计算机科学
COMPUTER SCIENCE

基于模糊逻辑的物联网流量攻击检测技术综述

商钰玲，李鹏，朱枫，王汝传

引用本文

商钰玲，李鹏，朱枫，王汝传. 基于模糊逻辑的物联网流量攻击检测技术综述[J]. 计算机科学，2024，51(3)：3-13.

SHANG Yuling, LI Peng, ZHU Feng, WANG Ruchuan. Overview of IoT Traffic Attack Detection Technology Based on Fuzzy Logic [J]. Computer Science, 2024, 51(3): 3-13.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230700130

基于模糊逻辑的物联网流量攻击检测技术综述

商钰玲[1]　李　鹏[1,2]　朱　枫[1]　王汝传[1,2]
1 南京邮电大学计算机学院　南京 210023
2 南京邮电大学网络安全与可信计算研究所　南京 210023
(1022041221@njupt.edu.cn)

摘　要　物联网越来越多地出现在日常活动中,将我们周围多样化的物理设备连接到互联网,奠定了智慧城市、电子健康、精准农业等应用的基础。随着物联网应用的迅速普及,针对这类设备和服务的网络攻击数量也有所增加,且这些攻击具有不精确性和不确定性,使得对其进行正确检测和识别更加困难。为了应对上述挑战,学者们引入了基于模糊逻辑的攻击检测框架,在各种操作步骤中结合不同的模糊技术,以便在数据不准确和不确定时更精确地检测网络攻击。文中首先对物联网的安全性进行了详细的探讨,如其应对的安全挑战、所需的安全要求、面临的攻击类型等;其次对入侵检测系统(Intrusion Detection Systems,IDS)进行了描述,进而简述了物联网中IDS的基础框架;然后阐述了模糊逻辑的技术原理,分析了将其应用在流量攻击检测中的合理性;接着比较了各种基于不同技术的流量攻击检测方案,以说明它们在该领域的性能和重要性;最后总结了本文的主要工作,指出了未来的研究方向,为该领域的研究者提供了新的视角,以更好地应对不断升级的网络攻击。

关键词:模糊逻辑;物联网;攻击检测;流量;网络安全
中图分类号　TP311

Overview of IoT Traffic Attack Detection Technology Based on Fuzzy Logic

SHANG Yuling[1],LI Peng[1,2],ZHU Feng[1] and WANG Ruchuan[1,2]
1 College of Computer Science,Nanjing University of Posts and Telecommunications,Nanjing 210023,China
2 Institute of Network Security and Trusted Computing,Nanjing University of Posts and Telecommunications,Nanjing 210023,China

Abstract　The Internet of things(IoT) is progressively permeating our daily activities,interconnecting an array of diverse physical devices to the Internet. This foundational connectivity underpins applications spanning smart cities,e-health,precision agriculture,and beyond. The swift proliferation of IoT applications,however,has been paralleled by an upsurge in the frequency of network attacks targeting these devices and services. The complex and dynamic nature of these attacks,coupled with their imprecision and uncertainty,has significantly compounded the intricacies of accurate detection and identification. In response to these exigencies,a novel approach has emerged in the form of fuzzy logic-based attack detection frameworks. These frameworks strategically integrate varied fuzzy techniques throughout diverse operational phases to facilitate heightened precision in the detection of network attacks,particularly in instances characterized by data inaccuracy and uncertainty. Within the expanse of this comprehensive survey paper,a meticulous exposition unfolds. It commences by delving deeply into the realm of IoT security,dissecting its multifaceted dimensions,such as the security challenges it responds to,the required security requirements,and the types of attacks it faces. Subsequently,it offers a detailed portrayal of intrusion detection systems(IDS) and further encapsulates the foundational framework of IDS within the IoT domain. The foundational tenets of fuzzy logic are subsequently expounded upon,followed by a discerning analysis of the rational underpinning the integration of fuzzy logic in traffic attack detection. In subsequent sections,a discerning comparative analysis of diverse traffic attack detection schemes,grounded in disparate technological methodologies,is meticulously presented. This analytical elucidation underscores their respective performance metrics and,by extension,their pivotal significance within this burgeoning sphere. Finally,the synthesis of the principal contributions encapsulated within this paper is meticulously articulated,concurrently outlining pathways for future research. These nascent trajectories are expected to provide researchers with new perspectives and enrich the academic discourse to mitigate escalating cyberattacks.

Keywords　Fuzzy logic,Internet of things,Attack detection,Traffic,Network security

到稿日期:2023-07-18　返修日期:2023-11-28
基金项目:国家自然科学基金(62102196);江苏省六大人才高峰高层次人才项目(RJFW-111)
This work was supported by the National Natural Science Foundation of China(62102196) and Six Talent Peaks Project of Jiangsu Province (RJFW-111).
通信作者:李鹏(lipeng@njupt.edu.cn)

1 引言

近年来，物联网系统在许多应用领域发挥了重大效益，包括医疗保健、公民生活质量（如电子融合）、物流与供应链管理、农牧业、智慧城市、智能电网、智能家居、环境监测、公共安全、数字孪生设计等[1]。随着物联网技术的快速发展，各种恶意攻击和网络入侵事件频发，威胁越来越大，危害也越来越严重。网络安全已经成为越来越多人关注的焦点。

目前，工业界已经实施了许多技术来保护物联网系统免受外部非法攻击，例如使用防火墙、防病毒软件和 IDS[2-5]。IDS 旨在根据规则、特征或模型区分正常和系统入侵[4]。它在检测未经授权的使用以及识别系统的更改和破坏方面发挥着重要作用[3]，因经过验证的效率和有效性而受到广泛关注[6]。入侵检测方法分为两类：异常检测和误用检测[7]。IDS 的异常检测方案定义了正常行为，与正常行为有任何偏差将被视为入侵，虽然该方法能够处理新型攻击，但在包含众多用户的大型动态组织中定义和更新正常行为并非易事[8]。另一方面，误用检测方法通过查找预先指定的攻击模式和特征来识别入侵，但其缺点是无法应对新型攻击。IDS 研究领域的主要问题是采用何种技术和算法来准确有效地检测恶意行为和入侵者。

针对上述问题，研究人员进行了多项研究，以提高检测的精确率和稳定性[9-11]。近年来，研究者们将决策树、神经网络和模糊逻辑等人工智能方法用于检测网络异常，其中基于模糊逻辑的系统在处理清晰边界问题上有许多优点，相比其他人工智能技术有更突出的优势[12]。术语模糊逻辑[13]是由 Zadeh 于 1965 年在其提出的模糊集合论中引入的，表示模糊和不精确信息的数学方法，属于能够指定中间值的多值逻辑。研究发现，基于模糊逻辑的检测框架具有计算模糊信息可用性的能力[14]。传统的控制系统依赖于环境的准确表示，而这在现实中通常不存在。模糊逻辑系统可以自然地处理语言规则，能够通过混合不同的参数产生合适的结果。此外，模糊规则使我们能够高效、轻松地构建 if-then 规则，以反映描述安全攻击的一般方式[15]。因此，模糊逻辑可以成为定义网络攻击的适当手段[15]。

研究表明，模糊逻辑技术在物联网领域的入侵检测中具有一定的适用性[16-17]。在物联网环境中，流量和事件的特征往往是模糊的，传统的二值逻辑可能无法准确地描述和处理这些模糊性。模糊逻辑技术通过模糊集合、模糊推理等方法，能够更好地处理这种模糊性，并提供更灵活的决策能力，帮助系统更好地适应动态的环境和未知的攻击模式，降低误报率，并提高系统的鲁棒性和准确性。

本文对各种最先进的针对物联网环境的模糊入侵检测方案进行了广泛的调查和分类，为了关注最新和重要的研究，在数据库中的查询输出已经过优化，仅包含最近五年发表的论文，同时排除了贡献不足或未进行必要的评估和验证步骤的文章。本文首先介绍了有关物联网安全、IDS、模糊逻辑的基本背景问题，然后对所提出的基于模糊逻辑的物联网流量攻击检测框架进行了分类，这些框架涉及其中使用的模糊算法和技术。本文重点讨论了每个入侵检测方案如何适应基于模糊逻辑的技术，以有效地处理特征选择和分类阶段的网络流量，提高检测性能。此外，还分析了检测方案的主要性质和局限性。本文的贡献总结如下：

