUF_{U_i}(C_i^{\text{new}})$.	$\xleftarrow{}$	
产生 n_5 和 T_5，计算	$(U_i \leftarrow FN_t$，通过开放信道)	
$A_9 = n_5 \oplus h(TID_i^{\text{new}} \Vert SK \Vert n_4 \Vert n_5 \Vert T_5)$，	步骤 6.	
$A_{10} = n_5 \oplus C_i^{\text{new}} \oplus R_i^{\text{new}}$，	检验 $\lvert T_5^* - T_5 \rvert \le \Delta T_1$？如果成立，	
$M_4 = h(TID_i^{\text{new}} \Vert TID_d^{\text{new}} \Vert R_i^{\text{new}} \Vert$	计算	
$n_4 \Vert n_5 \Vert T_4 \Vert T_5)$.	$n_5 = A_9 \oplus h(TID_i^{\text{new}} \Vert SK \Vert n_4 \Vert n_5 \Vert T_5)$，	
$\{A_9, A_{10}, M_4, T_5\}$	$R_i^{\text{new}} = A_{10} \oplus n_5 \oplus C_i^{\text{new}}$，	
$\xrightarrow{}$	$M_4^* = h(TID_i^{\text{new}} \Vert TID_d^{\text{new}} \Vert R_i^{\text{new}} \Vert n_4 \Vert n_5 \Vert T_4 \Vert T_5)$，	
$(U_i \rightarrow FN_t$，通过开放信道)	检验 $M_4^* = M_4$？如果成立，表示认证是同步	
	且成功的，存储用户和物联网设备的更新信息.	

图 4　UFD-AKE 协议简图

5　安全性分析

本节我们利用广泛认可的 Real-Or-Random (ROR)[79] 安全模型形式化分析提出的协议的安全性，并用非形式化分析方法表明提出的协议能够抵抗其他的已知攻击.

5.1　ROR 安全模型

ROR 模型中的几个组成部分含义如下：

参与者. 提出的协议中包括用户(U_i)、雾节点(FN_t)和物联网设备(S_d)等三个参与者，每个参与者可以执行多个实例，参与者的实例也称为预言机. 令 $\Pi_{U_i}^u$，$\Pi_{FN_t}^t$ 和 $\Pi_{S_d}^s$ 分别表示 U_i，FN_t 和 S_d 的实例 u，t 和 s.

伙伴关系. 当且仅当下面三个条件同时满身时，两个实例 $\Pi_X^{t_1}$ 和 $\Pi_X^{t_2}$ 被称为伙伴关系：(1) 两实例都进入接受模式；(2) 两实例共享相同的会话标识；(3) 两实例都是彼此的伙伴.

新鲜性. 如果两个参与方的会话钥没有泄漏给攻击者$\mathcal{A}$,那么实例Π_X^t或者Π_Y^t被称之为新鲜的.

敌手. 在ROR模型中,敌手能够完全控制通信信道,并能够对预言机执行下面的查询:

$Execute(\Pi_{U_i}^u,\Pi_{FN_t}^t,\Pi_{S_d}^s)$:该查询模拟被动攻击.敌手$\mathcal{A}$用该查询能够获取协议参与者之间交换的所有消息.

$Send(\Pi_X^t,m)$:该查询模拟主动攻击.执行该查询时,当敌手$\mathcal{A}$向实例Π_X^t发送一个消息m,他能够收到该实例的响应消息.

$CorruptMobileDevice(\Pi_{U_i}^u)$:该查询模拟雾用户的移动设备丢失攻击.使用此查询时,存储在移动设备中的秘密信息将显示给敌手$\mathcal{A}$.

$CorruptIoTDevice(\Pi_{S_d}^s)$:该查询模拟物联网设备被捕获攻击.使用此查询时,敌手$\mathcal{A}$能够提取存储在物联网设备中的秘密信息.

$CorruptFogNode(\Pi_{FN_t}^t)$:该查询模拟雾节点被破坏攻击.当使用此查询时,敌手$\mathcal{A}$能够获取存储在雾节点中的秘密信息.

$Test(\Pi_X^t)$:该模型根据ROR中的不可区分性来模拟会话钥的语义安全性.$Test$查询的输出由一个随机选择的隐藏位b决定.如果实例Π_X^t和它的伙伴没有被接受,$Test$查询返回未定义的符号$\perp$.如果实例Π_X^t的会话钥已经建立并且是新鲜的,那么,当$b=1$,$Test$查询返回真实的会话钥,当$b=0$时,$Test$查询返回与会话钥等长的随机数.

会话钥的语义安全. 根据ROR模型需要敌手$\mathcal{A}$来区分真实的会话钥和等长的随机数.$\mathcal{A}$可以对实例Π_X^t执行多次$Test$查询.在游戏结束时,$\mathcal{A}$猜测$Test$查询中b的值为b',如果$b'=b$,则表明$\mathcal{A}$能够赢得该游戏.用$Succ$表示$\mathcal{A}$赢得游戏的事件,则敌手破坏协议$\mathcal{P}$的优势为$Adv_{\mathcal{P}}^{ake}(\mathcal{A})=|2\cdot Pr[Succ]-1|$.对于任一概率多项式时间攻击者$\mathcal{A}$,如果存在一个可忽略的函数$\varepsilon$,满足$Adv_{\mathcal{P}}^{ake}(\mathcal{A})\leq\varepsilon$,则称协议$\mathcal{P}$在ROR模型下是语义安全的.

随机预言机. 协议中所有的参与者和敌手$\mathcal{A}$都可以访问密码哈希函数$h(\cdot)$和安全的PUF函数$PUF(\cdot)$,这两个函数都用随机预言机模拟.

5.2 形式化安全证明

第5.2节我们将证明提出的两个协议FD-AKE和UFD-AKE的语义安全性.

定理1. 令$\mathcal{P}_1$表示本文提出的FD-AKE协议,$\mathcal{A}$为在ROR模型中破坏协议$\mathcal{P}_1$的概率多项式时间敌手,N为攻击PUF所需要的CRPs的数量,m为PUF输出响应的长度,那么$\mathcal{A}$破坏协议$\mathcal{P}_1$会话钥语义安全的优势为

$$Adv_{\mathcal{P}_1}^{ake}(\mathcal{A})\leq q_h^2/|Hash|+q_p^2/|PUF|+2q_{s_1}/(2^m\cdot N),$$

其中q_{s_1},q_h,q_p,$|Hash|$和$|PUF|$分别表示$Send$查询次数、$Hash$查询次数、PUF查询次数、$h(\cdot)$的范围空间、$PUF(\cdot)$的范围空间.

