ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review

Article *in* IETE Technical Review · August 2016

DOI: 10.1080/02564602.2016.1192964

3 authors:

Omar Elejla
Islamic University of Gaza
14 PUBLICATIONS **101** CITATIONS
SEE PROFILE

Mohammed Anbar
Universiti Sains Malaysia
105 PUBLICATIONS **539** CITATIONS
SEE PROFILE

Bahari Belaton
Universiti Sains Malaysia
74 PUBLICATIONS **238** CITATIONS
SEE PROFILE

IETE Technical Review

ISSN: 0256-4602 (Print) 0974-5971 (Online) Journal homepage: http://www.tandfonline.com/loi/titr20

ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review

Omar E. Elejla, Mohammed Anbar & Bahari Belaton

To cite this article: Omar E. Elejla, Mohammed Anbar & Bahari Belaton (2016): ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review, IETE Technical Review, DOI: 10.1080/02564602.2016.1192964

To link to this article: http://dx.doi.org/10.1080/02564602.2016.1192964

IETE TECHNICAL REVIEW, 2016
http://dx.doi.org/10.1080/02564602.2016.1192964

ICMPv6-Based DoS and DDoS Attacks and Defense Mechanisms: Review

Omar E. Elejla[1], Mohammed Anbar[2] and Bahari Belaton[1]

[1]School of Computer Science, Universiti Sains Malaysia, Penang, Malaysia; [2]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia

ABSTRACT
The number of internet users and devices that are in need for more IP addresses to be assigned to them is rapidly increasing. A new protocol named IPv6 was developed in 1998 to overcome the addressing issue and to improve network communications in general. IPv6 is an improved protocol compared to IPv4 in terms of security since it provides built-in security mechanisms, such as IPSec. In addition, it brought new functionalities, such as Neighbour Discovery Protocol (NDP) procedure, which depends on Internet Control Message Protocol version 6 (ICMPv6) protocol messages. However, IPv6 inherited a number of attacks from IPv4 in addition to new attacks it brought within its new features. One of the most common attacks is the Denial of Service (DoS) attack due to its ease of being launched in different ways. A more serious DoS attack can be launched from many hosts called Distributed Denial of Service (DDoS). DoS and DDoS attacks are thorny and a grave problem of today's internet, resulting in economic damages for organizations and individuals. Therefore, this paper is created to study the properties of DoS and DDoS attacks against IPv6 networks using ICMPv6 messages. Additionally, it analyzes the various existing detection and prevention approaches that are proposed to tackle ICMPv6-based DoS and DDoS attacks. Moreover, it explains the existing tools that might be used for performing these attacks.

KEYWORDS
DDoS; DoS; ICMPv6; IPv6 security; NDP

1. INTRODUCTION

Limited studies on IPv6 Denial of Service (DoS) and Distributed Denial of Service (DDoS) problems have taken place and few surveys have been published. To the best of our knowledge, there is no survey specific to internet Control Message Protocol version 6 (ICMPv6) DoS and DDoS attacks in IPv6 network. Nevertheless, two surveys have been published in that area. First, Tripathi [1] has only covered DoS and DDoS attacks, which existed in IPv4 and still possibly do in IPv6 protocol. This means that the new DoS and DDoS attacks, which appeared with IPv6 new features, are not covered. Second survey by Saad et al. [2] focused on only one type of DoS and DDoS attacks which is the Flooding Attack. Moreover, there is no coverage for the solutions that are proposed to address such attacks by both survey papers. This paper presents a proper classification for ICMPv6-based DoS and DDoS attacks in addition to the approaches which are proposed to solve those attacks.

In the 1990s, internet engineers started to realize that IPv4 is going to suffer from the exhaustion problem in its pool of addresses. The IPv4 address pool (around 4 billion public IP) will not be able to serve all devices in 2020 (40.9 billion forecasted devices) [3]. This exhaustion forced the Internet Engineering Task Force (IETF) to come up with a new internet protocol, IPv6 with a larger address space. In 1998, IPv6 was designed as a successor to IPv4 and to eventually replace its capabilities [4]. IETF in RFC 2460 showed that IPv6 does not only provide expandability of addresses, it also brings new features and improvements (such as Extension Headers and Flow Label) that aim to provide better quality of service, ease-of-configuration, and fast routing of packet for networking, among others.

In fact, IPv6 introduced several diverse features that were unknown in IPv4. For example, it provides "plug-and-play" concept based on the Neighbour Discovery Protocol (NDP). NDP allows any new host to generate its own IPv6 address once it connects to a network [5]. Basically, NDP protocol uses ICMPv6 messages to accomplish its functions. ICMPv6 is a very important protocol since it is responsible for many functions. In addition to the neighbour and router discovery functions, it has other tasks related to diagnostics and error reporting of packets sending [6]. On the other hand, these new ICMPv6 mechanisms are accompanied by with new security vulnerabilities.

IPv6 networks are already being used for performing attacks, such as DoS attack [7]. This attack aims to prevent a legitimate user from accessing network services,

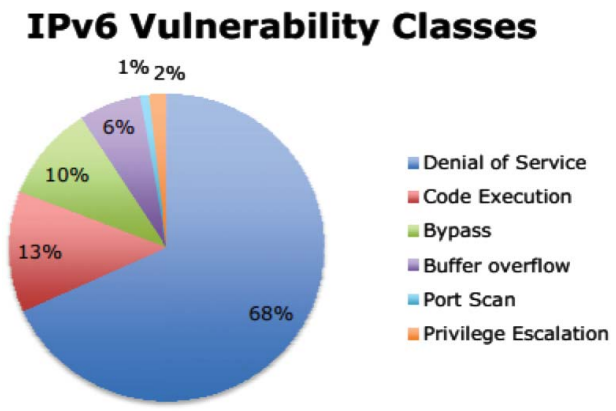

Figure 1: IPv6 vulnerability classes [8]

such as web, email, and online shopping. A report from the National Vulnerability Database showed that the majority of attacks against IPv6 are DoS attacks as illustrated in Figure 1. Another more serious DoS attack is called Distributed-DoS (DDoS) attack where the attack traffic comes from more than one address. These addresses can be fake; therefore, it is more difficult to identify the DDoS attacker's identity [9]. IPv6 DoS and DDoS attacks are considered as inherited attacks from IPv4.

These attacks can be remote attacks, where attackers remotely send their traffic to a vulnerable third party (zombie), with a spoofed source address (victim's address). Spoofing the addresses is possible in IPv6 as well as IPv4. As a result from the remote sending, the third party responds and replies to the victim, which causes a flood of traffic towards the victim [10]. Moreover, some of the new features of IPv6 make DoS and DDoS attacks much easier for attackers. For example, multicast addresses in IPv6 (e.g. All nodes have site-specific multicast addresses) provide a new easy way to launch a flooding DoS attack [11].

As a consequence, many approaches have been proposed to solve DoS and DDoS issues in IPv6 networks. Some of these approaches emphasize on preventing the attack before it actually happens and causes damages. The main advantage of this type of prevention is its ability to avoid the impact of destruction that might be caused by such an attack. IPv6 prevention approach is normally based on stopping source address spoofing, i.e. preventing address stealing or enforcing policies for network traffic [12]. Another type of approach tries to detect the attack based on active or passive techniques. Active techniques try to find out the impact of DoS or DDoS attacks as early as possible and respond to them. It also relies on its own network probing for its decision; hence, in active approaches, there is a possibility of causing network DoS itself. In contrast, passive techniques do not probe any packet, rather it only monitors the network and alarms operators of any potential attacks [13].

The rest of this paper is organized as follows: Section 2 explains the new improvements of IPv6 and their effects on networks security. Section 3 explains the importance of ICMPv6, and its security threats. Section 4 shows the most important task of ICMPv6 messages, which is neighbour discovery. In Section 5, we comprehensively classified and discussed the existing DoS and DDoS attacks based on ICMPv6 messages. Strengths and weaknesses of the proposed security mitigations of ICMPv6-based DoS and DDoS attacks are explained in Section 6. Section 7 lists the available IPv6 attacking tools and, finally, we conclude and highligh the future research directions in Section 8.

2. INTERNET PROTOCOL VERSION 6 (IPv6)

IPv6 is a network layer protocol of the standard OSI Model; hence, it only changes in the architecture of this layer without any changes in the other layers [14]. The main changes in IPv6 as compared to IPv4 are: first, the address of IPv6 is 128 bit, formatted as eight parts of six-bit integers that are separated by colons. IPv6 address space is 3.4×10^{38} IPs which is huge compared to IPv4 (4.2×10^{9} IP) [15]. IPv6 packet header format is changed to a fixed length of 40 bytes. Some fields of the new header are taken from the IPv4 format (same name or renamed) and others are new fields [16]. Moreover, IPv6 has the ability to provide quality of service when needed through the new field option, Flow Label [17]. Furthermore, the Next Header is a new field defined as a nested header to support six different options of sub-protocols.

IPv6 is designed to improve communication systems to keep pace with the huge need of IPs in the future. In addition to address this issue, IPv6 solved many issues that existed in IPv4, such as mobility and auto-configuration. On the other hand, IPv6 did not entirely solve issues of security. A typical example of an attack that affects IPv4 network as well as IPv6 network is the sniffing attack. The sniffing attack involves capturing data and information through network links to be misused especially when sent in plain text format [18]. Another common example of such attacks is the Flooding Attacks, also effecting IPv6. Flooding Attacks happen by overwhelming the victim with big amounts of packets which exceeds its tolerating ability. Moreover, IPv6 has new features which can help attackers in Flooding Attack

such as new extension headers, ICMPv6 messages and multicast address (e.g. all nodes are connected to one IP FF02::1) [19].

These new IPv6 features improved network security in many ways. For instance, IPsec protocol has been made mandatory in the IPv6 where it was optional in IPv4 [20]. In contrast, these IPv6 options result in new security threats to the networks and expose IPv6 to attacks based on these new features. Probing all the available IPv6 addresses in a network is impracticable in IPv6 compared to IPv4 due to the large number of possible IPv6 addresses. However, an attacker can use the multicast address feature as defined in RFC 2375 [21], such as the multicast address of All Routers (FF02::2). The attacker might send only one packet to All Routers multicast address and all available routers will reply to the packet, telling about its existence [22].

