计 算 机 研 究 与 发 展
Journal of Computer Research and Development
https://crad.ict.ac.cn
63(11): 2892−2908, 2026

可证明安全的物联网抗隐式攻击轻量级认证协议

郭奕旻[1,2,3] 姜 奇[4] 熊 平[1]

[1](中南财经政法大学信息工程学院 武汉 430073)

[2](人工智能交叉学科国际联合研究中心(中南财经政法大学) 武汉 430073)

[3](人工智能与数字人文交叉学科创新国际研究中心(中南财经政法大学) 武汉 430073)

[4](西安电子科技大学网络与信息安全学院 西安 710071)

(yiminguo@zuel.edu.cn)

A Provably Secure Lightweight Authentication Protocol Against Implicit Attacks for IoT

Guo Yimin[1,2,3], Jiang Qi[4], and Xiong Ping[1]

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

[2](*International Joint Research Center for Interdisciplinary Artificial Intelligence* (*Zhongnan University of Economics and Law*), *Wuhan* 430073)

[3](*International Research Center for Interdisciplinary Innovation in Artificial Intelligence and Digital Humanities* (*Zhongnan University of Economics and Law*), *Wuhan* 430073)

[4](*School of Cyber Engineering*, *Xidian University*, *Xi'an* 710071)

Abstract The Internet of things (IoT) environment, characterized by resource-constrained terminals and sophisticated threats, poses severe challenges to the design of authentication protocols. Notably, even protocols verified by formal tools often remain vulnerable to implicit attacks, where adversaries combine multiple capabilities such as channel control and secret extraction, to launch more complex and concealed attack strategies. To address this issue, we propose a provably secure, resource-efficient, and lightweight authentication protocol. The protocol employs lightweight cryptographic primitives, including Hash functions and physical unclonable functions (PUFs), and optimizes both communication and computational overhead through dynamic identity and message fusion mechanisms, without relying on expensive public-key operations. To establish a solid security foundation, we construct an extended real-or-random (ROR) model capable of characterizing composite attack scenarios, under which the semantic security of the session key is rigorously proven. Heuristic analysis further demonstrates that the protocol achieves all nine predefined security properties even under implicit attacks. Performance evaluation and comparative analysis indicate that the proposed protocol requires only 0.583 5 ms of computational time on smart devices and incurs a communication overhead of 3 168 b. While fulfilling comprehensive security objectives, its resource efficiency significantly outperforms existing schemes, offering a practical solution that balances security and lightweight design for IoT applications.

Key words implicit attack; authentication; security property; Internet of things; lightweight

收稿日期: 2025-11-28; **修回日期**: 2026-08-27

基金项目: 湖北省自然科学基金项目(2025AFC108); 国家自然科学基金项目(62102453, 62472337); 陕西省自然科学基础研究计划资助项目(2025JC-JCQN-084)

This work was supported by the Hubei Provincial Natural Science Foundation of China (2025AFC108), the National Natural Science Foundation of China (62102453, 62472337), and the Natural Science Basic Research Program of Shaanxi Province (2025JC-JCQN-084).

通信作者: 郭奕旻(yiminguo@zuel.edu.cn)

摘　要　物联网终端资源受限与复杂攻击并存的环境，对认证协议的设计提出了严峻挑战。尤其值得关注的是，即便通过形式化工具验证的协议，在攻击者组合多种基础攻击能力（如信道控制、秘密提取）所构成的隐式攻击下仍显脆弱。为解决上述问题，提出一种面向物联网的、可证明安全、资源高效且轻量级的认证协议。该协议采用哈希函数与物理不可克隆函数（physical unclonable functions, PUF）作为核心密码原语，通过动态身份与消息融合机制，同步优化通信与计算开销。在安全层面构建了可刻画复合攻击场景的扩展 ROR（real-or-random）模型，并在此模型下严格证明了所提协议会话密钥的语义安全性；启发式安全分析进一步证实，所提协议在面对各类最强隐式攻击时，仍能实现全部 9 项预设安全属性。性能对比实验表明，所提协议在智能设备上的计算耗时仅为 0.583 5 ms，通信开销为 3 168 b，在达成全面安全目标的同时其资源效率显著优于现有主流方案，为物联网应用提供了一个安全与轻量兼备的实用化解决方案。

关键词　隐式攻击；认证；安全属性；物联网；轻量级

中图法分类号　TP3；TP309

DOI: 10.7544/issn1000-1239.202550862　　**CSTR:** 32373.14.issn1000-1239.202550862

物联网（Internet of things, IoT）技术正将海量智能设备无缝接入网络，构建起支持智能家居、工业自动化、智慧医疗等关键应用的底层基础设施[1-2]。然而，物联网终端通常资源高度受限（计算能力、存储空间及电池能量有限），且部署于开放的物理环境中，这使得它们极易成为各类攻击的目标。认证协议作为建立实体间信任关系、保障通信安全的基石，其设计的优劣直接决定了整个物联网系统的安全性与可靠性[3-4]。

尽管学术界已提出众多面向物联网的认证协议[5-7]，但一个令人困扰的现象是，许多协议在发表后不久便被发现存在严重安全漏洞[8-9]。这一问题的根源在于，传统威胁模型（如 DY（Dolev-Yao）模型[10]和 CK（Canetti-Krawczyk）模型[11]）通常仅考虑攻击者具备单一或有限的能力。而现实中的攻击者能够组合多种基础攻击能力，例如同时控制通信信道并获取服务器端存储的秘密，形成更为复杂的隐式攻击[12]。正如第 1 节所述，大量现有协议在隐式攻击面前显得异常脆弱，陷入了“设计—发现漏洞—修补—再发现新漏洞”的循环[13]。这表明，仅依靠传统的可证明安全分析或自动化工具验证，已难以应对物联网环境中的复合威胁。

隐式攻击对认证协议设计提出了 2 个方面的严峻挑战：其一，在安全性上，协议必须能够抵抗最强隐式攻击，即针对特定安全属性，攻击者所能实施的、由多种基础能力构成的最大正交组合（其形式化定义见第 2 节）。其二，在效率上，为实现上述安全性，协议设计需避免引入复杂的公钥密码学操作，以确保其在资源受限的物联网终端上的可行性。然而，现有方案难以在二者间取得良好平衡：基于公钥密码学的协议虽能实现较多安全属性，但其高昂的计算开销难以被轻量级终端所承受；而许多采用轻量级原语的协议却又无法抵抗隐式攻击，存在安全隐患。

为应对上述挑战，文献 [12] 提出了隐式攻击的概念，并建立了安全属性与最强隐式攻击之间的映射关系，为该类攻击的形式化分析奠定了基础。然而，文献 [12] 并未给出具体的协议设计方案。本文在此基础上，设计一个兼具可证明安全性与资源高效性的轻量级认证协议，主要贡献如下：

1）协议脆弱性实证分析。以文献 [12] 建立的安全属性与最强隐式攻击的映射关系为分析工具，我们深入剖析了一个经典物联网认证协议在隐式攻击下的安全漏洞，揭示了现有安全分析范式的局限性。

2）抗隐式攻击的轻量级协议设计。提出了一种名为 ISEC-AKA 的抗隐式攻击轻量级认证协议。该协议巧妙运用哈希函数与物理不可克隆函数等轻量级原语，通过动态身份与消息融合机制，在保障安全性的同时，显著降低了通信与计算开销。

3）增强的形式化安全模型与证明。为精准评估协议在隐式攻击下的安全性，我们扩展了 ROR（real-or- random）模型，使其能够刻画攻击者的复合能力，并在此增强模型下严格证明了会话密钥的语义安全性。

4）全面的性能验证。系统性对比实验表明，ISEC-AKA 协议在实现全部 9 项安全属性的同时，在智能设备上仅需 0.583 5 ms 的计算时间和 3 168 b 的通信开销，其综合性能显著优于现有方案。

1　相关工作

物联网认证协议的研究历程，呈现出安全漏洞不断被发现、攻击模型持续深化的特点。本节按时

间顺序梳理代表性工作，旨在揭示一个核心问题：尽管协议设计不断改进，但传统安全分析模型在应对攻击者多种基础能力组合构成的隐式攻击时存在固有局限性。

1.1 初期方案与隐式攻击威胁的显现

早期研究揭示了物联网认证协议面临的新型威胁。Kalra 等人[14]提出了一个基于椭圆曲线密码学(elliptic curve cryptography, ECC)的认证方案，并通过AVISPA(automated validation of Internet security protocols and applications)工具验证了其安全性。然而，Kumari 等人[15]发现，该方案在面对 EC4-1 和 EC6 攻击时(具体攻击描述详见定义 1)，无法抵抗离线口令猜测攻击，也不能提供匿名性。这一案例表明，即使通过形式化工具验证的方案，在超越传统威胁模型的复合攻击下也可能失效。

几乎在同一时期，轻量级方案也面临类似挑战。Li 等人[16]为远程医疗系统提出了一个基于哈希函数的方案，但 Madhusudhan 等人[17]发现，该方案在{EC1, EC5-1}攻击下不支持用户匿名性，且无法抵抗离线口令猜测、中间人攻击等。这些早期发现共同预示了隐式攻击将成为物联网认证协议普遍面临的安全威胁。

1.2 改进方案与漏洞的持续存在

针对已发现漏洞的改进方案，往往未能从根本上解决问题。在 2018—2022 年间，Garg 等人[18]为智能电网提出了一个基于改进 ECC 的轻量级方案，但随后 Chaudhry 等人[19]演示其在 EC3 攻击下不能抵抗密钥泄露假冒攻击；Shuai 等人[20]的智能家居方案虽通过 ProVerif 验证，但被 Zou 等人[21]发现其在{EC1, EC3}攻击下不能提供前向安全；Li 等人[22]为车载 Ad hoc 网络提出的认证协议则在{EC1, EC2}攻击下被发现存在重放攻击漏洞[23]；Braeken[24]提出基于对称密码的 5GAKA 协议，声称具备匿名性等属性，但 Yadav 等人[25]演示其在{EC1, EC6}攻击下不能抵抗重放攻击和主密钥猜测攻击；Yang 等人[26]提出的基于区块链物联网认证协议被 Lansky 等人[27]发现在{EC1, EC3}攻击下不具备完美前向保密属性；Chunka 等人[28]提出的认证协议则在{EC1, EC4}攻击下存在临时信息泄露等问题[29]。

这一阶段显示，物联网认证协议陷入了“设计—发现漏洞—修补—发现新漏洞”的循环。其根本原因在于，修补通常针对特定已发现的攻击，而未从威胁模型层面进行系统性增强以涵盖复合攻击场景。

1.3 近期进展与尚未解决的核心挑战

近 5 年的研究仍未打破上述循环。2022—2024 年，Hajian 等人[30]提出的认证方案被发现在{EC1, EC5-2}攻击下存在口令离线猜测攻击和会话钥泄露漏洞[29]；Zerrouki 等人[31]提出的基于物理不可克隆函数(physical unclonable functions, PUF)的物联网协议在{EC2, EC4-2}攻击下被发现存在密钥泄露问题[32]；Kandar 等人[33]基于切比雪夫混沌映射提出的多服务器远程用户认证方案在{EC1, EC3}攻击下无法抵抗用户假冒攻击与会话钥泄露。Chen 等人[34]为无线传感器网络提出的 2 因素多网关认证协议在{EC1, EC4-2}攻击下存在智能设备假冒漏洞。Zhang 等人[35]为物联网电子健康系统提出的隐私保护快速 3 因素认证协议虽通过 ROR 模型证明和 AVISPA 工具验证，但在{EC1, EC4-1, EC6}攻击下仍被发现存在离线口令猜测和用户匿名性方面的缺陷。