1）简要概述了为保护物联网系统安全而提出的各种类型的入侵检测方案。

2）对所研究的基于模糊的物联网流量攻击检测方案进行分类，并描述了其架构和主要贡献。

3）强调了所研究的攻击检测方案的主要性质和局限性，并对其进行比较。

4）阐明了物联网环境中，基于模糊逻辑的入侵检测未来可能的关键研究领域。

2 研究背景

2.1 物联网安全

2.1.1 安全挑战

文献[18]中提出了一项调查，并重点关注严格检查物联网系统防御性能的必要性。入侵者的意图是通过发起一些攻击破坏系统，以发现网络中的漏洞并从敏感信息中获利。由于节点数量多、内存和处理能力低、能量受限，物联网安全极具挑战性[19-22]。主要的挑战如下：

1）大规模连接性：物联网连接了大量设备，这增加了攻击面。攻击者可以通过物联网设备入侵网络，造成数据泄露、服务中断等问题。

2）弱密码和认证机制：由于物联网设备的限制，如资源受限和计算能力较低，设备常常使用弱密码或不安全的认证机制，这使得攻击者更容易入侵。

3）数据隐私和保护：物联网设备收集了大量敏感数据，如个人身份信息、位置信息等，这些数据的泄露可能导致严重的隐私泄露问题。

4）更新和漏洞管理：物联网设备通常长时间运行，而且制造商可能不会及时提供安全更新和修补程序，这使得设备容易受到已知漏洞的攻击。

2.1.2 安全要求

物联网环境中所用协议和数据的异构性使得在物联网系统中利用安全机制的要求更高[23-24]。为了确保物联网安全，有以下几个关键要求[23]：

1）机密性：物联网设备和传输的数据需要保持机密性，防止未经授权的访问和数据泄露。

2）完整性：确保物联网设备和数据的完整性，防止数据被篡改或恶意修改。

3）可用性：保持物联网服务的可用性，防止服务中断或拒绝服务攻击。

4）认证和授权：确保只有经过授权的用户或设备能够才访问和操作物联网系统。

2.1.3 攻击类型

物联网面临各种类型的攻击，以下是常见的物联网攻击类型：

1）传输层攻击：包括拒绝服务（Denial of Service，DoS）和分布式拒绝服务（Distributed Denial of Service，DDoS）攻击，通过超载网络资源来中断物联网服务或使之瘫痪。

2）硬件攻击：攻击者通过物理手段对物联网设备进行攻击，例如侵入设备内部、修改硬件或破坏设备等。

3）软件攻击：包括恶意软件、恶意代码注入和远程执行代码等方式，用于控制物联网设备、窃取敏感信息或操纵设备行为。

4）隐私侵犯：攻击者通过监听、窃取或篡改物联网设备传输的数据，侵犯用户隐私，可能导致个人身份信息泄露或个人活动被追踪。

5）身份伪造：攻击者伪装成合法用户或设备，获取未经授权的访问权限，从而获取敏感信息或执行恶意操作。

6）物理层攻击：利用物理特性对物联网设备进行攻击，如电磁干扰、无线信号干扰或物理破坏等。

2.2 入侵检测系统

入侵检测系统（IDS）旨在检测威胁并在造成严重损害之前阻止它们[25]。Scarfone[26]将 IDS 全面定义为“一个完整的系统，用于监控独立计算机系统或网络中的事件，进行分析以找出违反系统安全策略的冲突事件，并将其识别为来自恶意或未授权实体的活动”。IDS 的基本目的是自动化入侵检测，试图中断完整性、可用性或机密性。以下是文献[27]中所述的 IDS 的一些基本功能：

1）观察网络的行为和流量。

2）识别系统或网络中不需要的活动。

3）在发现不需要的活动时启动警报。

没有一个 IDS 可以为各种攻击提供完美的解决方案，但每个系统的构建都旨在提供完美的安全解决方案。本节介绍了文献[10]中的典型 IDS。根据图 1 所示，IDS 由 4 个基本模块组成，即数据收集、数据预处理、入侵识别以及报告和响应。在图 1 中，实线表示数据流或控制流，虚线表示对入侵的响应。

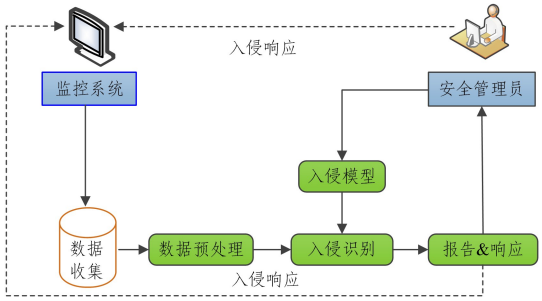


图 1 典型的入侵检测模型

Fig. 1 Typical intrusion detection model

1）数据收集：该模块负责从监视的系统收集审核数据。

2）数据预处理：此模块由一个或多个离散预处理器组成，以适合后续模块的格式量化和转换审计数据。

3）入侵识别：该模块负责根据入侵模型中提供的指令识别恶意活动。

4）入侵模型：此模块由安全管理员提供，包含已知入侵的行为配置文件以及将新到达的审核数据与配置文件进行匹配的说明。此外，它还能够从审计数据中获取有关异常行为的知识并对其进行相应的更新。

5）报告和响应：如果入侵识别模块检测到入侵，则该模块负责发起警报。

在物联网中，许多 IDS 是为网络流量设计的，它们通常由特征工程模块和分类器后端组成，如图 2 所示。

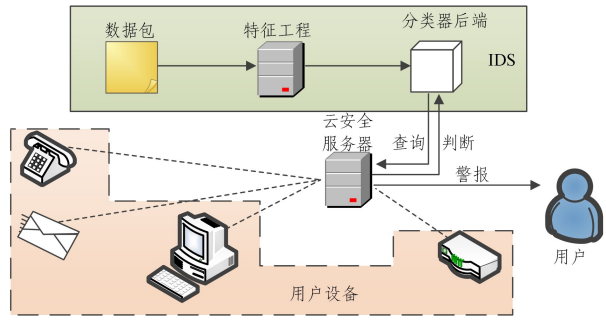


图 2 物联网系统中的 IDS

Fig. 2 IDS in IoT systems

2.3 模糊逻辑

模糊逻辑利用了语言变量，这些变量可以通过模糊集来定义。在模糊集合中，元素根据某种程度的成员资格归属集合。模糊推理系统尝试使用模糊 “if-then”规则将输入数据映射到输出数据。图 3 给出了模糊系统的架构，它由以下组件组成：

1）模糊化：模糊化是使用不相干隶属函数将数值信息（清晰尺度）转换为样本数据的技术。

2）规则库：抽象系统中一组基于专家的语言语句。此技术信息采用“if-then”规则集的形式。

3）模糊推理：根据模糊推理规则，采用模糊逻辑操作和推理方法，推理出模糊结论。非语言交流的过程包括所有揭示规则的隶属函数参数和运算符。

4）去模糊化：这是模糊化的逆过程。将模糊值转化为清晰值的过程被称为去模糊化。

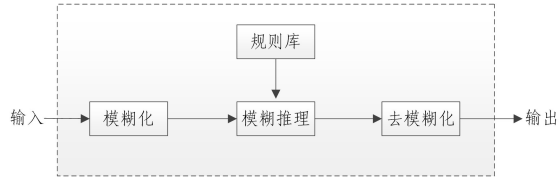


图 3 模糊系统架构

Fig. 3 Fuzzy system architecture

3 基于模糊逻辑的物联网流量攻击检测方案

本文对基于模糊逻辑的物联网流量攻击检测方案进行了广泛的调研，并根据使用的模糊技术将其分为 5 个类别，分别是模糊神经网络、模糊聚类、模糊粗糙集、模糊规则生成和模糊推理系统，本章将介绍这些方案的主要特点和贡献，并重点阐述相应的模糊技术在攻击检测过程中的运用。此外，我们在每个小节的末尾对各类模糊技术应用的代表性研究工作进行分析比较，如表 1－表 5 所列。

