文章编号:1671-4598(2023)08-0077-07 DOI:10.16526/j.cnki.11—4762/tp.2023.08.012 中图分类号:TP393 文献标识码:A

基于嵌入式及 ASG 技术的物联网节点捕获攻击检测系统

叶小波
(广东科学技术职业学院 教务部,广东 珠海 519090)

摘要:为精准检测攻击性节点所处位置,并对其实施定向化捕获处理,设计了基于嵌入式及 ASG 技术的物联网节点捕获攻击检测系统;通过数据报文捕获模块、数据报文解析模块、报文处理模块,优化由节点定义到节点实时处理的执行流程,根据攻击检测与定位模块运行情况,调试物联网节点对象,实现检测系统硬件设计;利用物联网主机所捕获到节点信息的加密、解密与秘钥管理结果,确定节点认证流程,完成嵌入式物联网防御机制的设计;按照 ASG 技术执行标准,收集蠕虫样本,并判断特征生成与分发处理指令的可行性,完成关键检测指令的制定,结合相关运行元件,实现基于嵌入式及 ASG 技术的物联网节点捕获攻击检测系统设计;实验结果表明,该设计系统对于攻击性节点位置信息的平均检测精准度高达 96.7%,能够精准检测攻击性节点所处位置,增强攻击性信息样本的定向化捕获与处理能力。

关键词:ASG 技术;物联网节点;捕获攻击检测系统;嵌入式;数据报文;节点调试;秘钥管理;蠕虫样本

An IoT Node Capture Attack Detection System Based on Embedded and ASG Technology

YE Xiaobo
(Academic Affairs Office, Guangdong Polytechnic of Science and Technology, Zhuhai 519090, China)

Abstract: In order to accurately detect the location of attacking nodes and implement targeted capture processing on them, an IoT node capture attack detection system based on embedded and ASG technology is designed. Through the data message capture module, data message analysis module, and message processing module, the execution process from node definition to node real-time processing is optimized, and the IoT node object is debugged according to the operation of the attack detection and location module to realize the hardware design of the detection system. Use the encryption, decryption and key management results of the node information captured by the IoT host to determine the node authentication process and complete the design of the embedded IoT defense mechanism. According to the ASG technology implementation standard, collect worm samples, judge the feasibility of feature generation and distribution processing instructions, complete the formulation of key detection instructions, and implement the design of the Internet of Things node capture attack detection system based on embedded and ASG technology. The experimental results show that the average detection accuracy of the designed system for the location information of aggressive nodes is as high as 96.7%, which can accurately detect the location of aggressive nodes and enhance the directional capture and processing ability of aggressive information samples.

Keywords: ASG technology; IoT nodes; capture attack detection system; embedded; data message; node commissioning; key management; worm samples

0 引言

物联网是以传统电信网络和应用互联网为基础,构建的新型信息承载体平台,可以将具有独立寻址能力的普通对象节点连接起来,从而在主机端模块中形成完整的互联网络。随着物联网运行速率的加快,网络内部数据信息样本的实时累积量也会不断增大,而其中所夹杂的风险性信息则会对其他数据文本造成攻击影响。因此,精准检测攻击节点所在位置,并对其进行定向化捕获,是保障物联网运行稳定性的必要条件。

文献[1]系统利用逻辑程序软件,判断攻击性节点对于数据信息样本的承载能力,再通过多次对比已定义节点与周围区域性节点组织之间差异性的方式,来判断节点对象大致所属区域。文献[2]系统借助 OpenFlow 软件,将节点对象与数据样本匹配起来,根据 NC 原则,判断攻击性节点对象在网络环境中所处运行位置。然而上述两种系统均不能精准检测攻击性节点位置信息,无法满足执行后续捕获处理指令的定向性需求。

物联网和嵌入式存在密不可分的关系,物联网就是嵌入式产品的网络化。嵌入式系统是由软件、硬件部分共同组成的应用体系平台,具有独立运行能力。其软件部分的

收稿日期:2023-01-30; **修回日期**:2023-03-20。

作者简介:叶小波(1983-),男,广东珠海人,硕士,助理研究员,主要从事高教方向的研究。

引用格式:叶小波.基于嵌入式及 ASG 技术的物联网节点捕获攻击检测系统[J].计算机测量与控制,2023,31(8):77-83.

组成情况相对较为简单，只包括基础运行环境与操作程序；硬件部分则包括处理器、通信模块、存储器等多个运行结构，可以在核心主机的调度下，响应终端平台发出的程序指令[3]。相较于常规的计算机处理系统，嵌入式系统虽然没有配置大容量的数据存储介质，但却可以借助多个开放的 API 接口组织，实现对运行数据的转存与处理。ASG 技术的核心执行目的就是对蠕虫特征的提取过程进行自动化处理，从而在抑制蠕虫数据转发速率的同时，增强网络体系的运行稳定性[4]。为避免蠕虫数据在网络体系中占据大量存储空间，在实施信息计算之前，必须准确定义每一个蠕虫对象的传输特征，特别是在执行指令转发任务之前，必须确保已定义对象样本准确转存至目标数据库主机之中。基于上述分析，设计基于嵌入式及 ASG 技术的物联网节点捕获攻击检测系统。