There is no perfectly secure IPv6 network area even if it is improved with several security features against attacks [23]. Another potential area of DoS and DDoS attacks is in the multi-functions of ICMPv6 [6] introduced in IPv6. ICMPv6 allows a host to perform neighbour discovery via Duplicate Address detection (DAD) as part of the process to automatically generate its IP address. Other functions include the discovery of Path Maximum Transmission Unit (PMTU), auto-configuration mechanism, address resolution, etc. Unfortunately, all these new features were designed for ease of use rather than for security purposes. Hence, the trust between soliciting and advertising hosts (routers and network devices alike) is not well taken care of. Thus, a malicious adversary can take advantage of this loophole to launch many types of attacks (including DoS and DDoS) [24].

3. INTERNET CONTROL MESSAGE PROTOCOL VERSION 6 (ICMPv6)

The Internet Control Message Protocol (ICMP) is part of IPv4 protocol suite [25]. It is used for diagnostic, testing, control purposes or generated in response to errors and to report problems in IP communication operations [26]. ICMPv4 is an optional and separated protocol from IPv4 communication protocols, while ICMPv6 is considered as an integral protocol, which works directly at the top of the IPv6 protocol [27]. The Next Header value for ICMPv6 messages is 58. ICMPv6 messages can be categorized into two categories namely, error messages with type value ranges from 1 to 127, and 128 to 255 for informational messages. Error messages are generated to report any errors that occur during the delivery of a message. Informational messages allow the sharing of required information between nodes to implement tests, diagnostics and support functions critical to the operations of IPv6.

ICMPv6 is the basic protocol in IPv6 networks and every node has to fully implement it to communicate using IPv6 because IPv6 network operations require the use of ICMPv6 messages for many important processes as described in RFC 4443 [6]. However, ICMPv6 protocol is considered as simple and has a lack of awareness of security. It is vulnerable to different types of attacks and exploitation, including DoS, Man in the Middle (MitM), and Scan attack [28]. There are security flaws in the current design of ICMPv6, such as the multicast addresses which can be misused by any user to perform reconnaissance attack by probing them. Blocking most of the ICMPv4 messages was a common practice in IPv4 network administrators, whereas, IPv6 networks cannot use this technique due to the important tasks of ICMPv6 messages (e.g. neighbour discovery, router discovery and path maximum transmission unit discovery mechanisms) [6].

4. NEIGHBOUR DISCOVERY PROTOCOL (NDP)

NDP is responsible for a group of important functions related to other IPv6 nodes based on ICMPv6 messages. For example, it is responsible for the auto-configuration process of IPv6 nodes. For instance, once an IPv6 node plugs-in to a network, it is able to generate its own IPv6 address automatically using NDP protocol [5]. Although NDP is a network layer protocol, it works for the communication of link local. The NDP mechanism depends on ICMPv6 code 0 messages exchange between hosts and host to router [6]. Exchanging NDP messages between nodes, which are ICMPv6 messages, can be misused for performing attacks. Therefore, understanding NDP working process helps in securing ICMPv6 protocol. NDP uses five types of ICMPv6 informational messages as explained in RFC 4861 [5] and shown in Table 1.

5. ICMPv6 DISTRIBUTED AND DENIAL OF SERVICE (DoS AND DDoS) ATTACKS

DoS attack is considered as one of the most serious problems in today's internet. DoS attacker aims to prevent a service or to limit access of a legitimated user to a network or server. Normally, this attack is performed by sending malformed packets to a victim's machine or overwhelming it with a large number of packets which exceeds its ability to handle them [29,30]. DDoS is a large-scale DOS and a more powerful technique to disrupt a user by sending the traffic from multiple

Table 1: NDP messages properties

Message name	Type	Sender	Receiver	Properties
Router solicitation (RS)	133	Nodes	All routers multicast-address (FF02::2)	Sent from hosts asking router to send router advertisement (RA) message
Router advertisement (RA)	134	Routers	If RS is sent: sender of the RS Otherwise: all-nodes multicast address (FF02::1)	Sent from routers periodically or in response to RS in order to advertise their presence and link-specific parameters, e.g. link prefixes, link MTU and hop limits
Neighbour solicitation (NS)	135	Nodes	Solicited node or target node	Sent by hosts to request another host's MAC address and for functions such as DAD and NUD processes
Neighbour advertisement (NA)	136	Nodes	If NS is sent: sender of the NS Otherwise: all-nodes multicast address (FF02::1)	Sent in response to NS messages. In addition, if a host changes its MAC address, it sends an unsolicited NA to advertise the new address
Redirect messages (RM)	137	Routers	Nodes	Sent from routers to redirect traffic of a user from one path to another better path

compromised source machines to its machine. This variety of sources makes the detection of the attack more complicated [2,6].

The only difference between DoS and DDoS attacks is in the manner of their execution. Basically, a DoS attack is launched from a single attacker's station by either exploiting vulnerabilities or flooding its victim. On the other hand, in DDoS attacks, multiple stations that can reach the victim are used in an action similar to DoS attack. These stations are known as botnets and can be spread around the world, making DDoS attacks harder to handle. Botnets are a group of stations infected by malicious software that allows a single station (attacker) to control them. Moreover, DoS and DDoS attacks can be sourced from fake addresses to make its detection and tracing more difficult.

IPv6 is already used in various real networks to route packets. For example, the number of users who reach Google server using IPv6 address equals to 8% of all users in August 2015 [31]. After IPv6 is practically deployed in real networks, many reports have shown that DoS and DDoS attacks are still possible in IPv6. A security report from Akamai organization showed that the number of DoS attacks in 2015 increased by 117% compared to 2014 [32]. Barker [33] and Yang et al. [34] showed that IPv6 is suffering from DoS attacks by performing different types of DoS attacks practically. ICMPv6 is already acquired as a media for DoS and DDoS attack [35]. Therefore, ICMPv6 protocol needs more security improvements.

In general, DoS attacks are broadly classified into different groups based on different criteria. In [29], DoS attacks are categorized based on four different criteria which include (1) degree of automation of the attacks, (2) exploited vulnerability of protocol, (3) rate dynamics of attacks, and (4) impact of the attacks. First, based on the degree of automation, DoS attacks are further classified into three subgroups: manual, semiautomatic, and automatic DoS attacks. Second, under the exploited vulnerability group, DoS attacks are classified into three classes: flood attacks, amplification attacks, protocol exploits attacks and malformed packet attacks. The third classification is based on the attack rate dynamics, which is either a continuous rate or a variable rate. The last classification studied the attack's impact on the targeted network. These impacts can be disruptive or slowly degrade the performance of the targets.

To provide a new perspective and insight about ICMPv6-based DoS and DDoS attacks, we classified them based on the exploited vulnerabilities used in the attacks. This is used because it is directly related to DoS and DDoS attacks. Therefore, ICMPv6 DoS attacks can be classified as shown in Figure 2. First, DoS attacks can be performed by flooding the victim with huge numbers of ICMPv6 packets. Second, an attacker can use Smurf or rSmurf (remote Smurf) way to overwhelm the victim, known as amplification attacks. Another way of DoS attack depends on the ICMPv6 protocol exploitation such as spoofing source address. ICMPv6 protocol

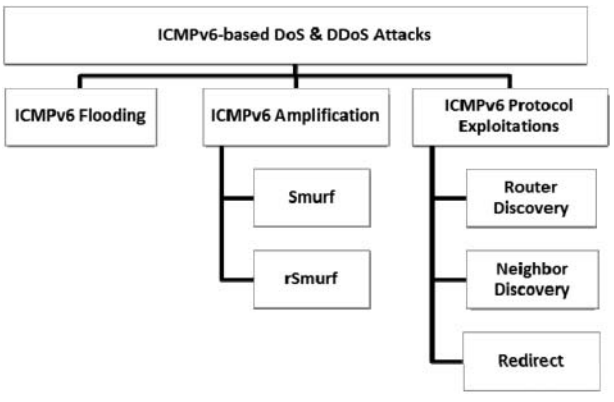

Figure 2: Categorization of ICMPv6-based DoS and DDoS attack

exploitation attacks are classified based on the messages used in them within redirect, neighbour discovery (NS, NA) and router discovery (RS, RA).

5.1 ICMPv6 Flooding DoS and DDoS Attack

ICMP flooding attack is considered as one of the most common attacks in both IPv4 and IPv6 networks. It aims to consume the bandwidth and resources of the targeted host or router by drowning it with an excessive amount of packets in a small period of time comparatively [11]. In such scenarios, the targeted device processes the received traffic as much as possible, eventually causing the victim to be busy in handling the huge amount of traffic and stops serving the legitimate packets.

Flooding attack aims to overwhelm the victim with big amounts of traffic. These traffic can be any ICMPv6 packets with a source address referring to another IPv6 node or to an used address [36]. Fabrication of source address is used to avoid being detected by any detection security mechanism. Practically, attackers can send a huge number of ICMPv6 error notification messages for both routers and hosts to distribute their functions. Nevertheless, they can send any ICMPv6 informational messages such as ECHO reply, ECHO request, router advertisement, neighbour advertisement (NA), neighbour solicitation (NS), and multicast listener discovery messages for the same purpose [37].

The results of each flooding DoS attack are distinct according to the nature of the used packets and the targeted victim. Some of them affect only the targeted node while others affect their victim plus other nodes. The second kind of flooding has more damaging effect to the network's efficiency. For example, in case the target was a host and the sent packets were NS from different addresses, typically the host is going to reply each packet with a NA packet. That causes a DoS attack (storm of NS) to the victim's machine as well as a storm of NA packets in the network, which usurps its bandwidth and other systems' CPUs.

5.2 Amplification ICMPv6-Based DoS and DDoS Attacks

Although IPv6 tried to eliminate most of the amplification attacks targeted in IPv4, there are still some possible techniques that allow attackers to perform DoS and DDoS amplification attacks. The mentioned techniques depend on the core ICMPv6 specifications, such as the multicast address which is a defined address representing a group of IPv6 addresses [38]. This type of attacks is named as amplification because it allows the attacker to generate excessive numbers of packets using a small number of packets. These packets are amplified to a large number of packets based on the multicast address feature. Amplification attack is considered as one of the unsolved threats common in IPv4 and still exists in IPv6 [39].