2024—2026 年，Shahparian 等人[36]提出的区块链车联网认证与密钥协商协议在{EC1, EC2, EC5-2}等多种攻击能力组合下仍存在重放攻击和会话钥泄露等安全漏洞。Wang 等人[37]提出了基于 3 因素和 PUF 的无人机辅助应急通信认证方案，采用哈希和异或运算以满足无人机计算限制，但其安全分析未考察隐式攻击下的安全性，无法抵抗{EC1, EC2, EC4-2}攻击带来的无人机假冒漏洞。2026 年，Ji 等人[38]提出了一种面向区块链辅助雾网络的轻量级无人机(unmanned aerial vehicle, UAV)认证方案，该方案通过 ProVerif 形式化工具验证了其在 DY 模型下的安全性，但其安全分析仍基于单一攻击能力的传统威胁模型。事实上，在该方案中，若攻击者具备{EC1, EC5-2}的组合能力，则可以通过提取的 UAV 长期秘密计算出动态认证参数，进而成功实施假冒攻击。这些发现进一步表明，即使是最新提出的、通过形式化工具验证的协议，在隐式攻击下仍存在显著的安全漏洞。Guo 等人[12]系统提出了“显式攻击”与“隐式攻击”的分类框架，指出大量通过形式化工具验证的协议在隐式攻击下仍存在安全漏洞，这一发现与本文的实证分析结论一致。

相关工作进展表明，即便是在最前沿的物联网认证协议研究中(如文献 [35, 37−42] 等)，安全分析大多仍基于传统模型，仅关注单一攻击类型或有限的攻击能力组合。这些协议均未针对第 2 节定义的最强隐式攻击组合进行系统性验证，因此无法保证在复杂的隐式攻击场景下实现所有安全属性。

综上所述，该领域的研究演变揭示了一个关键挑战：现有方案的安全分析，未能系统性地应对由多种基础攻击能力正交组合而成的隐式攻击。本文工

作的必要性在于：将安全属性与最强隐式攻击的对应关系作为核心设计准则，旨在为构建能够抵抗复合威胁、兼具安全与效率的物联网认证协议提供新的解决方案。

2 隐式攻击模型与安全目标

为构建普适性的物联网认证协议安全分析框架，本节形式化地定义隐式攻击模型的核心要素，包括攻击者能力、隐式攻击以及安全属性与最强隐式攻击之间的映射关系。该威胁模型是对传统 DY 模型与 CK 模型的扩展，旨在精确刻画物联网环境中攻击者可能具备的复合能力。本节定义的攻击能力框架（EC1~EC6）源自文献 [12]，本文在此基础上对各类能力进行了形式化细化，补充分类依据与互斥限制，并明确了能力的覆盖范围、排除边界与限制条件。

2.1 攻击者能力与隐式攻击的形式化定义

物联网环境中，攻击者的基础攻击能力可抽象为正交的核心维度。我们用Π表示任意物联网认证协议，$\mathcal{A}$表示攻击者，$\mathcal{E}$表示Π的交互实体集合（如用户、服务器、智能设备等通用实体类型）。

2.1.1 隐式攻击的直观内涵

在传统威胁模型（如 DY 模型）中，攻击者通常被抽象为具备“完全控制通信信道”能力的单一实体，其攻击行为主要表现为对传输消息的窃听、篡改与重放，这类攻击可称为“显式攻击”。然而，物联网环境中大量安全漏洞的根源在于：攻击者能够组合多种看似有限的基础攻击能力（如同时控制信道并窃取服务器端存储的秘密），从而间接破坏协议的安全属性。这种攻击方式并不直接针对某一安全机制发起正面攻击，而是通过多种能力的正交组合形成“1+1>2”的复合威胁，故称之为“隐式攻击”（implicit attack, IA）。隐式攻击的核心特征是：攻击者所具备的任意单一基础能力均不足以攻破目标安全属性，但其组合却能使协议失效。

定义 1. 基本攻击能力。令EC表示一个有限的基本攻击能力集合，包含 8 种核心能力：EC={EC1, EC2, EC3, EC4-1, EC4-2, EC5-1, EC5-2, EC6}，其含义如下：

1）EC1。$\mathcal{A}$可完全控制$\mathcal{E}$间的公共通信信道，对Π中所有传输消息执行拦截、篡改、伪造操作，且$\mathcal{E}$无法识别信道被控制。

2）EC2。$\mathcal{A}$可获取Π中任意会话的临时参数（如临时随机数、时间戳等）。该能力覆盖 CK 模型中的“会话状态揭露”，且不依赖具体协议的临时参数命名规则。

3）EC3。$\mathcal{A}$可获取$\mathcal{E}$中任意实体的长期秘密（如实体私钥、共享密钥等）。

4）EC4-1/EC4-2。$\mathcal{A}$可攻陷Π中的用户终端或者智能设备并提取其存储的秘密（二者互斥）。

5）EC5-1/EC5-2。$\mathcal{A}$作为Π的合法内部实体，可获取用户注册阶段的传输消息（EC5-1）或者服务器端存储的实体注册信息（EC5-2）（二者互斥）。

6）EC6。$\mathcal{A}$可在多项式时间内离线猜测Π中的弱秘密（如用户口令、简单凭证），并通过协议交互或参数验证判断猜测正确性。

定义 2. 隐式攻击。一个攻击能力组合IA是基本攻击能力EC的一个非空子集，即$IA \subseteq EC$且$IA \neq \varnothing$，表示攻击者$\mathcal{A}$同时具备IA中所有能力。由于物理互斥性，EC4-1 与 EC4-2 不能同时存在于一个IA中，EC5-1 与 EC5-2 亦然。当$|IA| = 1$时，该攻击退化为传统模型中的“显式攻击”（explicit attack），即攻击者仅具备单一基础能力；当$|IA| \geqslant 2$时，称为“隐式攻击”，强调多种能力组合产生的复合威胁。本文研究的重点为$|IA| \geqslant 2$的隐式攻击。

2.1.2 基础攻击能力的范围界定

本文定义的攻击能力集合EC（见定义 1）聚焦于物联网认证协议在逻辑层面的安全威胁。该集合的选择基于以下原则：1）覆盖现有文献中已知的攻击向量；2）刻画协议设计中的核心安全假设（如信道安全性、秘密存储安全性、临时参数安全性）；3）排除物理层攻击和拒绝服务攻击——这些属于协议运行环境的安全假设范畴，而非协议逻辑设计本身。

1）覆盖范围。EC中的 8 种能力系统性地刻画了以下 5 类威胁场景：

①信道与通信威胁（EC1）。对应 DY 模型中的标准攻击者能力，是所有认证协议的基础威胁假设。

②秘密泄露威胁（EC2, EC3）。覆盖临时会话状态泄露（EC2）与长期密钥泄露（EC3），后者是评估完美前向保密等属性的必要假设。

③物理终端攻陷威胁（EC4-1, EC4-2）。区分用户终端与智能设备 2 类实体，体现物联网环境中不同类型终端的安全假设差异，攻击者可能攻陷用户终端或者智能设备。

④内部人员威胁（EC5-1, EC5-2）。区分注册阶段信息泄露与服务器存储信息泄露，模拟特权内幕攻击。

⑤弱凭证威胁（EC6）。模拟离线口令/简单凭证猜测，是多因素认证协议必须考虑的现实威胁。

2)排除范围。以下攻击场景暂不属于本文模型的考虑范畴,其理由如下:

①物理层侧信道攻击。此类攻击(如功耗分析、时序攻击、故障注入等)需要攻击者对设备进行物理访问且具备特定测量设备,属于硬件实现安全性而非协议逻辑安全性。本文假设密码原语(哈希函数和 PUF)的实现是安全的。

②拒绝服务攻击(denial of service, DoS)。抗 DoS 能力通常作为独立的安全属性单独分析,且可通过速率限制、资源配额等机制在协议之外缓解。本文聚焦于认证协议的身份鉴别与密钥协商功能的安全性。

③量子计算攻击。超出当前物联网协议所基于的经典密码学假设,属于未来密码学演进的范畴。

3)能力覆盖的完备性论证。EC的 8 种能力并非穷举所有可能的攻击向量,但构成了一个正交且完备的最小集合——任一能力无法被其他能力的组合所逻辑蕴含(EC4-1 与 EC4-2 互斥除外),且现有文献中已发现的物联网认证协议安全漏洞均可归因于该集合中某子集的组合被忽略。这一论断已在文献 [12] 中通过实证分析得到验证。

2.1.3 攻击能力的限制条件

为使隐式攻击模型具有可分析性与现实合理性,对攻击能力的组合施加以下补充限制。

限制 1. 物理互斥性。EC4-1 与 EC4-2 不能同时存在于一个隐式攻击中,因为同一攻击者无法同时攻陷用户终端与智能设备的物理存储(二者在物理位置上分离,且攻陷一方不自动赋予攻陷另一方的能力)。同理,EC5-1 与 EC5-2 不能共存,前者模拟内部人员截获注册消息,后者模拟服务器数据库泄露,二者的攻击路径与所需权限互斥。此限制已在定义 2 中给出,此处进一步阐明其合理性。

限制 2. 能力依赖关系。EC6(离线猜测)的有效实施通常依赖其他能力的配合——攻击者需要借助例如 EC1, EC4-1, EC5 攻击获取可用于验证猜测结果的消息或参数。因此,EC6 在本文模型中总是与其他攻击能力组合出现,而非单独使用。

2.1.4 与传统威胁模型的对比

为清晰展示本文隐式攻击模型与传统威胁模型的区别,表 1 给出了 DY 模型、CK 模型、本文 IA 模型在攻击能力刻画维度上的对比。

Table 1 Comparison of Adversary Models

表 1 威胁模型对比

攻击能力维度	威胁模型		
	DY	CK	IA(本文)
信道控制(EC1)	√	√	√
临时秘密获取(EC2)	×	√	√
长期秘密获取(EC3)	×	√	√
终端物理攻陷(EC4)	×	×	√
内部人员攻击(EC5)	×	×	√
离线口令猜测(EC6)	×	×	√
能力组合分析	单一能力	极少组合	多种正交组合

2.2 安全属性与最强隐式攻击的映射

协议的安全目标由其所需满足的安全属性定义。一个认证协议若声称满足某安全属性,则必须能够抵抗针对该属性的最强威胁。

定义 3. 安全属性。令SP表示协议需要满足的安全属性集合。本文关注$SP^{*}=\{sp_1,sp_2,\cdots,sp_9\}\subseteq SP$,其具体含义如表 2 所示。

Table 2 Mapping Between Security Properties and the Strongest Implicit Attacks

表 2 安全属性与最强隐式攻击的映射关系

条目	安全属性sp	最强隐式攻击$\mathcal{M}(sp)=SIA_{sp}$
sp_1	相互认证与密钥建立	{EC1, EC2, EC5, EC6}, 或者 {EC1, EC3, EC5, EC6}
sp_2	抵抗重放攻击	{EC1, EC2, EC5, EC6}, 或者{EC1, EC3, EC5, EC6}
sp_3	抵抗中间人攻击	{EC1, EC2, EC5, EC6}, 或者{EC1, EC3, EC5, EC6}
sp_4	抵抗假冒攻击	{EC1, EC2, EC4/ EC5-2, EC6}, 或者{EC1, EC3/ EC4, EC6}, 或者{EC1, EC3/ EC5, EC6}
sp_5	抗离线口令猜测攻击	{EC1, EC4-1, EC5, EC6}
sp_6	会话钥安全	{EC1, EC2, EC4/ EC5-2, EC6}, 或者{EC1, EC3/ EC4, EC6}, 或者{EC1, EC3/ EC5, EC6}
sp_7	完美前向保密	{EC1, EC3}
sp_8	匿名性	{EC1, EC2, EC5, EC6}, 或者{EC1, EC3, EC5, EC6}
sp_9	抗去同步攻击	{EC1, EC2, EC5, EC6}, 或者{EC1, EC3, EC5, EC6}

定义 4. 最强隐式攻击。对于给定的安全属性$sp\in SP$,设IA_{sp}为所有能破坏sp的隐式攻击组合(即基本攻击能力的非空子集)的集合。其对应的最强隐式攻击SIA_{sp}是IA_{sp}中的一个元素,满足对于任何其他$IA\in IA_{sp}$,都有$IA\subseteq SIA_{sp}$。表 2 给出了各安全属性对应的最强隐式攻击组合实例。

定义 5. 安全属性与最强隐式攻击的映射。安全属性与最强隐式攻击的对应关系由一个映射函数$\mathcal{M}$定义:

$$\mathcal{M}:SP\rightarrow\mathcal{P}(EC),$$

其中SP为安全属性集合,EC为基本攻击能力集合,$\mathcal{P}(EC)$表示EC的幂集(即EC的所有子集构成的集

合)。对于任意安全属性$sp \in SP$, $\mathcal{M}(sp)$的输出是EC的一个子集,即针对该安全属性的最强隐式攻击能力组合SIA_{sp},表示为$\mathcal{M}(sp)=SIA_{sp}$。每个安全属性sp映射到其对应的最强隐式攻击能力集合SIA_{sp}的具体定义如表 2 所示。