证明. 本文的证明类似于文献[28,44]中的证明.为证明FD-AKE协议的语义安全性,我们定义一系列游戏$G_i(i=0,1,2,3,4,5)$.令$Succ_i$表示敌手在游戏G_i中猜出隐藏位b的事件.

G_0.该游戏模拟对协议$\mathcal{P}_1$的真实攻击,由于在游戏开始就要求猜测隐藏位b,因此敌手$\mathcal{A}$的优势为

$$Adv_{\mathcal{P}_1}^{ake}(\mathcal{A})=|2\cdot Pr[Succ_0]-1| \tag{1}$$

G_1.该游戏模拟在开放信道上的窃听攻击.在该游戏中,$\mathcal{A}$能执行$Execute(\Pi_{U_i}^u,\Pi_{FN_t}^t,\Pi_{S_d}^s)$查询,获取协议中参与方传输的所有消息,之后,$\mathcal{A}$执行$Test(\Pi_X^t)$查询,以确定$Test$的输出是真实会话钥还是一个随机数.假设已经窃听到所有传输的消息$\{TID_d,n_1,T_1\}$,$\{A_1,A_2,A_3,M_1,C_d,T_2\}$和$\{A_4,A_5,M_2,T_3\}$.在不知道$TID_d^{new}$,$R_d^{new}$,$h(R_d)$,$n_2$和$n_3$的情况下,$\mathcal{A}$是不能计算出会话钥$SK=h(TID_d\|TID_d^{new}\|R_d^{new}\|h(R_d)\|n_2\|n_3\|T_3)$,因此敌手在游戏$G_1$中的优势没有增加,那么我们有

$$Pr[Succ_1]-Pr[Succ_0]=0 \tag{2}$$

G_2.游戏G_2是在游戏G_1基础上增加了$Send$和$Hash$查询.该游戏模拟一个主动攻击.在这种攻击中,敌手$\mathcal{A}$先通过执行$Send$查询欺骗参与者接受伪造的消息,再重复使用$Hash$查询来检查是否发生哈希冲突.由于所有交换的消息都包含了随机数和时间戳,因此$\mathcal{A}$执行$Send$查询时不会发生冲突.根据生日悖论,式(3)成立

$$|Pr[Succ_2]-Pr[Succ_1]|\leq q_h^2/2|Hash| \tag{3}$$

G_3.游戏G_3是在游戏G_2基础上增加了$Send$和PUF查询.由于$h(\cdot)$函数和$PUF(\cdot)$函数都是单向函数,并用随机预言机模拟,因此G_3类似于游戏G_2,我们有:

$$|Pr[Succ_3]-Pr[Succ_2]|\leq q_p^2/2|PUF| \tag{4}$$

G_4.游戏增加了$CorruptIoTDevice(\Pi_{S_d}^s)$查询,模拟物联网设备被捕获攻击.由于物联网设备中只存储了临时身份,敌手不能根据该临时身份计算会话钥.敌手$\mathcal{A}$在游戏G_4中没有增加任何优势,所以

我们有

$$|Pr[Succ_4]-Pr[Succ_3]|=0 \quad (5)$$

G_5. 该游戏增加了 $CorruptFogNode(\Pi^t_{FN_t})$ 查询，它模拟雾节点被破坏攻击. 假设敌手 $\mathcal{A}$ 能够提取雾节点中所有信息 $\{TID_d, PID_d, C_d, h(R_d)\}$，根据这些信息，$\mathcal{A}$ 不能计算出会话钥 $SK=h(TID_d \| TID_d^{new} \| R_d^{new} \| h(R_d) \| n_2 \| n_3 \| T_3)$. $\mathcal{A}$ 可以根据 $h(R_d)$ 来猜测 R_d，以便能够获取足够的 (C_d, R_d) 而实施对 PUF 攻击. 假设有 N 对 CRPs 就能以较高的准确率建模 PUF，R_d 长度为 m 位，猜测 R_d 的概率大约为 $1/2^m$. 那么敌手 $\mathcal{A}$ 在该游戏中的优势增加为

$$|Pr[Succ_5]-Pr[Succ_4]|\leq q_{s_1}/(2^m \cdot N) \quad (6)$$

由于 $\mathcal{A}$ 已经执行了所有的查询，为了能够赢得游戏，他只能调用 $Test$ 查询来确定隐藏位 b，因此有

$$|Pr[Succ_5]|=1/2 \quad (7)$$

根据式(1)～式(7)，可以得到

$$Adv^{ake}_{\mathcal{P}_1}(\mathcal{A})\leq q_h^2/|Hash|+q_p^2/|PUF|+2q_{s_1}/(2^m \cdot N).$$

证毕.

定理 2. 令 $\mathcal{P}_2$ 表示本文提出的 UFD-AKE 协议，$\mathcal{A}$ 为在 ROR 模型中破坏协议 $\mathcal{P}_2$ 的概率多项式时间敌手，N 为攻击 PUF 所需要的 CRPs 的数量，m 为 PUF 输出响应的长度，$\mathcal{D}$ 表示均匀分布口令字典，l 表示指纹的位长，那么 $\mathcal{A}$ 破坏协议 $\mathcal{P}_2$ 会话钥语义安全的优势为

$$Adv^{ake}_{\mathcal{P}_2}(\mathcal{A})\leq q_h^2/|Hash|+q_p^2/|PUF|+2q_{s_1}/(2^m \cdot N)+2q_{s_2}/(2^l \cdot |\mathcal{D}|),$$

其中 $q_{s_1}, q_{s_2}, q_h, q_p, |\mathcal{D}|, |Hash|$ 和 $|PUF|$ 分别表示 $Send$ 查询 PUF 次数、$Send$ 查询口令字典 $\mathcal{D}$ 的次数、$Hash$ 查询次数、PUF 查询次数、$\mathcal{D}$ 的空间大小、$h(\cdot)$ 的范围空间、$PUF(\cdot)$ 的范围空间.

