高林, 李捍东, 郑华俊. 基于物联网物理捕获阶段攻击检测方法研究[J]. 智能计算机与应用,2024,14(4):151-156. DOI:10.20169/j.issn.2095-2163.240423

基于物联网物理捕获阶段攻击检测方法研究

高 林, 李捍东, 郑华俊
(贵州大学 电气工程学院, 贵阳 550025)

摘 要: 文章以优化物联网节点攻击检测的捕获率为研究目的,以多端柔性配电网管理物联网平台中的网络节点为研究对象,针对无线传感器网络节点捕获攻击的检测问题,分析了传感器节点被捕获时的特点,建立了传感器节点分级的网络拓扑模型。在此基础上,提出了改进的物理捕获阶段攻击检测方法,除了考虑缺席时间阈值外,还引入了心跳差阈值和异常事件数量阈值等多个阈值来增强检测能力。通过 OMNET++仿真平台搭建传感器网络拓扑结构并进行了仿真实验,结果表明所提出的方法在检测率等方面具有一定的优越性。

关键词: 心跳序列; 缺席时间阈值; 网络拓扑; OMNET++仿真
中图分类号: TP393 **文献标志码**: A **文章编号**: 2095-2163(2024)04-0151-06

Research on attack detection method in physical capture phase based on Internet of things

GAO Lin, LI Handong, ZHENG Huajun
(School of Electrical Engineering, Guizhou University, Guiyang 550025, China)

Abstract: This paper aims to optimize the capture rate of iot node attack detection, and takes the network nodes in the multi-terminal flexible distribution network management iot platform as the research object. Aiming at the problem of detecting node capture attacks in wireless sensor networks, this paper analyzes the characteristics of sensor nodes when they are captured, and establishes a hierarchical network topology model of sensor nodes, based on this, an improved attack detection method in physical capture phase is proposed. Besides the threshold of absence time, several thresholds such as the threshold of heartbeat difference and the threshold of the number of abnormal events are introduced to enhance the detection ability. Finally, the topology of sensor network is built by OMNET + + simulation platform and the simulation results show that the proposed method has advantages in detection rate and so on.

Key words: heartbeat sequence; absence time threshold; network topology; OMNET++simulation

0 引 言

随着物联网应用范围的扩大,无线传感器网络(Wireless Sensor Networks, WSN)作为数据传输网络在环境监测、军事监视和跟踪等各种应用场景发挥很大作用[1]。节点捕获攻击的检测是物联网中的一种入侵检测技术,可以用于保护 WSN 免受恶意攻击。在物联网系统中,由于设备数量庞大、网络复杂多样以及数据流动性强等特点,安全风险和入侵威胁也相应增加,因此需要采取有效措施进行检测和防范,本文就该问题以及检测方法进行了研究。

节点捕获攻击是一种主动针对 WSN 的攻击方式,其属于一种多阶段攻击,如何防止节点捕获或遭受捕获后能及时止损是 WSN 能否成功部署的关键[2]。

如图 1 所示,在无线传感网络数据正常传输的过程中,攻击者首先恶意捕获一个正常的节点,通过改装、伪装、破坏正常节点等方式,使得该节点对网

基金项目: 国家自然科学基金(52167007)。
作者简介: 高 林(2000-),男,硕士研究生,主要研究方向:物联网入侵检测,数字孪生; 郑华俊(1989-),男,博士,讲师,主要研究方向:柔性直流输电建模,稳定性分析。
通讯作者: 李捍东(1965-),男,硕士,教授,主要研究方向:计算机控制,嵌入式系统。Email:470394668@qq.com
收稿日期: 2023-12-12