The most known example of amplification attacks is Smurf attacks based on the ICMPv6 multicast address function. In Smurf attack, a DoS attack is performed by sending an ECHO request packet to a multicast address with a spoofed source address referring to the victim's address. The packet is received by all subscriber nodes of the targeted multicast address, this causing all IPv6 addresses that are subscribed to the multicast group to reply to the spoofed address (victim IP) and flooding it with a large number of ECHO reply packets. Thus, the victim will be overwhelmed and cannot respond to the normal activities [40]. Figure 3 illustrates an example of Smurf attacks in the IPv6 network.

There is another type of ICMPv6 amplification attack called remote Smurf attack (rSmurf). rSmurf attack is used to deny the services from all targeted networks as follows: Attacker remotely sends an ECHO request packet sources from a multicast IPv6 address, such as

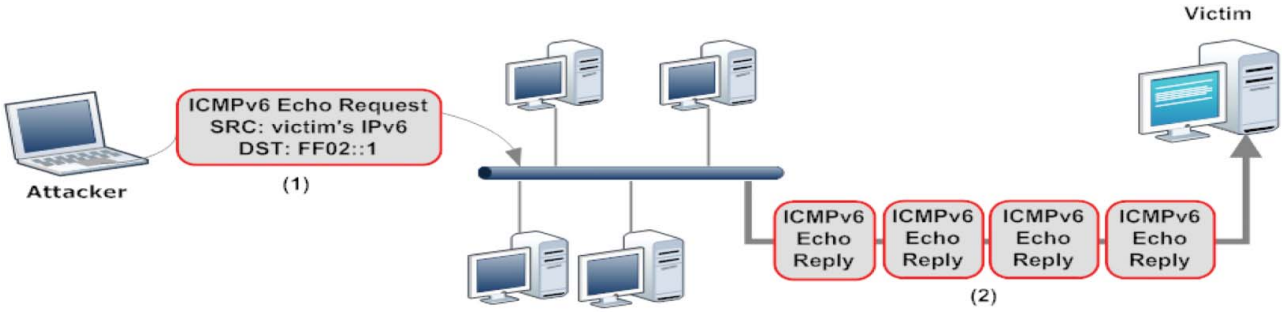

Figure 3: Smurf attack

FF02::1 with a destination address referring to an address in the targeted network. If the destination address exists, it will reply by sending an ECHO reply packet to the multicast address. That means a packet is sent to every node subscribed to the multicast group. As a consequence, a storm of traffic is generated in the victim's network from one malicious packet [7].

5.3 DoS and DDoS Attack Based on ICMPv6 Protocol Exploitation

This section focuses on DoS and DDoS attacks performed based on a misuse of ICMPv6 specifications. For example, any node can claim that it is a router by sending an ICMPv6 router advertisement (RA) packet. This feature allows attackers to perform MITM attacks by acting as a router for other users. The DoS and DDoS attacks are performed by misusing the ICMPv6 protocol features that are classified based on the packets used in the attack. First, DoS and DDoS use router discovery packets which are RS (ICMPv6 type 133) and RA (ICMPv6 type 134). Second, DoS and DDoS use neighbour discovery packets which are NS (ICMPv6 type 135) and NS (ICMPv6 type 136). Finally, DoS and DDoS attack using redirect packet (ICMPv6 type 137).

5.3.1 Router Discovery (Routing Related) DoS and DDoS Attacks

Router discovery process is related to the network layer which is responsible for packets routing. In IPv6, routing is initialized from hosts by sending an RS packet to all-routers multicast address (FF02::2). After that, an RA packet is going to be sent from the default router (the smallest metric router) to the host who sent the RS packet. Basically, RA packets contain information needed by hosts, such as specifications of the router, on-link prefix, and network parameters [14]. These two packets (RS and RA) can be used to launch attacks that are as follows:

- Default router is "killed"

Each node has to have a default routers table to list all the available routers (regularly sent RA packets) in its network. Once a node has no record in this table (means no available router), it will consider that all destinations are on-link [5]. Based on this fact, the attacker might cheat the victim by sending an RA packet with zero router lifetime with a spoofed source address (refers to the default gateway router of the node). When the victim is cheated, it is going to delete the router record because it believed that the lifetime of the router is zero and it will start to send all packets directly to the destination without a router. Thus, in the case of out-link destinations, a DoS attack happens between the victim and the real destination [1].

- Bogus address configuration prefix attack

Typically, when an IPv6 network does not have a DHCP server, nodes generate their own addresses based on the auto-configuration process using subnet prefixes of RA messages that are received from their default gateway router [24]. Mainly, routers send RA messages periodically to all node addresses to update their information. An attacker can craft an RA message with an invalid subnet prefix and send it to all nodes multicast address (FF02::1) in order to cheat them. After that, the prefix is used by the receivers to generate an invalid IPv6 address. As a result, this invalid IPv6 address will prevent the victim node from communicating with any other nodes (DoS attack) [34].

- Bogus on-link prefix

This attack also uses RA packet sent from an attacker. It is launched in the same way as the bogus address configuration prefix attack. However, in this attack, the crafted RA packet is used in order to convince the victim that an arbitrary length prefix is on-link (in fact, it is out-link). This basically means that whichever node that believes will never send any packet to one of the addresses that are generated from that prefix to the router because it believes that they reside on the same subnet. Thus, this causes a DoS attack between the victim and all addresses of the used prefix [14].

- Parameter spoofing

This attack also uses RA messages to cheat nodes. Basically, RA messages contain information and flags sent to nodes to be used for sending packets later and to know whether it has to use stateful address configuration or not [5]. These parameters can be forged by an attacker to prevent the victim from sending packets. In case the node believes the RA's wrong flags and uses it, it will be unable to send its packets. For example, an attacker sends an RA packet with a small value of hop limit which causes the drop of the packet before it reaches its destination [24].

5.3.2 Neighbour Discovery (Non-Routing Related) DoS and DDoS Attacks

Neighbour discovery depends on two types of ICMPv6 packets, which are NS and NA. These two messages are mainly responsible for the binding process between IPv6 address and MAC address, which was known as the Address Resolution Protocol (ARP) process in IPv4 [5].

In addition, the neighbour discovery process is used in other functions, such as neighbour unreachability and duplicate address detection. There are two DoS and DDoS attacks based on neighbour discovery process:

- Duplicate address detection DoS attack

Duplicate address detection (DAD) mechanism is used by a node when it needs a new IPv6 address. It sends an NS message to all nodes multicast address (FF02::1) to ensure that no one is using the requested address. If no node replies by NS packet, this technically means that the requested IP is not occupied and it can be used [41]. Based on this mechanism, attackers can respond each time to the victim's NS packets by replying with NA packets claiming that it is using the requested IPv6 address. Another way to reply is by sending an NS packet pretending that it is performing NS to the same requested address. Consequently, the node (victim) is prevented from getting an IP address, which means it cannot communicate with others and a DoS is performed against it [28].

- Neighbour unreachability detection failure

Neighbour unreachability detection (NUD) is a procedure invoked by a node when it stops receiving replies from a peer node for a while. The node sends an NS packet for the lost node address and waits for an NA reply from it for a period of time. If nothing is received, it will resend for a few more times, and when no NA is received, it deletes the peer node record from its neighbour cache table [41]. The DoS attack can be launched if a malicious node replies to each NS with an NA packet claiming that the node is still active (but is indeed unreachable) [34].

5.3.3 Redirect DoS and DDoS Attacks

Redirect message is an ICMPv6 message used to inform nodes about a better path to a particular destination. Router sends a redirect packet to a node to optimize the routing process of its packet [42]. Nodes accept the redirect message when it comes from the MAC address of its first hop router. Unfortunately, an attacker can fabricate a redirect message to be sourced with the MAC address of the first hop router of the victim in order to convince it [43]. This attack causes DoS in two ways:

- Victim's traffic can be redirected to a non-existent MAC address that will prevent a legitimated user from communicating with others, resulting in DoS.
- Large amounts of data can be redirected to an existing MAC address (victim), therefore overwhelming it to consume its resources. This results in another kind of DoS.

DoS and DDoS attacks are still possible in IPv6 in many techniques. Some of these techniques were similar in IPv4 and are known as inherited techniques, while others are attached with the new features which came with IPv6 protocol. The most used vulnerability in IPv6 for performing DoS or DDoS attacks is ICMPv6 vulnerabilities which cannot be disabled in networks (as was a common practice in IPv4) due to its importance. Therefore, ICMPv6 needs more security adjustments as well as protection against these attacks to avoid the threats that might be used to attack IPv6 networks. In this section, ICMPv6 DoS and DDoS attacks are classified based on their exploitation as shown in Figure 2. This classification is useful for interested readers to give them a new perspective on ICMPv6 attacks and help them understand what security requirements should be available in any ICMPv6 detection or protection technique.

6. EXISTING DEFENSE MECHANISMS OF ICMPv6-BASED DoS and DDoS

As mentioned in Section 5, IPv6 is vulnerable to DoS and DDoS attacks based on ICMPv6 packets. These vulnerabilities forced the developers of IPv6 to include security mechanisms in IPv6 protocol-based communication. The most common mechanism is IP Security (IPSec), which is an integrated part installed within IPv6 protocol, unlike IPv4 [14]. Even though IPSec provides end-to-end security level, it cannot be trustworthy due to its problem of bootstrapping [44]. Therefore, many security approaches were proposed to mitigate IPv6 threats generally and some were proposed specifically for DoS and DDoS attacks. For example, IETF proposed an extension for NDP protocol called secure neighbour discovery (SeND) [45] to protect all ICMPv6 packets used in NDP functionalities. This section provides a comprehensive classification of the proposed approaches based on analyzing their implantations as well as the actions taken against attackers. Thus, the defense mechanisms were mainly classified into prevention and detection approaches. Figure 4 portrays the classification of ICMPv6-based DoS and DDoS attacks' defense mechanisms.