证明. 为证明 UFD-AKE 协议的语义安全性，与定理 1 类似，我们定义一系列游戏 $G_i(i=0,1,2,3,4,5,6)$. 令 $Succ_i$ 表示敌手在游戏 G_i 中猜出隐藏位 b 的事件. 敌手在游戏 G_0～G_5 中的优势与定理 1 一样，只是 $Pr[Succ_5]\neq 1/2$.

G_6. 游戏增加 $CorruptMobileDevice(\Pi^u_{U_i})$ 查询，它模拟移动设备被盗攻击. 敌手使用该查询能够提取存储在移动设备中的秘密信息 $\{TID_i^{old}=\text{null}, TID_i^{new}=TID_i, Y_i, PID_i^*, Auth_i\}$. 由于 $HPW_i=h(PW_i \| \beta_i \| r_i)$，$Y_i=r_i \oplus h(ID_i \| PW_i \| \beta_i)$，$PID_i^*=PID_i \oplus HPW_i$，$Auth_i=h(PID_i \| r_i \| HPW_i)$，$\mathcal{A}$ 必须同时猜出用户的口令和指纹. 敌手猜出位长为 l 的指纹概率大约为 $1/2^l$，因此，敌手在游戏 G_6 中的优势增加为

$$|Pr[Succ_6]-Pr[Succ_5]|\leq q_{s_2}/(2^l \cdot |\mathcal{D}|) \quad (8)$$

在最后的游戏 G_6 中，显然有

$$|Pr[Succ_6]|=1/2 \quad (9)$$

根据式(1)～式(9)，可以得到：

$$Adv^{ake}_{\mathcal{P}_2}(\mathcal{A})\leq q_h^2/|Hash|+q_p^2/|PUF|+2q_{s_1}/(2^m \cdot N)+2q_{s_2}/(2^l \cdot |\mathcal{D}|).$$ 证毕.

5.3 非形式化安全分析

一些学者认为同时使用形式化安全分析方法和非形式化安全分析方法更能刻画认证协议的安全特性[80-81]，为此，在本节中，我们将用非形式化安全分析方法来评估 FD-AKE 协议和 UFD-AKE 协议取得的其他安全属性. 括号内表示该安全属性是该协议所具有的.

5.3.1 匿名和不可跟踪性(FD-AKE 协议和 UFD-AKE 协议)

两个协议中所有参与实体都具有匿名性和不可跟踪性. 两个协议中所有实体的真实身份没有以明文的形式传输，敌手不能通过窃听传输的消息来获取实体的身份信息，因此两个协议都具有匿名性. 另外，两个协议中实体的临时身份在每次会话后都会更新，每次交换的消息中都包含临时交互号和时间戳，也就是说每次会话时协议所交换的消息是不同的，因此，两个协议具有不可跟踪性.

5.3.2 密钥前向/后向保密(FD-AKE 协议和 UFD-AKE 协议)

在 FD-AKE 协议中会话钥为 $SK=h(TID_d \| TID_d^{new} \| R_d^{new} \| h(R_d) \| n_2 \| n_3 \| T_3)$，它包含了临时身份、临时交互号和时间戳等信息，这些信息是动态的，每次会话都不同，因此敌手在知道当前会话钥情况下是不能猜测以前或以后建立的会话钥. 在 UFD-AKE 协议中，会话钥是由雾节点随机生成的，每次会话随机生成的会话钥不同，因此，UFD-AKE 协议也具有密钥的前向和后向保密性.

5.3.3 物联网设备假冒攻击(FD-AKE 协议和 UFD-AKE 协议)

在 FD-AKE 协议中，敌手要假冒物联网设备，他必须构造有效的消息 $\{A_4, A_5, M_2, T_3\}$. 敌手可以产生临时交互号 n_3 和时间戳 T_3，但是没有其他信息，敌手不能计算 $A_4=n_3 \oplus h(TID_d^{new} \| C_d^{new} \| h(R_d) \| n_2 \| T_2 \| T_3)$，$A_5=n_3 \oplus R_d^{new}$，$M_2=h(TID_d^{new} \| R_d^{new} \| n_2 \| n_3 \| T_3)$，因此在 FD-AKE 协议假冒物联网设备

攻击是不成立的.同样在 UFD-AKE 协议的步骤 3 中,敌手要假冒物联网设备也必须构造有效的消息 $\{A_4, A_5, M_2, T_3\}$,这显然也是不成立的.

5.3.4 雾节点假冒攻击(FD-AKE 协议和 UFD-AKE 协议)

在 FD-AKE 协议的步骤 2 中,敌手要假冒雾节点,他必须构建有效的消息 $\{A_1, A_2, A_3, M_1, C_d, T_2\}$.敌手只能产生一个临时交互号 n_2 和当前时间戳 T_2,显然根据 n_2 和 T_2 是无法构造有效的消息.同样在 UFD-AKE 协议中要实施雾节点假冒攻击,敌手必须构造 UFD-AKE 协议步骤 2 中的消息 $\{TID_i, A_1, A_2, A_3, M_1, C_d, T_2, SK^*\}$ 或步骤 4 中的消息 $\{A_6, A_7, A_8, M_3, C_i, T_4, SK'\}$.在不知道一些秘密参数情况下,雾节点传输的两个消息都不能有效构建.

5.3.5 用户假冒攻击(UFD-AKE 协议)

在 UFD-AKE 协议的登陆过程中,敌手需获取用户的口令、指纹和移动设备的 PUF 才能通过登陆,显然敌手不可能知道这些信息和物理设备.所以,敌手在登陆过程中不能实施假冒用户攻击.在认证过程中,敌手只有有效构建步骤 5 中的消息 $\{A_9, M_4, T_5\}$ 才能假冒成功,由于该消息中包含许多秘密参数,所以敌手不能实施假冒用户攻击.

5.3.6 重放攻击(FD-AKE 协议和 UFD-AKE 协议)

假设敌手通过窃听方式获取两个协议中已经传输的消息,由于每个消息中包含了临时交互号和时间戳,每次会话中的临时交互号和时间戳都不同,这些临时交互号和时间戳只对某一次回话有效,因此,提出的两个协议都能抵抗重放攻击.