络安全性造成威胁。

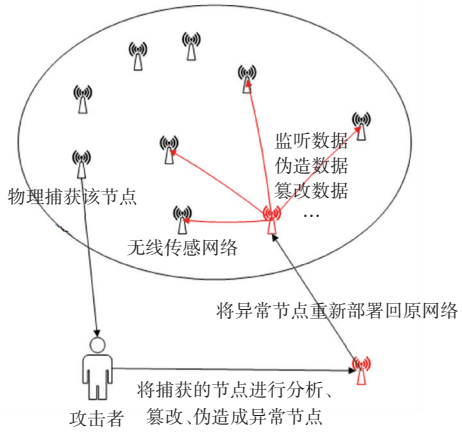


图 1 节点捕获攻击示意图

Fig. 1 Node capture attack diagram

物联网节点通常是嵌入式系统,在嵌入式系统上的物理攻击主要针对于微处理器与存储卡,对微处理器的篡改攻击主要分为 3 类,分别是侵入式、半侵入式与非侵入式。3 类篡改攻击均需将捕获的节点从部署区域进行移动和中断节点正常工作的操作[3]。

通常部署在某区域内正常工作的传感器节点之间会持续地进行数据传输,这意味着长期数据传输中断能被注意到。节点被物理捕获时可能遭受的情况如下[4]:

(1)攻击者不具备改装节点的能力,通常采取直接暴力破坏传感器节点的方式,导致数据传输功能受到影响;

(2)攻击者获得被捕获节点的访问权,并根据所要达到的目的更改传感器节点内部程序;

(3)攻击者能够使用工具观察到传感器节点内存的内容,可以根据烧录的信息对节点进行分析破解,从而获取传感器节点的重要信息和数据,比如加密密钥等;

(4)攻击者可以控制节点的无线传输功能,包括读取、修改、删除、创建无线消息等。

在物理捕获阶段进行检测可以早期发现攻击意图,使得后续攻击无法实现,其主要依据是传感器节点被捕获后攻击者需要将其从部署区域移动到可以对其进行分析的环境,所以会有一段时间缺席网络[5]。

1 改进攻击检测方法

通过介绍目前 3 种常用的利用缺席时间的物理捕获检测技术并进行特点分析,由此提出改进的物理捕获阶段攻击检测方法。

1)一般检测方法

一般的检测方法是将基于基站或特定监控节点记为 A,其余节点记为 Bi,i 标识节点编号。通常 A 记录了所有发送给 A 消息的节点,这样就能根据 A 是否收到 Bi 的消息以及时间间隔阈值,来判断节点是否被捕获[6]。

2)FSD 方法

FSD(First Stage Detection, FSD)方法是由 Ding 等[7]提出的检测方法,其也是以将物理捕获阶段的攻击节点从网络中移除所需时间为依据。其中设计了两种方案,包括 FSD 和 SEFSD(Sink Enhanced FSD, SEFSD),其分别是依靠物理捕获阶段检测方案的去中心化和半中心化实现。

3)CAT 方法

基于偶对的节点捕获检测(Couple-based Node Compromise Detection, CNCD)方法是由 Lin 等[8]提出的检测方法,也是物理捕获阶段检测方法,是一种基于偶对检测的方法。是通过传感器节点之间建立关系的方式来互相监控对方的状态。其假设在区域内每个传感器节点可以和其它节点形成偶对节点。CAT 方法包括 3 个阶段:传感器节点初始化和部署、偶对节点的构建、传感器节点的捕获检测。

4)本文改进的物理捕获阶段攻击检测方法

基于上述分析可知,现有的一些物理捕获阶段检测方法比如 FSD 是将传感器节点的缺席时间和一个阈值进行比较,若大于阈值还未响应就认为该传感器节点被捕获,这是值得借鉴的,但是单阈值对检测影响很大,而改进的物理捕获阶段攻击检测方法,可以减少因为单阈值限制带来的误检。