2.3 协议安全目标

基于定义 1~5,我们形式化定义抗隐式攻击认证协议的安全目标。

定义 6. 抗隐式攻击安全目标。令Π表示一个物联网认证协议,$SP^* \subseteq SP$为Π声称实现的安全属性集合,$\mathcal{M}$为定义 5 中的映射函数。协议Π达到抗隐式攻击安全目标,当且仅当对于$\forall sp \in SP^*$,协议在攻击者$\mathcal{A}$具备$\mathcal{M}(sp)$所定义的全部能力时,依然能保持属性sp成立。

定义 7. 完全抗隐式攻击协议。若协议Π对于安全属性全集SP达到抗隐式攻击安全目标,则称协议Π为完全抗隐式攻击协议。

定义 1~7 建立了评估物联网认证协议安全性的普适性框架。第 5 节将基于此模型对本文提出的 ISEC-AKA 协议进行形式化安全证明与启发式分析,验证其满足定义 7 所述的安全目标。

3 Wazid 协议在隐式攻击下的安全性分析

第 2 节建立的形式化模型揭示,隐式攻击对认证协议构成了超越传统认知的威胁。为实证这一威胁的普遍性与严重性,本节选取一个被广泛引用且声称安全的经典协议——Wazid 等人[40]为智能家居设计的轻量级认证方案作为案例,系统剖析其在隐式攻击下的脆弱性。

3.1 协议安全目标

Wazid 等人[40]的协议在显式攻击 EC1 下能够抵抗中间人攻击,但在隐式攻击{EC1, EC5-2}下不能抵抗中间人攻击。敌手在用户和网关之间执行中间人攻击过程如下。

1)执行 EC1 攻击,敌手截获到用户传输给网关的消息$\{TID_i, M_2, M_3, T_1\}$;

2)执行 EC5-2 攻击,敌手能够得到存储在网关中的用户存储信息$\{TID_i, ID_i, K_{GWN-U_i}\}$;

3)攻击者计算$M_1 = h(ID_i \| K_{GWN-U_i})$, $M_2 = M_1 \oplus r_{U_i}$, $M_3 = h(M_2 \| T_1 \| ID_i \| TID_i \| r_{U_i})$;

4)根据计算出的消息,敌手可以修改消息,按照协议的步骤将修改后的消息传给网关,网关认证攻击者是真实的;

5)执行 EC1 攻击,敌手截获网关传给用户的消息$\{M_{14}, M_{15}, M_{16}, T_3, T_4\}$,窃听到智能设备传给网关的消息$\{M_{10}, M_{11}, M_{12}, T_3\}$,其中$M_{14} = E_{M_4}[r_{U_i}, r_{GWN}, r_{SD_j}, ID_{SD_j}, ID_{GWN}, h(M_6)]$,敌手知道$M_4 = M_1 = h(ID_i \| K_{GWN-U_i})$,使用$M_4$解密$M_{14}$,敌手能够得到$M_{14}$中的所有秘密$\{r_{U_i}, r_{GWN}, r_{SD_j}, ID_{SD_j}, ID_{GWN}, h(M_6)\}$;

6)根据$M_{15} = TID_i^{\text{new}} \oplus h(TID_i \| M_4 \| T_3 \| T_4)$,敌手计算出$TID_i^{\text{new}}$,并能够计算出正确的$M_{16} = h(M_{11} \| T_4 \| r_{U_i})$。敌手拦截到网关传给用户的消息后,再修改消息传给用户,修改的消息能够通过用户的认证,因此,敌手在{EC1, EC5-2}隐式攻击下能够实施中间人攻击。

3.2 会话钥安全攻击之一

Wazid 等人[40]的协议在显式攻击 EC1 或者隐式攻击{EC1,EC2}或者隐式攻击{EC1,EC3}下能够保证会话钥安全,但在隐式攻击{EC1, EC5-2}下,敌手能计算出会话钥,攻击过程如下。

1)执行 EC5-2 攻击,敌手能够得到存储在网关中的用户存储信息$\{TID_i, ID_i, K_{GWN-U_i}\}$和智能设备信息$\{ID_{SD_j}, K_{GWN-SD_j}\}$;

2)敌手计算$M_1 = h(ID_i \| K_{GWN-U_i})$, $M_6 = h(ID_{SD_j} \| K_{GWN-SD_j})$;

3)执行 EC1 攻击,敌手窃听到消息$\{TID_i, M_2, M_3, T_1\}$和$\{M_7, M_8, T_2\}$;

4)根据$M_2 = M_1 \oplus r_{U_i}$计算出$r_{U_i} = M_1 \oplus M_2$;

5)使用M_6解密$M_7 = E_{M_6}[ID_i, ID_{GWN}, r_{U_i}, r_{GWN}, h(M_4)]$,得到$M_7$中的所有秘密;

6)由于$M_4 = M_1$,使用M_4解密$M_{14} = E_{M_4}[r_{U_i}, r_{GWN}, r_{SD_j}, ID_{SD_j}, ID_{GWN}, h(M_6)]$可以得到$M_{14}$中的所有信息;

7)敌手计算出会话钥$SK_{ij} = h(ID_i \| ID_{SD_j} \| ID_{GWN} \| r_{U_i} \| r_{GWN} \| r_{SD_j} \| h(M_4) \| h(h(ID_{SD_j} \| K_{GWN-SD_j})))$。

3.3 会话钥安全攻击之二

在隐式攻击{EC1, EC4-2}下,Wazid 等人[40]协议的会话钥也是不安全的,攻击过程如下。

1)执行 EC4-2 攻击,敌手得到存储在智能设备中的信息$h(ID_{SD_j} \| K_{GWN-SD_j})$和$ID_{SD_j}$,因此敌手知道$M_6 = h(ID_{SD_j} \| K_{GWN-SD_j})$;

2)执行 EC1 攻击,敌手得到消息$\{M_7, M_8, T_2\}$;

3)根据M_6,解密$M_7 = E_{M_6}[ID_i, ID_{GWN}, r_{U_i}, r_{GWN}, h(M_4)]$,得到$\{ID_i, ID_{GWN}, r_{U_i}, r_{GWN}, h(M_4)\}$;

4)执行 EC1 攻击,敌手得到消息$\{M_{10}, M_{11}, M_{12}, T_3\}$;

5)计算$r_{SD_j} = h(h(ID_{SD_j} \| K_{GWN-SD_j} \| T_3)) \oplus M_{10}$;

6)根据上面信息,敌手计算会话钥$SK_{ij} =$

$h(ID_i||ID_{SD_j}||ID_{GWN}||r_{U_i}||r_{GWN}||r_{SD_j}||h(M_4)||h(h(ID_{SD_j}||K_{GWN-SD_j})))$。

3.4 用户假冒攻击

Wazid 等人[40]的协议在显式攻击 EC1 下能够抵抗用户假冒攻击，但在隐式攻击{EC1, EC5-2}下，该协议则不能抵抗用户假冒攻击，其攻击过程如下。

1)执行 EC1 攻击，敌手能够窃听到传输的消息$\{TID_i, M_2, M_3, T_1\}$；

2)执行 EC5-2 攻击，敌手能够得到存储在网关中的用户存储信息$\{TID_i, ID_i, K_{GWN-U_i}\}$；

3)敌手产生一个随机数r和时间戳t，计算$M_1 = h(ID_i||K_{GWN-U_i})$，$M_2^* = M_1 \oplus r$，$M_3^* = h(M_2^*||t||ID_i||TID_i||r)$，并将$\{TID_i, M_2^*, M_3^*, t\}$传给网关，网关按照协议执行过程，认证攻击者是真实的用户。

3.5 智能设备假冒攻击

Wazid 等人[40]的协议在显式攻击 EC1 下能够抵抗智能设备假冒攻击，但在隐式攻击{EC1, EC5-2}下，敌手能够执行智能设备假冒攻击，其攻击过程如下。

1)执行 EC5-2 攻击，得到存储在网关中的智能设备信息$\{ID_{SD_j}, K_{GWN-SD_j}\}$；

2)敌手计算$M_6 = h(ID_{SD_j}||K_{GWN-SD_j})$；

3)执行 EC1 攻击，敌手能够窃听到传输的消息$\{M_7, M_8, T_2\}$；

4)使用M_6解密$M_7 = E_{M_6}[ID_i, ID_{GWN}, r_{U_i}, r_{GWN}, h(M_4)]$，得到$\{ID_i, ID_{GWN}, r_{U_i}, r_{GWN}, h(M_4)\}$；

5)产生一个随机数r和时间戳t，计算一个会话钥$SK^* = SK_{ij} = h(ID_i||ID_{SD_j}||ID_{GWN}||r_{U_i}||r_{GWN}||r||h(M_4)||h(h(ID_{SD_j}||K_{GWN-SD_j})))$；

6)计算$M_{10}^* = h(h(ID_{SD_j}||K_{GWN-SD_j})||t) \oplus r$，$M_{11}^* = h(SK_{ij}||t)$，$M_{12}^* = h(r||r_{GWN}||ID_{SD_j}||ID_{GWN}||t)$；

7)将$\{M_{10}^*, M_{11}^*, M_{12}^*, t\}$传给网关，网关验证攻击者是真实的，攻击者最后与用户执行相互认证，并共享一个会话钥SK^*。

4 抗隐式攻击的轻量级认证协议 ISEC-AKA

以云-雾协作网络模型为例[43]，本节提出一种面向边缘计算场景抗隐式攻击的物联网认证协议 ISEC-AKA。云-雾协作网络模型中，存在云服务器、雾服务器、用户/终端、智能设备、注册权威等实体，注册权威是可信实体，负责为不同实体分发密钥，雾服务器位于网络边缘，为了减少认证延迟，远程云服务器不参与认证，而由雾服务器认证物联网设备，本文所使用的网络模型如图 1 所示。

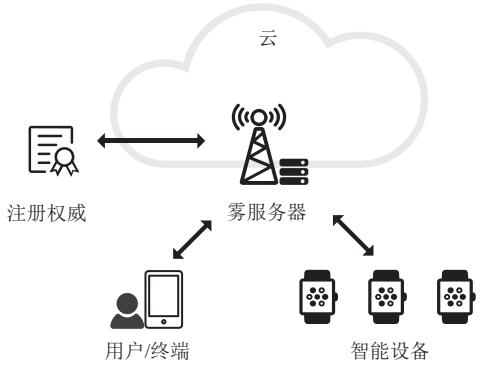


Fig. 1 Fog-assisted IoT network model

图 1 雾协作物联网网络模型

ISEC-AKA 协议包括初始化阶段、用户注册阶段、智能设备设置阶段、登录与认证阶段和用户口令更新阶段。协议所使用的符号及其含义如表 3 所示。

Table 3 Symbols and Corresponding Notations

表 3 符号和对应的含义

符号	定义
ID_i, ID_j	用户和智能设备的身份
PW_i	用户的口令
x, y	雾服务器的长期密钥
C_j, R_j	智能设备 PUF 的挑战和响应
a_i, b_i, r_i, n_i	随机数
$T_i, \Delta T_i$	时间戳和最大允许的传输延迟
SK	会话钥
$h(\cdot)$	单向哈希函数
$WPUF(\cdot)$	弱物理不可克隆函数
$\|\|, \oplus$	连接符和异或运算

4.1 初始化阶段

初始化阶段，注册权威为每个雾服务器生成各不相同的长期密钥$\{x, y\}$，雾服务器将长期密钥存储于与用户注册数据库隔离的安全硬件模块中。同时，注册权威选择一个抗碰撞的密码学哈希函数$h(\cdot)$，用于后续的注册和认证阶段。

4.2 用户注册阶段

用户使用用户终端在安全信道上向注册权威进行注册，该注册过程包括以下 5 个步骤。

步骤 1. 用户选择一个随机注册消息Reg_i传给注册权威。

步骤 2. 注册权威接收到用户的注册请求后，为用户产生一个随机响应消息Res_i，计算$Proc_t = Reg_i||Res_i$，随后将$\{Proc_t\}$传给用户。

