IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 5, 2021, accepted March 11, 2021, date of publication March 17, 2021, date of current version March 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3066630

Flow-Based Approach to Detect Abnormal Behavior in Neighbor Discovery Protocol (NDP)

ABDULLAH AHMED BAHASHWAN[1], MOHAMMED ANBAR[1], (Member, IEEE), IZNAN HUSAINY HASBULLAH[1], ZIYAD R. ALASHHAB[1], AND ALI BIN-SALEM[2]

[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang 11800, Malaysia
[2]School of Computer Science, Neijiang Normal University, Neijiang 641100, China

Corresponding author: Mohammed Anbar (anbar@usm.my)

This work was supported by the Research University (RU) Grant, Universiti Sains Malaysia (USM), under Grant 1001. PNAV.8011107.

ABSTRACT Internet Protocol version six (IPv6) is equipped with new protocols, such as the Neighbor Discovery Protocol (NDP). NDP is a stateless protocol without authentication that makes it vulnerable to many types of attacks, such as Router Advertisement (RA) and Neighbour Solicitation (NS) DoS flooding attacks. In these types of attacks, attackers send an enormous volume of abnormal NDP traffic, which causes congestion that degrades network performance. The expected behavior among these attacks is the existence of NDP traffic abnormalities. Thus, this research aims to propose a flow-based approach to detect abnormal NDP traffic behavior, which is considered an indicator of the presence of NDP-based attacks, such as RA and NS DoS flooding attacks. Also, the proposed approach relies on flow-based network traffic representation and adoption of the Entropy algorithm to detect the randomness in the network traffic. The proposed approach is evaluated in terms of detection accuracy, precision, recall, and F1-Score using a simulated dataset. The experimental result shows that the proposed approach obtained 98.1%, 55%, 100%, and 70.96% for average accuracy, precision, recall, and F1-Score, respectively, in detecting abnormal NDP traffic behavior caused by the RA DoS flooding attack. Meanwhile, the proposed approach obtained 99%, 91.3%, 100%, and 95.45% for average accuracy, precision, recall, and F1-Score, respectively, in detecting the abnormal NDP traffic behavior caused by the NS DoS flooding attack. Also, the proposed approach shows better results compared to other existing approaches.

INDEX TERMS Intrusion detection systems (IDS), NDP traffic abnormalities, RA DoS flooding attack, NS DoS flooding attack, network traffic representation, entropy algorithm, rule-based technique.

I. INTRODUCTION

The explosive growth of internet users led to the exhaustion of Internet Protocol version 4 (IPv4) addresses [1]. The main reason for the address shortage is the rise of many technologies, such as the Internet of Things (IoT), cloud computing [2], and wireless technology applications [2]–[4]. To overcome the exhaustion of the IPv4 addresses, Internet Protocol version 6 (IPv6) was introduced as the next-generation Internet Protocol (IP) and considered the successor of IPv4 [5], [6]. In January 2021, Google's IPv6 adoption statistics indicated that over 32.72% of its users connected to Google's services over IPv6 connectivity [7].

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

Several new protocols have been introduced into IPv6, such as Internet Control Message Protocol (ICMPv6) and Neighbor Discovery Protocol (NDP). The NDP protocol works on top of the ICMPv6 protocol to discover IPv6 nodes in the link-local network [8]. In addition to other functionalities, NDP protocol reserves five information messages from ICMPv6 informational messages [9], [10], which are listed as follows:

- Router Solicitation (RS) - type 133: IPv6 hosts inquire with RS messages to locate routers on the link-local network. Any routers in the network not addressed directly in the RS message generate RA immediately upon receipt of this message, rather than at their next scheduled time.
- Router Advertisement (RA) - type 134: RA messages are sent by routers periodically or in response to RS

requests. Routers use RA messages to inform others about their existence on the network and send system parameters, such as the Maximum Transmission Unit (MTU), Network Prefix, hop limits, etc.

- Neighbor Solicitation (NS) - type 135: IPv6 nodes use NS messages to determine the link-layer addresses of a neighbor, or in Duplicate Address Detection (DAD) process to verify the address uniqueness or to verify a neighbor's reachability status.
- Neighbor Advertisement (NA) - type 136: NA messages contain information about any changes in nodes' information, such as Media Access Control (MAC) address and the IP address, or it can be used to ask for a response to NS messages.
- Redirect Messages (RM) - type 137: RM messages forward traffic from one router to another [11]–[13].

NDP is a stateless protocol that does not force the use of authentication mechanisms, which exposes NDP messages to several threats and vulnerabilities [14]. Moreover, the NDP protocol allows any node in the IPv6 network to generate their IP addresses and initiate unauthenticated communications with one another within the network [15], [16]. Consequently, the NDP protocol comes with a standard security mechanism called Secure Neighbor Discovery (SEND). SEND uses Cryptographically Generated Addresses (CGA), a digital signature, and an X.509 certification to secure the NDP protocol [17], [18].

The purpose of SEND is to provide integrity to NDP messages, prevent IPv6 address spoofing, and offer a perfect way to verify routers' authority. Unfortunately, SEND does not work well as expected, and it is vulnerable to Denial of Service (DoS) attack [19]. DoS attack is considered as one of the most damaging attacks on IPv6 link-local network [20]. Thus, SEND does not fulfill the requirements to secure the NDP protocol [21].

This paper has three contributions: (i) the construction of a flow that represents NDP traffic. The constructed flow contributes to detecting the NDP traffic abnormalities, which are resulted in the presence of RA or NS DoS flooding attacks. (ii) The adoption of an Entropy-based algorithm to detect NDP traffic abnormalities based on a configurable threshold. (iii) A rule-based technique to detect NDP traffic abnormalities caused by RA or NS DoS flooding attacks.

The rest of this paper is organized as follows. Section II presents the background of abnormal NDP traffic caused by RA and NS DoS flooding attacks. Also, this section covers the network traffic representation and the Entropy-based approach (EBA). Section III discusses the literature review. Section IV underlines the proposed approach. Section V relays the design and work-flow of the proposed approach. Section VI presents the implementation and setup of the proposed approach. Section VII elaborates and discusses the experiment results and discussions. Finally, Section VIII presents the conclusion of this paper.

II. BACKGROUND

This section underlines the NDP traffic abnormalities, which are considered clues for detecting RA and NS DoS flooding attacks. This section also explains the network traffic representation thoroughly. Finally, this section discusses the Entropy-based approach (EBA).

A. RA DoS FLOODING ATTACK

Router Advertisement (RA) message is one of the key messages used by the NDP to perform many tasks, such as autoconfiguration. Routers also use RA to inform other routers about their existence on the network. Further, the RA message offers assistance to hosts in the link-local network by providing them with network prefix information and other information that may assist them in generating their IPv6 addresses dynamically [22], [23].

Moreover, several ways for attackers to execute RA DoS flooding attacks, for example, by forcing the default gateway to continuously send RA messages every 200 seconds to the (FF02::1) multicast group. The DoS attempt works because every node on the same link-local re-configures its routing table and default getaway accordingly. From the above scenario, attackers could also act as a fake default router to flood the network with spoofed RA messages to continuously force the nodes to update their routing tables and default getaways.

Another way for the RA DoS flooding attack to occur is by forcing the default router to send RA messages in response to RS messages that the attacker sent to the (FF02:2) multicast group. The default router in the network listens and responds with an RA message to (FF02:1) multicast group. Attackers take advantage of this situation by pretending to be the default gateway router and flood the network with spoofed RA messages, including invalid network prefix values [24]. Figure 1 presents RA and RS messages exchange between the nodes in a link-local network.

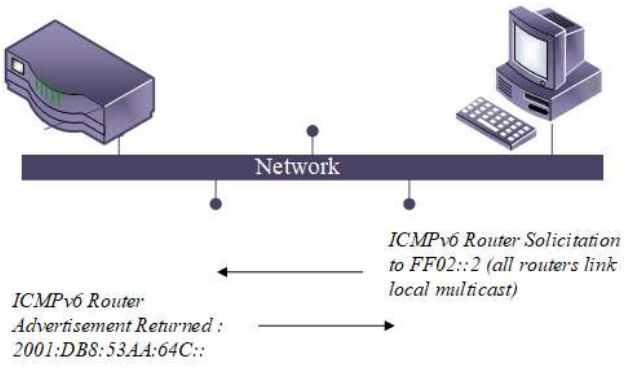

FIGURE 1. Illustrating the Stateless Address Autoconfiguration (SLAAC).

B. NS DoS FLOODING ATTACK

Neighbor Solicitation (NS) is an ICMPv6 information message with code 135. NS message is used for DAD to verify the uniqueness of an IP address [25]. A newly joined node initiates NS to start the autoconfiguration process after gen-

erating a link-local address for the interface. Then, the node must ensure that the address is not already being used by other nodes on the same link-local network. A node uses the NS message to verify the uniqueness of the address. Any node that is already using the address will reply to the NS message with an NA message to indicate that the address is taken. However, in the case where there is no response, the node will keep sending the NS message until it obtains a unique address and assigns it to the interface [26], [27].

Additionally, the NS message is also being used to determine the link-layer address of neighbors on the same link-local network. Any nodes in the IPv6 network can send NS messages at any time to request a link-layer address of a target node on the same link-local network. Concurrently, the sending node works on address resolution, and the NS message is sent via multicast to the Solicited Node Multicast Address (SNMA) of the target node [28]. When the target node receives the NS message, it immediately updates its neighbor cache table and replies with the NA message [29], [30]. Figure 2 illustrates NA and NS message exchanges between hosts in a link-local network.

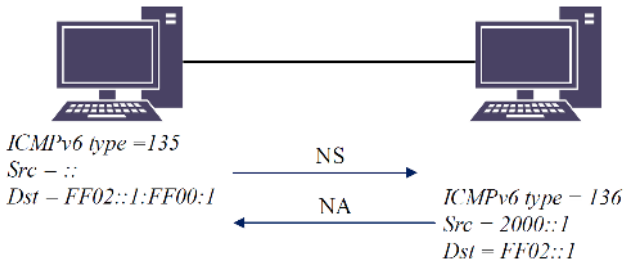

FIGURE 2. NA and NS messages exchange between hosts.

