文章编号：2095-4980(2024)11-1296-08

基于Snort的网络链路数据篡改自主防御系统

何　君，王　文，陈　侃，何成胜，滕　易
(湖北能源集团新能源发展有限公司，湖北 武汉 430000)

摘　要：由于开放性源码造成数据暴露，传统方法无法阻断被攻击数据包传递，导致数据无法自主防御。为此设计了基于Snort的网络链路数据篡改自主防御系统。使用数据包嗅探器捕捉Snort的报文，并通过信息解码模块将分层译码整合成文本信息，通过网络将其发送至系统数据库中，处理大信息量警报数据并进行存储记录；构建基于Snort的网络纵深防御模型，实现对篡改攻击实时探测和自动截获。根据网络中信息包传递特性，计算不同节点间传输距离，确定防御节点位置。推导链路层数据受到篡改攻击时数据传输路径，构建数据篡改自主防御函数，实现数据的自主防御。采用小波去噪数据处理技术，获得时序数据；利用小波逆变换重构，得到去噪后的数据，完成数据篡改自主防御系统设计。由实验结果可知，该系统网络链路数据安全传输密度高，最大密钥恢复成功率可达98%，具有较强的鲁棒性。

关键词：Snort开源软件；网络链路；数据篡改；自主防御
中图分类号：TN391　　**文献标志码：**A　　**doi：**10.11805/TKYDA2023402

An autonomous defense system for network link data tamper based on Snort

HE Jun，WANG Wen，CHEN Kan，HE Chengsheng，TENG Yi
(New Energy Development Co. Ltd. of Hubei Energy Group，Wuhan Hubei 430000，China)

Abstract：Due to the exposure of data caused by open source code, traditional methods cannot block the transmission of attacked data packets, resulting in the inability of data to autonomously defend. Therefore, a network link data tampering autonomous defense system based on Snort is designed. In the hardware part of the system, a packet sniffer is adopted to capture Snort messages, and the layered decoding is integrated into text information through an information decoding module. The integrated text information is sent to the system database through the network for processing high-volume alert data and storing records. In the system software section, a network depth defense model based on Snort is constructed to achieve real-time detection and automatic interception of tampering attacks. Based on the transmission characteristics of information packets in the network, the transmission distance between different nodes is calculated and the location of defense nodes is determined. The data transmission path is derived when the link layer data is subjected to tampering attacks, and an autonomous defense function is constructed for data tampering, therefore the autonomous defense of data is achieved. Using wavelet denoising data processing technology to obtain time-series data, using inverse wavelet transform reconstruction to obtain denoised data, the design of an autonomous defense system for data tampering is completed. According to the experimental results, the system has a high density of secure transmission of network link data, and the maximum success rate of key recovery can reach 98%, demonstrating strong robustness.

Keywords：Snort open-source software；network link；data tamper；autonomous defense

电子技术的快速发展使光纤网中的链路信息受到了极大威胁，恶意软件会强行进入光纤网络链路中，对光纤网络数据和程序进行侵害、篡改以及窃取，造成链路的数据丢失、离线，对数据的传送、辨识等造成极大的干扰。因此，防止链接的数据被篡改非常必要。文献[1]结合数据挖掘方法进行异常数据检测，通过分析光纤网

收稿日期：2023-12-05；修回日期：2024-04-03

中的数据性质，对其进行归类，并利用数据的特征密度决定区域范围。通过结合高阶统计分析方法获取光缆通信中的潜在威胁信息，并基于这些信息精准构建相应的安全防护节点，以此实现对光缆中数字入侵的有效监测与防护。这种方法具有较高的特征属性——依赖性，容易忽视网络传输的畸变，使网络反应速度较慢，整体防御效果较弱。文献[2]设计了一种基于大数据的安全防御系统，利用链路中的信息传递机制，对网络中的实时业务状况进行分析，发现故障信息并进行信息交互，实现安全防护。但这种方法具有目标多、效率低、难以精确定位问题点的位置等缺点，且代价高昂，实用性也较低。基于此，本文设计了基于网络入侵检测系统(Snort)的网络链路数据篡改自主防御系统。通过Snort的应用架构，将多个硬件器件组合起来，构建基于Snort的网络纵深防御模型，结合小波去噪数据处理技术，实现数据的自主防御。

1　系统硬件结构设计

系统硬件结构设计过程中应用Snort系统，通过网络报文对网络中攻击进行探测[3]。该系统可以很容易地在任意一个节点上进行安装和配置，不会对整个系统操作造成很大干扰。因此，基于该原理设计了网络链路数据篡改自主防御系统硬件结构，并在此基础上，为防止译码功能进行开放源代码的参数化，添加了分层协同解码模块及多条个性化规则兼容优化。