在传感器网络中会存在具有更强硬件支持的节点,通常为汇聚节点或者网关。这一类节点通常是传感器网络中数据的最终流向,也不易被捕获,所以是被重点保护的节点类型[9]。

如图 2 所示将节点进行分级,在网络模型中将汇聚节点视为网络的中心。一个典型的传感器网络,每个传感器节点都有其唯一标识符,并且在部署后位置不变,在小型传感器网络中,通常仅在汇聚节点周围分布一些传感器节点与之通信。在更大型的传感器网络中,传感器网络边缘的感知节点通常需要经过路由节点,以“多跳”的方式到达汇聚节点[10],将经过 k 跳的节点到达汇聚节点的节点称为 k 级节点。检测消息是以序列号的形式存在,就像

“心跳”向上下级节点报告自己的存活状态，可称之为心跳消息[11]。同时，引入序列号带来另一个判断节点捕获的依据，就是将当前序列号的值作为另一个阈值。假设序列值的上限是 m，序列值的差值阈值设为 n。值得注意的是，以下并不是严格意义上的区间，而是一个“约瑟夫环”，应当以当前值为基准倒推或者顺推[12]。

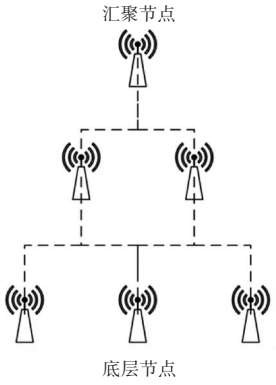


图 2　传感器节点分级

Fig. 2　Sensor node classification

当节点收到当前心跳的序列值为 a，上次收到的心跳的序列值为 b，若 a 等于 $(b+1)\%m$ 时，则表示当前序列值正确；若其序列值不在 0 到 $m-1$ 之间，则认为是严重异常，并标记为被捕获；当前序列值 a 不在序列值 b 倒推 n 次即 $(b-n+m)\%m$，以及当前序列值 a 不在序列值 b 顺推 n 次即 $(b+n)\%m$ 之间，则被判断处于被捕状态，考虑其是被捕获后重新加入网络状态或者是攻击者在进行测试，并将其记为状态 1。当序列值 a 处于倒推 n 次即 $(b-n+m)\%m$ 到 b 之间则可能是数据滞留在网络中，而被认为是一次异常事件；当序列值处于 $a+1$ 到顺推 n 次即 $(b+n)\%m$ 之间，则认为是检测消息在信息传输的过程中丢失，此时仍接收当前的消息并更新序列号的值，并且记为一次异常事件，将这两种异常事件记为状态 2。当异常事件数量超过设定的阈值时，会触发报警机制[8]。为进一步判断是节点捕获攻击还是传感器网络中的扰动导致的异常事件，需要进行人工检查进行确认。检测算法流程如图 3 所示。

将节点进行层次分级还有一个优势，当处于中间层级的节点被捕获时，其下级节点就无法接收到其心跳消息，这时根据时间阈值和节点缺席时间来判断出该节点被捕获，可以有效地防止攻击者获取传感器网络边缘的底层传感器节点所采集的数据[13]。

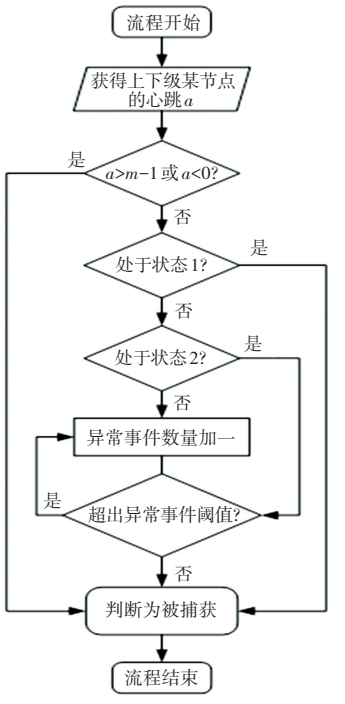


图 3　基于心跳序列的检测流程

Fig. 3　Detection flow chart based on heartbeat sequence

2　仿真实验

2.1　实验环境及参数设定

考虑到实验的传感器节点较多，因此对于 WSN 的搭建以及检测方法的测试均通过虚拟环境进行仿真模拟，实验环境配置见表 1。

表 1　实验环境

Table 1　Thresholds for detection methods

操作系统	Windows 8.1Pro 64 位
运行环境	处理器基准频率 2.3 GHz
网络协议	TCP/IP 协议
仿真平台	OMNET++
仿真环境	omnetpp.ini 文件

仿真实验共设置了 201 个节点，分别是 200 个传感器节点和 1 个基站节点。设置丢包率为 1%，实验设定捕获节点的最高比例为 25%，即最多被捕获 50 个传感器节点，每间隔 5 个被捕节点进行实验，实验一共均匀部署了 10 组 20 个节点的小型传感器网络最后组成一个传感器网络，数据从最外层节点产生最终到达汇聚节点，每个小型传感器网络有 2 个网关节点和 6 个中间路由节点。底层负责采集数据的传感器节点 12 个，数据每隔 10 s 产生一次，数据传输耗时 100 ms，模拟数据被采集并发送。

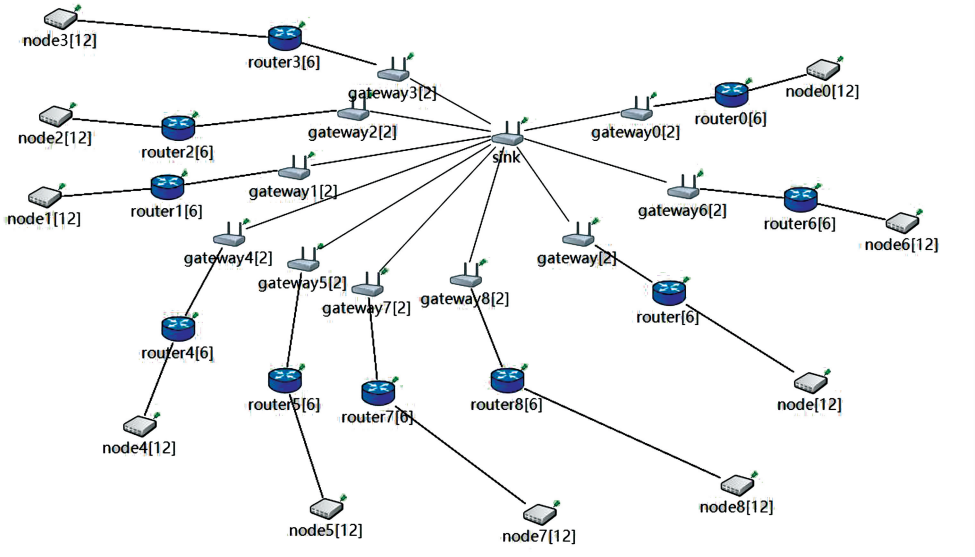
最理想的网络缺席时间阈值是节点被捕获后到

重新加入网络所需最短时间[14]。判断节点是否被捕获是通过节点缺席时间和阈值进行比较,除了物理捕获阶段常用的缺席时间阈值,改进的物理捕获阶段检测方还设置心跳差值阈值和异常事件数量阈值,阈值设置见表 2。实验网络拓扑图及实验运行图如图 4 所示。

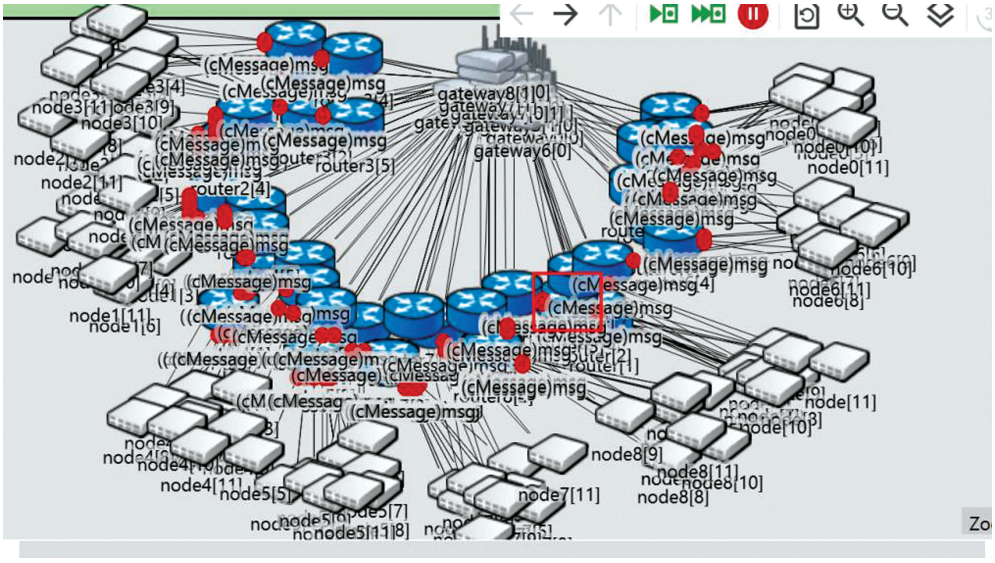
表 2 检测方法的阈值

Table 2 Thresholds for detection methods

阈值名	阈值
缺席时间阈值	10 s
心跳差值阈值	6
异常事件数量阈值	10



(a) 实验网络拓扑图



(b) 实验时节点发送检测消息

图 4 实验截图

Fig. 4 Experimental screenshot

2.2 评价指标

在测试的节点中,存在正常和被捕获的两类节点。因此,对总体样本的检测存在以下 4 种结果。

(1)正常节点被检测出的数量(记为 *TN*);

(2)正常的节点被误检为被捕获的节点数量(记为 *FP*);

(3)被捕获的节点误检为正常节点的数量(记为 *FN*);

(4)被捕获的节点被检测出的数量(记为 *TP*)。根据这几种结果可以量化为检测率、误报率、

漏报率。

检测率(Detection Rate，*DR*) 其计算公式如式(1)：

$$DR = \frac{TP}{TP + FN} \tag{1}$$

误报率(False Positive Rate，*FPR*) 其计算公式如式(2)：

$$FPR = \frac{FP}{TN + FP} \tag{2}$$

漏报率(False Negative Rate，*FNR*) 其计算公式如式(3)：

$$FNR = \frac{FN}{TP + FN} \tag{3}$$

2.3　结果分析

本文采用改进的物理捕获阶段检测方法以及 FSD 和 CAT 两种方法进行实验检测到被捕获节点的具体个数见表 3，个数柱状图如图 5 所示。所提方法检测的被捕获节点个数的数量最多。在被捕获的节点数量小于 25 时可以看到，3 种检测方法检测效果均能达到 90%以上，但是随着被捕获节点数量增加，检测的效果下降。

表 3　3 种方法检测出被捕节点数量比较

Table 3　Comparison of the number of captured nodes detected by three methods

被捕获节点	CAT	FSD	所提方法
0	0	0	0
5	5	5	5
10	9	10	10
15	14	14	14
20	17	18	19
25	21	22	23
30	24	26	27
35	26	28	30
40	29	31	33
45	32	34	36
50	35	37	40

经过计算，3 种方法的被捕获节点检测率如图 6 所示。检测率的值是正确识别为正例的样本数占所有正例样本数的比率，在这里正例样本是指被捕获的节点，3 种检测方法检测率均随着被捕节点的增加而下降。其中，CAT 的检测率下降最明显，在被捕节点个数为 50 时，检测率下降到 70%；所提方法的下降较为平缓，随着被捕节点的增加，检测率从 100%下降到 80%。

