International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 6, December 2021, pp. 5216~5228
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i6.pp5216-5228

Detection of ICMPv6-based DDoS attacks using anomaly based intrusion detection system: A comprehensive review

Adnan Hasan Bdair AIghuraibawi[1], Rosni Abdullah[2], Selvakumar Manickam[3], Zaid Abdi Alkareem Alyasseri[4]
[1,3]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia
[1]Baghdad College of Economic Sciences University, Baghdad, Iraq
[2]School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
[4]Center for Artificial Intelligence, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Malaysia
[4]ECE Dept. Faculty of Engineering, University of Kufa, Najaf, Iraq
[4]Artificial Intelligence Research Center (AIRC), College of Engineering and Information Technology, Ajman University, Ajman, United Arab Emirates

Article Info

Article history:

Received Oct 18, 2020
Revised May 21, 2021
Accepted Jun 12, 2021

Keywords:

Anomaly detection
DDoS attack
ICMPv6
IPv6
Machine learning

ABSTRACT

Security network systems have been an increasingly important discipline since the implementation of preliminary stages of Internet Protocol version 6 (IPv6) for exploiting by attackers. IPv6 has an improved protocol in terms of security as it brought new functionalities, procedures, i.e., Internet Control Message Protocol version 6 (ICMPv6). The ICMPv6 protocol is considered to be very important and represents the backbone of the IPv6, which is also responsible to send and receive messages in IPv6. However, IPv6 Inherited many attacks from the previous internet protocol version 4 (IPv4) such as distributed denial of service (DDoS) attacks. DDoS is a thorny problem on the internet, being one of the most prominent attacks affecting a network result in tremendous economic damage to individuals as well as organizations. In this paper, an exhaustive evaluation and analysis are conducted anomaly detection DDoS attacks against ICMPv6 messages, in addition, explained anomaly detection types to ICMPv6 DDoS flooding attacks in IPv6 networks. Proposed using feature selection technique based on bio-inspired algorithms for selecting an optimal solution which selects subset to have a positive impact of the detection accuracy ICMPv6 DDoS attack. The review outlines the features and protection constraints of IPv6 intrusion detection systems focusing mainly on DDoS attacks.

Corresponding Author:

Rosni Abdullah
National Advanced IPv6 Centre (NAv6)
Universiti Sains Malaysia
Penang, 11800, Malaysia
Email: rosni@usm.my

1. INTRODUCTION

The world has been witnessing drastic and monumental changes along with the rapid advancement and expansion of the Internet and networking technologies [1]. With this development, Smart computing environments and global information have massively become our societies use, but unfortunately, the design of the security system and policy followed in these environments does not meet the requirements, so the attackers took advantage of the vulnerabilities [2]. More precisely, cybersecurity has become one of the most

prominent fields of study in the real world with the proliferation of network breaches aimed at attempting to access sensitive information without permission or making information and networking networks vulnerable or inaccessible [3].

The abrupt rise in users accessing the internet from diversified devices have completely exhausted IPv4's address space. Wherefore, the introduction of IPv6 that intended to improve communication systems to fulfil the rising future demand for better IPs which Major measures were undertaken by the internet engineering task force (IETF) in 1990 to enhance and upgrade IPv6 from IPv4.Besides IPv6 has effectively processed some issues and limitations in IPv4, including auto-configuration, versatility, and extensibility, in addition, mobility options, security support and used in several fields the "Internet systems" for more effective applications, however, still a challenge [4]-[8]. Based on the data on 9th March 2020, Percentage of customers utilize Google services with IPv6 override 25.88%, however, numbers of user have been steadily increasing since then, as shown in Figure 1 [9].

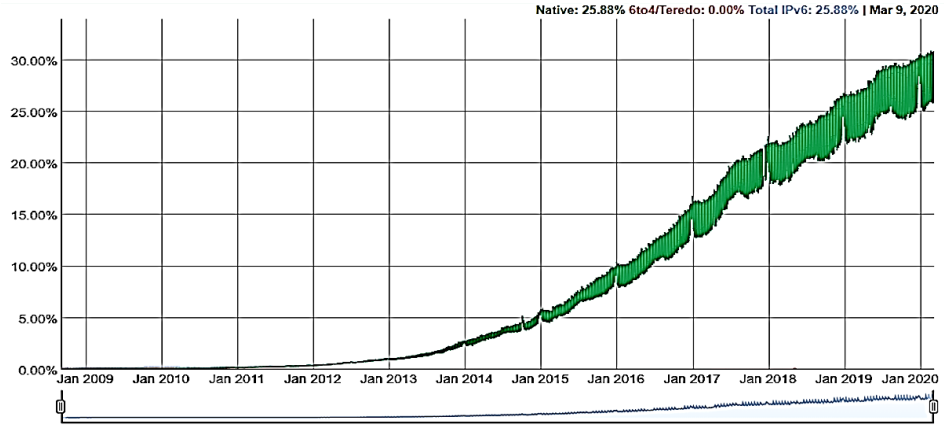

Figure 1. Users reaching Google services over IPv6

IPv6 implemented numerous functionalities one of them is the ICMPv6 Protocol is part of the internet protocol suite responsible for “Stateless Address Auto-configuration” (SLAAC) based on ICMPv6 messages such as neighbor discovery protocol (NDP) that are other roles related to the diagnosis and error reporting of packets being sent [10]-[14]. From the ICMPv6 specification demonstrates distinct and special enhancements, such as NDP replacing address resolution protocol (ARP) and other functional updates to IPv6 [15]. IPv6 implementation has sparked security challenges among network administrators. In order to improve network security, thereby, the administrator needs an effective approach for determining possible threats that can happen in networks [16], [17].

In turn, ICMPv6 protocol in practice is accompanied by security inadequacies susceptible to attacks. Currently. Wherefore, IPv6 networks are experiencing threats many, such as distributed denial-of-service (DDoS) attacks [18]. DDoS is the most dangerous type of threat that uses size and intensity that to deplete the available resources of a network, which are get up restrict access or prevent the use of services by target device customers [14], [19]-[21]. According to the National dataset, IPv6 is most commonly subjected to DoS and DDos attacks, as shown in Figure 2 [22].

In addition, which provide fake and duplicate information, one of important elements make the attack successfully [23]. In many ways, IPv6 implementation has sparked security challenges among network administrators. In order to improve network security, thereby, the administrator needs an effective approach for determining possible threats that can happen in networks [6], [7]. Wherefore, ICMPv6-DDoS attacks constitute one of the major threats and among the hardest security problems currently facing security of networks must be addressed for distinction abnormal anomalies in network traffic [24]-[27]. Wherefore, current methods of the network defense are using, such as antivirus, firewalls and "Intrusion Detection system (IDS)" is a technique to detect any indications of unusual activity across many systems or networks and which the most popular security method [25], [28]. IDS were divided into two types: Host-based IDSs (HIDSs) and network-based IDSs (NIDSs) and divided into three classes: signature, anomaly, and hybrid detection, signature detection systems can detect attacks by using pattern matching and a list of the attack patterns, anomaly detection employs machine learning and data mining algorithms to attacks detection and Hybrid IDS uses both signature and anomaly detection [29], [30]. In addition, the attack can be mitigated by using encryption algorithms in order to secure the mobility of data [31].

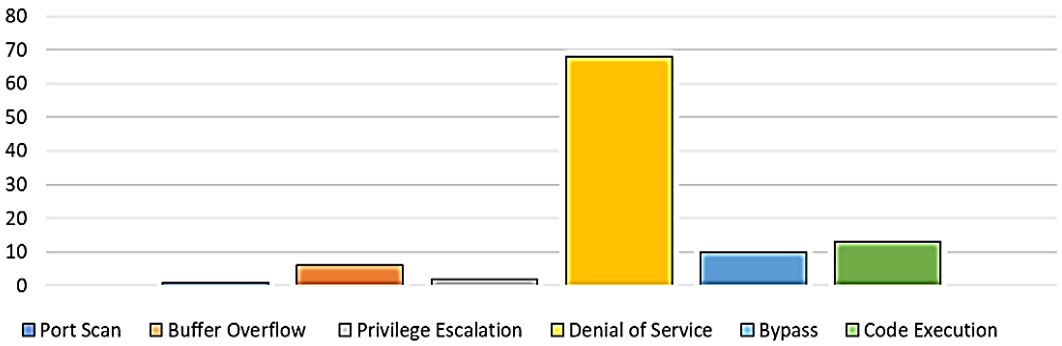

Figure 2. IPv6 vulnerability classes

In general, many approaches are currently for detection ICMPv6-DDoS attacks such as anomaly detection which divided to rule-based detection [32] and AI-based detection using [29], [30], for example machine learning-based detection (MLIDS) [13], [33] data Mining-based detection (DNIDS) [34], [35]. Entropy-based detection (EIDS) [36], [37] and deep learning-based detection [38]-[40]. These approaches are used to distinguishes between the normal and abnormal dataset and the ICMPv6-DDoS attacks detection.

Unfortunately, various IPv6 IDS have, but these are still unable to detect ICMPv6 DDoS attacks with precision because suffers big sized datasets, asymmetrical mobility of information, and the inability to distinguish between attack and regular traffic. Wherefore, this gap is a favorable area for research to construct or devise a model regarding the behaviors of DDoS attacks. For this reason, there are several approaches that had not focused on detection ICMPv6-DDoS attacks are proposed which is based on anomaly detection [13], [33], [41], [42]. Additionally, must design a model detection the ICMPv6-DDoS patterns in IPv6 network depends the review outlines the features and protection constraints of IPv6 detection systems focusing mainly on ICMPv6-DDoS attacks.

Special the literature was selected with this study carefully depending on its quality and effect. Figure 3 appear the primary source for ICMPv6-DDoS attack detection publications utilizing machine learning-based detection, Data mining-based detection, Entropy-based detection, and deep learning-based detection. The classified was works selected depended on the database digital utilized for papers retrieve such as IEEE Xplore, Elsevier, Springer and IAES journals in Figure 3. For further classifications, Figure 3 illustrate the division of ICMPv6-DDoS attack detection work depend on the kind of publication for detection approaches.

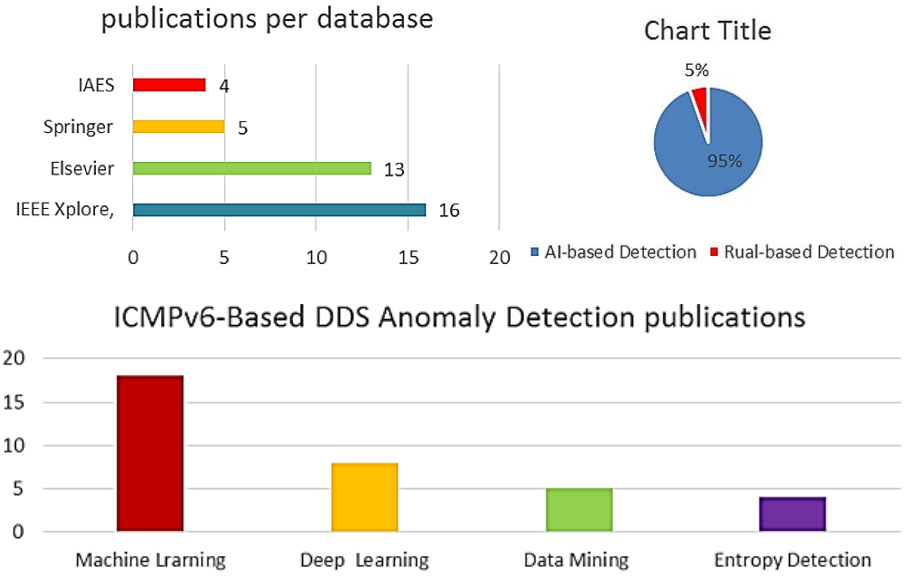

Figure 3. ICMPv6-DDoS attack anomaly detection works

This paper goal is to contribute to review a comprehensive of the latest anomaly-based detection methods used in detecting ICMPv6-DDoS attacks. Over 70 high-impact journals published studied in IEEE Xplore, Elsevier, Springer and IAES. Additionally, this paper could be utilized as a reference to the most widely utilized generic ICMPv6-DDoS attack datasets that other researchers can use.

This paper is answering the following research questions:

Q1- What are anomaly detection approaches implemented for detecting ICMPv6-DDoS attacks?
Q2- Are there any reference dataset that can be used for an evaluation to anomaly detection approaches?
Q3- What are the most of important metrics that can be used to evaluate anomaly detection approaches?
Q4- What are the appropriate anomaly detection techniques that can be used for various indicators of performance to detect ICMPv6-DDoS attacks?

The remainder of this review consists of the following sections: Section 2 introduced the suggested protocol for selecting detecting ICMPv6-DDoS attacks research.

2. PROTOCOL FOR IDENTIFYING RELATED WORKS OF ICMPV6-DDOS ATTACK DETECTION

The literature for this paper was collected using the most keywords relevant when searching, namely "ICMPv6-DDoS attacks detection", "anomaly detection" and "machine learning". This work is researched on English language studies only. The selection of relevant works was done using many digital databases such as IEEE Xplore, Elsevier, Springer and IAES journals, the protocol included the procedure of fifth stages. The first stage is to search these databases for related work on the threat of "DDoS attack". We ended up with 230 papers. To identify the selected paper related to the analysis of "anomaly detection" and machine learning techniques for “ICMPv6-DDoS attacks” threats. Three keywords were used in this stage, namely "ICMPv6-DDoS Attacks", "anomaly detection" and "machine learning" in different groups and were combined with the "IPv6" protocol that means remove the paper in the IPv4 protocol

For the second stage, the papers duplicate was excluded, as 65 papers were discarded. The third stage, the selected papers are nominated depend on the titles and the abstracts, as papers outside our field are excluded. More than 80 articles are discarded in this step and only 85 papers are chosen and passed for the next stage. For the fourth stage, we scroll by each paper to ensure it is within the specified range and as a result, 10 articles are excluded. Finally, we had 75 articles all related to anomaly detection and machine learning techniques for the threat of ICMPV6-DDoS attacks. The paper choosing procedure appears in the flowchart in Figure 4. The same criteria eligibility was used in all three stages by authors who conducted the filtration and sorting.

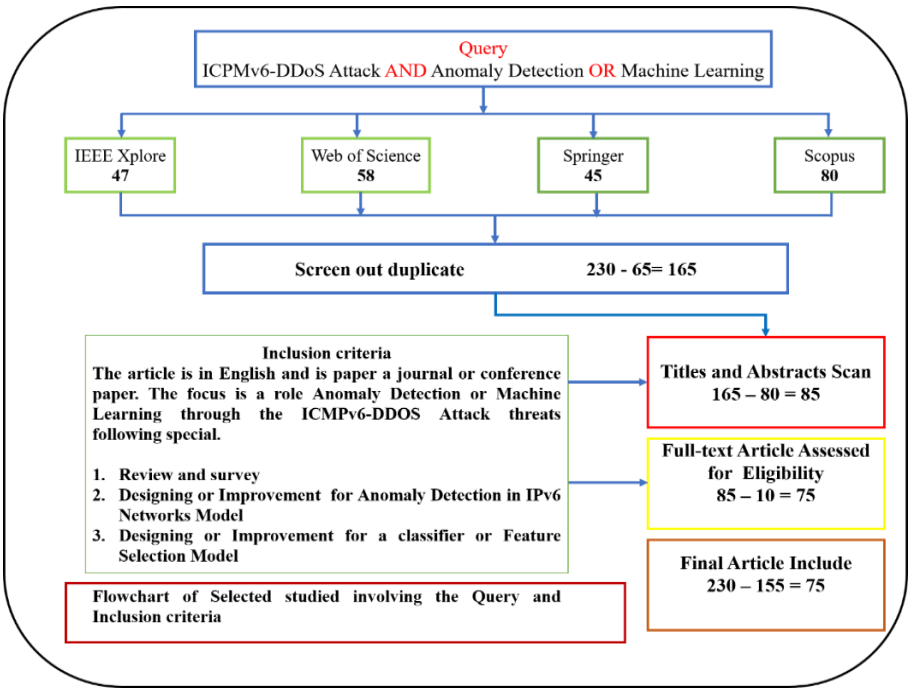

Figure 4. Flowchart for chosen studies involving query and inclusion criteria

3. ANOMALY DETECTION FOR ICMPv6 DDoS ATTACK

Given the severity of the DDoS attack in IPv6 network causes a lot of economic loss to the individual and the institutions, anomaly detection has been used to improve the performance to ICMPv6-DDoS attack detection techniques. The anomaly detection approach for detection ICMPv6-DDoS attack has been applying in two approaches such as Rule-based and AI-based which will be discussed in section 3.1. Furthermore, several AI-based have been used for ICMPv6-DDoS attack detection such as data mining, machine learning, entropy detection and deep learning which will be discussed in section 3.2. Figure 5 displays the classification of anomaly detection work for ICMPv6-DDoS attack detection techniques select in this work.

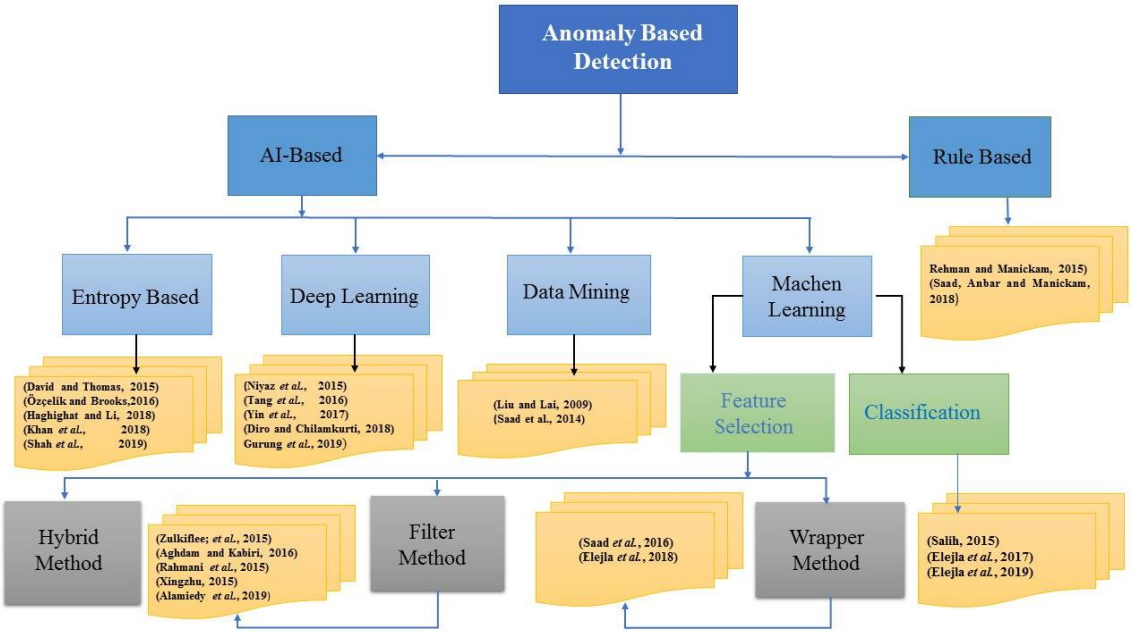

Figure 5. Taxonomy of anomaly-based detection

In this paper, the focus will be on the second type of IDS which is anomaly-based intrusion detection system (IDS) for ICMPv6 DDoS Attacks [34], [35]. From anomaly detection advantages, is determined attacks more effectively than the signature-based IDS with few incorrect positive rates, in addition, automated training is generally used to distinction normal system behavior from abnormal [41]. The anomaly detection consists of four steps the procedure data collection, data preparation, modelling and model evaluation [42]. In this paper there are divided the anomaly detection into two types are rule-based and artificial Intelligence-based.

3.1. Rule-based intrusion detection system (RIDS)

Rehman *et al.* [32] proposed a modern solution using a rule-based methodology that is capable of solving the shortcomings of current approaches for resolving one of the security problems relating to the use of vulnerabilities that occurs in the to DoS attacks. This mechanism has three main components that have been used, namely the rules called (ip6tables) to manage packet filtering at the entrance of the controller machine, the control system, and the address database. The results of the experiment were of improved accuracy and performance through the method used. However, Saad *et al.* [43] proposed a rule-based technique to detect anomaly ICMPv6 patterns. The method comprises of five criteria (rules), predetermined thresholds are defined based on existing values, deemed to be the baseline, to discriminate between irregular and regular behavior. The use of datasets obtained from the National Advanced IPv6 Center (NAv6). The results have shown that the method is capable of detecting ICMPv6 anomalous patterns with a high detection accuracy rate. Table 1 summaries approach of the rules-based.

3.2. Artificial Intelligence-based Intrusion detection system (AIDS)

Which uses AI-techniques to build its detection model, divided into four type mechanism detection.

Table 1. Summary of the existing defense approaches of rules-based

Author/year	Mechanism Proposed	Security Drawbacks
(Rehman and Manickam, 2015) [32]	Does not require any changes in Neighbor Discovery Protocol. A centralized network-based approach. Does not require any patching or installation of additional software. Improved accuracy and performance	The rules used are nothing but normal queries. Uses only one type of attacks (DOS) Process in IPv6 link-local communication only
(Saad *et al*. 2018) [43]	The efficiency of the detection accuracy rate. The false-positive rate is reduced. Detection used real datasets to validate the efficiency obtained from the NAv6 laboratory	Only anomalous behavior traffic is classified as ICMPv6 anomalous behavior traffic. All the parameters are not involved as inputs to generate a new dataset

3.2.1. ICMPv6 data mining-based AIDS

Data mining is a field of study that encompasses both statistics and machine learning, and it is a subfield of computer science that enables intelligent extraction of useful information [44]. Tasks solved using data mining techniques are broadly divided into six categories: cluster analysis, anomaly detection, classification, summarization, regression, and association rule learning [34]. Proposed the DENFIS mechanism in IPv6 networks by [45] to ICMPv6 flood attack detection. ICMPv6 flood attack packet application generates flood packets using different attack rates ranging between 1000 pings to 1500 pings which generate regular traffic packets using different ping rates starting from 10 to 15 pings for each ICMPv6 packet. The fuzzy logic classifier detected ICMPv6 attacks with high accuracy and a smaller number of samples used with unqualified features. In [35] proposed Apriori base algorithm to detect Dos/DDoS attacks. This approach is the first-time has been used to detect router header attacks on the IPv6 network. The IPv6 dataset was used to detect Dos/DDoS attacks. The results high detection accuracy of 72.2% and the same minimum support changed to 0.1. Table 2 summarizes the approaches of anomaly-based data mining methods for attack detection.

Table 2. Summary of the existing defense approaches of data mining

Author/year	Mechanism Proposed	Security Drawbacks
(Saad *et al*. 2014) [45]	ICMPv6 Flood Attack Detection using DENFIS algorithms. Learning-based Artificial Intelligence IDS (Fuzzy Logic). The flooding packets were generated using different attack rates. High accuracy and low Root mean square error of 0.26.	It does not cover all ICMPv6-based DDOS attacks. The dataset of testing is few. The ECOH Request attacks to detect ICMPv6 only. The number of samples is small. Some unqualified features are included.
(Liu and Lai, 2009) [35]	The base Apriori algorithm to detect Dos/DDoS attacks in IPv6. The improved the base Apriori algorithm to detect Dos/DDoS attacks The number of features used in packet traffic was six.	The accuracy rate was low (72.2%). The testing used a small network (four PCs). The features Irrelevant to the attacks.

3.2.2. ICMPv6 machine learning-based AIDS

Machine learning is choice the most suitable classifier is already guided by constraints machine learning that contributes to the rate of Accuracy of the classifier which is the criterion characterizing its performance [46]. Many ICMPv6 machine learning classifiers have been used to detect ICMPv6-DDoS attacks such [47] had used naive bayes algorithm (NBA) to identify the hidden channels in IPv6 networks. This analysis extracted ten traffic characteristics to be used in the classification phase. The real dataset of the researchers was used to test the system for various attacking techniques. The method high accuracy proved about 94.55%. However, the study did not encompass other IPv6 attacks, such as DoS/DDoS. While [4] proposed six classifiers to detection ICMPv6 DDoS attack, the used dataset flow traffic to detect attack was generated in (USM) laboratory included real data and abnormal data have been used to execute RA flood attacks. The Ten features proposed have attained reasonable agog accuracy of detection ranging and alow false-positive rates. Nonetheless, they have poor false-positive detection levels. can be further enhanced the accuracy by changing the classifier parameters. In [48] used seven learning techniques for the ICMPv6-based DDoS attacks detection, creating flow-based datasets based on derived attributes and fixed-time impacts contans Ten attributes. The proposed flow-based method achieved high accuracy ranging between 73.96 to 85.83% and exhibited low false-positive rates (~17 to 30.8%). Elejla *et al.* [24] proposed five classifications for detecting the common IPv6 attacks, particularly ICMPv6-based DDoS attacks. Datasets containing normal and abnormal labelled traffic have been used the experimental results showed that most of the included attacks were identified by classifiers, ranging from 73 per cent to 85 per cent for true positive values.

Other researchers have used machine learning with selection feature (FS) technical to is a process for selecting a subset of significant features by eliminating the irrelevant and unnecessary features from the data set, FS categorized into three types: wrapper, hybrid method, and filter [49]. From researchers used wrapper method for IPv6 network attack detection [50] proposed the particle swarm optimization (PSO) and SVM classifer to detect the RA DoS flood attacks detection. The aim of this model is to a feature selection using IPv6 network attack data was generated using the IPv6 test platform. In the process of determining the best features for detecting IPv6 attacks, the accuracy rate 99.95. However, the RA DoS flood attack detection and the lack of details provided by the dataset. While [51] proposed ant colony optimization algorithm in intrusion detection, wherein the implementation of this approach was simple and of low computational complexity. The findings of the KDD Cup 99 and NSL-KDD intrusion detection test data sets indicate that higher accuracy is obtained when detecting and lowers false positives with a reduced number of features. In addition, A hybrid GA algorithm and SVM intrusion detection system were proposed by [52], the process is a combination algorithm that was used to decrease the number of features from 41 to 10. The features were grouped into three based on GA algorithms. The result shows that hybrid algorithms can achieve a true positive estimate of 0.973 and that the false-positive value was 0.017. In [53] proposed to combine the ant colony algorithm (ACO) with support vector machine classification (SVM), use the proposed algorithm for capabilities search to achieve optimal solutions feature subset to feature search using data set by KDD-CUP99. The results showed to decrease the number of features the use SVM classification network and accuracy and speed to detection. In [54] proposed the anomaly-based ID using a multi-objective grey wolf optimization (GWO) algorithm. The GWO algorithm has been designated as a feature selection NSL–KDD dataset was used to illustrate the usefulness of the approach across multiple attack scenarios. The result shows a high degree of accuracy of the classification method and a decrease in the number of features included in the classification.

Feature selection (filters method) which dataset analyzing and filters unimportant attributes [55]. In [25] proposed an Intelligent ICMPv6 DDoS flood-attack detection system utilizing the back-spread neural network (v6IIDS) in IPv6 networks, using actual datasets collected from the NAv6 laboratory. High efficiency and accuracy of the v6IIDS method demonstrate that the ICMPv6 DDoS flood attack can be identified by the detection accuracy and reducing the time taken to detect the attack. Beside the v6IIDS framework, unable to detect unknown ICMPv6 DDoS flood attack as false-positive ICMPv6 echo rate requires some time flood attack detection. While [56] three phases have been used for the proposed approach which is based on IGR and PCA algorithms to selects the right features with SVM classifier to detection RA flood attacks. The result showed that the solution is effective in detecting RA flood attacks. The decrease in the features has a positive effect and dramatically contributes to the identification of RA flood attacks. Table 3 summarizes the different approaches of anomaly-based by machine learning.

3.2.3. ICMPv6 entropy detection-based AIDS

Entropy detection is a totally new approach through entropy identifies the most significant characteristics of the distribution of network traffic that used to distinguish normal and abnormal network traffic [37]. Several researchers have sought to entropy detection method to detect these attacks such [36] had developed a novel entropy-based strategy called Edmund to detection network attacks. Although complete payload network traffic analysis was not advised due to consumer safety, Edmund used Flow traffic data to detect malicious activities. Flow dataset generated by USM campus the experimental results showed that Edmund was able to detect attacks with an accuracy of approximately 95% on different applications. White [57] proposed a rapid entropy technique, DDoS attacks focused on flow-related network traffic were detected to select a wide variety of attributes from flow data. The research used an adaptive threshold algorithm to define abnormality based on network traffic changes. This technique's detection accuracy rate was good, but the limitation of this detection mechanism was that the experimental investigation was conducted in an IPv4 network environment. In [58] a combination of cumulative sum (CUSUM) algorithm and entropy-based approach was developed for detecting DDoS attacks and achieve high accuracy d by applying signal processing supported by wavelet filtering to the packet header field entropy, the detection performance can be increased. Experimental research had just used an entropy IP source address. The test shows a detection rate as high as 95% and a low false-positive rate. This approach incorporation in the IPv4 network environment. Shah *et al.* [59] proposed a hybrid entropy-based approach combined with an adaptive threshold attack detection algorithm. Ingress packets from the network are captured by a traffic capture engine that stores packets as evaluation datasets, the suggested methodology achieves 98% detection accuracy. But the reliance on many tables that add overloads, and the proposed approach can only detect RA DoS flooding attack in an IPv6 connection local network. Table 4 is under summaries approaches of anomaly-based entropy-based attack detection methods.

Table 3. Summary of the existing defense approaches of classification

Author/year	Mechanism Proposed	Security Drawbacks
(Salih, 2015) [47]	Detect covert channels. Learning-based AIDS (naive bayes). Use ten packet-based features. High accuracy (94.55%).	DoS and DDoS attack are not included. Unqualified features included.
(Elejla *et al.* 2017) [4]	Detection for one of these attacks ICMPv6 protocol Learning-based artificial intelligence IDS (six different classifiers). The dataset was a flow-based representation of the network traffic. The proposed features have achieved an acceptable detection accuracy range.	Have dependency on several tables which add overloads. Depend on packet features which are inappropriate to detect. Need tuning the parameters of the classifier. The database contains only ten features.
(Omar E Elejla *et al.* 2018) [48]	A flow-based IDS to detect ICMPv6 attacks. Learning-based artificial intelligence IDS (seven classifiers) The dataset was a flow-based representation of the network traffic. High accuracy as well as low false-positive rates	Unable to accurately detect the attacks and suffer from high false alarms. Used packet-based representations of the network traffic. Irrelevant feature to the attacks. The database contains only ten features.
(Elejla *et al.* 2019) [24]	Detection ICMPv6-based DDoS attack Learning-based Artificial Intelligence IDS (five) different classifiers. Flow-based datasets which are labeled datasets, detection accuracies were larger than 73.5% with 30% false alarms	Unqualified build models to be implemented. Improvement of the results by optimizing the classification is required. Tune the classifiers' parameters. unqualified features included. Need adopting from other similar attacks features. The database contains only ten features.
(Zulkiflee *et al.* 2015) [50]	Detection IPv6 network attacks include DDOS. Apply the PSO with SVM. Depending on six features in packer capture High accuracy detection	Uncovering all DDoS attacks in IPv6. Shortage details are given about the dataset experiment. unqualified some features include
(Aghdam and Kabiri, 2016) [51]	Anomaly detection-based feature selected technique of ant colony optimization (ACO) with SVM function. The experiment by dataset on the KDD Cup 99 and NSL-KDD Higher accuracy detection and low false alarm with a decreasing number of features	DDoS was not among the attack's detection. The experiments and implements in IPv4 network.
(Rahmani *et al.* 2015) [52]	Anomaly detection based on a hybrid technique of genetic algorithm (GA) with SVM function. The experiment by dataset on the KDD Cup 99. The results reveal a true- positive is 0.973 and false-positive is 0.017.	DDoS was not among the attack's detection. The experiments and implements in IPv4 network.
Xingzhu, 2015) [53]	Anomaly detection based on a hybrid t algorithm (ACO) with SVM function. The experiment by dataset on the KDD Cup 99. The result was improved detection both to accuracy, speed, and reduce features.	DDoS was not among the attack's detection. The experiments and implements in IPv4 network
(Alamiedy *et al.* 2019) [54]	Anomaly detection based on multi-objective grey wolf optimization (GWO) algorithm with SVM function. The experiment by dataset on NSL-KDD. High accuracy with an optimal subset of features	Uncovering DDoS attack. The experiments and implements in IPv4 network. 20% of dataset only was used to show an experiment result.
(Saad *et al.* 2016) [25]	Anomaly detection ICMPv6 DDoS flooding-attack detection. Utilizing IGR and PCA algorithms. Real datasets obtained from a NAv6 laboratory. High performance and accuracy detection.	Detection ICMPv6 ECOH Request only. Shortage details are given about the dataset experiment.
(Anbar *et al.* 2018) [56]	Anomaly detections detect RA Flooding Attacks in ICMPv6. Utilizing IGR and PCA algorithms. A real dataset obtained from the National Advanced IPv6 Center. High accuracy of attack detections	Need for increasing the detection using more efficient training algorithms. Use another algorithm to reduction impact dimensionality.

3.2.4. ICMPv6 deep learning detection based AIDS

Deep learning is a new science in machine learning that recently developed due to the development of GPU acceleration technology utilizing artificial intelligence that allows the computer to imitate human behavior [38], [39]. Niyaz *et al.* [40] proposed a designing NIDS that is both effective and flexible. A self-taught learning (STL), a deep learning technique, on NSL-KDD-a benchmark data set including (DoS/DDoS) network intrusion attacks is currently being explored. The implemented NIDS performed very well compared to the earlier NIDS system used for normal/anomaly detection when evaluated on the test

data. While [60] applied Approach for the identification of flow-based anomaly in an SDN environment. We build a deep neural network (DNN) model for an intrusion detection system and train the NSL-KDD dataset model, which contains DoS attacks. The inferences confirmed that a deep learning approach has a high potential to be used for flow-based anomaly detection. In addition, [61] proposed a novel technique for detecting intrusions utilizing recurrent neural networks (RNN-IDS) which the model's success in binary classification and multiclass classification in the test used data set that included DoS attack detection. The proposed approach has the ability to detect intrusion also delivers good performance in both binary and multiclass classification systems. In response to ever-changing network attacks. However [62] proposed the anomaly detection using a deep neural network (DNN). The DNN algorithm was implemented to refined data to create a learning model, and the entire KDD Cup 99 dataset was utilized to test it. Overall, the proposed approach delivers good accuracy results. In a study by [63] proposed a framework used a series of a deep network to detect the abnormal in network traffic. A framework used the NSL-KDD dataset to detection attack. Overall, the framework has 87.2% accurate compared with the SIDS-based signature approach, with higher accuracy rates for the proposed model than the SIDS-based signature approach. Table 5 Summaries different approaches of anomaly-based deep learning for attack detections.

Table 4. Summary of the existing defense approaches of entropy method

Author/year	Mechanism Proposed	Security Drawbacks
(David and Thomas, 2015) [57]	The fast entropy method based on the flow-based analysis to detect the DDoS attack in (SDN). The carried out on a subset of dataset (CAIDA). the high accuracy detection result.	The experiments and implements in IPv4 network.
(Özçelik and Brooks, 2016) [58]	Anomaly detection based on entropy cumulative sum (Cusum) for DDoS attack detection. The tested using operational network traffic and performing DDoS attacks. The result High detection and low false-positive rates.	The experiments and implements in IPv4 network.
(Haghighat and Li, 2018) [36]	Anomaly detection based on a novel entropy and mitigation (EDMund) to detection DDoS attacks. Used two different Net Flow data dataset. The results show a high accuracy attack detection.	The analyzed was not the whole network traffic including and payload packet headers. The experiments and implements in IPv4 network.
(Shah *et al.* 2019) [59]	Proposed hybrid detection technique detects RA DoS flooding attack. Learning-based artificial intelligence IDS (adaptive threshold algorithm). Dataset used captured by the traffic capture engine. Technique yields 98% detection accuracy	Detects RA DoS flooding attack only. Non-inclusion of more attack scenarios. Non-qualified features included. Shortage details are given about the dataset experiment.

Table 5. Summary of the existing defense approaches of deep learning method

Author/year	Mechanism Proposed	Security Drawbacks
(Quamar Niyaz *et al.* 2016) [40]	Anomaly detection based deep learning by multi-vector to DDoS detection. Applying the approach to traffic traces collected from various scenarios. The result showed high accuracy detection and a low false-positive	The experiments and implements in IPv4 network. The approach has a few limitations in terms of processing capabilities.
(Tang *et al.* 2016) [60]	Anomaly detection based Deep learning using Neural Network (DNN) model. The experimental by dataset on the NSL- KDD. The accuracy detection in the DNN model (75.75)	DDoS was not among the attack's detection. The experiments and implements in IPv4 network. Only Six features used to detect.
(Yin *et al.* 2017) [61]	Anomaly detection based deep learning using recurrent neural networks (RNN-IDS). The experimental by dataset on the NSL- KDD. The result shows high detection (97.09%)	DDoS was not among the attack's detection. The experiments and implements in IPv4 network.
(Kim *et al.* 2017) [62]	Anomaly detection using a deep neural network (DNN) The experiment by dataset on the KDD Cup 99. The detection rate was high accuracy	DDoS was not among the attack's detection. The experiments and implements in IPv4 network
Gurung *et al.* 2019) [63]	Anomaly detection based deep learning using sparse auto-encoder with logistic regression. The experimental by dataset on the NSL- KDD. Higher accuracy rate, and also decreases the chances of False Positives and Negatives.	DDoS was not among the attack's detection. The experiments and implements in IPv4 network

4. EVALUATION MEASURES FOR ICMPV6-DDoS ATTACKS USING ANOMALY DETECTION

In this section, the evaluation measures for detecting ICMPv6-DDoS attacks used with anomaly detection are reviewed. Figure 6 presents the evaluation measures used to evaluate ICMPv6-DDoS attacks used with anomaly detection. Observed there is more than one for the state-of-the-art procedure, used in the most recent research. Which the accuracy rate are the criteria of major evaluation most researchers use. While taking ranks second the false positive rate. Figure 7 presents the classifiers utilized for evaluation of Anomaly detection for ICMPv6-DDoS attacks that the main technique used is the SVM classifiers by many researchers in detecting ICMPv6-DDoS attacks. While taking the naive bayes classifier ranks second and third in the random forest classifier based on the percentage of these classifiers utilized in the research papers.

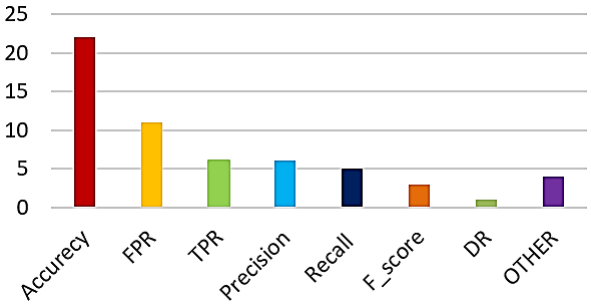

Figure 6. Evaluation measures of ICMPV6-DDoS attack anomaly detection

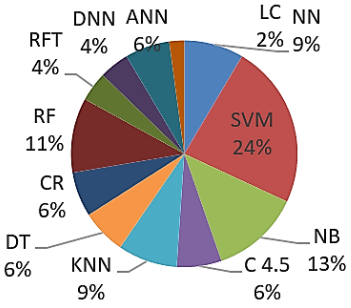

Figure 7. The percentage of anomaly detection for ICMPv6-DDoS attack

5. CONCLUSION

In this paper, a comprehensive review is performed to study the anomaly detection approach used in detecting ICMPv6-DDoS attacks. The prime purpose of this article is to previous studies was summarize and their applied applications for detecting ICMPv6-DDoS attacks. The reviewed studies were chosen from many public and good research databases such as Springer, IEEE, Elsevier, and IAES journals. These sheets selection goes through many filters for removing the related content duplicate ideas for ICMPv6-DDoS attack detection using anomaly detection approach.

In general, the studies related was summarized in detecting ICMPv6-DDoS attacks are analyzed and discussed based on anomaly detection approaches, that classified into two classes: Rule-based detection and AI-based detection. Moreover, AI-based detection studies related are categorized into machine learning, data mining, entropy, deep learning, and optimization with machine learning. All of the studies were summarized either used for detection the ICMPv6-DDoS attacks means of analyzing the detection approaches. Moreover, several studies utilize either machine learning, deep learning, data mining or entropy detection to detection ICMPv6-DDoS attack. In overall, SVM, NVB, KNN, RF, C4.8, RFT, K-means, and DT as a machine learning algorithm, NN, DNN, NNN, and LC as a deep learning algorithm, Fuzzy logic and Apriori Algorithm as data mining and threshold, cumulative, EDMund and Cusum as entropy detection are used for detection ICMPv6-DDoS attack. In conclusion, for detection ICMPv6-DDoS attack, SVM is the most suitable machine learning mechanism and NN is the most suitable deep learning mechanism.

In this review paper, the most recent and public ICPMv6-DDoS attack datasets used by other researchers to evaluate and compare their methods are reported and their accessibility is provided in Tables 1 to 5. The evaluation measurements used to detect ICPMv6-DDoS attacks-based anomaly detection is summarized. In conclusion, the accuracy, false-positive rate and precision are the most widely used measurements in the previous studies. This is in line with the previous studies using anomaly detection approaches for the detection process. With respect to the previous anomaly detection approaches related ICPMv6-DDoS attack studies, this review paper can be considered as a rich resource that inspires the future studies to turn their attentions to study the ICPMv6-DDoS Attack concerns in different perspectives such as: i) Unknown attacks: Anomaly detection approaches shall be tweaked to ICPMv6-DDoS attack unknown with constraints related by using other algorithms, ii) Monitoring the network: Anomaly detection approaches can be used to monitor and observe the effects of ICPMv6-DDoS attacks, iii) Real-time systems: The researchers shall build a real-time system using anomaly detection approaches to detection ICPMv6-DDoS attacks.

Other anomaly detection approaches for ICPMv6-DDoS Attacks detection. Recently, there is a plethora of efficient anomaly detection approaches are proposed. The reinforcement anomaly can be used to improve machine learning, deep learning, data mining and Entropy detection with the optimization algorithms to improve their efficiency.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM) for providing necessary facilities and support. The funding for this research was provided by Universiti Sains Malaysia (USM) and Iraq Airways Company (IA).

REFERENCES

[1] R. U. and S. S. Agarwal, P., P. Yadav, N. Sharma, "Network security is a key for internet users: a perspective Pooja," *Indian J. Eng.*, vol. 1, no. 1, pp. 28–36, 2012.

[2] M. Tahir, M. Li, N. Ayoub, U. Shehzaib, and A. Wagan, "A Novel DDoS Floods Detection and Testing Approaches for Network Traffic based on Linux Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 2, pp. 341–357, 2018, doi: 10.14569/IJACSA.2018.090248.

[3] O. Brun, Y. Yin, E. Gelenbe, Y. M. Kadioglu, J. Augusto-Gonzalez, and M. Ramos, "Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments," *Commun. Comput. Inf. Sci.*, vol. 821, no. January, pp. 79–89, 2018.

[4] O. E. Elejla, B. Belaton, M. Anbar, and I. M. Smadi, "A New Set of Features for Detecting Router Advertisement Flooding Attacks," in *Proceedings - 2017 Palestinian International Conference on Information and Communication Technology, PICICT 2017*, 2017, pp. 1–5, doi: 10.1109/PICICT.2017.19.