1.1 防火墙入侵数据包嗅探器

数据包嗅探器的主要作用是在网络中捕捉Snort的报文，然后根据传输控制协议/网际协议(Transmission Control Protocol/Internet Protocol，TCP/IP)的级别对报文进行分析。数据包嗅探器结构如图1所示。

Snort通过Linux防火墙获取大量的数据，数据采集完成后，将其上传至防火墙进行相关操作。数据包嗅探器将搜索和安全报文抓取功能集于一体，当设备处于持续的接入模式时，备份数据迅速占满整个系统数据库的数据储存空间[4-6]。在入侵数据积累下，可迅速生成一个可阅读主体。该主体经过文件过滤后形成编译体结构，结构中的数据会慢慢靠近被捕获的系统，最后变成一个固定的数据包结构体[7]。

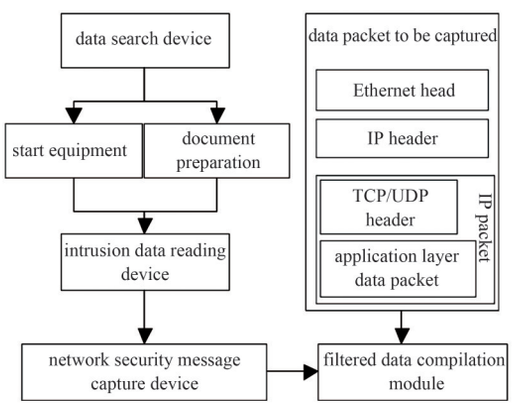


Fig.1 Structure of packet sniffer

图1 数据包嗅探器结构

1.2 信息分层协同解码模块

信息解码模块中的信息译码部分主要完成网络安全应用程序的传输和包装。通过该功能，可根据已有的探测和防止译码功能进行开放源代码的参数化[8]。信息解码模块结构如图2所示。

在入侵信息到达系统网关后，该信息译码模块会从断开状态转换为连接状态，在TCP/IP的影响下，该机制的各个层级可对该分组进行分层译码，并将最后的处理结果整合成文本信息[9-10]。为保证传输安全，不能将所有的文本信息都传送至底层的应用程序中，而是将其保存在一个临时的检测和预处理模块中，然后通过网络将其发送至系统数据库中。

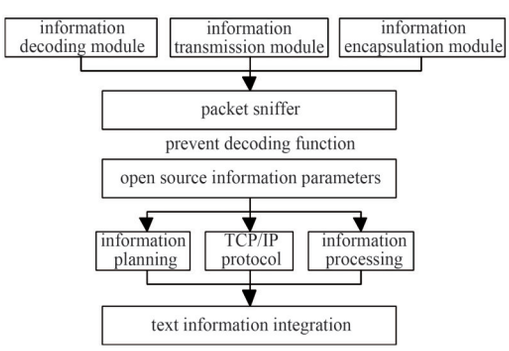


Fig.2 Structure of information layered collaborative decoding module

图2 信息分层协同解码模块结构

1.3 数据库服务器模块

数据库服务器的任务是采集来自入侵的警报信息，然后存储在一个关联数据库中。运用关联数据库组织和处理具有较大信息量的警报数据，是目前最有效的手段[11]。在警报存储器中，可将警报数据进行归类、检索及排序等。本系统使用MySQL数据库，MySQL是一种功能强大、灵活性好、应用程序编程接口多、系统架构巧妙的数据库管理体系[12]。启动MySQL数据库，在Snort文件夹下，利用Snort中的指令码，为Snort提供必要的数据表格，用于存储记录警报数据。

1.4 Snort 规则兼容配置优化模块

Snort 网页是针对用户访问控制的主要应用程序，可通过 IP 地址的输出方式决定相应的用户名。如果在每个配置过程中产生一个单独发送文档，则 Snort 可根据用户需要自由设定 Snort 页[13]，该规则组态模组可使用户设定的 Snort 检测规则变得独立且具有个性化。为使该模组与 Snort 执行主系统具有同一守护程式通信，需更改 Snort 检测概要[14]。该模块通过在本地平台备份 Snort.conf，可使 Snort 入侵检测系统的平台界面对 Snort.conf 和所有规范进行兼容性更改，并将其与 Snort Recorder 进行通信，将修改后的 Snort.conf 和所有规则文档传送至初始文件集中，重新启动 Snort，为网络链路数据篡改自主防御提供基本规则。