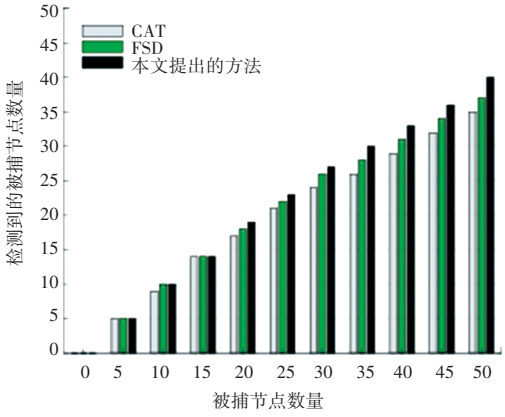


图 5　3 种方法检测出被捕节点柱状

Fig. 5　The arrest node column was detected by three methods

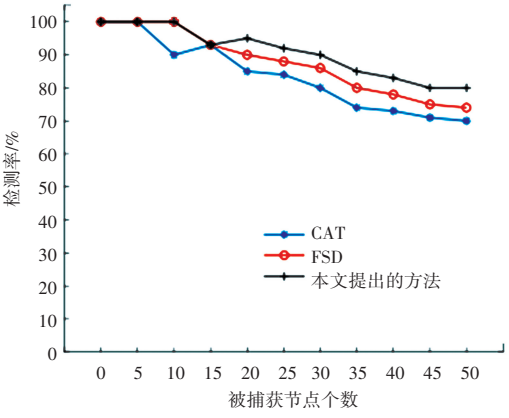


图 6　3 种方法的检测率

Fig. 6　Detection rate of three methods

3 种方法的误报率如图 7 所示。误报率的含义在评价指标一节中给出，其值是指错误将负例样本识别为正例的样本数占所有负例样本数的比率，在这里正例样本是指被捕获的节点。由图 7 所见，3 种方法的误报率随着被捕节点数量的增加而呈上升趋势。其中，CAT 方法从 0%上升到 19%，FSD 方法最后达到 25%的误报率，所提方法在被捕节点数量为 20 个时开始上升，从 0%一直增加到 14%，相对 FSD 和 CAT 两种方法的误报率最低。

3 种方法的漏报率如图 8 所示。漏报率值是指分类器错误地将正例样本识别为负例的样本数占所有正例样本数的比率，在这里正例样本是指被捕获的节点。由图 8 所见，3 种方法随着被捕节点的数量增加而呈上升趋势，其中漏报率上升最明显的是 CAT 方法，一直上升至 31%，其次是 FSD 方法，上升至 27%，所提方法漏报率为 20%，相对 FSD 和 CAT 两种方法的漏报率最低。