1 物联网节点捕获攻击检测系统硬件设计

物联网节点捕获攻击检测系统硬件设计，包括对数据报文捕获模块、数据报文解析模块、报文处理模块等多个硬件应用结构的设计，本章节将针对具体设计方法展开研究，基于嵌入式及 ASG 技术设计物联网节点捕获攻击检测系统结构如图 1 所示。

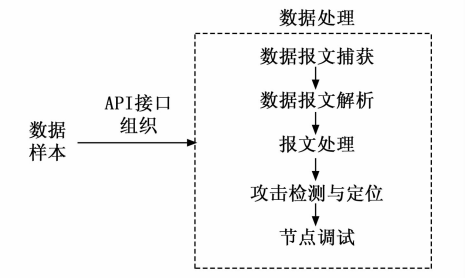

图 1 物联网节点捕获攻击检测系统结构图

在图 1 中，通过 API 接口组织转存数据信息，该结构利用数据报文捕获模块、数据报文解析模块、报文处理模块、攻击检测与定位模块和节点调试模块对数据样本进行处理，为建立防御机制、实现检测奠定基础。

1.1 数据报文捕获模块

数据报文捕获模块的实现主要借助 Libpcap 主机中的物联网信息调度函数，整个执行过程较长，需要多个设备元件的共同配合。NULL 芯片负责提取物联网主机中存储的数据信息样本，并借助输出信道组织，将这些信息参量按需分配至下级负载节点，由于每一个节点对象都对应一个独立的数据库主机，所以在捕获数据报文的过程中，并不会出现信息错传、误传的现象[5]。ProcessPkt 芯片具有较强的信息处理与信息辨别能力，可以对 Libpcap 主机捕获到的数据样本进行初步分类，在处理过程中，来源于攻击性节点的信息参量会被存储于嵌入式数据库设备中，而来源于常规节点的信息参量则可以经由信道传输组织，在系统核心数据库设备中形成长期记忆文件，以供检测主机的直接调取与利用。在物联网体系中，数据样本传输行为具有明显的方向性，所以为避免信息回传行为的出现，每一个目标节点都只能与一个独立数据库主机保持对应连接关系[6]。数据报文捕获模块结构如图 2 所示。

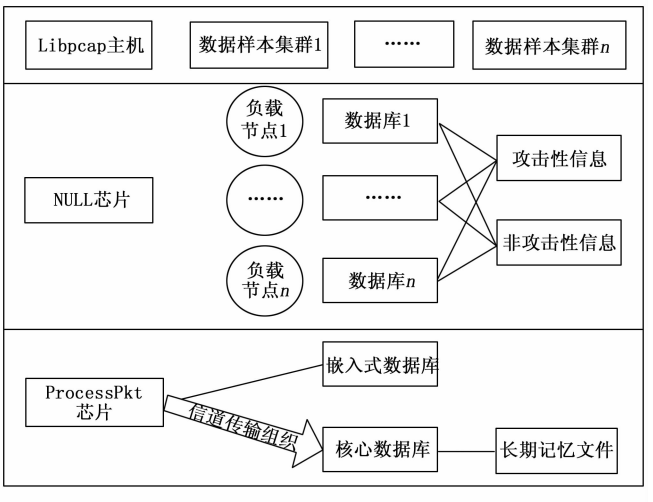

图 2 数据报文捕获模块

在物联网节点捕获攻击检测系统中，数据报文捕获模块只负责采集信息样本，故为维持系统的稳定运行能力，所采集到的数据参量还必须随着信息流进入下级应用模块之中。

1.2 数据报文解析模块

数据报文解析模块对于物联网信息样本的处理遵循的操作原则如图 3 所示。

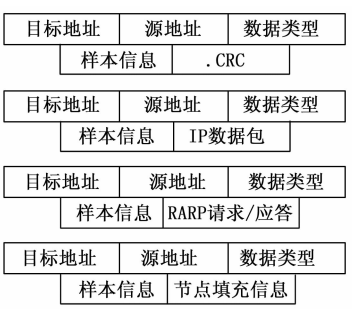

图 3 物联网数据报文解析格式

为使系统检测主机能够对攻击性节点对象进行精准捕获，数据报文解析模块对于信息样本的处理主要遵循如下四类原则：

1）CRC 型：模块主机首先获取数据报文的目标地址，并根据源地址编码结果，判断数据信息所属类型，将完成解析的数据对象定义为样本信息，并为其添加 .CRC 后缀描述。

2）IP 数据包：作为物联网环境中的主要数据类型，模块主机对其进行的前期解析处理行为与 .CRC 型数据样本相同，但在完成数据打包处理后，则必须将原样本与报文捕获模块所记录的数据样本进行对比。

3）RARP 请求/应答：模块主机所能解析处理的主要数据报文类型，存储模式相对较为单一，在检测系统中的传输行为需要多个应用节点的共同配合[7-8]。

4）节点填充信息：对于数据报文解析模块而言，已提取到数据样本中节点填充信息的含量越大，就表示模块主机在单位时间内所需处理的数据样本越多，因此该类型信息参量实际存储情况直接影响系统主机对于物联网节点攻击性行为的检测与捕获处理能力。

