计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
[doi: 10.15888/j.cnki.csa.010116] [CSTR: 32024.14.csa.010116]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

物联网环境下轻量级双向安全认证协议级联漏洞检测①

张　杰, 景　雯, 王　强

(山西大同大学 计算机与网络工程学院, 大同 037009)
通信作者: 张　杰, E-mail: zhangjie@sxdtdx.edu.cn

摘　要: 在物联网环境中, 由于资源受限, 设备采用随机的节能策略, 如动态睡眠机制, 导致协议交互时序出现不可预测的断开/重连行为. 这种行为使得传统的有限状态机模型难以充分描述状态转换路径, 进而降低了协议一致性偏差的检测率, 并增加了级联漏洞检测的漏检率. 为了解决这一问题, 本文提出了一种轻量级双向安全认证协议级联漏洞检测方法. 该方法利用图卷积网络对物联网环境中轻量级双向安全认证协议的交互图进行建模, 并结合漏洞特征向量计算余弦相似度以进行状态关联检测. 通过动态图建模, 捕获间断通信特征, 并结合余弦相似度量化协议状态与漏洞模式之间的时空关联, 有效克服了节能策略对漏洞检测造成的时间不确定性影响. 基于关联检测结果, 使用马尔可夫决策过程量化漏洞传播的依赖关系, 并构建状态转移概率矩阵来表征拓扑动态. 基于依赖关系, 采用图注意力网络将传播概率转化为节点属性, 并使用多头注意力机制聚合邻居信息. 最终, 结合全局池化实现级联漏洞分类. 实验结果表明, 本文提出的方法在漏洞检测方面具有良好的准确性, 协议一致性偏差稳定在 0.12–0.21 范围内, 漏检率始终低于 0.5%, 展现出理想的检测效果.

关键词: 物联网环境; 轻量级; 双向安全认证协议; 级联漏洞; 检测方法

引用格式: 张杰,景雯,王强.物联网环境下轻量级双向安全认证协议级联漏洞检测.计算机系统应用. http://www.c-s-a.org.cn/1003-3254/10116.html

Lightweight Bidirectional Security Authentication Protocol Cascade Vulnerability Detection in the IoT Environment

ZHANG Jie, JING Wen, WANG Qiang

(School of Computer and Network Engineering, Shanxi Datong University, Datong 037009, China)

Abstract: In the Internet of Things (IoT) environment, resource-limited devices adopt random energy-saving strategies, such as dynamic sleep mechanisms, which lead to unpredictable disconnection and reconnection behaviors in protocol interaction timing. Such behavior makes it difficult for traditional finite state machine models to fully describe the state transition path, thereby reducing the detection rate of protocol consistency deviation and increasing the missed detection rate of cascade vulnerabilities. To address this problem, a lightweight bidirectional security authentication protocol cascade vulnerability detection method is proposed. Graph convolutional networks are employed to model the interaction graphs of lightweight bidirectional security authentication protocols in the Internet of Things environment, and cosine similarity is calculated based on vulnerability feature vectors to perform state association detection. Through dynamic graph modeling, intermittent communication characteristics are captured, and cosine similarity is used to quantify the spatiotemporal correlation between protocol states and vulnerability patterns, which effectively mitigates the impact of temporal uncertainty caused by energy-saving strategies on vulnerability detection. Based on the results of association detection, a Markov decision process is adopted to quantify the dependency relationships of vulnerability propagation, and

① 基金项目: 山西省基础研究计划 (202403021221180); 教育部产学合作协同育人项目 (221002722062521); 山西大同大学教学改革项目 (XJG2023269)
收稿时间: 2025-08-26; 修改时间: 2025-10-10, 2025-11-03; 采用时间: 2025-11-07; csa 在线出版时间: 2026-03-13

a state transition probability matrix is constructed to characterize topological dynamics. According to the dependency relationships, a graph attention network is utilized to transform propagation probabilities into node attributes, and a multi-head attention mechanism is employed to aggregate neighboring information. Ultimately, cascade vulnerability classification is achieved by combining global pooling. The experimental results show that the proposed method achieves good accuracy in vulnerability detection. The protocol consistency deviation remains stable within the range of 0.12–0.21, and the missed detection rate is consistently lower than 0.5%, demonstrating effective detection performance.