6.1 Prevention Approaches for ICMPv6-Based DoS and DDoS Attacks

In general, DoS or DDoS attack is not considered as a stand-alone attack due to its dependence on other attacks. In other words, an attacker needs to perform

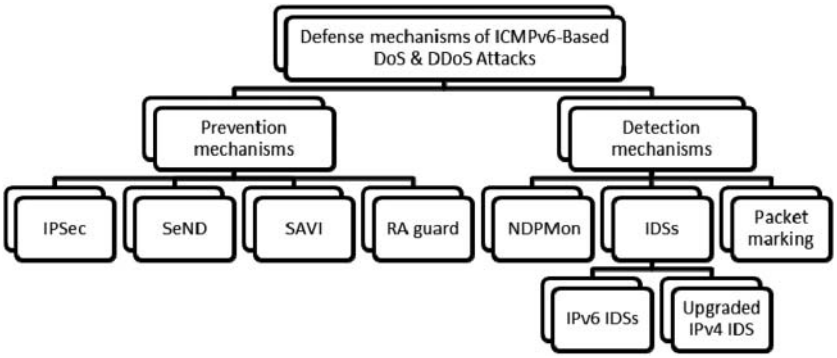

Figure 4: Classification of ICMPv6-based DoS and DDoS attacks defense mechanisms

other attacks before performing a DoS or DDoS attack. If these attacks succeed in redirecting a user's traffic to a non-existing node or address, it will definitely result in DoS about that user. Typical examples of these attacks are IPv6 address spoofing, neighbour discovery poisoning, MAC address spoofing, MITM attacks, etc. Therefore, early prevention of these attacks makes DoS and DDoS attacks more difficult for attackers [1].

Attack prevention approaches aim to stop an attack before it happens. These approaches assume that the source address of the malicious traffic might be spoofed, which is true in many situations of IPv6 attacks. Address spoofing is used by attackers to hide their addresses in order to avoid detection [46]. Another common assumption is that even the MAC address can be spoofed in order to convince a node to accept some malicious traffic. Therefore, most prevention techniques try to ensure that addresses are not spoofed [1]. However, it is a difficult task to define a filtering rule which is able to differentiate malicious traffic from legitimate traffic accurately. ICMPv6-based DoS mitigation methods can be summarized as follows:

- Internet Protocol Security (IPSec)

IPSec is the first prevention technique for IPv6 protocol. It aims to provide IPv6 packets with authentication, integrity, and confidentiality. IPsec utilizes two sub-protocols, Encapsulation Security Payload (ESP) and Authentication Header (AH), to provide the required security. IPsec requires information about the two communicating nodes before providing any security to the communication. Security association (SA) is the required information that describes how the security looks between the two nodes. SA defined a number of attributes, including secret keys [47]. ICMPv6 DoS attacks can be prevented using IPSec based on the fact that these attacks are performed using spoofed source addresses [34]. The full details of IPSec can be found in [48]. Notwithstanding all the advantages of IPsec, it still cannot be considered as a trustworthy mechanism due to its shortcomings. In [34], the author tested IPv6 network with IPSec installed and concluded that IPSec cannot solve security problems of IPv6 attacks including DoS and DDoS attacks. Moreover, a number of researches have highlighted disadvantages of IPSec which can be summarized as follows:

(1) IPSec depends on Internet Key Exchange (IKE) which needs a valid IPv6 address. This IP address cannot be provided during the initial phase of a new IP generation process. This basically means that the ICMPv6 messages, which are used to get a new IPv6 address, will be sent without provided security from IPSec [14].
(2) Most of the IPv6 users do not implement IPSec because of the lack of knowledge about its configuration and management [4].
(3) Using IPv6 makes the network administrator a blind monitor because all the traffic is sent encrypted. Thus, the administrators cannot monitor the network or even apply any policies or rules between any two IPv6 nodes [39].
(4) The cryptography used by IPSec is rather complex and costs high resource consumption due to the increased number of headers added by it [49].

- Secure Neighbour Discovery (SeND)

RFC 3971 [45] defines SeND approach as an internet security standard that protects NDP messages. SeND introduces options to be added to NDP header which are, first, Cryptographically Generated Addresses (CGA) option to prevent address spoofing based on the public–private key to be generated by all nodes. CGA is an option used by SeND to verify the ownerships of the used addresses by generated a new IP addresses based on a one-way hash function applied on a public key from

the node and other parameters such as network prefix. Receivers verify the binding between the generated CGA and IPv6 address by using the same one-way hash function. It is believed that SeND stops addresses spoofing based on this option.

Another two options are nonce and timestamp to prevent replay attacks against bi-directional messages such as NS/NA and uni-directional messages such as unsolicited RAs and redirects, respectively. The last option is Rivest-Shamir-Adleman (RSA) signature option which aims to provide integrity and authentication to the identity of source address. Therefore, nodes have a pair of RSA public and private keys and NDP messages are signed with RSA option [50]. In spite of all the security options offered by SeND protocol, it is still uncommonly used as a security mechanism. One of the reasons for not being widely deployed is the lack of implementation knowledge offered in the RFC. This encouraged the researchers to do more analysis and test for SeND practically.

Authors of [51] studied ICMP message in four scenarios, including ICMPv4, pure NDP, SeND without RSA, and full SeND. The conclusion of their study showed that SeND increases the processing time of NDP messages by 99% compared to pure NDP. Moreover, it showed that RSA signature is the main factor in increasing the processing time of SeND, which is a main part of it for ensuring integrity and authenticity of packets and SeND is useless without RSA. Another work in [52] reviewed the CGA option with different Sec bit values (used in CGA computation). It showed that the CGA option increased the computational time, especially when Sec value is larger than 1. It also showed that SeND increases the bandwidth consumption where it adds more than 1 kbit overload for each packet.

In addition to the long processing time and bandwidth consumption of SeND, it has other disadvantages. One of them, based on the complex processes of SeND that are used to calculate its option values, might cause DoS attacks. Usually, SeND node proceeds 442 NS messages in 1.43 second [53]. Based on this fact, an attacker can send large amounts of packets to its victim with the four SeND options, forcing it to handle the packets. The victim will be busy handling that amount of packets and stop serving other packets. Moreover, the CGA cannot verify the real identity of users and is also insufficient to ensure CGA address that belongs to a particular node. Therefore, an attacker can change the CGA parameters and steal NDP messages.

- Source Address Validation Improvement (SAVI)

SAVI is a prevention technique against address spoofing in IPv6 that was proposed in 2013 by a number of researchers from Tsinghua University [54]. The idea of this technique is to build an information anchor to store trusted details such as port number and MAC address in each IPv6 node. SAVI prevents address spoofing by binding each switch's physical port with an IPv6 source address or binding each MAC address, IPv6 address, and switch port together. Based on this binding, SAVI filters traffic in the switches and only forwards the packets with correctly matched details according to the stored information. Moreover, it has been combined with other prevention techniques to improve its efficiency. For example, it has been implemented with SeND in [55,56] to protect link-local addresses spoofing.

SAVI has possible threats and limitation challenges that are preventing it from being applied in real networks. Some of these threats and challenges are explained in RFC 6959 [57]. For example, applying SAVI could be a major problem with Stateless Address Auto-Configuration (SLAAC) due to nodes' changing of addresses. Moreover, it is normal for IPv6 devices to have more than one IPv6 address; therefore, SAVI binding is difficult to be implemented in cases of multiple address devices. Another discouraging threat is that each SAVI device works individually without any information exchange between them. As a result, it exposes SAVI devices to traffic spoofing when it is connected to a vulnerable device [58]. Finally, SAVI cannot handle flooding DoS or DDoS attack when it is launched by the real identity of the attacker (registered in the anchor).

- Router Advertisement guard (RA guard)

RA guard technique is proposed and explained in RFC 6105 [59] in 2011 to handle threats of RA messages. RA guard is installed in layer-2 switches to filter traffic based on certain criteria. It compares its criteria with some information extracted from IPv6 frames, such as MAC source address, physical port, IPv6 source, and prefix list. If the switch receives an RA message, it will decide to discard or forward it based on the comparison result. Therefore, rules are needed to be applied to the switch in order to determine the port that is connected to a router so RA is allowed from it. The determination can be based either on layer 2 configurations with configured access rules or on dynamically learning procedures of RA senders during a learning period. Thus, RA Guard prevents DoS attacks that are based on RA messages only and this is one of its drawbacks. Moreover, it has more shortcomings as explained in [60,61] that prevented its implementation in IPv6 network. Those limitations are:

(1) RA guard cannot provide any security protection for devices connecting without cables such as Wi-Fi devices.
(2) RA guard does not offer protection for the egress direction of traffic where it only monitors ingress traffic in switch ports.
(3) RA guard cannot be used on trunk ports with merge mode of ports.
(4) RA guard filtration can be spanned using different extension header values. An attacker can use an extension header to make it impossible for a layer-2 device to identify ICMPv6 router advertisements.
(5) Common and cheap switches do not support RA guard functionalities; therefore, the network administrator needs to buy new expensive switches.

The first proposed approach is IPSec, which is an integrated part of IPv6 protocol aimed to prevent such DoS and DDoS attacks. IPSec suffers from implementation drawbacks, such as key exchanging problems during its bootstrapping stage. Few prevention approaches were proposed to replace IPSec. Some of them failed to be trusted security mechanisms due to performance issues. For instance, SeND approach uses complex signature options and encryption methods which might take a long time to prepare a single packet before sending. Other approaches, such as SAVI and RA Guard, tried to avoid the complexity of encryption by applying rules on network traffic. The SAVI approach tried to stop address spoofing by binding MAC and IPv6 addresses. Nevertheless, normally an NIC card has more than one IPv6 address with the same Mac address, which is not allowed in SAVI. Therefore, it is an impractical approach. RA guard works only against RA messages' attacks by applying rules on them to be allowed only from a certain physical port of the switch. Moreover, these kinds of rules are only available in special switches where they are not supported in common and popular switches.

6.2 Detection Approaches for ICMPv6-Based DoS and DDoS Attacks

After reviewing state-of-the-art prevention mechanisms for preventing DoS and DDoS attacks, this section presents another type of solutions which is attacks detection. DoS and DDoS attack detection is needed due to several reasons. First, detecting DoS or DDoS attacks before their actual damage helps legitimate users to get more time to take proper reaction. Second, attacks detection helps in identifying the attacker, and hence legal actions can be taken against them. Finally, detecting attacks reduces bandwidth consumption that could be wasted by the malicious traffic. In this section, the existing detection techniques that are defending against ICMPv6 DoS and DDoS attacks are discussed.

