This is an author pre-published version of the paper which has been accepted in journal Information Sciences

Fuzzy Logic-Based DDoS Attacks and Network Traffic Anomaly Detection Methods: Classification, Overview, and Future Perspectives

Danial Javaheri[1], Saeid Gorgin[1], Jeong-A Lee[1], Mohammad Masdari[2*]
javaheri@chosun.ac.kr; gorgin@chosun.ac.kr; jalee@chosun.ac.kr; m.masdari@iaurmia.ac.ir

[1] Department of Computer Engineering, Chosun University, Gwangju 61452, Republic of Korea
[2] Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran

*Corresponding author: Mohammad Masdari (m.masdari@iaurmia.ac.ir); Jeong-A Lee (jalee@chosun.ac.kr)

Abstract: Nowadays, cybersecurity challenges and their ever-growing complexity are the main concerns for various information technology-driven organizations and companies. Although several intrusion detection systems have been introduced in an attempt to deal with zero-day cybersecurity attacks, computer systems are still highly vulnerable to various types of distributed denial of service (DDoS) attacks. This complicated cyber-attack caused many system failures and service disruptions, resulting in billions of dollars of financial loss and irrecoverable reputation damage in recent years. Considering the nonnegligible importance of business continuity in the Industry 4.0 era, this paper presents a comprehensive, systematic survey of DDoS attacks. It also proposes a hierarchy for this severe cyber threat, besides conducting deep comparisons from various perspectives between the studies published by reputed venues in this area. Furthermore, this paper recommends the most effective defensive strategies, with a focus on recently offered fuzzy-based detection methods, to mitigate such threats and bridge the gaps existing in the current intrusion detection systems and related works. The outcomes and key findings of this survey paper are highly advantageous for private companies, enterprises, and government agencies to be implemented in their local or global businesses to significantly improve business sustainability.

Keywords: Anomaly Detection, Fuzzy Logic, Cyber-attacks, Denial of Service, Network Security, Business Sustainability.

1. Introduction

Over recent years, cyber threats and malicious attacks have increased drastically against numerous domains, ranging from IT companies to finance, energy, and health sectors [1]. Computer networks and systems are susceptible to a variety of reported and undiscovered anomalies, including DDoS attacks. Despite the fact that security solutions like encryption algorithms, authentication procedures, firewalls, and honeypots can reduce security threats to a certain extent, computer networks continue to be plagued by numerous harmful activities [2]. Intrusion detection systems (IDS) are intriguing instruments aiming to locate and identify cyber-attacks. Multiple strategies have been investigated by the research community to improve the accuracy and performance of intrusion detection systems. Depending on their characteristics, intrusion detection systems can be classified as signature-based, anomaly-based, and hybrid approaches. The signature-based detection methods are able to scan unique sequences among network traffic related to a certain attack and precisely identify that attack [3]. Nonetheless, as a disadvantage, they cannot recognize zero-day attacks and attacks with different signatures since they have not learned their behavioral or structural patterns. As a result, signature-based detection schemes need an accurate and up-to-date database containing all known attacks, making maintenance very complicated and cumbersome. The other type of intrusion detection system is based on anomaly detection, which relies on the profile of typical actions and detects any deviation as a potential intrusion. However, the threshold between normal and abnormal activities may not be well-defined in establishing the essential profiles for normal behaviors. As a result, even a little change in the monitored traffic may be misidentified as an attack, increasing the rate of false-positive alarms. Hybrid approaches can benefit from the privileges of both categories of intrusion detection systems; however, they are difficult to be implemented and synchronize.

Consequently, the imprecise and uncertain nature of today's security attacks makes it much harder to detect and recognize them correctly. To deal with the before-mentioned challenges, fuzzy anomaly detection frameworks have recently been introduced to incorporate different fuzzy techniques in various operations steps in order to detect cyber-attacks more accurately when the data is inaccurate and uncertain. The methodologies for anomaly detection can be categorized as host-based or network-based schemes. This article focuses on the fuzzy approaches from the latter category. In the following, Fig. 1 illustrates different types of intrusion detection systems where the classes studied in this survey paper were highlighted.

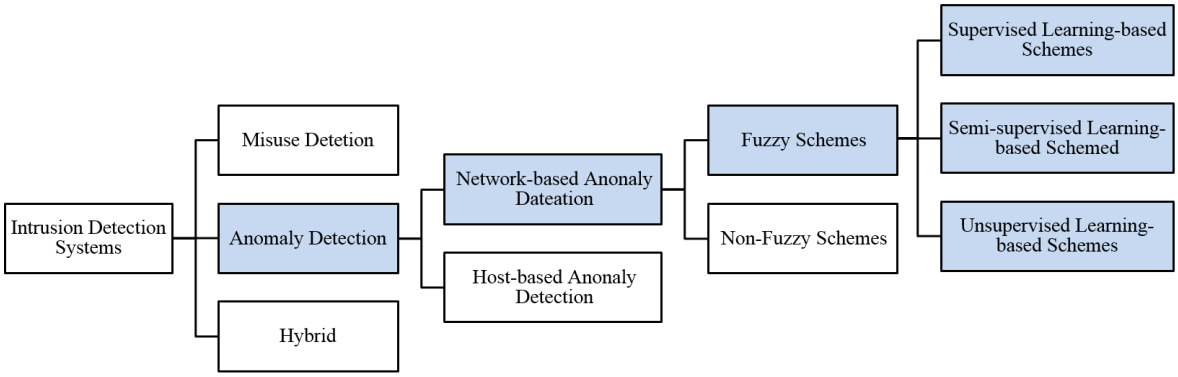


Fig. 1: Intrusion detection system categories and the classes studied in this paper.

As shown in Fig. 1, fuzzy schemes for network-based anomaly detection are classified into supervised, unsupervised, and semi-supervised learning. According to the results of running queries on the academic libraries, several fuzzy logic-based solutions have been presented in the literature, aiming to deal with DDoS attacks and other anomalies in computer networks. However, there is a significant lack of comprehensive surveys to study and discuss these schemes, as well as demonstrate their advantages, disadvantages, and shortcomings. To bridge this gap, we present a comprehensive study on the fuzzy DDoS anomaly detection approaches introduced in recent years by reputable venues. At first, the details and properties of our systematic survey are presented, and then, we cover the background concepts and knowledge in the anomaly detection domain to identify DDoS attacks. This study explores different types of DDoS attacks and various properties of anomaly-based IDS schemes. Afterward, we classify the investigated schemes based on the applied fuzzy algorithms and methods. The main contribution, details, and properties, such as applied datasets, evaluation metrics, fuzzy membership functions, and, most importantly, their limitations, are indicated. Besides, a comparative comparison between these schemes from various perspectives is presented. This comparison includes the name and rates of fuzzy algorithms, evaluation metrics, datasets used in the literature, etc. Eventually, the main challenges and future research directions in the contexts of fuzzy DDoS and anomaly detection are highlighted.

2. Research method

This section demonstrates the systematic research method applied to conduct this survey, including the steps and library addresses. A systematic process containing four steps was used to search and find the fuzzy-based intrusion detection methods proposed in the literature. Fig. 2 shows the steps of this systematic review. In addition, the list and addresses of scientific libraries used in this survey to run queries are reported in Table 1.

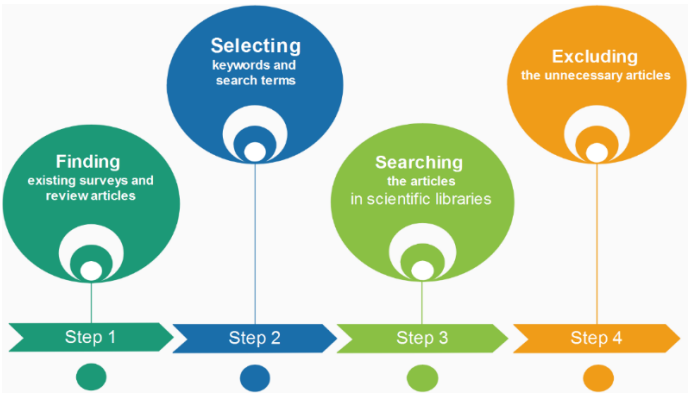


Fig. 2: The systematic review and steps taken in this survey.

Table 1: The name and address of libraries used in this survey.

#	LibrarName	Library Address
1	IEEE explorer	ieeexplore.ieee.org
2	ScienceDirect	www.sciencedirect.com
3	Wiley	www.wiley.com/en-us
4	Springer	www.springer.com
5	Hindawi	www.hindawi.com
6	Inderscience	www.inderscience.com
7	Google Scholar	scholar.google.com
8	OXFORD academic	academic.oup.com
9	Emerald	www.emeraldinsight.com

10	Sage	journals.sagepub.com
11	ACM	www.acm.org
12	MDPI	www.mdpi.com
13	PLOS	journals.plos.org

To search and retrieve published review papers related to the topic of this survey, the following search terms have been applied.

- Survey Network Intrusion Detection
- Review Network Intrusion Detection
- Study Network Intrusion Detection
- Overview Network Intrusion Detection
- Survey Network Anomaly Intrusion Detection
- Review Network Anomaly Intrusion Detection
- Study Anomaly Intrusion Detection
- Overview Anomaly Intrusion Detection

Several related works were found using the above-mentioned research queries. Table 2 indicates and categorizes these related woks, in addition to the limitations for each related work.

Table 2: The current related surveys.

Item	Ref.	Main Topic	Limitations
1	[3]	Misuse detection	This survey only discusses the fuzzy misuse detection schemes
2	[4]	Intrusion detection	This survey only studies the schemes provided for wireless ad hoc networks
3	[5]		This survey only studies the intrusion detection methods in SDN
4	[6]		This survey only studies the intrusion detection approaches in data-driven SDN
5	[7]		This survey only studies the network-based intrusion detection approaches
6	[8]	Anomaly detection	This survey only studies the anomaly detection approaches in SDNs
7	[9]		This survey only studies the deep learning-based anomaly detection schemes
8	[10]		This survey has only studied DDoS detection method regarding IoT devices

As shown in Table 2, some related works focused on the topics like deep learning, machine learning, ensemble learning, etc. In contrast, others addressed specific environments like mobile ad hoc networks, sensor networks, cloud computing, and software-defined network (SDN). SDN is a new approach to networking that, unlike conventional networks, applies software-based controllers to manage the data traffic on the network hardware equipment. SDN has emerged as a revolutionary technology in computer networks, and its architecture consists of three layers, including the infrastructure layer, control layer, and application layer. Generally, SDN attempts to decouple the data routing capabilities of computer networks from network control. Using this method, the underlying network infrastructure will be abstracted from the upper layers, enabling the computer network's control to be programmable. In recent years, SDN has been introduced to be one of the effective solutions in the detection of networks-based attacks [6]. Some surveys have also focused on network intrusion detections, and some others have addressed host-based intrusion detections. However, none of them has covered the detection of DDoS attacks and various anomalies using fuzzy logic-based techniques. Hence, our survey is the first attempt to provide a comprehensive study, discussion, and comparison of papers focused on employing fuzzy logic to detect anomalies of DDoS attacks. The following search terms and strings were used to find literature reviews on fuzzy logic-based network anomaly detection:

- Survey Fuzzy Anomaly Detection
- Overview Fuzzy Anomaly Detection
- Review Fuzzy Anomaly Detection
- Study Comparative Fuzzy Anomaly Detection
- Survey Fuzzy DDoS Detection
- Overview Fuzzy DDoS Detection
- Review Fuzzy DDoS Detection
- Comparative Study Fuzzy DDoS Detection

As mentioned, no survey article has been found related to fuzzy logic and network anomaly detection context using the above-mentioned terms up to this date. To search and find the new fuzzy techniques used for anomaly detection approaches, we used the following search strings:

- C-Means Anomaly Detection Fuzzy
- Clustering Anomaly Detection Fuzzy

- K-Medoids Anomaly Detection Fuzzy
- K-Means Anomaly Detection Fuzzy
- ANFIS Anomaly Detection Fuzzy
- Fuzzy Adaptive Network FIS Anomaly Detection
- KNN Anomaly Detection Fuzzy
- Neural Network Anomaly Detection Fuzzy
- Rule Interpolation Anomaly Detection Fuzzy
- Inference System Anomaly Detection Fuzzy
- Rule Generation Anomaly Detection Fuzzy
- PCA Anomaly Detection Fuzzy
- Principal Component Analysis Fuzzy
- Intuitionistic Fuzzy Set Anomaly Detection
- Bayesian Anomaly Detection Fuzzy
- Rough Set Anomaly Detection Fuzzy
- SVM Anomaly Detection Fuzzy
- DDoS attacks Anomaly Detection Fuzzy
- Distributed Denial-of-Service attacks Fuzzy
- Security Attacks Anomaly Detection Fuzzy