2 系统软件部分设计

在各项硬件设备元件的支持下，构建基于 Snort 的网络纵深防御模型。通过 Snort NIDS(Network Intrusion Detection System)探测子网，实现对各个子网进行实时探测和自动截获；通过篡改攻击检测过程，计算不同节点间数据传输距离，进而确定防御节点；通过构建数据篡改自主防御函数，实现数据篡改自主防御。

2.1 基于 Snort 的网络纵深防御模型构建

在网络纵深防御中，攻击者的目的是为了获得更大带宽。为达到自主防御目的，需在攻击过程中对目标节点进行数据包阻断。Snort 协议是一种基于转发机制的路由协议，可为网络防御提供一个高效的路径选择策略。为此，本文构建基于 Snort 的网络纵深防御模型，有效应对网络攻击中的路径选择问题。通过增加 inline，可以很容易地建立入侵防御屏障，同时该模型具备了实时探测和主动反应能力，是建设一个强大的网络安全体系的理想方案[15]。

在 Snort 的入侵性防范机制的末尾处理环节，根据规范显示的真实级别，计算系统最大存储信息量：

$$\lambda=\left(Rx-\frac{e\left|E_2-E_1\right|^2}{S}\right)\times\frac{1}{t\delta} \tag{1}$$

式中：R 为 Snort 检测数据识别权限；x 为单位时间内数据输入量；e 为相关数据检测防御量化差值；S 为待展示规则数据量级水平，该值越大，说明入侵行为过滤结果越精准；t 为 Snort 网络检测时长；δ 为数据特征指标；E_1、E_2 分别为 2 个入侵数据的入侵强度。

通过分析网络流量数据，识别异常流量模式，如数据包的突然增加或减少、传输速率的异常变化。基于此，确定篡改攻击的具体节点数量及位置。在篡改自主防御过程中受链路层影响，不同层级之间数据随意交换，使链路层受到网络篡改和冲突。因此，加强对链接层的攻击探测，提高其抵抗能力。基于 Snort 的网络纵深防御模型如下：

$$\mu=\frac{\sqrt{x_t-y_t}}{\lambda\times\varphi\times\left(i^2-j^2\right)\sum_{t=1}x_t} \tag{2}$$

式中：φ 为链路层受到篡改攻击出现信号的强弱；i、j 分别为链路数据层全部篡改攻击节点和网络传输数量；x_t 为传输链路总数据输入集；y_t 为包含所有数据传输链路层种类集。

可使用 NIDS 保证网络的安全性。在该安全领域的各个子网中，利用 Snort NIDS 探测子网，然后通过网络管理员进行相应的分析和处理。各领域中的入侵检测/防御系统不会分离，而是与其他领域中的入侵检测/防御系统相关。在特定的关键领域，采用网络入侵防御系统(Network-based Intrusion Prevention System，NIPS)技术，实现实时探测和自动截获，避免对系统的破坏。

2.2 网络链路数据篡改自主防御

通过构建的网络纵深防御模型，获取系统最大存储信息量；通过确定防御节点，准确判断出链接数据受到恶意程序或数据侵害节点位置，推导出链路层数据受到篡改攻击时的数据传输路径；根据检测出的数据，构建数据篡改自主防御函数，从而实现数据篡改自主防御。

2.2.1 防御节点确定

通过篡改攻击检测过程，准确判断出链接数据是否受到恶意程序或数据侵害，保证后续防御节点的建立。防御节点建立步骤为：

1) 假定链路是一个双向的数据链接，以 A 为传输节点，将数据传送至节点 B，而节点 B 也可将数据传送至节

点 A，由此导出在链路层中的每一个节点都具有相应的密钥。节点 A 的密钥为 $(c_{\mathrm{r}},c_{\mathrm{e}})$，其中 c_{r} 为公共密钥，c_{e} 为隐私密钥；

2) 在确定防御节点的定位过程中，根据网络中信息包传递特性，确定被入侵网络中数据分组发送间隔，并获取不同节点间的传输距离：

$$L_{ab}=\sum_{k=1}^{n}t_{ak}\times v_k \tag{3}$$

式中：L_{ab} 为节点 A 和节点 B 之间的总传输距离；n 为节点 A 和节点 B 之间链路的数量；t_{ak} 为信号在第 k 个链路上的传输时间；v_k 为第 k 个链路的实际传输速度。