- NDP Monitoring (NDPMon)

NDPMon [62] is a software tool developed based on ArpWatch [63] which was used in IPv4 network monitoring. NDPMon uses a passive technique aimed to detect NDP-based attacks, including DoS attack by monitoring NDP activities in networks, such as the appearance of a new address, non-local source address, Ethernet address mismatch, node changes its Ethernet address, node keeps changing between two different IPv6 address, and node using old Ethernet address. NDPMon constructs a database of NDP messages to learn the legitimated activities allowed in the network. After this learning phase, any suspicious activity will be reported to the administrator.

NDPMon requires some information from the network administrator about its network before it starts to work. This information can be a list of legitimated routers in the network and a list of authorized network prefix. Moreover, it needs a long time before being applied to a network for the learning phase. In case an attack with a spoofed address started before the NDPMon tool, the databases will record the spoofed addresses as legitimated addresses that will lead to false alarms [64]. In addition, an experiment conducted by Herrera [65] showed that NDPMon failed to detect DAD-based DoS and spoofed RA/NA attacks.

- Intrusion Detection System (IDS)

The presence of IPv6 threats brings new demands for network protecting mechanisms against them. One of the possible choices that might work in IPv6 network is IPv4 IDSs, but it needs some adaptation to handle new functions of IPv6, such as neighbour discovery, router discovery, and auto-configuration process [66]. Another choice is to propose new IDSs that work exclusively for IPv6 networks. Therefore, IDSs that support IPv6 came in two main categories. The first category is an upgraded version from IPv4's IDSs which is able to solve IPv6-specific threats. The second category contains new approaches that are developed recently to solve IPv6 security issues. These IDSs do not support IPv4 attacks.

  - IPv6 IDSs

As aforementioned, IPv6 brought new main features that are different from IPv4. Thus, most of IPv4 IDSs can no

longer be used efficiently in IPv6. These differences open the door for researches to propose new IDSs exclusively for IPv6 threats. There are two new IPv6 IDS approaches that have been proposed to detect ICMPv6 NA and NS addresses spoofing. They depend on the anomaly of IPv6 attacks, such as a mismatching between IP−Mac pairs to detect addresses spoofing.

- ✓ The first approach was proposed by Barbhuiya et al. [44] based on active techniques. This approach defines two main algorithms called NS handler and NA handler to detect spoofing of NS and NA source addresses, respectively. Also, it stores information extracted from network traffic in six database tables, named as NS table, NA table, probe table, authenticated table, log table, and unsolicited table. It sends a probe packet to validate a non-recorded pair of MAC−IP of NA or NS packet.
- ✓ A similar active technique was proposed by Bansal et al. [67] based on Multicast Listener Discovery (MLD) protocol to detect spoofing of ICMPv6 NA or NS source addresses. MLD is used in IPv6 networks by routers to know the listener for each multicast address. Since this approach uses MLD, it does not add any traffic overload to the network because MLD is already an existing protocol in IPv6 networks. It uses four tables which are IP−MAC table, DAD table, DOS table, and log table to collect extracted information from the network traffic.

These two active mechanisms use many tables in addition to the already existing tables of NDP process. NDP process has four tables which are the neighbour chase, destination chase, default routers list, and prefix list. Barbhuiya et al. approach adds six more tables, while Bansal et al. approach adds four tables, so there are at least eight tables in each IPv6 node to prevent DoS and DDoS attacks. These tables add an overload to the nodes' CPU resources as well as consume more processing time. Moreover, there are other DoS threats that can be launched by other than NA and NS packets (such as RA and RS) which are not included here. Also, false-positive alarms can be reported in case of a change in node's NIC because that creates a conflict between MAC and IPv6 addresses. Additionally, fragmenting the ICMPv6 packets can be used to evade these detection mechanisms [68,69].

- ○ Upgraded IPv4 IDSs

In addition to the new IDSs for IPv6, a few IPv4 IDSs were upgraded to support IPv6 and detect the new attacks. So far, there is little effort to expand the current set of IDSs to support IPv6 protocol [25] due to the lack of demand by IPv6 users and due to the lack of experience in industrial companies that develop IDSs. Owners of three IPv4 IDSs have upgraded their tools to support IPv6 networks which are Snort, BRO, and Suricata. This subsection explains more about these three IDSs.

- ✓ *Snort* [70] is an open source, flexible, multi-platform IDS developed by Sourcefire. It detects intrusion based on the two common detection techniques which are attack signature and anomaly. It is considered as one of the most commonly deployed IDS tools worldwide [71]. Snort architecture consists of four stages as shown in Figure 5. First, the packets decoder stage which is used to fit the captured traffic into the data structure needed by the next stage. The preprocessor stage is the most important stage where it identifies suspicious activities (listed in [72]) in the network. The third stage is the detection engine that is used to identify patterns based on a rule text file updated by a Snort user. The last stage is responsible for formatting and sending alert notifications to the user.

A few reviews and evaluations have been done on Snort for detecting IPv6 attacks. Schütte [73] concluded that Snort cannot solve fundamental problems such as DoS and insecure Ethernet. Moreover, Atlasis and Rey [74] discussed Snort issues and showed that it can be evaded in two ways: (1) if the number of fragments sent is more than 10 even if the Next Header of the last fragment was wrong; (2) if nine or more destination option headers are used and sent in an unfragmented packet. Another review was done by Gehrke [75] by conducting different

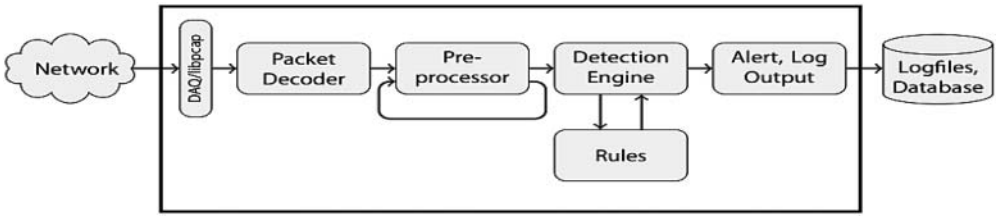

Figure 5: Snort IDS architecture [73]

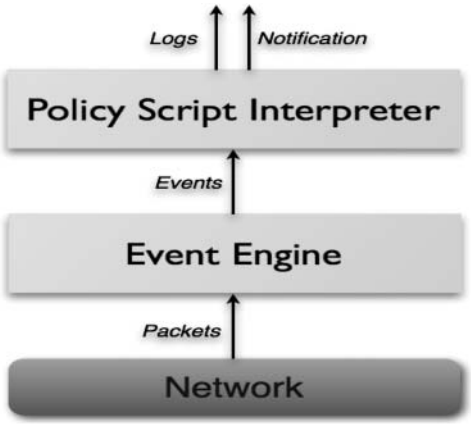

Figure 6: BRO IDS architecture

attacks in a network with Snort IDS installed. It showed that Snort detected only 52% of the attacks where it did not detect attacks such as DoS attack by announcing fake router using a fabricated RA message.

- *BRO* [23] is an open source, Unix-based IDS that detects attacks by passively monitoring a network traffic, looking for any suspicious activities. It extracts application-level semantics from the network traffic, and then compares the extracted activities to patterns that are considered as suspicions [76]. BRO works based on three stages as shown in Figure 6, starting with the capturing of packets from the network concerned. Then, the event engine stage checks the packet header to ensure that it is well formatted. In addition, it generates an event in case of intrusion signature matching. At the last stage, it executes a script written by BRO's special language and generates notifications if a match happens [77].

BRO started to support IPv6 since version 0.8 was released in 2003. In order to know how valid it is for IPv6, a few researchers conducted experiments on it. One of them was conducted on snorts, also by Gehrke [75]. It showed that BRO detected only 8% of the performed attacks, less than Snort. Moreover, it concluded that BRO is not yet ready to be trusted for the detection of IPv6 attacks. In Gehrke's experiment, BRO failed to detect many DoS attacks, such as flooding and rogue routers. Moya [77], in his experiment, showed that BRO is a slow IDS, by measuring the time needed by it and Snort to handle particular rules. He concluded that BRO needs more than double the time Snort needs to analyse the same rules.

- *Suricata* [78] is an open source IDS, developed by the Open Information Security Foundation (OISF). Suricata is considered as one of the fastest IDSs due to the multithreading techniques that are used in its detection. Moreover, it uses both signature- and anomaly-based detection techniques [79]. It aims to replace Snort by overcoming its development and architecture limitations. Therefore, it introduced new and experimental features, such as parallelism and multicore support, within its implementations. As shown in Figure 7, it uses the same concept of stages in Snort except that it executes the detection pipeline stage in separated threads.

Several tests were conducted to test Suricata in Atlasis and Rey [74]. It found out that it can be evaded in the following cases: (1) if an IPv6 destination option header is used as a part of the fragmented packet; (2) if it is padded with more than six octets of bytes in the end; (3) or, the datagram is fragmented into more than seven pieces and sent out of order. Moreover, nested fragmentation and transferring big amounts of arbitrary data cannot be successfully detected by Suricata as mentioned in [80]. Moreover, Suricata has a big memory usage compared to the other two IDSs as shown in an experiment accomplished by Pihelgas [81].

➢ Packet marking

Usually, DoS and DDoS attackers hide their identities to make the detection process more difficult and cause more damages to a victim. Attackers can easily spoof IPv6 addresses and use fake addresses instead of them.

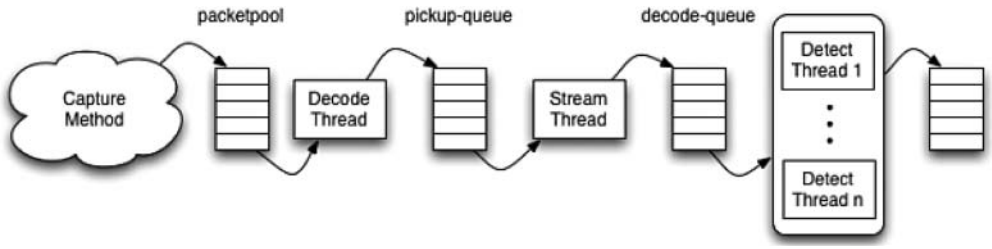

Figure 7: Suricata IDS architecture

Table 2: Summary of the existing defense approaches

Approach name	Issues
	Prevention approaches
Internet Protocol Security (IPSec) [83]	• Key exchange problem in bootstrapping • Knowledge limitations of its configuration and management • Makes network administrator as a blind monitor • Use complex cryptography
Secure Neighbour Discovery (SeND) [45]	• Too complex • Consumes more bandwidth • Lack of source addresses validation • Not applicable for all OS • It can be the reason for DoS attacks
Source Address Validation Improvement (SAVI) [54]	• Once anchor is spoofed, SAVI opens new attack vector • Hard to be implemented in case of multiple address devices and stateless auto-configuration • Useless when DoS comes from real IPv6 address
Router Advertisement Guard (RA Guard) [59]	• Cannot be used on trunk ports • Common and cheap switches do not support RA guard functionalities • Does not support non-cable devices • Works only against RA messages DoS and DDoS attacks of egress direction traffic
	Detection approaches
NDP Monitoring (NDPMon) [62]	• Depends on network administrator to give information • Learning phase needs a long time • Can be falsified if attacks started before applying it
IPv6 IDSs [44,67]	• Add more overload to CPU and resources • Add more time for NDP process • Work only against NS/NA messages DoS attack • NIC address changing causes false positive alarm • Can be avoided using fragmentation header
Upgraded IPv4 IDSs [23,72,78]	• Some of them cannot detect DoS and DDoS attack such as Snort and BRO. • Can be evaded using extension header, fragmentation, and destination header options. • Consumes large amount of memory such as Suricata • Need a long time to analysis its rules such as BRO.
Packet Marking [82]	• Add overload in routers • Useless when attack perfumed by real address or insider attack • Time gap between detection and learning phase

Based on these facts, An and Kim proposed a DoS detection approach called Real-Time IP Checking and Packet Marking [82]. It depends on routers for classifying packets as normal and abnormal based on their addresses. Since NDP protocol is a local protocol, IPv6 addresses in its header should be for local nodes. Based on this fact, the approach marks a packet as normal in case it belongs to a used local address; otherwise, it is suspicious. For suspicious packets, the router stores them in a packet buffer, and then sends an NS packet to ensure that its address really exists or is not based on the reply.

An and Kim approach supports the provision of quality of services feature to the traffic based on the proven priority from the approach. Packets with known IPv6 addresses (used in the network) get a high-priority treatment while the packets with unknown IPv6 addresses (not used in the network) get lower priority and can be discarded. However, this approach has many shortcomings, such as it adds more tasks to routers by queueing the packets, sending NS packets and then waits for the replies. This overload exposes routers to DoS attacks. Moreover, in case a DoS attack is performed from a real user's address, it cannot be detected. Additionally, there is a time needed for the learning phase to build node IP table by the router before the real detection starts. Thus, attacks can be launched within this time gap.

Table 2 summarizes the existing approaches and tools that are proposed to solve ICMPv6-based DoS and DDoS attacks.

6.3. Summary

After researchers and security companies realized that there is a real need to secure ICMPv6 messages and IPv6 protocol in general, they started to take actions to propose security solutions for such a problem. Some of these solutions depend on cryptography to avoid spoofing of IPv6 addresses. However, evaluations of such solutions showed that they suffered from time consumption and can be themselves the reason for the DoS and DDoS. Other researches applied specific rules as solutions in network traffic to either prevent the attacks or detect any attempts by monitoring the traffic. These kinds of researches suffer from low accuracy because they do not consider all features of attacks, which contribute in detecting DoS and DDoS attacks. Furthermore, a few solutions were proposed to work against a specific kind of DoS and DDoS attack. Thus, they cannot be generalized as standard securing mechanisms.

Table 3: Existing tools for ICMPv6-based DoS and DDoS attacks

The Hacker's Choice (THC) IPv6 [84]	
A complete toolkit developed by Marc Heuse for testing purpose. THC is considered as the most common IPv6 testing tool. It has the ability to perform several kinds of IPv6 attacks, including DoS and DDoS. THC depends on many command lines; each of them performs for different kind of attacks. Some of these commands perform DoS or DDoS attacks	Fake_router6: sends a RA message with the highest priority (small metric) to a victim announcing itself as a router Redir6: redirects victim's traffic to attacker node. It results in a DoS attack when no valid router MAC address is specified in the redirect packet to handle the traffic Dos-new-ip6: performs DAD-DoS attack by replying any NS packets asking about an address to use. The attacker claims that it is using that IPv6 address each time Flood_router6, Flood_advertise6/26 and Flood_solicitate6: overwhelms a targeted network with a big number of RA, NA, and NS, respectively. The packets are sent from fake source addresses to FF02::1 Smurf6: performs smurf DoS attack by sending packet to FF02::1 with spoofed source address (refers to a victim address) Rsmurf6: performs remote DoS attack to a victim network by sending spoofed packet from source address FF02::1 Denial6: sends huge number of packets to particular IPv6 address to cause DoS attack to that IPv6
Tribe Flood Network (TFN *and TFN2k) [85]*	
TFN is a command line interface tool. TFN2k is considered as more advanced version of TFN as it can launch attacks from spoofed source address [86]	Both tools have the ability to perform various DoS attacks such as ICMP flood, and Smurf attack in IPv6 network using command lines. For example: 'i' command in TFN2K performs Smurf to a victim IPv6 address
SI6 network [87]	
SI6is a set of IPv6 testing and troubleshooting toolkit. It can send arbitrary packets, including ICMPv6 messages. Therefore, attackers can fabricate a malicious packet using it to perform DoS attack	It has the ability to alter and send all ICMPv6 messages with the following commands: ICMP6: used to perform attacks based on error messages Na6, Ni6, Ns6, Ra6, Rd6, Rs6: alters and sends NA, ICMPv6, NS, RA, redirect, and RS messages, respectively
Evil Foca [88]	
Evil Foca is a GUI attacking tool, performs attacks in both IPv4 and IPv6 protocols. It is capable of performing DoS and MITM attacks	Evil Foca provides the user the ability to perform DoS attack based on Stateless address auto-configuration (SLAAC). It sends a vast number of RA packets to the victim IPv6 address from fake source addresses
Scapy [89]	
Scapy is a Python-based packet manipulation program. It does not impose any semantic rules, so the programmer is free to build packets in any way which can be illegal packets	It is used to create any type of packets (realistic and unrealistic). Used to manipulate fragmentation and Next Headers in order to avoid some detection methods such as IDS. Moreover, it can be used for flooding attack where it is able to send hundreds of packets per second
Router advertisement Daemon RADVD [90]	
RADVD is a Linux open source tool used to send RA messages. Users can specify network prefix, lifetime, and frequency of sending RA messages	Since RADVD gives the chance to send RA messages, it can be used in a malicious faith by sending fabricated RA messages to fraud the victim. This mechanism performs DoS attack by announcing a bad prefix to the users convincing them to generate invalid IPv6 addresses for them [91]

This review of all the proposed solutions shows that each one has its drawbacks in detecting DoS and DDoS attacks. Table 2 lists some of these drawbacks. We concluded that there is still much work to be done before the existing solutions are ready to meet the demands of everyday consumption. Also, by reviewing the existing solutions, we realized that each solution has its strengths in many ways of securing IPv6 networks. Therefore, DoS and DDoS might be solved if one or more of the available mechanisms form a hybrid, which might contribute to the detection process and gain a better security mechanism. This hybridization should take advantages of the strengths as well avoid the drawbacks of the existing techniques.

7. EXISTING TOOLS FOR ICMPv6-BASED DOS AND DDOS ATTACKS

There are several tools available to launch DoS and DDoS attacks in IPv6 network based on ICMPv6 packets. Some of these tools were proposed in good faith to conduct testing and validation purposes by researchers who propose new securing mechanisms. Meanwhile, bad faith hackers developed other tools for attacking purposes including DoS and DDoS. Moreover, all these tools are available online and can be easily obtained to be used in performing these attacks. Table 3 summarizes some of the most commonly and efficiently used tools.

8. CONCLUSIONS

Blocking ICMP protocol was a commonly used action in IPv4 networks to avoid its vulnerabilities. In contrast, it cannot be totally clocked in IPv6 networks due to its important functionalities which are compulsory for any IPv6 node to use IPv6 probably [7]. Unfortunately, ICMPv6 is abused for malicious purposes in order to attack IPv6 networks. Undoubtedly, one of the most serious attacks is DoS and DDoS, which can be based on ICMPv6 messages where it has adverse effects on network functionality. ICMPv6 messages can be used to

deny networks' services in many ways, such as flooding attack which negatively affects networks' performance.

In this paper, we have tried to show a clear view of DoS and DDoS attacks based on ICMPv6 messages and the numerous defense solutions that have been proposed for such attacks. This clear view of the problem helps in finding more effective solutions to solve such a security problem. This paper presents different scopes of ICMPv6 security issues and specifically DoS and DDoS attacks using ICMPv6 messages. Additionally, it categorizes ICMPv6-based DoS and DDoS attacks into three main categories based on ICMPv6 protocol exploited vulnerabilities. Several existing approached that were proposed to mitigate these attacks were investigated by showing the strengths and drawbacks of each one. The existing approaches were classified in this review according to their actions against the attacks where it can be a prevention or detection reaction.

As a main conclusion, ICMPv6 protocol is still vulnerable to DoS and DDoS attacks using different techniques due to the shortcomings of its current defense mechanisms. Furthermore, some of the existing mechanisms can be the reason for DoS or DDoS attack themselves, such as SeND approach. Therefore, ICMPv6 security vulnerabilities must be considered prior to any real deployment of any solutions. Thus, in this work, a survey to improve the understanding of the detection methodologies of ICMPv6-based DoS and DDoS attacks is presented with a focus on the open issues within each category of the detection taxonomy provided earlier.