步骤 3. 用户接收到注册权威传输的消息后，用户

终端恢复Res_i，选择用户名ID_i和口令PW_i，2个随机数$\{a_i,b_i\}$，计算$RID_i=h(ID_i||a_i)$，$RPW_i=h(ID_i||PW_i||a_i)\oplus b_i$，$Proc_i=RID_i\oplus Res_i$，随后将$\{Proc_i,RPW_i\}$传给注册权威。

步骤 4. 注册权威接收到用户的注册请求后，为用户产生一个随机数r_i，计算$RID_i=Proc_i\oplus Res_i$，$A_i=h(r_i||x)\oplus RPW_i$，$B_i=h(x||y)\oplus h(RPW_i)$，将$\{A_i,B_i\}$传给用户，并在雾服务器中存储用户的注册信息$\{RID_i,r_i\}$。

步骤 5. 用户接收到注册权威传输的消息，用户终端计算$h(r_i||x)=A_i\oplus RPW_i$，$h(x||y)=B_i\oplus h(RPW_i)$，$C_i=h(ID_i||PW_i)\oplus a_i$，$D_i=h(r_i||x)\oplus h(RID_i||PW_i)$，$E_i=h(x||y)\oplus h(RID_i||ID_i||PW_i)$，$F_i=h(h(r_i||x)||h(x||y)||RID_i||PW_i||a_i)$，最后，在用户终端中存储$\{C_i,D_i,E_i,F_i\}$。

设计说明：用户在注册时选择Reg_i和后续2个随机数$\{a_i,b_i\}$，以及注册权威为用户选择Res_i，其中Reg_i和b_i只是在用户向注册权威发送注册请求时使用，注册结束被用户丢弃，而Res_i只是在注册权威响应用户注册消息时使用，注册结束被注册权威丢弃，$\{Reg_i,b_i,Res_i\}$在后续的认证阶段不会使用，其目的是防止特权内幕攻击。这是因为特权内幕攻击者在得到RPW_i后，无法计算任何有用的信息。使用随机数a_i的目的是用于隐藏用户名和口令，以便阻止攻击者实施离线口令猜测攻击。采用这个方法能够抵抗Wang等人[9]定义的具有强大攻击能力的敌手所实施的攻击，他们分析发现攻击者有一定的概率同时猜测用户名和口令，在我们的方法中，当攻击者得到了用户的终端，能够提取存储其中的信息$\{C_i,D_i,E_i,F_i\}$，敌手只能通过C_i来猜测用户的口令，攻击者猜测一个ID_i^*和PW_i^*，然后计算$a_i=h(ID_i^*||PW_i^*)\oplus C_i$来判断猜测的用户名和口令是否正确，由于攻击者不知道a_i，所以敌手无法判断猜测的用户名和口令是否正确。

4.3 智能设备设置阶段

智能设备的设置阶段是在安全信道上进行的，其中每个智能设备中嵌入一个弱物理不可克隆函数（weak physically unclonable function, WPUF）。WPUF基于半导体制造工艺的固有随机性生成响应信号，其实现具有硬件成本低和环境适应性好的双重优势。该技术仅需采用标准CMOS工艺即可完成实现，无需额外配置专用加密芯片，特别适合资源受限的传感器设备；同时通过温度补偿算法，能在宽温域范围内将响应错误率维持在较低水平。

在这个阶段，注册权威为智能设备选择一个身份ID_j，产生一个挑战C_j和当前注册时间戳T_j，计算$S_j=h(ID_j||x||T_j)$，$R_j=WPUF\left(C_j\right)$。在雾服务器中存储$\{ID_j,h\left(R_j\right)\oplus h(x||T_j),T_j\}$，在智能设备中存储$\{ID_j,C_j,S_j\}$。

4.4 登录与认证阶段

在协议登录与认证过程中，用户首先使用用户终端登录，登录成功后，通过雾服务器与远程的智能设备执行相互认证，并生成一个让用户和智能设备能够后续通信的安全会话钥。

步骤 1. 用户登录。用户输入用户名ID_i^*和口令PW_i^*，用户终端计算$a_i^*=h(ID_i^*||PW_i^*)\oplus C_i$，$RID_i^*=h(ID_i^*||a_i^*)$，$h(r_i||x)=D_i\oplus h(RID_i^*||PW_i^*)$，$h(x||y)=E_i\oplus h(RID_i^*||ID_i^*||PW_i^*)$，计算$F_i^*=h(h(r_i||x)||h(x||y)||RID_i^*||PW_i^*||a_i^*)$是否与存储的$F_i$相等，如果相等，用户登录成功。

步骤 2. 用户发起认证。用户终端选择要访问的智能设备ID_j，产生一个随机数n_1和当前时间戳t_1，计算$M_1=n_1\oplus h(h(r_i||x)||t_1)$，动态身份$TID_i=RID_i\oplus h(h(x||y)||t_1)$，认证因子$Auth_1=h(h(r_i||x)||RID_i||TID_i||n_1||t_1)$，$M_2=ID_j\oplus h(Auth_1||h(r_i||x)||t_1)$，$M_3=h(RID_i||PW_i||n_1||t_1)\oplus h(h(r_i||x)||ID_j||n_1)$，其中$M_2$是为了隐藏智能设备身份，$M_3$是为了向雾服务器传输秘密参数$h(RID_i||PW_i||n_1||t_1)$。用户最后将$Meg_1=\{M_1,TID_i,M_2,M_3,Auth_1,t_1\}$传给雾服务器。

步骤 3. 雾服务器认证用户。雾服务器收到消息后，检查消息的新鲜性（即判断接收到消息的时间戳与发送消息的时间戳的差值是否小于预先设定的最大传输延迟），如果消息是新鲜的，雾服务器计算$RID_i=TID_i\oplus h(h(x||y)||t_1)$，在自己的数据库中检查是否存在$RID_i$，如果存在，找到$RID_i$对应的$r_i$，并计算$n_1=M_1\oplus h(h(r_i||x)||t_1)$，$Auth_1^*=h(h(r_i||x)||RID_i||TID_i||n_1||t_1)$，判断$Auth_1^*$是否与接收到的$Auth_1$相同，如果二者相同，雾服务器认证用户是真实的，并计算$ID_j=M_2\oplus h(Auth_1||h(r_i||x)||t_1)$，$h(RID_i||PW_i||n_1||t_1)=M_3\oplus h(h(r_i||x)||ID_j||n_1)$。

雾服务器在自己的数据库中检查是否存在ID_j，如果存在，找到对应的$\{h(R_j)\oplus h(x||T_j),T_j\}$，恢复$h(R_j)$并产生1个随机数$n_2$和当前时间戳$t_2$，并计算$S_j=h(ID_j||x||T_j)$，$M_4=n_2\oplus h(S_j||h(R_j)||t_2)$，$M_5=h(RID_i||PW_i||n_1||t_1)\oplus h(ID_j||h(R_j)||n_2||t_2)$，$M_6=h(x||n_2)\oplus h(S_j||h(R_j)||n_2)$，$Auth_2=h(h(RID_i||PW_i||n_1||t_1)||h(x||n_2)||ID_j||h(R_j)||n_2||t_2)$。其中$M_4$，$M_5$，$M_6$是为了分别向智能设备传输秘密参数$\{n_2,h(RID_i||PW_i||n_1||t_1),h(x||n_2)\}$。雾服务器最后将消息$Meg_2=\{M_4,M_5,M_6,Auth_2,t_2\}$传给智能设备。

步骤 4. 智能设备认证雾服务器。智能设备收到消息后，检验所接收到消息的新鲜性，如果消息是新鲜的，根据内存中的C_j，计算$R_j=WPUF(C_j)$，随后计算$n_2=M_4\oplus h(S_j||h(R_j)||t_2)$，$h(RID_i||PW_i||n_1||t_1)=M_5\oplus h(ID_j||h(R_j)||n_2||t_2)$，$h(x||n_2)=M_6\oplus h(S_j||h(R_j)||n_2)$，$Auth_2^*=$

$h(h(RID_i||PW_i||n_1||t_1)||h(x||n_2)||ID_j||h(R_j)||n_2||t_2)$，并检验$Auth_2^*$是否与$Auth_2$相等，如果二者相等，则表示智能设备认证了雾服务器。

智能设备产生一个随机数n_3和当前时间戳t_3，计算$M_7=n_3\oplus h(h(RID_i||PW_i||n_1||t_1)||ID_j||t_3)$，$M_8=h(x||n_2)\oplus h(h(RID_i||PW_i||n_1||t_1)||n_3)$，$SK=h(h(RID_i||PW_i||n_1||t_1)||h(x||n_2)||ID_j||n_3||t_3)$，$Auth_3=h(h(RID_i||PW_i||n_1||t_1)||SK||ID_j||t_3)$。之后，智能设备将消息$Meg_3=\{M_7,M_8,Auth_3,t_3\}$传给用户。

步骤 5. 用户认证智能设备。用户接收到智能设备传输的消息后，检验该消息的新鲜性，如果接收到的消息是新鲜的，用户计算$n_3=M_7\oplus h(h(RID_i||PW_i||n_1||t_1)||ID_j||t_3)$，$h(x||n_2)=M_8\oplus h(h(RID_i||PW_i||n_1||t_1)||n_3)$，$SK=h(h(RID_i||PW_i||n_1||t_1)||h(x||n_2)||ID_j||n_3||t_3)$，$Auth_3^*=h(h(RID_i||PW_i||n_1||t_1)||SK||ID_j||t_3)$。接着用户检验$Auth_3^*$是否等于接收到的$Auth_3$，如果二者相等，则用户认证了智能设备。到此为止，用户和智能设备执行了相互认证，并生成一个共享的会话钥SK用于后续的安全通信。

4.5 口令更新阶段

用户口令更新不需要与注册中心进行交互，只需在本地用户终端上执行。口令更新过程包括下面步骤：

步骤 1. 用户输入用户名ID_i'和口令PW_i'，用户终端计算$a_i'=h(ID_i'||PW_i')\oplus C_i$，$RID_i'=h(ID_i'||a_i')$，$h(r_i||x)=D_i\oplus h(RID_i'||PW_i')$，$h(x||y)=E_i\oplus h(RID_i'||ID_i'||PW_i')$，$F_i'=h(h(r_i||x)||h(x||y)||RID_i'||PW_i'||a_i')$，并判断$F_i'$是否与存储的$F_i$相等，如果二者相等，则执行下面的步骤。

步骤 2. 用户终端提示用户选择一个新口令PW_i^{new}，然后计算$C_i^{\text{new}}=h(ID_i||PW_i^{\text{new}})\oplus a_i$，$D_i^{\text{new}}=h(r_i||x)\oplus h(RID_i||PW_i^{\text{new}})$，$E_i^{\text{new}}=h(x||y)\oplus h(RID_i||ID_i||PW_i^{\text{new}})$，$F_i^{\text{new}}=h(h(r_i||x)||h(x||y)||RID_i||PW_i^{\text{new}}||a_i)$。最后，用户终端删除$\{C_i,D_i,E_i,F_i\}$，存储$\{C_i^{\text{new}},D_i^{\text{new}},E_i^{\text{new}},F_i^{\text{new}}\}$。

5 安全分析

在本节中，我们对 ISEC-AKA 协议进行形式化安全证明和启发式安全分析。根据会话钥安全属性与最强隐式攻击之间的关系，扩展著名的 ROR 安全模型，在扩展的 ROR 模型下证明 ISEC-AKA 协议的安全性。然后启发式安全分析 ISEC-AKA 协议在隐式攻击下能够提供各种安全属性。

5.1 形式化安全证明

第 2 节给出了针对会话密钥安全性的最强隐式攻击，其攻击能力集合为{EC1, EC2, EC4/EC5-2, EC6}或{EC1, EC3/EC4, EC6}或{EC1, EC3/EC5, EC6}。原始 ROR 模型仅能刻画具备特定攻击能力的敌手，无法描述拥有上述最强隐式攻击能力的敌手。为此，我们增加了若干新的查询，以刻画能力更强的隐式攻击敌手。ROR 模型中各组件(如参与者、接收状态、伙伴关系、新鲜性等)的详细定义参见文献 [44−46]。

在提出的 ISEC-AKA 协议中涉及用户(U)、智能设备(SD)、雾服务器(F)三个参与者，每个参与者有许多实例。用X_{U_i}，X_{SD_j}，X_{F_v}分别表示第i个用户的实例，第j个智能设备的实例，第v个雾服务器的实例。在下面的描述中，有时也使用X来表示U，SD，F中的任何一个实例。