Moreover, to include the fuzzy techniques used for detecting DDoS attacks, the following search queries were used on each scientific library:

- C-Means DDOS Detection Fuzzy
- Clustering DDOS Detection Fuzzy
- K-Medoids DDOS Detection Fuzzy
- K-Means DDOS Detection Fuzzy
- ANFIS DDOS Detection Fuzzy
- Fuzzy Adaptive Network FIS DDOS Detection
- KNN DDOS Detection Fuzzy
- Neural Network DDOS Detection Fuzzy
- Rule Interpolation DDOS Detection Fuzzy
- Inference System DDOS Detection Fuzzy
- Rule Generation DDOS Detection Fuzzy
- PCA DDOS Detection Fuzzy
- Principal Component Analysis Fuzzy
- Intuitionistic Fuzzy Set DDOS Detection
- Bayesian DDOS Detection Fuzzy
- Rough Set DDOS Detection Fuzzy
- SVM DDOS Detection Fuzzy
- DDoS Attacks DDOS Detection Fuzzy
- Distributed Denial-of-Service Attacks Fuzzy
- Security Attacks DDOS Detection Fuzzy

Running these search terms resulted in retrieving many articles. To focus on the most recent and important studies, the query output has been refined to include papers published in recent four years. Also, we have merely investigated the papers primarily dedicated to the security and intrusion detection contexts and dealt with challenges in these domains. In this process, the articles that focused on anomaly detection in a context rather than security were removed and excluded from further processing. In addition, articles that lacked the proper contributions or did not conduct the required evaluation and verification steps were excluded. Fig. 3 illustrates the proportion of each scientific library publishing paper on DDoS detection approaches and fuzzy network anomaly detection architectures.

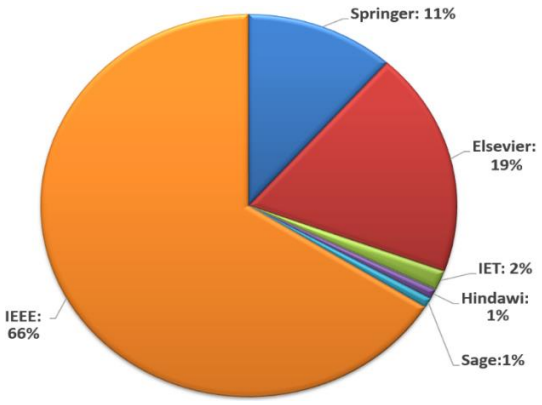


Fig. 3: The portion of the scientific libraries in published papers related to this survey's topic.

As shown in Fig. 3, the majority of articles were obtained from conferences or journals in the IEEE library, followed by the Elsevier library. Besides, the number of fuzzy anomalies and DDoS detection schemes published in various scientific libraries since 2016 is shown in Fig. 4; however, as mentioned, papers published in recent four years have been investigated in this survey, aiming to focus on the most recent works and introduce novel methodologies.

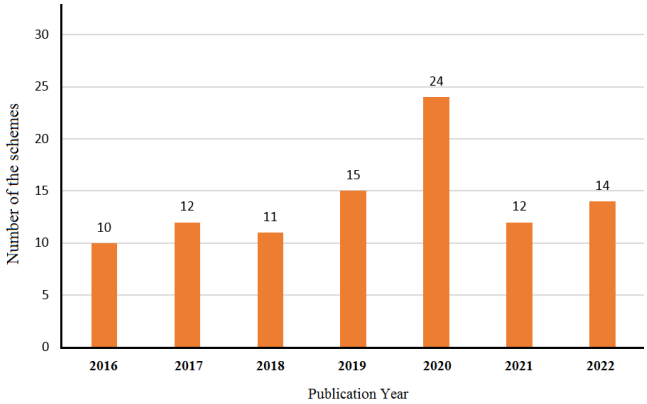


Fig. 4: The number of papers related to fuzzy anomalies and DDoS detection frameworks.

Considering the number of recently published papers, it can be concluded that employing fuzzy techniques to detect network traffic anomalies is an active and ongoing research topic. Therefore, the main research questions that are covered and addressed by this survey are listed as follows:

RQ1- Which fuzzy-based algorithms and data mining techniques have been employed to detect anomalies in network traffic?

RQ2- Which security services and capabilities are provided by each studied scheme?

RQ3- What are the advantages, disadvantages, and limitations of the studied fuzzy anomaly detection schemes?

RQ4- Which evaluation metrics and datasets have been used to evaluate the investigated fuzzy approaches?

RQ5- What are the possible subsequent issues that should be addressed in the future in the fuzzy anomaly detection and DDoS detection domains?

3. Background concepts

This section explains the fundamental concepts in cybersecurity related to DDoS attacks, data anomalies, and intrusion detection to help readers better comprehend the approaches for anomaly-based intrusion detection under investigation.

3.1. Distributed Denial of Service attacks

The most common type of DDoS is flooding attacks, where the attacker floods the target with an excessive amount of traffic. In addition, flooding attacks vary regarding the protocol type employed to flood the victim. In Bandwidth Distributed DDoS (BW-DDoS), the attacker tries to deprive the victim of valid traffic. This type of attack and malicious activities heavily are carried out by botnets where a large number of compromised zombies are responsible for sending spoofed IP packets.

In Reflection-based DDoS attacks, uncompromised systems were incorporated to send a massive traffic load to the victim system in order to consume and over flow its network bandwidth. As an advantage, this tactic allows attackers to transfer traffic to the victim system implicitly and assists the attacker in staying undetected for a long time. The attacker sends IP packets containing the victim's IP address in the field of the IP packet's source address. As the server receives this request, it sends its response to the victim node, never to the real packet source node. Smurf is one of the most well-known Reflection-based DDoS attacks.

In amplification attacks, the attacker manages a set of slave and master zombies and instructs them to flood a huge volume of requests into the reflector systems. To intensify the attack and prevent detection, botnets may be used by attackers to launch more extreme reflective attacks. The amplifying Reflective DDoS attacks, which use certain protocols to augment the victim's reflected traffic, are a special subtype of DDoS attacks. The underlying challenge with this attack is that there are more applied response messages than the attacker's request messages. Consequently, the reflector servers, overwhelming the resources and bandwidth of the victim host or site, exacerbate the data flow toward the victim system. To launch amplification attacks running protocols like domain name service (DNS) or network time protocol (NTP) that amplify the traffic is needed. A comprehensive hierarchy of DDoS attacks is indicated in Fig. 5.

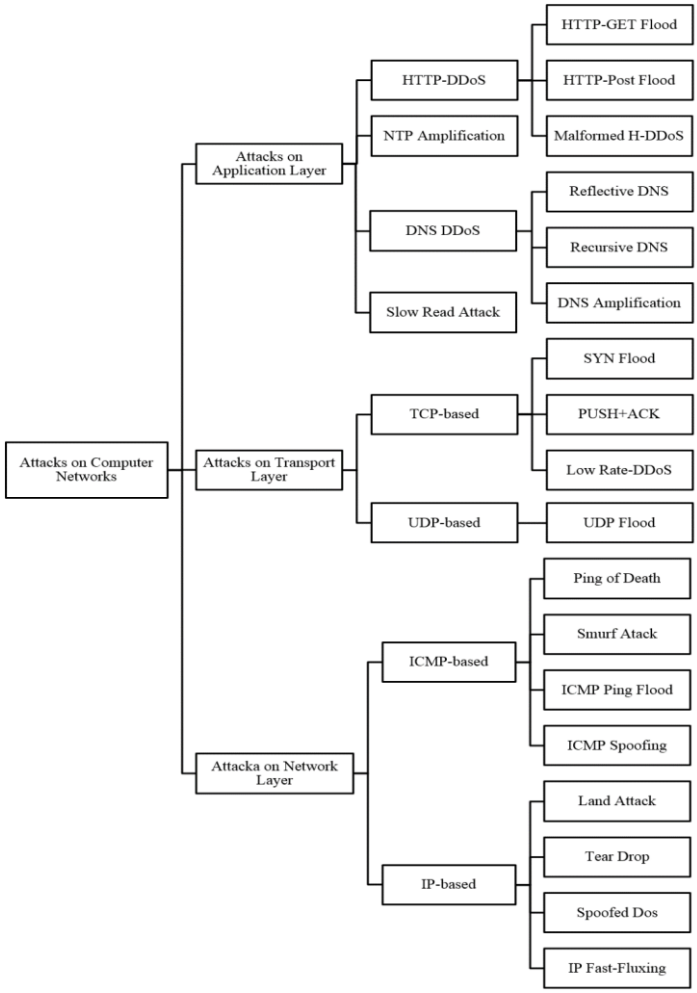


Fig. 5: A hierarchy of DDoS attacks on TCP/IP layers.

3.1.1. Zero-day DDoS attacks

Zero-day attacks attempt to exploit unpublished and unknown vulnerabilities, including security flaws and system faults, in network protocols, operating systems, and software applications. Dealing with these attacks is a very hard and complicated task as they cannot be detected by traditional signature-based IDS methods. Although anomaly-based IDS schemes can deal with these attacks by distinguishing the normal behavior of protocols from under-attack traffic, the novel attack patterns are able to mislead even the anomaly-based methods.

3.1.2. Slow-rate DDoS attacks

Unlike other large-scale DDoS attacks that exhaust the destination with a huge amount of traffic, this kind of DDoS attack targets the victim servers by benefiting from a small and slow traffic pattern, aiming to bypass the

anomaly-based intrusion detectors. This attack pattern is very similar to legitimate traffic as it comes with a very slow rate, making it hard to detect. In this type of attack, there is no need for a substantial amount of systems resources; it can be taken place with merely one single computer or network component. This makes it possible for the attackers to establish unrecognizable large-size botnets to launch DDoS attacks as they are based on running a tiny malware stub on the victim's systems for a long time with gaps between the attack's events. Hence, this type can be considered an advanced persistent threat (APT) attack pattern.

3.2. Datasets

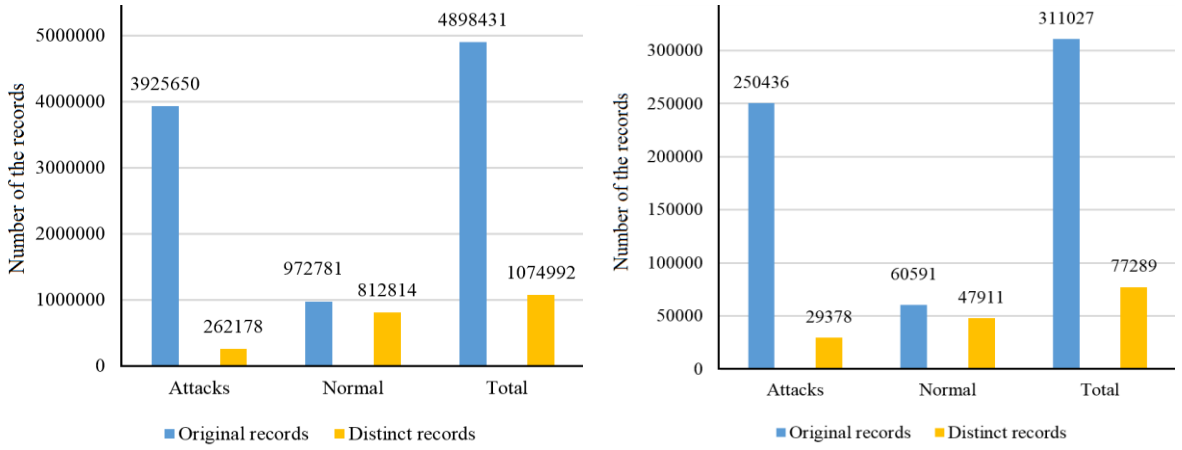
This subsection introduces and describes the datasets employed by the anomaly detection methods studied in this paper. Some of these datasets are pretty old; in the evaluation of newly proposed anomaly detection schemes, the most up-to-date and state-of-the-art datasets should be used as they contain newer attack traffic to malicious behavior.