The NS DoS flooding attacks happen when a victim node is forced to create fake entries that map IPv6 addresses with their corresponding MAC addresses in the neighbor cache table of the victim nodes. Consequently, the kernel memory would be exhausted because the size of the neighbor cache table is limited. Thus, the victim nodes will be unavailable. Since the NS messages are sent to the FF02::1 multicast group, all nodes on the same link-local network will receive the messages and update their neighbor caches table accordingly [27].

C. NETWORK TRAFFIC REPRESENTATION

In recent years, networks' growth grew significantly. Thus, security analysis techniques must accommodate the exponential increase in network throughput accordingly. Intrusion detection systems (IDS) are categorized into two categories: host-based IDS and network-based IDS (NIDS), which will be underlined in this research. NIDS are more suited in high-speed network infrastructure, and it is typically used to check network traffic for illegitimate and malicious packets. There are two types of NIDS characterized by the kind of network traffic representation used, either packet-based or flow-based [31], [32], which will be discussed in the following subsections.

1) PACKET-BASED NETWORK TRAFFIC

Packet-based network traffic is the traditional method of network traffic representation. The monitoring devices capture all inbound and outbound network traffic (including payload and header) without filtration and packet loss. The monitoring devices capture the packets as representing the actual network traffic [33]. The most common network traffic capturing software is TCP-Dump [34] and WireShark [35], which are typically placed at the edge point of the network.

One of the benefits of packet-based representation is having complete details of every packet, including its headers and payloads. Also, the detection system could perform deep packet-inspections. However, the number of network traffic details creates an extensive dataset, especially in today's high-speed networks. Consequently, detection systems that use a packet-based approach must process and analyze enormous network traffic data, which adds complexity. Finally, the packet-based representation could reveal sensitive or confidential information from the network packets. Thus, based on the limitations of packet-based traffic representation, it could be stated that packet-based representation is not suited for high-speed networks [36]. Table 1 summarizes the two types of network traffic representation's strengths and weaknesses.

2) FLOW-BASED NETWORK TRAFFIC

The flow-based is an advanced method in network traffic representation, defined in RFC3917 [37]. It is a set of IP packets that pass through a checkpoint during a specific time interval [38]. The IP flow comprises several packets that share common features. Generally, IPv4 traffic flows are formatted by five common features: source IPv4 address, Destination IPv4 address, source port number, destination port number, and protocol type [39], which is not suitable to represent NDP traffic flow as NDP message does not have source and destination port numbers. Therefore, there is a need to identify the tuples to represent NDP traffic flow (i.e., IPv6 source, IPv6 destination, NDP message types, and network prefix), not just for the purpose of this research but also for the research community at large.

Furthermore, flow-based traffic representation presents remarkable advantages, such as (i) creates a small size dataset of network traffic, (ii) less computation complexity compared to packet-based IDS to analyze the same network traffic, (iii) discards the content of the packets and focus on header information, (iv) suitable for high-speed networks and preferred to be used for securing networks. Besides that, many current research works, such as [15], [33], [36], [40], [41], have proved that flow-based IDS outperforms packet-based IDS. Overall, based on both traffic representations' advantages and disadvantages in Table 1, the flow-based IDS is superior in detecting NDP traffic abnormalities.

TABLE 1. Flow-based NID vs Packet-Based NID [33], [36].

Flow-based NIDS	Packet-based NIDS
Advantages	
The flow-based NIDS does not inspect the payload.	Inspect the header and payload.
Fewer privacy issues.	The data is immediately presented at NIDS, which means no delay.
It is efficient for high-speed networks.	
Lightweight flow-based NIDS.	
Disadvantages	
There will be limited data without filtration.	Process all the network packets without filtration.
Additional pre-processing to construct the network flows.	In the case of encrypted payload, signature matching will be impossible.
In flow-based, there are delays in data catching and accessibility to the NIDS.	Exposing the confidential information.
	Heavyweight packet-based NIDS.
	Not efficient for high-speed networks.

D. ENTROPY-BASED APPROACH (EBA)

The EBA is considered one of the most efficient detection approaches in detecting network abnormalities. The entropy is an efficient way of measuring the randomness of network traffic that comes into the network [42], [43]. Therefore, EBA is used to compute the distribution and randomness of the traffic attributes in the network [44], [45]. Many features can be used in EBA, for example, source IP address, destination IP address, and the network prefix information. The entropy is used to measure the uncertainty associated with a random variable. The entropy Equation 1 can be defined as follows:

$$H(X) = -\sum_{1-i}^{n} P_i \, log_2 \, P_i. \tag{1}$$

From Equation1, let X represent the dataset and X = x1, x2, x3.....xn, pi is the probability of xi in X [46]. Besides, in this technique, the entropy of the most important network traffic features is calculated. The selected features are used to detect normal and abnormal network traffic. The entropy technique can select numerous attributes of network flow records that play a vital role in the IDS [40].

III. LITERATURE REVIEW

In recent years, network security has a primary focus because it is a compulsory requirement to prevent intrusions of unauthorized users from accessing the network. Currently, many security devices and tools exist that are being used, such as anti-spyware, anti-virus, and firewalls. The first line of defense has been supplied by additional tools to monitor network traffic to detect any unauthorized intrusions that may break into the network. The intrusion can be distinguished by its behavior as its behavior has distinct and identifiable patterns [47].

Furthermore, IDSs aims to safeguard and protect the network from various kinds of attacks that threaten network confidentiality, integrity, and availability. IDSs are designed to distinguish abnormal activities from normal behavior, which offers a chance to defend the network before collapsing. IDS also provides an alerting mechanism regarding any hostile activity [48]. This section underlies a comprehensive study regarding the existing IDSs with their advantages and disadvantages.

David *et al.*,(2015) [49] proposed a mechanism to detect Distributed Denial of Service (DDoS) attacks using fast entropy approach and flow-based network traffic analysis to select many attributes from flow records. They also used an adaptive threshold algorithm to detect an abnormality based on variation in the network traffic. The detection accuracy of this technique is considered good. However, it was designed for the IPv4 network environment.

Mousavi *et al.*,(2015) [50] used the entropy approach to detect DDoS attacks in a software-defined network (SDN) environment. This research uses the entropy technique because it shows efficient results and resulted in high accuracy rates. Their approach uses a window size of 50 packets, then the entropy is calculated for each window size, then compared with the previously specified threshold value. Based on the authors' evaluation, this approach resulted in 96% detection accuracy. However, this approach is implemented in the IPv4 network.

Özçelik *et al.*,(2016) [51] performed a combination of cumulative sum (CUSUM) algorithm and EBA to detect network anomalies with high detection accuracy. The implementation of this research utilized the entropy of source IP addresses. The detection accuracy of this approach is 95%. However, this approach is designed and implemented for the IPv4 networks.

Shukla *et al.*,(2018) [46] proposed an intrusion detection system "Snort" to improve network security and to detect network attacks. The research approach uses the Renyi cross-entropy method and Shannon entropy to calculate the network attributes. The detection accuracy of this approach can detect 90% of network traffic attacks. However, this approach is designed and implemented for the IPv4 network environment, and this method is based on packet-based traffic representation, which is not suitable for high-speed networks.

Ibrahim *et al.*,(2019) [23] proposed an efficient approach using entropy-based technique and adaptive threshold algorithm to detect RA DoS flooding attack with 98% detection accuracy. However, the approach relies on packet-based traffic representation. The drawbacks of packet-based traffic representation include a lengthy processing time and more complex methods to analyze a massive amount of network traffic. Also, this approach is only suitable to detect the RA DoS flooding attack. Table 2 summarizes the limitations of the existing approaches in detecting NDP attacks.

Table 2 shows that none of the existing approaches are designed to detect NDP traffic abnormalities, which are the

TABLE 2. Limitations of existing mechanisms.

Mechanism (Author/year)	Limitations
David et al., (2015) [49].	Limited to the IPv6 network. This mechanism is designed for IPv4 network. This mechanism is based on the packet-based traffic representation, which is not efficient for high-speed networks.
Mousavi et al., (2015) [50].	Limited to the IPv6 network. This mechanism is designed for IPv4 network. This mechanism based on the packet-based traffic representation, which is not efficient for high-speed networks.
Özçelik et al., (2016) [51].	Limited to the IPv6 network. This mechanism is designed for IPv4 network. This mechanism is based on the packet-based traffic representation, which is not efficient for high-speed networks.
Shukla et al., (2018) [46].	Limited to IPv6 network. This mechanism is designed for IPv4 network. This mechanism is based on the packet-based traffic representation, which is not efficient for high-speed networks.
Ibrahim et al., (2019) [23].	This approach relies on packet-based traffic representation, which is not efficient for high-speed networks. Limited to detecting RA DoS flooding attack. Lacking efficient features that are significant in detecting such attacks

expected behavior among all NDP-based attacks. Therefore, a properly designed approach to detect abnormal NDP traffic might improve NDP-based attacks' detection accuracy. In addition, the existing approaches also suffer from other limitations: (i) inefficient for high-speed networks since reliance on packet-based network traffic representation will result in packet drops and lead to increasing the false positive (FP) rates, (ii) increased complexity since packet-based approaches are required to process and analyze the massive amounts of network traffic, (iii) exposing confidential information from the network packet payloads. Therefore, the proposed approach avoids the existing approach's limitations by relying on flow-based network traffic representation instead of packet-based network traffic representation.

IV. PROPOSED APPROACH

This section provides an overview of the proposed flow-based approach that consists of three interconnected stages to detect NDP traffic abnormalities caused by RA or NS DoS flooding attacks. Figure 3 illustrates the architecture of the proposed approach.

A. STAGE 1 - GATHERING NETWORK TRAFFIC AND PRE-PROCESSING

This subsection discusses the first and core stage of this proposed approach. This stage aims to generate and capture network traffic, convert the traffic in an appropriate format, and filter the network traffic before passing it to the next stage. This stage comprises three steps: generating and gathering network traffic, ICMPv6 packet filtration, and RA/NS packet attributions selection.

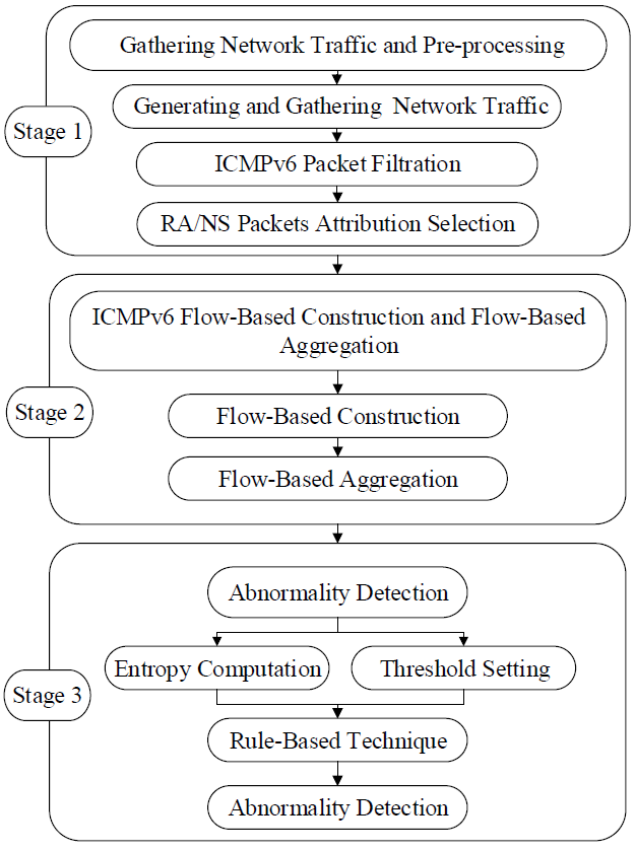

FIGURE 3. Architecture of the proposed approach.

1) GENERATING AND GATHERING NETWORK TRAFFIC

The first step is to capture the network traffic from the network interface card (NIC) of the monitored host. The gathered traffic, which includes normal and abnormal traffic, forms the datasets to be used as the input for the following stages. Figure 4 illustrates the generating and gathering network traffic step.

FIGURE 4. Generating and gathering network traffic.

2) ICMPv6 PACKET FILTRATION

Traffic filtration is the key part of the network traffic gathering and pre-processing stage. This process filters out unnecessary and unrelated traffic to reduce the dataset size. After receiving a dataset from the previous step, the filtration process begins by sending the dataset to a decoder module for IPv6 packet types extraction. Consequently, there are

additional pre-processing and packet analysis steps to extract the ICMPv6 packet types, source IP address, destination IP address, and network prefix. The rationales of selecting these attributes are: (i) the ICMPv6 packet types (i.e., RA = 134 and NS = 135) are utilized by the attackers to trigger RA and NS DoS flooding attacks, (ii) the source IP address is regularly spoofed by the attackers, (iii) the destination IP address is used by the victim machines, and (iv) the network prefix is exploited by the attacker in case the attacker stops spoofing the source address and changing or specifying invalid network prefix. All mentioned attributes are stored as datasets. The filtration process is shown in Figure 5.

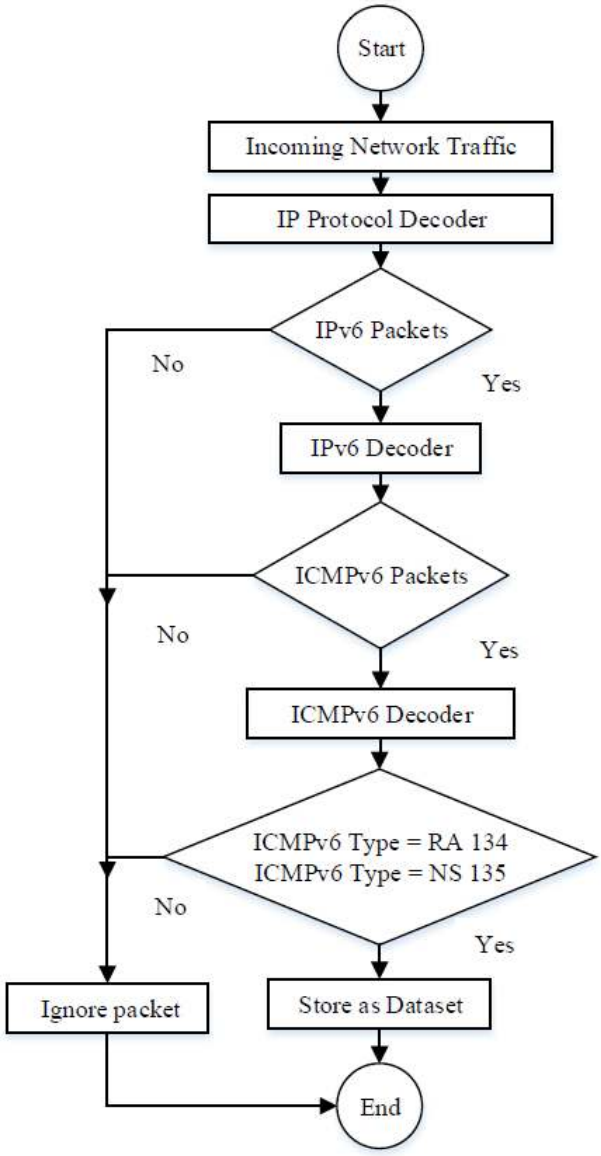

FIGURE 5. Flowchart of ICMPv6 packet filtration.

3) RA/NS PACKET ATTRIBUTIONS SELECTION

IPv6 packets comprise two parts, the header and payload. The header contains several fields, of which only some are considered in this research. Meanwhile, the payload is discarded to prevent exposing any confidential information from the network traffic [33]. Although every network packet has many attributes, not all of them contribute to detecting abnormal NDP traffic. Thus, this step aims to select the relevant attributes from the packets, which will be used in the next stage. The following attributes are considered: source IP address, destination IP address, ICMPv6 packet types (i.e., RA = 134 and NS = 135), and network prefix. All selected attributes for each packet will be used as a flow feature in the next stage.

B. STAGE 2 - FLOW-BASED CONSTRUCTION AND FLOW-BASED AGGREGATION

The network flow is a group of IP packets with the same features that pass through and are collected by a monitoring point in the network within a specific time interval. This stage uses flow-based traffic representation for various reasons, such as maintaining privacy by removing some of the network details, better efficiency in detecting intrusions for high-speed networks [37], and several promising results in IDS that are mentioned in [38].

Moreover, this stage is responsible for representing the IPv6 traffic in a flow-based form. Conventionally, the flow in IPv4 is classified based on five tuples: source IP address, destination IP address, source port, destination port, and IP protocol (TCP or UDP) [52]. Therefore, the IPv4 flow construction method cannot be used for ICMPv6 flow construction because the ICMPv6 is a network layer protocol and does not have source and destination ports. Under those circumstances, Elejla *et al.*, [33] considered the source IP address, destination IP address, and ICMPv6 type within a time interval (T) as a tuple for constructing ICMPv6 flow. The flow is represented as follows:

$$F_{\text{ICMPv6}} = (IPsrc, IPdst, ICMPv6\ types)_T.$$

In F_{ICMPv6}, the ICMPv6 types are used as a tuple key for two reasons. First, ICMPv6 has several messages, and each one of those messages has specific purposes and characteristics. Second, the attacker can utilize any type of ICMPv6 message to send an abnormal flow, such as an RA DoS flooding attack. Similarly, given that this research focuses on NDP traffic abnormality, which indicates RA and NS DoS flooding attacks, the ICMPv6 type will be RA = 134 and NS = 135. Also, this approach depends on two network traffic features, the source IPv6 address and network prefix, which are used for the precise detection of abnormal NDP traffic caused by the RA DoS flooding attack. Meanwhile, the source IPv6 address is used to detect abnormal NDP traffic caused by the NS DoS flooding attack.

There are several reasons for selecting the two features. The source IPv6 address is regularly spoofed by the attacker but not the destination address because it is the attack's designated target. The sole dependency on the source IP for detecting abnormal NDP traffic caused by the RA DoS flooding attack will degrade the detection accuracy. The reason for the degradation is the attacker's not spoofing

the source IP address but changing the network prefix. Therefore, the network prefix feature has been selected as one of the entropy calculation inputs. Under those circumstances, the current ICMPv6 flow construction proposed by Elejla *et al.* [33] has a drawback because their flow construction ignored the network prefix feature, which could lead to a high false positive (FP) rate or low detection accuracy in detecting RA DoS flooding attack. In our proposed approach, the flow-based form can be expressed as follows:

Flow-based construction for the detection of NDP traffic abnormal caused by the NS DoS flooding attack is expressed as follows:

$F_{ICMPv6} = (IPv6\ Src, IPv6\ Dst, ICMPv6\ type)_T$.

Flow-based construction for the detection of abnormal NDP traffic caused by the RA DoS flooding attack is expressed as follows:

$F_{ICMPv6} = (IPv6\ Src, IPv6\ Dst, ICMPv6\ type)_T$. or $F_{ICMPv6} = (IPv6\ Src, IPv6\ Dst, ICMPv6\ type, Prefix)_T$.

Where: *(Src)* is source address.

(Dst) is destination address.

(ICMPv6 type) is RA and NS messages.

(Prefix) is used by hosts as information to dynamically allocate their IP address in IPv6 link-local network.

(T) is for time of each flow record.

Another aspect of this stage is the flow-based aggregation. It is responsible for equipping the flow with selected attributes that contribute to detecting such attacks. The attributes that are selected as contributing features to distinguish between normal or abnormal NDP traffic behavior flows are IPv6 source address, IPv6 destination address, ICMPv6 packet types (RA = 134 and NS = 135), network prefix, and time interval. Also, these attributes are attached to every flow record to enhance detection accuracy. The flow will be aggregated every (t) time, where (t) is a configurable value. In this research, the value of (t) is set to one second based on the experimental data. It has been observed that just one second of attack time is enough to gather a massive number of network flows.

C. STAGE 3 - ABNORMALITY DETECTION

Stage 3 is the last stage of the proposed approach with the goal to detect abnormality in the NDP traffic caused by RA and NS DoS flooding attacks. This stage underlines the entropy computation to calculate the selected network flow features. Also, this stage presents the threshold setting to define a specific baseline value for abnormal NDP traffic behavior. Finally, this subsection describes the rule-based technique to enhance the detection accuracy of the proposed flow-based approach.

1) ENTROPY COMPUTATION

The entropy-based Approach (EBA) has been used in various attack detection approaches, such as [22]. It is known to provide impressive results and effective performance in detecting attacks. In this research, two entropy values are calculated. The first value calculates the entropy for the source IP address that contributes to the detection of the NDP traffic abnormality caused by RA or NS DoS flooding attacks. The second value calculates the entropy for the network prefix that contributes to the detection of the NDP traffic abnormality caused by the RA DoS flooding attack.

There are two reasons for selecting the two features. First, the attackers always spoof the source IP address but not the destination IP address because the destination IP address is used by the victim nodes. Besides that, based on a previous study [22], the source IP address is the most crucial feature in detecting RA DoS flooding attacks. Second, to accommodate the scenario where the attacker stops spoofing the source IP address and changing or specifying invalid network prefix. Thus, this research selects the network prefix as a qualifying feature, and it is one of the contributions of our proposed approach.

2) THRESHOLD SETTING

A threshold can be defined as a specific value used as a baseline for abnormal NDP traffic behavior caused by RA and NS DoS flooding attacks. The threshold values are based on monitoring network traffic from a simulated dataset. Any deviation from the threshold values will trigger an alarm. This step discusses the three threshold values used in the proposed approach.

- The threshold value for the time window of the flow construction and flow aggregation. The time window is set to one second for abnormal NDP traffic caused by RA and NS DoS flooding attacks. This is because, in just one second of attack time, the record of a single flow already contains a massive number of network packets and based on the experiments, the entropy value of one second is high. Under those circumstances, the threshold value for the time window of the flow construction and flow aggregation is configured to one second.
- The threshold value for the entropy is statically set at one for abnormal NDP traffic caused by RA and NS DoS flooding attacks. The reason for configuring this value "β" at one is based on the experiments and observation of the detection efficiency when this value is used. Also, the use of the selected threshold value (one) resulted in the lowest false positive (FP) and false-negative (FN) rates. Equation 2 illustrates the threshold of the entropy value.

$$H(X) = -\sum_{1-i}^{n} P_i \log_2 P_i > 1. \tag{2}$$

- The threshold value for the number of times the entropy value is exceeded. If the entropy value exceeded the threshold value "α" three times successively, the traffic flow will be considered abnormal. The reason for setting the threshold value to three is because it increases the performance of the proposed flow-based approach in terms of detection accuracy and reducing the FP rate.

In addition, this value has been used in many existing approaches, such as in [23].

3) RULE-BASED TECHNIQUE

This subsection underlines the rule-based technique that is used as an essential step in the proposed approach. The reason for using the rule-based technique is to enhance the detection accuracy of the proposed approach. This step is used to compare the output of the entropy computation function with the threshold value. This section introduces two rules to detect the abnormal NDP traffic caused by RA or NS DoS flooding attacks.

The first rule, shown in Algorithm 1, contributes to detecting abnormal NDP traffic caused by RA and NS DoS flooding attacks. If the entropy value of the source IP address exceeded the threshold three times successively, then it is considered as an abnormal NDP traffic behavior. The reason for considering the entropy value of the source IP address is due to the attackers could spoof the source IP address to amplify the attack traffic volume.

Algorithm 1 First Rule-Based Algorithm

Count $= 0$
If Entropy (Source IP address) $> \beta$ *then*
count $=$ *count* $+1$
If (*count* $\geq \alpha$) *then*
Alert $=$ *turn*
End if
End if

Where β is a threshold ($\beta = 1$) violation of entropy value before the alarm is triggered. Where α is a threshold value ($\alpha = 3$).

The second rule, shown in Algorithm 2, contributes to increasing the detection accuracy of abnormal NDP traffic behavior caused by the RA DoS flooding attack to accommodate the scenario where the attacker stops spoofing the source IP address and changing or specifying invalid network prefix. The network prefix is used by hosts to allocate their IP addresses in IPv6 link-local network dynamically. The second rule will be triggered if the entropy value of the network prefix exceeded the threshold three times successively. Then, it is considered abnormal NDP traffic caused by the RA DoS flooding attack.

Algorithm 2 Second Rule-Based Algorithm

Count $= 0$
If Entropy (Network Prefix) $> \beta$ *then*
count $=$ *count* $+1$
If (*count* $\geq \alpha$) *then*
Alert $=$ *turn*
End if
End if

Where β is a threshold ($\beta = 1$) violation of entropy value before the alarm is triggered. Where α is a threshold value ($\alpha = 3$).

V. WORK-FLOW OF THE PROPOSED APPROACH

This section provides a brief discussion of the operational steps of the proposed flow-based approach.

1) Start capturing inbound and outbound incoming network traffic via NIC.
2) The filtration process begins when the decoder filters in the IPv6 packets. An extra pre-processing is done to extract the ICMPv6 packets, then filter in the RA messages (ICMPv6 type 134) and NS messages (ICMPv6 type 135).
3) Flow-based construction is responsible for representing the NDP (RA and NS) network traffic in a flow form, and the flow is aggregated every one second for both message types.
4) The EBA will calculate the entropy of the source IP addresses and the network prefixes to detect the presence of RA DoS flooding attack; and for the detection of NS DoS flooding attack, the EBA calculates the entropy of the source IP addresses.
5) The output of the entropy values of RA and NS are compared with the threshold. If the entropy value of the massages exceeded the threshold three times successively, then it will be considered as abnormal NDP traffic caused by RA and NS DoS flooding attacks.

Figure 6 illustrates the workflow of the proposed flow-based approach.

VI. IMPLEMENTATION OF THE PROPOSED APPROACH

This section discusses the software tools and programming language that are used to implement the proposed approach. Besides, the generated datasets used to evaluate the proposed approach are thoroughly discussed as well.

A. SOFTWARE TOOLS AND PROGRAMMING LANGUAGE

The proposed flow-based approach for detecting abnormality in NDP traffic caused by RA and NS DoS flooding attacks is implemented using several tools.

1) THC-IPv6 [53] toolkit to generate the two types of attacks, RA DoS flooding attack and NS DoS flooding attack.
   - Flood_router6 tool is used to generate RA DoS flooding attacks by overwhelming the network with spoofed RA messages.
   - Flood_solicitate6 tool is used to generate the NS DoS flooding attack by overwhelming the network with spoofed NS messages.
2) Wireshark [35] to capture and analyze the link-local IPv6 network traffic.
3) Graphical Network Simulator 3 (GNS3) [54] is used to construct an isolated testbed topology. The network topology comprises one Kali Linux virtual machine that plays the role of the attacker. Moreover, the testbed also includes two virtual machines running

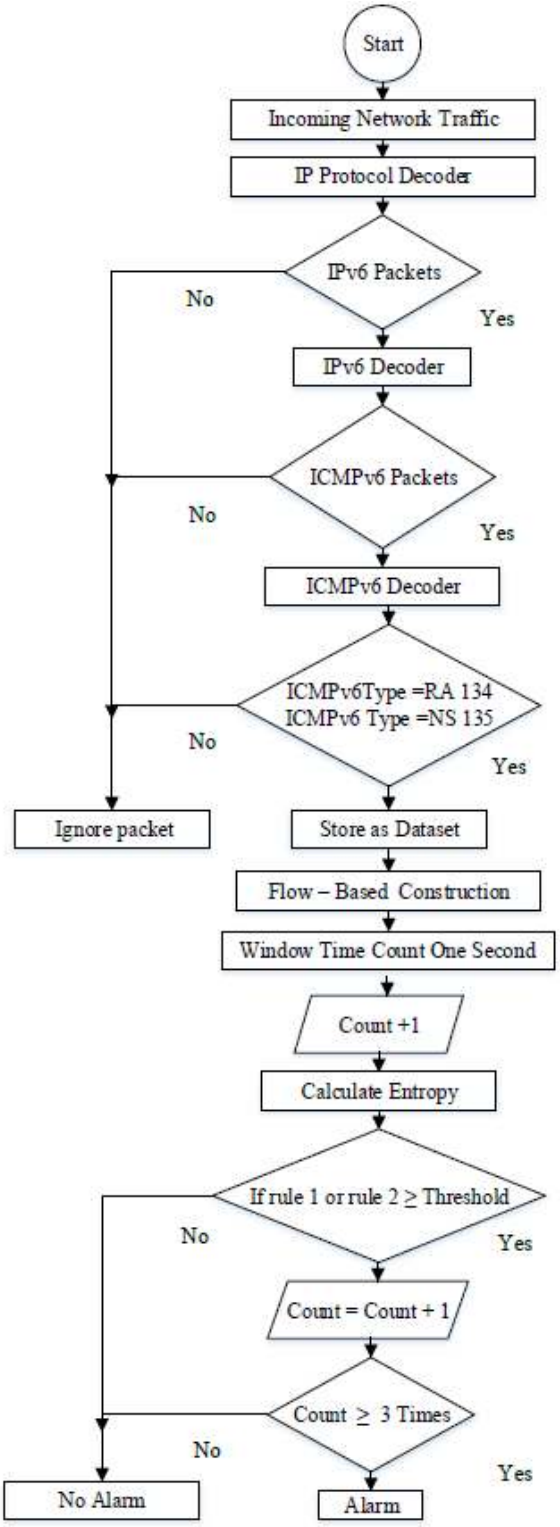

FIGURE 6. Flowchart of the proposed approach.

Windows 10 and Windows 7, playing the role of the victims' machines. Additionally, the testbed included a hub, which is used to connect the network topology. Given that the hub is a single collision domain, it will forward the traffic to all network topology. Finally, the testbed also has a router that acts as the legitimate default gateway of this link-local network. Figure 7 depicts the testbed network topology.

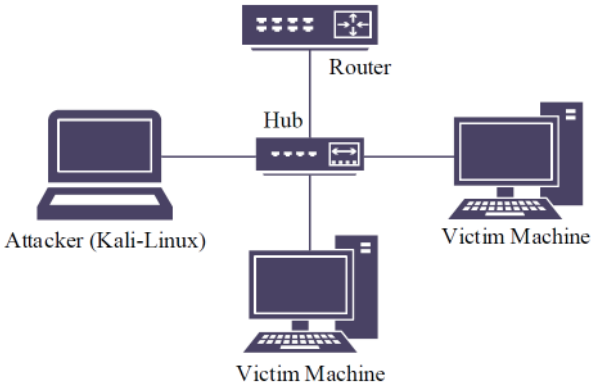

FIGURE 7. IPv6 network topology.

4) The Python programming language is used for the implementation of the proposed approach with open-source Python packages, such as NumPy, SciPy, and Pyshark.

B. GENERATED DATASETS

Given that no dataset exists that fulfills the proposed flow-based approach requirements to detect abnormal NDP traffic behavior caused by RA and NS DoS flooding attacks, an urgent need for new datasets remains. This section presents the key features of the generated flow-based datasets.

1) The generated flow-based datasets are formed on the basis of the definition of flow-based features, as mentioned in SubsectionIV-B.
2) The generated flow-based datasets are grounded on flow-based traffic representation because it is more suited for high-speed networks and reduces the amount of data, which must be analyzed by the proposed approach and at the same time protects the confidential information by removing some of the network details.
3) The proposed flow-based datasets are generated based on the most qualified features. For the RA dataset, five qualified features were used: source IPv6 address, Destination IPv6 address, ICMPv6 messages type, network prefix, and time interval. For the NS dataset, four qualified features are used: the source IPv6 address, Destination IPv6 address, ICMPv6 messages type, and time interval.
4) The flow-based datasets are designed for detecting abnormal NDP traffic caused by RA and NS DoS flooding attacks. Table 3 shows the packets distribution in each dataset.

VII. EXPERIMENTAL RESULTS

This section discusses the evaluation metrics used to evaluate the proposed approach. In addition, this section provides an in-depth discussion of the results obtained from imple-

TABLE 3. Datasets packets distribution.

Packets Datasets	Number of Features	Normal Traffic	Abnormal Traffic	Total Traffic
RA	5 features	17,224	329,449	346,673
NS	4 features	56,976	56,975	113,951

menting the proposed flow-based approach on the generated datasets.

A. EVALUATION METRICS

The proposed flow-based approach is evaluated in terms of several evaluation metrics. The evaluation metrics used are detection accuracy, precision, recall, and F1-Score. These metrics are calculated using the parameters listed in Table4.

TABLE 4. Evaluation metrics parameters [55].

Parameters	Description
True Negative (TN)	Normal traffic behavior is detected as normal.
True Positive (TP)	Abnormal traffic behavior is detected as abnormal.
False Positive (FP)	Normal traffic behavior is detected as abnormal.
False Negative (FN)	Abnormal traffic behavior is detected as normal.

1) **Detection Accuracy** evaluates the IDS by providing accurate alerts in the event of abnormal flow traffic and keeping silent for regular flow traffic. Equation 3 is used to calculate the accuracy of the proposed flow-based approach.

$$Accuracy\,Detection = \frac{TP+TN}{TP+TN+FP+FN} \times 100. \tag{3}$$

2) **Precision** is the proportion of attack cases that are correctly predicted relative to the predicted size of the attack [56]. Equation 4 is the standard formula to calculates the precision.

$$Precision = \frac{TP}{TP+FP} \times 100. \tag{4}$$

3) **Recall** is the proportion of correctly predicted attack cases to the actual size of the attack [57]. Equation 5 is the standard formula to calculate the recall.

$$Recall = \frac{TP}{TP+FN} \times 100. \tag{5}$$

4) **F1-Score** is the average value of recall and precision to evaluate the proposed approach accurately [58]. Equation 6 is the standard formula to calculate F1-Score.

$$F1-Score = \frac{2 \times (Recall \times Precision)}{Recall + Precision} \tag{6}$$

In brief, the flow-based approach is evaluated in terms of detection accuracy, precision, recall, and f1-score, which are commonly used to evaluate an IDS's effectiveness. The proposed flow-based approach is evaluated on the basis of these metrics to check its capability in detecting abnormal NDP traffic behavior caused by RA or NS DoS flooding attacks with a high detection accuracy and a low FP rate.

B. RESULTS AND DISCUSSION

In this subsection, two scenarios were used and taken as baselines to evaluate the effectiveness of the proposed flow-based approach. The first scenario aims to check the robustness of the proposed approach in detecting the presence of abnormal NDP traffic behavior caused by the RA DoS flooding attack. Meanwhile, the second scenario aims to check the robustness of the proposed approach in detecting the presence of abnormal NDP traffic behavior caused by the NS DoS flooding attack. Figure 8 illustrates the taxonomy of the experiments' scenarios runs.The following Subsections VII-B1 and VII-B2 present both scenarios in further details. Finally, Subsection VII-B3 illustrates a comparison of the proposed flow-based approach with other existing approaches.

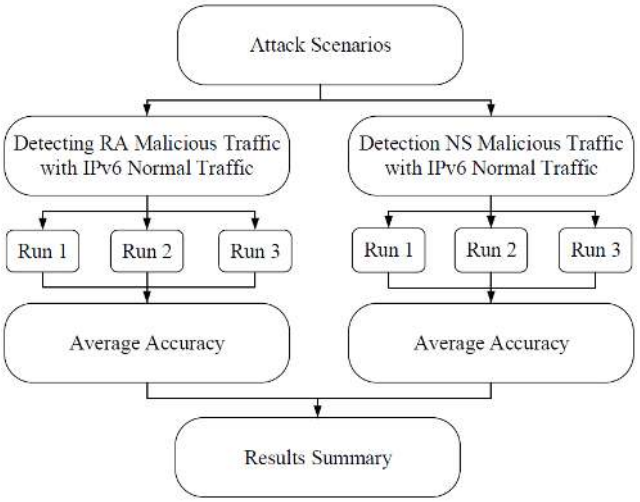

FIGURE 8. Taxonomy of experiment runs.

1) DETECTION ACCURACY OF ABNORMAL NDP TRAFFIC CAUSED BY RA DoS FLOODING ATTACK

This subsection presents the experimental result and discussion of the proposed flow-based approach to detect abnormal NDP traffic caused by the RA DoS flooding attack. In this type of attack, two entropy values were calculated. First, the entropy value for the source IP address. Second, the entropy value for the network prefix. Then we compared the output of entropy values with a predefined threshold value, whereas the predetermined threshold value (β) is set to 1.

After that, the rule-based technique is applied; if the entropy value of the source address and network prefix exceeded the threshold value repeatedly three times, then it is considered abnormal NDP traffic behavior caused by the RA DoS flooding attack. Figure 9 depicts the entropy values of the source address against a predefined threshold, and Figure 10 shows the entropy values of the network prefix against the predefined threshold for the network traffic caused by RA DoS flooding attack.

Figures 9 and 10 show the entropy values of the network prefix and source address. The maximum entropy values were recorded at 10.2. This is the point at which the randomness

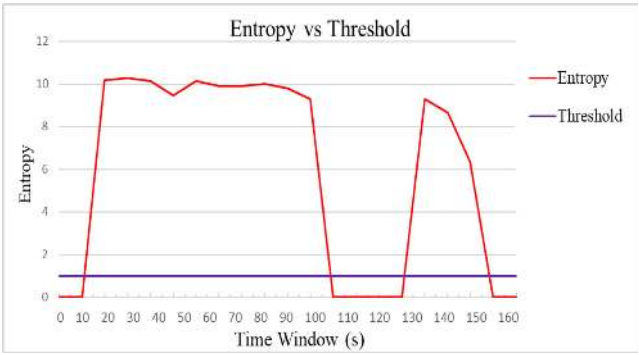

FIGURE 9. Entropy value of source address vs. Predetermined threshold value (β) for network traffic caused by RA DoS flooding attack.

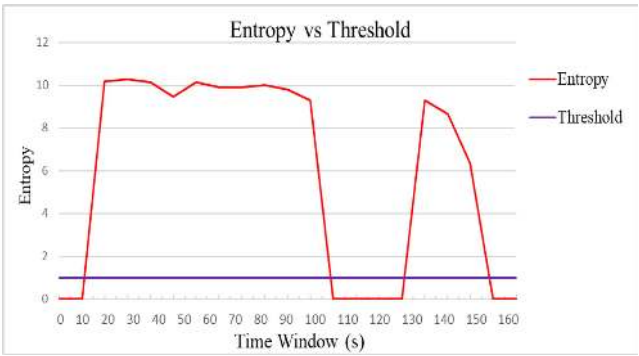

FIGURE 10. Entropy value of network prefix vs. Predetermined threshold value (β) for the network traffic caused by RA DoS flooding attack.

of the network prefix and source IP address are at their highest entropy values. This high entropy value is due to the massive number of source IP addresses and network prefixes used as the input for the entropy calculation. Meanwhile, the entropy value leveled off to 1 or lower after three or more successive violations of the predetermined threshold. If the entropy values drop below the predetermined threshold value, then it is considered normal NDP traffic.

It can be noticed that the entropy values in both Figure 9 and 10 are similar, and this is due to the nature of RA DoS flooding attack where the attacker sends a myriad amount of RA packets to the victim where each RA packet carries a unique network prefix, and its source IP address is spoofed. Therefore, the victim will receive the same number of spoofed source IP addresses and network prefixes.

Moreover, the experiments were run only three times because the experiments are grounded on simulated datasets to ensure that the proposed approach is reliable among all run times. Then, the results were averaged out to obtain precise average detection accuracy, precision, recall, and F1-Score. Table 5 shows the detection accuracy, precision, recall, and F1-Score results for three run times.

The average accuracy result of all three runs experiments is calculated as shown in Equation 7:

$$Average\ Accuracy = \frac{98.1 + 98.1 + 98.1}{3} = 98.1\%. \quad (7)$$

TABLE 5. Detection accuracy, Precision, Recall, and F1-Score for the Abnormal NDP traffic behavior caused by RA DoS flooding attack.

Experiment	FP	FN	TP	TN	Detection Accuracy	Precision	Recall	F1-Score
Run 1	18	0	22	922	98.1%	55%	100%	70.96%
Run 2	18	0	22	922	98.1%	55%	100%	70.96%
Run 3	18	0	22	922	98.1%	55%	100%	70.96%

whereas the average precision of all three runs experiments is calculated in Equation 8:

$$Average\ Precision = \frac{55 + 55 + 55}{3} = 55\%. \quad (8)$$

whereas the average recall of all three runs experiments is calculated in Equation 9:

$$Average\ Recall = \frac{100 + 100 + 100}{3} = 100\%. \quad (9)$$

Finally, the F1-Score is used to calculate the average recall and precision percentage value of all three runs experiments are calculated in Equation 10:

$$F1 - Score = \frac{2 \times (100 \times 55)}{100 + 55} = 70.96\%. \quad (10)$$

From Equations 7, 8, 9, and 10 the average accuracy is 98.1% for all three run times, the average precision percentage is 55%, the average recall percentage is 100%, and the F1-Score percentage is 70.96%. This proves that the flow-based approach can detect the abnormal NDP traffic caused by the RA DoS flooding attack accurately with a high detection rate. As for precision, the proposed approach has a medium average precision percentage of 55%, which means it has a medium false-positive rate. Besides, the proposed approach has no FN rate as the average result of recall is 100%. The proposed approach archives 70.96% for F1-Score, which means that the average value of recall and the precision percentage is high.

2) DETECTION ACCURACY OF ABNORMAL NDP TRAFFIC CAUSED BY NS DoS FLOODING ATTACK

This subsection presents the experimental results and discussions of the proposed flow-based approach to detect NDP traffic abnormality caused by the NS DoS flooding attack. In this type of attack, one entropy value for the source IP address was calculated. Then the output of entropy value is compared with the predetermined threshold value, whereas the predetermined threshold value (β) is set to 1.

Henceforth, the rule-based technique is applied; if the entropy value of the source address exceeded the predetermined threshold value repeatedly for three times, then it is considered abnormal NDP traffic behavior caused by the NS DoS flooding attack. Figure 11 illustrates the entropy values of the source IP addresses against the predetermined threshold value.

As shown in Figure 11, the maximum entropy values of the source IP addresses are recorded at 13. This is the point at which the randomness of source IP addresses is at its highest entropy value. This entropy value has a high value

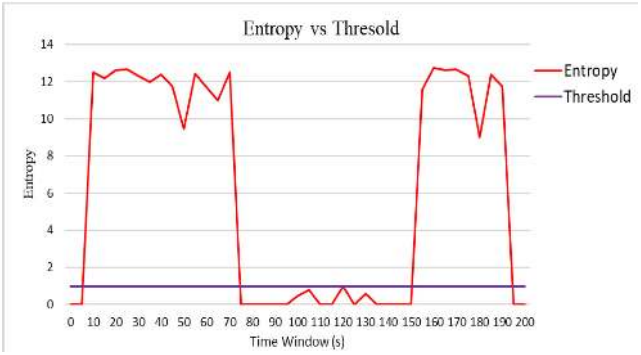

FIGURE 11. Entropy value of source IP vs. Predetermined threshold value (β) for the network traffic caused by NS DoS flooding attack.

due to the massive number of source IP addresses used as input to the entropy value calculation. Meanwhile, the value of the threshold leveled off to 1 or lower after three or more successive violations of the predetermined threshold. If the entropy values drop under the leveled off threshold, then it is considered normal network traffic.

The experiments were run only three times because the experiments are grounded on simulated datasets and to ensure that the proposed approach is reliable among all run times. Then, the results were averaged out to obtain precise average detection accuracy, precision, recall, and F1-Score Table 6 show the detection accuracy, precision, recall, and F1-Score results for three run times.

TABLE 6. Detection accuracy,Precision, Recall, and F1-Score for the Abnormal behavior caused by NS DoS flooding attack.

Experiment	FP	FN	TP	TN	Detection Accuracy	Precision	Recall	F1-Score
Run 1	2	0	21	13421	99%	91.3%	100%	95.45%
Run 2	2	0	21	13421	99%	91.3%	100%	95.45%
Run 3	2	0	21	13421	99%	91.3%	100%	95.45%

The average accuracy result of all three runs experiments is calculated as shown below in Equation 11:

$$Average\ Accuracy = \frac{99 + 99 + 99}{3} = 99\%. \quad (11)$$

whereas the average precision result is calculated using the Equation 12:

$$Average\ Precision = \frac{91.3 + 91.3 + 91.3}{3} = 91.3\%. \quad (12)$$

whereas the average recall result is calculated using the following Equation 13:

$$Average\ Recall = \frac{100 + 100 + 100}{3} = 100\%. \quad (13)$$

Finally, the F1-Score is used to calculate the average recall and precision percentage value of all three runs experiments are calculated in Equation 14:

$$F1 - Score = \frac{2 \times (100 \times 91.3)}{100 + 91.3} = 95.45\%. \quad (14)$$

Equations 11, 12, 13, and 14 show that the average accuracy is 99%, the average precision percentage is 91.3%, the average recall percentage is 100%, and the F1-Score percentage is 95.45%. for all run times. This proves that the flow-based approach can detect the abnormal behavior caused by the NS DoS flooding attack accurately with a high detection rate. Meanwhile, the average precision percentage of 91.3% indicates that the proposed approach has a low FP rate. The average recall is 100% means that there is no FN in the proposed approach. The average value of F1-Score is 95.45%, which means that the proposed approach indicates perfect precision and recall percentages.

In the final analysis, it can be noticed that the reported results in both Table 5 and 6 have the same values in different runs. This is because the proposed approach was applied over the same dataset without tuning. Also, since there are no publicly available datasets to evaluate the proposed flow-based approach. Having the same result in each run proves that the proposed approach is reliable and accurate. The evaluation of the proposed approach is done by taking into account two scenarios in evaluating the effectiveness of the proposed flow-based approach in terms of detection accuracy, precision, recall, and F1-Score. The first scenario validates the abnormal behavior caused by the RA DoS flooding attack, while the second scenario validates the abnormal behavior caused by the NS DoS flooding attack.

Fundamentally, the proposed approach is evaluated in terms of detection accuracy, precision, recall, and F1-Score to check its performance in detecting abnormal NDP traffic caused by RA and NS DoS flooding attacks. The proposed flow-based approach achieves high detection accuracy and medium precision rate in detecting abnormal behavior caused by the RA DoS flooding attack. The medium precision (55%) rate is due to the moderate number of false-positive, which is equal to 18 and which is the result of using a static threshold (equals to 1) for the first and second rules. The FP rate can be reduced if a dynamic threshold is used instead. The reduction of the FP rate will lead to an increase in the precision rate.

Meanwhile, the proposed flow-based approach achieves high detection accuracy and high precision rate in detecting abnormal behavior caused by the NS DoS flooding attack. The high accuracy, high recall, and moderate to high precision achieved by the proposed flow-based approach are conclusive evidence that the use of the Entropy and the proposed rules significantly contribute to detecting the presence of abnormal behavior caused by RA and NS DoS flooding attacks. Table 7 shows the result of the average detection accuracy for both experiments, while Figure 12 shows the average precision, recall, and F1-Score results for both experiments.

TABLE 7. Summary of average detection accuracy results.

Scenarios	Average Accuracy
Abnormal behavior of RA DoS Flooding Attack	98.1%
Abnormal behavior of NS DoS Flooding Attack	99%
Total Average Accuracy For both Scenarios	98.55%

TABLE 8. Comparison of the proposed approach with other approaches.

Author and Year	Technique	Dataset Type	Network Traffic Representation	Attacks Type	Average Accuracy	Average Precision	Average Recall	Average F1-Score
Our flow-based approach.	Entropy-Based Algorithm, Rule-based Algorithm, and Configurable Threshold Values.	Generated Datasets.	Flow-based IDS.	RA and NS DoS flooding attack.	RA DoS attack 98.1%. NS DoS attack 99%.	RA DoS attack 55%. NS DoS attack 91.3%.	RA DoS attack 100%. NS DoS attack 100%.	RA DoS attack 70.96%. NS DoS attack 95.45%.
Saad et al., (2016) [11]	Back-propagation Algorithm.	Generated Datasets.	Packet-based IDS.	ICMPv6 Echo request DDoS flooding attack .	ICMPv6 DDoS attack 98.3%.			
Elejla et al., (2018) [36]	Machine learning Algorithms.	Generated Datasets.	Flow-based IDS.	ICMPv6-based DDoS attacks.	ICMPv6 DDoS From 73.96% to 85.83%.			
Ibrahim et al., (2019) [23]	Entropy-based Algorithm and Adaptive Threshold Algorithm.	Generated Datasets.	Packet-based IDS.	RA DoS flooding attack.	RA DoS attacak 98%.			
Alsadhan et al., (2019) [59]	Locally Weighted Learning techniques, with three different machine learning models.	Generated Datasets	Flow-based IDS.	NDP DDoS attacks, replayed attacks, and identifying the normal traffic.	DDoS attack 99%, Replayed attacks 91.17%, and Normal traffic 94% .			

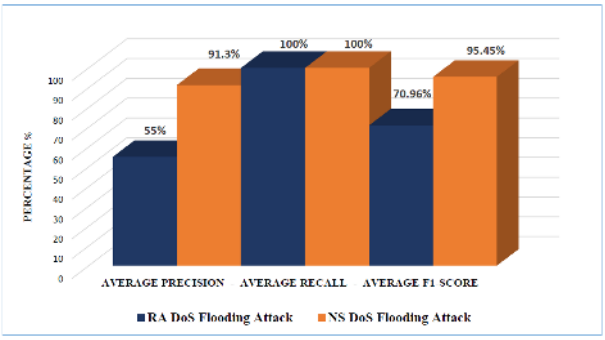

FIGURE 12. The summary results of average precision, Average recall and average F1-Score.

3) COMPARISON OF PROPOSED FLOW-BASED APPROACH WITH EXISTING APPROACHES

This subsection provides a comparison between the proposed flow-based approach and existing approaches. Table 8 tabulates the comparison of our flow-based approach and the existing approaches. The comparison is based on specific metrics, such as (i) the technique used, (ii) type of dataset, (iii) network traffic representation, (iv) type of attack, (v) average accuracy, (vi) average precision, (vii) average recall, and (viii) average F1-Score.

As shown in Table 8, the proposed flow-based approach obtained significant results compared to other existing approaches in terms of the average accuracy, average precision, average recall, and average F1-Score. The approach proposed by Ibrahim *et al.*, (2019) [23] uses an Entropy algorithm combined with an adaptive threshold to detect RA DoS flooding attack; this approach achieved 98% average detection accuracy. A framework proposed by Saad *et al.*, (2016) [11] uses the back-propagation neural network algorithm to detect only ICMPv6 Echo request DDoS flooding attack and achieved 98.3% detection accuracy. However, both approach and framework rely on packet-based traffic representation, which is inefficient for high-speed networks.

Moreover, the approach by Elejla *et al.*, (2018) [36] uses the flow-based traffic representation but achieved a lower detection accuracy compared with our proposed approach. This is because the network prefix was not used in their approach when constructing the network flow as opposed to the proposed approach. The use of the network prefix as one of the features in the construction of the flow contributes to more accurate detection of the abnormal NDP traffic behavior caused by the RA DoS flooding attack. Additionally, the network prefix is also used as an input to calculate the entropy value.

One more approach by Alsadhan *et al.*, (2019) [59] proposes three IDS models and uses flow-based traffic representation to detect NDP DDoS attacks and replayed attacks. Their approach achieved 99% and 91.17% for NDP DDoS attacks and replayed attacks, respectively. However, our proposed approach mainly focuses on constructing a flow that represents NDP traffic, which contributed to detect NDP traffic abnormalities caused by RA and NS DoS flooding attacks. Besides, our proposed approach achieved remarkable results in terms of detection accuracy, precision, recall, and F1-Score.

VIII. CONCLUSION

In this paper, an efficient flow-based approach is proposed, which has been shown to be highly capable of detecting abnormal NDP traffic caused by RA and NS DoS flooding attacks. It proposes qualified features that play vital roles in distinguishing normal and abnormal network flows accurately. In addition, this research adopts the entropy algorithm to calculate the randomness of source IP address and network prefix, which are considered the clues to detect abnormal NDP traffic behavior caused by RA and NS DoS flooding attacks.

The effectiveness of the proposed flow-based approach was evaluated using four performance metrics: detection accuracy, precision, recall, and F1-Score. The experimental result shows that the proposed flow-based approach obtained 98.1%, 55%, 100%, and 70.96% for the average accuracy, precision, recall, and F1-Score, respectively, for the detection of the abnormal NDP traffic behavior caused by the RA DoS flooding attack. As for the detection of the abnormal NDP traffic behavior caused by the NS DoS flooding attack, the proposed flow-based approach obtained 99%, 91.3%,

100%, and 95.45% for the average accuracy, precision, recall, and F1-Score, respectively. Also, the effectiveness of the proposed flow-based approach was verified by comparing it with the existing approaches and shows significant results.

Additionally, the proposed approach is destined to detect abnormal NDP traffic behavior caused by RA and NS DoS flooding attacks. The proposed flow-based approach has the flexibility to be extended in several directions for future work. For example, to detect NDP abnormal behavior results from RA and NS DDoS and DoS flooding attacks in IPv6 real-time implementation. Also, further research is needed to use various techniques such as dynamic/adaptive threshold algorithm.

REFERENCES

[1] A. Al-Ani, M. Anbar, A. K. Al-Ani, and I. H. Hasbullah, "DHCPv6Auth: A mechanism to improve DHCPv6 authentication and privacy," *Sādhanā*, vol. 45, no. 1, Dec. 2020, Art. no. 33, doi: 10.1007/s12046-019-1244-4.

[2] M. Zulkiflee, M. Azmi, 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.

[3] Z. R. Alashhab, M. Anbar, M. M. Singh, Y.-B. Leau, Z. A. Al-Sai, and S. A. Alhayja'a, "Impact of coronavirus pandemic crisis on technologies and cloud computing applications," *J. Electron. Sci. Technol.*, vol. 2, Nov. 2020, Art. no. 100059, doi: 10.1016/j.jnlest.2020.100059.

[4] A. A. O. Bahashwan, S. Manickam, and M. M. Penang, "A brief review of messaging protocol standards for Internet of Things (IoT)," *J. Cyber Secur. Mobility*, vol. 8, no. 1, pp. 1–14, 2018, doi: 10.13052/jcsm2245-1439.811.

[5] S. Deering and R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, document RFC 8200, 2007. [Online]. Available: https://www.rfc-editor.org/info/rfc8200, doi: 10.17487/RFC8200.

[6] A. K. Al-Ani, M. Anbar, S. Manickam, C. Y. Wey, Y.-B. Leau, and A. Al-Ani, "Detection and defense mechanisms on duplicate address detection process in IPv6 link-local network: A survey on limitations and requirements," *Arabian J. for Sci. Eng.*, vol. 44, no. 4, pp. 3745–3763, Apr. 2019, doi: 10.1007/s13369-018-3643-y.

[7] *Google*. Accessed: Jan. 24, 2021. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption

[8] T. Narten, E. Nordmark, and W. Simpson, *Neighbor Discovery for IP Version 6 (IPv6)*, document RFC 2461, Dec. 1998. [Online]. Available: https://www.rfc-editor.org/info/rfc2461, doi: 10.17487/RFC2461.

[9] M. Tayyab, B. Belaton, and M. Anbar, "ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review," *IEEE Access*, vol. 8, pp. 170529–170547, 2020, doi: 10.1109/ACCESS.2020.3022963.

[10] R. Radhakrishnan, M. Jamil, S. Mehfuz, and M. Moinuddin, "Security issues in IPv6," in *Proc. Int. Conf. Netw. Services (ICNS)*, Jun. 2007, p. 110, doi: 10.1109/icns.2007.106.

[11] R. M. Saad, M. Anbar, S. Manickam, and A. E. Alomari, "An Intelligent ICMPv6 DDoS flooding-attack detection framework (v6iids) using back-propagation neural network," *IETE Tech. Rev.*, vol. 33, no. 3, pp. 244–255, Dec. 2016, doi: 10.1080/02564602.2015.1098576.

[12] F. Najjar and M. M. Kadhum, "Reliable behavioral dataset for IPv6 neighbor discovery protocol investigation," in *Proc. 5th Int. Conf. IT Converg. Secur. (ICITCS)*, Aug. 2015, pp. 1–5, doi: 10.1109/ICITCS.2015.7293014.

[13] A. K. Al-Ani, M. Anbar, A. Al-Ani, and D. R. Ibrahim, "Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in IPv6 link-local network," *IEEE Access*, vol. 8, pp. 27122–27138, 2020, doi: 10.1109/ACCESS.2020.2970787.

[14] A. Alsadhan, A. Abdullah, A. Hussain, T. Baker, and O. Alfandi, "Detecting distributed denial of service attacks in neighbour discovery protocol using machine learning algorithm based on streams representation," in *Proc. Int. Conf. Intell. Comput.* Cham, Switzerland: Springer, 2018, pp. 551–563, doi: 10.1007/978-3-319-95957-3_58.

[15] A. A. Alsadhan, A. Hussain, and M. M. Alani, "Detecting NDP distributed denial of service attacks using machine learning algorithm based on flow-based representation," in *Proc. 11th Int. Conf. Develop. eSystems Eng. (DeSE)*, Sep. 2018, pp. 134–140, doi: 10.1109/DeSE.2018.00028.

[16] O. E. Elejla, M. Anbar, and B. Belaton, "ICMPv6-based DoS and DDoS attacks and defense mechanisms: Review," *IETE Tech. Rev.*, vol. 34, no. 4, pp. 390–407, Jul. 2017, doi: 10.1080/02564602.2016.1192964.

[17] A. AlSa'deh and C. Meinel, "Secure neighbor discovery: Review, challenges, perspectives, and recommendations," *IEEE Secur. Privacy Mag.*, vol. 10, no. 4, pp. 26–34, Jul. 2012, doi: 10.1109/MSP.2012.27.

[18] A. A. Bahashwan, M. Anbar, and S. M. Hanshi, "Overview of IPv6 based DDoS and DoS attacks detection mechanisms," in *Proc. Int. Conf. Adv. Cyber Secur.* Singapore: Springer, 2020, pp. 153–167, doi: 10.1007/978-981-15-2693-0_11.

[19] T. Zhang and Z. Wang, "Research on IPv6 neighbor discovery protocol (NDP) security," in *Proc. 2nd IEEE Int. Conf. Comput. Commun. (ICCC)*, Oct. 2016, pp. 2032–2035, doi: 10.1109/CompComm.2016.7925057.

[20] E. Mahmood, A. H. Adhab, and A. K. Al-Ani, "Review paper on neighbour discovery protocol in IPv6 link-local network," *Int. J. Services Oper. Inform.*, vol. 10, no. 1, pp. 65–78, 2019, doi: 10.1504/IJSOI.2019.100622.

[21] 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, Dec. 2018, doi: 10.1007/s00521-017-2967-y.

[22] S. Frankel, R. Graveman, and J. Pearce, *Guidelines for the Secure Deployment of IPv6*. Gaithersburg, MD, USA: NIST, 2010, p. 119.

[23] S. Shah, S. B. Ibrahim, 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," in *Computational Science and Technology*. Singapore: Springer, 2019, pp. 315–323, doi: 10.1007/978-981-13-2622-6_31.

[24] S. Thomson, T. Narten, and T. Jinmei, *IPv6 Stateless Address Autoconfiguration*, document RFC 4862, Sep. 2007. [Online]. Available: https://www.rfc-editor.org/info/rfc4862, doi: 10.17487/RFC4862.

[25] G. Bansal, N. Kumar, S. Nandi, and S. Biswas, "Detection of NDP based attacks using MLD," in *Proc. 5th Int. Conf. Secur. Inf. Netw.* , 2012, pp. 163–167, doi: 10.1145/2388576.2388600.

[26] A. Hines, "Neighbour discovery in IPv6," *Organiser Christian Schindelhauer*, vol. 2, pp. 1–12, Dec. 2004.

[27] M. Anbar, R. Abdullah, R. M. Saad, E. Alomari, and S. Alsaleem, "Review of security vulnerabilities in the IPv6 neighbor discovery protocol," in *Information Science and Applications*. Singapore: Springer, 2016, pp. 603–612, doi: 10.1007/978-981-10-0557-2_59.

[28] A. K. Al-Ani, M. Anbar, S. Manickam, and A. Al-Ani, "DAD-match; Security technique to prevent denial of service attack on duplicate address detection process in IPv6 link-local network," *PLoS ONE*, vol. 14, no. 4, Apr. 2019, Art. no. e0214518, doi: 10.1371/journal.pone.0214518.

[29] A. K. Al-Ani, M. Anbar, S. Manickam, A. Al-Ani, and Y. B. Leau, "Proposed DAD-match security technique based on hash function to secure duplicate address detection in IPv6 link-local network," in *Proc. Int. Conf. Inf. Technol.*, 2017, pp. 175–179, doi: 10.1145/3176653.3176707.

[30] S. Praptodiyono, I. H. Hasbullah, M. Anbar, R. K. Murugesan, and A. Osman, "Improvement of address resolution security in IPv6 local network using trust-ND," *Telkomnika Indonesian J. Electr. Eng.*, vol. 13, no. 1, pp. 195–202, Jan. 2015.

[31] L. Foschini, A. V. Thapliyal, L. Cavallaro, C. Kruegel, and G. Vigna, "A parallel architecture for stateful, high-speed intrusion detection," in *Proc. Int. Conf. Inf. Syst. Secur.* Berlin, Germany: Springer, 2008, pp. 203–220, doi: 10.1007/978-3-540-89862-7_18.

[32] T. A. Alamiedy, M. Anbar, Z. N. Alqattan, and Q. M. Alzubi, "Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm," *J. Ambient Intell. Hum. Comput.*, vol. 2, pp. 1–22, Nov. 2019, doi: 10.1007/s12652-019-01569-8.

[33] O. E. Elejla, M. Anbar, and B. Belaton, "Labeled flow-based dataset of ICMPv6-based DDoS attacks," *Neural Comput. Appl.*, vol. 31, no. 8, pp. 1–18, Aug. 2018, doi: 10.1007/s00521-017-3319-7.

[34] *TCPDUMP/LIBPCAP Public Repository*. Accessed: May 6, 2020. [Online]. Available: http://www.tcpdump.org/

[35] Wireshark. *Go Deep*. Accessed: Mar. 16, 2020. [Online]. Available: https://www.wireshark.org/

[36] O. E. Elejla, M. Anbar, B. Belaton, and B. O. Alijla, "Flow-based IDS for ICMPv6-based DDoS attacks detection," *Arabian J. Sci. Eng.*, vol. 43, no. 12, pp. 7757–7775, Dec. 2018, doi: 10.1007/s13369-018-3149-7.

[37] J. Quittek, T. Zseby, B. Claise, and S. Zander, *Requirements for IP Flow Information Export (IPFIX)*, document RFC 3917, 2004. [Online]. Available: https://www.rfc-editor.org/info/rfc3917, doi: 10.17487/RFC3917.

[38] A. Sperotto, R. Sadre, F. Van Vliet, and A. Pras, "A labeled data set for flow-based intrusion detection," in *Proc. Int. Workshop IP Oper. Manage.* Berlin, Germany: Springer, 2009, pp. 39–50, doi: 10.1007/978-3-642-04968-2.

[39] M. Chakraborty, N. Chaki, and A. Cortesi, "A new intrusion prevention system for protecting smart grids from ICMPv6 vulnerabilities," in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2014, pp. 1539–1547, doi: 10.15439/2014F287.
[40] M. F. Umer, M. Sher, and Y. Bi, "Flow-based intrusion detection: Techniques and challenges," *Comput. Secur.*, vol. 70, pp. 238–254, Sep. 2017, doi: 10.1016/j.cose.2017.05.009.
[41] A. Sperotto, "Flow-based intrusion detection," Ph.D. dissertation, Centre Telematics Inf. Technol., Univ. Twente, Enschede, The Netherlands, 2010.
[42] P. Berezi ski, J. Pawelec, M. Małowidzki, and R. Piotrowski, "Entropy-based Internet traffic anomaly detection: A case study," in *Proc. Int. Conf. Dependability Complex Syst.* Cham, Switzerland: Springer, 2014, pp. 47–58, doi: 10.1007/978-3-319-07013-1_5.
[43] P. Berezi ski and B. Jasiul, "An entropy-based network anomaly detection method," *Entropy*, vol. 17, no. 4, pp. 2367–2408, 2015, doi: 10.3390/e17042367.
[44] M. A. Aladaileh, M. Anbar, I. H. Hasbullah, Y. W. Chong, and Y. K. Sanjalawe, "Detection techniques of distributed denial of service attacks on software-defined networking controller–a review," *IEEE Access*, vol. 8, pp. 143985–143995, 2020, doi: 10.1109/ACCESS.2020.3013998.
[45] M. A. Al-Adaileh, M. Anbar, and Y. W. Chong, "Proposed statistical-based approach for detecting distribute denial of service against the controller of software defined network (SADDCS)," in *Proc. MATEC Web Conf.*, vol. 218, 2018, p. 02012, doi: 10.1051/matecconf/201821802012.
[46] A. S. Shukla and R. Maurya, "Entropy-based anomaly detection in a network," *Wireless Pers. Commun.*, vol. 99, no. 4, pp. 1487–1501, Apr. 2018, doi: 10.1007/s11277-018-5288-2.
[47] S. Ransewa, N. Elz, and T. Intajag, "Anomaly detection using source port data with Shannon entropy and EWMA control chart," in *Proc. 18th Int. Conf. Control, Autom. Syst. (ICCAS)*, 2018, pp. 596–601.
[48] D. Papamartzivanos, D. Mármol, and Georgios Kambourakis, "Dendron: Genetic trees driven rule induction for network intrusion detection systems," *Future Gener. Comput. Syst.*, vol. 79, pp. 558–574, Dec. 2018, doi: 10.1016/j.future.2017.09.056.
[49] J. David and C. Thomas, "DDoS attack detection using fast entropy approach on flow-based network traffic," *Procedia-Procedia Comput. Sci.*, vol. 50, pp. 30–36, Dec. 2015, doi: 10.1016/j.procs.2015.04.007.
[50] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, 2015, pp. 77–81, doi: 10.1109/ICCNC.2015.7069319.
[51] I. Özçelik and R. R. Brooks, "Cusum-entropy: An efficient method for DDoS attack detection," in *4th Int. Istanbul Smart Grid Congr. Fair (ICSG)*, 2016, pp. 1–5, doi: 10.1109/SGCF.2016.7492429.
[52] J. Rajahalme, A. Conta, B. Carpenter, and S. Deering, *IPv6 Flow Label Specification*, document RFC 3697, Mar. 2004. [Online]. Available: https://www.rfc-editor.org/info/rfc3697, doi: 10.17487/RFC3697.
[53] THC-IPV6. *Penetration Testing Tools*. Accessed: Mar. 16, 2020. [Online]. Available: https://tools.kali.org/information-gathering/thc-ipv6
[54] GNS3. *The Software That Empowers Network Professionals*. Accessed: Mar. 16, 2020. [Online]. Available: https://www.gns3.com/
[55] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, and D. Burgos, "An evolutionary SVM model for DDOS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020, doi: 10.1109/ACCESS.2020.3009733.
[56] M. Anbar, R. Abdullah, I. H. Hasbullah, Y.-W. Chong, and O. E. Elejla, "Comparative performance analysis of classification algorithms for intrusion detection system," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Dec. 2016, pp. 282–288, doi: 10.1109/PST.2016.7906975.
[57] 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.
[58] K. S. Sahoo and D. Puthal, "SDN-assisted DDoS defense framework for the Internet of multimedia things," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 16, no. 3s, pp. 1–18, Jan. 2021, doi: 10.1145/3394956.
[59] A. Alsadhan, A. Hussain, P. Liatsis, M. Alani, H. Tawfik, P. Kendrick, and H. Francis, "Locally weighted classifiers for detection of neighbor discovery protocol distributed denial-of-service and replayed attacks," *Trans. Emerg. Telecommun. Technol.*, vol. 2, p. e3700, Jul. 2019, doi: 10.1002/ett.3700.

ABDULLAH AHMED BAHASHWAN received the B.Sc. degree in computer applications from Osmania University, Hyderabad, India, in 2012, and the M.Sc. degree in internet engineering from the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), in 2020, where he is currently pursuing the Ph.D. degree. His research interests include computer networks, Internet Protocol version 6 (IPv6) security, network security, intrusion detection systems (IDS), cloud computing, software defines networks (SDN), and the Internet of Things (IoT).

MOHAMMED ANBAR (Member, IEEE) received the Ph.D. degree in advanced computer network from Universiti Sains Malaysia (USM). He is currently a Senior Lecturer with the National Advanced IPv6 Centre (NAv6), USM. His current research interests include malware detection, Web security, intrusion detection systems (IDS), intrusion prevention systems (IPS), network monitoring, the Internet of Things (IoT), and IPv6 security.

IZNAN HUSAINY HASBULLAH received the B.Sc. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently pursuing the M.Sc. degree in advanced network security. He has experience working as a Software Developer, a Research and Development Consultant, and a Network Security Auditor prior to joining the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, in 2010, as a Research Officer. His research interests include unified communication, telematics, network security, network protocols, and next-generation networks.

ZIYAD R. ALASHHAB received the B.S. degree in business networking and systems management from the University of Philadelphia, Philadelphia, in 2005, and the M.S. degree in management information systems from Arab Academy for Banking and Financial Sciences (AABFS), Jordan, in 2008. He is currently pursuing the Ph.D. degree with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM), Penang. His research interests include network security, the Internet security, and cloud computing and security.

ALI BIN-SALEM received the B.S. degree in computer science from Al-Ahgaff University, Yemen, in 2006, the M.S. degree in computer science from Universiti Sains Malaysia (USM), Malaysia, in 2009, and the Ph.D. degree from the National Advanced IPv6 Center (NAv6), (USM), in 2017. He was involved as an Operator with the East Asia-wide AI3 [Ay-triple-Ei] (Asian Internet Interconnections Initiative) Project, to help the use of Unidirectional Links over Satellite for interactive multimedia communications. He was also involved in CONNECT2SEA project, a project funded under FP7 that supports the European Union and South East Asia strategic partnership and policy dialogue. He is currently an Associate Professor with the School of Computer Science, Neijiang Normal University, Neijiang, China. His current research interests include the IoT, wireless LAN, QoS, 4G and 5G Networks, cross-layer, optimization techniques, distributed systems, and client-server architecture.