扩展后的 ROR 模型中，敌手的攻击能力是通过执行下列查询来模拟：

1) $ExecuteEC1\left(X_{U_i},X_{SD_j},X_{F_v}\right)$。该查询模拟 EC1 中的被动攻击。敌手$\mathcal{A}$执行该查询能够得到协议执行中交换的所有消息。

2) $SendEC1(X,m)$。该查询模拟 EC1 中的主动攻击。使用该查询，如果$\mathcal{A}$向实例X发送消息m，$\mathcal{A}$能够得到实例X对消息m的响应。

3) $CorruptEC2(X)$。该查询模拟敌手具有 EC2 的攻击能力。使用该查询，$\mathcal{A}$能够得到实例X在某个特定会话中的临时秘密。

4) $CorruptEC3(X)$。该查询模拟敌手具有 EC3 的攻击能力。使用该查询，$\mathcal{A}$能够得到实例X的长期秘密。

5) $CorruptEC4\text{-}1\left(X_{U_i}\right)$。该查询模拟 EC4 中针对用户终端的攻击能力。使用该查询，$\mathcal{A}$能够得到用户终端中存储的所有信息。

6) $CorruptEC4\text{-}2\left(X_{SD_j}\right)$。该查询模拟 EC4 中针对智能设备的攻击能力。使用该查询，$\mathcal{A}$能够得到智能设备中存储的所有信息。

7) $CorruptEC5\text{-}1\left(X_{U_i}\right)$。该查询模拟 EC5 中特权内幕攻击能力。使用该查询，$\mathcal{A}$能够得到用户向注册权威传输的消息。

8) $CorruptEC5\text{-}2\left(X_{F_v}\right)$。该查询模拟 EC5 中的特权内幕雾服务器泄露攻击。使用该查询，$\mathcal{A}$能够得到雾服务器中存储的用户或者智能设备的注册信息。

9) $Hash(string)$。该查询用于查询一个随机预言机，密码学中的哈希函数被模拟为一个预言机。通过该查询，$\mathcal{A}$发送一个输入字符串$string$，能够得到哈希函数的输出。

10) $Test(X)$。该查询不是用于模拟敌手的攻击

能力，而是用于测试会话钥语义安全性。在 ROR 模型中，敌手可以多次执行$Test$查询。使用$Test$查询时，如果会话钥没有建立，返回无效的字符。如果会话钥已经建立，使用一个随机隐藏位b来决定$Test$查询的输出。如果b=1，向敌手输出真实会话钥；如果b=0，向敌手输出一个与会话钥等长的随机数。

定义 8. 会话钥的语义安全。在扩展 ROR 模型中，常使用游戏来模拟认证协议的语义安全性，在游戏中敌手需要区分一个真实的会话钥和一个等长的随机数。敌手$\mathcal{A}$能够执行 1)~9)的查询，之后使用$Test$查询猜测隐藏随机位b的值，如果敌手$\mathcal{A}$的猜测值b'与随机位b相同，那么敌手$\mathcal{A}$就赢了游戏。假设用$Succ(\mathcal{A})$表示$\mathcal{A}$赢得游戏的事件，$Pr[Succ(\mathcal{A})]$表示$\mathcal{A}$在游戏中胜利的概率，那么敌手$\mathcal{A}$破解协议 ISEC-AKA 的优势可以表示为$Adv_{\mathcal{A}}^{\text{ISEC-AKA}}(t)=|2\cdot Pr[Succ(\mathcal{A})]-1|$。如果$Adv_{\mathcal{A}}^{\text{ISEC-AKA}}(t)$是可以忽略的，则称 ISEC-AKA 协议是语义安全的。

定理 1. 假设$\mathcal{A}$是在扩展 ROR 模型中破解 ISEC-AKA 协议语义安全的多项式时间敌手，口令分布遵循 Zipf's 定律，那么敌手$\mathcal{A}$破解 ISEC-AKA 协议语义安全的优势为

$$Adv_{\mathcal{A}}^{\text{ISEC-AKA}}(t)\leqslant q_h^2/|Hash|+2C'q_s^{s'},$$

其中q_h表示执行$Hash$的查询次数，q_s表示执行$Send$查询次数，$|Hash|$是哈希函数空间范围，C'和s'是 Zipf's 参数。

证明. 敌手$\mathcal{A}$针对会话钥安全的隐式攻击包括{EC1, EC2, EC4/ EC5-2, EC6}或{EC1, EC3/ EC4, EC6}或{EC1, EC3/ EC5, EC6}。我们分别证明这 3 种隐式攻击下 ISEC-AKA 协议的语义安全性。首先定义一系列游戏$G_i(i=0,1,2,3,4,5,6,7)$，并假设$Succ(\mathcal{A},G_i)$表示$\mathcal{A}$在游戏G_i中正确猜出b的事件，$Pr[Succ(\mathcal{A},G_i)]$表示$\mathcal{A}$在游戏$G_i$中获胜的优势，证明过程如下：

游戏G_0. 该游戏模拟对 ISEC-AKA 协议的真实攻击，在游戏开始时，$\mathcal{A}$被要求猜测位b，由语义安全定义可知

$$Adv_{\mathcal{A}}^{\text{ISEC-AKA}}(t)=|2\cdot Pr[Succ(\mathcal{A},G_0)]-1|。\quad(1)$$

游戏G_1. 这个游戏模拟敌手执行 EC1 中的被动攻击。$\mathcal{A}$执行$ExecuteEC1$查询窃听到协议中传输的所有消息$\{Meg_1, Meg_2, Meg_3\}$，随后，$\mathcal{A}$使用$Test$查询确定输出是真实的会话钥还是一个随机数。由于会话钥$SK=h(h(RID_i||PW_i||n_1||t_1)||h(x||n_2)||ID_j||n_3||t_3)$中包含了多个仅凭窃听消息无法计算出的秘密参数，敌手无法计算出会话钥，因此有

$$Pr[Succ(\mathcal{A},G_1)]=Pr[Succ(\mathcal{A},G_0)]。\quad(2)$$

游戏G_2. 这个游戏模拟敌手执行 EC1 中的主动攻击。在该游戏中，$\mathcal{A}$使用$SendEC1$和$Hash$查询来检测是否有哈希冲突发生。由于传输的消息中包含了敌手不知道的秘密，直接找到哈希冲突是不可行的，敌手在游戏G_2的优势只能由生日悖论的结果来确定，因此有

$$|Pr[Succ(\mathcal{A},G_2)]-Pr[Succ(\mathcal{A},G_1)]|\leqslant q_h^2/2|Hash|。\quad(3)$$

游戏G_3. 该游戏模拟敌手能够执行 EC2 攻击，$\mathcal{A}$使用$CorruptEC2$查询能够得到协议传输中的临时秘密n_1，n_2，n_3。

游戏G_4. 该游戏模拟敌手执行 EC3 攻击，$\mathcal{A}$使用$CorruptEC3$查询能够得到雾服务器的长期秘密x和y。

游戏G_5. 该游戏模拟敌手能够执行 EC4-1 或 EC4-2 攻击，即可使用$CorruptEC$4-1 查询或者$CorruptEC$ 4-2 查询，敌手能够得到用户终端里存储的所有信息$\{C_i,D_i,E_i,F_i\}$，或者得到智能设备中存储的所有信息$\{ID_j,C_j,S_j\}$。

游戏G_6. 该游戏模拟敌手$\mathcal{A}$能够执行$CorruptEC$ 5-1 查询，敌手能够得到用户在注册阶段向注册权威传输的消息$\{Reg_i,Proc_i,RPW_i\}$。

游戏G_7. 该游戏模拟敌手$\mathcal{A}$能够执行$CorruptEC$ 5-2 查询，敌手能够得到存储在服务器中的用户和智能设备的注册信息$\{RID_i, r_i\}$和$\{ID_j,h(R_j)\oplus h(x||T_j),T_j\}$。

1)在会话钥安全攻击的最强隐式攻击之一{EC1, EC2, EC4/ EC5-2, EC6}下，敌手依次进行游戏G_1，G_2，G_3，G_5/G_7。

在该类攻击的游戏G_3下，敌手能够查询到协议传输中的临时秘密n_1，n_2，n_3，结合该类攻击的G_1，G_2游戏中得到的信息，敌手可以通过M_1，M_4，M_7计算出一些参数，如$h(h(r_i||x)||t_1)$。但这些参数均无法为攻击者计算会话钥提供优势，攻击者无法计算出会话钥，因此有

$$Pr[Succ(\mathcal{A},G_3)]=Pr[Succ(\mathcal{A},G_2)]。\quad(4)$$

在该类攻击的游戏G_5下，使用$CorruptEC$4-1 查询，$\mathcal{A}$能够得到存储在用户终端中的信息C_i，D_i，E_i，F_i，结合该类攻击的G_1，G_2，G_3游戏中得到的信息，使用这些信息敌手$\mathcal{A}$仍无法计算出a_i、RID_i和与雾服务器长期密钥x相关的参数，因此无法计算出会话钥，$\mathcal{A}$只能直接猜测用户的口令，根据已有的结果[47]，具有 EC6 攻击能力的敌手定向猜出口令的最大概率为$C'q_s^{s'}$。类似地，使用$CorruptEC$4-2查询，$\mathcal{A}$能够得到存储在智能设备中的信息ID_j，C_j，S_j，其中$S_j=h(ID_j||x||T_j)$。

结合该类攻击前面游戏G_1, G_2, G_3得到的信息,敌手仍无法计算出会话钥需要的参数$h(RID_i||PW_i||n_1||t_1)$和$h(x||n_2)$等。所以*CorruptEC*4-2查询无法为攻击者计算会话钥提供优势。

在该类攻击的游戏G_7下,当执行*CorruptEC*5-2查询时,$\mathcal{A}$能够得到雾服务器中存储的用户和智能设备的注册信息$\{RID_i, r_i\}$和$\{ID_j, h(R_j)\oplus h(x||T_j), T_j\}$。会话钥的计算公式为$SK=h(h(RID_i||PW_i||n_1||t_1)||h(x||n_2)||ID_j||n_3||t_3)$。结合该类攻击前面游戏$G_1$, G_2, G_3得到的信息,敌手无法计算出$h(R_j)$, $h(RID_i||PW_i||n_1||t_1)$, $h(x||n_2)$,无法推算出会话钥,因此有

$$|Pr[Succ(\mathcal{A},G_5/G_7)]-Pr[Succ(\mathcal{A},G_3)]|\leqslant C'q_s^{s'}。\quad(5)$$

2)在会话钥安全攻击的最强隐式攻击之二{EC1, EC3/ EC4, EC6}下,敌手依次进行游戏G_1, G_2, G_4/G_5。

在该类攻击的游戏G_4下,$\mathcal{A}$使用*CorruptEC*3查询能够得到雾服务器的长期秘密x, y,结合该类攻击的G_1, G_2游戏中得到的信息,使用这些信息敌手$\mathcal{A}$可以计算出RID_i,但由于无法计算出r_i, $h(r_i||x)$, n_1, n_2, n_3, $h(R_j)$等与随机数和PUF响应相关的参数,无法为攻击者计算会话钥提供优势。

在该类攻击的游戏G_5下,使用*CorruptEC*4-1查询,与1)的分析一致,攻击者$\mathcal{A}$无法计算出会话钥,只能直接猜测用户的口令,根据已有的结果[47],具有EC6攻击能力的敌手定向猜出口令的最大概率为$C'q_s^{s'}$。同样,使用*CorruptEC*4-2查询无法为攻击者计算会话钥提供优势,因此有

$$|Pr[Succ(\mathcal{A},G_4/G_5)]-Pr[Succ(\mathcal{A},G_2)]|\leqslant C'q_s^{s'}。\quad(6)$$

3)在会话钥安全攻击的最强隐式攻击之三{EC1, EC3/EC5, EC6}下,敌手依次进行游戏G_1, G_2, $G_4/\{G_6, G_7\}$。

在该类攻击的游戏G_4下,使用*CorruptEC*3查询,与2)的分析一致,无法为攻击者计算会话钥提供优势。

在该类攻击的游戏G_6下,使用*CorruptEC*5-2查询,$\mathcal{A}$能够得到用户在注册阶段向注册权威传输的消息$\{Reg_i, Proc_i, RPW_i\}$。但攻击者仍无法推算出r_i, $h(r_i||x)$, n_1, n_2, n_3, $h(R_j)$等与会话钥相关的随机数和PUF响应相关的参数,因此该游戏无法为攻击者计算会话钥提供优势。

在该类攻击的游戏G_7下,使用*CorruptEC*5-2查询,与1)的分析一致,$\mathcal{A}$无法推算出会话钥,因此有

$$Pr[Succ(\mathcal{A},G_4/\{G_6,G_7\})]=Pr[Succ(\mathcal{A},G_2)]。\quad(7)$$

至此,在执行完最强隐式攻击后,$\mathcal{A}$使用*Test*查询后猜测随机位b的值,有

$$Pr[Succ(\mathcal{A},G_{end})]=1/2。\quad(8)$$

由式(1)~(8),可以得到在最强隐式攻击下,敌手破解ISEC-AKA协议语义安全的优势为

$$Adv_{\mathcal{A}}^{\text{ISEC-AKA}}(t)\leqslant q_h^2/|Hash|+2C'q_s^{s'}。$$

证毕.