3) 规划已知传输域范围，当节点 A 将数据分组发送至节点 B 时，该节点会被计算出启动速度。这样不断重复，可计算出传送和接收时间间隔 Δt。根据传送距离，得出 2 个节点之间的单程传输距离为：

$$G=\left(\frac{\Delta t}{2}\right)\times v \tag{4}$$

式中 v 为实际节点间传输速度。通过式(4)可以判断出 2 个节点之间的位置，从而确定防御节点位置。

假设有 3 个已知位置的节点 A、B、C，它们到目标节点 D 的距离分别为 G_{AD}、G_{BD} 和 G_{CD}，则目标防御节点 D 必然位于以 A、B、C 为圆心，相应距离为半径的 3 个圆的交点上。通过方程组(5)找到目标防御节点 D 的坐标：

$$\begin{cases}(x_D-x_A)^2+(y_D-y_A)^2=G_{AD}^2\\(x_D-x_B)^2+(y_D-y_B)^2=G_{BD}^2\\(x_D-x_C)^2+(y_D-y_C)^2=G_{CD}^2\end{cases} \tag{5}$$

求解该方程组可得到目标防御节点 D 的估计位置 (x_D,y_D)。

2.2.2 数据篡改自主防御

在确定防御节点情况下，建立路径选择函数。在建立路径选择函数 $F(a,b)$ 时，综合考虑多个因素，包括节点间的传输距离、攻击概率：

$$F(a,b)=\alpha G+\beta R(a,b) \tag{6}$$

式中：α 与 β 为权重系数，用于调整传输距离和攻击风险在路径选择中的重要程度；$R(a,b)$ 为节点 A 到节点 B 的路径中遭受的攻击风险：

$$R(a,b)=\sum_{a=1,b=1}^{m}(S_mP_m) \tag{7}$$

式中：m 为路径上的一个节点；S_m 为节点 m 的安全状态评分；P_m 为数据通过节点 m 时遭受攻击的概率。

根据路径选择函数 $F(a,b)$ 确定受到篡改攻击时的数据传输路径，并根据篡改攻击时链路数据发出的信号，可获取检测数据：

$$x=\max_{\alpha}\frac{1}{2}\sum_{i=1}^{t}\sum_{j=1}^{t}E_iE_j\varsigma_i\varsigma_jL(z_iz_j) \tag{8}$$

式中：$\max\limits_{\alpha}$ 为防御最大检测数值；E 为数据受攻击阈值，根据节点的安全状态进行阈值设定：$E\leqslant 1-S_m$；ς 为数据检测阈值，根据防御最大检测数值进行阈值设定：$\varsigma\leqslant\max\limits_{\alpha}$；$z$ 为实际检测数据取值范围。

将检测数据通过 Snort 规则兼容配置模块重新配置后，得到数据篡改自主防御函数为：

$$h(z)=\mathrm{sgn}\left\{\sum_{i=1}^{t}\varsigma_iE_iL(z_i)+\omega\right\} \tag{9}$$

式中 ω 为受攻击阈值取值范围。

经过以上计算可以看出，网络中的网络信息被篡改的程度越高，所检测节点也越容易捕捉到攻击信号，由此实现数据的自主防御。

2.3 基于小波去噪的噪声数据处理

由于受到的攻击次数和类型越来越多，所需的运算和检测数据的节点数目也越来越多，超过了负载。当网络中的数据被传送时，网络被入侵的概率会不断增大，在光纤网的传输中，由于存在噪声，造成有用信息的遮挡，影响后续的数据检测，使被攻击的探测能力逐渐减弱，直至最终无法做出正确判断，造成检测失效。因此，必须对光缆线路中的数据进行降噪处理。为此，提出一种基于小波去噪的数据处理技术。

网络链路层连接数据可表示为：

$$f(x)=g(x)+\gamma(x) \tag{10}$$

式中：$g(x)$为原始链路数据；$\gamma(x)$为白噪声。

采用离散采样方法对链路层数据采样，获取 n 个离散信号，然后应用阈值法进行去噪。利用小波对光纤网络中的含有噪声的传输信号进行处理，从而获得时序数据：

$$T=\frac{\text{median}(|D1|)}{dB}\sqrt{2\ln\varepsilon}/\log_2(k+1) \tag{11}$$

式中：$D1$ 为第一层分解系数；dB 为小波基；ε 为数据长度；k 为分解层数。分解系数 $D1$ 反映了原始信号与噪声的相对强度。较大的分解系数 $D1$ 意味着原始信号中所包含的有效信息相对较强，而噪声相对较弱。在密钥恢复过程中，较大的 $D1$ 值有助于提取到更多的有效信息，从而提高密钥恢复成功率。分解层数 k 决定了小波分解的深度和细节级别。较大的 k 值表示进行了更深的分解，可获得更多的细节信息，确保密钥恢复的成功性。