3.2.1. KDD-Cup99

This dataset is the most famous and established produced from the DARPA 1998 dataset and presented by the Lincoln Labs at MIT University. It contains 41 features, which can be classified as host-based traffic features, time-based features, basic features, as well as content features. The KDD-Cup'99 dataset consists of 4,898,430 records of attacks, such as:

- User to root (U2R) attacks, in which the attacker logs in to the computer systems like normal users. Afterward, exploiting some existing vulnerabilities, the attacker tries to scale their role to an administrator user.
- Remote to local (R2L) attacks, in which the attacker exploits certain security flaws to log in to the remote systems.
- Probing attacks, in which the attacker attempt to extract and gather some data about the network equipment and systems.
- DDoS Attacks.

The main challenge with this dataset is the existence of many duplicated records, in which 78% of the training dataset and 75% of the testing data are replicated. Fig. 6 indicates the number of records in the KDD-Cup99.



(a) Training dataset (b) Testing dataset

Fig. 6: The number of records in the KDD-Cup'99 dataset

3.2.2. UCLA

This dataset was created by the network research lab at the University of California, Los Angeles (UCLA), in August 2001. It consists of UDP flood traffic traces with 1001 bytes of data packets. In its captured file, the attack was aborted at the end of the tracing process and proceeded with normal traffic. This dataset is quite old and cannot effectively train detector models considering today's complicated cyber-attacks.

3.2.3. ISOT

The ISOT dataset is generated from two malicious traffic datasets of Waledac and Storm botnets involved in the Honeynet Project. Typically, Waledac is the successor of the Storm botnet and is considered a well-known peer-to-peer (P2P) botnet that uses a decentralized protocol for communication. It uses Overnet and a fast-flux-based DNS network to establish communication channels. In contrast, traffic from two separate datasets - one from the Lawrence Berkeley National Lab and the other from the Ericsson research traffic lab in Hungary - represents non-malicious traffic. The Ericsson Lab dataset consists of five subclasses containing applications' traffic, such as web

browsing, gaming, and BitTorrent. This dataset collected data from 22 sub-networks from October 2004 to January 2005.

3.2.4. CAIDA

The Center for Applied Internet Data Analysis (CAIDA) published this DDoS dataset produced by the Networks Laboratory of Ahmad Dahlan University in Indonesia. This dataset has been created in the Pcap format using a packet sniffer program installed on the routers in a network with a star topology. This dataset consists of 5 minutes of anonymous network traffic under a DDoS attack that occurred on 4th August 2007. CAIDA dataset does not contain benign traffic; it only has malicious traffic, including the inbound attacks and victims' responses to the attacks.

3.2.5. NSL-KDD

NSL-KDD is a descendant of the KDD-cup'99, which has rectified many of its problems, such as eliminating the duplicated records from both testing and training subsets. This important modification can lead to unbiased results in intrusion detection schemes and improve the detection rate. NSL-KDD has contained 37 types of attacks, of which 14 are in the testing subset, and 24 are in the training subset. In addition, this dataset has 41 features with five traffic classes, including one normal traffic and four malicious traffic.

3.2.6. CTU-13

The CTU-13 has been captured at Czech Technical University (CTU) in the Czech Republic and has real botnet traffic containing normal and background traffic. This dataset was created in 2013 and included thirteen scenarios of various samples. To produce this dataset, malware programs were run with some protocols in which each scenario has three different traffic packets in a Pcap file. In the CTU-13, each scenario has the following files:

- The Pcap file (*.pcap)* contains the botnet traffic traces.
- The bidirectional NetFlow file (*.biargus)* contains types of traffic and labels. These files differentiate between the server and client and have more data and detailed labels**.**
- An executable (.exe) file.

3.2.7. UNSW-NB 15

The UNSW-NB 15 dataset was created at the University of New South Wales in Sydney. It contained 49 different features and was produced by generating synthetic attacks and modern normal behaviors using the Tcpdump tool from 100 Gigabytes of raw traffic. Furthermore, the Argus and Bro-IDS software tools and several algorithms were employed to generate features and the classes' labels. This dataset has 2,540,044 records with nine types of attacks, including:

- Fuzzers: The attacker discovers security loopholes by feeding massive data, aiming to crash the system.
- Generic: It causes a collision in the block cipher that applies hash functions.
- Shellcode: Attackers send a code for the victim aiming to obtain its control.
- Backdoor: Bypassing authentication mechanisms and providing illegal access to the remote hosts.
- DoS: Overloading the computer resources and preventing authorized access to a host.
- Reconnaissance: Gathering information from computer networks to bypass their defensive mechanism.
- Worm: Attackers replicate themselves to be spread on other computers.
- Analysis: A kind of intrusion that penetrates the victim's web applications via emails, scripts, and ports.
- Exploit: Taking advantage of bugs or vulnerabilities, leading to unsuspected behaviors at the victim.

Six groups of features, such as basic features, flow features, time features, content features, labeled features, and additional features, have been provided in this dataset. Flow features have server-to-client or client-to-server features, while basic features represent protocols' connections. The content features demonstrate the attributes of TCP/IP, and time features have properties such as round trip time, start/end packet time, and arrival time of packets. The additional features indicate general connection attributes, and eventually, the labeled features indicate the label/s for each record.

3.2.8. CICDDoS 2019

This dataset in relatively new and contains real-world traffic of DDoS attacks, labeled based on the timestamp, ports, IPs, protocols, and the name of attack. Similar to other datasets, CICDDoS2019 has a training set (about 7 hours of captured data) and a testing set (about 6 hours of captured data), in which the training set consists of 175,341 records while the testing part has 82,332 records. Moreover, this dataset contains the traffic of various network protocols, such as HTTPS, HTTP, SSH, FTP, etc.

There are 12 different DDoS attacks in the training part of this dataset, such as TFTP, WebDDoS, MSSQL, PortMap, LDAP, NetBIOS, UDP, UDP-Lag, NTP, SYN, SNMP, and DNS, besides seven types of cyber-attacks in the testing part. These attacks are NetBIOS, UDP-Lag, MSSQL, SYN, UDP, PortScan, and LDAP. Deficiencies with this dataset are the size of WebDDoS traffic, which is very small and insufficient for accurate model training. PortScan traffic can only be found in the testing set, making it an imbalanced dataset.

3.2.9. IoT-23

In recent years, IoT botnets connected to external command and control (C&C) centers have been responsible for conducting large-scale distributed DDoS attacks. Detecting DDoS attacks initiated from IoT botnets is more difficult as these devices are often heterogeneous. Mirai and Athena are the most notorious samples of IoT botnets able to perform DDoS attacks and are responsible for many recent cyber-attacks against big companies and the financial sector [11]. The IoT-23 dataset was published in January 2020 by the Avast AIC laboratory and contained the real and labeled IoT traffic, aiming to train models to deal with DDoS attacks originating from IoT devices. In this dataset, three non-malicious devices - these IoT devices are real hardware and not simulated, such as Somfy smart door's lock, an Amazon Echo home intelligent personal assistant, and a Philips HUE smart LED lamp - were used to generate benign traffic traces. Then, the traffic traces of twenty malicious devices were captured under different attack scenarios and added to the dataset.

In the following, Table 3 conducts a comparison between the properties of the datasets used by anomaly detection schemes studied in this paper.

Table 3: A comparison between datasets employed by fuzzy-based anomaly detection schemes.

#	Dataset Names	Pub. Year	Num. of Features	Dataset Size	Types of Attacks	Access Link
1	KDD-Cup'99	1999	42	Training data: 4,898,430 records Testing data: 2,000,000 records	24 attacks in the training set and 14 attacks in the testing set.	http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
2	UCLA	2001	N/A	UDP flood traffic with 1001 bytes of data packets	DDoS Attacks	http://www.lasr.cs.ucla.edu/ddos/traces/public/usc.
3	ISOT	2004	N/A	N/A	N/A	N/A
4	CAIDA	2007	N/A	5 minutes of DDoS attacks in the form of anonymized traffic	DDoS Attacks	https://www.caida.org/catalog/datasets/ddos-0070804_dataset/
5	NSL-KDD	2009	42	Training data: Total: 4,898,431 Attacks: 3,925,650 Normal: 972,781 Testing data: Total: 311,027 Attacks: 250,436 Normal: 60,591	This dataset contains 24 attacks in the training set and 14 attacks in the testing set.	1- https://www.kaggle.com/datasets/hassan06/nslkdd 2- https://www.unb.ca/cic/datasets/nsl.html
6	CTU-13	2013	6	N/A	Botnet traffic	https://www.stratosphereips.org/datasets-ctu13
7	UNSW-NB 15	2015	49	2,540,044 records	9 attacks: Reconnaissance, Generic, Fuzzers, Analysis, DoS, Exploits, Shellcode, Backdoors, and Worms.	https://research.unsw.edu.au/projects/unsw-nb15-dataset
8	CICDDoS 2019	2019	Over 80	Training data: 175,341 records, Testing data: 82,332	Training data: 12 DDoS attacks Testing data: 7 attacks	https://www.unb.ca/cic/datasets/ddos-2019.html
9	IoT-23	2020	N/A	Captured traffic of 3 benign IoT devices. Traffic traces of 20 malicious devices	DDoS Attacks	https://www.stratosphereips.org/datasets-iot23

3.3. Machine Learning Classifiers

Considering the sheer number of cyber-attacks occurred daily, AI-assisted systems are vitally required to detect and confront them automatically. Hence, machine learning techniques have been widely employed to train

detector and classifier models accurately in recent years [12]. This subsection introduces the classifiers used by the fuzzy anomaly detection schemes studied in this paper.

3.3.1. ANFIS

Adaptive Neuro-Fuzzy Inference System (ANFIS) is an interesting method consisting of a Takagi-Sugeno-based fuzzy inference system (FIS) and a neural network. In this method, fuzzy logic has been employed to convert input data into output using a neural network model. Also, ANFIS uses the ANN to tune the FIS and deep learning hyper-parameters, like learning rate, batch size, number of hidden layers, number of neurons, etc. In recent studies, fuzzy adaptive models have widely been employed to detect new deception cyber-attacks, including DDoS [13]. Although the ANFIS model can solve many classification problems in different domains, One of the disadvantages of the ANFIS is its sensitivity to its initial fuzzy rules. Besides, the computation overhead is another drawback of the ANFIS, worsened by increasing the number of fuzzy rules required to address the problem.

3.3.2. ANNs

The biological neural networks of the human brain to solve decision-making, classification, and prediction problems inspire artificial neural networks (ANN). An ANN model is a set of connected artificial neurons that can get some signals and sends them to the other connected neurons after conducting a certain process. Different kinds of ANN models have been presented, which benefit from different architectures, optimization techniques, hash functions, and learning methods to solve linear and non-linear problems. ANN models need larger size datasets compared to traditional machine learning algorithms, but there is no need for reprogramming and manual feature extraction as they can select and extract the most effective features automatically. Besides, given the parallel nature of ANNs, if any elements of the model get failed, the model is still able to proceed and complete the task, but the accuracy might be affected. Nonetheless, the training and testing process of the ANN models is time-consuming and incurs high computational overheads.

3.3.3. Bayesian network

A Bayesian network aims to represent knowledge using a probabilistic graphical model that performs probability computation using the Bayesian theorem. In a Bayesian network, each node represents random variables, and an edge is a conditional probability for the transition between random variables. Therefore, by indicating conditional dependence in a directed acyclic graph, a Bayesian network can model the conditional dependence. Consequently, it can be used to conduct inference on random variables. As an advantage, the Bayesian network's training and classification can be carried out very fast without any sensitivity to unrelated features. Furthermore, it is able to handle different types of data. However, as a disadvantage, it considers that features are independent of each other.

3.3.4. SVM

In machine learning, Support Vector Machine (SVM) is a supervised method widely have been used for regression and classification problems. In an SVM classifier, the classification process applies a non-linear transformation using a hyper-plane to separate two data items. Different types of SVM classifiers have been provided in the literature for binary and multi-class classification and have been effectively used in intrusion detection functions. The SVM classifier can be a better option when the data structure is unknown, as it can handle semi-structured and even unstructured data. Besides, the risk of over-fitting errors is much less in this classifier, so noisy data can be tolerated up to a good point. However, selecting a proper kernel function for the SVM and tuning its parameters is not an easy task. As another disadvantage, the training time of this algorithm is relatively high for large-size datasets.