3.1 基于模糊神经网络的方案

模糊神经网络结合了模糊系统和神经网络，用神经网络的输入、输出表示模糊系统的输入、输出，将模糊系统的隶属

函数、模糊规则加入神经网络的隐含节点中，充分发挥神经网络的并行处理能力和模糊系统的推理能力，参考文献中提供了几种基于模糊神经网络的入侵检测方案。

Perumalla 等[28]在无人机物联网环境中提出了一种基于深度神经模糊网络的入侵检测机制，在使用熵函数对数据进行特征选择后，融合了神经网络与模糊逻辑，以降低峰值并将成本最小化，实现了有效优化。在考虑海王星攻击时，所提方案的端到端延迟、精确率和召回率明显优于传统方案，解决了传统方案面临的安全传输、时延和计算复杂度等问题，但没有考虑绩效评估的效率和吞吐量等指标。Mittal 等[29]提出了一种基于神经模糊网络的无线传感网入侵检测方案。该模型将数据集激发到自组织映射神经网络，将数据集分类为正常和异常聚类集。模糊规则将数据集排列为离散向量，并对信息包中的规律性和异常性进行深入检查，获得了非常熟练的特性识别框架，但该方案侧重于对无线传感网节点能耗的把控，未就神经模糊网络技术的使用在安全性上与其他技术进行比较。车辆自组织网络(Vehicular Ad-hoc Network，VANET)是物联网的一种重要组成网络，有潜力成为智慧城市中开放的数据交换平台，检测 VANET 系统中的攻击对于给所有车辆之间提供更安全可靠的通信非常重要，因此，Shubha 等[30]提出了一种基于多层感知器神经网络训练的模糊逻辑系统来检测 VANET 中汽车的异常行为。首先使用多层感知器神经网络和反向传播算法训练数据，之后将准备好的数据用于基于模糊逻辑的系统来检测攻击指标。与现有的聚类方法相比，该方案的误差率降低、精确率更高，有效检测了车辆在自组织网络中传递信息时的攻击。Hu 等[31]通过集成多个受限玻尔兹曼机和模糊神经网络，提出了一种基于多层神经网络的智能家居入侵检测算法。该算法应用 T-S 模糊神经网络算法作为监督分类器，利用输出误差来评估输出层的前一层误差，通过逐层传递学习获取其他层的误差估计值，以实现多层神经网络的权重微调。仿真结果表明，所提方案的检测准确率高于现有方法，对 DoS 和 R2L 攻击的检测准确率达到 94%，对正常行为的误检率低于 1%，被测新型攻击的检测准确率超过 60%，在智能家居网络入侵检测方面具有性能优势和良好的适应性。

Jang[32]于 1993 年首次提出了自适应神经模糊推理系统(Adaptive Neuro-Fuzzy Inference System，ANFIS)，该系统由 T-S 模糊推理系统和神经网络组成，在入侵检测领域得到了广泛的应用。ANFIS 在开始学习之前通过减法聚类或网格分割的方法创建模糊推理系统，并使用反向传播或最小二乘法调整模糊推理系统参数。Farhin 等[33]将软件定义网络(Software-Defined Network，SDN)的概念与物联网集成，提出了一种基于 ANFIS 的模糊神经网络(Fuzzy Neural Networks，FNN)架构，FNN 模型由 4 个 ANFIS 组成，结合不同 ANFIS 的功能来提升检测攻击的能力。仿真结果表明，所提方案能够以较高的准确率检测物联网中经常发生的 DDoS 攻击以及大部分已有方案尚未探索的恶意代码、侧信道、中间人攻击，但未与其他已有方案进行相关性能比较。

在最近的研究中，学者们将 ANFIS 应用于多种物联网具体应用场景中检测攻击。针对未经授权进入智能家居的危险水平评估问题，Sedova 等[34]提出了两个模糊方案，其中之一是以 ANFIS 算法为基础。该方案使用没有聚类的网格方法，训练了 128 个具有不同内部参数的神经模糊系统，用于评估未经授权的访问级别。但该方案仅在与单独使用模糊系统的方案的性能比较中表现更优，未与其他技术方案展开对比讨论。Pajila 等[35]应用 FIS 和 ANFIS 两种模糊技术，以有效地检测和处理无线传感网中的泛洪攻击。首先使用模糊方法进行基于移动性因子、剩余能量和信任因子等因素的聚类；然后由 ANFIS 模型对锚节点收集的集群数据进行评估，利用数据包传输速率和节点能耗等指标来识别数据包的恶意性。作者将方案与一些最新的安全解决方案进行对比，结果表明，该方案在检测率、能耗、检测延迟和吞吐量等指标中表现优异。Karthiga 等[36]引入了一种应用卷积神经网络和 ANFIS 来检测 VANET 中安全攻击的检测方法。其使用 ANFIS 分类器对已知攻击进行检测和分类，使用深度学习算法来检测未知攻击。该方案可实现对 DoS 攻击、僵尸网络攻击、端口扫描攻击和暴力破解攻击等外部攻击的检测。将实验结果与其他最先进的方法进行比较，结果表明该方法在准确率、精确率、灵敏性和计算复杂度等性能上均有优势。

在智能电网领域，Bedoya 等[37]同时考虑了电力系统的网络模型和物理模型，在 2019 年提出了一种基于 ANFIS 的算法来检测智能电网中的网络入侵，将网格的网络和物理组件集成到分层信息与通信技术模型中，监控网络物理电网的状态变量，并将其与预测的网络状态进行比较，当网络物理系统状态变量与 ANFIS 预测的网格状态不匹配时将检测到入侵。仿真实验表明了该方案具有较好的预测精确率，在电力系统网络入侵检测领域做出了原创性贡献，但需要对未来应用于电网或通信系统的升级进行调整。无独有偶，Abazari 等[38]于 2022 年开发了基于 ANFIS 的在线检测和缓解方案，以应对直流微电网等现代智能电网的虚假数据注入(False Data Injection，FDI)攻击。该方案采用基于密度的聚类方法提取直流微电网测量的规范特征，并将其聚类在正常和受攻击行为中训练 ANFIS 架构以在线识别 FDI 攻击，开发了一种自适应模型预测控制器，利用 ANFIS 获得的攻击向量更新功率、共享指令和缓解 FDI 攻击。在几种不同的情景下评估了该方法的性能，结果表明，与以往几种基于学习的方法相比，在时变攻击和巨大的不确定性下，所提出的检测策略能够更准确地识别攻击并估计其值。

如表 1 所列，模糊神经网络因其综合了模糊逻辑和神经网络的优势，将学习、联想、识别、信息处理汇集于一体，可以解决上述不同场景的攻击检测问题。但其也存在一定缺陷，特别是模型有许多参数需要调整时，该方案要考虑处理过拟合问题。在一些典型的模糊神经网络模型中，ANFIS 是近几年研究较为活跃的领域，虽然 ANFIS 的缺点之一是对初始模糊规则具有敏感性，同时由于增加了解决问题所需的模糊规则的数量，ANFIS 产生了较大的计算开销，但不可否认，它在处理非线性问题时能够提供更好的灵活性和适应性。

表 1 基于模糊神经网络的物联网流量攻击检测方案对比分析

Table 1 Comparative analysis of IoT traffic attack detection schemes based on fuzzy neural networks