5.3.7 移动设备丢失/被盗攻击(UFD-AKE 协议)

假设敌手偷盗了移动设备,并提取了存储在移动设备中的信息 $\{TID_i^{\text{old}} = \text{null}, TID_i^{\text{new}} = TID_i, Y_i, PID_i^*, Auth_i\}$,其中 $\beta_i = PUF_{U_i}(\alpha_i)$,$HPW_i = h(PW_i \| \beta_i \| r_i)$,$Y_i = r_i \oplus h(ID_i \| PW_i \| \beta_i)$,$PID_i^* = PID_i \oplus HPW_i$,$Auth_i = h(PID_i \| r_i \| HPW_i)$.要计算上面的式子,敌手必须同时知道口令 PW_i 和用户的指纹 α_i,显然这不可能完成.因此,UFD-AKE 协议能够抵抗移动设备丢失/被盗攻击.

5.3.8 物联网设备被捕获攻击(FD-AKE 协议和 UFD-AKE 协议)

当物联网设备被捕获后,敌手能够提取存储在其中的所有信息.在两个协议中,物联网设备只存储了临时身份,敌手根据物联网设备的临时身份无法计算出会话钥.

5.3.9 雾节点被破坏攻击(FD-AKE 协议和 UFD-AKE 协议)

假设敌手 $\mathcal{A}$ 破坏了雾节点,他能够提取存储在雾节点中的信息.雾节点中存储了 $\{TID_d, PID_d, C_d, h(R_d)\}$ 和 $\{TID_i, C_i, h(R_i)\}$.首先,敌手根据这些信息无法计算两个协议的会话钥.其次,如果敌手打算通过获取多个 CRPs 来对 PUF 执行攻击,但敌手不能根据哈希值 $h(R)$ 反向计算 R,因此,两个协议都能抵抗雾节点被破坏攻击.

5.3.10 中间人攻击(FD-AKE 协议和 UFD-AKE 协议)

假设敌手截获了协议中所有传输的消息,为了发起中间人攻击,敌手必须修改截获的消息,目的让对方相信篡改的消息是真实的.在 FD-AKE 协议中,在不知道 $h(R_d)$、n_2、TID_d^{new} 等情况下,敌手修改 $\{A_1, A_2, A_3, M_1, C_d, T_2\}$ 或者 $\{A_4, A_5, M_2, T_3\}$ 是不可行的.同样在 UFD-AKE 协议中,敌手在不知道秘密参数情况下也无法修改传输中的消息.因此,两个协议都能抵抗中间人攻击.

5.3.11 特权内幕攻击(UFD-AKE 协议)

假设一个特权内幕的攻击者知道用户注册时传给注册权威的消息 $\{Req_i\}$ 和 $\{R_i\}$,由于 R_i 是 PUF 相关的,敌手不能计算出对应的挑战 C_i,也无法根据这些信息计算会话钥.即使敌手还盗取了移动设备,能够提取移动设备中存储的信息 $\{TID_i^{\text{old}} = \text{null}, TID_i^{\text{new}} = TID_i, Y_i, PID_i^*, Auth_i\}$,如果不知道 PW_i、PID_i、α_i 等信息,敌手也不能成功登录移动设备,也不能计算出会话钥.

5.3.12 去同步攻击(FD-AKE 协议和 UFD-AKE 协议)

FD-AKE 协议和 UFD-AKE 协议都采用捎带同步验证方式来检查协议是否失去同步,也就是在认证消息中包含双方更新的信息,如 TID_d^{new}、C_d^{new}、TID_i^{new} 等,如果协议失去同步,协议也无法认证成功.另外,每个实体中都存储了新旧两个临时身份,当敌手实施去同步攻击时,阻止协议的某个临时身份更新不一致,但总存在一个临时身份是一致的,因此,提出的两个协议都能抵抗去同步攻击.

6 性能分析

在第 6 节我们对比提出的协议与 Guo 等人[41]、

Naoui 等人[54]、Gupta 等人[82]、Wazid 等人[68]和 Jiang 等人[83]的相关协议的安全属性、通信代价和计算代价.

6.1　安全属性

表 2 显示了几个认证协议所具有的安全属性. 在这些协议中，FD-AKE 协议只实现了物联网设备与雾节点之间的相互认证，其余协议实现了用户、雾节点(或者网关)和物联网设备之间的相互认证. 所以与用户相关的安全属性在 FD-AKE 协议中都不适用. 值得注意的是，只有 Guo 等人协议[41]、FD-AKE 协议和 UFD-AKE 协议能够抵抗雾节点(或者网关)被破坏攻击. 另外，Naoui 等人[54]的协议还不支持匿名性和不可跟踪性，并且不能抵抗移动设备被盗攻击、物联网设备被捕攻击、网关假冒攻击和去同步攻击. Gupta 等人[82]的协议不能抵抗离线口令猜测攻击，也存在用户假冒、物联网设备假冒和网关假冒攻击. Wazid 等人[68]的协议在物联网设备被捕和去同步攻击下是不安全的. Jiang 等人[83]的协议不能抵抗物联网设备被捕攻击，也不能抵抗网关被破坏攻击. 与其他相关协议对比，UFD-AKE 协议则实现了更多的安全属性，能够抵抗各种已知攻击.

表 2　安全属性对比

安全属性	文献[41]	文献[54]	文献[82]	文献[68]	文献[83]	FD-AKE	UFD-AKE
F_1	√	√	×	√	√	N/A	√
F_2	√	×	√	√	√	N/A	√
F_3	√	×	√	×	×	√	√
F_4	√	×	×	×	×	√	√
F_5	√	√	√	√	√	N/A	√
F_6	√	√	√	√	√	√	√
F_7	√	√	×	√	√	N/A	√
F_8	√	√	×	√	√	√	√
F_9	√	×	×	√	√	√	√
F_{10}	√	×	√	√	√	√	√
F_{11}	√	×	√	√	√	√	√
F_{12}	√	√	√	√	√	√	√
F_{13}	√	√	√	√	√	√	√
F_{14}	√	×	√	×	√	√	√
F_{15}	√	√	√	√	√	√	√
F_{16}	√	√	√	√	√	√	√

注：F_1：离线口令猜测攻击；F_2：移动设备被盗攻击；F_3：物联网设备被捕攻击；F_4：雾节点或者网关被破坏攻击；F_5：特权内幕攻击；F_6：重放攻击；F_7：用户假冒攻击；F_8：物联网设备假冒攻击；F_9：雾节点或网关假冒攻击；F_{10}：匿名；F_{11}：不可跟踪性；F_{12}：中间人攻击；F_{13}：相互认证；F_{14}：去同步攻击；F_{15}：密钥协商；F_{16}：密钥前向/后向保密；√：表示支持该属性；×：表示不支持该属性；N/A：不适用.