[5] C. E. Caicedo, J. B. D. Joshi, and S. R. Tuladhar, "IPv6 security challenges," *Computer (Long. Beach. Calif).*, vol. 42, no. 2, pp. 36–42, 2009, doi: 10.1109/MC.2009.54.

[6] I. S. Alsukayti, "The support of multipath routing in IPv6-based internet of things," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 2, pp. 2208–2220, 2020, doi: 10.11591/ijece.v10i2.pp2208-2220.

[7] R. M. A. Saad, S. Manickam, E. Alomari, M. Anbar, and P. Singh, "Design and deployment of testbed based on ICMPv6 flooding attack," *Journal of Theoretical and Applied Information Technology*, vol. 64, no. 3, pp. 795–801, 2014.

[8] J. L. Shah and J. Parvez, "Optimizing Security and Address Configuration in IPv6 SLAAC," *Procedia Comput. Sci.*, vol. 54, pp. 177–185, 2015, doi: 10.1016/j.procs.2015.06.020.

[9] "Ipv6, Google," 2021. [Online], Available: https://www.google.com/intl/id/ipv6/statistics.html.

[10] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," 2007. [Online], Avaible: https://datatracker.ietf.org/doc/html/rfc4861.

[11] A. Conta, S. Deering, and M. Gupta, "Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification," 2006. [Online], Available: https://datatracker.ietf.org/doc/html/rfc4443.

[12] E. Durdağı and A. Buldu, "IPV4/IPV6 security and threat comparisons," *Procedia - Soc. Behav. Sci.*, vol. 2, no. 2, pp. 5285–5291, Jan. 2010, doi: 10.1016/j.sbspro.2010.03.862.

[13] O. E. Elejla, B. Belaton, M. Anbar, and A. Alnajjar, "Intrusion Detection Systems of ICMPv6-based DDoS attacks," *Neural Comput. Appl.*, vol. 30, no. 1, pp. 1–12, 2016, doi: 10.1007/s00521-016-2812-8.

[14] J. Postel, "'Internet protocol,' Internet Eng. Task Force." 1981.

[15] S. E. Frankel, R. Graveman, J. Pearce, and M. Rooks, "Guidelines for the secure deployment of IPv6," *Special Publication (NIST SP), National Institute of Standards and Technology*, Gaithersburg, MD, 2010. [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=907211.

[16] A. Rosli, A. M. Taib, W. N. A. Wan Ali, and R. S. Hamid, "Application of Grounded Theory in Determining Required Elements for IPv6 Risk Assessment Equation," in *MATEC Web of Conferences*, 2018, vol. 150, doi: 10.1051/matecconf/201815006005.

[17] S. Deering, W. Fenner, and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6," 1999. [Online]. Available: https://www.ietf.org/rfc/rfc2710.txt.

[18] E. Hogg, S.; Vyncke, "IPv6 SECURITY," 2008.

[19] M. A. Naagas, E. L. Mique, T. D. Palaoag, and J. S. D. Cruz, "Defense-through-deception network security model: Securing university campus network from DOS/DDOS attack," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 7, no. 4, pp. 593–600, 2018, doi: 10.11591/eei.v7i4.1349.

[20] A. Fadlil, I. Riadi, and S. Aji, "Review of detection DDOS attack detection using naive bayes classifier for network forensics," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 6, no. 2. pp. 140–148, 2017, doi: 10.11591/eei.v6i2.605.

[21] N. Hoque, M. H. Bhuyan, R. C. Baishya, D. K. Bhattacharyya, and J. K. Kalita, "Network attacks: Taxonomy, tools and systems," *Journal of Network and Computer Applications*, vol. 40, pp. 307–324, 2014, doi: 10.1016/j.jnca.2013.08.001.

[22] A. H. Bdair, R. Abdullah, S. Manickam, and A. K. Al-Ani, "Brief of Intrusion Detection Systems in Detecting ICMPv6 Attacks," *Computational Science and Technology*, pp. 199–213, 2020, doi: 10.1007/978-981-15-0058-9_20.

[23] H. Pan, E. Hou, and N. Ansari, "M-NOTE: A Multi-part ballot based E-voting system with clash attack protection," in *IEEE International Conference on Communications*, 2015, vol. 2015, pp. 7433–7437, doi: 10.1109/ICC.2015.7249514.
[24] O. E. Elejla, B. Belaton, M. Anbar, B. Alabsi, and A. K. Al-ani, "Comparison of Classification Algorithms on ICMPv6- Based DDoS Attacks Detection," *Computational Science and Technology, Lecture Notesin Electrical Engineering*, vol. 481, pp. 347–357, 2019, doi: 10.1007/978-981-13-2622-6_34.
[25] R. M. A. Saad, M. Anbar, S. Manickam, and E. Alomari, "An intelligent ICMPv6 DDoS flooding-attack detection framework (V6IIDS) using back-propagation neural network," *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 33, no. 3, pp. 244–255, 2016, doi: 10.1080/02564602.2015.1098576.
[26] D. Arivudainambi and K. A. V. Kumar, "Performance analysis of security framework for software defined network architectures," *Int. J. Adv. Appl. Sci.*, vol. 8, no. 3, pp. 232–242, 2019, doi: 10.11591/ijaas.v8.i3.pp232-242.
[27] O. Elejla, B. Belaton, M. Anbar, and A. Alnajjar, "A Reference Dataset for ICMPv6 Flooding Attacks," *Journal of Engineering and Applied Sciences*, vol. 11, no. 3, pp. 476–481, 2016, doi: 10.36478/jeasci.2016.476.481.
[28] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, 2004, doi: 10.1145/997150.997156.
[29] M. Rezvani, "Assessment Methodology for Anomaly-Based Intrusion Detection in Cloud Computing," *Journal of AI and Data Mining*, vol. 6, no. 2, pp. 387–397, 2018, doi: 10.22044/JADM.2017.5581.1668.
[30] W. Li, W. Meng, and L. F. Kwok, "Investigating the influence of special on-off attacks on challenge-based collaborative intrusion detection networks," *Futur. Internet*, vol. 10, no. 1, pp. 1–16, 2018, doi: 10.3390/fi10010006.
[31] H. Pan, E. Hou, N. Ansari, "RE-NOTE: An E-voting scheme based on ring signature and clash attack protection," *GLOBECOM-IEEE Glob. Telecommun. Conf.*, 2013, pp. 867–871, doi: 10.1109/GLOCOM.2013.6831182.
[32] S. U. Rehman and S. Manickam, "Rule-based mechanism to detect Denial of Service (DoS) attacks on Duplicate Address Detection process in IPv6 link local communication," in *2015 4th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2015*, 2015 pp. 1–6, doi: 10.1109/ICRITO.2015.7359243.
[33] M. Manninen, "Using Artificial Intelligence in Intrusion Detection Systems," Helsinki Univ. Technol., vol. 13, 2002, Art. no. 6.
[34] A. M. Farayola, A. N. Hasan, and A. Ali, "Optimization of PV Systems Using Data Mining and Regression Learner MPPT Techniques Comparative Study of MPPT charge controllers on a non-isolated DC-DC converter View project epistmology of economics View project Optimization of PV Systems Using Data Min," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 10, no. 3, pp. 1080–1089, 2018, doi: 10.11591/ijeecs.v10.i3.pp1080-1089.
[35] Z. Liu and Y. Lai, "A data mining framework for building intrusion detection models based on IPv6," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2009, vol. 5576 LNCS, pp. 608–618, doi: 10.1007/978-3-642-02617-1_62.
[36] M. H. Haghighat and J. Li, "EDMund: Entropy based attack detection and mitigation engine using netflow data," *ACM Int. Conf. Proceeding Ser.*, pp. 107–111, 2018, doi: 10.1145/3290480.3290484.
[37] M. F. Umer, M. Sher, and Y. Bi, "Flow-based intrusion detection: Techniques and challenges," *Comput. Secur.*, vol. 70, pp. 238–254, 2017, doi: 10.1016/j.cose.2017.05.009.
[38] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, 2018, doi: 10.1109/TETCI.2017.2772792.
[39] I. B. K. Sudiatmika, F. Rahman, Trisno, and Suyoto, "Image forgery detection using error level analysis and deep learning," *TELKOMNIKA Telecommunication Comput. Electron. Control*, vol. 17, no. 2, pp. 653–659, 2019, doi: 10.12928/telkomnika.v17i2.8976.
[40] Q. Niyaz, W. Sun, A. Y. Javaid, and M. Alam, "A deep learning approach for network intrusion detection system," *EAI Int. Conf. Bio-inspired Inf. Commun. Technol.*, 2015, doi: 10.4108/eai.3-12-2015.2262516.
[41] J. P. Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han, and L. Shu, "Policy and Network-based Intrusion Detection System for IPv6-enabled Wireless Sensor Networks," *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 1796–1801, doi: 10.1109/ICC.2014.6883583.
[42] S. C. Poh, Y. F. Tan, S. N. Cheong, C. P. Ooi, and W. H. Tan, "Anomaly detection on in-home activities data based on time interval," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 15, no. 2, pp. 778–785, 2019, doi: 10.11591/ijeecs.v15.i2.pp778-785.
[43] R. M. A. Saad, M. Anbar, and S. Manickam, "Rule-based detection technique for ICMPv6 anomalous behaviour," *Neural Comput. Appl.*, vol. 30, no. 12, pp. 3815–3824, 2018, doi: 10.1007/s00521-017-2967-y.
[44] A. I. Adekitan, A. Adewale, and A. Olaitan, "Determining the operational status of a three phase induction motor using a predictive data mining model," *international journal of power electronics and drive systems (IJPEDS)*, vol. 10, no. 1, pp. 93–103, 2019, doi: 10.11591/ijpeds.v10.i1.pp93-103.
[45] R. M. A. Saad, A. Almomani, A. Altaher, B. B. Gupta, and S. Manickam, "ICMPv6 flood attack detection using DENFIS algorithms," *Indian J. Sci. Technol.*, vol. 7, no. 2, pp. 168–173, 2014, doi: 10.17485/ijst/2014/v7i2.5.
[46] N. Settouti, M. E. A. Bechar, and M. A. Chikh, "Statistical Comparisons of the Top 10 Algorithms in Data Mining for Classi cation Task," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 4, no. 1, pp. 46–51, 2016, doi: 10.9781/ijimai.2016.419.
[47] A. Salih, X. Ma, and E. Peytchev, "Detection and Classification of Covert Channels in IPv6 Using Enhanced Machine Learning," *Proc. of The International Conference on Computer Technology and Information Systems*, 2015, doi: 07. ICCTIS.2015.1.1.

[48] O. E. O. Elejla, "Flow-Representation Approach For ICMPV6-Based Ddos Attacks Detection," 2018. [Online]. Available: http://eprints.usm.my/43724/1/OMAR%20E.%20O.%20ELEJLA.pdf.
[49] T. A. Alamiedy, M. Anbar, A. K. Al-Ani, B. N. Al-Tamimi, and N. Faleh, "Review on Feature Selection Algorithms for Anomaly-Based Intrusion Detection System," *International Conference of Reliable Information and Communication Technology*, 2018, doi: 10.1007/978-3-319-99007-1_57.
[50] M. Zulkiflee, M. S. Azmi, S. S. S. Ahmad, S. Sahib, and M. Ghani, "A framework of features selection for ipv6 network attacks detection," *WSEAS Trans Commun*, vol. 14, no. 46, pp. 399–408, 2015.
[51] M. H. Aghdam and P. Kabiri, "Feature Selection for Intrusion Detection System Using Ant Colony Optimization," *International Journal of Network Security*, vol. 18, no. 3, pp. 420–432, May 2016.
[52] B. M. Aslahi-Shahri *et al.*, "A hybrid method consisting of GA and SVM for intrusion detection system Cloud Computing View project a View project A hybrid method consisting of GA and SVM for intrusion detection system," *Neural Comput and Applic*, 2015, doi: 10.1007/s00521-015-1964-2.
[53] W. Xingzhu, "ACO and SVM Selection Feature Weighting of Network Intrusion Detection Method," *Int. J. Secur. Its Appl.*, vol. 9, no. 4, pp. 129–270, 2015, doi: 10.14257/ijsia.2015.9.4.24.
[54] T. A. Alamiedy, M. Anbar, Z. N. M. Alqattan, and Q. M. Alzubi, "Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, pp. 3735–3756, Nov. 2019, doi: 10.1007/s12652-019-01569-8.
[55] S. Binitha and S. S. Sathya, "A survey of bio inspired optimization algorithms," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, no. 2, pp. 137 - 151, 2012.
[56] M. Anbar, R. Abdullah, B. N. Al-Tamimi, and A. Hussain, "A Machine Learning Approach to Detect Router Advertisement Flooding Attacks in Next-Generation IPv6 Networks," *Cognit. Comput.*, vol. 10, no. 2, pp. 201–214, Apr. 2018, doi: 10.1007/s12559-017-9519-8.
[57] J. David and C. Thomas, "DDoS attack detection using fast entropy approach on flow-based network traffic," *Procedia Comput. Sci.*, vol. 50, pp. 30–36, 2015, doi: 10.1016/j.procs.2015.04.007.
[58] I. Özçelik and R. R. Brooks, "Cusum - Entropy: An efficient method for DDoS attack detection," in *4th International Istanbul Smart Grid Congress and Fair, ICSG 2016*, 2016, pp. 1–5, doi: 10.1109/SGCF.2016.7492429.
[59] S. B. I. Shah, M. Anbar, A. Al-Ani, and A. K. Al-Ani, "Hybridizing entropy based mechanism with adaptive threshold algorithm to detect RA flooding attack in IPv6 networks," *Lect. Notes Electr. Eng.*, vol. 481, pp. 315–323, 2019, doi: 10.1007/978-981-13-2622-6_31.
[60] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," *Proc. - 2016 Int. Conf. Wirel. Networks Mob. Commun. WINCOM 2016 Green Commun. Netw.*, 2016, pp. 258–263, doi: 10.1109/WINCOM.2016.7777224.
[61] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.
[62] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of Intrusion Detection using Deep Neural Network," *2017 IEEE International Conference on Big Data and Smart Computing (BigComp)*, 2017, pp. 313–316, doi: 10.1109/BIGCOMP.2017.7881684.
[63] S. Gurung, M. Kanti Ghose, and A. Subedi, "Deep Learning Approach on Network Intrusion Detection System using NSL-KDD Dataset," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 3, pp. 8–14, 2019, doi: 10.5815/ijcnis.2019.03.02.