模糊技术	文献	数据集	应用场景	攻击类型	局限性	评价指标
模糊神经网络	Perumalla 等[28]	KDD-Cup99	无人机物联网	海王星攻击 蓝精灵攻击	未考虑效率、吞吐量等指标	端到端延迟、精确率和召回率等
	Mittal 等[29]	自收集数据集	无线传感网	未针对特定攻击	未与其他方案比较	能量性能
	Shubha 等[30]	自收集数据集	车辆自组织网络	未针对特定攻击	—	检测率、假阳性率、检测时间
	Hu 等[31]	KDD-Cup99	智能家居	DoS、Probing、R2L 等以及新型攻击	—	检测率、误报率、算法性能
	Farhin 等[33]	NSL-KDD	物联网	恶意代码、侧信道、中间人和 DDoS 攻击	未与其他方案比较	F 度量、召回率、精确率和准确率
	Sedova 等[34]	自收集数据集	智能家居	未针对特定攻击	未与其他方案比较	学习的均方根误差值
	Pajila 等[35]	自收集数据集	无线传感网	泛洪攻击	仅能检测 1 种攻击	检测率、丢包率、延迟等
	Karthiga 等[36]	i-VANET 和 CIC-IDS 2017	车辆自组织网络	DoS 攻击、僵尸网络攻击、端口扫描攻击和暴力破解攻击	未与其他方案比较	准确率、精确率、灵敏性和特异性
	Bedoya[37]	自收集数据集	智能电网	中间人、DDos 攻击等	需要针对未来应用于电网或通信系统的升级进一步调整	准确率
	Abazari[38]	自收集数据集	直流微电网	虚假数据注入攻击	仅能检测 1 种攻击	准确率、稳定性

3.2 基于模糊聚类的方案

与非模糊聚类方法（硬聚类）不同，在模糊聚类（软聚类）中，每个数据点在某种程度上可以同时属于多个聚类。基于模糊聚类的方法中没有用于入侵检测的标记数据集，通过结合优化算法来调整参数以提高模糊聚类的准确性[39]。模糊 C-均值聚类算法（Fuzzy C-means，FCM）是应用最广泛且较成功的模糊聚类方法，它被应用于许多入侵检测方法中。

例如，Andrè 等[40]提出了一种名为 FROST 的物联网模糊入侵检测系统，用于识别物联网上不同类型的网络攻击。该系统基于模糊集理论，使用 FCM 使学习任务更能适应数据中可能出现的不准确性。同时，使用了一种机制来过滤和检测异常，允许识别和分析系统未知的新型攻击。他们还将所提方案与另一种方法进行了比较，结果表明，FROST 在不同类型的攻击分类中具有良好的性能，且所使用的模糊技术有助于减少错误和识别异常，但实验仅对比了一组方案，具有一定的局限性。Hafeez 等[41]提出了一个轻量级系统 IoT-Keeper，使用异常检测技术在边缘网关上执行流量分析以保护物联网的通信。他们使用 FCM 和模糊插值方案的组合来分析网络流量并检测恶意网络活动。一旦检测到恶意活动，IoT-Keeper 会自动对生成此活动的物联网设备实施网络访问限制，并防止其攻击其他设备或服务。将其与多种入侵检测的最新技术进行对比，所提技术在检测恶意网络活动方面实现了 98%的高精确率和 2%的低误报率，且资源占用量低，可以检测和缓解各种网络攻击，而无需明确的攻击特征或复杂的硬件。Khalafi 等[42]提出了一种基于静态估计和数据聚类算法的入侵检测系统，用于准确检测电力系统攻击的数量和位置，并确定网络中哪些相量测量单元（Phasor Measurement Unit，PMU）包含恶意数据。结果状态向量分两步进行聚类：首先，采用减法聚类来获取簇数，确定完整性攻击的数量；其次，FCM 将状态向量分配给相应的聚类，从而确定受攻击的 PMU。硬件在环实验结果表明，即使在多个攻击同时发生的情况下，该方法也能检测完整性攻击，确定攻击数量，获得正确的状态向量，并对攻击进行局部定位。

FCM 不仅被用于分类器后端设计，也在特征工程中发挥着重要作用。Fu 等[43]提出了一种基于多距离集成和特征聚类的特征选择方法，旨在解决物联网基于机器学习的入侵检测系统中高维和不平衡的数据增加了成本的问题。首先将 4 个不同的距离指标与 ReliefF 算法相结合，生成一个集成特征子集，然后利用 FCM 对该子集进行聚类，最终要素将从功能冗余较少的不同集群中选择。实验结果表明，在精确率和 F 度量方面，该算法的性能优于其他特征选择算法。

但是，在聚类过程中 FCM 算法会均衡各个聚类以使其样本数量大致相等，这导致 FCM 在应用于不平衡数据集时表现不佳。针对此问题，Kou 等[44]提出了一种具有密度感知特性的核模糊聚类算法，以解决数据集样本分布不平衡聚类的问题。为了提高距离聚类中心较远数据点分类的准确性，使用模糊支持向量机对距离样本中心距离远的数据点进行分类，仿真实验证明了所提方法能有效提高算法的检测准确率和效率。

此外，FCM 对初始质心敏感，需要提前手动确定聚类数量[45-46]，部分方案接受了 FCM 的缺陷，并将其与不同的入侵检测策略相结合。例如，Huang 等[47]以丰富的物联网数据为支撑，提出了一种基于密度峰值加权 FCM 的聚类方法来检测生产过程中的异常情况，密度峰值算法正好弥补了这一缺陷，与 FCM 相结合，提高了聚类模型的性能；同时引入基于互信息的相似性作为权重系数来指导聚类过程，从而提高了收敛速度和聚类质量。通过物联网加工车间的真实案例，验证了所提方法在制造过程异常检测中的准确性和有效性。Li 等[16]引入了用于物联网流量识别的全贝叶斯可能性 C-均值聚类算法（Full Bayesian Possibilistic C-means Clustering，FBPCM），使模糊聚类适应贝叶斯框架。他们认为，在 FBPCM 中选择最优聚类数量与在光谱分析中选择主成分的数量是同构的，因此将最优聚类数量的选择简化为最大后验估计。实验结果验证了该系统在精确率和稳定性方面相比其他算法的优势。

如表 2 所列，模糊聚类因能够更加灵活地识别异常，具有较好的可解释性和理解性，能够提高聚类的准确性和稳定性，被广泛应用于入侵检测中，其中最为典型的是 FCM。该方案灵活运用模糊聚类技术并整合检测系统以解决当下物联网攻击检测中的新型攻击检测、在线分析以及概念漂移等问题，在与其他方案的对比中，精确率、效率、检测率等性能均表现优异。但该算法也存在一定局限性，如需要提前手动确定聚类数量、不适应不平衡数据集等，需要结合其他算法共同作用。

表 2 基于模糊聚类的物联网流量攻击检测方案对比分析

Table 2 Comparative analysis of IoT traffic attack detection schemes based on fuzzy clustering

模糊技术	文献	数据集	应用场景	攻击类型	局限性	评价指标
模糊聚类	André 等[40]	UNSW-NB15	物联网	未针对特定攻击	未在其他数据集上测试	假阳性率、假阴性率、错误率
	Hafeez 等[41]	自收集数据集、YTY2018 和 MSI2017	物联网中的边缘网络	网络扫描、漏洞扫描、中间人、数据盗窃等攻击	在深度数据包检测、设备行为的演变、MAC 地址欺骗、拒绝服务等方面存在限制	真阳性率、假阳性率、F 度量、漏报率、准确率
	Khalafi 等[42]	自收集数据集	智能电网	隐形攻击	系统规模较小，不适用于更复杂的情况	欧几里得距离、范数差异、聚类数等
	Fu 等[43]	NSL-KDD	物联网	未针对特定攻击	未对特征聚类阶段选择最佳阈值	准确率和 F 度量
	Kou[44]	WSN-DS	物联网感知层	黑洞攻击、灰洞攻击、洪泛攻击等	不适用于逐渐发展的移动感知节点场景	检测率、真阳性率、真阴性率、误报率等
	Huang 等[47]	自收集数据集	物联网加工车间	未针对特定攻击	由于缺乏实时感知手段，未考虑加工过程中工件质量异常的问题	聚类精确率、CHI 和轮廓系数等聚类性能指标
	Li 等[16]	自收集数据集、KDD-Cup99、UNSW-NB15 和 CIC-IDS 2017	物联网	未针对特定攻击	需要对标记的流量数据集进行初始化，且超参数的自适应选择仍然是在线 IDS 面临的挑战	时间、精确率、召回率和 F 度量

3.3 基于模糊粗糙集的方案

特征选择方法通过删除要素中的冗余属性来生成最佳要素子集，可以减少计算负载。粗糙集可以处理网络数据中的不确定性和冗余信息问题，减少整个特征集的冗余，在保持特征分类有效的同时选择最优特征子集，在大数据挖掘中起到重要作用[48]。然而，传统的粗糙集理论仅面向离散数据。为了应对传统粗糙集理论的局限性，研究人员提出了将模糊理论应用于粗糙集。模糊粗糙集通过模糊相似关系描述两个对象之间的相似程度，因其用模糊关系优化等价关系，使得模糊粗糙集同时适用于离散属性和连续属性。

基于模糊粗糙集的特征选择方法在处理实值和噪声数据时具有许多优点。例如，Wu 等[49]在设计可防御物联网边缘网络的各种网络攻击检测方案时，为了实现实时和轻量级的入侵检测，首先提出了一种基于模糊粗糙集的特征提取算法，从原始数据流中提取低维特征，并保持特征的有效性，以减少计算负载；之后基于选定的特征结合卷积神经网络和生成对抗网络设计了一个入侵检测模型，将所提方法与现有评价方法进行了对比，该方法的精确率比现有方法提高了 4%。Liu 等[50]提出了一种基于深度模糊粗糙卷积神经网络的大规模多目标联邦神经进化框架，用于提高物联网的安全和隐私保护。在联邦学习中通过将模糊粗糙集理论引入深度卷积神经网络，以处理复杂的输入，然后通过神经进化优化了网络架构，但未展开实验对算法进行可行性验证。

粗糙集和模糊集理论虽然有各自的优缺点，但存在一定的相容性和相似性，在处理不确定性问题时具备互补性，将其结合能够对数据进行更有效的分析，生成更加可信、合理的规则集。因此，上述方案将两者应用到入侵检测的特征选择阶段，减少整个功能集和最佳功能子集的冗余。特征相关后，在保证特征有效性和分类有效性的前提下，得到最优特征集。但如表 3 所列，近几年在物联网入侵检测领域对于此技术的应用并不多，且在研究时均针对广义上的攻击，仍存在一定的扩展空间。

表 3 基于模糊粗糙集的物联网流量攻击检测方案对比分析

Table 3 Comparative analysis of IoT traffic attack detection schemes based on fuzzy rough sets

模糊技术	文献	数据集	应用场景	攻击类型	局限性	评价指标
模糊粗糙集	Wu 等[49]	CIC-DDoS2019 和 CSE-CIC-IDS2018	物联网中的边缘网络	未针对特定攻击	—	准确率、精确率、召回率、误报率和 F 度量
	Liu 等[50]	—	物联网	未针对特定攻击	未进行实验验证算法的有效性	—

3.4 基于模糊规则生成的方案

基于模糊规则的入侵检测方案可以更好地处理噪声和不精确的数据。此外，如果它们使用的模糊集是预定义的，并且反映了入侵检测专业知识，则它们是可解释的。相关文献中提供了几种基于模糊规则生成的入侵检测方法。

Pajila 等[17]提出了一种无线传感网中基于模糊规则的 DDoS 攻击检测和恢复机制(FBDR)。FBDR 方案分析每个传感器的能耗、响应时间和数据包计数，使用一型模糊规则来检测 DDoS 攻击的发生，快速识别受 DDoS 攻击影响的传感器节点；同时为避免数据包丢失，方案对每个节点的数据包大小、能耗和距离进行分析，基于二型模糊规则通过备用路径重定向到接收器。与相关方案相比，所提方法优化了检测率、丢包率、执行时间、计算复杂度等性能指标。Fang 等[51]提出了一种用于检测医疗物联网环境中非法行为的异常检测系统，该系统能够分析医疗物联网设备传输的数据包，自主学习设备运行规则，并提醒管理人员设备处于异常运行状态，以

确保控制服务的安全。为提高该系统异常分类的准确率，他们构建了一种基于粗糙集理论和模糊核心向量机的系统异常分类模型(Rough set-Fuzzy Core Vector Machine，R-FCVM)，并将其与支持向量机和孤立森林算法进行了比较，发现 R-FCVM 算法在处理任务时的准确性和时间成本均优于其他两种算法。

针对绝大多数现有的物联网入侵检测方法都只集中在准确性而忽视了可解释性的问题，Gorzałczany 等[52]从新近的 MQTT-IOT-IDS2020 数据集着手，提出了一种基于模糊规则分类器实现的知识发现数据挖掘/机器学习方法，并进行了对多目标进化优化算法的推广，以优化物联网入侵分类系统的准确性和可解释性之间的平衡，在与逻辑回归、k-最近邻、随机森林等 7 种可用替代方法的比较中，所提方案具有更高的准确率和更低的复杂性，因此具有非常高的可解释性。

由于数据流在绿色物联网环境中快速、动态、持续到达，数据流的概率分布会随时间变化，降低了训练模型对数据流问题的分类准确性。针对此类问题，Jiang 等[53]提出了一种在绿色物联网中动态增量集成模糊分类的算法。首先将基于模糊规则的分类器与动态加权算法相结合，以提高分类精确率。此外，通过增量学习数据流的特征来更新模型，可以有效处理数据流中数据分布变化引起的概念漂移。对无人机入侵检测、智能建筑和其他数据集进行实验评估，结果证明了所提算法的高性能，并展现了其在绿色物联网中处理不同类型问题的能力。

如表 4 所列，根据上述方案对模糊规则生成技术的使用，可以发现大多数方案是将模糊规则与其他分类器相结合，使得在处理模糊异常行为数据时具有更好的分类率和分类精确率，在与单独使用分类器的算法进行比较时表现出了更好的分类效果和更低的时间成本。但获得模糊规则及隶属函数凭经验进行，需要结合相关智能优化算法。

表 4 基于模糊规则的物联网流量攻击检测方案对比分析

Table 4 Comparative analysis of IoT traffic attack detection schemes based on fuzzy rules

模糊技术	文献	数据集	应用场景	攻击类型	局限性	评价指标
模糊规则	Pajila 等[17]	自收集数据集	无线传感网	DDoS 攻击	未与其他方案比较	网络生存周期、活动节点数、丢包率、能量消耗、响应时间、缓冲区使用情况、检出率、执行时间
	Fang 等[51]	自收集数据集	医疗物联网	重放攻击、肩窥攻击、恶意软件分析	—	准确率、误报率、平均时间成本、检测效率
	Gorzalczany 等[52]	MQTT-IOT-IDS2020	物联网	基于 MQTT 协议的物联网系统中不同类型的模拟网络攻击	未考虑特定攻击场景的数据集的组合	敏感性、精确率、F 度量
	Jiang 等[53]	自收集数据集	绿色物联网	未针对特定攻击	—	分类精确率、曲线下面积、几何平均值、F 度量、最长和平均训练时间

3.5 基于模糊推理系统的方案

模糊推理系统(Fuzzy Inference System，FIS)是使用模糊集合论将输入变量映射到输出空间的系统。在模糊化步骤中，输入值在隶属函数的帮助下转换为隶属度。“if-then”规则描述了输入和输出之间的关系。模糊推理应用模糊“if-then”规则从输入值计算模糊输出值。最后，在去模糊化阶段，使用适当的方法将从推理中获得的输出值映射到指定的值[54]。有两种常见的模糊推理方法：Mamdani 模型和 Tsukamoto Sugeno 模型。Mamdani 系统因具有更直观和更易于理解的规则基础而被更广泛地使用。

Hoang 等[55]提出了一种基于小 IOT23 数据集的模糊入侵检测系统，该系统被应用于采用边缘计算的物联网中。其运用粒子群优化算法对 FIS 参数进行优化，与现有方法相比，具有高精确率、低误报率和可扩展性。Awotunde 等[56]提出了一种基于模糊推理系统的入侵检测多级随机森林算法。首先结合过滤器和包装器方法的优势，以创建更先进的多级特征选择技术，从而增强网络安全；然后使用随机森林分类器提高检测精确率；最后使用 FIS 将入侵分类为正常、低、中或高，以降低错误分类的可能性。将所提方案与其他现有模型进行比较，结果表明其准确率、精密度、灵敏性、特异性和 F1 得分均有优势。同时，使用模糊推理系统对攻击进行分类也表明所提方法可以正确对攻击进行分类，减少错误分类。