1.3　报文处理模块

在报文处理模块中，系统主机将直接根据解析模块执行结果来判断当前样本是否符合实际检测需求。如果当前报文属于攻击性报文类别，则直接将其丢弃，同时将该类型信息收入系统黑名单之中，并再次捕获其他信息样本，以避免其对系统主机造成二次攻击[9]。在实现报文处理的过程中，对于可能发生的物联网节点 IP 错乱问题，系统主机可以按照报文处理模块运行原理进行处理，如图 4 所示。

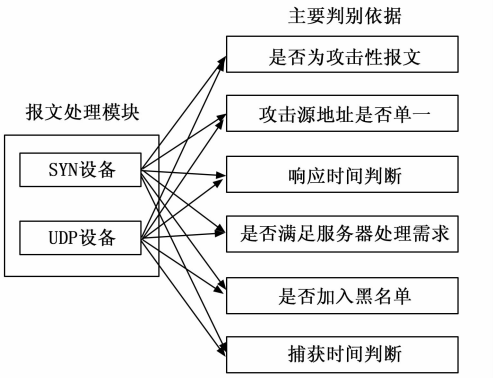

图 4　报文处理模块运行原理

图 4 中，报文处理模块主要有 SYN 设备和 UDP 设备，通过判断攻击性报文、攻击源地址、响应时间、黑名单等信息处理报文。发生 IP 错乱问题时，同一类型数据报文的攻击性等级、源地址信息等属性条件都会发生错乱，而 SYN 设备、UDP 设备的存在，则可以在正式执行检测指令之间，对已发生属性错乱的信息样本进行复原处理。SYN 设备、UDP 设备作为报文处理模块的核心组成结构，对于报文捕获模块采集到的数据样本，可以同时判断其攻击性等级、源地址信息、响应时间等属性条件[10]。SYN 设备的运行等级较高，在单位时间内所能处理的数据报文也就相对较多；UDP 设备的运行等级较低，但由于其响应速率较快，故而在单位时间内可以对捕获到的数据报文进行多次识别。

1.4　攻击检测与定位模块

攻击检测与定位模块是包含两条执行路径的硬件应用结构，检测部分确定物联网节点所捕获信息样本的攻击性能力，定位部分负责对已捕获数据所处位置进行精准定位。

1）攻击检测部分：模块体系攻击检测能力的实现需借助 Check 主机。在物联网环境中，数据信息经由捕获模块、解析模块、处理模块进入该模块体系之中，其所包含攻击性信息对于网络节点的影响能力已经减弱。但对于核心网络执行设备而言，任何细小的攻击性行为都有可能导致系统运行出现偏差，故而该条执行路径的最主要运行职能就是为物联网节点提供绝对安全的数据信息样本[11]。

2）攻击定位部分：定位部分作为检测部分的下级附属结构，不具备捕获数据信息样本的能力，且该部分运行设备不与报文处理模块建立数据互传关系，其内部运行的所有信息全部来自模块体系内的上级执行结构[12]。由于信息样本在模块内传输依然存在一定程度的损耗，所以在设置攻击定位子模块时，要设置一个具有输出能力的数据库主机，以用于补充被攻击检测子模块消耗的信息参量。

1.5　节点调试模块

当物联网节点的位置发生变化时，节点调试模块能够精准感知到该变化，并能够及时更新攻击检测与定位模块中的数据报文特征，如信息接收强度、信息目标传输区域等。运行检测指令时，核心检测主机与物联网接入点间距离的变化可能会导致数据报文存储格式发生变化[13]。该模块在面对上述问题时，采取零散布局物联网节点的方式，为数据报文提供一个相对广泛的传输空间，使其在节点与节点之间的连接不受任何束缚，即便是在攻击性信息、非攻击性信息混杂的情况下，这些数据样本的源地址信息也不会改变，这也是该模块的最主要运行目的。具体的节点调试模块连接结构如图 5 所示。

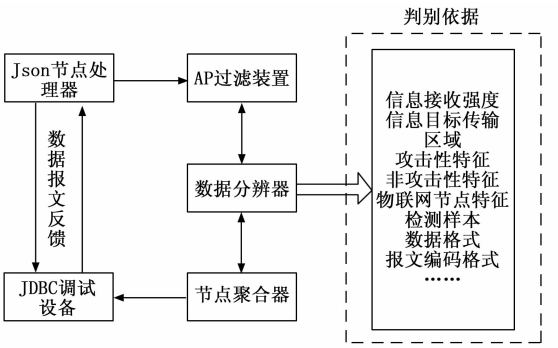

图 5　节点调试模块结构简图

由图 5 可以看出，通过 AP 过滤装置、数据分辨器、节点聚合器、Json 节点处理器、JDBC 调试设备五部分组成了节点调试模块的运行闭环。数据报文在 Json 节点处理器、JDBC 调试设备之间来回反馈时，数据分辨器根据主要判别依据，确定当前捕获信息的攻击作用能力，若其行为能力过强，则经由 AP 过滤装置再次回到节点调试模块的前端运行部分，跟随未检测数据报文进行再次反馈传输；若其行为能力符合系统主机的检测需求，节点聚合器对这些数据报文进行打包处理，并将其回传至物联网节点之中[14]。

2　嵌入式物联网的基础防御机制

物联网防御机制对攻击性数据报文起到了一定的抵御作用，为实现系统主机对于攻击性节点的精准捕获与检测，完善防御机制构建原则，按照嵌入式物联网的运行需求，完成加密、解密、秘钥管理与检测节点认证。

2.1　加密、解密与秘钥管理

加密、解密、秘钥管理是 3 个完全独立的处理流程。加密就是借助密码模板定义物联网检测信息的编码格式；

解密的执行流程则与加密完全相反，但两者对于物联网检测信息的处理遵循统一的密码模板；秘钥管理就是在物联网环境中开辟独立空间，以用于编写密码模板[15-16]。物联网节点捕获攻击检测系统对于加密、解密、秘钥管理表达式的求解满足如下公式。

加密表达式：

$$Q(\chi)=\frac{\dot{w}}{1+\chi^{-e}} \tag{1}$$

解密表达式：

$$R(\chi)=\left(\frac{1}{2\alpha}\right)\times\sum_{-\infty}^{+\infty}\chi(r_{\max}^2-r_{\min}^2) \tag{2}$$

秘钥管理表达式：

$$Y(\chi)=\sum_{-\infty}^{+\infty}\chi\left(\frac{\hat{u}}{\beta\cdot|\Delta U|}\right) \tag{3}$$

式中，χ 表示一个待检测的信息样本，$\dot{w}$ 表示编码系数，e 表示攻击性检测参数，α 表示待检测信息转码系数，$r_{\max}$ 表示转码向量的最大取值，$r_{\min}$ 表示转码向量的最小取值，$\hat{u}$ 表示待检测信息样本在物联网节点中的转存特征，ΔU 表示信息样本的单位累积量，β 表示密码编译参数。由于物联网体系具有嵌入式网络的全部特征，所以在实施加密、解密、秘钥管理指令之前，检测主机必须将攻击性、非攻击性捕获信息区分开来，并将其分别存储于不同的数据库主机之中。

2.2 节点认证

节点认证就是系统主机基于加密、解密与秘钥管理思想所制定的防御机制考核原则，对于嵌入式物联网体系而言，数据报文捕获模块所提取到的信息不具有针对性，随着系统主机的持续运行，这些信息样本会传输至各个网络节点之中，这也增加了针对性检测指令的执行难度[17-18]。而节点认证原则可以有效避免上述问题的出现，处理数据报文捕获模块所提取到的信息样本之前，系统主机将能够承担攻击性风险的节点对象挑选出来，并对其进行重点检测，不但可以避免攻击性信息的扩散，还能够大大增强嵌入式物联网体系对于攻击性行为的防御能力。对于节点认证定义式的推导满足式（4）：

$$\boldsymbol{I}=\frac{\delta^2(\vec{\boldsymbol{A}}+\vec{\boldsymbol{S}}+\vec{\boldsymbol{L}})\sqrt{\frac{1}{Q(\chi)}\cdot\frac{1}{R(\chi)}\cdot\frac{1}{Y(\chi)}}}{p'-1} \tag{4}$$

其中：$\boldsymbol{I}$ 表示节点认证向量，$\vec{\boldsymbol{A}}$ 为攻击性信息样本的加密向量，$\vec{\boldsymbol{S}}$ 为解密向量，$\vec{\boldsymbol{L}}$ 为实时管理向量，δ 为标准认证参数，p' 为检测主机对于嵌入式物联网节点的认证权限。加密向量、解密向量、实时管理向量任何一个指标参量的取值结果为零，都表示系统主机无法完成对嵌入式网络节点的精准检测。

3 基于 ASG 技术的检测指令实现方法

为增强物联网节点捕获攻击检测系统的精准检测能力，还需要在 ASG 技术的支持下，收集并检测嵌入式物联网环境中的蠕虫样本，计算其分发特征的具体数值。

3.1 基本蠕虫检测

实现 ASG 技术的第一步就是实施蠕虫检测，只有所收集到攻击性蠕虫信息的实例足够多，才能以此为基础制定物联网主机所遵循的检测执行指令[19-20]。规定 d_1、d_2、…、d_n 表示 n 个随机选取的蠕虫行为特征，其定义式如下：

$$\begin{cases}d_1=\gamma_1\cdot g_1\\ d_2=\gamma_2\cdot g_2\\ \quad\vdots\\ d_n=\gamma_n\cdot g_n\end{cases},n\geqslant 1 \tag{5}$$

式中，γ_1、γ_2、…、γ_n 为 n 个不相等的 ASG 执行系数，g_1、g_2、…、g_n 为随机选取的蠕虫信息实例标记参数。

根据式（4）、式（5），可将基于 ASG 技术的基本蠕虫检测表达式定义为：

$$H_\varepsilon=I\times\frac{f}{(d_1^{\,2}+d_2^{\,2}+\cdots+d_n^{\,2})}\times(\varphi-\bar{\omega})^2 \tag{6}$$