通过上述时序数据的获取对信号进行小波分解，分解后可获取小波系数；再利用小波逆变换，结合傅里叶逆变换方法进行数据重构，如图 3 所示。

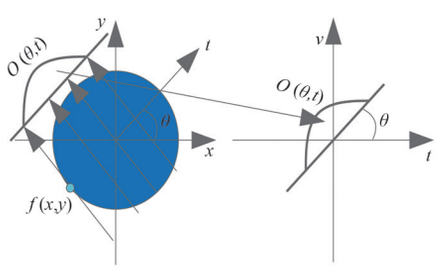


Fig.3 Data reconstruction based on inverse Fourier transform
图 3 基于傅里叶逆变换数据重构

表 1 实验参数

Table1 Experimental parameters

parameter	value
distance between nodes/km	300
transmission speed/Gbps	60
fiber optic network configuration	multimode
number of attacked nodes	4
tampering attack signals strength	40% of data has been tampered
attack threshold	5% data tampering rate
number of defense nodes	5
packet size/MB	0.001~1
data packet transmission frequency/(packs/s)	100~800
alarm threshold	0.1

由图 3 可知，假设每旋转 1°就重新扫描一次，当数据旋转 180°之后，可获取 180 根投影线。对 180 个投影信号进行傅里叶变换处理，可获取一维频域信号；根据相对应的扫描角度，在空间旋转排列后，获取二维频域空间；再通过数据拼接处理，可得到重构数据。

3 实验

对基于 Snort 的网络链路数据篡改自主防御系统，从网络链路数据安全传输密度和有干扰的密钥恢复成功率 2 个维度进行系统鲁棒性实验。实验参数设定如表 1 所示。

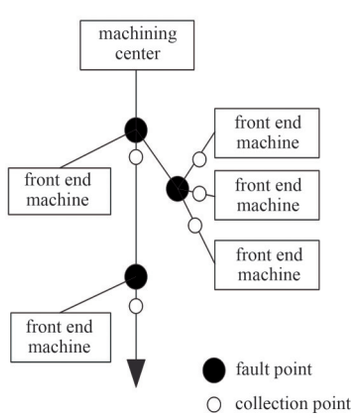


Fig.4 Topology diagram of network link
图 4 网络链路拓扑结构图

实验参数对基于 Snort 的网络链路数据篡改自主防御系统的鲁棒性实验结果至关重要：节点间距离会影响数据传输延迟；传输速度决定传输效率；多模光纤提高容量和效率；模拟攻击涉及节点会影响防御复杂性；数据篡改程度体现攻击强度；数据篡改率的阈值关乎防御反应时机、防御节点覆盖范围和冗余度；数据包损失率大小会触发安全警报。这些参数共同决定了系统挑战和性能表现，通过调整参数评估系统鲁棒性和性能。

3.1 网络链路数据采集

将网络传感器布局在图 4 所示的额定位置上，利用光纤光栅传感器进行数据采集，设置采集时间间隔为 3 s。

3.2 网络链路数据安全传输密度实验分析

数据安全传输密度是指成功传输的有效数据量与总链路容量的比值。将防御节点放置在链路的关键位置，可更有效地控制数据流量，监测和过滤潜在的恶意流量或篡改攻击，提高链路数据传输的安全性，对于评估系统的性能、效率和安全性至关重要。其表达式为：

$$D=\frac{M_{\mathrm{a}}}{M_{\mathrm{f}}} \tag{12}$$

式中：M_{a}为成功传输的数据量；M_{f}为总链路容量。

在完全无侧信道防御上进行系统测试，分别使用基于数据挖掘的异常数据检测方法、基于大数据的安全防御系统和基于Snort的篡改自主防御系统，分析网络链路数据安全传输密度，如图5所示。