3.3.5. *k*-NN

k-Nearest Neighbors (*k*-NN) is a non-parametric algorithm proposed by Joseph Hodges and Evelyn Fix in 1951. This algorithm is a supervised learning method that applies *k* nearest data points as input to address the regression and classification problems. As the advantages, *k*-NN is easy to understand and be implemented, its training time is very fast, and it is resilient against noisy data. However, the classification (inference) time for this algorithm is relatively long and consumes much memory. Besides, *k*-NN requires all features of the dataset to be trained accurately.

3.3.6. SOM

In machine learning, self-organizing map (SOM) is an unsupervised dimensionality reduction method to produce low-dimension data from a higher-dimension dataset while the data structure is maintained. Generally, SOM is a kind of artificial neural network that uses a competitive learning approach instead of error-correction learning for training mode. SOMs operate in training to generate a lower-dimensional dataset, and then, in the mapping step, the input data are classified using a generated map. As an advantage, the algorithm provides reasonable

interpretation and visualization. However, sometimes sub-optimal results can be seen in the output. Also, SOM needs similar behavior for nearby data to be effective.

In the following, Table 4 exhibits a comparison between the machine learning classifiers applied by the fuzzy anomaly detection approaches studied in this survey paper.

Table 4: A comparison between the classifiers employed by anomaly detection schemes

#	Classifier's name	Advantages	Disadvantages
1	ANN	Handling non-linear problems	High training and testing time Incurs high computational overheads
2	Bayesian Network	High training and classification speed No sensitivity to unrelated features Can handle different types of data.	Features independence assumption
3	SVM	Support for semi-structured and unstructured data. Low over-fitting risk Tolerance for noisy data	High training time Difficult to learn Need for kernel selection Tuning its parameters
4	*k*-NN	Easy to understand Easy to learn Low training time Resilience against noisy data	Long classification time High memory requirements Need for all features
5	SOM	Easy to understand Observable process Low training time	Need sufficient data

4. Fuzzy-based DDoS and anomaly detection approaches

This section presents a comprehensive study of fuzzy techniques for detecting DDoS attacks and network anomalies. To this aim, this paper first classifies the existing methods based on the type of fuzzy techniques, as indicated in Fig. 7. Then, it describes the capabilities of these methods in detecting network anomalies and DDoS attacks. Besides a comparison between the studied approaches is presented at the end of each section. In a holistic view, these schemes highly benefit from the Sugeno or Mamdani fuzzy models. Despite the Mamdani model, the number of output functions and fuzzy rules in the Sugeno models is the same. The Sugeno model also uses a weighted average to evaluate the crisp outputs during the defuzzification stage, whereas the Mamdani model merely generates fuzzy outputs without any evaluation.

Some of the studied schemes operate offline, which cannot be useful in preventing ongoing attacks and anomalies. In contrast, some others allow real-time detection, which can effectively be employed to deal with ongoing attacks. A hierarchy of fuzzy-based approaches to detect DDoS attacks and networks anomalies is shown in Fig. 7.

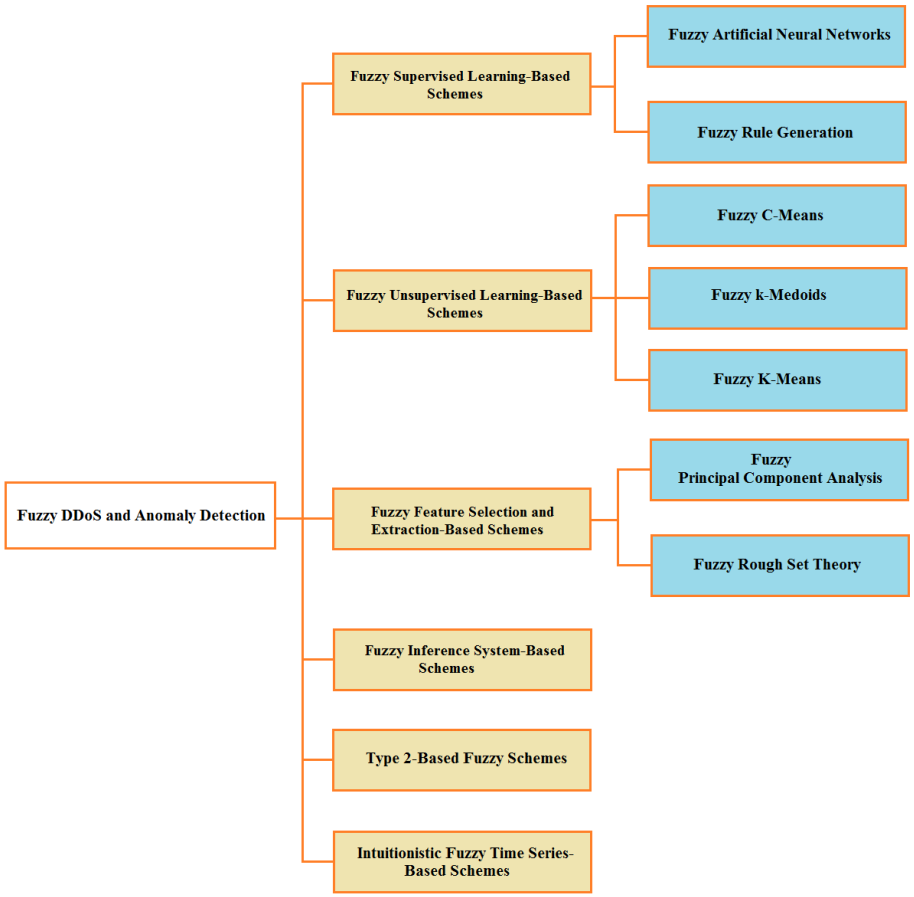


Fig. 7: A taxonomy of the fuzzy-based anomaly detection approaches.

4.1. Fuzzy Supervised Learning-Based Schemes

This subsection studies the DDoS detection approaches that benefit from a fuzzy supervised learning method to detect DDoS attacks, as well as some other anomalies in computer networks.

4.1.1. Fuzzy ANN

The most recent approaches that have applied any kind of fuzzy neural network to detect DDoS and anomalies are presented in this subsection.

Alsaadi *et al.* [14] presented an IDS scheme that applies an information gain method to choose eight essential features in the intrusion detection process. Moreover, ANFIS is used to process the achieved features and classify network data packets into normal or attack packets. This scheme applies two functions, i.e. denoted faster-scaled conjugate gradient and Jang's Neuro-fuzzy. In the experiments conducted in MATLAB software, datasets such as ISCX, NSL-KDD, and KDDcup99 are applied to evaluate this fuzzy anomaly detection scheme. The authors indicated that the scheme could achieve higher precision in finding attack or normal behaviors regarding the root mean square error (RMSE) metric. In addition, it gains better time processes and accuracy in the classification process and detects different intrusions more effectively. Nonetheless, the authors failed to compare their scheme with other recently proposed IDS schemes to further verify the achieved results.

In [15], the authors applied two fuzzy techniques, namely a FIS and an ANFIS model, to efficiently detect and handle flooding attacks in a homogeneous WSN. This method uses a fuzzy method for clustering based on factors such as trust factor, mobility, and residual energy. Afterward, the cluster's data is collected by the anchor node and then evaluated by the ANFIS model, which utilizes metrics such as packet transfer rate and node's energy consumption to recognize the maliciousness of data packets. In the next step, if the data packets are recognized to have been sent from a non-malicious node, then the anchor node sends the packets to the sink node located in the middle of the WSN. The authors evaluated their scheme in MATLAB software by considering 500 sensor nodes with 1J energy over a 500×500 square meter area. These tests evaluate the proposed scheme and some other recent security solutions regarding metrics such as detection delay, detection rate, energy consumption, packet drop ratio, delay, and throughput.

Vijayakumar *et al.* [16] presented a fuzzy logic-based scheme for recognizing jamming attacks, which may lead to denial of service in wireless sensor networks. For this purpose, they applied ANFIS and FIS to detect the

jamming regarding detection metrics such as Received Signal Strength Indicator (RSSI) and packet delivery ratio. If there is a jammed sensor in the cluster, this scheme detects it based on such metrics. The scheme utilizes a Takagi–Sugeno-based FIS to optimize the jamming detection metrics. The authors conducted experiments in MATLAB software to evaluate their presented ANFIS and FIS models based on metrics such as false detection and true detection ratios.

Karthiga *et al.* [17] introduced an anomaly-based detection method that applies convolutional neural networks and ANFIS for detecting security attacks in Vehicular Ad Hoc Networks (VANETs). This method consists of two components denoted as unknown and known IDS modules for detecting unknown and unknown attacks. This scheme applies ANFIS to detect known malicious attacks and deep learning to find unknown attacks. Besides, it presents MLNET, a Modified LeeNET architecture for recognizing the unknown attack type. For the evaluation of this scheme, datasets such as i-VANET and CIC-IDS 2017 are applied. The latter consists of infiltration attacks, web attacks, DDoS attacks, heart-bleed attacks, botnet attacks, and Brute Force attacks. The authors carried out their experiments using MATLAB software based on metrics, including accuracy, precision, sensitivity, and specificity.

Farhin *et al.* [18] proposed a security solution for the Internet of Things that detects malicious attacks using an SDN. In this scheme, the incoming and outgoing traffic flows are analyzed using the SDN controller, and the anomalies are detected and blocked. SDN applies a fuzzy neural network-based attack detection system that recognizes malicious behaviors such as malicious code, side-channel, man-in-the-middle, and DDoS attacks. The authors conducted the necessary experiments on the Matlab-Simulink software tool. They applied the expert opinion for designing the fuzzy rule-based system and, afterward, trained the model and tested it based on the features attained from the NSL-KDD dataset. Carried out with an F-1 score, recall, precision, and accuracy, these evaluations show that this scheme can accurately recognize the malicious attacks against the IoT. Nonetheless, the scheme was not evaluated on the more recent IDS and DDoS datasets.

In order to mitigate the false alarm rate and improve the accuracy of intrusion detection, Manimurugan *et al.* [19] applied the ANFIS and Crow Search Optimization algorithm in a network intrusion detection system. They applied the Crow search optimization algorithm to optimize the proposed ANFIS model. The authors performed their experiments and tests on the NSL-KDD dataset and analyzed the performance of their approach based on metrics such as accuracy, false positive rate, precision, and recall. This scheme was compared with other schemes such as PSOANFIS, GA-ANFIS, FC-ANN, and BPNN. It was demonstrated that the detection rate of this scheme was 95.80%, with a false positive rate of 3.45%. Nonetheless, the authors failed to evaluate the performance of their scheme using other new datasets and the old dataset used for their evaluations, which may not contain the recent attacks.

4.1.2. Fuzzy Rule Generation-Based Schemes

This subsection addresses the fuzzy DDoS and anomaly detection schemes that try to extract a minimized subset of rules, which can recognize anomalies with high accuracy and a low false-positive rate.

In [20], the authors introduced the FT-EHO, a fuzzy DDoS attack detection framework that uses the Taylor-elephant herd optimization algorithm and a deep belief network. It performs a rule-learning process using the Taylor series, EHO, and a fuzzy classifier. Using KDD-Cup99 and two other synthetic datasets, the authors analyzed their scheme and exhibited that it could present percentages of 93.81%, 97.20%, 94.981%, and 93.833% for accuracy, detection rate, precision, and recall, respectively.

Moreover, the authors of [21] put forward an approach for the classification of logs using a time-varying evolving fuzzy-rule-based classification model and sliding time windows. They extracted time window attributes to develop an evolving Gaussian fuzzy classifier and improved its accuracy and compactness.

To detect DDoS attacks in cloud computing environments, Velliangiri and Pandey [22] introduced FT-EHO-DBN, a classifier created by combining the T-EHO optimization algorithm, fuzzy logic, and DBN classifier. In this scheme, requests are sent to a feature extraction module for extracting the packets' features. The extracted features are then sent to a feature selector engine for extracting the selective features using a holoentropy-based feature selection method. Afterward, the classification module is tasked to detect DDoS attacks by applying the fuzzy classifier and DBN. In this scheme, the T-EHO algorithm is used for rule learning in the fuzzy classifier. The KDDcup database was used to evaluate this scheme, and the proposed scheme was compared with the other classifiers such as SVM, ANN, and an ensemble regarding evaluation metrics such as precision, accuracy, detection accuracy, and recall. Nonetheless, this scheme suffers from high computational costs.