其中：f 为节点规划系数，φ 为蠕虫行为在物联网环境中的嵌入式特征，φ 为蠕虫样本定义特征。

在嵌入式物联网环境中，为准确捕获节点攻击行为，必须正确发现所有隐藏的蠕虫行为。衡量系统主机所执行检测指令是否具备可行性，应针对蠕虫行为特征进行甄别，以此精准捕获攻击性信息。

3.2 蠕虫样本收集

根据基本蠕虫检测标准，选定一个关键蠕虫信息，并针对该信息进行针对性运算的处理环节就是对蠕虫样本的收集。系统主机对于物联网节点攻击行为的捕获与检测必须遵循 ASG 技术原理，而判断所收集到蠕虫样本能否满足检测嵌入式物联网节点的应用需求，才是捕获攻击性信息样本的基础环节[21-22]。在集合空间中选定一个关键检测参量 j，对其取值范围进行约束如式（7）所示：

$$j=\sum_{\varepsilon=1}^{+\infty}H_\varepsilon\cdot\left(\kappa J-\sqrt{1-\frac{\hat{G}^2}{2\lambda}}\right) \tag{7}$$

式中，ε 为蠕虫样本筛查系数的最小取值，κ 为方向性检测变量，J 为蠕虫样本检测特征，λ 为物联网节点实时捕获系数，$\hat{G}$ 为基于 ASG 技术所选取的蠕虫样本捕获特征。在式（7）的基础上，设 ι_j 表示攻击性信息样本检测系数，ν_j 表示非攻击性信息样本检测系数，μ 为蠕虫行为能力定义条件，$\bar{z}_j$ 为蠕虫 j 的标准检测变量。联立上述物理量，推导蠕虫样本收集表达式为：

$$K_j=\frac{1}{\dfrac{\iota_j\times\nu_j}{|j-1|^{(1/\mu)^2}\big|_{\mu>1}}}\dot{z}_j \tag{8}$$

若 $\iota_j>\nu_j$ 成立，表示攻击性信息样本累积量大于非攻击性信息样本，利用 ASG 技术检测蠕虫行为时，应利用相关硬件应用设备对物联网信息参量进行多次捕获。

3.3 特征生成与分发处理

特征生成与分发处理就是根据蠕虫样本收集结果，将必要检测特征提取出来，再遵循 ASG 技术应用原则，将这些信息样本反馈至系统主机中，以供其制定运行所需的捕获处理与检测执行指令[23-24]。设 m_1、m_2、…、m_n 表示物联网节点中 n 个已经生成的蠕虫行为特征，b_1、b_2、…、b_n 表示与蠕虫行为特征匹配的信息分发系数，联立式（8），推导物联

网节点捕获攻击检测系统的特征生成与分发处理表达式为：

$$V = K_j\left(\frac{b_1}{m_1}\cdot\frac{b_2}{m_2}\cdot\cdots\cdot\frac{b_n}{m_n}\right) \tag{9}$$

在不考虑其他干扰条件的情况下，联合相关软、硬件应用结构，完成基于嵌入式及 ASG 技术的物联网节点捕获攻击检测系统设计，具体设计步骤如图 6 所示。

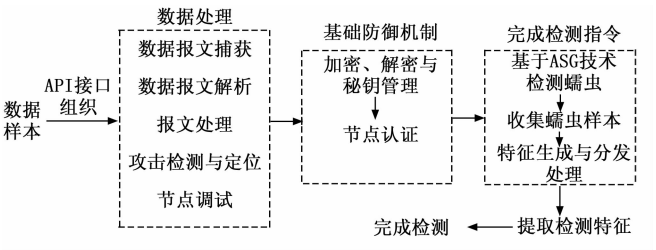

图 6　基于嵌入式及 ASG 技术设计物联网节点捕获攻击检测系统

由图 6 可知，通过 API 接口组织转存数据信息，利用数据报文捕获模块捕获节点攻击数据，采用数据报文解析模块、报文处理模块、攻击检测与定位模块和节点调试模块对数据样本进行处理，采用加密、解密与秘钥管理机制和节点认证机制完成基础的网络防御，检测蠕虫后收集蠕虫样本，生成样本特征，提取必要特征后完成检测。

4　实验分析

4.1　实验设置

为验证基于嵌入式及 ASG 技术的物联网节点捕获攻击检测系统的有效性，利用如表 1 所示的实验设备选型搭建如图 7 所示的物联网实验环境。

表 1　实验设备选型

名称/参数	型号/数值
物联网主机	UTX-3117 双网口设备
处理器	i7-13700K 13 代处理器
数据寄存器	74HC595PW 型移位寄存器
网卡	TL-WDN5200H 双频网卡
信息捕获量	1.0 T
网络带宽	500 M