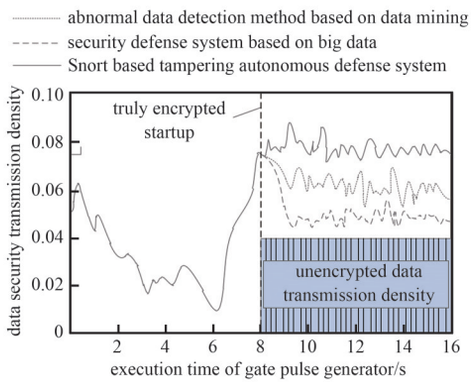


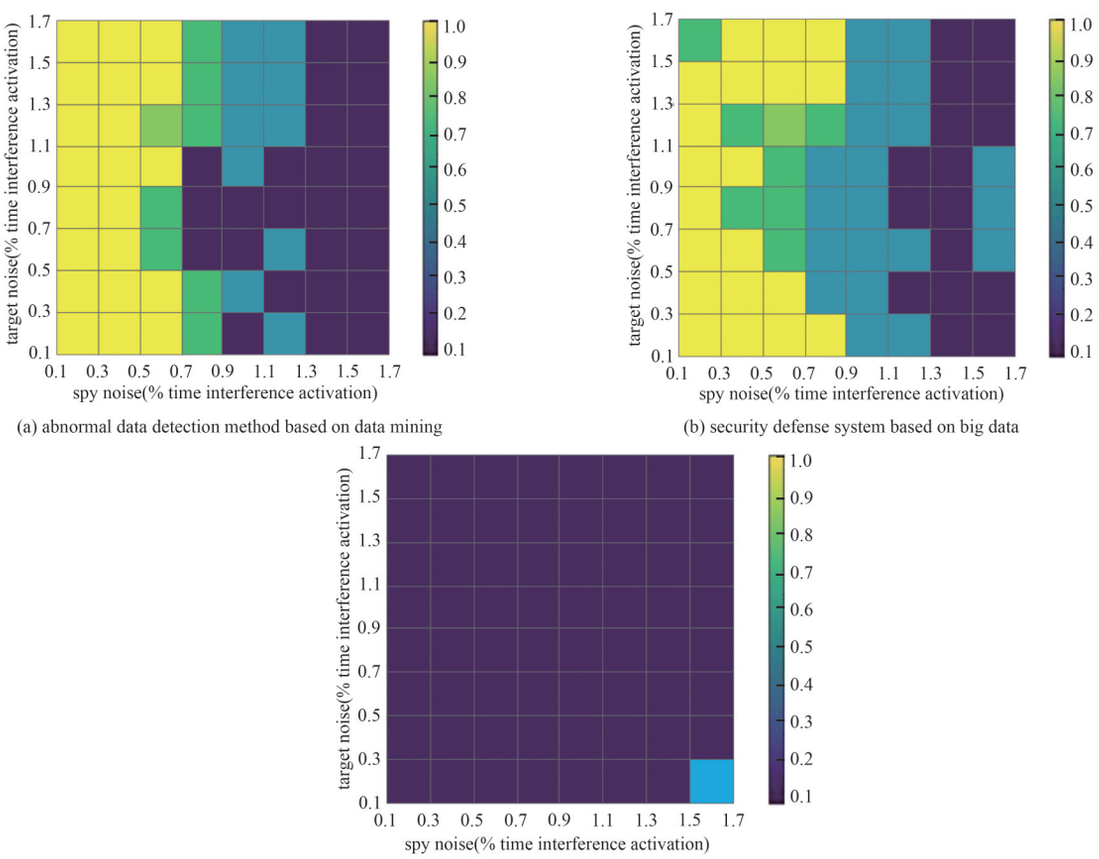
Fig.5 Experimental results of network link data security transmission density

图5 网络链路数据安全传输密度实验结果

由图5可知，3种方法均比无加密数据传输密度高，使用基于Snort的篡改自主防御系统在密钥相关程序开始时与其他两种方法存在显著差异，说明使用所设计系统数据安全传输密度显著较高，证明了系统应用可靠性较高。

3.3 有干扰的密钥恢复成功率实验分析

在网络链路层数据传输过程被干扰情况下，测试系统的鲁棒性。将3种方法进行对比，结果如图6所示。由图6可知，使用基于数据挖掘的异常数据检测方法有干扰的密钥恢复成功率比基于大数据的安全防御系统要高，但比基于Snort的篡改自主防御系统要低。基于Snort的篡改自主防御系统最大密钥恢复成功率可达到98%，说明所设计系统具有较强鲁棒性，可抵御干扰，避免传输信道受噪音影响，具有精准传输效果。



(a) abnormal data detection method based on data mining

(b) security defense system based on big data

(c) Snort based tampering autonomous defense system

Fig.6 Experimental results of key recovery success rate with interference

图6 有干扰的密钥恢复成功率实验结果

4 结论

面对网络安全日益凸显的问题，设计了基于Snort的网络链路数据篡改自主防御系统。将开源软件Snort作为一种防御手段，通过构建基于Snort的网络纵深防御模型，实现对篡改攻击实时探测和自动截获；利用Snort NIDS加强对链接层的攻击探测，通过计算不同节点间传输距离，确定防御节点位置；构建数据篡改自主防御函数，实现数据的自主防御。实验结果表明，设计系统的数据安全传输密度高，最大密钥恢复成功率可达到98%，说明所设计系统具有较强鲁棒性，可抵御干扰，避免传输信道受噪音影响，具有精准传输效果。

参考文献：

[1] 马莉莉,刘江平. 基于数据挖掘的光纤通信网络异常数据检测研究[J]. 应用光学, 2020,41(6):1305-1310. (MA Lili,LIU Jiangping. Research on abnormal data detection of optical fiber communication network based on data mining[J]. Journal of Applied Optics, 2020,41(6):1305-1310.) doi:10.5768/JAO202041.0608003.

[2] 齐赫,刘光楠. 基于大数据的计算机网络安全防御系统构建[J]. 材料保护, 2021,54(3):214-215. (QI He,LIU Guangnan. Construction of computer network security defense system based on big data[J]. Materials Protection, 2021,54(3):214-215.)

[3] 杨昕,李挥,邬江兴,等. 融合广义随机Petri网的二维拟态安全评估模型[J]. 中国科学:信息科学, 2020,50(12):1944-1960. (YANG Xin, LI Hui, WU Jiangxing, et al. A two-dimension security assessing model for CMDs combined with Generalized Stochastic Petri net[J]. Scientia Sinica(Informationis), 2020,50(12):1944-1960.)

[4] 周刚,吴树霖,张江龙,等. 基于拓扑链路识别的光网络流量数据合成算法[J]. 光通信研究, 2022(1):31-36. (ZHOU Gang,WU Shulin,ZHANG Jianglong, et al. Traffic data synthesis algorithm for optical network based on topological link recognition[J]. Study on Optical Communications, 2022(1):31-36.) doi:10.13756/j.gtxyj.2022.01.007.

[5] 刘广睿,张伟哲,李欣洁. 基于边缘样本的智能网络入侵检测系统数据污染防御方法[J]. 计算机研究与发展 ,2022,59(10):2348-2361. (LIU Guangrui, ZHANG Weizhe, LI Xinjie. Data contamination defense method for intelligent network intrusion detection systems based on edge examples[J]. Journal of Computer Research and Development, 2022,59(10):2348-2361.) doi:10.7544/issn1000-1239.20220509.

[6] 丁朝晖,张伟,杨国玉. 基于动态伪装技术的网络安全防御系统研究[J]. 电子技术应用, 2022,48(1):129-132. (DING Zhaohui, ZHANG Wei, YANG Guoyu. Research on network security defense system based on dynamic camouflage technology[J]. Application of Electronic Technique, 2022,48(1):129-132.) doi:10.16157/j.issn.0258-7998.211522.

[7] 高春刚,王永杰,熊鑫立. MTD增强的网络欺骗防御系统[J]. 计算机工程与应用, 2022,58(15):124-132. (GAO Chungang, WANG Yongjie, XIONG Xinli. MTD enhanced cyber deception defense system[J]. Computer Engineering and Applications, 2022,58(15):124-132.) doi:10.3778/j.issn.1002-8331.2105-0169.

[8] 王小瑞,陈冬冬,何红杰. 一种基于蚁群算法的深空光通信网络链路性能研究[J]. 光通信技术,2022,46(4):22-26. (WANG Xiaorui,CHEN Dongdong,HE Hongjie. Research on link performance of deep space optical communication network based on ant colony algorithm[J]. Optical Communication Technology, 2022,46(4):22-26.) doi:10.13921/j.cnki.issn1002-5561.2022.04.004.

[9] 徐飞阳,薛安成,常乃超,等. 电力系统自动发电控制网络攻击与防御研究现状与展望[J]. 电力系统自动化, 2021,45(3):3-14. (XU Feiyang, XUE Ancheng, CHANG Naichao, et al. Research status and prospect of cyber attack and defense on automatic-generation control in power system[J]. Automation of Electric Power Systems, 2021, 45(3): 3-14.) doi: 10.7500/AEPS20200331013.

[10] MIN Minghui, XIAO Liang, XIE Caixia, et al. Defense against advanced persistent threats in dynamic cloud storage: a Colonel Blotto game approach[J]. IEEE Internet of Things Journal, 2018,5(6):4250-4261.