6.2　通信代价

我们用协议中所有交换消息的总位数来表示通信代价. 假设身份、伪身份、临时身份、临时交互号、会话钥、PUF 的挑战和响应的长度都是 128 bits，时间戳是 32 bits，哈希摘要(使用 SHA-256 哈希算法)和 MAC 长度是 256 bits，对称加密/解密块大小为 128 bits，群上的点长为 1024 bits. 各个协议的通信代价对比如表 3 所示. Guo 等人[41]的协议中交换了三个消息，其长度分别是 1184 bits、1312 bits 和 800 bits，总通信代价为 (1184 + 1312 + 800) = 3296 bits. Naoui 等人协议[54]、Gupta 等人协议[82]、Wazid 等人协议[68]和 Jiang 等人协议[83]的总通信代价分别是(1824 + 288 + 544) = 2656 bits，(1536 + 384 + 384 + 384) = 2688 bits，(672 + 1056 + 768 + 1344) = 3840 bits 和(1568 + 1056 + 672 + 1376) = 4672 bits. 在 FD-AKE 协议中，需要交换的消息分别是 $\{TID_d, n_1, T_1\}$，$\{A_1, A_2, A_3, M_1, C_d, T_2\}$，$\{A_4, A_5, M_2, T_3\}$，它们的位长分别是 (128 + 128 + 32) = 288 bits，(256 + 256 + 256 + 256 + 128 + 32) = 1184 bits 和 (256 + 256 + 256 + 32) = 800 bits，因此 FD-AKE 协议的总通信代价为 2272 bits. UFD-AKE 协议需要交换 5 个消息，其总通信代价为(416 + 1440 + 800 + 1312 + 544) = 4512 bits.

表 3　通信代价比较

协议	总消息数	总通信代价/bits
文献[41]	3	3296
文献[54]	3	2656
文献[82]	4	2688
文献[68]	4	3840
文献[83]	4	4672
FD-AKE	3	2272
UFD-AKE	5	4512

6.3　计算代价

我们用协议中所有参与方执行密码原语的总操作时间来评估计算代价. 令 T_h，T_e，T_p，T_{epm}，T_{mac}，T_{hmac} 和 T_{puf} 分别表示哈希函数、对称密码加密或者解密、对称多项式、ECC 点乘、MAC、哈希 MAC 和 PUF 的运算时间. 我们使用已有的测试结果[41,44,49,84]，并且 $T_h \approx T_{mac} \approx T_{hmac}$，这些密码原语近似操作时间如表 4 所示.

表 4　密码原语近似运行时间　(单位：ms)

设备	T_h	T_e	T_p	T_{epm}	T_{puf}
移动设备(MD)	0.067	0.085	1.072	13.56	0.023
物联网设备(S)	1.420	2.180	7.720	21.82	0.023
雾节点(FN)	0.037	0.055	0.592	8.77	N/A

在 Guo 等人[41]的协议中，移动设备的执行时间为 $2T_p + 8T_h \approx 2.68$ ms，物联网设备的执行时间是 $2T_p + 9T_h \approx 28.22$ ms，雾节点的执行时间是 $3T_p +$

$10T_h \approx 2.146$ ms，总计算代价大约为 33.046 ms. 在 Naoui 等人[54]的协议中，移动设备的执行时间是 $10T_h + 3T_e + 2T_{hmac} + 2T_{epm} \approx 28.179$ ms，物联网设备的执行时间是 $1T_h + 1T_e \approx 3.6$ ms，网关的执行时间是 $11T_h + 4T_e + 2T_{hmac} + 2T_{epm} \approx 18.241$ ms，总计算代价为 50.02 ms. Gupta 等人[82]的协议中，移动设备、物联网设备和网关的执行时间分别是 $2T_{epm} + 3T_h \approx 27.321$ ms，$3T_h \approx 4.26$ ms，$1T_{epm} + 7T_h \approx 9.029$ ms，总计算代价为 40.61 ms. Wazid 等人[68]协议的总计算代价是 $(0.353 + 10.7 + 0.443) = 11.496$ ms. Jiang 等人[83]的协议中，移动设备、传感器节点和数据中心的执行时间分别是 $T_{puf} + 13T_h + 2T_{epm} + T_e \approx 28.099$ ms，$T_{puf} + 12T_h + T_{epm} \approx 38.883$ ms，$T_{epm} + 19T_h \approx 9.473$ ms，总计算代价为 76.455 ms. 在 FD-AKE 协议中，物联网设备的执行时间是 $7T_h + 2T_{puf} \approx 9.986$ ms，雾节点的执行时间是 $7T_h \approx 0.259$ ms，总计算代价大约为 10.245 ms. 在 UFD-AKE 协议中，移动设备的执行时间为 $7T_h + 2T_{puf} \approx 0.515$ ms，物联网设备的执行时间是 $6T_h + 2T_{puf} \approx 8.566$ ms，雾节点的执行时间是 $13T_h \approx 0.481$ ms，总计算代价大约为 9.562 ms. 几个协议的计算代价归纳如表 5 所示.

表 5 计算代价对比

协议	MD/ms	S/ms	(FN/G)/ms	总代价/ms
文献[41]	$2T_p + 8T_h \approx 2.68$	$2T_p + 9T_h \approx 28.22$	$3T_p + 10T_h \approx 2.146$	33.046
文献[54]	$10T_h + 3T_e + 2T_{hmac} + 2T_{epm} \approx 28.179$	$1T_h + 1T_e \approx 3.6$	$11T_h + 4T_e + 2T_{hmac} + 2T_{epm} \approx 18.241$	50.020
文献[82]	$2T_{epm} + 3T_h \approx 27.321$	$3T_h \approx 4.26$	$1T_{epm} + 7T_h \approx 9.029$	40.610
文献[68]	$4T_h + 1T_e \approx 0.353$	$6T_h + 1T_e \approx 10.7$	$9T_h + 2T_e \approx 0.443$	11.496
文献[83]	$T_{puf} + 13T_h + 2T_{epm} + T_e \approx 28.099$	$T_{puf} + 12T_h + T_{epm} \approx 38.883$	$T_{epm} + 19T_h \approx 9.473$	76.455
FD-AKE	—	$7T_h + 2T_{puf} \approx 9.986$	$7T_h \approx 0.259$	10.245
UFD-AKE	$7T_h + 2T_{puf} \approx 0.515$	$6T_h + 2T_{puf} \approx 8.566$	$13T_h \approx 0.481$	9.562

7 结 论

在本论文中，我们为雾辅助物联网两个场景提出了认证协议，其中 FD-AKE 协议实现了物联网设备和雾节点之间的相互认证；UFD-AKE 协议则在用户、雾节点和物联网设备之间实现了相互认证. 提出的两个协议都与雾计算的特征相符合，特别是当雾节点被破坏时，协议中的敏感信息也不会泄漏. 另外，两个协议采用验证方无显式存储 CRPs 和捎带同步验证方式，因此具有较高的安全性和较好的效率. 我们使用 ROR 安全模型证明了提出的两个协议是安全的，并且分析了提出的协议能够抵抗各种已知的攻击. 最后，我们与相关研究进行对比分析，结果显示提出的协议能支持更多的安全属性，也具有较低的通信代价和计算代价，比较适合应用在雾辅助的物联网环境中.

参 考 文 献

[1] Roman R, López J, Mambo M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 2018, 78: 680-698

[2] Ni J, Zhang K, Lin X, et al. Securing fog computing for Internet of Things applications: Challenges and solutions. IEEE Communications Surveys and Tutorials, 2018, 20(1): 601-628

[3] Bonomi F, Milito R A, Zhu J, et al. Fog computing and its role in the Internet of Things//Proceedings of the 1st Edition of the MCC Workshop on Mobile Cloud Computing. Helsinki, Finland, 2012: 13-16

[4] Zhou Yue-Zhi, Zhang Di. Near-end cloud computing: Opportunities and challenges in the post-cloud computing era. Chinese Journal of Computers, 2019, 42(4): 677-700 (in Chinese)
(周悦芝，张迪. 近端云计算：后云计算时代的机遇与挑战. 计算机学报，2019，42(4)：677-700)

[5] González L M V, Rodero-Merino L. Finding your way in the fog: Towards a comprehensive definition of fog computing. Computer Communication Review, 2014, 44(5): 27-32

[6] Bonomi F, Milito R A, Natarajan P, et al. Fog computing: A platform for Internet of Things and analytics//Bessis N, Dobre C ed. Big Data and Internet of Things: A Roadmap for Smart Environments. Switzerland: Springer, 2014: 169-186

[7] Yi S, Hao Z, Qin Z, et al. Fog computing: Platform and applications//Proceedings of the 3rd IEEE Workshop on Hot Topics in Web Systems and Technologies. Washington, USA, 2015: 73-78

[8] Stojmenovic I, Wen S. The fog computing paradigm: Scenarios and security issues//Proceedings of the 2014 Federated Conference on Computer Science and Information Systems. Warsaw, Poland, 2014, 2: 1-8

[9] Mukherjee M, Shu L, Wang D. Survey of fog computing:

Fundamental, network applications, and research challenges. IEEE Communications Surveys and Tutorials, 2018, 20(3): 1826-1857

[10] Sarkar S, Misra S. Theoretical modelling of fog computing: A green computing paradigm to support IoT applications. IET Networks, 2016, 5(2): 23-29

[11] Hu P, Dhelim S, Ning H, et al. Survey on fog computing: Architecture, key technologies, applications and open issues. Journal of Network and Computer Applications, 2017, 98: 27-42

[12] Mutlag A A, Abd Ghani M K, Arunkumar N, et al. Enabling technologies for fog computing in healthcare IoT systems. Future Generation Computer Systems, 2019, 90: 62-78

[13] Li J, Jin J, Yuan D, et al. EHOPES: Data-centered fog platform for smart living//Proceedings of the International Telecommunication Networks and Applications Conference. Sydney, Australia, 2015: 308-313

[14] Verma P, Sood S K. Fog assisted-IoT enabled patient health monitoring in smart homes. IEEE Internet of Things Journal, 2018, 5(3): 1789-1796

[15] Rahimi M, Songhorabadi M, Kashani M H. Fog-based smart homes: A systematic review. Journal of Network and Computer Applications, 2020, 153: 102531

[16] Stantchev V, Barnawi A, Ghulam S, et al. Smart items, fog and cloud computing as enablers of servitization in healthcare. Sensors & Transducers, 2015, 185(2): 121-128

[17] Farahani B, Firouzi F, Chang V I, et al. Towards fog-driven IoT ehealth: Promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems, 2018, 78: 659-676

[18] Cao Y, Chen S, Hou P, et al. FAST: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation//Proceedings of the 10th IEEE International Conference on Networking. Boston, USA, 2015: 2-11

[19] Silva B N, Khan M, Han K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable Cities and Society, 2018, 38: 697-713

[20] Tang B, Chen Z, Hefferman G, et al. Incorporating intelligence in fog computing for big data analysis in smart cities. IEEE Transactions on Industrial Informatics, 2017, 13(5): 2140-2150

[21] Gharaibeh A, Salahuddin M A, Hussini S J, et al. Smart cities: A survey on data management, security, and enabling technologies. IEEE Communications Surveys and Tutorials, 2017, 19(4): 2456-2501

[22] He J, Wei J, Chen K, et al. Multitier fog computing with large-scale IoT data analytics for smart cities. IEEE Internet of Things Journal, 2018, 5(2): 677-686

[23] Kang J, Yu R, Huang X, et al. Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(8): 2627-2637

[24] Zhang W, Zhang Z, Chao H. Cooperative fog computing for dealing with big data in the internet of vehicles: Architecture and hierarchical resource management. IEEE Communications Magazine, 2017, 55(12): 60-67

[25] Wang X, Ning Z, Wang L. Offloading in internet of vehicles: A fog-enabled real-time traffic management system. IEEE Communications Society Magazine, 2018, 14(10): 4568-4578

[26] Huang C, Lu R, Choo K R. Vehicular fog computing: Architecture, use case, and security and forensic challenges. IEEE Communications Magazine, 2017, 55(11): 105-111