5.2 启发式安全分析

为验证ISEC-AKA协议在各类隐式攻击下的实际安全性,本节采用启发式分析方法,逐项检验其安全属性的实现情况。

1)相互认证与密钥建立

在隐式攻击{EC1, EC2, EC5, EC6}或者{EC1, EC3, EC5, EC6}下,雾服务器能够通过检验$Auth_1^*$是否与$Auth_1$相同来认证用户,智能设备通过检验$Auth_2^*$是否与$Auth_2$相同来认证雾服务器和用户(这是由于$Auth_2$中同时包含了雾服务器和用户的秘密信息),用户通过检验$Auth_3^*$是否与$Auth_3$相同来认证雾服务器和智能设备。在相互认证之后,参与方协商出会话钥$SK=h(h(RID_i||PW_i||n_1||t_1)||h(x||n_2)||ID_j||n_3||t_3)$,因此,ISEC-AKA协议能够实现相互认证与密钥建立。

2)抗重放攻击

针对重放攻击,敌手$\mathcal{A}$可以执行的隐式攻击是{EC1, EC2, EC5, EC6}或者{EC1, EC3, EC5, EC6}。$\mathcal{A}$能够窃听到协议交换中所有的消息,知道除去临时交互号之外的临时秘密(或者知道雾服务器的长期秘密x, y),知道用户注册时传输的消息(或者雾服务器中存储的用户和智能设备注册信息)。由于临时交互号是由哈希函数所隐藏,具有隐式攻击的$\mathcal{A}$不能从哈希函数中获取临时交互号,因此,ISEC-AKA协议在隐式攻击下能够抵抗重放攻击。

3)抗中间人攻击

要执行中间人攻击,敌手$\mathcal{A}$必须能够修改或伪造交换的消息,并让接收方认可收到的消息为真。对于用户传给雾服务器的消息$Meg_1=\{M_1, TID_i, M_2, M_3, Auth_1, t_1\}$,其中$M_1=n_1\oplus h(h(r_i||x)||t_1)$, $TID_i=RID_i\oplus h(h(x||y)||t_1)$, $M_2=ID_j\oplus h(Auth_1||h(r_i||x)||t_1)$, $M_3=h(RID_i||PW_i||n_1||t_1)\oplus h(h(r_i||x)||ID_j||n_1)$, $Auth_1=h(h(r_i||x)||RID_i||TID_i||n_1||t_1)$,在这些消息中包含了临时秘密、长期秘密、用户的秘密信息。在最强隐式攻击下,$\mathcal{A}$不能同时获得临时秘密和长期秘密,这表明$\mathcal{A}$无法修改或伪造传输的消息,类似地,$\mathcal{A}$也不能修改或伪造其他消息。因此,ISEC-AKA协议在隐式攻击下能够抵抗中间人攻击。

4)抗假冒攻击

在该属性中,敌手$\mathcal{A}$能够执行3类最强隐式攻击:

{EC1, EC2, EC4/EC5-2, EC6}, {EC1, EC3/EC4, EC6}, {EC1, EC3/EC5, EC6}。

如果$\mathcal{A}$执行隐式攻击{EC1, EC2, EC4/EC5-2, EC6}, 就能够知道传输的消息、临时秘密、某个终端中存储的信息或者雾服务器中存储的注册信息, 另外, $\mathcal{A}$也具有在多项式时间内离线猜测口令的能力。$\mathcal{A}$要假冒用户, 必须生成一个有效的$Meg_1=\{M_1,TID_i,M_2,M_3,Auth_1,t_1\}$, 其中$M_1=n_1\oplus h(h(r_i\|x)\|t_1)$, $TID_i=RID_i\oplus h(h(x\|y)\|t_1)$, $M_2=ID_j\oplus h(Auth_1\|h(r_i\|x)\|t_1)$, $M_3=h(RID_i\|PW_i\|n_1\|t_1)\oplus h(h(r_i\|x)\|ID_j\|n_1)$, $Auth_1=h(h(r_i\|x)\|RID_i\|TID_i\|n_1\|t_1)$。$\mathcal{A}$知道临时秘密$\{n_1,n_2,n_3\}$, 也知道时间戳$t_1$和用户的用户终端中存储的信息$\{C_i,D_i,E_i,F_i\}$, 其中$C_i=h(ID_i\|PW_i)\oplus a_i$, $D_i=h(r_i\|x)\oplus h(RID_i\|PW_i)$, $E_i=h(x\|y)\oplus h(RID_i\|ID_i\|PW_i)$, $F_i=h(h(r_i\|x)\|h(x\|y)\|RID_i\|PW_i\|a_i)$, 或者$\mathcal{A}$知道在雾服务器中存储的用户注册信息$\{RID_i,r_i\}$, 其中$RID_i=h(ID_i\|a_i)$。由于口令与随机数一起由哈希函数隐藏, $\mathcal{A}$无法猜出和确定用户口令。由于Meg_1中不仅包含$\mathcal{A}$通过隐式攻击获得的信息, 也包含长期秘密、用户的口令和随机数等信息, 因此$\mathcal{A}$无法生成一个合法的Meg_1来假冒用户。同样地, $\mathcal{A}$既不能假冒智能设备, 因为他无法计算出$h(RID_i\|PW_i\|n_1\|t_1)$和$h(x\|n_2)$, 无法生成一个合法的$Meg_3=\{M_7,M_8,Auth_3,t_3\}$; $\mathcal{A}$也不能假冒雾服务器, 因为他无法计算出$h(x\|n_2)$和$h(r_i\|x)$, 无法生成一个合法的$Meg_2=\{M_4,M_5,M_6,Auth_2,t_2\}$。

如果$\mathcal{A}$执行隐式攻击{EC1, EC3/EC4, EC6}, 就能够窃听到传输的消息及雾服务器的长期秘密x, y, 或者某个终端中存储的信息, 并具有在多项式时间内离线猜测口令的能力。为了假冒用户, 敌手必须构造一个合法的Meg_1。由于Meg_1中还包含了临时秘密、用户的口令和随机数a_i, 要生成一个合法的Meg_1是不可行的, 因此, $\mathcal{A}$无法假冒用户。同样地, 因为$\mathcal{A}$无法计算出临时秘密, 无法生成一个合法的Meg_3或者Meg_2, 因此$\mathcal{A}$也无法假冒雾服务器或者智能设备。

如果$\mathcal{A}$执行隐式攻击{EC1, EC3/EC5, EC6}, 就能够窃听到协议中传输的所有消息和雾服务器的长期秘密x和y, 或者知道用户注册时传输给注册中心的消息, 或者知道雾服务器中存储的用户和智能设备注册信息, 并具有在多项式时间内离线猜测口令的能力。$\mathcal{A}$要假冒用户, 必须生成一个有效的$Meg_1=\{M_1,TID_i,M_2,M_3,Auth_1,t_1\}$。消息$Meg_1$不仅包含$\mathcal{A}$执行{EC1, EC3/EC5, EC6}攻击时得到的秘密信息, 也包含其他秘密如r_i, a_i, n_1, 因此$\mathcal{A}$不能构造一个有效的Meg_1以执行假冒用户攻击。同样, $\mathcal{A}$因为无法计算出临时秘密, 也不能构造有效的消息来假冒雾服务器和智能设备。因此, ISEC-AKA协议在隐式攻击下能够抵抗假冒攻击。

5)抗离线口令猜测攻击

敌手$\mathcal{A}$执行隐式攻击{EC1, EC4-1, EC5, EC6}能够获取协议中传输的所有消息Meg_1, Meg_2, Meg_3, 能够攻陷用户终端并提取存储的信息$\{C_i,D_i,E_i,F_i\}$, $\mathcal{A}$也能够得到用户注册时传给注册中心的信息$\{Reg_i,Proc_i,RPW_i\}$, 或者知道存储在雾服务器中用户的注册信息$\{RID_i,r_i\}$, $\mathcal{A}$也具有在多项式时间内离线猜测口令的能力, 其中$C_i=h(ID_i\|PW_i)\oplus a_i$, $D_i=h(r_i\|x)\oplus h(RID_i\|PW_i)$, $E_i=h(x\|y)\oplus h(RID_i\|ID_i\|PW_i)$, $F_i=h(h(r_i\|x)\|h(x\|y)\|RID_i\|PW_i\|a_i)$, $RID_i=h(ID_i\|a_i)$, $RPW_i=h(ID_i\|PW_i\|a_i)\oplus b_i$。由于$a_i$是$\mathcal{A}$不知道的随机数, 从$C_i$中猜出用户的口令是不可行的。显然, 从$\{D_i, E_i, F_i, RID_i, RPW_i\}$猜测用户口令也是不可行的。因此, ISEC-AKA协议在隐式攻击下能够抵抗离线口令猜测攻击。

6)完美前向保密

敌手$\mathcal{A}$执行EC1攻击时能够窃听到协议中传输的所有消息$\{Meg_1, Meg_2, Meg_3\}$, 执行EC3时能够得到长期秘密, 并假设$\mathcal{A}$能够知道所有参与者(用户、雾服务器、智能设备)的长期秘密, 即$\mathcal{A}$知道了$\{RID_i, a_i, x, y, S_j\}$。在ISEC-AKA协议中, 会话钥计算公式为$SK=h(h(RID_i\|PW_i\|n_1\|t_1)\|\ h(x\|n_2)\|ID_j\|n_3\|t_3)$, 可以看到, SK中不仅包含了三方的长期秘密, 也包含了用户口令PW_i、智能设备身份ID_j和一些动态参数如n_1, n_2, n_3, 显然$\mathcal{A}$执行隐式攻击{EC1, EC3}所得到的信息不足以计算出以前的会话钥, 所以, ISEC-AKA协议在隐式攻击下能够保持完美前向保密。

7)用户匿名性

敌手$\mathcal{A}$执行{EC1, EC2, EC5, EC6}或者{EC1, EC3, EC5, EC6}能够知道协议中传输的所有消息、临时秘密或者长期秘密, 还有用户注册时传输的消息或者存储在雾服务器中的注册信息。要破坏ISEC-AKA协议, $\mathcal{A}$要么能够从窃听的消息中计算出用户的身份ID_i, 或者根据2个不同的消息关联到同一个用户。传输的消息$\{Meg_1, Meg_2, Meg_3\}$都同时包含了临时秘密、长期秘密、用户的口令、多个随机数等, 并用单向哈希函数隐藏这些秘密, 所以直接从窃听的消息中计算出用户的身份ID_i是不可行的。另外, 在$Meg_1=\{M_1,TID_i,M_2,M_3,Auth_1,t_1\}$中不存在固定的消息, 每次会话时$M_1$, TID_i, M_2, M_3, $Auth_1$, t_1都不同, $\mathcal{A}$不能通过多次窃听消息Meg_1来关联到同一个用户, 因此, ISEC-AKA协议在隐式攻击下具有用户匿名性。

8)抗去同步攻击

敌手$\mathcal{A}$执行{EC1, EC2, EC5, EC6}或者{EC1, EC3, EC5, EC6}攻击能够阻止某次会话时传输的消息{Meg_1, Meg_2, Meg_3},并获得一些秘密参数,其目的是让参与各方在下一次认证时失去同步。假设$\mathcal{A}$阻止了消息Meg_1,该消息中包含了与用户身份相关的动态信息$TID_i = RID_i \oplus h(h(x||y)||t_1)$,而在雾服务器中存储的用户的注册信息是$\{RID_i, r_i\}$。在每次认证后,用户的注册信息不需要更新,当$\mathcal{A}$阻止了消息$Meg_1$,只能终止此次认证过程,不影响下一次各方的相互认证。因此,ISEC-AKA 协议在隐式攻击下能够抵抗去同步攻击。

6 性能对比分析

本节比较分析 ISEC-AKA 协议与其他相关认证协议(包括 Wazid 等人[40]、Srinivas 等人[41]、Srinivas 等人[42]、Chen 等人[34]、Zhang 等人[35] 和 Wang 等人[37] 的协议)所实现的安全属性、计算代价、通信代价。

6.1 安全属性对比

表 4 列出了 ISEC-AKA 协议和其他物联网认证协议所实现的安全属性。在这些协议中,Wazid 等人[40] 的协议、Zhang 等人[35] 的协议和本文提出的 ISEC-AKA 协议采用轻量级密码原语,比较适合物联网环境。在 5.2 节的分析可以看到,ISEC-AKA 协议实现了所有的安全属性。Wazid 等人[40] 的协议没有实现 S3, S4, S6, S9 安全属性,Zhang 等人[35] 的协议则没有实现 S4, S6, S7 安全属性。Srinivas 等人[41] 的协议、Srinivas 等人[42] 的协议、Chen 等人[34] 和 Wang 等人[37] 的协议采用公钥密码技术,其中部分协议(Srinivas 等人[41] 的和 Srinivas 等人[42] 的协议)比 Wazid 等人[40] 的协议和 Zhang 等人[35] 的协议实现了更多的安全属性,但仍然不支持 S4, Chen 等人[34] 的协议不支持 S4, S6, S9, Wang 等人[37] 的协议不支持安全属性 S2, S4, S6。这些协议没有实现 S4 的原因是当长期密钥泄露时,攻击者容易执行假冒攻击。从表 4 可以看出,在本文所比较的认证协议中,采用公钥密码技术的认证协议总体上覆盖了更多的安全属性,但其具体表现仍取决于协议设计和所考虑的攻击模型。与此同时,这些认证协议涉及的公钥密码运算会给资源受限的物联网设备带来较大的计算负担,增加认证过程的时间开销。后续计算代价比较将进一步展示所比较协议在计算代价方面的差异。

Table 4 Comparison of Security Attributes Achieved by the Protocols

表 4 协议所实现的安全属性对比

安全属性	协议						
	文献[40]	文献[41]	文献[42]	文献[34]	文献[35]	文献[37]	ISEC-AKA(本文)
S1	√	√	√	√	√	√	√
S2	√	√	√	√	√	×	√
S3	×	√	√	√	√	√	√
S4	×	×	×	×	×	×	√
S5	√	√	√	√	√	√	√
S6	×	√	√	×	×	×	√
S7	√	√	√	√	×	√	√
S8	√	√	√	√	√	√	√
S9	×	√	√	×	√	√	√

注:S1 表示相互认证与密钥建立;S2 表示抗重放攻击;S3 表示抗中间人攻击;S4 表示抗假冒攻击;S5 表示抗离线口令猜测攻击;S6 表示会话钥安全;S7 表示完美前向保密;S8 表示用户匿名性;S9 表示抗去同步攻击;✓表示支持该属性;×表示不支持该属性。

6.2 通信代价对比

为了比较不同认证协议的通信代价,我们假设以下参数位长:身份和临时交互号的位长为 128 b;时间戳的位长为 32 b;对称加密/解密的块大小为 128 b;哈希函数摘要的位长为 256 b;椭圆曲线点长为 320 b(基于 160 b ECC 的安全强度相当于 1 024 b RSA 的安全强度)。这些参数的选择基于当前密码学标准和实际应用中的常见配置,能够反映实际场景中的通信需求。各个认证协议在执行过程中需交换的总位长(通信代价)如表 5 所示。

Table 5 Comparison of Communication Costs

表 5 通信代价比较

协议	总消息数	总通信代价/b
文献[40]	4	4 000
文献[41]	3	2 912
文献[42]	3	3 424
文献[34]	4	4 800
文献[35]	4	3 328
文献[37]	4	3 648
ISEC-AKA(本文)	3	3 168

每个协议的通信代价通过计算其消息交换过程中所有字段的总位长得到。具体计算方法如下:

1)Wazid 等人[40] 的协议。交换 4 个消息,位长分别为 672 b, 1 056 b, 800 b, 1 472 b。总通信代价为 672 + 1 056 + 800 + 1 472 = 4 000 b。

2)Srinivas 等人[41] 的协议。交换 3 个消息,位长分别

为 1 312 b, 1 056 b, 544 b。总通信代价为 1 312 + 1 056 + 544 = 2 912 b。

3）Srinivas 等人[42]的协议。交换 3 个消息，位长分别为 1 440 b, 864 b, 1 120 b。总通信代价为 1 440 + 864 + 1 120 = 3 424 b。

4）Chen 等人[34]的协议。交换 4 个消息，位长分别为 1 504 b, 1 248 b, 928 b, 1 120 b。总通信代价为 1 504 + 1 248 + 928 + 1 120 = 4 800 b。

5）Zhang 等人[35]的协议。交换 4 个消息，位长分别为 1 152 b, 512 b, 512 b, 1 152 b。总通信代价为 1 152 + 512 + 512 + 1 152 = 3 328 b。

6）Wang 等人[37]的协议。交换 4 个消息，位长分别为 1 120 b, 1 120 b, 832 b, 576 b。总通信代价为 1 120 + 1 120 + 832 + 576 = 3 648 b。

7）ISEC-AKA 协议。交换 3 个消息，$Meg_1=\{M_1, TID_i, M_2, M_3, Auth_1, t_1\}$，其位长为 256 + 256 + 256 + 256 + 256 + 32 = 1 312 b，$Meg_2=\{M_4, M_5, M_6, Auth_2, t_2\}$，其位长为 256 + 256 + 256 + 256 + 32 = 1 056 b，$Meg_3=\{M_7, M_8, Auth_3, t_3\}$，其位长为 256 + 256 + 256 + 32 = 800 b。总通信代价为 1 312 + 1 056 + 800 = 3 168 b。

从表 5 可以看出，ISEC-AKA 协议的总通信代价为 3 168 b，仅略高于 Srinivas 等人[41]的协议（2 912 b），但显著低于其他协议（如 Wazid 等人[40]的 4 000 b, Chen 等人[34]的 4 800 b）。这种较低的通信代价主要归因于 ISEC-AKA 协议的消息设计优化。较低的通信代价意味着 ISEC-AKA 协议在实际应用中能够减少网络带宽的占用，特别适用于资源受限的物联网环境。同时，ISEC-AKA 协议在保持较低通信代价的同时，仍然满足高安全性的要求，体现了通信效率与安全性之间的良好平衡。

6.3 计算代价对比

在物联网认证协议中，计算代价是一个关键性能指标，尤其是在资源受限的智能设备上。为了比较不同协议的计算代价，我们考虑了以下 2 个因素：1）忽略异或运算。由于异或运算的执行时间远小于其他密码原语的操作时间，因此在计算代价比较中不予考虑。2）不同硬件环境下的密码原语执行时间。同一密码原语在不同硬件环境中的执行时间可能差异显著。我们采用文献 [48] 提供的硬件环境配置：用户终端（Intel Atom Z3740 4 核处理器、1.86 GHz、2 GB LPDDR3 内存）、雾服务器/网关（Intel Core i5-4210U 处理器、1.70 GHz、16 GB DDR3 内存）和智能设备（四核 Cortex-A7 处理器、1.3 GHz、1 GB 内存）。密码原语在不同的硬件环境中的运行时间如表 6 所示。

Table 6 Approximate Runtime of Cryptographic Primitives in Different Environments

表 6 密码原语在不同环境的近似运行时间 ms

设备	T_h	T_{ECC}	T_{cm}	T_{ed}
用户终端	0.002 162	3.330 9	2.389 1	0.483 4
雾服务器/网关	0.000 038	0.507 8	0.311 8	0.008 2
智能设备	0.058 35	73.931 9	45.468 1	2.955 6

注：T_h 表示哈希函数操作时间，物理不可克隆函数运行时间 T_{PUF} 和弱物理不可克隆函数运行时间 T_{WPUF} 近似等于哈希函数运行时间 T_h；T_{ECC} 表示 ECC 点乘操作时间；T_{cm} 表示切比雪夫混沌映射操作时间；T_{ed} 表示对称加密/解密操作时间。另外，生物特征模糊提取器操作时间 T_{fe} 近似等于 T_{ECC}。

表 7 列出了 7 个认证协议在不同设备上的执行时间和总计算代价。

Table 7 Comparison of Computational Costs

表 7 计算代价对比 ms

协议	用户终端计算代价	雾服务器/网关计算代价	智能设备计算代价	总计算代价
文献 [40]	$9T_h+T_{ed}+T_{fe}\approx 3.833\,8$	$10T_h+2T_{ed}\approx 0.016\,78$	$6T_h+T_{ed}\approx 3.305\,7$	7.156 2
文献 [41]	$13T_h+2T_{cm}+T_{fe}\approx 8.137\,2$	$10T_h\approx 0.000\,38$	$6T_h+2T_{cm}\approx 91.286\,3$	99.423 9
文献 [42]	$16T_h+5T_{ECC}+T_{fe}\approx 20.020\,0$	$12T_h+2T_{ECC}\approx 1.016\,1$	$8T_h+4T_{ECC}\approx 296.194\,4$	317.230 5
文献 [34]	$10T_h+3T_{ECC}\approx 10.014\,3$	$12T_h+4T_{ECC}\approx 2.031\,7$	$3T_h+3T_{ECC}\approx 221.970\,8$	234.016 8
文献 [35]	$6T_h+2T_{ed}\approx 0.979\,8$	$5T_h+6T_{ed}\approx 0.049\,4$	$3T_h+2T_{ed}\approx 6.086\,3$	7.115 5
文献 [37]	$10T_h+3T_{ECC}+T_{fe}\approx 13.345\,2$	$12T_h+T_{ECC}\approx 0.508\,3$	$9T_h+2T_{ECC}+T_{PUF}\approx 148.447\,3$	162.300 8
ISEC-AKA（本文）	$15T_h\approx 0.032\,43$	$14T_h\approx 0.000\,532$	$9T_h+T_{WPUF}\approx 0.583\,5$	0.616 5

注：T_h 表示哈希函数操作时间；T_{PUF} 和 T_{WPUF} 表示物理不可克隆函数和弱物理不可克隆函数运行时间；T_{ECC} 表示 ECC 点乘操作时间；T_{cm} 表示切比雪夫混沌映射操作时间；T_{ed} 表示对称加密/解密操作时间；T_{fe} 表示生物特征模糊提取器操作时间。

无论采用公钥密码技术还是轻量级密码原语的认证协议，在雾服务器/网关上的计算代价差别不大。

这是因为雾服务器/网关是计算资源丰富的设备,能够高效处理复杂的密码运算。

采用公钥密码技术的协议(如 Srinivas 等人[41]、Srinivas 等人[42]、Chen 等人[34]、Wang 等人[37]的协议)在智能设备上的计算代价分别为 91.286 3 ms, 296.194 4 ms, 221.970 8 ms, 148.447 3 ms, 远高于采用轻量级密码原语的认证协议中智能设备的计算代价。

在采用轻量级密码原语的认证协议中,本文提出的 ISEC-AKA 协议的总计算代价约为 0.616 5 ms, 远低于 Wazid 等人[40]和 Zhang 等人[35]的轻量级认证协议的总计算代价。特别是在智能设备上, ISEC-AKA 协议的执行时间仅需 0.583 5 ms。

ISEC-AKA 协议的低计算代价主要归因于其优化的密码原语使用和高效的消息设计。这种低计算代价使得 ISEC-AKA 协议特别适用于资源受限的物联网设备,能够在保证安全性的同时显著提高协议的执行效率。

7 研究局限与未来展望

本文存在一定研究局限。首先,第 2 节描述的攻击模型明确排除了物理层侧信道攻击(如功耗分析、时序攻击、故障注入)、拒绝服务攻击以及量子计算攻击,因此协议在该类攻击下的安全性未经形式化验证;其次,协议的安全性基于哈希函数的抗碰撞性与弱物理不可克隆函数(WPUF)的理想假设,未考虑实际部署中极端环境导致的 PUF 响应不稳定或哈希函数实现的侧信道泄露风险;最后,协议以云-雾协作网络为典型场景,对于无雾服务器支持的纯对等物联网架构或高移动性环境(如跨雾域快速切换),其认证流程的适用性尚需进一步验证。

针对上述局限,未来拟从 2 个方向开展研究:一是扩展威胁模型,将量子计算攻击纳入可证明安全框架,探索量子安全的轻量级认证方案(如基于哈希的后量子签名);二是发展隐式攻击的形式化自动分析工具,使得安全分析能够直接输出给定攻击能力组合下协议是否满足预定安全属性,从而在协议设计阶段即可判定其抗隐式攻击能力,简化验证流程并避免“设计—发现漏洞—修补”的循环。

8 结 论

本文根据安全属性与最强隐式攻击之间的关系,分析了一个经典物联网认证协议的脆弱性。随后提出了一个面向物联网的抗隐式攻击的认证协议,该协议采用轻量级密码原语,巧妙地实现了各种安全属性。为了能够形式化安全分析抗隐式攻击认证协议的安全性,我们扩展了 ROR 模型,形式化证明了提出的协议在扩展 ROR 模型下的会话钥语义安全性。另外,我们采用启发式安全分析方法检验了提出的协议在隐式攻击下能够实现安全属性目标。与经典协议的性能对比表明,提出的协议在所实现的安全属性、计算代价和通信代价上有较大的优势。尽管本文所提出的认证协议适用于多数物联网应用场景,但在特定场景下,可能仍需依据实际情况进行调整与优化。尤其是在高安全需求的零信任物联网环境中,未来的研究将聚焦于为该环境设计更为高效且可靠的认证协议,以充分满足这些特定场景下的需求。

作者贡献声明:郭奕旻负责方案整体设计、实现与理论证明、实验方法制定并撰写论文;姜奇和熊平提出指导意见和参与修改论文。

参 考 文 献

[1] Liu Xinzhong, Cui Jie, Zhang Jing, et al. BAST: Blockchain-assisted secure and traceable data sharing scheme for vehicular networks[J]. IEEE Transactions on Information Forensics and Security, 2025, 20: 4664−4678

[2] Jin Zengwang, Liu Yitong, Diao Jingdong, et al. Privacy protection of cyber-physical system under eavesdropping attack based on sensor-based transmission strategy[J]. SCIENTIA SINICA Informationis, 2025, 55(3): 619−638 (in Chinese)
(金增旺, 刘奕彤, 刁靖东, 等. 窃听攻击下基于传感器传输策略的信息物理系统隐私保护[J], 中国科学: 信息科学, 2025, 55(3): 619−638)

[3] Li Zhecheng, Zhang Bo. A lightweight blockchain-based cross-domain authentication and data sharing scheme for the industrial internet of things[J]. Journal of Computer Research and Development, 2025, 62(10): 2416−2427 (in Chinese)
(李哲成, 张波. 基于区块链的轻量级工业物联网跨域认证与数据共享方案[J]. 计算机研究与发展, 2025, 62(10): 2416−2427)

[4] Jiang Qi, Yang Xue, Wang Jinhua, et al. Device capture resilient authentication and key agreement protocol for IoV[J]. SCIENTIA SINICA Informationis, 2022, 52(12): 2351−2370 (in Chinese)
(姜奇, 杨雪, 王金花, 等. 面向车联网的抗设备捕获认证密钥协商协议[J]. 中国科学: 信息科学, 2022, 52(12): 2351−2370)

[5] Zeng Dake, Badshah A, Tu Shanshan, et al. A security-enhanced ultra-lightweight and anonymous user authentication protocol for telehealthcare information systems[J]. IEEE Transactions on Mobile Computing, 2025, 24(5): 4529−4542

[6] Zhang Qingyang, Zhou Xiaolong, Zhong Hong, et al. Device-side

lightweight mutual authentication and key agreement scheme based on chameleon hashing for industrial Internet of things[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 7895−7907

[7] Hu Mingming, Wang Ding, Li Chen, et al. Behavioral biometrics-based continuous authentication using a lightweight latent representation masked one-class autoencoder[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(3): 1908−1923

[8] Wang Qingxuan, Wang Ding. Understanding failures in security proofs of multi-factor authentication for mobile devices[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 597−612

[9] Wang Ding, He Debiao, Wang Ping, et al. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12(4): 428−442

[10] Dolev D, Yao A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198−208

[11] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels [C]//Proc of the 20th Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2001: 453−474

[12] Guo Yimin, Guo Yajun, Xiong Ping, et al. Deeper insight into why authentication schemes in IoT environments fail to achieve the desired security[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 4615−4627

[13] Wang Chenyu, Wang Ding, Duan Yihe, et al. Secure and lightweight user authentication scheme for cloud-assisted Internet of things[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2961−2976

[14] Kalra S, Sood S K. Secure authentication scheme for IoT and cloud servers[J]. Pervasive and Mobile Computing, 2015, 24: 210−223

[15] Kumari S, Karuppiah M, Das A, et al. A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers[J]. The Journal of Supercomputing, 2018, 74: 6428−6453

[16] Li Chunta, Lee C, Weng Chiyao, et al. A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems[J]. Journal of medical systems, 2016, 40: 233: 1−233: 10

[17] Madhusudhan R, Nayak C. A robust authentication scheme for telecare medical information systems[J]. Multimedia Tools and Applications, 2019, 78: 15255−15273

[18] Garg S, Kaur K, Kaddoum G, et al. Secure and lightweight authentication scheme for smart metering infrastructure in smart grid[J]. IEEE Transactions on Industrial Informatics, 2019, 16(5): 3548−3557

[19] Chaudhry S A, Nebhan J, Yahya K, et al. A privacy enhanced authentication scheme for securing smart grid infrastructure[J]. IEEE Transactions on Industrial Informatics, 2021, 18(7): 5000−5006

[20] Shuai Mengxia, Yu Nenghai, Wang Hongxia, et al. Anonymous authentication scheme for smart home environment with provable security[J]. Computers & Security, 2019, 86: 132−146

[21] Zou Shihong, Cao Qiang, Wang Chenyu, et al. A robust two-factor user authentication scheme-based ECC for smart home in IoT[J]. IEEE Systems Journal, 2021, 16(3): 4938−4949

[22] Li Quanrun, Hsu C, Raymond C, et al. A provably secure and lightweight identity-based two-party authenticated key agreement protocol for vehicular ad hoc networks[J]. Security and Communication Networks, 2019: 7871067

[23] Hajian R, Haghighat A, Erfani S H. A secure anonymous D2D mutual authentication and key agreement protocol for IoT[J]. Internet of Things, 2022, 18: 100493

[24] Braeken A. Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability[J]. Computer Networks, 2020, 181: 107424

[25] Yadav A, Misra M, Pandey P, et al. An improved and provably secure symmetric-key based 5G-AKA protocol[J]. Computer Networks, 2022, 218: 109400

[26] Yang Xu, Yang Xuechao, Yi Xun, et al. Blockchain-based secure and lightweight authentication for Internet of things[J]. IEEE Internet of Things Journal, 2021, 9(5): 3321−3332

[27] Lansky J, Rahmani A M, Ali S, et al. BCmECC: A lightweight blockchain-based authentication and key agreement protocol for Internet of Things[J]. Mathematics, 2021, 9(24): 3241

[28] Chunka C, Banerjee S, Goswami R S. An efficient user authentication and session key agreement in wireless sensor network using smart card[J]. Wireless Personal Communications, 2021, 117(2): 1361−1385

[29] Lee J Y, Oh J H, Kwon D K, et al. PUFTAP-IoT: PUF-based three-factor authentication protocol in IoT environment focused on sensing devices[J]. Sensors, 2022, 22(18): 7075

[30] Hajian R, Erfani S H, Kumari S. A lightweight authentication and key agreement protocol for heterogeneous IoT with special attention to sensing devices and gateway[J]. The Journal of Supercomputing, 2022, 78(15): 16678−16720

[31] Zerrouki F, Ouchani S, Bouarfa H. PUF-based mutual authentication and session key establishment protocol for IoT devices[J]. Journal of Ambient Intelligence and Humanized Computing, 2023, 14(9): 12575−12593

[32] Sun Dazhi, Yangguang. Security of a PUF mutual authentication and session key establishment protocol for IoT devices[J]. Mathematics, 2022, 10(22): 4310

[33] Kandar S, Ghosh A. Smart card based remote user authentication scheme in multi-server environment using Chebyshev chaotic map[J]. Wireless Personal Communications, 2023, 133(4): 2657−2685

[34] Chen Chen, Guo Hua, Wu Yapeng, et al. A novel two-factor multi-gateway authentication protocol for WSNs[J]. Ad Hoc Networks, 2023, 141: 103089

[35] Zhang Liping, Zhu Yue, Ren Wei, et al. Privacy-preserving fast three-factor authentication and key agreement for IoT-based e-health systems[J]. IEEE Transactions on Services Computing, 2023, 16(2): 1324−1333

[36] Shahparian J, Erfani S, Zamanifar A. A secure and efficient authentication and key agreement protocol in blockchain-enabled VANETs[J]. Computers and Electrical Engineering, 2025, 122: 109947

[37] Wang Di, Cao Yue, Lam K, et al. Authentication and key agreement

based on three factors and PUF for UAVs-assisted post-disaster emergency communication[J]. IEEE Internet of Things Journal, 2025, 11(11): 20457−20472

[38] Ji Haoran, Cao Liefeng, Cao Junmin, et al. A lightweight UAV authentication scheme in blockchain-assisted fog networks[J]. Computer Networks, 2026, 275: 111956

[39] Yoon S, Han S, Hwang E. Joint heterogeneous PUF-based security-enhanced IoT authentication[J]. IEEE Internet of Things Journal, 2024, 10(20): 18082−18096

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

[41] 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, 2020, 17(6): 1133−1146

[42] Srinivas J, Das A K, Wazid M, et al. Designing secure user authentication protocol for big data collection in IoT-based intelligent transportation system[J]. IEEE Internet of Things Journal, 2021, 8(9): 7727−7744

[43] Guo Yimin, Zhang Zhenfeng, Xiong Ping, et al. PUF-based lightweight authentication protocols for fog assisted IoT[J]. Chinese Journal of Computers, 2022, 45(7): 1412−1430 (in Chinese)
(郭奕旻, 张振峰, 熊平, 等. 基于 PUF 的轻量级雾辅助物联网认证协议[J]. 计算机学报, 2022, 45(7): 1412−1430)

[44] Guo Yimin, Guo Yajun. CS-LAKA: A lightweight authenticated key agreement protocol with critical security properties for IoT environments[J]. IEEE Transactions on Services Computing, 2023, 16(6): 4102−4114

[45] Guo Yimin, Zhang Zhengfeng, Guo Yajun. Anonymous authenticated key agreement and group proof protocol for wearable computing[J]. IEEE Transactions on Mobile Computing, 2022, 21(8): 2718−2731

[46] Guo Yimin, Zhang Zhenfeng, Guo Yajun, et al. BSRA: Blockchain-based secure remote authentication scheme for fog-enabled Internet of things[J]. IEEE Internet of Things Journal, 2023, 11(2): 3348−3361

[47] Wang Ding, Cheng Haibo, Wang Ping, et al. Zipf's law in passwords[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(11): 2776−2791

[48] Far H A N, Bayat M, Das A K, et al. LAPTAS: Lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT[J]. Wireless Networks, 2021, 27(2): 1389−1412



Guo Yimin, born in 1992. PhD, associate professor. Senior member of CCF. Her main research interests include identity authentication, security protocols, IoT security, and password security.

郭奕旻, 1992 年生。博士, 副教授。CCF 高级会员。主要研究方向为身份认证、安全协议、物联网安全、口令安全。



Jiang Qi, born in 1983. PhD, professor. Senior member of CCF. His main research interests include security protocols, Internet of things security, and data security.

姜　奇, 1983 年生。博士, 教授。CCF 高级会员。主要研究方向为安全协议、物联网安全、数据安全。



Xiong Ping, born in 1974. PhD, professor. His main research interests include information security, machine learning, and privacy computing.

熊　平, 1974 年生。博士, 教授。主要研究方向为信息安全、机器学习、隐私计算。