[11] 甘瑞蒙,贾泽坤,王洋洋,等. 无人机辅助车联网的网络传输链路优化[J]. 太赫兹科学与电子信息学报, 2022,20(7):673-677, 696. (GAN Ruimeng, JIA Zekun, WANG Yangyang, et al. Optimization of network transmission link in UAV assisted vehicle network[J]. Journal of Terahertz Science and Electronic Information Technology, 2022, 20(7): 673-677, 696.) doi: 10.11805/TKYDA2021237.

[12] 杨惠. 基于Q-Learning反馈机制的无线传感网络通信节点自愈算法[J]. 传感技术学报, 2022,35(7):974-979. (YANG Hui. Self-healing algorithm of wireless sensor network communication node based on Q-Learning feedback mechanism[J]. Chinese Journal of Sensors and Actuators, 2022,35(7):974-979.) doi:10.3969/j.issn.1004—1699.2022.07.016.

[13] 连鸿鹏,程志强,余丰盈. 光纤通信网络中链路数据篡改攻击与防御方法[J]. 激光杂志, 2022,43(8):125-129. (LIAN Hongpeng,CHENG Zhiqiang,YU Fengying. Attack and defense of link data tamper in optical fiber communication network[J]. Laser Journal, 2022,43(8):125-129.) doi:10.14016/j.cnki.jgzz.2022.08.125.

[14] 孙凯祺,邱伟,李可军,等. 面向快速频率响应系统的网络攻击防御控制策略[J]. 中国电机工程学报, 2021,41(16):5476-5486. (SUN Kaiqi, QIU Wei, LI Kejun, et al. Cyber attack defense control for fast frequency response system[J]. Proceedings of the CSEE, 2021,41(16):5476-5486.) doi:10.13334/j.0258-8013.pcsee.210038.

[15] 高翔. 基于知识图谱的通信网络链路数据篡改攻击保护方法[J]. 通信与信息技术, 2023(4):57-59,95. (GAO Xiang. Method for protecting communication network link data tampering attacks based on knowledge spectrum graph[J]. Communication & Information Technology, 2023(4):57-59,95.)

作者简介：

何　君(1973-)，男，学士，工程师，主要研究方向为电力生产网络安全.email:qiudong6080@163.com.

王　文(1979-)，男，学士，政工师，主要研究方向为电力生产网络安全.

陈　侃(1988-)，男，学士，工程师，主要研究方向为电力生产网络安全.

何成胜(1996-)，男，学士，助理工程师，主要研究方向为电力生产网络安全.

滕　易(1992-)，男，学士，工程师，主要研究方向为电力生产网络安全.

（上接第1261页）

[20] 蒋伊琳,刘梦楠,郜丽鹏,等. 运动多站无源时差/频差联合定位方法[J]. 系统工程与电子技术, 2019,41(7):1441-1449. (JIANG Yilin, LIU Mengnan, GAO Lipeng, et al. Multi-station passive time difference/frequency difference joint positioning method for sports[J]. Journal of Systems Engineering and Electronics, 2019,41(7):1441-1449.)

[21] 郭福成. 空间电子侦察定位原理[M]. 北京:国防工业出版社, 2012:96-97. (GUO Fucheng. Localization principles in space electronic reconnaissance[M]. Beijing:National Defense University Press, 2012:96-97.)

[22] ZHANG Wei,ZHANG Gengxin. An efficient algorithm for TDOA/FDOA estimation based on approximate coherent accumulative of short-time CAF[C]// 2011 International Conference on Wireless Communications and Signal Processing(WCSP). Nanjing, China:IEEE, 2011:1-4. doi:10.1109/WCSP.2011.6096807.

[23] 刘晶晶,吴传生. 一种带杂交算子的改进的粒子群优化算法[J]. 青岛科技大学学报(自然科学版), 2008,29(1):3. (LIU Jingjing, WU Chuansheng. An improved particle swarm optimization algorithm with hybrid operator[J]. Journal of Qingdao University of Science and Technology(Natural Science Edition), 2008,29(1):3.)

[24] LEUNG Y W, WANG Y P. An orthogonal genetic algorithm with quantization for global numerical optimization[J]. IEEE Transactions on Evolutionary Computation, 2001,5(1):41-53. doi:10.1109/4235.910464.

作者简介：

杨　光(1998-)，男，在读硕士研究生，主要研究方向为卫星无源定位.email:yg19991314@163.com.

屈德新(1966-)，男，博士，副教授，博士生导师，主要研究方向为卫星无源定位、卫星通信等.

张更新(1966-)，男，博士，教授，博士生导师，主要研究方向为卫星通信、卫星导航与测控、深空通信等.