[27] Masud M, Alazab M, Choudhary K, et al. 3P-SAKE: Privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks. Computer Communications, 2021, 175: 82-90

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

[29] Wu F, Li X, Sangaiah A K, et al. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems, 2018, 82: 727-737

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

[31] Srinivas J, Das A K, Kumar N, et al. Cloud centric authentication for wearable healthcare monitoring system. IEEE Transactions on Dependable and Secure Computing, 2020, 17(5): 942-956

[32] Wang Liang-Min, Jiang Shun-Rong, Guo Yuan-Bo. Composable-secure authentication protocol for mobile Sensors roaming in the Internet of Things. Scientia Sinica Informationis, 2012, 42(7): 815-830(in Chinese)
(王良民，姜顺荣，郭渊博. 物联网中移动 Sensor 节点漫游的组合安全认证协议. 中国科学：信息科学，2012，42(7)：815-830)

[33] Delvaux J, Gu D, Schellekens D, et al. Secure lightweight entity authentication with strong PUFs: Mission impossible?//Proceedings of the Cryptographic Hardware and Embedded Systems. Busan. South Korea, 2014: 451-475

[34] Rührmair U, Sölter J, Sehnke F, et al. PUF modeling attacks on simulated and silicon data. IEEE Transactions on Information Forensics and Security, 2013, 8(11): 1876-1891

[35] Sahoo D P, Nguyen P H, Mukhopadhyay D, et al. A case of lightweight PUF constructions: Cryptanalysis and machine learning attacks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34(8): 1334-1343

[36] Liu Y, Xie Y, Bao C, et al. A combined optimization-theoretic and side-channel approach for attacking strong physical unclonable functions. IEEE Transactions on Very Large Scale Integration Systems, 2018, 26(1): 73-81

[37] Chatterjee U, Govindan V, Sadhukhan R, et al. Building PUF based authentication and key exchange protocol for IoT

without explicit CRPs in verifier database. IEEE Transactions on Dependable and Secure Computing, 2019, 16(3): 424-437

[38] Ibrahim M H. Octopus: An edge-fog mutual authentication scheme. International Journal of Network Security, 2016, 18(6): 1089-1101

[39] Wazid M, Das A K, Kumar N, et al. Design of secure key management and user authentication scheme for fog computing services. Future Generation Computer Systems, 2019, 91: 475-492

[40] Jia X, He D, Kumar N, et al. Authenticated key agreement scheme for fog-driven IoT healthcare system. Wireless Networks, 2019, 25(8): 4737-4750

[41] Guo Y, Zhang Z, Guo Y. Fog-centric authenticated key agreement scheme without trusted parties. IEEE Systems Journal, 2021, 15(4): 5057-5066

[42] Wu F, Li X, Xu L, et al. A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server. Computers and Electrical Engineering, 2017, 63: 168-181

[43] Jiang Q, Zhang N, Ni J, et al. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. IEEE Transactions on Vehicular Technology, 2020, 69(9): 9390-9401

[44] Guo Y, Zhang Z, Guo Y. Anonymous authenticated key agreement and group proof protocol for wearable computing. IEEE Transactions on Mobile Computing, 2021, DOI: 10.1109/TMC.2020.3048703

[45] Wazid M, Das A K, Odelu V, et al. Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet of Things Journal, 2018, 5(1): 269-282

[46] Darbandeh F G, Safkhani M. A new lightweight user authentication and key agreement scheme for WSN. Wireless Personal Communications, 2020, 114(4): 3247-3269

[47] Ali R, Pal A K, Kumari S, et al. An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring. Journal of Ambient Intelligence and Humanized Computing, 2018, DOI: 10.1007/s12652-018-1015-9

[48] Sureshkumar V, Amin R, Vijaykumar V R, et al. Robust secure communication protocol for smart healthcare system with FPGA implementation. Future Generation Computer Systems, 2019, 100: 938-951

[49] Poh G S, Gope P, Ning J. PrivHome: Privacy-preserving authenticated communication in smart home environment. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1095-1107

[50] Chatterjee K. An improved authentication protocol for wireless body sensor networks applied in healthcare applications. Wireless Personal Communications, 2020, 111(4): 2605-2623

[51] Odelu V, Saha S, Prasath R, et al. Efficient privacy preserving device authentication in WBANs for industrial e-health applications. Computers & Security, 2019, 83: 300-312

[52] Xie Q, Hwang L. Security enhancement of an anonymous roaming authentication scheme with two-factor security in smart city. Neurocomputing, 2019, 347: 131-138

[53] Hammi B, Fayad A, Khatoun R, et al. A lightweight ECC-based authentication scheme for Internet of Things (IoT). IEEE Systems Journal, 2020, 14(3): 3440-3450

[54] Naoui S, Elhdhili M E, Saïdane L A. Lightweight and secure password based smart home authentication protocol: LSP-SHAP. Journal of Network and Systems Management, 2019, 27(4): 1020-1042

[55] Shuai M, Yu N, Wang H, et al. Anonymous authentication scheme for smart home environment with provable security. Computers & Security, 2019, 86: 132-146

[56] Li X, Sangaiah A K, Kumari S, et al. An efficient authentication and key agreement scheme with user anonymity for roaming service in smart city. Personal and Ubiquitous Computing, 2017, 21(5): 791-805

[57] Gope P. LAAP: Lightweight anonymous authentication protocol for D2D-aided fog computing paradigm. Computers & Security, 2019, 86: 223-237

[58] Frikken K B, Blanton M, Atallah M J. Robust authentication using physically unclonable functions//Proceedings of the International Conference on Information Security. 2009: 262-277

[59] Aman M N, Chua K C, Sikdar B. Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet of Things Journal, 2017, 4(5): 1327-1340

[60] Bansal G, Naren N, Chamola V, et al. Lightweight mutual authentication protocol for V2G using physical unclonable function. IEEE Transactions on Vehicular Technology, 2020, 69(7): 7234-7246

[61] Kaveh M, Mosavi M R. A lightweight mutual authentication for smart grid neighborhood area network communications based on physically unclonable function. IEEE Systems Journal, 2020, 14(3): 4535-4544

[62] Patil A S, Hamza R, Hassan A, et al. Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. Computers & Security, 2020, 97: 101958

[63] Aman M N, Javaid U, Sikdar B. A privacy-preserving and scalable authentication protocol for the internet of vehicles. IEEE Internet of Things Journal, 2021, 8(2): 1123-1139

[64] Liang W, Xie S, Long J, et al. A double PUF-based RFID identity authentication protocol in service-centric Internet of Things environments. Information Sciences, 2019, 503: 129-147

[65] Zhu F, Li P, Xu H, et al. A lightweight RFID mutual authentication protocol with PUF. Sensors, 2019, 19(13): 2957

[66] Barbareschi M, Benedictis A D, Montagna E L, et al. A PUF-based mutual authentication scheme for cloud-edges IoT systems. Future Generation Computer Systems, 2019, 101: 246-261

[67] Sarkar P. A simple and generic construction of authenticated encryption with associated data. ACM Transactions on Privacy and Security, 2010, 13(4): 33:1-33:16

[68] Wazid M, Das A K, Odelu V, et al. Secure remote user authenticated key establishment protocol for smart home environment. IEEE Transactions on Dependable and Secure Computing, 2020, 17(2): 391-406

[69] Byun J W, Jeong I R. Comments on physically unclonable function based two-factor authentication protocols. Wireless Personal Communications, 2019, 106(3): 1243-1252

[70] Dolev D, Yao A C. On the security of public key protocols. IEEE Transactions on Information Theory, 1983, 29(2): 198-207

[71] Kocher P C, Jaffe J, Jun B. Differential power analysis// Proceedings of the 19th Annual International Cryptology Conference. Santa Barbara, USA, 1999: 388-397

[72] Messerges T S, Dabbish E A, Sloan R H. Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers, 2002, 51(5): 541-552

[73] Spreitzer R, Moonsamy V, Korak T, et al. Systematic classification of side-channel attacks: A case study for mobile devices. IEEE Communications Surveys and Tutorials, 2018, 20(1): 465-488

[74] Nguyen P H, Sahoo D P, Chakraborty R S, et al. Security analysis of arbiter PUF and its lightweight compositions under predictability test. ACM Transactions on Design Automation of Electronic Systems, 2017, 22(2): 20:1-20:28

[75] Guo Y, Zhang Z, Guo Y. Optiwords: A new password policy for creating memorable and strong passwords. Computers & Security, 2019, 85: 423-435

[76] Mouradian C, Naboulsi D, Yangui S, et al. A comprehensive survey on fog computing: State-of-the-art and research challenges. IEEE Communications Surveys and Tutorials, 2018, 20(1): 416-464

[77] Guo Y, Guo Y. FogHA: An efficient handover authentication for mobile devices in fog computing. Computers & Security, 2021, 108: 102358

[78] Gope P, Sikdar B. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. IEEE Internet of Things Journal, 2019, 6(1): 580-589

[79] Abdalla M, Fouque P, Pointcheval D. Password-based authenticated key exchange in the three-party setting// Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography. Les Diablerets, Switzerland, 2005: 65-84

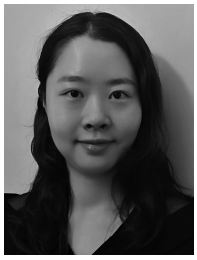
[80] Wang D, Wang P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Transactions on Dependable and Secure Computing, 2018, 15(4): 708-722

[81] Qiu S, Wang D, Xu G, et al. Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices. IEEE Transactions on Dependable and Secure Computing, 2020, DOI: 10.1109/TDSC.2020.3022797

[82] Gupta A, Tripathi M, Shaikh T J, et al. A lightweight anonymous user authentication and key establishment scheme for wearable devices. Computer Networks, 2019, 149: 29-42

[83] Jiang Q, Zhang X, Zhang N, et al. Three-factor authentication protocol using physical unclonable function for IoV. Computer Communications, 2021, 173: 45-55

[84] Gope P, Das A K, Kumar N, et al. Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. IEEE Transactions on Industrial Informatics, 2019, 15(9): 4957-4968



GUO Yi-Min, Ph. D., lecturer. Her research interests include password security and identity authentication.

ZHANG Zhen-Feng, Ph. D., professor. His research interests include cryptography and information security.

XIONG Ping, Ph. D., professor. His research interests include information security, machine learning and data mining.

GUO Ya-Jun, Ph. D., professor. His research interests include information security and modern cryptography.

Background

An important problem that needs to be solved in fog computing is how to implement authentication between incompletely trusted fog nodes and IoT devices. It is very difficult to design an effective authentication protocol for a fog computing environment. The main reason is that there are multiple different trust domains such as cloud, fog service providers and users in fog computing. Cloud nodes are considered trusted in multiple trust domains, but fog nodes and fog devices are not considered trusted.

The authentication scheme in fog computing should meet the following three conditions: (1) The authentication process in fog computing should only be done by the cooperation of fog nodes. Although the fog computing architecture contains clouds, cloud servers should not be involved in the authentication of IoT devices. this is due to the introduction of a fog layer for the purpose of reducing the average network latency. (2) The secret information of IoT devices cannot be stored in fog nodes. Because fog nodes are not completely

trusted, if a fog node is malicious or compromised, the attacker can carry out various attacks. (3) Fog devices have constrained computing, storage, and battery resources, designing authentication schemes for such resource-constrained devices should be lightweight. The existing authentication schemes designed for fog computing can effectively authenticate IoT devices, but these schemes cannot meet the above conditions.

Our protocol achieves mutual authentication among IoT devices, fog nodes and users without the participation of trusted cloud or other third parties, so it meets the low latency. And PUFs are used to achieve the expected security and efficiency requirements in the fog computing environment. In addition, we use many ingenious methods to make our protocols resistant to various known attacks. In particular, explicit CRPs are not stored in any party participating in the authentication, so as to eliminate the security risk caused by the need to store CRPs in the "challenge-response" authentication mechanism using PUFs.

This study is sponsored by the National Natural Science Foundation of China (Grant No. 62102453) and the Fundamental Research Funds for the Central Universities, Zhongnan University of Economics and Law (Grant No. 2722022BQ049). The aim of these projects is to address various privacy problems arising in cyberspace. Our team has been engaged in the design and analysis of cryptographic protocols, SMC, password security, identity authentication for over 10 years. We have published over 50 papers, of which over 30 have been indexed by SCI.