4.2. Fuzzy Unsupervised Learning-Based Schemes

Unlike the non-fuzzy clustering methods (hard clustering), in fuzzy clustering (soft clustering), each data point can simultaneously belong to several clusters to some degree. Fuzzy clustering-based methods are widely incorporated for unsupervised anomaly detection problems in which no labeled dataset exists for anomaly

detection. Fuzzy clustering has widely been used in various approaches to detect DDoS attacks and network security anomalies in combination with optimization algorithms for tuning hyper-parameters and improving the accuracy of fuzzy clustering [23]. Table 5 summarizes the properties of the fuzzy supervised learning-based schemes.

Table 5: The properties of the fuzzy supervised learning-based schemes.

Ref.	Pub. Year	Dataset Names	Simulation Factors	Membership Function	Restrictions
[24]	2019	Self-collected	Sensitivity, Specificity	--	It should be tested on other datasets as well.
[19]	2020	NSL-KDD	Precision, False-positive rate, Recall	--	Only one outdated dataset was used for analysis. It is not contrasted with other approaches for detecting anomalies.
[20]	2020	KDD-Cup'99, Two synthetic datasets	Accuracy, Detection rate, Precision, Recall	--	--
[21]	2020	Self-collected	Accuracy, Number of Rules, Time	Gaussian	It can only handle host-based anomaly detection schemes.
[22]	2020	KDD-Cup'99	Recall, Accuracy, Precision	Triangular	Only one outdated dataset was used for evaluation.
[25]	2020	Self-collected	Energy consumption	--	It is not contrasted with other algorithms and anomaly detection techniques.
[26]	2020	KDD-Cup'99	Accuracy, Sensitivity, Specificity, AUC	Gaussian	Only one outdated dataset is used for evaluation. It was not properly compared to other anomaly detection techniques.
[27]	2020	NSL-KDD, UNSW-NB15	Accuracy, Average time cost, Influence of device traffic on detection efficiency	--	More comparisons with different classifiers are required to confirm the findings because this technique was only tested against the SVM classifier.
[28]	2021	DDoS-2016	True positive rate, True negative rate, False negative rate, False positive rate, Detection rate	--	It was not compared with other approaches.
[29]	2021	NSL-KDD, UCI dataset	Accuracy, Number of rules, Run time	Triangular	The results were only compared using the accuracy metric, and other metrics were not considered in comparisons.

4.2.1. FCM-Based schemes

Fuzzy c-means (FCM) is a fuzzy clustering method applied in many anomaly intrusion detection approaches. FCM allows soft data clustering in which each data point belongs to several clusters by some membership degrees. However, the results show that FCM is sensitive to the initial centroids or cluster centers and may suffer from local optima problems. The computation complexity of the algorithm is $O(NF \times P^2 \times DI)$, in which DI is the dimension, P is the number of subsets, and NF is the number of features. Some anomaly intrusion detection-based schemes have improved the FCM clustering method using metaheuristic algorithms or other techniques. On the other hand, some systems have accepted the deficiencies of the FCM and applied it in combination with different strategies for anomaly detection. Moreover, selecting the optimal number of clusters in FCM is another issue that should be dealt with in this clustering algorithm. Plenty of FCM-based anomaly detection approaches have been proposed in the literature.

In [30], the authors suggested a detection algorithm for DDoS attacks based on various graph features such as index, outdegree, betweenness, and eigenvector centrality. These functions calculate node values, such as source and destination IP addresses. The standard and attack behaviors of the network are modeled using these features. In addition, suspicious and safe IP addresses are identified using a fuzzy clustering method. The algorithm was tested on the real data obtained from the network of Boğaziçi University. However, the authors failed to verify their anomaly detection approach by conducting the necessary experiments on standard datasets.

4.2.2. Fuzzy k-Medoids-Based schemes

k-Medoids is a clustering algorithm proposed by Kaufman and Rousseeuw to partition the dataset into clusters. Then, it minimizes the distance between the centroids and data points assigned to each cluster. In selecting the centroids, the k-Medoids algorithm selects the data points as centroids, which performs better than other clustering algorithms such as k-Means. Besides, as an advantage, the k-Medoids algorithm can be applied with any dissimilarity metric, but the k-Means method needs Euclidean distances. The computation complexity of the k-

Medoids algorithm is $O(N^2)$, in which N is the number of data items. Some schemes employ this clustering algorithm for detecting anomalies and DDoS attacks.

4.2.3. Fuzzy K-Means-Based schemes

Another popular clustering technique in data mining, K-means, seeks to separate the data into a predetermined number of clusters. The key issue is its sensitivity to the original data, which could result in the local optima problem [31]. The computation complexity of this clustering algorithm is $O(N^2)$, in which N is the number of data items. A variety of fuzzy k-means-based DDoS attacks and anomaly detection schemes have been presented in the literature, some of which will be studied in this section.

Table 6 lists the properties of the Fuzzy Unsupervised Learning-Based and Fuzzy Feature Extraction-Based approaches, as well as makes a comparison between them.

Table 6: Properties of the fuzzy unsupervised learning-based and fuzzy feature extraction-based approaches

Ref.	Pub. Year	Dataset Names	Simulation Factors	Membership Function	Restrictions
[30]	2019	Self-collected	N/A	Triangular Trapezoidal	It does not provide the required experimental results on the standard datasets.
[32]	2019	UCI dataset, msnbc.com	Detection rate, False-positive rate	N/A	It can only handle session anomalies and cannot be used for network anomalies.
[33]	2019	KDD-Cup'99	Detection rate False-positive rate	Gaussian	N/A
[34]	2020	Synthetic dataset, UCI dataset	Recall, Precision, F-measure, AUC	N/A	N/A
[35]	2020	NSL-KDD	Accuracy, Missing rate False-positive rate, F1-measure	Gaussian	Experiments were conducted only on one dataset.
[36]	2020	KDDCup-99, NGIDS-DS, ToN_IoT	Detection rate, False negative rate, False-positive rate	Gaussian	N/A
[37]	2020	N/A	Decryption times, Execution times, Encryption times, Specificity, Sensitivity	Triangular	The number of clusters should be indicated and reported.
[38]	2020	Synthetic dataset, IBRL, NSL-KDD Benchmark, Numenta Anomaly,	Accuracy False-positive rate,	N/A	N/A
[39]	2021	Synthetic dataset	F-Measure, Precision, Recall	N/A	N/A
[40]	2021	Synthetic dataset	Accuracy, Calinski–Harabasz Index, Silhouette Coefficient	N/A	It has not applied standard IDS datasets to further verify the results.
[41]	2021	N/A	Accuracy, False-positive rate	N/A	It lacks evaluation and comparison against other anomaly detection methods.

4.3. Fuzzy Feature Extraction-Based Schemes

This section investigates DDoS and anomaly detection approaches that have applied fuzzy feature selection and extraction methods.

4.3.1.Fuzzy Principal Component Analysis-Based Schemes

Principal component analysis (PCA) is a feature extraction method employed in the anomaly intrusion detection field by a few researchers. Since these works were not new, they were excluded from this survey.

4.3.2.Fuzzy-Rough Set Theory-Based Schemes

Fuzzy rough set theory is used by several schemes for DDoS and anomaly detection. Furthermore, the anomaly detection framework in [33] applies a fuzzy rough set-based SVM classifier and a fuzzy rough set. This scheme uses two intelligent agents for feature selection and decision-making. The first one selects better features using a fuzzy rough set. In contrast, the second tries to make a decision. It also uses a fuzzy rough-based SVM for finding anomalies. They used the KDD-Cup'99 dataset and demonstrated that they could provide better results in terms of the false-positive rate and accuracy.

Furthermore, an anomaly detection model is presented in [35] that uses a fuzzy rough set and information gain ratio in feature selection and presents a GA-based pattern learning method. The authors provided a clustering method, named GA-GOGMM, based on a Gaussian mixture model and used it to extract normal and intrusion

patterns. GA-GOGMM attains the optimal GMM for pattern clustering and avoids the clustering method's susceptibility to the initial data. In this scheme, the required experiments were conducted using NSL-KDD and self-collected network traffic. They proved that their approach outperformed other schemes regarding detection accuracy and false-positive rate.

In [36], the authors proposed FGMC-HADS or Fuzzy Gaussian Mixture-based Correntropy, which operates using mechanisms such as correntropy, GMM, or Gaussian mixture model, and FRAR or fuzzy rough set attribute reduction. FGMC-HADS uses the GMM and Correntropy approaches for fusing multivariate features and conducting anomaly detection. The FGMC-HADS was evaluated using the KDDCup-98, NGIDS-DS, and ToN_IoT datasets. The authors indicated that their proposed scheme made hosts more secure against unknown attacks.

4.4. Fuzzy Inference System-Based Schemes

A fuzzy inference system processes the input values and produces an output vector by considering the fuzzy set theory and using some fuzzy rules and fuzzy membership functions. In addition, it is important to note that the FIS output is a fuzzy set. Generally, a fuzzy inference system consists of a fuzzifier, defuzzifier, and inference engine, of which two types, namely Mamdani and Sugeno, are used. The fuzzifier is responsible for converting crisp values into fuzzy sets. The fuzzification process applies various membership functions such as Gaussian, triangular, and trapezoidal to represent the fuzzy sets. In this step, three different fuzzifiers, such as trapezoidal or triangular fuzzifiers, Gaussian fuzzifiers, and singleton fuzzifiers can be applied. At last, in the defuzzification step, a decision-making algorithm is used to achieve a crisp value from the fuzzy inference results. Besides, methods such as the center of the largest area, center of sums, maxima, and center of gravity can be employed in the defuzzification step. Fig. 8 exhibits the architecture of a fuzzy inference system.

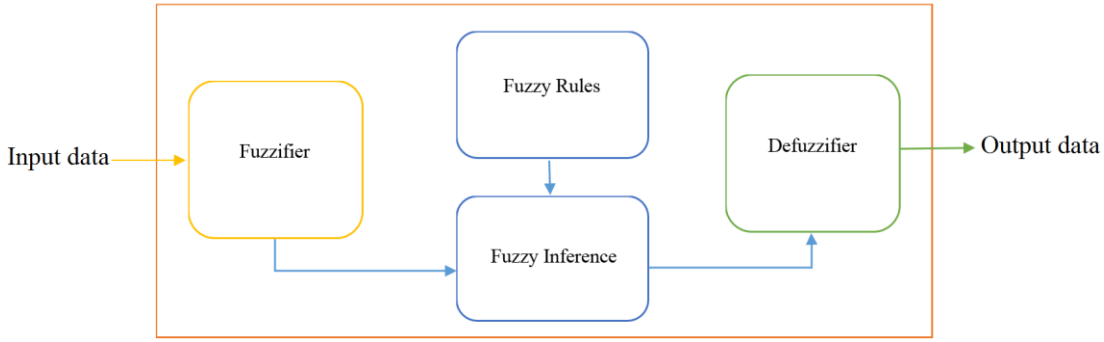


Fig. 8: The schematic of the fuzzy inference system.

Several schemes have applied the FIS for DDoS detection and anomaly detection. For Instance, Scarnati *et al.* [42] put forward an anomaly detection system that applies the artificial immune system to detect network event variations to recognize attacks with no prior information. In this scheme, fuzzy logic is employed to decrease uncertainty when a clear boundary does not exist between abnormal and normal traffics. They applied a dataset containing different DDoS attacks and evaluated attacks such as flooding and portscan. They proved that their system could outperform the naive Bayes and KNN classifiers regarding metrics such as F-measure. However, this approach has not addressed distinguishing the DDoS attacks from the flash crowd.

In [43], Novaes *et al.* introduced LSTM-FUZZY, a solution for monitoring, detecting, and decreasing network anomalies in the SDN. The architecture of this method for anomaly detection is shown in Fig. 9.

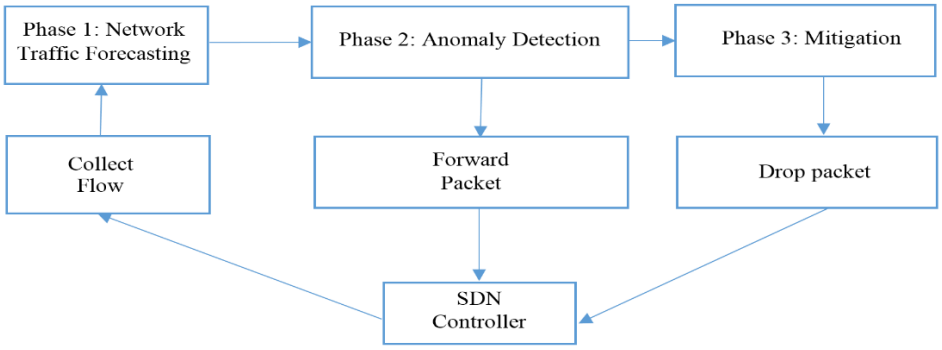


Fig. 9: The architecture of network anomaly detection [43].

