Wireless Sensor Network Access user Security Authentication Against Composite Attacks*

LIU Zhen[1], LI Bo[2*]
(1.School of Information Engineering, Hubei Light Industry Technology Institute, Wuhan Hubei 430000, China;
2.College of Informatics, Huazhong Agricultural University, Wuhan Hubei 430070, China)

Abstract: Wireless sensor network (WSN) has the feature of open transmission and the corresponding are limited resources, making it vulnerable to composite attacks. Single dimensional data are difficult to meet the requirements of dynamic role identification, and cannot accurately identify malicious access. In addition, the original symmetric secret matrix authentication poses risks of key leakage and node collaborative attacks. Therefore, a wireless sensor network access user security authentication method that is resistant to composite attacks is proposed. An auxiliary database is built and the sliding time window mechanism is combined to calculate the daily role value of users, user traffic characteristics and information entropy statistics are integrated to construct a malicious user behavior identification architecture. For potential malicious access requests, a pseudo secret matrix is constructed based on the global secret matrix, combined with Horner's rule, elliptic curve cryptography, and Vandermonde matrix to complete bidirectional verification key generation and dynamic identity authentication. The simulation results show that the proposed method has a false positive rate of 1 in most simulation scenarios, and can accurately complete wireless sensor network user security authentication with a success rate of 85% to 100%, effectively ensuring user security.

Key words: computer networks and information security; resistance to composite attacks; user security authentication; visit; wireless sensor network
EEACC: 7230 **doi**: 10.3969/j.issn.1004-1699.2026.09.028

抗复合攻击的无线传感网络访问用户安全认证*

刘 震[1], 李 博[2*]
(1.湖北轻工职业技术学院信息工程学院, 湖北 武汉 430070; 2.华中农业大学信息学院, 湖北 武汉 430070)

摘 要: 无线传感网络(Wireless Sensor Network, WSN)开放传输、资源受限, 易遭复合攻击。单一维度数据难满足动态角色辨识需求, 无法精准识别恶意访问, 且原始对称秘密矩阵认证存在密钥泄露与节点协同攻击风险。为此, 提出一种抗复合攻击的无线传感网络访问用户安全认证方法。通过组建辅助数据库, 结合滑动时间窗口机制计算用户日角色值, 整合用户流量特征与信息熵统计量构建恶意用户行为辨识架构; 对潜在恶意访问请求, 基于全局秘密矩阵构造伪秘密矩阵, 结合霍纳法则、椭圆曲线密码学和范德蒙矩阵完成双向验证密钥生成与动态身份认证。仿真结果表明, 所提方法在多数仿真场景下的误报率为 1, 能精准完成无线传感网络用户安全认证, 认证成功率为 85%~100%, 有效保障用户安全。

关键词: 计算机网络与信息安全; 抗复合攻击; 用户安全认证; 访问; 无线传感网络
中图分类号: TM773 **文献标识码**: A **文章编号**: 1004-1699(2026)09-2157-07

无线传感网络(Wireless Sensor Network, WSN)作为物联网的核心支撑技术, 被广泛应用于环境监测和智能城市等多个研究领域中[1-2]。然而, 其开放性传输环境和资源受限特性, 促使无线传感网络面临严峻挑战。近年来, 针对 WSN 的复合攻击频发, 传统单一防御机制难以抵御多维度协同攻击, 导致用户身份认证成为系统安全的薄弱环节。因此, 设计一种抗复合攻击的用户安全认证方法对保障 WSN 安全性和可用性具有重要意义。现阶段, WSN 用户认证[3-4]主要依赖于对称/非对称等技术, 上述方法具有比较强的局限性: 一方面, 密码学方法十分容易受到资源约束, 无法有效应对暴力破解和重放

项目来源: 国家社会科学基金青年项目)16CGL005); 湖北省教育厅科学技术研究项目)B2021368); 湖北省教育厅科学技术研究项目)B2022406); 教育部产学合作协同育人项目
收稿日期: 2025-07-25 **修改日期**: 2025-08-26

攻击的叠加威胁;另外一方面,生物或者行为特征分析方案虽然可以抵御部分伪造攻击,但是缺少对多种攻击类型的动态适应能力,造成认证体系存在隐蔽漏洞。

基于上述方法存在的不足,相关研究者对无线传感网络访问用户安全认证方面的内容展开大量研究,并且取得较为显著的研究成果。例如,喇元等[5]应用改进标识密码算法 SM9(Identity-Based Cryptography Algorithm SM9)有效实现用户安全认证。但该方法主要聚焦于改进 SM9 算法解决证书管理问题及私钥分割存储签名等,未明确提及针对多种复合攻击的全面防御策略,在应对复杂多变的复合攻击场景时,存在安全漏洞。赵宗渠等[6]主要采用双线性映射算法和身份匿签名相结合的方式完成身份认证。但该方法主要侧重于静态的身份认证和会话密钥协商,而缺乏动态的身份认证机制,存在密钥泄露的风险。吴宁等[7]通过椭圆曲线公钥密码算法 SM2(Elliptic Curve Cryptography Algorithm SM2)有效实现系统安全认证。然而,该方法主要基于数字证书和 SM2 算法进行身份认证,缺乏对用户行为特征、流量模式等多维度数据的综合分析,导致恶意访问行为无法被识别。Sahoo 等[8]采用基于雾计算的工业无线传感器网络(Industrial Wireless Sensor Network,IWSN)三因素用户认证方案完成身份认证。虽然通过 ROR 模型证明了会话密钥的保密性,但未充分考虑在节点协同攻击等情况下,密钥面临的泄露风险。

基于上述几种研究方法的局限性,提出一种抗复合攻击的无线传感网络访问用户安全认证方法。

1 无线传感网络访问用户安全认证

1.1 无线传感网络用户恶意访问行为辨识

无线传感网络因开放性和资源受限易受复合攻击,单一维度数据难以全面识别恶意行为。为此,本文构建辅助数据库,基于用户行为特征计算日角色值,结合滑动时间窗口建立角色辨识模型,并融合流量特征与信息熵统计量,实现恶意访问的精准辨识。

辅助数据库中,爬虫网段库的来源主要包括公开的恶意爬虫 IP 段信息发布平台、安全机构定期发布的威胁情报以及网络流量监测中主动识别出的异常高频访问 IP 段集合;收集方法上,一方面通过爬虫技术自动抓取公开平台的 IP 段数据,另一方面结合人工审核机制对监测到的异常 IP 进行筛选,确认后纳入库中,同时设置定期全网扫描任务以补充潜在未知爬虫 IP 段;其更新机制采用动态增量更新与定期全量更新相结合的方式,当有新的威胁情报或异常 IP 被发现时立即增量更新库内容,且每周进行一次全量数据校验与更新,以确保数据的时效性和准确性。用户信息数据集的服务类字段来源于用户注册时填写的服务类型信息、用户实际访问网络服务的行为日志记录以及第三方合作方提供的用户服务属性数据;收集方法包括在用户注册环节通过表单直接收集服务类型信息,在用户访问过程中通过流量解析和行为分析提取实际使用的服务特征,并与第三方数据源通过安全接口进行数据对接和整合;更新机制则是根据用户服务使用情况的变化实时更新行为日志中的服务类字段,同时定期与第三方数据源进行数据同步和比对,对用户注册信息进行复核和更新,以保证服务类字段数据的完整性和准确性。

设定用户的 IP 地址为 x,假设 x 在第 n 天发生访问行为,则可以得到用于 IP 地址 x 在第 n 天的日角色值,应用 $E_n(x)$ 表示,如式(1)所示:

$$E_n(x)=\begin{cases}0 & \text{其他}\\ 1 & x\in F\,|\,x\in G\,|\max\limits_{\text{hour}}(x)\geqslant\beta\,|\,\text{act}_n(x)\geqslant\alpha\end{cases}\tag{1}$$

式中:F 和 G 分别代表辅助数据集中的爬虫网段库和用户信息数据集的服务类字段;$\max\limits_{\text{hour}}(x)$ 代表 IP 地址 x 的单日小时访问量峰值;$\text{act}_n(x)$ 代表 IP 地址 x 在 n 天的活跃小时数;β 代表用户访问次数;α 代表用户活跃时长。