在无线网络中，媒介信道的开放广播特性使得节点间的数据转发容易受到噪音或者干扰的影响。特别地，有意地进行干扰被称为干扰攻击(Jamming Attack)。为应对检测无线传感网的干扰攻击，Meenalochani 等[57]提出了一种基于模糊逻辑和蚁群优化的混合算法。将受干扰影响的因素作为 FIS 中的输入，并在此基础上对成功的数据路由使用蚁群优化，实验结果证明了所提出的混合优化技术优于蚁群优化技术。Savva 等[58]提出了一种基于模糊逻辑的分布式无线网状物联网中干扰攻击检测方案。该方案同时使用本地节点和接收器收集的信息作为 FIS 的输入，以干扰指数作为系统的输出，以期找到最佳输入集。但实验仅仅是为了寻找方案内部最优参数，没有与其他算法进行相关性能的对比讨论。

此外，物联网上最突出的路由协议之一是 RPL(低功耗和有损网络的 IPv6 路由协议)，可能会受到本地修复攻击等特定攻击。为应对这种攻击，Farzaneh 等[59]提出了一种基于模糊的 RPL 路由协议本地修复攻击检测方法，使用模糊推理方法将距离、剩余能量和预期传输计数 3 项指标作为模糊输入参数。在 Contiki OS 中使用 Cooja 模拟器获得的结果表明，所提方案具有极高的真阳性率和极低的误报率。

上述方案将模糊推理系统应用于入侵检测中，如表 5 所列，系统构建简单易懂，类似于人类的推理和决策。选取部分

参数作为模糊推理系统的输入，将入侵程度作为模糊推理系统的输出，能够有效解决相关问题。但该系统也有其局限性，当系统的参数受到外部干扰或者发生改变时，可能会出现不稳定的问题。

表 5 基于模糊推理系统的物联网流量攻击检测方案对比分析

Table 5 Comparative analysis of IoT traffic attack detection schemes based on fuzzy inference system

模糊技术	文献	数据集	应用场景	攻击类型	局限性	评价指标
模糊推理系统	Hoang 等[55]	小 IoT-23 数据集	物联网中的边缘网络	DDoS 攻击	未在其他数据集上进行测试	准确率、精确率、召回率、F 度量等
	Awotunde 等[56]	NSL-KDD	物联网	未针对特定攻击	未在其他数据集上进行测试	准确率、精确率、灵敏性、特异性和 F 度量
	Meenalochani 等[57]	自收集数据集	无线传感网	干扰攻击	仅和原始技术比较，未与其他混合优化技术比较	数据路由延迟、阻塞节点开销
	Savva 等[58]	自收集数据集	分布式无线网状物联网	干扰攻击	未与其他方案比较	准确率、精确率、特异性、假阳性率、召回率、假阴性率和分类器的接收器工作特性
	Farzaneh 等[59]	自收集数据集	物联网	本地修复攻击	仅能检测 1 种攻击	真阳性率、误报率

4 对比分析

1)模糊技术：如图 4 所示，大多数研究方案使用不同类型的模糊神经网络模型和 FCM 聚类算法来处理物联网异常流量和攻击检测。在模糊神经网络模型中，ANFIS 得到了更广泛的应用，但利用模糊神经网络模型的安全方案应该处理过拟合问题，特别是当模糊神经网络模型有许多参数需要调整时。FCM 之类的聚类方法处理速度非常快，并且开销非常低，因为它们不需要任何训练，因此非常适合低功耗环境以及缺乏标记数据的情况。但它仍存在很高的误报率，并且对初始数据很敏感。因此，大多数基于聚类的方法都尝试使用元启发式算法等方法来改进聚类方法，以获得更好的检测结果。

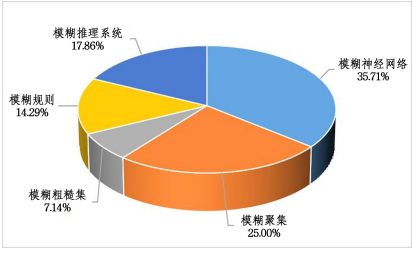


图 4 物联网流量攻击检测方案中模糊技术的应用百分比

Fig. 4 Percentage of applications of fuzzy technology in IoT traffic attack detection schemes

2)数据集：用于攻击检测的数据集至关重要，因为它们代表实际的攻击模式，并具有直接影响 IDS 性能的不同数据属性。如图 5 所示，很多方案仍在使用较过时的 KDD-Cup99 以及 NSL-KDD 数据集，很少有方案使用较新的 CIC-DDOS2019 和 MQTT-IOT-IDS2020 数据集。

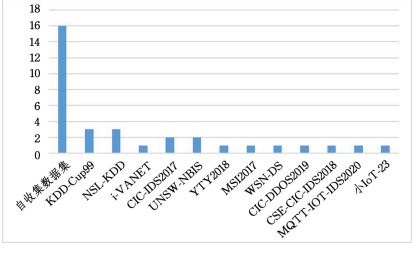


图 5 物联网流量攻击检测方案中数据集的应用数量

Fig. 5 Number of applications of data sets in IoT traffic attack detection scheme

需要说明的是，应该使用较新的数据集来评估现有的模糊攻击检测方法，以更好地验证它们在较新的攻击模式和特征方面的性能。同时，部分方案使用了专门的物联网数据集如 IoT-23 数据集等，以更好地评估算法。此外，考虑到物联网入侵检测数据集的不足，大量方案在真实系统和网络中自收集数据集，以对所提出的攻击检测方案进行评估，这样有助于真正确定所设计方案的优点和局限性。

3)应用场景：相关研究工作不仅局限于广义的物联网，更多研究人员将视角定位在物联网具体的应用场景上，如智能家居、智能电网、车辆自组织网络、无人机物联网、医疗物联网、无线传感网等(见图 6)，这有助于结合具体场景特点，进行有针对性的检测方案设计，进一步提高方案的适配度。

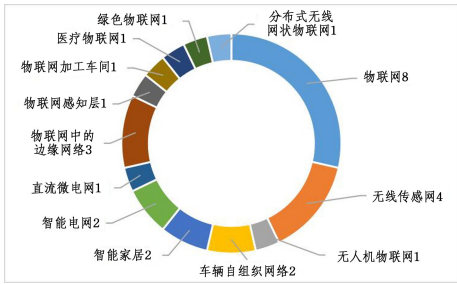


图 6 物联网流量攻击检测方案中应用场景的数量

Fig. 6 Number of application scenarios in IoT traffic attack detection scheme

4)攻击类型：大多数方案针对特定攻击进行检测方案设计，如图 7 所示，少量方案致力于处理异常检测问题，未指出特定攻击。

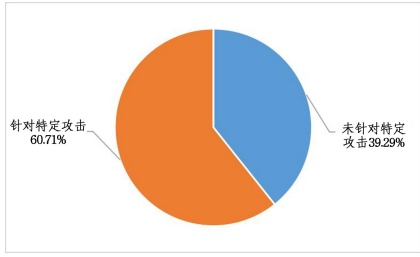


图 7 物联网流量攻击检测方案中是否针对特定攻击的比例

Fig. 7 Proportion of IoT traffic attack detection schemes targeting specific attacks

5)评估测试：现有方案在评估和分析攻击检测方案时，主

要利用F度量、召回率、准确率和精确率等指标。尽管这些指标表明了方案在识别攻击和入侵方面的表现,但也应考虑针对新方案可能产生的开销并进行改进。此外,很多方案都应用MATLAB软件进行测试和评估,这表明需要专用的软件模拟器,来支持各种机器学习与数据挖掘技术和算法的攻击检测。

5 研究展望

结合对现有模糊逻辑的物联网流量攻击检测技术的深入分析,未来研究可以考虑以下方向:

1)过于准确的模型可能不适合处理大量的网络流量,并且在决策时处理速度可能非常慢,低运行时,其系统的复杂性又是实时异常检测方法面临的挑战。因此,未来应探索和开发新的低成本方法,设计一个有效的系统来检测大多数入侵者攻击并使其适用于实时目的。

2)模糊攻击检测方案的性能会因入侵检测数据集中数据的庞大数量和高维性而降低。在这种情况下,可以在各种数据集中识别重要特征并确定其优先级,以用于入侵检测过程。因此,应进一步研究特征选择/提取方法,在尽可能低的开销下找到最佳特征。

3)上述方案大多都是在旧数据集或不标准的自收集数据集上进行评估。因此,在随后的安全研究中,应该针对标准和最新数据集进行完整的实验。此外,应使用真实的网络跟踪来验证实现的结果。考虑到新出现的安全攻击,应创建新的数据集,或者更新现有数据集,以进一步评估攻击检测环境中的新方案。

4)在文献中提出的众多新型元启发式算法中,只有少数被应用于调整FIS的参数或定位模糊规则。因此,未来一代模糊入侵检测框架应利用更新的元启发式算法,尤其是多目标算法。

5)聚类是一种无监督学习方法,已成功集成到入侵检测方法的各个步骤中。但是,大多数应用的聚类算法需要提前确定聚类的数量。因此,在未来的研究中,应进一步研究自动聚类和动态确定聚类数量的算法。

6)应进一步研究针对特定环境的攻击检测方法,以应对信息技术领域的快速发展。为此,还需要设计特定环境的数据集来评估这些新方法。

7)关于架构风格,本文所研究的模糊攻击检测方案大多是中心化的,很少有研究分布式架构。因此,关于分布式物联网,应在后续研究中重点关注其模糊攻击检测方案,以处理更广泛的网络异常。

结束语 随着物联网设备使用的逐渐普及,寻求从这些设备窃取重要信息的入侵者数量也在同步增加。物联网环境中所用协议和数据的异构性使得在物联网系统中利用安全机制的要求更高。由于节点数量多、内存和处理能力低以及能量受限,应用物联网安全技术面临挑战。IDS是一种安全框架,旨在保护网络上的信息系统。研究表明,模糊逻辑可以有效地融入各种物联网攻击检测方案中,作为一种高度可靠的解决方案,其目的是在保持网络性能的同时提高入侵检测的准确性。

本文旨在对基于模糊逻辑的流量攻击检测技术进行深入调查和分类,以提高物联网系统的安全性。为此,我们首先提供了有关物联网安全、IDS和模糊逻辑的基本概念。然后,根据模糊算法对应用于物联网领域的攻击检测方案进行分类,总结其主要特点和贡献,重点介绍模糊技术在入侵处理过程中的应用。此外,针对各类别的模糊攻击检测方法,比较了所使用的数据集、应用场景、攻击类型、局限性和性能评估因子。最后,对所研究的攻击检测解决方案的各种特性进行了比较,为今后的研究指明了方向。

参 考 文 献

[1] BANSAL S,TOMAR V K. Challenges & Security Threats in IoT with Solution Architectures[C]// 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control(PARC). Mathura:IEEE,2022:1-5.

[2] HUAN W M,LIN H T. Design of Intrusion detection System based on sampling integration Algorithm [J]. Computer Science,2021,48(S2):705-712.

[3] BUCZAK A L,GUVEN E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection [J]. IEEE Communications Surveys & Tutorials,2016,18(2):1153-1176.

[4] GU J,LU S. An effective intrusion detection approach using SVM with naïve Bayes feature embedding[J]. Computers & Security,2021,103:102158.

[5] GUEZZAZ A,ASIMI A,ASIMI Y,et al. A Lightweight Neural Classifier for Intrusion Detection[J]. General Letters in Mathematics,2017,2(2):57-66.

[6] JIANG Z T,ZHOU TAN S Z,HAN L Y. Nearest neighbor Intrusion detection algorithm based on perceptual hash matrix [J]. Acta Electronica Sinica,2019,47(7):1538-1546.

[7] ZHOU J H,PENG F,QIU R F,et al. Intrusion detection based on Fusion random forest and gradient Lift Tree [J]. Journal of Software,2021,32(10):3254-3265.

[8] ZHANG L,CUI Y,LIU J,et al. Application of Machine Learning in Cyberspace security research [J]. Journal of Computers,2018,41(9):1943-1975.

[9] MODI C,PATEL D,BORISANIYA B,et al. A survey of intrusion detection techniques in Cloud[J]. Journal of Network and Computer Applications,2013,36(1):42-57.

[10] WU S X,BANZHAF W. The use of computational intelligence in intrusion detection systems:A review[J]. Applied Soft Computing,2010,10(1):1-35.

[11] YANG P F,CAI R J,GUO S C,et al. A container-based Intrusion detection method for Cisco IOS-XE system [J]. Journal of Computer Science,2012,50(4):298-307.

[12] SHANMUGAVADIVU R,NAGARAJAN N. Network intrusion detection system using fuzzy logic[J]. Indian Journal of Computer Science and Engineering(IJCSE),2011,2(1):101-111.

[13] ZADEH L A. Fuzzy sets[J]. Information and Control,1965,8(3):338-353.

[14] SHERAZI H H R,IQBAL R,AHMAD F,et al. DDoS attack

detection: A key enabler for sustainable communication in Internet of vehicles[J]. Sustainable Computing: Informatics and Systems, 2019, 23: 13-20.

[15] DICKERSON J E, DICKERSON J A. Fuzzy network profiling for intrusion detection[C]// 19th International Conference of the North American Fuzzy Information Processing Society-NAFIPS(Cat. No. 00TH8500). Atlanta: IEEE, 2000: 301-306.

[16] LI F, ZHAO R, WANG S, et al. Online Intrusion Detection for Internet of Things Systems With Full Bayesian Possibilistic Clustering and Ensembled Fuzzy Classifiers[J]. IEEE Transactions on Fuzzy Systems, 2022, 30(11): 4605-4617.

[17] PAJILA P J B, JULIE E G, ROBINSON Y H. FBDR-Fuzzy Based DDoS Attack Detection and Recovery Mechanism for Wireless Sensor Networks[J]. Wireless Personal Communications, 2022, 122(4): 3053-3083.

[18] SHAH Y, SENGUPTA S. A survey on Classification of Cyber-attacks on IoT and IIoT devices[C]// 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference(UEMCON). New York: IEEE, 2020: 406-413.

[19] SETHI P, SARANGI S R. Internet of Things: Architectures, Protocols, and Applications[J]. Journal of Electrical and Computer Engineering, 2017, 2017: 1-25.

[20] OMOLARA A E, ALABDULATIF A, ABIODUN O I, et al. The internet of things security: A survey encompassing unexplored areas and new insights[J]. Computers & Security, 2022, 112: 102494.

[21] ALHIRABI N, RANA O, PERERA C. Security and Privacy Requirements for the Internet of Things[J]. ACM Transactions on Internet of Things, 2021, 2(1): 1-37.

[22] LIU Q X, JIN Z, CHEN C H, et al. Internet of Things access control security review [J]. Computer Research and Development, 2022, 59(10): 2190-2211.

[23] MOHAMAD M B, HASSAN W H. Current research on Internet of Things(IoT) security: A survey[J]. Computer Networks, 2019, 148: 283-294.

[24] AZROUR M, MABROUKI J, FARHAOUI Y, et al. Security Analysis of Nikooghadam et al.'s Authentication Protocol for Cloud-IoT[M]. Intelligent Systems in Big Data, Semantic Web and Machine Learning. Cham: Springer International Publishing, 2021: 261-269.

[25] MOUDNI H, ER-ROUIDI M, MOUNCIF H, et al. Fuzzy logic based intrusion detection system against black hole attack in mobile ad hoc networks[J]. International Journal of Communication Networks and Information Security, 2018, 10(2): 366-373.

[26] SCARFONE K, MELL P. Guide to intrusion detection and prevention systems (idps)[J]. NIST Special Bublication, 2007, 800(2007): 94.

[27] DEBAR H, DACIER M, WESPI A. Towards a taxonomy of intrusion-detection systems[J]. Computer Networks(Amsterdam, Netherlands: 1999), 1999, 31(8): 805-822.

[28] PERUMALLA S, CHATTERJEE S, KUMAR A P S. Block Chain-based access control and intrusion detection system in IoD [C]// 2021 6th International Conference on Communication and Electronics Systems(ICCES). Coimbatre: IEEE, 2021: 511-518.

[29] MITTAL M, SARASWAT L K, IWENDI C, et al. A Neuro-Fuzzy Approach for Intrusion Detection in Energy Efficient Sensor Routing[C]// 2019 4th International Conference on Internet of Things: Smart Innovation and Usages(IoT-SIU). Ghaziabad: IEEE, 2019: 1-5.

[30] SHUBHA R S, MANJAIAH D H. Multi-Layer Perceptron Based Fuzzy Logic Technique for Detection of Attacks in VANETS[C]// 2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI). Gwalior: IEEE, 2022.

[31] HU X, ZHANG Q, YANG X, et al. An Intrusion Detection Method Fused Deep Learning and Fuzzy Neural Network for Smart Home[C]// ICIC 2022: Intelligent Computing Theories and Application. Cham: Springer International Publishing, 2022: 627-637.

[32] JANG J S R. ANFIS: adaptive-network-based fuzzy inference system[J]. IEEE Transactions on Systems, Man, and Cybernetics, 1993, 23(3): 665-685.

[33] FARHIN F, SULTANA I, ISLAM N, et al. Attack Detection in Internet of Things using Software Defined Network and Fuzzy Neural Network[C]// 2020 Joint 9th International Conference on Informatics, Electronics & Vision(ICIEV) and 2020 4th International Conference on Imaging, Vision & Pattern Recognition(icIVPR). Kitakyushu: IEEE, 2020.

[34] SEDOVA N A, ARKHIPOVA Z V, LAVROV E A, et al. Smart System for Detecting Unauthorized Entry into a Smart Home [C]// 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). Yaroslavl: IEEE, 2020: 63-67.

[35] BESLIN PAJILA P J, GOLDEN JULIE E, HAROLD ROBINSON Y. ABAP: Anchor Node Based DDoS Attack Detection Using Adaptive Neuro-Fuzzy Inference System[J]. Wireless Personal Communications, 2023, 128(2): 875-899.

[36] KARTHIGA B, DURAIRAJ D, NAWAZ N, et al. Intelligent Intrusion Detection System for VANET Using Machine Learning and Deep Learning Approaches[J]. Wireless Communications and Mobile Computing, 2022, 2022: 1-13.

[37] BEDOYA J C, LIU C, XIE J. Adaptive Neuro Fuzzy Inference System for Cyber-Intrusion Detection in a Smart Grid[C]// 2019 20th International Conference on Intelligent System Application to Power Systems(ISAP). New Delhi: IEEE, 2019.

[38] ABAZARI A, ZADSAR M, GHAFOURI M, et al. A Data Mining/ANFIS and Adaptive Control for Detection and Mitigation of Attacks on DC MGs[J]. IEEE Transactions on Smart Grid, 2023, 14(3): 2406-2422.

[39] JAVAHERI D, GORGIN S, LEE J, et al. An improved discrete harris hawk optimization algorithm for efficient workflow scheduling in multi-fog computing[J]. Sustainable Computing: Informatics and Systems, 2022, 36: 100787.

[40] ANDRÉ L C, DOUGLAS D L, RODOLFO I M, et al. A Fuzzy Intrusion Detection System for Identifying Cyber-Attacks on IoT Networks[C]// 2020 IEEE Latin-American Conference on Communications(LATINCOM). Santo Domingo: IEEE, 2020.

[41] HAFEEZ I, ANTIKAINEN M, DING A Y, et al. IoT-KEEPER: Detecting Malicious IoT Network Activity Using Online Traffic Analysis at the Edge[J]. IEEE Transactions on Network and Service Management, 2020, 17(1): 45-59.

[42] KHALAFI Z S, DEHGHANI M, KHALILI A, et al. Intrusion Detection, Measurement Correction, and Attack Localization of PMU Networks[J]. IEEE Transactions on Industrial Electronics, 2022, 69(5): 4697-4706.

[43] FU G H, LI B C, WEI Q J, et al. A Multi-Distance Ensemble and Feature Clustering Based Feature Selection Approach for Network Intrusion Detection[C]// 2022 International Symposium on Sensing and Instrumentation in 5G and IoT Era (ISSI). Shanghai: IEEE, 2022: 160-164.

[44] KOU L. Research on security defense Technology of IoT Sensing Layer [D]. Harbin: Harbin Engineering University, 2019.

[45] ZENG S, TONG X, SANG N. Study on multi-center fuzzy C-means algorithm based on transitive closure and spectral clustering[J]. Applied Soft Computing, 2014, 16: 89-101.

[46] SHAN D H, SHI Y C, ZHAO W Z, et al. Segmentation fusion fuzzy clustering algorithm for Cloud data security storage [J]. Computer Science, 2017, 44(5): 166-169.

[47] HUANG S, GUO Y, YANG N, et al. A weighted fuzzy C-means clustering method with density peak for anomaly detection in IoT-enabled manufacturing process [J]. Journal of Intelligent Manufacturing, 2021, 32(7): 1845-1861.

[48] WANG Z Y, LI L J, MI Z S, et al. Variable precision fuzzy Rough Set attribute reduction based on error cost [J]. Computer Science, 2022, 49(4): 161-167.

[49] WU Y, NIE L, WANG S, et al. Intelligent Intrusion Detection for Internet of Things Security: A Deep Convolutional Generative Adversarial Network-Enabled Approach[J]. IEEE Internet of Things Journal, 2023, 10(4): 3094-3106.

[50] LIU X, ZHAO J, LI J, et al. Large-Scale Multiobjective Federated Neuroevolution for Privacy and Security in the Internet of Things[J]. IEEE Internet of Things Magazine, 2022, 5(2): 74-77.

[51] FANG L, LI Y, LIU Z, et al. A Practical Model Based on Anomaly Detection for Protecting Medical IoT Control Services Against External Attacks[J]. IEEE Transactions on Industrial Informatics, 2021, 17(6): 4260-4269.

[52] GORZALCZANY M B, RUDZINSKI F. Intrusion Detection in Internet of Things With MQTT Protocol—An Accurate and Interpretable Genetic-Fuzzy Rule-Based Solution[J]. IEEE Internet of Things Journal, 2022, 9(24): 24843-24855.

[53] JIANG J, LIU F, NG W W Y, et al. Dynamic Incremental Ensemble Fuzzy Classifier for Data Streams in Green Internet of Things[J]. IEEE Transactions on Green Communications and Networking, 2022, 6(3): 1316-1329.

[54] LI F Y, LI Y, YANG J. Review of interpolation inference algorithms based on fuzzy rules [J]. Journal of Computers, 2022, 45(8): 1687-1711.

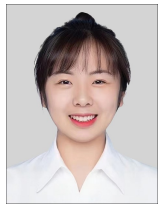
[55] HOANG T M, TRAN N H, THAI V L, et al. An efficient IDS using FIS to detect DDoS in IoT networks[C]// 2022 9th NAFOSTED Conference on Information and Computer Science (NICS). Ho Chi Minh City: IEEE, 2022: 193-198.

[56] AWOTUNDE J B, AYO F E, PANIGRAHI R, et al. A Multilevel Random Forest Model-Based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks[J]. International Journal of Computational Intelligence Systems, 2023, 16(1): 31.

[57] MEENALOCHANI M, SUDHA S. Jammed Node Detection and Routing in a Multihop Wireless Sensor Network Using Hybrid Techniques [J]. Wireless Personal Communications, 2019, 104(2): 663-675.

[58] SAVVA M, IOANNOU I, VASSILIOU V. Fuzzy-Logic Based IDS for Detecting Jamming Attacks in Wireless Mesh IoT Networks[C]// 2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet). Pafos: IEEE, 2022: 54-63.

[59] FARZANEH B, KOOSHA M, BOOCHANPOUR E, et al. A New Method for Intrusion Detection on RPL Routing Protocol Using Fuzzy Logic[C]// 2020 6th International Conference on Web Research (ICWR). Tehran: IEEE, 2020: 245-250.



SHANG Yuling, born in 1999, postgraguate. Her main research interests include cyberspace security and Internet of things technology.

LI Peng, born in 1979, Ph.D, professor, Ph.D supervisor, is a member of CCF (No. 48573M). His main research interests include computer communication networks, cloud computing and information security.

(责任编辑:何杨)