This literature provides evidence to many cases where the existing approaches still have some limitations related to the performance complexity and the covered attacks. Therefore, there is still a need for new approaches toward the detection of ICMPv6-based DoS and DDoS attacks. This review also shows that each of the existing approaches has its strength in many ways as well as its weaknesses. Therefore, from reviewing the existing solutions, we are suggesting a combination of two or more of the existing techniques to take advantage of their strengths as well as avoid their weaknesses. Hybridization of two or more of the existing approaches may help the research community to produce better tools and techniques for mitigating the threat of ICMPv6-based DoS and DDoS attacks.

In addition, Artificial Intelligence (AI) is the only area which has not been applied for proposing mitigation mechanisms for such ICMPv6-based DoS and DDoS attacks. AI techniques were being widely used by IDS researchers in IPv4 due to their capabilities and proved their efficiency in such problems. Therefore, the AI trend has the potential to be a promising area to be applied in order to get a novel and efficient mitigation mechanism. Moreover, the AI technique helps IDS systems to detect unknown attacks where it has the ability to detect intrusions that have not been seen before, which are called "Zero Day" attacks. This feature is important for IDSs to be able to predict future attacks as well as reduce false alarm rates.

ACKNOWLEDGMENTS

This research was supported by the Short Term Research Grant, Universiti Sains Malaysia (USM) No: 304/PNAV/6313272.

REFERENCES

1. N. Tripathi, "DoS and DDoS attacks: Impact, analysis and countermeasures," 2013.
2. R. M. Saad, S. Ramadass, and S. Manickam, "A study on detecting ICMPv6 flooding attack based on IDs," *Australian J. Basic Appl. Sci.*, Vol. 7, no. 2, pp. 175–81, Feb. 2013.
3. A. Research, "The internet of things will drive wireless connected devices to 40.9 billion in 2020 | ABI research," *ABI Res.*, 2014. Available: https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect/
4. C. E. Caicedo, J. B. Joshi, and S. R. Tuladhar, "IPv6 security challenges," *Computer*, no. 2, pp. 36–42, 2009.
5. T. Narten, W. A. Simpson, E. Nordmark, and H. Soliman, "Neighbor discovery for IP version 6 (IPv6)," 2007. Request for Comments 4861 [online]. Available: https://tools.ietf.org/html/rfc4861. Last accessed on 2015 December.
6. A. Conta and M. Gupta, "Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification," 2006. Request for Comments 4443 [online]. Available: https://tools.ietf.org/html/rfc4443. Last accessed on 2015 August.
7. S. Hogg and E. Vyncke, *Ipv6 Security: Protection Measures for the Next Internet Protocol*. Indianapolis, IN: Pearson Education, 2008.
8. J. B. Ard, *Internet Protocol Version Six (IPv6) at UC Davis: Traffic Analysis with a Security Perspective*. Davis (CA): University of California, Davis, 2012.
9. K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using cluster analysis," *Expert Syst. Appl.*, Vol. 34, no. 3, pp. 1659–65, 2008.
10. M. Handley and A. Greenhalgh, "Steps towards a DoS-resistant internet architecture," presented at the Proceedings of the ACM SIGCOMM Workshop on Future Directions in Network Architecture, Portland, OR, 2004, pp. 49–56.
11. E. Durdağı and A. Buldu, "IPv4/IPv6 security and threat comparisons," *Proc. Social Behav. Sci.*, Vol. 2, no. 2, pp. 5285–91, 2010.
12. 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.

13. S. Axelsson, "Intrusion detection systems: A survey and taxonomy," *Tech. Report Chalmers Univ. Technol.*, Goteborg, Sweden, 2000.
14. Supriyanto, I. H. Hasbullah, R. K. Murugesan, and S. Ramadass, "Survey of internet protocol version 6 link local communication security vulnerability and mitigation methods," *IETE Tech. Rev.*, Vol. 30, no. 1, pp. 64–71, 2013.
15. J. Davies, "Introduction to IP version 6," *Microsoft Word Version*, 2002.
16. S. E. Deering, "Internet protocol, version 6 (IPv6) specification," 1998. Request for Comments 2460 [online]. Available: https://tools.ietf.org/html/rfc2460. Last accessed on 2015 October.
17. J. Rajahalme, S. Amante, S. Jiang, and B. Carpenter, "IPv6 flow label specification," 2011. Request for Comments 6437 [online]. Available: https://tools.ietf.org/html/rfc6437. Last accessed on 2015 December.
18. D. Zagar, and K. Grgic, "IPv6 security threats and possible solutions," in *The Automation Congress, 2006. WAC'06. World, IEEE*, Budapest, Hungary, 2006, pp. 1–7.
19. R. M. Saad, A. Almomani, A. Altaher, B. Gupta, and S. Manickam, "ICMPv6 flood attack detection using DENFIS algorithms," *Indian J. Sci. Technol.*, Vol. 7, no. 2, pp. 168–73, 2014.
20. V. Alangar and A. Swaminathan, "IPv6 security: Issue of anonymity," *Int. J. Eng. Comput. Sci.*, Vol. 2, p. 7, 2013.
21. R. M. Hinden and S. E. Deering, "IPv6 multicast address assignments," 1998. Request for Comments 2375 [online]. Available: https://tools.ietf.org/html/rfc2375. Last accessed on 2015 September.
22. D. Žagar, K. Grgić, and S. Rimac-Drlje, "Security aspects in IPv6 networks—implementation and testing," *Comput. Electr. Eng.*, Vol. 33, no. 5, pp. 425–37, 2007.
23. O. E. Elejla, A. B. Jantan, and A. A. Ahmed, "Three layers approach for network scanning detection," *J. Theor. Appl. Info. Technol.*, Vol. 70, no. 2, pp. 251–64, 2014.
24. P. Nikander, J. Kempf, and E. Nordmark, "IPv6 neighbor discovery (nd) trust models and threats," 2004. Request for Comments 3756 [online]. Available: https://www.ietf.org/rfc/rfc3756.txt. Last accessed on 2015 November.
25. R. M. 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.*, Vol. 32, pp. 1–12, 2015.
26. J. B. Postel, *Internet Protocol. Internet Engineering Task Force*. Marina del Rey, CA: Information Sciences Institute, 1981. Request for Comments 791 [online]. Available: https://tools.ietf.org/html/rfc791. Last accessed on 2015 September.
27. J. Weber, C. Wegener, and J. Schwenk, "IPv6 security test laboratory," Master dissertation, Department of Network and Data Security, Ruhr-University Bochum, Germany, 2013.
28. Z.-W. Lin, L.-H. Wang, and Y. Ma, "Possible attacks based on IPv6 features and its detection," in *Asia-Pacific Advanced Network (APAN) 24th Meeting*, Xi'an, China, 2006.
29. C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: Classification and state-of-the-art," *Comput. Networks*, Vol. 44, no. 5, pp. 643–66, 2004.
30. T. Ma, "A link signature based DDoS attacker tracing algorithm under IPv6," presented at the IJCA TM, Citeseer, 2009 Available: www.ijcaonline.org
31. Google, "Google IPv6 statistics," 2015. Available: http://www.google.com/intl/en/ipv6/statistics.html
32. Akamai, "State of the internet," 2015. Available: www.stateoftheinternet.com
33. K. Barker, "The security implications of IPv6," *Network Security*, Vol. 2013, pp. 5–9, 2013. Available: http://linkinghub.elsevier.com/retrieve/pii/S1353485813700680
34. X. Yang, T. Ma, and Y. Shi, "Typical DoS/DDoS threats under IPv6," presented at the International Multi-Conference on Computing in the Global Information Technology, 2007. ICCGI 2007, IEEE, Guadeloupe, French Caribbean, 2007, pp. 55–55.
35. G. B. Satrya, R. L. Chandra, and F. A. Yulianto, "The detection of DDoS flooding attack using hybrid analysis in IPv6 networks," presented at the 2015 3rd International Conference on Information and Communication Technology (ICoICT), IEEE, 2015, pp. 240–4.
36. J. Gao and Y. Chen, "Detecting DoS/DDoS attacks under IPv6," in *Proceedings of the 2012 International Conference on Cybernetics and Informatics*. New York City, NY: Springer, 2014, pp. 847–55.
37. C. E. Martin and J. H. Dunn, "Internet protocol version 6 (IPv6) protocol security assessment," presented at the Military Communications Conference, 2007. MILCOM 2007, IEEE, 2007, pp. 1–7.
38. F. Gont, "Security implications of IPv6 options of type 10xxxxxx," 2013. Internet Draft [online]. Available: https://tools.ietf.org/html/draft-gont-6man-ipv6-smurf-amplifier-01. Last accessed on 2015 March.
39. F. Najjar and H. El-Taj, "IPv6 change threats behavior," *Int. J. Adv. Comput. Sci. Appl.*, Vol. 6, p. 1, 2015.
40. O. Santos, *End-to-End Network Security: Defense-in-Depth*. New York City, NY: Pearson Education, 2007.
41. A. Raghavan, "Secure neighbour discovery: A report," 2013, Available: http://arunraghavan.net/downloads/academia/send-report.pdf. Last accessed on 2015.
42. C. E. Caicedo and J. Joshi, "Security issues in ipv6 networks," *International Telecommunications Research and Education Association (ITERA)*, Louisville, Kentucky, 2008.
43. J. Arkko, T. Aura, J. Kempf, V.-M. Mäntylä, P. Nikander, and M. Roe, "Securing IPv6 neighbor and router discovery," in *The Proceedings of the 1st ACM Workshop on Wireless Security*, ACM, Atlanta, GA, 2002, pp. 77–86.
44. F. A. Barbhuiya, S. Biswas, and S. Nandi, "Detection of neighbor solicitation and advertisement spoofing in IPv6 neighbor discovery protocol," presented at the Proceedings of the 4th International Conference on Security of Information and Networks, ACM, Sydney, Australia, 2011, pp. 111–8.
45. J. Arkko, J. Kempf, B. Zill, and P. Nikander, "Secure neighbor discovery (send)," 2005. Request for Comments 3971 [online]. Available: http://www.rfc-editor.org/info/rfc3971. Last accessed on 2015 July.
46. T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Comput. Surveys (CSUR)*, Vol. 39, no. 1, p. 3, 2007.
47. P. Hermann-Seton, *Security Features in IPv6*. Singapore: SANS Institute, 2002.
48. K. Seo and S. Kent, "Security architecture for the internet protocol," Request for Comments 4301 [online], 1998. Available: http://www.hjp.at/doc/rfc/rfc4301.html. Last accessed on 2015.