It has three modules, in which the first one characterizes the network traffic and predicts the network's normal behavior by using short-term long memory. In the second module, attacks are recognized using fuzzy logic and Bienaymé-Chebyshev's inequality. The third module applies automatic anomaly reduction policies to reduce the attack damages. The authors validated their scheme using the Floodlight controller and Mininet emulator and considered Portscan and DDoS attacks in the first scenario. They also applied the CICDDoS2019 dataset in another scenario. They proved that their scheme could outperform KNN, SVM, LSTM-2, MLP, as well as PSO-DS regarding precision, false-positive rate, recall, and area under the curve (AUC) rate. Nevertheless, this scheme was not evaluated against other types of DDoS attacks and vulnerabilities in different SDN topologies.

Nguyen *et al.* [44] introduced an entropy-based FIS model to detect the data anomaly from the packets' interval arrival time. This FIS model provided the required rules to find the varied mean and sensor traffic variance. The authors showed that this scheme outperformed the entropy-based Shannon method in terms of detection rate with the conducted experiments. However, analyzing their schemes with other intrusion detection metrics and various types of anomalies can provide useful insight into their system, which the authors failed to achieve.

Alsirhani *et al.* [45] presented a DDoS detection approach that employs a fuzzy logic system, a distributed system, and some classifiers. In this scheme, the classifiers are applied to classify the network traffic into normal traffic and DDoS attacks. To be more specific, this scheme benefits from classifiers such as random forest, decision tree (Gini), decision tree (entropy), and naive Bayes. In addition, for recognizing the DDOS attacks, it applies the fuzzy logic for choosing one of these classifiers dynamically based on their execution delay and accuracy. This scheme applies the real-world traffic traces of the CAIDA collected from high-speed monitors on a commercial backbone link from 2008 to 2019. In this process, they used a software tool, T-shark, a command terminal version of the Wireshark network analysis tool. T-shark is applied for getting packet fields from the dataset and converting the dataset into the CSV format. They exhibited that the selection of the appropriate classification algorithm can be carried out using the fuzzy logic system based on the traffic status. In these experiments, they used evaluation metrics, including false positive rate, F-measure, Recall, precision, and accuracy. The results of the experiments indicated that the fuzzy logic could choose the correct classifier, and this scheme could get a trade-off between delay and accuracy. Nonetheless, their scheme cannot get the same performance for different datasets.

Since the SDN controller is among the important components of the SDNs, it is vulnerable to various types of DDoS security attacks, and successful attacks can make them unreachable to the rest of the SDNs. This can be more sensible in the wireless SDNs that employ wireless links between the SDN devices and controllers. To deal with this issue, Rios *et al.* [46] introduced a DDoS detection scheme using Euclidean Distances, MLP, and a FIS for the detection of RoQ or Reduction of Quality DDoS attacks that try to reduce the QoS (Quality of Service) of the victim service regardless of the transport protocol used for communication. This method does not employ a feature selection method, and the authors handpicked the applied features to achieve good results in the classification step. They used three features such as entropy, an average inter-arrival time, and packet number, for the classification and detection of DDoS attacks. The scheme applies four Internet traffic traces, two of which are used for evaluation and obtained from real and emulated environments. The authors created a dataset for each of these traces, consisting of three features, i.e. the number of packets, entropy rate, and the average inter-arrival time. They created an attack tool named M-RoQ for generating attacks used to create the traffic traces. In their experiments, they used metrics such as confusion matrix, F1-score, precision, and recall and indicated that their proposed fuzzy approach could outperform MLP in detecting RoQ attacks. However, this scheme was not analyzed over well-known standard datasets, and more evaluations are needed to be verified. Besides, no feature selection method was used in this scheme, and it could be enhanced by various feature selection techniques.

4.5. Type 2-Based Fuzzy Schemes

The DDoS detection schemes that have applied type-2 fuzzy sets will be addressed in this subsection. For instance, Srilatha and Shyam [47] introduced an IDS scheme for cloud computing environments, which applies the kernel FCM integrated with a classifier to prevent unauthorized activities in cloud computing. This scheme for finding new attacks trains the type-2 fuzzy neural network using attack data and clusters the training data with the kernel FCM method. In addition, the lion optimization algorithm is used for tuning the parameters of the type-2 fuzzy neural network. This scheme, after the training step, will be able to recognize security attacks. The training and testing steps were carried out using the NSL-KDD dataset. Besides, for evaluating this scheme, experiments were conducted in the CloudSim tool and JDK 1.6 using metrics such as F-measure, recall, and precision. The achieved results were compared against other classifiers such as the k-nearest neighbor, fuzzy logic controller, ANN, and naive Bayes. Nonetheless, a legacy dataset was employed for testing this scheme.

Pajila *et al.* [48] introduced FBDR, a solution for detecting and handling DDoS attacks in WSNs. It applies to type-1 fuzzy logic to recognize the DDoS attacks in sensor nodes and utilizes the type-2 fuzzy sets for

recovering from the attacks. Detecting DDoS attacks, this scheme is able to mitigate the power consumption of sensor nodes and enhance the WSNs' lifetime. The authors conducted their experiments using MATLAB software in a 500×500 square environment, in which the number of sensor nodes varied from 50 to 500. The evaluations were conducted regarding metrics such as network lifetime, number of alive nodes, packet drop rate, energy consumption, response time, buffer usage, detection rate, and execution time.

4.6. Intuitionistic Fuzzy Time Series-Based Schemes

Intuitionistic fuzzy time series are used by some schemes to handle DDoS attacks and anomalies in computer networks. For instance, Wang *et al.* [49] applied intuitionistic fuzzy time series-based graph mining to detect anomalies in the network traffic. First, they used multiple parallel variable ordering heuristic intuitionistic fuzzy time series to present forecasting models for multi-dimension feature entropy of traffic data. Then, they built an intuitionistic fuzzy time-series-based graph using change amplitudes in entropy and edge weights between vertices defined by similarity. Finally, they frequently performed the mining of subgraphs on the intuitionistic fuzzy time-series graph and built anomaly vectors using the mining results. The authors analyzed this scheme using three datasets; the first one was the DDoS 2007 dataset; the second one was achieved from the traffic traces from the trans-Pacific backbone link in 2007; the third one was the Witty Worm dataset. Besides, in those experiments, the proposed anomaly detection scheme was regarding false alarm rate and detection rate.

Fan *et al.* [50] have proposed a long-term intuitionistic fuzzy time series method to forecast network traffic. In this method, the network traffic was intuitionistically fuzzyfied and vector quantized, and the time series vectors were created using an improved version of intuitionistic fuzzy c-means clustering techniques. The authors have claimed that their proposed fuzzy c-mean clustering algorithm can enhance the discrimination of time series segments and improves the efficiency of forecasting while the computational complexity reduces compared to other related works. Furthermore, this makes it possible to perform preprocessing data, mimicking nonlinear features of a network to be applied in detecting DDoS anomalies in realtime.

A comparison between the FIS-based intrusion detection methods is reported in Table 7.

Table 7: The properties of the FIS-based anomaly intrusion detection schemes

Ref.	Pub. Year	Dataset Names	Simulation Factors	Membership Function	Restrictions
[44]	2019	Synthetic traffic	Abnormal detection rate	N/A	It was not compared with other intrusion detection metrics and other anomalies.
[42]	2020	CICDDoS 2019	Precision, Accuracy, ROC curve, False-positive rate, Recall, F-measure	Triangular Gaussian	It cannot distinguish DDoS attacks originating the flash crowd; only one dataset was used in experiments.
[43]	2020	CICDDoS 2019	Recall, Precision, AUC rates, False-positive rate	Triangular	This method was evaluated against other DDoS attacks in different SDN topologies.
[49]	2020	DDoS 2007 dataset, the traffic traces from the trans-Pacific backbone link, Witty Worm dataset	False alarm rate, Detection rate	N/A	N/A
[45]	2021	Self-collected dataset	Recall, Accuracy, F-Measure, precision, False-positive rate, True-positive rate	Triangular	N/A
[46]	2021	Self-collected	Confusion matrix, F1-score, Precision, Recall		This scheme was not evaluated with the standard IDDS and DDoS attacks datasets.
[47]	2021	NSL-KDD	F-measure, recall, and precision	Gaussian	A legacy dataset was employed for testing this scheme.
[48]	2022	N/A	Network lifetime, number of alive nodes, packet drop rate, energy consumption, response time, buffer usage, detection rate, and execution time	Triangular, Gaussian	Standard datasets were not applied for the evaluation of this scheme.

5. Discussion

This section provides useful information regarding the methods and techniques used to defend against network anomalies and DDoS attacks. Such information is very useful in finding the areas that can be further studied in the next research. To be more specific, the following are analyzed in this section:

- Percentage of the schemes provided using different learning and fuzzy techniques
- Percentage of the applied fuzzy classifiers
- Percentage of the datasets utilized anomaly detection processes
- Percentage of the employed FLC types
- Percentage of anomaly detection and DDoS detection schemes
- Number of the schemes that have applied different membership functions

Fig. 10 demonstrates the percentage of the applied different techniques in the investigated schemes. As shown in this figure, most of the studied schemes use fuzzy supervised and unsupervised learning methods to identify anomalies and confront DDoS attacks. Since unsupervised learning-based DDoS detection methods do not require any training, they are much faster than the supervised detection approaches, but the latter provides more accuracy in detecting anomalies and attacks.

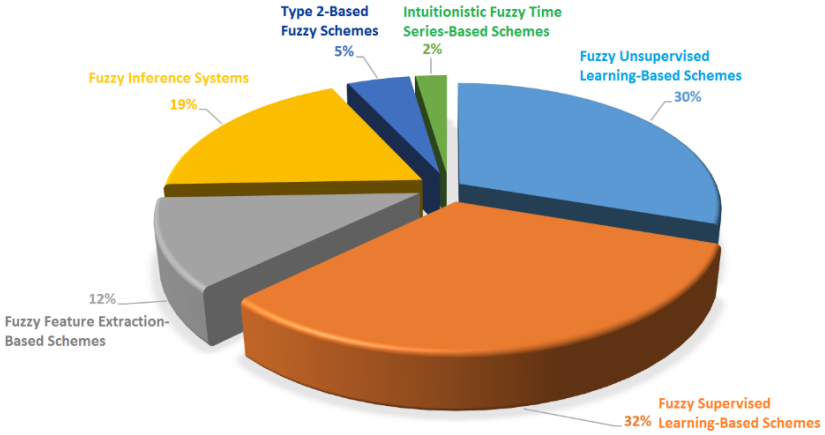


Fig. 10: The percentage of the applied fuzzy techniques.

The number of the schemes that have applied different fuzzy algorithms in the fuzzy supervised learning and fuzzy unsupervised learning-based categories are depicted in Fig. 11. As shown in this figure, different types of fuzzy ANN models and FCM clustering algorithms are used by most investigated schemes to deal with DDoS attacks and network anomalies. Nonetheless, the security schemes that utilize the fuzzy ANN models should deal with the overfitting problem, especially when the fuzzy ANN models have many parameters to be tuned. Clustering methods such as FCM are very fast and incur very low overhead because they do not need any training. This makes them ideal for low-powered environments, as well as cases where there is a lack of labeled data. Nonetheless, they suffer from a high false positive rate and are sensitive to the initial data. Therefore, most clustering-based methods try to improve the clustering method by using, for instance, metaheuristic algorithms and achieve better results.