基于累积的 IP 地址行为监测数据,可准确判定用户角色属性。鉴于访问行为的动态特性,单日或短期数据不足以支撑可靠的角色评估。因此,采用滑动时间窗口机制。该机制具备窗口可调和动态滑移特性,用户角色评估结果取决于最近 T 个窗口的每日角色评估值 $E_n(x)$,且赋予临近窗口更高权重。对于第 m 个窗口($m=1,2,\cdots,k$),其权重 $w_m=\dfrac{2(k-m+1)}{k(k+1)}$,满足 $\sum\limits_{m=1}^{k}w_m=1$。用户在第 n 天的角色评估值 $E_n(x)=\sum\limits_{m=1}^{k}w_mE_{n-m+1}(x)$。伴随时间推移,角色评估值呈现显著动态演化,使该模型能有效识别无线传感网络恶意访问行为。定义 $D_n(x)$ 为用户 x 在第 n 天的角色评估值,并对其实施二分处理,临界点设定为 0.5,是基于大量仿真数据的综合分析结果。在仿真过程中,对不同场景下正常用户与恶意用户的角色评估值分布进行了全面统计,发现正常用户的角色评估值大多集中在小于 0.5 的区间,而恶意用户的角色评估值多处于大于 0.5 的区间,二者在该临界点附近有较为明显的区分度,能够较为

精准地将正常访问行为与恶意访问行为划分开来,从而保障恶意访问行为辨识的准确性和有效性。定义用户行为得分函数 $D_n(x)$,其取值区间为[0,1],当 $x\geqslant 0.5$ 时,$D_n(x)=1$,表示其访问行为特征表明源于人类主动操作;当 $x<0.5$ 时,$D_n(x)=0$,则存在较高概率由自动化程序执行。据此,构建式(2)所示的用户角色辨识模型 $R_n(x)$:

$$R_n(x)=\begin{cases}1 & D_n(x)\geqslant 0.5\\ 0 & D_n(x)<0.5\end{cases} \tag{2}$$

设定采用滑动时间窗口机制 T[9],推导出该 IP 地址的流量特征值 $z_n(x)$,对应的计算式如下:

$$z_n(x)=\max[\mathrm{dz}_n(x,m),\mathrm{cz}_n(x,m,T)] \tag{3}$$

式中:m 代表高爆发性流量参数;$\mathrm{dz}_n(x,m)$ 代表用户 IP 在第 n 天的流量函数;$\mathrm{cz}_n(x,m,T)$ 代表时段 T 内该 IP 地址的持续流量函数。

为检测恶意流量,本文采用信息熵特征分析技术,通过计算特定时间窗口内网络流量中 IP 地址的熵值[10]来评估目标地址访问的离散性。其中,用户 IP 地址对应的全部目的 IP 地址的熵特征值 $f_n(D)$ 可表示为式(4)的形式:

$$f_n(D)=-\sum_{i=1}^{n}p_i\ln p_i \tag{4}$$

式中:p_i 代表概率分布函数。

基于用户角色辨识模型 $R_n(x)$ 的识别,将用户流量特征 $z_n(x)$ 和用户信息熵特征 $f_n(D)$ 展开加权,建立用户恶意访问评价函数 I,进而完成用户恶意访问行为精准辨识:

$$I=\frac{1}{2}z_n(x)\times\omega+\frac{1}{2}f_n(D)\times\omega \tag{5}$$

式中:ω 代表权重系数。当式(5)中用户恶意访问评价函数 I 的取值高于 0,则说明用户发生恶意访问。

1.2　抗复合攻击的无线传感网络访问用户安全认证

无线传感网络在认证环节存在安全隐患,若直接使用原始对称秘密矩阵,可能因固定运算系数和有限独立元素导致密钥泄露。为此,设计抗复合攻击的认证协议,以增强网络安全性。

解析用户密钥生成流程,公钥中心需构建两个独立集合 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2$。其中,集合 $\boldsymbol{H}_2$ 用于推导公钥中心的验证参数 K_{ij}。随后,将哈希集合 $\boldsymbol{H}=\{h_{j0},h_{j1},\cdots,h_{jn}\}$ 传输至申请簇首节点[11-12]。利用参数 K_{ij} 对特定矩阵结构实施解析,进而得到矩阵 $[\boldsymbol{D}'\boldsymbol{I}\boldsymbol{D}]^{\mathrm{T}}$。

设定全局秘密矩阵 $\boldsymbol{D}$ 中元素 d_{ij} 为未知数据 x_{ij},针对各个簇首申请节点,构造伪秘密矩阵 $\boldsymbol{D}'$,分析式(6)的推导过程。

$$y=[\mathrm{Id}_1\times x^{(n-1)}+\mathrm{Id}_2\times x^{(n-2)}+\cdots+\mathrm{Id}_{n-1}\times x^{(1)}]\bmod(p) \tag{6}$$