49. B. Stockebrand, "Ip security (ipsec)," in *IPv6 in Practice: A Unixer's Guide to the Next Generation Internet*, Berlin Heidelberg: Springer, 2007, pp. 311−7.
50. Y. E. Gelogo, R. D. Caytiles, and B. Park, "Threats and security analysis for enhanced secure neighbor discovery protocol (send) of IPv6 NDP security," *Int. J. Control Automat.*, Vol. 4, no. 4, pp. 179−84, 2011.
51. G. An, K. Kim, J. Jang, and Y. Jeon, "Analysis of send protocol through implementation and simulation," presented at the Convergence Information Technology, 2007. International Conference IEEE, Gyeongju, Korea, 2007, pp. 670−6.
52. A. Alsa'deh and C. Meinel, "Secure neighbor discovery: Review, challenges, perspectives, and recommendations," *Security Privacy, IEEE*, Vol. 10, no. 4, pp. 26−34, 2012.
53. 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, 2015.
54. J. Wu, J. Bi, M. Bagnulo, F. Baker, and C. Vogt, "Source address validation improvement (SAVI) framework," 2013. Internet Draft [online]. Available: http://tools.ietf.org/html/draft-ietf-savi-framework-06. Last accessed on 2015 December.
55. A. Kukec, M. Bagnulo, and M. Mikuc, "Send-based source address validation for IPv6," presented at the 10th International Conference on Telecommunications, 2009. ConTEL 2009, IEEE, Zagreb, Croatia, 2009, pp. 199−204.
56. P. Lin and J. Bi, "A novel send based source address validation mechanism (SAVM-SEND)," presented at the Ninth Annual International Symposium on Applications and the Internet, 2009. SAINT'09, IEEE, Washington, DC, 2009, pp. 149−52.
57. D. Mcpherson, J. Halpern, and F. Baker, "Source address validation improvement (SAVI) threat scope," *Request for Comments 6959* [online], 2013. Available: https://tools.ietf.org/html/rfc6959.html. Last accessed on 2015.
58. G. Yao, J. Bi and P. Xiao, "Source address validation solution with OpenFlow/NOX architecture," presented at the 19th IEEE International Conference on Network Protocols (ICNP), 2011, IEEE, Vancouver, BC, Canada, 2011, pp. 7−12.
59. E. Levy-Abegnoli, G. Van De Velde, C. Popoviciu, and J. Mohacsi, "IPv6 router advertisement guard," 2011. Request for Comments 6105 [online]. Available: http://www.rfc-editor.org/info/rfc6105. Last accessed on 2015 June.
60. F. Gont, "IPv6 router advertisement guard (RA-guard) evasion," 2011. Internet Draft [online], Available: https://tools.ietf.org/html/draft-gont-v6ops-ra-guard-evasion-00. Last accessed on 2015 July.
61. Cisco, *IPv6 Configuration Guide, Cisco IOS Release 15.2s*. San Jose, CA: Cisco Systems, Inc., 2011.
62. F. Beck, T. Cholez, O. Festor, and I. Chrisment, "Monitoring the neighbor discovery protocol," presented at the Second International Workshop on IPv6 Today-Technology and Deployment-IPv6TD 2007, Guadeloupe, French Caribbean, 2007.
63. D. C. Plummer, "RFC 826: An ethernet address resolution protocol," InterNet Network Working Group, 1982. Request for Comments 826 [online]. Available: https://tools.ietf.org/html/rfc826. Last accessed on 2015 December.
64. N. Kumar, G. Bansal, S. Biswas, and S. Nandi, "Host based IDs for NDP related attacks: NS and NA spoofing," presented at the India Conference (INDICON), 2013 Annual IEEE, Mumbai, India, 2013, pp. 1−6.
65. A. Herrera, "How secure is the next-generation internet? An examination of IPv6," DTIC 2013, Available: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA595640. Last accessed on 2015 March.
66. Z. Liu and Y. Lai, "A data mining framework for building intrusion detection models based on IPv6," presented at the Advances in Information Security and Assurance, Seoul, Korea, Springer, 2009, pp. 608−18.
67. G. Bansal, N. Kumar, S. Nandi, and S. Biswas, "Detection of NDP based attacks using MLD," presented at the Proceedings of the Fifth International Conference on Security of Information and Networks, ACM, Jaipur, India, 2012, pp. 163−7.
68. F. Gont, "Hacking IPv6 networks," presented at the Hack in Paris 2011 Conference, Paris, France, 2011.
69. F. Gont, "Security implications of the use of IPv6 extension headers with IPv6 neighbor discovery," 2012. Internet Draft [online]. Available: https://tools.ietf.org/html/draft-ietf-6man-nd-extension-headers-05. Last accessed on 2015 December.
70. M. Roesch, "Snort - lightweight intrusion detection for networks," in *Proceedings of the 13th USENIX Conference on System Administration Seattle*, Washington, 1999, pp. 229−38.
71. Snort, "Snort homepage," 2013. Available: https://www.snort.org/
72. M. Schütte, T. Scheffler, and B. Schnor, "Development of a snort ipv6 plugin − detection of attacks on the neighbor discovery protocol," *International Conference on Security and Cryptography (SECRYPT 2012)*, Rome, Italy, 2012.
73. M. Schütte, "The IPv6 snort plugin," 2014, Available: https://www.snort.org/. Last accessed on 2015 March.
74. A. Atlasis and E. Rey, "Evasion of high-end IPS devices in the age of IPv6," presented at the BlackHat EU 2014, 2015.
75. K. A. Gehrke, "The unexplored impact of IPv6 on intrusion detection systems," Master dissertation, Department of Computer Science Monterey, Naval Postgraduate School, California, 2012.
76. M. S. Hoque, M. Mukit, M. Bikas, and A. Naser, "An implementation of intrusion detection system using genetic algorithm," arXiv preprint arXiv:1204.1336, 2012.
77. M. A. C. Moya, *Analysis and Evaluation of the Snort and bro Network Intrusion Detection Systems*. Madrid: Universidad Pontificia Comillas, 2008.
78. R. Hassan, A. S. Ahmed, and N. E. Osman, "Enhancing security for IPv6 neighbor discovery protocol using cryptography," *Am. J. Appl. Sci.*, Vol. 11, no. 9, pp. 1472, 2014.
79. A. H. Alqahtani and M. Iftikhar, "TCP/IP attacks, defenses and security tools," *Int. J. Sci. Modern Eng.*, Vol. 1, no. 10, pp. 42−7, 2013.
80. A. Atlasis, "Security impacts of abusing IPv6 extension headers," presented at the Black Hat Security Conference, USA, 2012, pp. 1−10.
81. M. Pihelgas, "A comparative analysis of open source intrusion detection systems," Master dissertation, Department of Computer Science, Tallinn University of Technology, Tallinn, Estonia, 2012.

82. G. An and K. Kim, "Real-time IP checking and packet marking for preventing ND-DoS attack employing fake source IP in IPv6 Lan," presented at the Autonomic and Trusted Computing, 5th International Conference, ATC 2008, Springer, 2008, pp. 36–46.
83. S. Kent and K. Seo, "Security architecture for the internet protocol 2005," RFC 4301, 2008. Request for Comments 4301 [online]. Available: https://tools.ietf.org/html/rfc4301. Last accessed on 2015 May.
84. M. Heuse, "Thc IPv6 attack tool kit," 2013. Available: http://www.aldeid.com/wiki/THC-IPv6-Attack-Toolkit
85. P. Storm, "Tribe flood network 2000 (TFN2k) DDoS tool," 2000. Available: http://packetstormsecurity.org/distributed
86. H. Chau, "Network security—defense against DoS/DDoS attacks," Vol. 20, 2004. Available: http://efiko.org/material/Network
87. F. Gont, "Si6 networks' IPv6 toolkit," 2012. Available: http://www.si6networks.com
88. C. Alonso, "Fear the Evil FOCA attacking internet connections with IPv6," 2013, Available: https://www.youtube.com/watch?v=gWf89h9uIXs. Last accessed on 2015 December.
89. P. Biondi, "Scapy," 2011. Available: http://www.secdev.org/projects/scapy/
90. P. Savola, "Linux IPv6 router advertisement daemon (RADVD)," Vol. 28, 2011. Available: http://www.litech.org/radvd/. Last accessed on 2015.
91. R. D. Doshi and B. Chandavarkar, "Preventing bad prefixes attack in IPv6 stateless address auto-configuration protocol," presented at the 7th IEEE International Conference on Industrial and Information Systems (ICIIS), 2012, IEEE, Chennai, India, 2012, pp. 1–4.

Authors

Omar E. Elejla received his BEng degree in Computer Engineering from Islamic University of Gaza, Palestine in 2013, and MSc in Computer Sciences from Universiti Sains Malaysia (USM) in 2014. Currently, he is a PhD fellow in School of Computer Science, Universiti Sains Malaysia (USM). His research interest includes Computer Networks, Internet Communication Protocols (IPv6), Network Security, and IPv6 Security.

E-mail: oeoe14_com063@student.usm.my

Mohammed Anbar obtained his PhD in Advanced Computer Networks from University Sains Malaysia (USM). He is currently a senior lecturer at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include Malware Detection, Web Security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Network Monitoring, Internet of Things (IoT), and IPv6 Security.

E-mail: anbar@nav6.usm.my

Bahari Belaton, is an Associate Professor in Computer Science School of Universiti Sains Malaysia, He has BAppSc. (Comp. Studies) from South Australian Institute of Technology, Australia, BSc(Hons) from Flinders University and PhD from University of Leeds, UK. His research interests are Scientific Data Visualization, Computer Graphics & Network Security. Currently, he is Acting Research Dean and Information & Communications Technology Research Platform and Head of Visualization and Graphics Group.

E-mail: bahari@usm.my