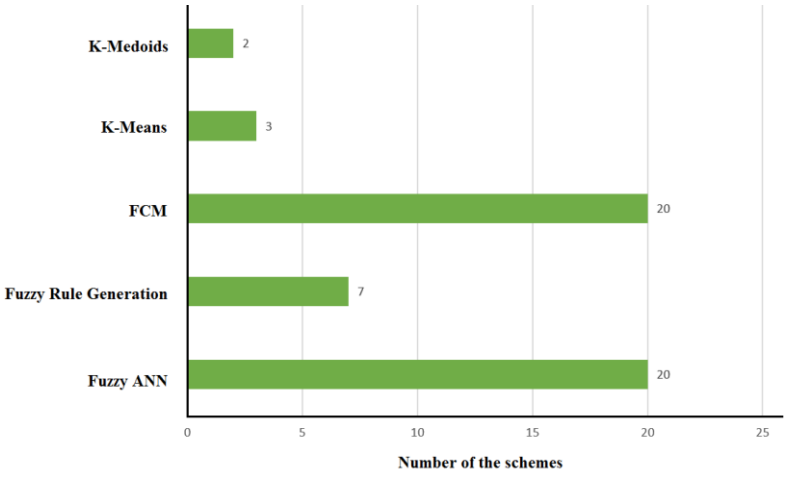


Fig. 11: The number of fuzzy methods applied in the fuzzy supervised and unsupervised learning-based schemes.

In the following, the anomaly detection datasets applied in the studied fuzzy logic-based DDoS detection and anomaly detection methods are indicated in Fig. 12. As shown in this figure, the majority of the approaches have used KDD-Cup'99, synthetic, and self-collected datasets. In addition, few schemes have used the new datasets, such as UNSW-NB15 and CICDDoS datasets. The important issue in this context is that almost 69% of the investigated approaches have used only one dataset, 26% have used two datasets, and only 5% have used three or more datasets in their evaluations.

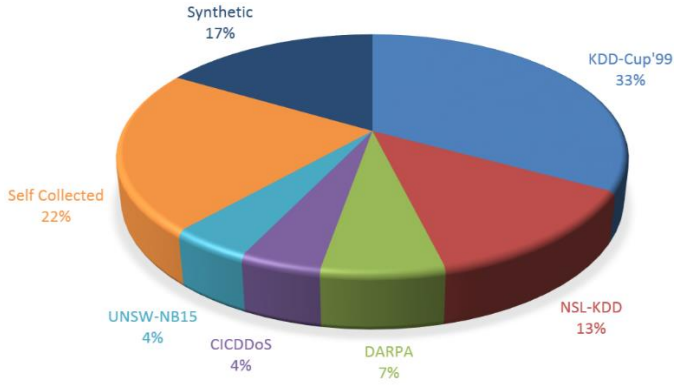


Fig. 12: The datasets used in the studied anomaly detection methods.

The percentage of FLC types used in the examined frameworks is shown in Fig. 13. As shown in this chart, Mamdani FLC has been the most widely used fuzzy DDoS detection and anomaly detection approach due to its simplicity and efficiency.

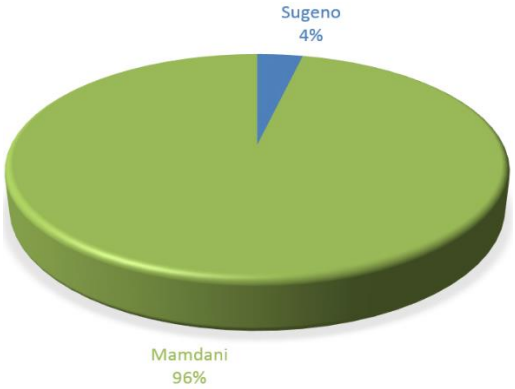


Fig. 13: The percentage of the FLC types used in the studied methods.

Additionally, Fig. 14 lists the number of various membership functions used in a few fuzzy anomaly detection techniques, which has helped shed light on the specifics of their fuzzy methodology.

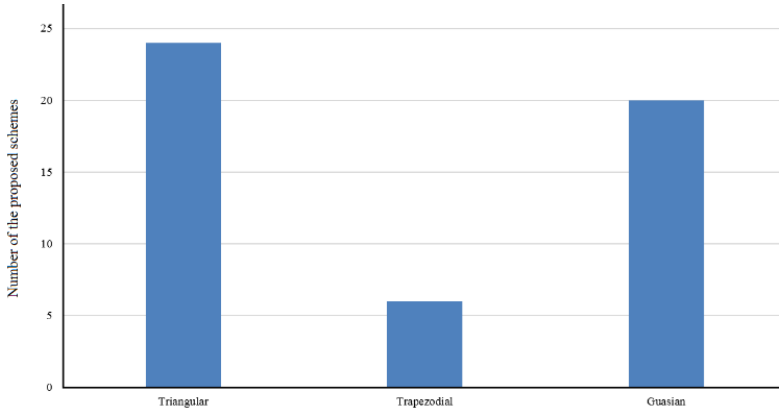


Fig. 14: The number of the schemes that have applied different membership functions.

Besides, the percentage of fuzzy DDoS detection and anomaly detection systems is shown in Fig. 15. Considering this figure, it is evident that merely a few fuzzy DDoS detection systems have been presented so far, and the majority of the schemes are devoted to dealing with anomaly detection issues. Therefore, more efforts might be made to further enhance fuzzy DDoS detection techniques.

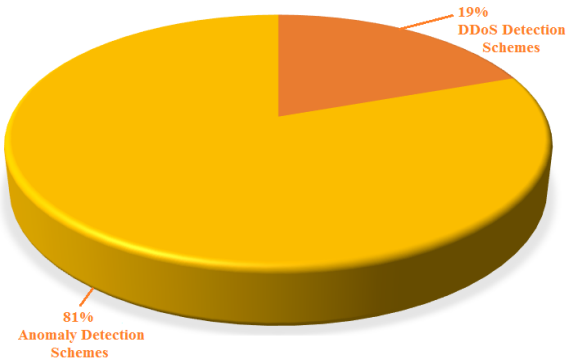


Fig. 15: The percentage of anomaly detection and DDoS detection schemes.

At the end of this section, Table 8 indicates a comparison from various perspectives between the IDS models that have employed various datasets, including CICDDoS, NSL-KDD, and KDD-Cup'99, to evaluate their proposed solutions.

Table 8: A Comparison of the IDS schemes applying different datasets

Ref.	Dataset Name	Accuracy Rate	Detection Rate	False-positive Rate	Precision	Recall	F-value
[42]	CICDDoS	89.03	--	--	88.65	26.46	92.28
[43]		--	--	2.2	97.89	93.13	--
[19]	NSL-KDD	97.41	95.80	3.45	--	--	--
[29]		94.54	--	--	--	--	--
[38]		--	97.59	1.05	--	--	--
[20]	KDD-Cup'99	93.811%	97.200	--	94.981	93.833	--
[22]		--	--	--	--		--
[26]		93.811	97.200	--	94.981	93.833	--
[36]		75.24	--	6.73	--	--	--

Furthermore, it can be concluded that, in addition to the accuracy of detection and performance, the energy consumption of intrusion detection systems should be taken into account due to rapid advances and the pervasive nature of wireless environments like wireless sensor networks, as well as new smart battery-powered devices. The usage of these devices and wireless communications have become more frequent than ever with emerging new smart cities and the Internet of Things.

6. Conclusions and future researches directions

Albeit rapid advances in information technology and artificial intelligence has offered many facilities, including ease of access and high availability, they caused a paradigm shift in cybersecurity threats. The large number of daily cyber-attacks indicates that computer systems and networks are highly vulnerable to cybersecurity threats. Anomaly detection systems have played a critical role in the security of organizations and businesses by finding new and Zero-day malicious behavior and cyber-attacks. These systems employ AI-powered models to learn the normal profiles and behavioral patterns and identify any deviation from such patterns as anomalies. However, distinguishing between normal and suspicious behavior patterns is difficult in today's large-scale networks and the sheer amount of data production. In this paper, we conducted a systematic literature review and comprehensive survey on recent advances have made in the area of anomaly-based intrusion detection systems that employ fuzzy logic to correlate network behavioral features. This paper also presented a new hierarchy to categorize various types of DDoS attacks based on their internal mechanism and technology. Our findings indicated that fuzzy logic could effectively be incorporated into a wide variety of network anomaly detection schemes as a highly reliable solution with the purpose of increasing the accuracy of intrusion detection while the performance of the network is maintained.

Over recent years, cyber-attacks led to billions of dollars in financial loss to companies, businesses, individuals, universities, and even hospitals, while most victims were well-equipped with intrusion detection and anti-malware devices. The underlying reason is that there were several gaps and security holes in the secure configuration of defensive devices. The key findings and outcomes of this survey paper pave the way to implement novel generations of anomaly-based intrusion detection systems and tackle a wide range of challenges and gaps

that exist in the current intrusion detection systems and methods. Providing the most effective and best-offered defensive strategies, this paper's recommendations are highly beneficial for institutions, enterprises, and governmental agencies to mitigate cyber threats and make their digital data more secure and their business more sustainable.

6.1. Future Perspectives

Although the fuzzy DDoS detection and anomaly detection domains are studied deeply and thoroughly, some limitations and issues can be considered for the next study:

- Low run-time complexity should be a requirement for real-time anomaly detection methods. Therefore, it is important to explore and develop new, low-cost methods in the future.
- The performance of the fuzzy anomaly detection schemes is decreased by a large amount of data and high dimensionality found in the anomaly detection datasets. In that case, the features used for detecting different anomalies can be investigated, and in various datasets, important features can be recognized and prioritized to be used in the anomaly detection process. Thus, further research on the feature selection/extraction methods should be conducted, and new methods should be devised to find the best features with the lowest possible overhead.
- The investigated fuzzy schemes have often used the Mamdani-based FLCs, and very few have used the Sugeno FLCs. Consequently, Sugeno FLCs can be further focused on in the future.
- A few anomaly intrusion detection techniques have used type-2 fuzzy sets, but the majority of the schemes under study have used type-1 fuzzy sets. Consequently, type-2 fuzzy sets should be studied in future research.
- Only a small number of the numerous novel metaheuristic algorithms proposed in the literature have been applied to adjusting the FIS's parameters or locating fuzzy rules. Thus, the future generation of fuzzy anomalous intrusion detection frameworks should make use of more recent metaheuristic algorithms, especially multi-objective ones.
- Network intrusion detection systems protect organizations whose operations are evolving and changing from time to time. Ideally, network anomaly detection approaches should deal with such changes; otherwise, their false-positive rate will increase. Although a few methods, such as incremental learning, are provided for dealing with such issues, this issue must be investigated further in subsequent studies.
- Only a few investigated frameworks are specially designed for environments such as cloud computing, SDNs, WSNs, WBANs, IoT, etc. Thus, environment-specific anomaly detection approaches should be further studied regarding the IT domain's rapid developments. For this purpose, environment-specific datasets are also needed to evaluate these new methods.
- Other machine learning and data mining methods can be integrated with them to further enhance the fuzzy network anomaly detection process and cover the possible limitations of the fuzzy solutions.
- Most fuzzy network anomaly detection approaches apply the genetic algorithm to produce rules and collect a compact set of them. However, the other metaheuristic algorithms are not involved in this context, which should be addressed in future fuzzy anomaly detection approaches.
- Failing to deal with encrypted traffic is one of the common vulnerabilities of the security components such as firewalls and intrusion detection systems. In this context, only a few network anomaly detection models are developed to deal with anomalies in encrypted traffic. Thus, further research in this domain seems necessary.
- Clustering is an unsupervised learning method that has been successfully integrated into various steps of anomaly detection methods. However, most applied clustering algorithms need to know the number of clusters to prove helpful. Thus, in future studies, auto-clustering and dynamically determining the number of clusters should be further investigated.
- Regarding the architectural style, from the studied fuzzy anomaly detection schemes, one can conclude that most of them are centralized, and few studies enjoy a distributed architecture. Thus, regarding the distributed nature of computer networks, distributed fuzzy network anomaly detection schemes should be focused on in subsequent studies to deal with a broader range of network anomalies.
- Challenging issues in the DDoS attacks detection domain, such as distinguishing DDoS attacks from the flash crowd, should be further investigated in the subsequent fuzzy network anomaly detection schemes.
- Different kinds of fuzzy deep learning techniques introduced in this survey can be beneficial for detecting various types of DDoS attacks and anomaly detections in different environments.
- Online training or incremental learning for continuous training of the DDoS and anomaly detection schemes should be further investigated in the future.
- The investigated schemes have often been evaluated on old datasets or un-standard self-collected datasets. Thus, a complete set of experiments on standard and up-to-date datasets should be conducted in subsequent security studies. Also, real network traces should be used to verify the achieved results.