Key words: Internet of Things (IoT) environment; lightweight; bidirectional security authentication protocol; cascade vulnerability; detection method

双向安全认证协议是保障物联网设备间合法通信的核心机制, 其安全性直接影响物联网系统的整体防护能力. 随着物联网 (Internet of Things, IoT) 在智能家居、工业控制、智慧城市等领域的广泛应用, 轻量级认证协议因其低开销特性得到广泛部署. 然而, 资源受限设备常采用动态休眠等随机性能源管理策略, 导致协议交互过程中出现不可预测的断连与重连行为. 这种由节能策略导致的时序不确定性问题, 使得传统基于有限状态机的建模方法难以准确描述非连续状态转移路径, 进而引发协议一致性偏离, 显著提高了级联漏洞的漏检风险.

在物联网漏洞检测领域, 国内外学者已开展了多方面研究. 国际上, Masud 等人[1]提出了一种生成式模糊测试方法, 通过深度生成模型自动创建测试用例以发现物联网协议漏洞. 该方法在协议一致性测试中表现出色, 但其核心机制仍依赖于输入空间的随机探索, 对协议状态机在节能策略下的动态演化行为缺乏专门建模. Hulayyil 等人[2]系统比较了多种机器学习算法在物联网设备漏洞检测中的性能, 发现基于树模型的方法在静态特征分类上效果最佳. 然而, 该研究主要关注设备固件层面的静态特征提取, 未能充分考虑设备间认证协议交互过程中因动态休眠引发的时序异常.

在国内研究中, 王璇等人[3]将 DistilBert 预训练模型与 LSTM 序列建模相结合, 实现了代码语义层面的漏洞特征提取. 但该方法依赖于完整的代码上下文, 难以适用于资源受限设备中经过裁剪的轻量级协议实现. 潘睿等人[4]构建了多维度漏洞关键词库, 通过正则表达式匹配实现行级别的快速漏洞筛查. 这种基于模式匹配的方法虽然效率较高, 但无法识别由多个微小缺陷通过复杂交互引发的复合型漏洞. 陈旭等人[5]首次将双曲空间几何引入图神经网络, 利用双曲图卷积网络捕捉代码切片中的层次化结构特征. 该方法在复杂代码依赖关系建模上取得进展, 但未考虑物联网设备动态休眠导致的协议状态空间时变特性. 曹子亨等人[6]提出结合双向数据流分析与图抽象嵌入的漏洞检测框架, 通过同时考虑前向和后向数据传播路径增强漏洞上下文感知. 这一设计提升了传统数据流分析的完整性, 但其图结构生成仍基于静态代码分析, 难以适应物联网协议运行时的拓扑动态变化.

由于物联网设备的随机节能策略导致协议交互时序不稳定, 轻量级双向认证协议面临状态转换路径建模的严峻挑战. 动态睡眠机制引发的非预期断开/重连行为会破坏协议交互的连续性, 使得基于传统有限状态机的检测方法难以准确捕获异常状态迁移, 最终造成协议一致性验证偏差和级联漏洞的漏检问题. 因此, 提出物联网环境下轻量级双向安全认证协议级联漏洞检测方法. 本文突破传统有限状态机对时序中断场景的建模局限, 将图卷积网络与动态图建模引入协议漏洞检测领域, 通过时空关联分析解决节能策略导致的检测盲区. 融合余弦相似度度量与马尔可夫决策过程, 建立协议状态与漏洞模式的概率化关联模型, 并运用图注意力网络实现漏洞传播路径的可解释性建模. 通过多头注意力机制实现拓扑动态与节点属性的联合优化, 最终构建端到端的级联漏洞分类框架, 显著提升间断通信环境下的检测鲁棒性.

1 轻量级双向安全认证协议级联漏洞检测

1.1 物联网环境下的交互图建模

考虑到物联网设备间认证通常为多轮消息交互, 因此, 为了对这种交互时序和拓扑变化进行捕捉, 选择将物联网设备间的双向认证过程抽象为动态有向图, 通过图卷积网络 (graph convolutional network, GCN)

聚合邻居信息[7]. 物联网环境下交互图建模能直观刻画设备间的动态认证流程, 包括消息交换时序和状态依赖关系, 尤其适合描述资源受限设备因节能策略产生的非连续通信特征. 通过可视化协议交互路径, 可清晰识别潜在的状态跳变异常和时序冲突点, 为后续漏洞检测提供拓扑结构基础. 交互图的时间维度建模能力可有效捕捉动态休眠机制引发的断连重连行为, 弥补传统有限状态机在非确定性场景中的描述缺陷.

结合漏洞模式特征向量计算余弦相似度, 实现协议状态与已知漏洞的时空关联建模. 在动态有向图中$G_t=(V,E_t,A_t,X_t)$, 假设节点集合V包含了参与轻量级双向安全认证的设备, $v_i\in V$对应第 i 个设备. 边集合E_t包含了第 t 轮交互的消息传输消息, $e_{ij}^t\in E_t$代表设备v_i在t时刻向v_j发送消息. A_t代表邻接矩阵, 用于动态更新以反映双向安全认证交互的拓扑变化, X_t代表节点特征矩阵, 包括编码设备状态以及认证参数[8]. 然后通过 GCN 聚合邻居设备的特征, 捕捉局部交互上下文, 假设邻接矩阵的归一化结果为$\hat{A}_t$, 则具体特征聚合表达式如式 (1)、式 (2) 所示:

$$H_t^1=ReLU\left(\hat{A}_t,X_t,W^0\right) \tag{1}$$

$$H_t^{l+1}=ReLU\left(\hat{A}_t,H_t^1,W^l\right) \tag{2}$$

其中, H_t^1代表第 1 层 GCN 输出的节点特征矩阵, 表示物联网设备在第 1 层聚合后的状态向量, W^0代表该层的可训练权重矩阵[9]. H_t^1代表第 1 层 GCN 输出的节点特征矩阵, W^l代表第 l 层的可训练权重矩阵, 用于逐层提取跨设备的认证交互模式.

将重放攻击以及密钥泄露等已知的漏洞模式编码为特征向量, 通过余弦相似度计算协议状态与漏洞的关联[10]. 具体计算公式如式 (3) 所示:

$$Sim\left(v_i^t,P_k\right)=\frac{H_{i,t}^L\cdot P_k}{\left\|H_{i,t}^L\right\|\cdot\left\|P_k\right\|} \tag{3}$$

其中, $H_{i,t}^L$代表设备在最终层的特征向量, P_k代表已知漏洞模式 k 的特征向量. $Sim\left(v_i^t,P_k\right)$的值越大, 代表设备在 t 时刻的状态与漏洞 k 的匹配程度越高, 最终得到协议状态与漏洞的关联集合S.

采用动态有向图建模物联网双向认证协议, 通过 GCN 聚合设备交互特征捕捉非连续通信行为. 邻接矩阵和节点特征矩阵动态更新认证拓扑及状态, 逐层提取跨设备交互模式. 结合漏洞特征向量计算余弦相似度, 实现协议状态与已知漏洞的时空关联检测, 从而有效解决节能策略导致的时序不确定性对漏洞检测的影响.

1.2 级联漏洞传播依赖关系量化分析

在上述轻量级双向安全认证协议交互图建模的基础上, 本文借助马尔可夫决策过程 (Markov decision process, MDP), 以设备状态、漏洞触发状态及网络拓扑为状态空间, 以消息交互类型作为动作空间[11]. 通过构建状态转移概率矩阵刻画漏洞传播的动态依赖关系, 为后续的漏洞分类与检测提供帮助.

这种方法在国内外已有应用, 尤其是在网络安全和漏洞检测领域. 例如, Ruiz-Torrubiano 等人[12]使用 MDP 对局部搜索元启发式算法进行建模, 通过分析状态转移概率来优化算法的搜索策略. 这种方法为我们提供了一种强大的工具, 可以用来分析和预测网络安全事件的发展.

本研究通过将 MDP 与图结构学习相融合, 利用状态转移概率矩阵对漏洞传播的动态依赖关系进行量化建模. 这种融合方法既能准确刻画漏洞传播的动态演变特征, 又可通过图结构学习技术深入挖掘潜在的级联漏洞模式, 为物联网协议安全分析领域提供了一种具有理论依据和实践价值的分析框架.

首先将物联网设备的协议交互状态、漏洞触发状态及网络拓扑关系联合建模为状态空间, 每个状态由三元组$s=(s_d,s_v,s_n)\in S$进行表示. 其中, s_d代表协议参与设备的当前认证阶段, s_v代表设备是否触发特定漏洞, s_n表示当前网络之间的连接关系[13]. 将动作空间A直接映射为协议中的消息交互类型, 具体包括发送认证请求a_1、发送密钥材料a_2以及发送认证完成消息a_3. 定义状态转移概率$P(s'|s,a)$为在交互状态s的条件下执行协议交互动作a后状态转移到s'的概率[14]. $P(s'|s,a)$的具体分解表达式如下所示:

$$P(s'|s,a)=P_d\left(s'_d|s_d,a\right)\cdot P_v(v'|v,a)\cdot P_d(s'_n|s_n,a) \tag{4}$$

其中, $P_d\left(s'_d|s_d,a\right)$代表协议状态转移概率, $P_v(v'|v,a)$代表漏洞触发概率, $P_d(s'_n|s_n,a)$代表网络拓扑转移概率[15]. s_d和s'_d分别表示物联网设备在认证协议中的当前阶段和下一阶段, v和v'分别表示设备当前是否触发特定漏洞的布尔向量, s_n和s'_n分别表示物联网设备间通信链路的当前状态和下一状态[16]. 通过 MDP 求解最优策略X^*从而最大化攻击者的累积奖励. 具体策略表达式如式 (5) 所示:

$$X^* = \arg\max E\left[\sum_{t=0}^{T}\gamma^t R(s_t,a_t,s_{t+1})|\pi\right]P(s'|s,a) \quad (5)$$

其中, γ代表折扣因子, T代表攻击步数. $R(s_t,a_t,s_{t+1})$代表执行消息交互动作a_t后, 从状态s_t转移到s_{t+1}时所得到的即时反馈值.

1.3 级联漏洞分类检测

通过马尔可夫决策过程建立的漏洞传播量化模型为图注意力网络提供了结构化输入特征, 将状态转移概率与拓扑动态性转化为可学习的节点属性. 将 MDP 量化的传播依赖关系嵌入图结构学习, 利用漏洞传播概率等动态特征初始化节点属性, 引入图注意力网络 (graph attention network, GAT) 生成节点级表示, 并结合全局池化操作实现图级分类, 来判断是否存在级联漏洞.

将 MDP 量化的传播依赖关系嵌入图结构学习, 是以系统状态、漏洞触发状态及网络拓扑构成 MDP 状态空间, 以消息交互类型为动作空间构建状态转移概率矩阵来刻画漏洞传播动态依赖关系, 接着把状态转移概率作为图结构中节点间边的权重, 将漏洞传播概率等动态特征初始化节点属性, 同时把 MDP 中状态对应到图节点, 如此就把 MDP 量化的传播依赖关系融入图结构, 以便后续利用图注意力网络进行节点级表示生成和级联漏洞分类.

将最优求解策略X^*输入到图注意力网络中, 图节点表示协议状态或动作, 其特征向量为漏洞传播概率, 边表示状态或动作之间的依赖关系. 将级联漏洞传播概率编码为节点特征, 则使用 K 个独立注意力头聚合邻居信息, 从而生成节点级表示. 具体表达式如式 (6) 所示:

$$h_i' = \|_{k=1}^{K}\sigma\left(\sum_{j\in N(i)} a_{ij}^k W^k x_j\right) \quad (6)$$

其中, $N(i)$代表节点i的邻居集合, σ代表激活函数. h_i'代表节点 i 的最终嵌入表示, 反映了协议状态或动作在漏洞触发链中的重要性. a_{ij}^k代表第 k 个注意力头下节点 j 对节点 i 的注意力系数, 高a_{ij}^k对应高概率的漏洞依赖路径. W^k代表第 k 个注意力头的可训练权重矩阵, x_j代表X^*中邻居节点 j 的初始特征向量[17]. 结合全局平均池化操作生成图表示z_G并输出分类器中, 对级联漏洞进行分类识别. 具体表达式如式 (7) 所示:

$$\hat{y} = \sigma\left(w^{\mathrm{T}} z_G + b\right)h_i' \quad (7)$$

其中, $\hat{y}$代表级联漏洞存在概率, w^{T}和b分别代表分类器的可训练权重和偏置, 用于将图表示映射到二分类空间. GAT 的损失函数L表达式如式 (8) 所示:

$$L = -\frac{\sum_{n=1}^{N}[y_n\log\hat{y}_n + (1-y_n)\log(1-\hat{y}_n)] + \lambda\|\Theta\|_2}{N} \quad (8)$$

其中, y_n代表真实标签, 1 代表协议交互图中存在可触发的级联漏洞, 0 代表不存在. $\hat{y}_n$代表模型对第 n 个样本的预测概率, 表示存在级联漏洞的概率. 交叉熵损失衡量了模型预测概率与真实标签之间的差异. 当模型预测准确时, 交叉熵损失较小; 预测不准确时, 损失较大. N代表训练样本数量, $\lambda\|\Theta\|_2$代表 L2 正则化项, 用于惩罚过大的模型参数Θ[18]. L2 正则化通过惩罚过大的模型参数, 防止过拟合, 从而提高模型的泛化能力. 整个损失函数L是二分类交叉熵损失和 L2 正则化项的加权和. 通过最小化这个损失函数, 模型可以学习到更准确的级联漏洞检测能力, 同时避免过拟合.

通过采用上述损失函数对 GAT 模型进行训练, 最终模型可以输出对应的二分类结果, 从而判断是否存在级联漏洞. 这种方法利用图注意力机制捕捉协议状态之间的复杂依赖关系, 并通过优化损失函数提高检测的准确性和鲁棒性.

2 测试实验

2.1 实验准备

为全面评估本文方法的性能, 构建了自有的仿真测试环境与数据集, 并引入一个公开的开源基准数据集进行对比验证, 以确保结果的可靠性与泛化能力.

(1) 实验环境与自建数据集

实验共部署 200 个物联网设备节点, 包括终端设备、边缘网关和云服务器这 3 类, 其中, 云服务器作为协议认证中心占比 10%. 所有节点均通过互联网实现数据汇聚和远程管理, 其中, 150 个节点通过互联网承载的 LoRaWAN 进行无线连接, 50 个节点通过互联网基础的有线以太网连接. 边缘网关同时支持 WiFi 6 和 5G 蜂窝网络接入互联网, 实现无线异构网络的智能切换. 云服务器部署在互联网云端, 通过 HTTPS 加密通道与各节点建立安全连接. 实验特别模拟了互联网环境下常见的网络抖动和延迟波动场景, 在边缘网关配置了基于 SD-WAN 的动态路由策略, 以应对互联网

传输的不确定性. 所有设备均注册至互联网 DNS 系统, 实现基于域名的服务发现和动态寻址. 具体网络局部拓扑结构如图 1 所示.

实验选择 3 种典型轻量级双向认证协议作为测试对象, 具体参数如表 1 所示.

为了进行级联漏洞检测, 实验对正常流量以及恶意流量进行模拟. 设定每个终端设备每 5 s 发送 1 条认证请求, 具体包括时间戳、设备 ID 和随机数. 设定边缘网关每 1 s 聚合 10 条请求并将其转发至云服务器, 以此模拟出批量认证场景. 对于恶意流量, 实验模拟的攻击类型包括重放攻击、畸形报文以及侧信道攻击. 设定每分钟发送 5 条重复认证消息, 并每 10 min 注入 1 条长度超限的报文, 通过模拟功耗分析, 每 30 min 尝试进行 1 次密钥推断.

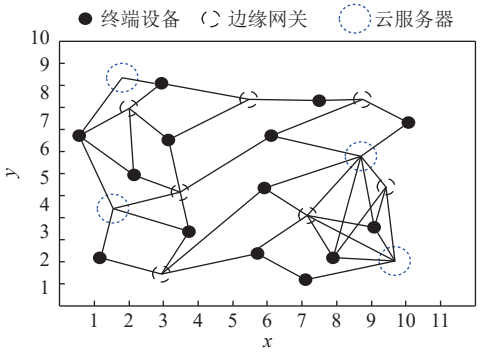

图 1 物联网认证网络局部拓扑结构

表 1 轻量级双向认证协议参数

协议名称	密钥长度 (bits)	认证轮次	消息完整性机制	已知漏洞类型 (注入比例)
TinySec	64	2	CRC-16	重放攻击 (30%)、弱密钥 (20%)
ContikiMAC	96	3	HMAC-SHA1 (截断)	缓冲区溢出 (25%)、身份伪造 (15%)
LwM2M-DTLS	128	4	AES-CCM (128-bit)	侧信道攻击 (20%)、协议降级 (10%)

实验构建的数据集包含 1 250 000 条协议交互记录, 覆盖了正常通信以及攻击场景. 在采用本文方法进行漏洞检测时, 借助 GCN 网络对邻居信息进行聚合, 由此实验得到的部分特征聚合结果如表 2 所示.

表 2 基于 GCN 的物联网设备双向认证特征聚合结果

时间步	节点ID	节点原始特征向量	GCN聚合权重	聚合后特征向量
t=1	Device_A	[0.82, 0.15, 0.03]	[0.6, 0.4]	[0.79, 0.17, 0.04]
	Device_B	[0.75, 0.20, 0.05]	[0.7, 0.3]	[0.79, 0.17, 0.04]
t=2	Device_A	[0.79, 0.17, 0.04]	[0.5, 0.3, 0.2]	[0.83, 0.15, 0.03]
	Device_B	[0.79, 0.17, 0.04]	[0.4, 0.4, 0.2]	[0.78, 0.17, 0.04]
t=3	Device_A	[0.83, 0.15, 0.03]	[0.4, 0.3, 0.2, 0.1]	[0.87, 0.12, 0.02]
	Gateway	[0.90, 0.08, 0.02]	[0.5, 0.3, 0.1, 0.1]	[0.89, 0.10, 0.02]

结合上述特征聚合操作可以实现双向安全认证协议交互图建模, 然后通过量化级联漏洞传播依赖关系并结合图注意力网络对级联漏洞发生概率进行计算, 从而实现漏洞检测. 对此, 实验以基于 DistilBert-LSTM 与多项朴素贝叶斯的漏洞检测方法以及基于关键词的行级别漏洞检测方法作为对比对象, 通过记录不同检测方法得到的实际检测结果与数据集标注之间的一致性, 从而实现实验对比.

(2) 开源基准数据集

为进行公平和可复现的对比, 额外选用了物联网安全领域广泛使用的公开数据集 IoT-VVD (IoT vulnerability and vulnerability detection dataset). 该数据集包含真实的物联网网络流量和各种攻击日志, 从中提取了与双向认证协议相关的交互流量及对应的漏洞标签, 共构建约 800 000 个有效的协议交互图样本用于本次对比实验.

所有实验均在相同的硬件平台 (NVIDIA RTX 3080) 和软件环境 (PyTorch 1.12) 下进行. 数据集按 7:2:1 的比例随机划分为训练集、验证集和测试集.

2.2 结果分析

(1) 级联漏洞检测结果

本文结合 GAT 全局池化操作得到的级联漏洞判断结果如图 2 所示.

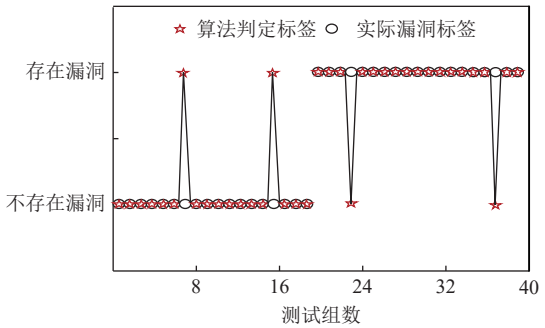

图 2 级联漏洞检测结果

从图 2 级联漏洞检测结果可知, 算法判定标签与实际漏洞标签在多数测试组中高度重合. 在测试组 8、16 等场景下, 算法精准捕捉到实际存在的漏洞; 在测试组 24、32 等场景, 也能正确识别无漏洞状态. 以此可以证明本文结合 GAT 全局池化操作的级联漏洞检测

方法能够有效识别物联网轻量级双向安全认证协议中的级联漏洞, 在异构网络切换等复杂场景中展现出优势, 可快速且准确地判断配电系统级联漏洞状况, 为保障配电系统稳定运行提供可靠依据.

(2) 协议一致性偏离度

在物联网动态环境中, 协议实现与标准规范的潜在偏差会形成安全盲区. 轻量级协议受设备节能策略影响易产生异常状态转移, 通过一致性偏离度测试可量化协议实际运行与理论模型的差异, 识别因时序错乱或状态跳变导致的隐蔽漏洞路径, 为级联漏洞检测提供关键判定依据. 并且将本文方法与静态分析技术、图嵌入技术进行对比测试, 3 种方法的协议一致性偏离度结果如表 3 所示.

表 3 协议一致性偏离度

迭代次数	本文方法	静态分析技术	图嵌入技术
50	0.15	0.42	0.38
100	0.18	0.51	0.45
150	0.12	0.39	0.41
200	0.14	0.47	0.36
250	0.20	0.53	0.49
300	0.17	0.44	0.42
350	0.13	0.50	0.37
400	0.19	0.46	0.44
450	0.16	0.41	0.50
500	0.21	0.55	0.47
550	0.15	0.48	0.39
600	0.18	0.52	0.43

从表 3 数据可以看出, 本文方法在协议一致性偏离度上表现出显著优势. 在所有迭代次数下, 本文方法的偏离度始终稳定保持在 0.12–0.21 的低水平区间, 波动幅度不超过 0.09, 展现出良好的稳定性. 相比之下, 静态分析技术和图嵌入技术的偏离度数值普遍高出 2–3 倍, 且波动范围分别达到 0.39–0.55 和 0.36–0.50, 显示出明显的检测不稳定现象. 特别是在高迭代次数条件下, 当静态分析技术偏离度攀升至 0.55 时, 本文方法仍能维持在 0.21 以下, 充分证明其在应对物联网动态环境时, 能更精准地捕捉协议实际运行状态与理论模型的一致性关系, 有效避免了传统方法因非连续通信导致的检测偏差问题.