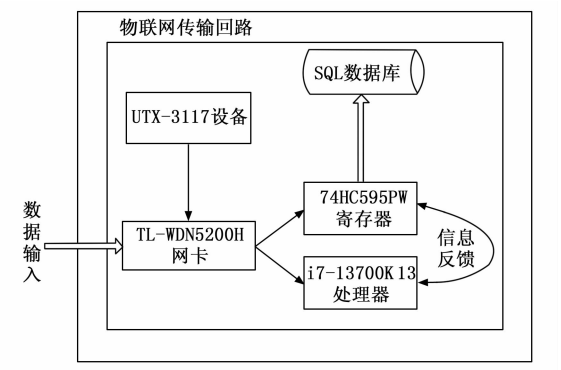

图 7　物联网实验环境

图 7 中，应用 UTX-3117 双网口设备为物联网边缘智能网关，将实验数据输入至 TL-WDN5200H 网卡中，再传输到 74HC595PW 寄存器和 i7-13700K 13 处理器中，完成信息反馈，将最终数据输出到 SQL 数据库中。

由于 TL-WDN5200H 网卡不能自主控制数据样本的输入与输出行为，所以实验过程中必须通过人工干预的方式，控制数据样本的传输方向。

将文献［1］系统和文献［2］系统作为对比系统，分析三组不同检测系统作用下，物联网主机对于攻击性信息样本的定向化捕获与处理能力。

4.2　实验步骤

物联网主机对于攻击性节点位置信息的检测准确性由数据样本检测长度、攻击性强度标记值两个指标共同决定。

首先，搭建如图 6 所示的物联网实验环境，分别利用所设计系统、文献［1］系统、文献［2］系统，对主机元件所捕获到的信息样本进行检测；

其次，分别记录三组不同检测系统作用下，数据样本检测长度与攻击性强度标记值指标的具体数值；

再次，按照式（10），对所得数据进行运算；

$$\eta = \frac{|\sigma_2 - \sigma_1|}{\sigma_1}\times\xi\times 100\% \tag{10}$$

式中，η 为检测精准度，σ_1 为数据样本实际长度，σ_2 为数据样本检测长度，ξ 为攻击性强度标记值。

最后，统计所得计算结果，总结实验规律。

4.3　实验结果

基于上述实验设置和实验步骤，得到三组不同检测系统作用下，数据样本的实际长度与检测长度如图 8 所示。

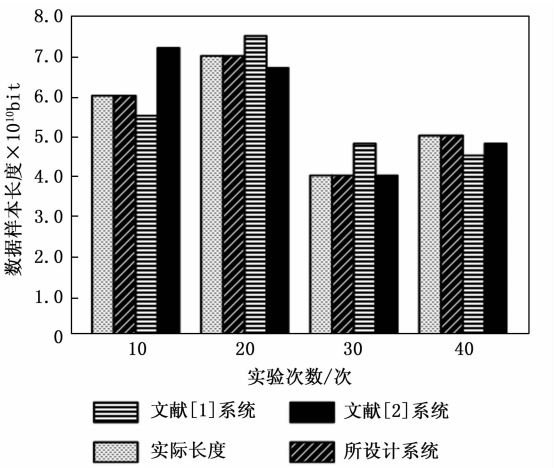

图 8　数据样本长度

由图 8 可知，在检测过程中，所设计系统检测的数据样本长度与实际样本长度一致，证明所设计系统的检测能力更佳，而文献［1］系统和文献［2］系统检测的数据样本长度与实际样本长度存在一定的偏差，检测能力还需进一步提升。

得到三组不同检测系统作用下，攻击性强度标记值的实验结果如图 9 所示。

在图 9 中，所设计系统的攻击性强度标记值与实际数值的数据重合，证明所设计系统对攻击性强度的标记更加

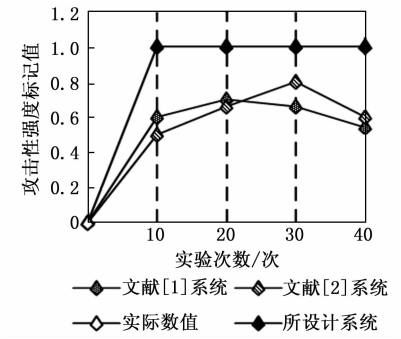

图 9 攻击性强度标记值

准确，检测效果更好。而文献［1］系统和文献［2］系统对攻击性强度的标记值较低，且与实际数据的差距较大，检测效果还需加强。

物联网主机对于攻击性节点所在位置的检测精确性，决定了该网络对于攻击性信息样本的定向化捕获与处理能力，通常情况下，检测精准度大于 95%，表示网络体系对于攻击性信息样本的定向化捕获与处理能力较强。选择图 7 中的最大值实验结果，并对应该结果，确定当前情况下，攻击性强度标记指标的具体数值，按照式（10），对所设计系统、文献［1］系统、文献［2］系统的检测精准度进行计算，得到三组不同检测系统作用下的检测精准度对比结果如表 2 所示。

表 2 三组不同检测系统的检测精准度对比结果

实验次数	三组不同检测系统/%		
	文献[1]系统	文献[2]系统	所设计系统
10	89.6	92.4	96.2
20	88.4	91.8	96.8
30	89.1	92.3	97.3
40	89.7	93.2	96.5

根据表 2 可知，当实验次数达到 40 次时，文献［1］系统和文献［2］系统的平均检测精准度分别为 89.2% 和 92.4%，而所设计系统的平均检测精准度高达 96.7%。由此可知，所设计系统的检测精确性较高。

实验结论：文献［1］系统、文献［2］系统的检测精准度均未达到 95%，因此，这两类系统并不满足定向化处理物联网攻击信息的实际应用需求；而所设计系统的检测准确度达到了 96.7%，能够精准检测攻击性节点所处位置，并对其实施定向化捕获处理。

5 结束语

本文设计了物联网节点捕获攻击检测系统，在 ASG 技术的支持下，针对嵌入式物联网主机不能精准检测攻击性节点所在位置的问题进行改进，联合解析模块、节点调试模块等多个硬件应用设备，在建立完整防御机制的同时，收集蠕虫样本，并对其分发特征进行计算。从实验结果可以看出，这种新型检测系统的应用，可以大幅提升物联网主机对于攻击性节点信息的检测准确性，在定向化捕获数据样本并对其进行深入检测方面，具有突出应用价值。

参考文献：

[1] 张华强，李凯航，王继刚. 基于线性时态逻辑的物联网操作系统安全性设计［J］. 电子技术应用，2020，46（2）：92－97，102.

[2] 张立群，林海涛，郇文明，等. 基于 OpenFlow 的软件定义网络流规则冲突检测系统［J］. 计算机应用，2022，42（2）：528－533.

[3] 王 爽，段晓萌，赵 婷，等. 智能物联电能表用嵌入式操作系统驱动程序检测技术研究［J］. 电测与仪表，2022，59（4）：8－14.

[4] 陈 飞，陈诗怡，蒙堆强. 压水堆核电厂 ASG 汽动泵蒸汽入口隔离阀开启故障分析［J］. 核动力工程，2020，41（4）：161－165.

[5] 赵 宇，殷树娟，李翔宇. 一种可重构以太网数据包解析器中可重构单元的设计［J］. 计算机工程与科学，2020，42（2）：220－228.

[6] 杨春霞，李欣栩，瞿 涛，等. 基于深度 BLSTM 和分类元数据的自定义情感分类［J］. 小型微型计算机系统，2020，41（9）：1853－1857.

[7] 唐 群，韦源生，劳景寮. 利用 Spatialite 数据库处理宗地数据及 GIS 入库实现［J］. 桂林理工大学学报，2013，33（1）：90－94.

[8] 邹同华，高云鹏，伊慧娟，等. 基于 Thompson tau-四分位和多点插值的风电功率异常数据处理［J］. 电力系统自动化，2020，44（15）：156－162.

[9] 左志斌，常朝稳，祝现威. 一种基于数据平面可编程的软件定义网络报文转发验证机制［J］. 电子与信息学报，2020，42（5）：1110－1117.

[10] 洪嘉炜，杨剑友，奚洪磊，等. 基于移动互联的变电站故障录波及报文分析装置研究［J］. 电力系统保护与控制，2020，48（1）：157－163.

[11] 邱若男，胡岸琪，彭国军，等. 基于 RASP 技术的 Java Web 框架漏洞通用检测与定位方案［J］. 武汉大学学报（理学版），2020，66（3）：285－296.

[12] 刘振鹏，王仕磊，郭 超，等. 软件定义网络中基于深度神经网络的 DDoS 攻击检测［J］. 云南大学学报（自然科学版），2022，44（4）：729－735.

[13] 蔡欢星，马 宁，刘文杰，等. 精细化管理在福清核电 5 号机组主控室可用节点的应用［J］. 核科学与工程，2021，41（1）：194－200.

[14] 王 楠，靳永毅，张占军，等. 堆芯中子注量率测量系统安装与调试典型问题处置［J］. 核电子学与探测技术，2020，40（2）：234－238.

[15] 李 航，冯朝胜，刘帅南，等. 支持离线/在线加密及可验证外包解密的 CP-WABE 方案［J］. 电子学报，2020，48（11）：2146－2153.

[16] 李 莉，杜慧娜，李 涛. 基于群签名与属性加密的区块链可监管隐私保护方案［J］. 计算机工程，2022，48（6）：132－138.

[17] 田洪亮，王佳玥，李晨曦. 基于混合算法区块链和节点身份认证的数据存储方案 [J]. 计算机应用，2022，42 (8)：2481－2486.

[18] 张之森，李　芳，王丽芳，等. 基于 HMAC 和 TEA 算法的 CAN 总线身份认证方法研究 [J]. 电工电能新技术，2021，40 (9)：57－63.

[19] 李　忠，靳小龙，王亚杰，等. 属性网络中基于变分图自编码器的异常节点检测方法 [J]. 模式识别与人工智能，2022，35 (1)：17－25.

[20] 吴晓晓，李刚强，张胜利. 分布式协作频谱感知网络中恶意节点检测和定位方法研究 [J]. 电子学报，2022，50 (6)：1370－1380.

[21] 赵琪琪，马慧芳，刘海姣，等. 融合节点属性与结构信息的子空间异常社区检测方法 [J]. 计算机工程，2020，46 (6)：94－102.

[22] 周步祥，杨明通，林　楠，等. 利用 PMU 测量节点间相角差进行孤岛故障诊断 [J]. 电测与仪表，2020，57 (6)：102－107.

[23] 吴云亮，邓韦斯，姚海成，等. 基于两级结构的电网运行断面特征选择与在线生成 [J]. 科学技术与工程，2020，20 (27)：11137－11142.

[24] 肖雨寒，江爱文，王明文，等. 基于视觉－语义中间综合属性特征的图像中文描述生成算法 [J]. 中文信息学报，2021，35 (4)：129－138.

(上接第 63 页)

总连接数为 16 000 的时候，吞吐率和读吞吐量的值相对较低，且响应时间的值最高，说明此时平台服务性能较差。

5　结束语

论文针对基于 Hyperledger Fabric 区块链的公路工程交通产品质量控制平台的性能测试展开研究及量化评估分析，建立了一个面向工程领域具体行业场景下的区块链应用平台性能测试模型、测试架构及测试环境和以吞吐率、读吞吐量、写吞吐量、响应时间、区块生成速率以及交易延迟作为性能测试指标的方法体系，系统研究了节点数、出块时间、区块最大交易条数、区块最大字节数、区块首选字节数以及总连接数等不同因素对区块链应用平台服务性能的影响，并对产生原因进行了一定的分析综述。值得说明的是，论文选取的各影响因素最优值在实际应用过程中能够支撑业务开发及运行取得较好性能，系统运行稳定，服务响应及时，用户反馈良好。最后，论文研究成果对现有主流区块链平台在不同行业场景上的开发应用和系统服务性能优化提升等工作可提供相关理论支撑和参考。

参考文献：

[1] 袁　勇，王飞跃. 区块链技术发展现状与展望 [J]. 自动化学报，2016，42 (4)：481－494.

[2] 徐艺娜. 基于区块链与物联网对智能物流产业应用的解决方案分析 [J]. 数码世界，2018 (4)：604－605.

[3] 王继业，高灵超，董爱强，等. 基于区块链的数据安全共享网络体系研究 [J]. 计算机研究与发展，2017，54 (4)：742－749.

[4] 王　锐. 区块链系统的性能评估与优化 [D]. 北京：中国科学院大学，2021.

[5] 王　旭，甘国华，吴凌云. 区块链性能的量化分析研究 [J]. 计算机工程与应用，2020，56 (3)：55－60.

[6] 李雪飞，严　悍，周亚茹，等. 分布式 Fabric raft 区块链性能影响因素定量研究 [J]. 计算机与数字工程，2021，49 (9)：1855－1859.

[7] 刘亚茹，叶振军，聂建军. 基于用户视角的区块链平台综合评价方法研究 [J]. 系统工程，2022，40 (4)：142－150.

[8] 朱　立，俞　欢，詹士潇，等. 高性能联盟区块链技术研究 [J]. 软件学报，2019，30 (6)：1577－1593.

[9] WESTON N，WILLARD J，WANG P. Performance of blockchain technology on DoD tactical network [C] //Disruptive Technologies in Information Sciences II，2019.

[10] FAN C，GHAEMI S，KHAZAEI H，et al. Performance evaluation of blockchain systems：a systematic survey [J]. IEEE Access，2020，8：126927－126950.

[11] ZHENG P，ZHENG Z，LUO X，et al. A detailed and real-time performance monitoring framework for blockchain systems [C] //2018 IEEE/ACM 40th International Conference on Software Engineering：Software Engineering in Practice Track (ICSE-SEIP). IEEE，2018：134－143.

[12] KUZLU M，PIPATTANASOMPORN M，GURSES L，et al. Performance analysis of a hyperledger fabric blockchain framework：throughput，latency and scalability [C] //2019 IEEE International Conference on Blockchain (Blockchain)，2019：536－540.

[13] DINH T T A，WANG J，CHEN G，et al. Blockbench：A framework for analyzing private blockchains [C] //Proceedings of the 2017 ACM international conference on management of data，2017：1085－1100.

[14] 新华社. 中共中央国务院印发《交通强国建设纲要》[EB/OL]. (2019-09-19)[2022-11-20]. http://www.gov.cn/zhengce/2019-09/19/content_5431432.htm.

[15] 邵奇峰，金澈清，张　召，等. 区块链技术：架构及进展 [J]. 计算机学报，2018，41 (5)：969－988.

[16] 蒋　勇，文　延，嘉　文. 白话区块链 [M]. 北京：机械工业出版社，2018.

[17] 杨永强，蔡宗辉，刘雅卓. 区块链＋大数据分析 [M]. 北京：机械工业出版社，2019.

[18] 李亚楠. 基于区块链的数据存储应用研究 [D]. 北京：北京交通大学，2018.

[19] 李牧阳. 基于联盟区块链的物流信息平台关键技术研究 [D]. 南京：南京邮电大学，2019.

[20] 陆　尧，文　捷. 基于比特币技术的供应链管控与溯源方案 [J]. 计算机工程，2018，44 (12)：85－93.

[21] 中华人民共和国交通运输部. 公路水运行业产品质量监督抽查管理办法 (交科技规 [2020] 2 号) [EB/OL]. (2020-02-27)[2022-11-20]. https://xxgk.mot.gov.cn/2020/jigou/kjs/202112/t20211231_3634123.html.