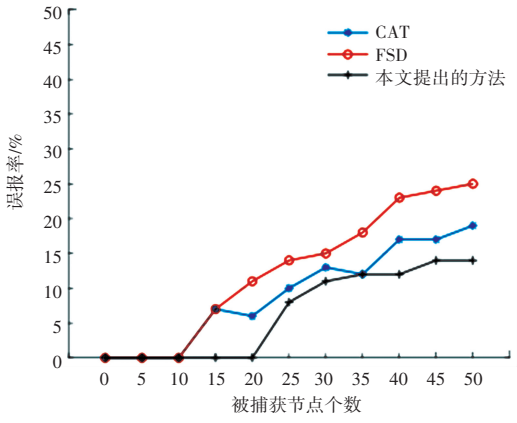


图 7 3 种方法的误报率

Fig. 7 False positive rate of three methods

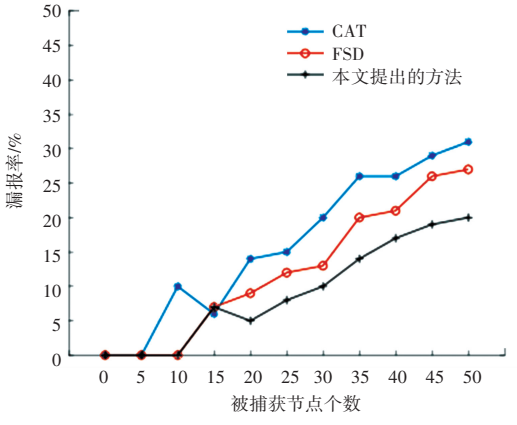


图 8 3 种方法的漏报率

Fig. 8 Missing negatives of three methods

3 结束语

本文介绍了 WSN 中的节点捕获攻击,该攻击手段分为物理捕获、节点重新部署和内部攻击 3 个阶段,且随着攻击层级的递进而威胁程度越来越大。为了降低损失风险,在攻击早期进行检测至关重要。详细分析了节点捕获攻击的物理捕获阶段,并介绍了现有的检测方法。总结了物理捕获阶段检测方法主要基于节点缺席时间这一特征来判断是否被物理捕获,并提出了改进的物理捕获阶段攻击检测方法,除了考虑缺席时间阈值外,还引入了心跳差值阈值和异常事件数量阈值等多个阈值来增强检测能力。最后,通过 OMNET++仿真平台搭建传感器网络拓扑结构并进行了仿真实验。结果表明,所提出的方法在检测率等方面具有优越性。

由于本文研究的物理捕获阶段的检测方法面向的平台所在区域是厂区,所以节点供能充足,不用担心节点能量消耗完的情况。但是在物联网中可能存在节点被部署在农田、森林等空旷环境,此时节点能量消耗需要考虑,也就是节点有时会休眠,这种在异步休眠模式下如何判断节点被捕获将在后续进行研究和改进。

参考文献

[1] 刘强, 蔡志平, 殷建平,等. 网络安全检测框架与方法研究[J]. 计算机工程与科学, 2017, 39(12): 2224-2229.

[2] SARITA A, MANIK L D, JAVIER L. Detection of node capture attack in Wireless Sensor Networks[J]. IEEE Systems Journal, 2019, 13(1): 238-247.

[3] ANDERSON J P. Computer security threat monitoring and surveillance[R]. Technical Report. Anderson Company, 1980.

[4] VINAYAKUMAR R, ALAZAB M, KP S, et al. Deep learning approach for intelligent intrusion detection system[J]. IEEE Access, 2019, 7:41525-41550.

[5] JAVAID A Y, NIYAZ Q, SUN W, et al. A Deep learning approachfor network intrusion detection system [J]. ICST (Institute for Computer Sciences, Social - Informatics and Telecommunications Engineering), 2015.DOI:10.4108/eai.3-12-2015.2262516.

[6] INGREB, YADAV A. Performance analysis of NSL-KDD dataset using ANN [C]//Proceedings of International Conference on Signal Processing and Communication Engineering Systems. IEEE, 2015: 92-96.

[7] DING W, YU Y, YENDURI S. Distributed first stage detection for node capture [C]//Proceedings of Globecom Workshops. IEEE, 2011:1566-1570.

[8] LIN X. CAT: Building couples to early detect node compromise attack in wireless sensor networks [C]// Proceedings of the Global Telecommunications Conference. IEEE, 2009:1-6.

[9] 周捷, 郭渊博, 胡凌燕. WSN 中针对节点捕获攻击的检测与控制[J]. 西安电子科技大学学报, 2012, 39(1): 185-190.

[10] 朱国强, 洪占勇, 王强. 基于物联网的电动叉车远程监测系统的研究和设计[J]. 电子测量技术, 2017, 40(1): 189-193.

[11] 曾凡锋, 田雨丝, 王景中. 物联网中节点捕获攻击早期检测方法研究[J]. 计算机仿真, 2022, 39(8): 477-481.

[12] 董俊杰, 彭亚斌. Micro Python 软件开发平台的 ESP32-C3 通信性能测试[J]. 单片机与嵌入式系统应用, 2023, 23(2): 6057-6065.

[13] DING W, YU Y, Yenduri S. Distributed first stage detection for node capture[C]//Proceedings of Globecom Workshops. IEEE, 2011: 1566-1570.

[14] SARITA A, MANIK L D, JAVIER L. Detection of node capture attack in wireless sensor networks.[J]. IEEE Systems Journal, 2019, 13(1): 238-247.