式中:p 代表模数;n 代表正整数;Id_n 代表第 n 个用户的 Id;mod( )代表模运算,即取余运算。

应用霍纳法则,可将变量 x 作为公共因子,从降阶多项式中实施因子分解,将其表示为式(7)的形式:

$$y=\{x\times x\{x\cdots[\mathrm{Id}_1\times x^{(1)}+\mathrm{Id}_2]+\cdots+\mathrm{Id}_{n-1}\}+\mathrm{Id}_n\}\bmod(p) \tag{7}$$

完成上述操作后,对公钥中心展开如下处理:

步骤 1　确定一个素数 s,建立循环群 P 的结构。在 P 上定义椭圆曲线 S,并指定点 C 作为其基点。

步骤 2　选定公称矩阵 $\boldsymbol{D}$ 作为操作对象,执行安全存储操作。该矩阵需严格遵循对称性约束,其维度固定为($n\times n$)。

步骤 3　组建两个哈希函数,分别为 θ_1 和 θ_2。

步骤 4　构造簇首身份识别所需的范德蒙矩阵 $\boldsymbol{ID}$,基于簇首集生成具有单向映射特性的多项式 y_i 和 y_j,将其表示为式(8)的形式:

$$\begin{cases}y_i=r_x^i=\langle\sum_{i=1}^{n}(\mathrm{Id}_i\times x^{(n-i)})\rangle\bmod(p)\\ y_j=r_x^j=\langle\sum_{i=1}^{n}(\mathrm{Id}_i\times x^{(n-j)})\rangle\bmod(p)\rangle\end{cases} \tag{8}$$

步骤 5　依据不同的簇首节点形成不同的伪秘密矩阵元素,应用公钥中心对簇首层广播 P、S、C、θ_1 和 θ_2。

其中,伪秘密矩阵与身份绑定多项式具体计算步骤如下:

步骤 1　伪秘密矩阵生成

对于每个簇首节点,公钥中心利用其 Id 和多项式 y 生成一组系数,这些系数与全局秘密矩阵 $\boldsymbol{D}$ 的某些元素相结合,通过模运算生成伪秘密矩阵 $\boldsymbol{D}'$ 的元素。

步骤 2　身份绑定多项式构造

利用簇首节点的 Id、伪秘密矩阵 $\boldsymbol{D}'$ 的元素以及哈希函数 θ_1 和 θ_2,构造身份绑定多项式。

而各技术间的接口连接方式为:辅助数据库与角色辨识模型通过数据库查询接口连接,辅助数据库提供用户行为特征数据供角色辨识模型计算日角色值 $E_n(x)$;角色辨识模型与流量/信息熵特征分析模块通过数据共享接口或消息队列连接,角色辨识模型输出角色评估值 $D_n(x)$,流量/信息熵特征分析模块利用这些值及实时流量数据计算流量特征值 $z_n(x)$ 和熵特征值 $f_n(D)$;认证协议各步骤之间通过

安全的通信渠道传输数据,如申请者用公钥加密连通身份信息发送给公钥中心,公钥中心解密处理后将加密结果回传。

接下来,给出抗复合攻击的无线传感网络访问用户安全认证的详细操作步骤:

步骤 1 生成一个随机椭圆曲线点 $Q=(x_i,y_i)$,并确定 $Q=(x_i,y_i)$ 为私钥分量,同步确定一个随机值 c;随后,基于 ϕ_i 与 Q 的映射运算,推导出用于用户身份认证的验证凭证 $V_i=\phi_i Q=(V_x,V_y)$。

步骤 2 申请者秘密保存随机数 c,将自身的 V_i 连通身份信息 Id_i 合并后,将 $[V_i \parallel \mathrm{Id}_i]$ 发送给公钥中心。

步骤 3 当公钥中心接收到信息后,采用单向函数多项式 y 和秘密矩阵 $\boldsymbol{D}$ 中元素 d_{ij} 形成一个伪秘密矩阵 $\boldsymbol{D}'$ 中元素 d'_{ij},进而获取伪秘密矩阵。

步骤 4 公钥中心在 **ID** 中任意选取一列,和步骤 3 形成的 $\boldsymbol{D}'$ 联合。进而获取用户 Id_i 的公钥 Y_i 以及公钥中心的验证参数 K_{ij}。

步骤 5 公钥中心发送用户公钥 Y_i、H_1 和 K_{ij} 至申请者。

步骤 6 申请者获取公钥中心反馈的数据后,需要完成验证参数 K_{ji} 的运算。随后,将此计算结果与前述步骤确立的 K_{ji} 基准值展开比对。若比对一致,则进入公钥申请环节。此时,申请者必须严格保密其私钥信息,同时公钥中心将对外发布该用户的公钥数据。反之,若验证未通过,则说明申请无效。

步骤 7 公钥中心将 $\{Y_i,H_1,K_{ij}\}$ 发送给用户。

步骤 8 用户检查 H_1 是否和本地计算的 Id_i 一致,假设一致,则确定身份绑定,依据私钥 Q 和 K_{ij} 展开验证值计算 $\rho'_i=h[Y_i \parallel K_{ij}]$,将其与公钥中心返回的 ρ_i 展开对比,假设两者一致,则用户通过认证;反之,则连接并触发安全警报。

综合以上步骤,通过组建相关数据库结合滑动时间窗口计算用户日角色值,整合流量特征与信息熵设计恶意用户行为辨识架构精准识别恶意行为;对潜在恶意风险未确定用户,基于全局秘密矩阵构造伪秘密矩阵,结合多种技术构造身份绑定多项式,通过公钥中心协同完成双向验证密钥生成与动态身份认证以抵御攻击、保障安全。

2 仿真分析

2.1 仿真设置

为了有效验证抗复合攻击的无线传感网络访问用户安全认证方法的有效性,搭建图 1 所示的无线传感网络用于仿真分析。

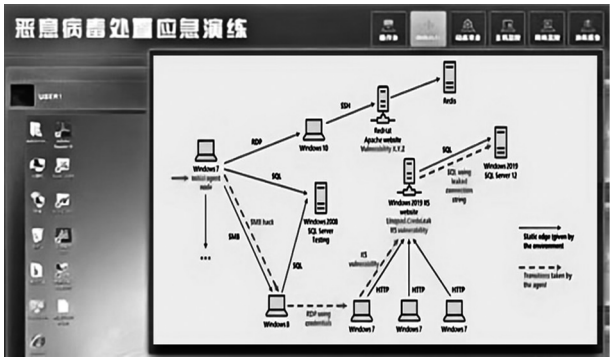

图 1 无线传感网络

无线传感网络的相关仿真参数设置如表 1 所示。

表 1 仿真参数设置情况

参数	设置情况
节点数量/个	80
数据传输距离/m	100
能量扩散因子	2.0
节点接收信息	3
能量吸收函数	0.85
接收能耗系数/J	0.75
发送能耗系数/J	0.75
功率下限/mW	3.5
传送功率衰减	0.10
迭代次数/次	500

此外,所有对比方法均在同一无线传感网络仿真环境下进行,采用相同的节点配置、攻击流量模拟参数及评估指标计算方式。

2.2 无线传感网络用户恶意访问行为辨识性能分析

为了有效验证所提方法的无线传感网络用户恶意访问行为辨识性能,选取文献[5]SM9 门限签名方法和文献[8]雾计算方法作为对比方法,分析不同用户数量下各个方法的误报率变化情况,仿真结果如图 2 所示。

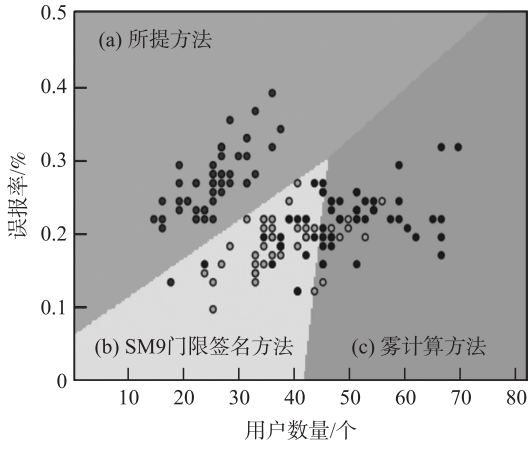

图 2 不同用户数量下各个方法的误报率仿真结果对比

分析图 2 可知,所提方法在用户数量增长过程中,误报率始终维持在极低水平,仅出现 1 次误报,这表明该方法对无线传感网络用户恶意访问行为的辨识具有高度精准性,且不受用户数量变化的影响,展现出优异的稳定性。这种优异性源于动态滑动窗口机制与多维度特征的加权融合,动态滑动窗口机制能够根据实时网络流量动态调整检测窗口大小,更精准地捕捉恶意行为的时间特征;多维度特征加权融合则整合了用户流量特征与信息熵统计量等多方面信息,从不同角度刻画用户行为,有效区分了正常访问与恶意行为,避免了传统单一特征分析方法容易导致的误判问题。SM9 门限签名方法和雾计算方法随用户数量增多,误报率明显上升。用户数量较小时,误报率已有一定数值;用户数量增大后,误报率快速增长。这一对比结果表明,传统方法在处理无线传感网络用户恶意访问行为辨识任务时,其性能受用户规模影响显著,在大规模用户场景下容易频繁出现将正常访问误判为恶意行为的情况,严重影响了系统的可用性。综合来看,所提方法在恶意访问行为辨识方面具有显著优势,其极低的误报率既能有效减少对正常用户的误拦截,又能确保对恶意行为的精准识别,为后续的用户安全认证环节提供了可靠的技术支撑。

2.3　安全性能分析

针对多种不同类型的复合攻击,分析各个认证方法的安全性能,详细的仿真结果如表 2 所示。

表 2　不同无线传感网络访问用户安全认证方法的安全性对比

复合攻击类型	方法		
	所提方法	SM9 门限签名方法	雾计算方法
钓鱼+恶意软件+数据泄露	✓	✓	×
DDoS+漏洞利用	✓	×	✓
物理入侵+网络攻击	✓	✓	✓
假冒身份+水坑攻击	✓	✓	×
深度伪造+钓鱼	✓	×	✓

深入分析表 2 可以看出,所提方法对所有列出的复合攻击类型均具备有效防御能力,展现出全面且稳定的安全防护能力。这得益于所提方法在设计上充分考虑了多种攻击场景的复杂性和多样性,通过综合运用多种安全机制和技术手段,构建了一个较为完善的认证防护体系。例如,基于全局秘密矩阵构造伪秘密矩阵,利用伪秘密矩阵替代原始对称秘密矩阵,结合霍纳法则、椭圆曲线密码学和范德蒙矩阵构造身份绑定多项式,通过公钥中心协同用户完成双向验证密钥生成与动态身份认证,这种独特的设计使得在面对各种复合攻击时,能够从认证流程、数据加密、身份验证等多个层面进行全方位防范,有效阻止攻击者获取用户敏感信息或篡改网络数据。在面对钓鱼+恶意软件+数据泄露这种涉及多种攻击手段的复合攻击时,所提方法能够从认证流程、数据加密、身份验证等多个层面进行防范,有效阻止攻击者获取用户敏感信息或篡改网络数据。在 DDoS+漏洞利用攻击场景下,所提方法能够通过伪秘密矩阵的动态派生,确保网络在遭受大规模流量攻击和利用漏洞的攻击时,依然能够维持正常的认证服务和网络通信;相比之下,SM9 门限签名方法和雾计算方法无法精准抵抗各个类型的复合攻击,在不同复合攻击场景下表现差异较大,整体安全性能不均衡。这表明在实际应用中,所提方法更适合用于无线传感网络的安全认证,能够为网络提供更可靠、更全面的安全保障。

2.4　无线传感网络访问用户安全认证成功率分析

图 3 为无线传感网络访问用户安全认证成功率结果。

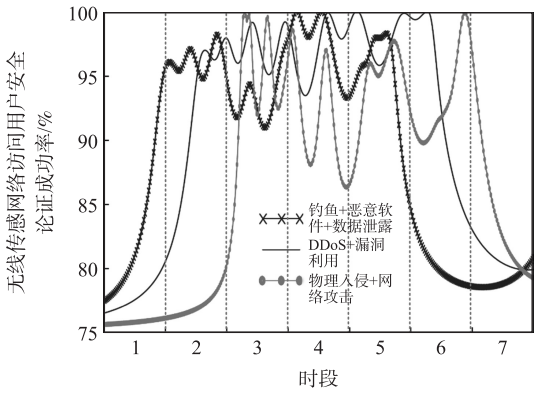

图 3　无线传感网络访问用户安全认证成功率

从图 3 可以清晰地观察到,所提方法在整个观察时段内展现出了卓越的性能,其认证成功率基本维持在 85%~100%的高水准。这主要是因为所提方法通过组建用户信息辅助数据库和 IP 辅助数据库,结合滑动时间窗口机制等计算用户日角色值,能够更精准地刻画用户行为特征,为安全认证提供更准确的依据;同时,整合用户流量特征与信息熵统计量设计恶意用户行为辨识架构,精准辨识恶意访问行为,对合法用户和恶意用户进行有效区分,从而保障了认证流程的顺利进行。表明所提方法在不同时段测试阶段,对无线传感网络访问用户的安全认证流程稳定、有效,能持续可靠地完成认证,保障网络访问安全;同时也更进一步说明面对复合攻击时,所提方法能有效识

别攻击、保障合法用户认证通过,即通过高且稳定的认证成功率,体现出对复合攻击的有效抵抗能力。

2.5 不同复合攻击类型下的性能分析

为了更全面深入地评估所提方法在不同复合攻击场景下的性能表现,仿真选取了钓鱼+恶意软件+数据泄露、DDoS+漏洞利用、物理入侵+网络攻击、假冒身份+水坑攻击、深度伪造+钓鱼这五种典型的复合攻击类型。且仿真环境与前文保持一致,在搭建的无线传感网络中,模拟不同攻击类型的攻击流量和攻击行为。同时,在原有仿真基础上,增加轻量级 ECC 变体、基于机器学习的认证机制作为对比方法。并以认证延迟、计算开销、内存占用、运行时间、防御成功率、攻击成功拦截率为评估指标,仿真结果如表 3 所示。

表 3 不同复合攻击类型下不同方法的性能对比

复合攻击类型	评估指标	所提方法	SM9 门限签名方法	雾计算方法	轻量级 ECC 变体	基于机器学习的认证机制
钓鱼+恶意软件+数据泄露	认证延迟/ms	120	180	150	130	200
	计算开销/J	0.32	0.50	0.40	0.38	0.60
	内存占用/kB	12	18	15	14	22
	运行时间/s	2.3	3.8	3.2	2.8	4.5
	防御成功率/%	98	90	85	92	88
	攻击成功拦截率/%	97	88	82	90	85
DDoS+漏洞利用	认证延迟/ms	150	220	180	160	250
	计算开销/J	0.42	0.65	0.50	0.45	0.75
	内存占用/kB	13	22	18	16	25
	运行时间/s	3.0	4.5	3.8	3.2	5.0
	防御成功率/%	96	82	88	85	80
	攻击成功拦截率/%	95	80	85	83	78
物理入侵+网络攻击	认证延迟/ms	130	190	160	140	210
	计算开销/J	0.38	0.55	0.45	0.40	0.65
	内存占用/kB	13	19	16	15	23
	运行时间/s	2.8	4.0	3.5	3.0	4.8
	防御成功率/%	97	88	86	80	84
	攻击成功拦截率/%	96	86	84	88	82
假冒身份+水坑攻击	认证延迟/ms	110	170	140	130	190
	计算开销/J	0.32	0.48	0.38	0.35	0.58
	内存占用/kB	11	17	14	13	21
	运行时间/s	2.3	3.5	3.0	2.5	4.2
	防御成功率/%	99	92	87	93	89
	攻击成功拦截率/%	98	90	85	91	87
深度伪造+钓鱼	认证延迟/ms	130	200	170	150	230
	计算开销/J	0.40	0.60	0.48	0.42	0.70
	内存占用/kB	14	20	17	15	24
	运行时间/s	2.9	4.2	3.6	3.1	4.9
	防御成功率/%	95	85	83	87	81
	攻击成功拦截率/%	94	83	81	85	79

由表 3 分析可知,在不同复合攻击类型下,所提方法在各项评估指标上优势显著。认证延迟方面,所提方法在五种攻击场景下均低于其他对比方法,认证流程高效;计算开销上,明显低于 SM9 门限签名方法和基于机器学习的认证机制,能量消耗小,适合资源受限的无线传感网络;内存占用也处于较低水平,能有效节省节点内存资源。运行时间上,所提方法最短,可保证认证及时性。在防御成功率和攻击成功拦截率方面,所提方法在各攻击类型下均保持较高水平,能有效抵御和拦截攻击。这充分证明了所提方法在无线传感网络访问用户安全认证中的可靠性和有效性。

3 结束语

本研究针对无线传感网络中复合攻击威胁下的用户安全认证问题,提出了一种创新性安全认证方案。通过系统性仿真与对比分析证实,该方案在恶意访问行为检测方面,采用动态滑动窗口机制结合多维度特征的加权评估模型,在 80 节点规模的仿真环境中表现出色,仿真数据显示在不同用户数量(20~100

节点)下误报率接近零,显著优于传统方法;在安全认证协议设计方面,通过伪秘密矩阵替代原始对称矩阵,结合椭圆曲线密码学与范德蒙矩阵构建的双向验证机制,有效解决了密钥泄露风险,仿真结果表明该方案能够抵御包括 DDoS+漏洞利用、物理入侵+网络攻击等 5 类复合攻击,认证成功率稳定维持在 85%~100%的高水平。此外,本文所提方法的动态滑动窗口机制和多维度特征加权评估模型可根据网络规模灵活调整参数,适用于不同节点密度的网络;椭圆曲线密码学与范德蒙矩阵的组合设计在资源开销上具有可控性,可适配资源受限型与资源相对充裕型等不同类型的无线传感网络,未来研究可进一步优化特征提取算法并在更大规模网络中进行验证。

参考文献:

[1] 邝应攀,钟节辉,柳晓龙. 基于区块链的物联网安全轻量级认证方案[J]. 计算机工程与设计,2024,45(11):3225-3232.

[2] Delwar S T,Aras U,Mukhopadhyay S,et al. The Intersection of Machine Learning and Wireless Sensor Network Security for Cyber-Attack Detection:A Detailed Analysis [J]. Sensors,2024,24(19):6377.

[3] 张应辉,胡凌云,李艺昕,等. 空间信息网络中基于动态撤销机制的安全高效批量认证方案[J]. 通信学报,2022,43(4):164-176.

[4] 阮福,吴珊丹. SM2 密码算法下信息聚合通信安全认证方法[J]. 计算机仿真,2024,41(6):232-236.

[5] 喇元,赵继光,张伟. 基于 SM9 门限签名的电力终端安全认证方案[J]. 电力科学与技术学报,2022,37(4):183-188,226.

[6] 赵宗渠,郭小杰,殷明辉,等. 物联网环境下基于身份匿签密的认证方法研究[J]. 重庆邮电大学学报(自然科学版),2023,35(2):343-351.

[7] 吴宁,蔡杰,梁公豪. 基于 SM2 的电力广域测量系统安全认证方案[J]. 电气传动,2023,53(8):84-90.

[8] Sahoo S S,Mohanty S,Majhi B. An Efficient Three-Factor User Authentication Scheme for Industrial Wireless Sensor Network with Fog Computing[J]. International Journal of Communication Systems,2022,35(3):e5028.

[9] 田腾,石茂林,宋学官,等. 基于滑动窗口的时间序列异常检测方法[J]. 仪表技术与传感器,2021(7):112-116.

[10] 王浩,李兵,贺倩筠,等. 基于改进物元信息熵的计量生产设备健康度评价模型[J]. 中国测试,2022,48(8):164-169.

[11] Madireddy B,Yarrabothu R S. A Stable Cluster Head Selection Algorithm to Minimize the Frequent Failure of the Cluster Head Nodes in Cognitive WSNs[J]. Wireless Personal Communications,2025,140(1):635-657.

[12] 张凌浩,梁晖辉,邓东,等. 面向无线传感器网络的多因素安全增强认证协议[J]. 电子科技大学学报,2023,52(5):699-708.

刘　震(1983—),男,汉族,河南许昌人,硕士,副教授,研究方向:计算机通信技术、信息系统项目管理。2005 年参加工作,现就职于湖北轻工职业技术学院,一直从事计算机专业教学。曾在《安阳工学院学报》上发表多篇学术论文,主持和参与多项省级、国家级教科研项目;受聘多省科技厅技术专家,whliuzhen@foxmail.com;

李　博(1982—),男,汉族,陕西渭南人,硕士,讲师,研究方向:物联网、云计算。2001 年参加工作,现就职于华中农业大学,一直从事计算机专业教学。曾于《Food Hydrocolloids》(SCI),《Food Chemistry》(SCI)等期刊发表多篇学术论文,主持和参与多项省级、国家级教科研项目,libo3213155@163.com。