(3) 漏检率

在物联网动态环境中, 设备非连续通信行为会引发隐蔽漏洞路径. 漏检率测试能有效评估检测模型对异常状态转移的识别能力, 验证方法在协议时序紊乱时的鲁棒性, 为级联漏洞检测效果提供量化依据, 确保安全认证协议在实际部署中的可靠性. 3 种方法的漏检率结果如图 3 所示.

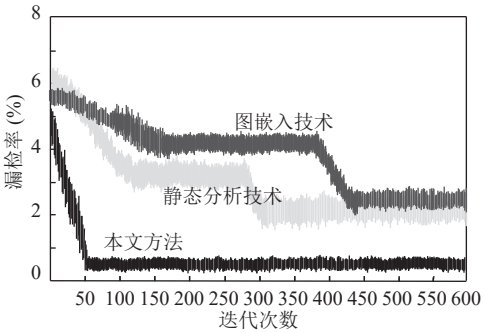

图 3 不同检测方法的漏检率对比结果

从图 3 中可清晰地看出, 本文方法在漏检率方面优势显著. 在迭代次数为 50 时, 本文方法漏检率近乎为 0.5%, 而静态分析技术约为 5.5%, 图嵌入技术约为 6%; 迭代至 100 次, 本文方法仍维持极低水平, 静态分析技术约 5%, 图嵌入技术约 4.8%; 迭代到 400 次, 本文方法漏检率依旧趋近于 0, 静态分析技术约 3%, 图嵌入技术约 3.8%; 直至迭代到 600 次, 本文方法始终保持在极低漏检率状态, 静态分析技术约 2.2%, 图嵌入技术约 2.8%. 这表明本文方法在整个迭代过程中, 对异常状态转移识别精准度极高, 能有效应对物联网动态环境下设备非连续通信引发的隐蔽漏洞路径, 相比其他两种方法, 漏检率控制能力更强, 鲁棒性更佳, 为级联漏洞检测提供了更可靠的保障.

选取了以下 3 种分别代表国际最新研究方向、国内经典静态分析与先进图学习模型的方法.

Generative-Fuzzer: Masud 等人[1]提出的生成式模糊测试驱动漏洞检测方法. 该方法代表了一种主动式的、基于变异的国际前沿检测范式.

NB-LSTM: 王璇等人[3]提出的基于 DistilBert-LSTM 与多项朴素贝叶斯的漏洞检测方法. 该方法代表了国内基于代码语义和序列建模的经典静态分析技术.

Hyper-GCN: 陈旭等人[5]提出的基于双曲图卷积网络的切片级漏洞检测方法. 该方法代表了国内利用新兴图神经网络处理复杂代码结构的最新进展.

采用 $F1$-Score 作为检测精度的核心指标, 以平衡准确率与召回率; 同时汇报协议一致性偏离度与漏检率, 以综合评估方法在动态物联网环境下的鲁棒性.

为了清晰对比本文方法与所选前沿工作的性能, 在开源数据集 IoT-VVD 上进行了测试, 关键结果汇总于表 4.

表 4 不同方法在 IoT-VVD 数据集上的性能对比

方法	*F*1-Score (%)	平均协议一致性偏离度	平均漏检率 (%)
NB-LSTM	71.5	0.48	5.2
Hyper-GCN	80.2	0.39	3.8
Generative-Fuzzer	85.8	0.35	2.5
本文方法	92.4	0.18	0.4

综合表 4 结果可知, 本文方法在检测精度、协议一致性保持及漏检控制上均全面优于对比方法. 具体而言, NB-LSTM 受限于静态代码分析, 对动态交互行为不敏感, 性能最低; Hyper-GCN 虽能捕捉代码结构信息, 但其静态图模型难以适应协议运行时的拓扑变化; Generative-Fuzzer 作为国际前沿方法, 展现了生成式测试的潜力, 但对协议状态机的动态性建模不足, 导致其性能上限受限. 本文方法通过动态图建模直接刻画设备间非连续通信行为, 并利用 MDP 量化漏洞传播的随机依赖关系, 从而有效克服了节能策略引发的时序不确定性问题, 最终在 3 项核心指标上均取得了显著优势, 验证了所提框架在面对物联网动态环境挑战时的先进性与鲁棒性.

3 结论

物联网环境下轻量级双向安全认证协议的级联漏洞检测是保障物联网安全的关键环节. 资源受限设备的随机性节能策略带来协议交互时序的不确定性, 使传统检测方法面临挑战. 本文提出的检测方法, 以图卷积网络建模交互图, 结合余弦相似度实现状态关联检测, 有效克服了时序不确定性影响. 再基于马尔可夫决策过程量化漏洞传播依赖关系, 利用图注意力网络实现级联漏洞分类. 实验结果充分验证了该方法的有效性, 漏洞检测精度高, 协议一致性偏离度稳定在合理区间, 漏检率极低. 这为物联网安全认证协议的漏洞检测提供了新的思路与可靠手段, 有助于提升物联网系统的安全性与稳定性, 推动物联网技术在更多领域的广泛应用与深入发展.

参考文献

1 Masud MT, Koroniotis N, Keshk M, *et al*. Generative fuzzer-driven vulnerability detection in the Internet of Things networks. Applied Soft Computing, 2025, 174: 112973. [doi: 10.1016/j.asoc.2025.112973]

2 Hulayyil SB, Li SC, Xu LD. Machine-learning-based vulnerability detection and classification in Internet of Things device security. Electronics, 2023, 12(18): 3927. [doi: 10.3390/electronics12183927]

3 王璇, 王馨彤, 陈燕俐, 等. 基于 DistilBert-LSTM 与多项朴素贝叶斯的漏洞检测方法. 南京邮电大学学报 (自然科学版), 2023, 43(2): 102–110.

4 潘睿, 范希明, 左洪盛, 等. 基于关键词的行级别漏洞检测方法. 计算机工程与设计, 2025, 46(6): 1648–1655.

5 陈旭, 陈子雄, 景永俊, 等. 基于双曲图卷积神经网络的切片级漏洞检测方法. 计算机工程与科学, 2025, 47(5): 851–863. [doi: 10.3969/j.issn.1007-130X.2025.05.009]

6 曹子亨, 何立风, 贾鸥, 等. 基于双向数据流分析与图抽象嵌入的漏洞检测方法. 计算机应用研究, 2025, 42(7): 2176–2183.

7 张雨轩, 黄诚, 柳蓉, 等. 结合提示词微调的智能合约漏洞检测方法. 信息网络安全, 2025, 25(4): 664–673. [doi: 10.3969/j.issn.1671-1122.2025.04.014]

8 Bhardwaj M, Kumari U, Kumar S, *et al*. An efficient user authentication and key agreement scheme wireless sensor network and IoT using various security approaches. SN Computer Science, 2023, 4(5): 574. [doi: 10.1007/s42979-023-01964-1]

9 李敏, 时瑞浩, 张莹, 等. 基于混合风格迁移的智能合约漏洞检测方法. 重庆大学学报, 2024, 47(12): 70–82.

10 Arenas LA, Yactayo-Arias C, Quispe SR, *et al*. Leveraging security modeling and information systems audits to mitigate network vulnerabilities. International Journal of Safety and Security Engineering, 2023, 13(4): 763–771. [doi: 10.18280/ijsse.130420]

11 庄园, 樊泽楷, 王诚, 等. 基于预训练与新型时序图神经网络的智能合约漏洞检测方法. 通信学报, 2024, 45(9): 101–114. [doi: 10.11959/j.issn.1000-436x.2024163]

12 Ruiz-Torrubiano R, Dhungana D, Paudel S, *et al*. Modeling local search metaheuristics using Markov decision processes. Algorithms, 2025, 18(8): 512. [doi: 10.3390/a18080512]

13 任家东, 李尚洋, 任蓉, 等. 基于站点地图的 Web 访问控制漏洞检测方法. 计算机科学, 2024, 51(9): 416–424. [doi: 10.11896/jsjkx.230900075]

14 李坤, 李斌, 朱文静, 等. 融合语义与属性特征的跨架构漏洞检测. 计算机科学与探索, 2025, 19(3): 787–801.

15 李秋月, 韩道军, 张磊, 等. 基于分层注意力网络和积分梯度的细粒度漏洞检测方法. 计算机科学, 2024, 51(12): 326–333. [doi: 10.11896/jsjkx.231000174]

16 陈锦富, 冯乔伟, 蔡赛华, 等. 基于形式化方法的区块链系统漏洞检测模型. 软件学报, 2024, 35(9): 4193–4217. [doi: 10.13328/j.cnki.jos.007133]

17 Sengupta A, Anshul A, Chourasia V, *et al*. Security vulnerability (Backdoor Trojan) during machine learning accelerator design phases. IT Professional, 2025, 27(1): 65–72. [doi: 10.1109/MITP.2024.3519632]

18 李飞序, 严飞, 程斌林, 等. 面向 LPWAN 的受限设备协议漏洞自动化检测框架. 山东大学学报 (理学版), 2023, 58(9): 39–50. [doi: 10.6040/j.issn.1671-9352.0.2022.660]

(校对责编: 李慧鑫)