- Since very few schemes from the investigated ones addressed the imbalanced datasets problem, this problem can be investigated and handled in the future.
- Considering the emerging security attacks, new datasets should be created, or the existing ones should be updated to thoroughly evaluate the new proposals in the DDoS attacks and anomaly detection contexts.

Acknowledgment
This research was supported by Personal Basic Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (RS-2022-00166712).

References

[1] D. Javaheri, P. Lalbakhsh, and M. Hosseinzadeh, "A Novel Method for Detecting Future Generations of Targeted and Metamorphic Malware Based on Genetic Algorithm," *IEEE Access*, vol. 9, pp. 69951-69970, 2021, doi: 10.1109/ACCESS.2021.3077295.

[2] S.-W. Lee *et al.*, "Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review," *Journal of Network and Computer Applications*, vol. 187, p. 103111, 2021/08/01/ 2021, doi: https://doi.org/10.1016/j.jnca.2021.103111.

[3] M. Masdari and H. Khezri, "A survey and taxonomy of the fuzzy signature-based intrusion detection systems," *Applied Soft Computing*, p. 106301, 2020.

[4] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," *Journal of Systems Architecture*, vol. 105, p. 101701, 2020.

[5] Y. Hande and A. Muddana, "A survey on intrusion detection system for software defined networks (SDN)," *International Journal of Business Data Communications and Networking (IJBDCN)*, vol. 16, no. 1, pp. 28-47, 2020.

[6] P. Wang, L. T. Yang, X. Nie, Z. Ren, J. Li, and L. Kuang, "Data-driven software defined network attack detection : State-of-the-art and perspectives," *Information Sciences*, vol. 513, pp. 65-83, 2020/03/01/ 2020, doi: https://doi.org/10.1016/j.ins.2019.08.047.

[7] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Computers & Security*, vol. 86, pp. 147-167, 2019.

[8] T. Jafarian, M. Masdari, A. Ghaffari, and K. Majidzadeh, "A survey and classification of the security anomaly detection mechanisms in software defined networks," *Cluster Computing*, pp. 1-19, 2020.

[9] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Cluster Computing*, pp. 1-13, 2019.

[10] R. Chaganti, B. Bhushan, and V. Ravi, "A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions," *Computer Communications*, vol. 197, pp. 96-112, 2023/01/01/ 2023, doi: https://doi.org/10.1016/j.comcom.2022.10.026.

[11] Z. Shao, S. Yuan, and Y. Wang, "Adaptive online learning for IoT botnet detection," *Information Sciences*, vol. 574, pp. 84-95, 2021/10/01/ 2021, doi: https://doi.org/10.1016/j.ins.2021.05.076.

[12] D. Javaheri, M. Hosseinzadeh, and A. M. Rahmani, "Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines," *IEEE Access*, vol. 6, pp. 78321-78332, 2018, doi: 10.1109/ACCESS.2018.2884964.

[13] H. He, W. Qi, H. Yan, J. Cheng, and K. Shi, "Adaptive fuzzy resilient control for switched systems with state constraints under deception attacks," *Information Sciences*, vol. 621, pp. 596-610, 2023/04/01/ 2023, doi: https://doi.org/10.1016/j.ins.2022.11.074.

[14] H. I. H. Alsaadi, R. M. ALmuttari, O. N. Ucan, and O. Bayat, "An adapting soft computing model for intrusion detection system," *Computational Intelligence*, vol. 38, no. 3, pp. 855-875, 2022.

[15] P. Beslin Pajila, E. Golden Julie, and Y. Harold Robinson, "ABAP: Anchor Node Based DDoS Attack Detection Using Adaptive Neuro-Fuzzy Inference System," *Wireless Personal Communications*, pp. 1-25, 2022.

[16] K. Vijayakumar, K. Pradeep Mohan Kumar, K. Kottilingam, T. Karthick, P. Vijayakumar, and P. Ganeshkumar, "An adaptive neuro-fuzzy logic based jamming detection system in WSN," *Soft Computing*, vol. 23, no. 8, pp. 2655-2667, 2019.

[17] B. Karthiga, D. Durairaj, N. Nawaz, T. K. Venkatasamy, G. Ramasamy, and A. Hariharasudan, "Intelligent Intrusion Detection System for VANET Using Machine Learning and Deep Learning Approaches," *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[18] F. Farhin, I. Sultana, N. Islam, M. S. Kaiser, M. S. Rahman, and M. Mahmud, "Attack detection in internet of things using software defined network and fuzzy neural network," in *2020 Joint 9th International Conference on Informatics, Electronics & Vision (ICIEV) and 2020 4th International Conference on Imaging, Vision & Pattern Recognition (icIVPR)*, 2020: IEEE, pp. 1-6.

[19] S. Manimurugan, A.-q. Majdi, M. Mohmmed, C. Narmatha, and R. Varatharajan, "Intrusion detection in networks using crow search optimization algorithm with adaptive neuro-fuzzy inference system," *Microprocessors and Microsystems*, vol. 79, p. 103261, 2020.

[20] S. Velliangiri and H. M. Pandey, "Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms," *Future Generation Computer Systems*, 2020.

[21] L. Decker, D. Leite, L. Giommi, and D. Bonacorsi, "Real-time anomaly detection in data centers for log-based predictive maintenance using an evolving fuzzy-rule-based approach," in *2020 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, 2020: IEEE, pp. 1-8.

[22] S. Velliangiri and H. M. Pandey, "Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms," *Future Generation Computer Systems*, vol. 110, pp. 80-90, 2020.

[23] D. Javaheri, S. Gorgin, J.-A. Lee, and M. Masdari, "An improved discrete harris hawk optimization algorithm for efficient workflow scheduling in multi-fog computing," *Sustainable Computing: Informatics and Systems*, vol. 36, p. 100787, 2022/12/01/ 2022, doi: https://doi.org/10.1016/j.suscom.2022.100787.

[24] A. Alabdulatif, I. Khalil, H. Kumarage, A. Y. Zomaya, and X. Yi, "Privacy-preserving anomaly detection in the cloud for quality assured decision-making in smart cities," *Journal of Parallel and Distributed Computing*, vol. 127, pp. 209-223, 2019.

[25] H. Fan, "Data Monitoring and Anomaly Analysis for Information Systems based on Balanced Scorecard and Fuzzy Neural Network," in *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020: IEEE, pp. 117-120.

[26] P. V. de Campos Souza, A. J. Guimarães, T. S. Rezende, V. J. Silva Araujo, and V. S. Araujo, "Detection of anomalies in large-scale cyberattacks using fuzzy neural networks," *AI*, vol. 1, no. 1, pp. 92-116, 2020.

[27] L. Fang, Y. Li, Z. Liu, C. Yin, M. Li, and Z. J. Cao, "A practical model based on anomaly detection for protecting medical IoT control services against external attacks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4260-4269, 2020.

[28] M. Almseidin, J. Al-Sawwa, and M. Alkasassbeh, "Anomaly-based intrusion detection system using fuzzy logic," in *2021 International Conference on Information Technology (ICIT)*, 2021: IEEE, pp. 290-295.

[29] W. Guendouzi and A. Boukra, "A new differential evolution algorithm for cooperative fuzzy rule mining: application to anomaly detection," *Evolutionary Intelligence*, pp. 1-12, 2021.

[30] Ç. Ateş, S. Özdel, and E. Anarım, "Graph–Based Anomaly Detection Using Fuzzy Clustering," in *International Conference on Intelligent and Fuzzy Systems*, 2019: Springer, pp. 338-345.

[31] M. H. Nadimi-Shahraki and H. Zamani, "DMDE: Diversity-maintained multi-trial vector differential evolution algorithm for non-decomposition large-scale global optimization," *Expert Systems with Applications*, vol. 198, p. 116895, 2022/07/15/ 2022, doi: https://doi.org/10.1016/j.eswa.2022.116895.

[32] R. Xiao, J. Su, X. Du, J. Jiang, X. Lin, and L. Lin, "SFAD: Toward effective anomaly detection based on session feature similarity," *Knowledge-Based Systems*, vol. 165, pp. 149-156, 2019.

[33] K. Selvakumar *et al.*, "Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs," *Information Sciences*, vol. 497, pp. 77-90, 2019.

[34] X. Wang, H. Wang, and Y. Wang, "A density weighted fuzzy outlier clustering approach for class imbalanced learning," *Neural Computing and Applications*, vol. 32, no. 16, pp. 13035-13049, 2020.

[35] J. Liu *et al.*, "Adaptive intrusion detection via GA-GOGMM-based pattern learning with fuzzy rough set-based attribute selection," *Expert Systems with Applications*, vol. 139, p. 112845, 2020.

[36] W. Haider, N. Moustafa, M. Keshk, A. Fernandez, K.-K. R. Choo, and A. Wahab, "FGMC-HADS: Fuzzy Gaussian mixture-based correntropy models for detecting zero-day attacks from linux systems," *Computers & Security*, vol. 96, p. 101906, 2020.

[37] P. Santhosh Kumar and L. Parthiban, "Scalable Anomaly Detection for Large-Scale Heterogeneous Data in Cloud Using Optimal Elliptic Curve Cryptography and Gaussian Kernel Fuzzy C-Means Clustering," *Journal of Circuits, Systems and Computers*, vol. 29, no. 05, p. 2050074, 2020.

[38] S. Garg *et al.*, "En-ABC: An ensemble artificial bee colony based anomaly detection scheme for cloud environment," *Journal of Parallel and Distributed Computing*, vol. 135, pp. 219-233, 2020.

[39] D. Wang, Z. Shen, and W. Wu, "A Fuzzy Clustering Based Anomaly Node Detection Method for Publish/Subscribe Distributed Systems," in *Journal of Physics: Conference Series*, 2021, vol. 1813, no. 1: IOP Publishing, p. 012046.

[40] S. Huang, Y. Guo, N. Yang, S. Zha, D. Liu, and W. Fang, "A weighted fuzzy C-means clustering method with density peak for anomaly detection in IoT-enabled manufacturing process," *Journal of Intelligent Manufacturing*, vol. 32, no. 7, pp. 1845-1861, 2021.

[41] S. Lu, J. Wu, R. Gu, W. Liu, and M. Zhu, "An anomaly detection parameter optimization algorithm for data center data," in *2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2021, vol. 5: IEEE, pp. 1782-1785.

[42] G. F. Scaranti, L. F. Carvalho, S. Barbon, and M. L. Proença, "Artificial Immune Systems and Fuzzy Logic to Detect Flooding Attacks in Software-defined networks," *IEEE Access*, 2020.

[43] M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, "Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment," *IEEE Access*, vol. 8, pp. 83765-83781, 2020.

[44] V.-T. Nguyen, T.-X. Nguyen, T.-M. Hoang, and N.-L. Vu, "A new Anomaly Traffic Detection Based on Fuzzy Logic Approach in Wireless Sensor Networks," in *Proceedings of the Tenth International Symposium on Information and Communication Technology*, 2019, pp. 205-209.

[45] A. Alsirhani, S. Sampalli, and P. Bodorik, "DDoS detection system: Using a set of classification algorithms controlled by fuzzy logic system in apache spark," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 936-949, 2019.

[46] V. de Miranda Rios, P. R. Inácio, D. Magoni, and M. M. Freire, "Detection of reduction-of-quality DDoS attacks using Fuzzy Logic and machine learning algorithms," *Computer Networks*, vol. 186, p. 107792, 2021.

[47] D. Srilatha and G. K. Shyam, "Cloud-based intrusion detection using kernel fuzzy clustering and optimal type-2 fuzzy neural network," *Cluster Computing*, vol. 24, no. 3, pp. 2657-2672, 2021.

[48] P. Pajila, E. G. Julie, and Y. H. Robinson, "FBDR-Fuzzy based DDoS attack Detection and Recovery mechanism for wireless sensor networks," *Wireless Personal Communications*, vol. 122, no. 4, pp. 3053-3083, 2022.

[49] Y.-N. Wang, J. Wang, X. Fan, and Y. Song, "Network Traffic Anomaly Detection Algorithm Based on Intuitionistic Fuzzy Time Series Graph Mining," *IEEE Access*, vol. 8, pp. 63381-63389, 2020.

[50] X. Fan, Y. Wang, and M. Zhang, "Network traffic forecasting model based on long-term intuitionistic fuzzy time series," *Information Sciences*, vol. 506, pp. 131-147, 2020/01/01/ 2020, doi: https://doi.org/10.1016/j.ins.2019.08.023.

Declaration of interests

☒ The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: