Roadmap of Security threats between IPv4/IPv6.

Fadi Abusafat
Information system Department-Algorithm centre.
University of Minho.
Guimaraes, Portugal.
[0000-0001-8821-9549]

Tiago Pereira
Information system Department-Algorithm centre.
University of Minho.
Guimaraes, Portugal.
[0000-0001-5075-6189]

Henrique Santos
Information system Department-Algorithm centre.
University of Minho
Guimaraes, Portugal.
[0000-0001-5389-3285]

2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS) | 978-1-6654-4067-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/IEMTRONICS52119.2021.9422653

***Abstract*— The idea of the Internet of Things is to connect every physical device with internet. Each device should be presented by a unique address of Internet Protocol. There are two versions of IP known by IPv4 and IPv6. IPv4 assumed to cover whole network interfaces. Since the appearance of IoT, number of connected devices increased sharply and IPv4 could not afford this enormous numbers. Therefore, the solution came by introduced IPv6 to afford this massive number in IoT environment. Despite IPv4 provided interoperability with several types of protocols, robust and easy implementation but it's vulnerable for several kinds of attacks. Therefore, IPv6 introduced while having security protocols such as IPsec, neighbour discovery protocol and Secure Neighbour Discovery Protocol. However, due to IPv4 still working as well as updated with security components, there is need to interact between both versions of protocol. Therefore, there is need for interacting mechanism between both them. These mechanisms made implantation of IPv6 complicated and consumed more resources. Besides, there are threats for attacks. Therefore, security features in IPv6 are not enough and there is need for a new defense line that can secure network services and IP from attacks. Intrusion Detection mechanism considered good mechanism to provide protection due to it works based on two levels Host and Network. Besides, it uses several security approaches such as signature-based and network-based. However, considering this tool as it's in IoT environment will not bring the light of security in IoT. Therefore, it should be developed while considering features of IoT devices to secure IoT environment. To achieve this, we have to investigate every feature, component and operation in network. This review paper aims to analyse difference between IPv4/IPv6 and point out security threats related to IP in both versions. Also, identifying main security threats to IPv6.**

Keywords*— *IPv4, IPv6, IP Security threats, ICMPv6, Network Layer attacks.

I. INTRODUCTION.

The 21st century is considered the time of development of technology due to the appearance of Internet-Of-Things (IoT). The main core of IoT is to associate physical devices in human life through connections over internet. This association provided several facilities for human activities. IoT has several application such as Smart City, Smart Home, Smart Grids and Smart Buildings [1]. Ideally, it should apply with every industrial fields. This association leads to massive financial gains. Several studies estimate the financial impact of IoT from 2018 to 2023 to have increased from 249.4 to 2,0030.1 Million Dollar respectively [2]. This massive impact came from massive numbers of newly connected devices that interact and share data over internet. Studies suggest the estimated number of connected devices over internet increased from 7 to 21.5 billion device from 2018 to 2025 [3]. However, devices need Internet Protocol/Transmission Control Protocol IP/TCP to exchange data. The main advantage of IP/TCP is to allocate unique addresses to recognise of each device. Since the introduction of IoT, IP has been changed sharply from version 4 (IPv4) to version 6 (IPv6). This amendment introduced several security challenges for security mechanism as well as security attacks due to IPv4 still working and there is need to interacts between both versions while these mechanisms have interoperability challenges and vulnerable for network layer attacks [4]. In this review paper, we are going to draw a roadmap of potential security threats based on IPv4 and IPv6 in IoT/Smart City environment. To achieve this purpose, I am going to use my knowledge in Pentesting as well as most updated works toward it. Updated work will be collected from strong conference and journals. Ideally, there are three main questions to be highlighted through this study:

A. What are differences between IPv4 and IPv6?

B. What are security threats for IPv4 and IPv6?

C. What are specific threats for IPv6?

II. IPV4 VS IPV6

A. Open Source Interconnection model

The Open Source Interconnection (OSI) model is considered to be the updated model in communication and interacting data between devices. It consists from seven layers known by Application, Presentation, Session, Transport, Network, Data Link and physical layer. Application layer is responsible for providing access to applications that are in connection with an internet. Presentation layer is responsible to present data into translated formats. Session layer is responsible for creating, opening and closing sessions in order to share data between

978-1-6654-4067-7/21/$31.00©2021 European Union

Authorized licensed use limited to: UNIVERSITY OF STRATHCLYDE. Downloaded on May 24,2021 at 22:31:03 UTC from IEEE Xplore. Restrictions apply.

devices. Transport layer is responsible for processing message delivery between senders and receivers. Network layer is responsible for identifying addresses, destinations, and routes of data through different networks. Data link layer is responsible for error detection, corrections, link access, framing and reliable delivery. While the physical layer is responsible to define physical network. Since IP is located in network layer, we can assume rules for IP. Fig1, shows several protocols in each layer [5], [6]

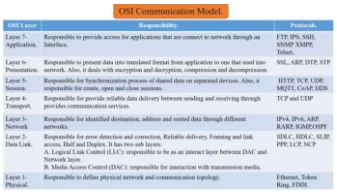

Fig 1, OSI communication model.

B. *Length of Address.*

The length/size of IPv4 is 32 bit while it is 128 bit in IPv6. Therefore, the number of available address in IPv4 and IPv6 are 2^{32} and 2^{128} respectively. The format of address used in IPv6 is alphanumeric hexadecimal notation while it is numeric dot decimal notation in IPv4. Prefix notation is 24 in IPv4 while it's 48 in IPv6. Also, IPv6 is represented by four hexadecimal digits in eight groups while in IPv4 is presented by three numeric dot decimal in four groups. Beside IPv6 supports auto configuration while in IPv4 support Dynamic Host Configuration Protocol (DHCP) or manual configuration. Table 1, shows comparison between IPv4 and IPv6 based on address features [7].

Table 1 address features between IPv4 and IPv6.

IPv4	**IPv6**
Length: 32 bit	Length : 128 bit
Available address: 2^{32}	Available address : 2^{128}
Format: numeric dot decimal notation	Format: Alphanumeric hexadecimal notation
Prefix notation : 24	Prefix notation : 48
Represented by: Four hexadecimal digits with eight groups	Represented by: Three numeric dot decimal in four groups.
Supports: DHCP and Manual configuration.	Supports: Auto configuration.

C. *Header.*

Header in IPv4 consists of 14 fields. Firstly, the version value is 4 bits. Internet Header Length (IHL) have varying sizes between 20 to 60 bytes and is used to avoid errors. The type of services (ToS) used to provide quality of services such as Voice over IP (VoIP). Explicit Congestion notification (ECN) is optional, and it used to notify senders or receivers network updates. Total length size is 16 bits and is used to point out the size of total datagram. The size can be ranged between 20 to 65535 bytes. Since this, fragmentation process has been introduced to deal with packet that have size bigger than this range. Identification (ID) is a feature used to identify fragment of IP uniquely. Flags are used to control and identify fragment. There are three flags known by Bit 0, Bit 1 and Bit 2 which are used for reserved, do not fragment and more fragments respectively. Fragment Offset has a length of 13 bit and is used to specify the offset of a fragment relative to the beginning of IP datagram. Time to live (TTL) has length 8 bit and used to present maximum time of datagram will be live on the internet. TTL is measured in seconds and it range between 0-255. In the case TTL value is zero then datagram will be removed. Protocol is used to present used Protocol in portion of datagram such as 6 present TCP and 17 present UDP. Checksum of header has 16 bit and is used to check errors in header. It is used to compare values of header checksum at each hop and discards packets in case of mismatch. Source Address has 32 bit and it present sender of data. Destination Address has 32 bit and present destination of sent packet Options it used for settings related for security, route, time-stamp and usually used when value of IHL is set to more than 5 [7]–[9].

It is unlikely for IPv4, IPv6 has less than 8 fields. Starting by version and it represent the version of IP and has 4 bits. Traffic Class has 8 bits and is divided into two main parts. First one consists of first six bits and is used to make router familiar with kind of services that should be provided. Secondly, last two bits and used for ECN. Flow label has 20 bits and designed for real-time media and streaming. Also, it used to maintain sequential flow of packets. This help router to identify particular packet belonging to specific flow of information. Therefore, it helps to avoid reordering of packets. Payload length has 16 bits and used to inform router with size of information that packet have. The size can be up to 65535 bytes and it will set for zero in case the maximum size is exceeded. Next header has 8 bits and used to indicate the type of extension header or Upper layer in case header is not present. Hop limit has 8 bits and used to stop looping packet in network. It is the equivalent to TTL in IPv4. Source address and destination address have 128 bits [7]–[9].

D. *Quality of Service.*

Quality of Service (QoS) is a set of requirements that are used to ensure proper delivery for packets. Ideally several parameters are used to construct metrics of QoS such as bandwidth, transmitted data, delay, lost data, received data and other parameters. Therefore, to evaluate the QoS between IPv4 and IPv6, will be based onto fields that indicate proper delivery. In IPv4, the flow of packets will be based on source, destination, ports and type of protocol in transport layer. However, these parameters could be affected due to fragmentation and encryption process. While in IPv6, the flow of packets based on previous fields plus flow labelled which is pre-defined in header. Flow labelled consists of 20 bits. The field of 8 bits for traffic class and used to distinguish between classes or priorities of IPv6 packets. This distinction made by source node and router. Flow labelled provided several advantages such as reduce average time for processing in router

Authorized licensed use limited to: UNIVERSITY OF STRATHCLYDE. Downloaded on May 24,2021 at 22:31:03 UTC from IEEE Xplore. Restrictions apply.

in network, reduce delays of packet, reduce the use of resources that caused by frequent change route [10].

E. Auto Configuration.

The main aim of this feature is to connect devices such as PC to internet automatically without need for manual configuration or software. Also, it provides a unique IP address to overcome scalability issues. This feature is an improvement of Link Layer Discovery Protocol (LLDP) which uses a set of attributes to discover neighbour devices. The set of attributes known by Type Length Value (TLV) which consists of type, length, and descriptions of value [11]–[14].

Dynamic Host Configuration Protocol (DHCP) is used for automatic configuration of devices in network. It is used elements in configurations such as IP, subnet mask, gateway, and other information. Generally, this process consists of discover, offer, request and Knowledge. There are some similarities on functionality of DHCP in IPv4 and IPV6. Firstly, the components of DHCP are DHCP Client, DHCP Server and DHCP Relay. These components are not changed in both IPv4 and IPv6. DHCP client is a device on a network that utilise a DHCP protocol to get network configuration. DHCP server is a component that provides a network configuration to DHCP client. This server is configured by a network administrator with network parameters to meet client needs. DHCP relay also known by DHCP relay agent and it used to pass messages in DHCP client and DHCP server are in different network. Secondly, scopes and leases. Scopes is a group if information that are used to configure device on network while lease is determine how long device on network can use that configuration. Finally, both use four messages to provide basic configuration of device on network. These configurations are discover message/solicit message, offer message/advertise message, request message/request message and acknowledgment messages/ replay message [11]–[14].

There are differences between DHCP for IPv4 and IPv6. Firstly called a reservation. In IPv4, MAC address been used to obtain IP address while in IPv6 used DHCP unique identifier (DUID) to allocated IP address. This mechanism is more sophisticated. However, reservation always require updating, as IPv4 is based on MAC while in IPv6 is based on DUIDs. The second difference is stateful and stateless. IPv6 have these two methods to configure devices on the network. Stateful stores device configuration while stateless not. In stateful DHCP sever knows IP address for all devices on network while in stateless it does not record any IP address and devices use router advertisement message to configure itself with an IP. A part of this IP is configured by device itself. In IPv4, it's not possible for a device to configure a part of IP for itself due to limitation on number of usable addresses. Second difference is Broadcast and Multicast. IPv6 uses multicast rather than broadcast. Broadcast packets goes to all devices on the network once the device is loaded on a network. This consumes more resources if the network has many devices. IPv6 uses multicast which it sent packets for selected devices on network rather than all devices. This reduce traffic on network [11]–[14].

F. Mobility.

The main idea behind Mobile IP protocol (MIP) is to keep devices connected to the internet while device in continuous mobility. In IPv4, mobility mechanism consists from three functional units known by home agent (HA), forgiven agent (FA) and mobile node (MN). Every MN has permanent home address allocated from home network but when it moves out, it gets a temporary address (CoA) which is used to identify MN in visited network. However, routing issue cause delays in mobility in IPv4. While IPv6 provide a great support for mobility due to its uses two IP address known by home address and CoA. However, routing has been improved in IPv6 [15].

G. Security.

IPv6 loaded with IP security series (IPsec) for security, authentication and data integrity provides authentication on header and encapsulating security payload extension (ESP). Also, it is designed based on end-to-end encryption and it supports more-secure name resolution. Besides, the secure neighbour discover protocol (SEND) added extra security features to neighbour discovery protocol (NDP) which is responsible for discovering other node on local link. However, NDP is not secure but SEND secure it with cryptographic method. Updated IPv4 include IPsec features. Therefore, security is different but not that big [4] [7].

III. Security Threats towards IPv4 and IPv6.

In this section, we are going to investigate Cyber security attacks based on bothIP addresses. We would like to mention new sophisticated attacks are multi-use which means it will be based on IP and other services. However, we are going to classify attacks based onto previous features and operations in IPv4 and IPv6..

A. Fragmentation attacks

Fragmentation process is used when sent packet in more than maximum size therefore, attacks related for this process are:

1) Ping of death.

The main aim of this attack is to destroy services on destination machine. Idyllically, this attack used ping feature to create a small fragment and when these fragments assemble at destination, they exceed the max size of IP packet of 65535 bytes. This attack belong for Denial of Service (DoS) but it utilised connection features to be conducted [16].

2) Drop attack.

This attack based on reassemble rules of fragmentation. One of these rules is to indicate location of fragment to reassemble successfully at destination. Hence, hackers utilise this rule

Authorized licensed use limited to: UNIVERSITY OF STRATHCLYDE. Downloaded on May 24,2021 at 22:31:03 UTC from IEEE Xplore. Restrictions apply.

through sending fragment with overlap in order to make destination node unable to reassemble sent packet [16].

3) Overlapping.

The main aim of this attack is to gain access based on TCP flags. It sends first fragment with TCP flag in order to reach the destination. The second fragment is sent with different value of TCP flag. This fragment is not blocked due to verification conducted only at the first fragment and when both fragments reach the destination, flag of first fragment will be over written with value of second fragment [16].

4) UDP and ICMP attack.

The main aim of this attack is to consume resources through sending UDP or ICMP packets bigger than network MTU [16].

B. Routing attacks.

Routing is a process to identify path of traffic inside or outside the network. It works in both versions of IP. Therefore, there is a threat for several attacks such as:

1) Flood attack.

This attack is based on sending large amount of traffic that make the destination unable to process sent packets. This attack belong for DoS. This attack utilises several types of protocols such as TCP, UDP and ICMP [17]–[19].

2) Sniffing attack.

This attack aims to capture traffic while being sent through a network. It has many aims such as stealing confidential data or dropping some packet. The best example of this attack is Man in the Middle (MiTM) which is based on fool router and source to make traffic passed through it [17]–[19].

3) Fake attack.

This attack is based on introducing a fake device or access point which is not authorised to be inside a network. Once this fake device is installed inside a network, it can pass traffic through it in order to steal data [17]–[19].

4) ARP spoofing.

ARP protocol is used to enable network communication between devices. It is used to map MAC and IP address and this mapping information stored in ARP table. This attack is based on sending wrong ARP messages over local networks to connect hacker MAC addresses with legitimate devices. Hence, hacker devices will obtain IP address and start spoofing, modifying and blocking communication. This attack belongs for MITM [17]–[19].

IV. Security Threats towards IPv6.

There are some threats toward IPv6 such as:

1) ICMP Threat.

IPv6 networks use ICMP message to conduct some important mechanisms such as router discovery when router respond for end node with router solicitation message (RS) with router advertisement (RA). This information saved for a time in routing tables. Therefore a threat here hackers could fool victims with RA messages to present itself as a router. Therefore, hackers can steal and see traffic. This attack conducted by MiTM tools. Unlikely in IPv4, blocking messages of ICMP is common development of secure features in IPv4 network [7].

2) Fragmentation process.

In IPv6, fragmentation processes are denied by an intermediate node and it conducts only by source node. The minimum recommendation size for MTU is 1280 bytes. Some security features recommend discarding all fragment with less than that value except if it's in the last round of flow. Using fragments, an attacker establishes that port numbers are not in the first fragment. This helps in overcoming security mechanisms and in order to send massive numbers of small fragments which cause system crashes. Therefore, it is recommended to limit number of fragments [20].

3) Transition mechanism.

IPv4 and IPv6 protocols still coexist. Therefore, there is a need for compatible transmission in order to avoid risk of failure in internet connection. Despite the core of IPv6 is to provide improvements of IPv4 but different between both protocols resulting in two completely different protocols. This case compatibility problem means IPv4 hosts and routers will not be in a position to directly manage IPv6 neither IPv6 will directly manage Ipv4. Therefore, there is a need for transition mechanisms such as tunnelling, and dual-stack configuration. Tunnelling is capable of dealing with address selection and DNS resolution but it increases routing process and consumes more memory and CPU. Once it increased routing process, it will be vulnerable for routing attacks. Translation is easy to implement, works with private address and configured NAT node but it shows administration challenges due to its complexity and requires extra configuration which causes slow packet flow. Finally, it poses security threats with NAT due to it keeping sessions to apply address and port transition for inbound and outbound traffic. So, in case an injection of unknown packet came from inside network, a new session will be created. Tunnelling mechanism allows IPv6 packets to transport over IPv4 but it causes problems such as delay loaded CPU to perform encapsulation [21]. To clarify these threats, we use NAT64 which used to translate between IPv6 and IPv4. It consists from three main parts known by NAT64 prefix, DNS64 server and NAT64 router. Let's presume, two networks A and B needs to communicate. Network A is a network IPv6-based and Network B is a network IPv4-based. In network A, there is a device need to communicate with a Website in network B. The first step is a device in network A communicate with DNS64 server asking about IPv6 for website in network B. Suppose, DNS64 server does not have record about this website. So, it will communicate IPv6 DNS server asking about it. IPv6 DNS server communicate with IPv4 DNS server about address of website. IPv4 DNS server replies with address of website in Network B due to it is located at the same network. Then IPv6 DNS server forward it to DNS64 which will do prefixing for it in hexadecimal. After that, it will forward it for a device which it used to communicate with NAT64 router

Authorized licensed use limited to: UNIVERSITY OF STRATHCLYDE. Downloaded on May 24,2021 at 22:31:03 UTC from IEEE Xplore. Restrictions apply.

which be the main components between both networks. NAT64 router made translation between IPv6 and IPv4 header. Finally, translated IPv4 packet will be forward it for website to conduct communication. This whole process is very complicated and need high resources such as CPU and routing process. Hence, it will be vulnerable for several attacks such as sniffing, DoS and routing.

4) Secure Neighbour Discovery Protocol.

ICMPv6 include Neighbor discovery Protocol (NDP). It is designed for several services in IP such as multicast, NDP, and neighbor discover (ND). It uses several messages such as router solicitation, router advertisement, neighbor solicitation, and neighbor advertisement. However, security in NDP is based on its scope and without securing NDP, IPv6 is still vulnerable for several attack such as MiTM, rouge and replay.

Secure Neighbour Discovery protocol (SEND) introduced to protect NDP and make IPv6 safe protocol. However, deployment of SEND is not easy and it computes intensively besides massive bandwidth consumption. So, IPv6 is still vulnerable for these attacks [22].

5) IPsec.

Internet Protocol Security (IPsec) is used to secure network packets at IP through enables cryptographic. It used widely in build Virtual Private Network (VPNs) by establishing Internet Key Exchange Protocol (IKE). IKE consists from two versions, each one in different mode and phases. Also it uses several authentication methods and configuration options. In case pair keys refused at different versions and modes in IKE, can introduce bypass authentication and made network vulnerable for authentication attack [23].

V. FUTURE WORK.

The main aim of this review paper is to point out security threats for IP in both versions. I plan to use this knowledge in my PhD research which is titled "identify security architecture compromised Intrusion Detection Mechanisms (IDS) to detect major attack in IoT and Smart City context". IDS is considered a promising security mechanism but not suitable to apply as it currently stands and should be improved, therefore we need to recognise threats related to IPv4 and IPv6 [24].

VI. CONCLUSION.

IPv6 have been introduced in order to overcome of IPv4 challenges in IoT context which it's limited to number of address while scalability issue is very clear in IoT. Besides, it introduced to overcome security issues in IPv4 through adapting several security protocols such as IPsec and SEND. However, existing of IPv4 introduced requirement of interoperability issue with IPv6. Several mechanism been introduced to server this purpose such as tunneling. These mechanism consumed many resources and this made network vulnerable for several types of network attacks. Besides, security features in IPv6 such as IPsec is also vulnerable for authentication and MiTM attacks.

There are several feature of IoT nodes, one of them is lightweight due to only capability to send small size of packet. Therefore, adapting IPv6 while holding translation mechanism that consumed plenty of resource introduced challenges for interoperability in IoT devices. Therefore, proposed solution for adapting IPv6 in IoT network, should be lightweight.

REFERENCES

[1] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horiz.*, vol. 58, no. 4, pp. 431–440, 2015, doi: 10.1016/j.bushor.2015.03.008.

[2] F. S. Market, "IoT in Banking and Financial Services Market," 2020. https://www.marketsandmarkets.com/Market-Reports/iot-banking-financial-services-market-172304505.html (accessed Feb. 20, 2021).

[3] K. L. Lueth, "State of the IoT 2018: Number of IoT devices now at 7B-Market accelerating Market Update Global number of Connected Devices: 17B," 2018. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (accessed Aug. 02, 2020).

[4] S. Praptodiyono, R. K. Murugesan, I. H. Hasbullah, C. Y. Wey, M. M. Kadhum, and A. Osman, "Security mechanism for IPv6 stateless address autoconfiguration," *Proc. 2015 Int. Conf. Autom. Cogn. Sci. Opt. Micro Electro-Mechanical Syst. Inf. Technol. ICACOMIT 2015*, pp. 31–36, 2016, doi: 10.1109/ICACOMIT.2015.7440150.

[5] A. H. Alhamedi, V. Snasel, H. M. Aldosari, and A. Abraham, "Internet of things communication reference model," *2014 6th Int. Conf. Comput. Asp. Soc. Networks, CASoN 2014*, pp. 61–66, 2014, doi: 10.1109/CASoN.2014.6920423.

[6] M. Bagga, P. Thakral, and T. Bagga, "A study on IoT: Model, communication protocols, security hazards countermeasures," *PDGC 2018 - 2018 5th Int. Conf. Parallel, Distrib. Grid Comput.*, pp. 591–598, 2018, doi: 10.1109/PDGC.2018.8745984.

[7] M. Shrivastava, "Threats and Security Aspects of IPv6," *Glob. J. Comput. Technol. Vol*, vol. 1, no. 2, pp. 51–55, 2015, [Online]. Available: https://www.researchgate.net/profile/Manish_Shrivastava8/publication/280568665_Threats_and_Security_Aspects_of_IPv6/links/55ba56b608aed621de0ace20.pdf.

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

[9] D. G. Chandra, M. Kathing, and D. P. Kumar, "A comparative study on IPv4 and IPv6," *Proc. - 2013 Int. Conf. Commun. Syst. Netw. Technol. CSNT 2013*, no. June, pp. 286–289, 2013, doi: 10.1109/CSNT.2013.67.

[10] O. J. S. Parra, A. P. Rios, and G. L. Rubio, "Quality of service over IPV6 and IPV4," *7th Int. Conf. Wirel. Commun. Netw. Mob. Comput. WiCOM 2011*, pp. 4–7, 2011, doi: 10.1109/MACE.2011.6040165.

[11] Y. Cui, Q. Sun, K. Xu, W. Wang, and T. Lemon,

Authorized licensed use limited to: UNIVERSITY OF STRATHCLYDE. Downloaded on May 24,2021 at 22:31:03 UTC from IEEE Xplore. Restrictions apply.

"Configuring IPv4 over IPv6 Networks: Transitioning with DHCP," *IEEE Internet Comput.*, vol. 18, no. 3, pp. 84–88, 2014, doi: 10.1109/MIC.2014.49.

[12] J. Montavont, C. Cobarzan, and T. Noel, "Theoretical analysis of IPv6 stateless address autoconfiguration in low-power and lossy wireless networks," *Proc. - 2015 IEEE RIVF Int. Conf. Comput. Commun. Technol. Res. Innov. Vis. Futur. IEEE RIVF 2015*, pp. 198–203, 2015, doi: 10.1109/RIVF.2015.7049899.

[13] H. Rafiee and C. Meinel, "A secure, flexible framework for DNS authentication in IPv6 autoconfiguration," *Proc. - IEEE 12th Int. Symp. Netw. Comput. Appl. NCA 2013*, pp. 165–172, 2013, doi: 10.1109/NCA.2013.37.

[14] ITfreetaining, "Key Concepts Both protocols use DHCP Client / Relay / Server," 2019. https://www.youtube.com/watch?v=YDqUZJnB14g (accessed Feb. 25, 2021).

[15] D. Le, Y. Yao, Y. Jin, and M. Zhu, "Modelling and performace analysis of mobility on CNGI," *Proc. - 2011 IEEE Int. Conf. Comput. Sci. Autom. Eng. CSAE 2011*, vol. 4, pp. 733–737, 2011, doi: 10.1109/CSAE.2011.5952949.

[16] M. Bouabdellah, N. Kaabouch, F. El Bouanani, and H. Ben-Azza, "Network layer attacks and countermeasures in cognitive radio networks: A survey," *J. Inf. Secur. Appl.*, vol. 38, pp. 40–49, 2018, doi: 10.1016/j.jisa.2017.11.010.

[17] A. K. Abdelaziz, M. Nafaa, and G. Salim, "Survey of routing attacks and countermeasures in mobile ad hoc networks," *Proc. - UKSim 15th Int. Conf. Comput. Model. Simulation, UKSim 2013*, pp. 693–698, 2013, doi: 10.1109/UKSim.2013.48.

[18] R. K. Kapur and S. K. Khatri, "Analysis of attacks on routing protocols in MANETs," *Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015*, pp. 791–798, 2015, doi: 10.1109/ICACEA.2015.7164811.

[19] M. Karthigha, L. Latha, and K. Sripriyan, "A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks," *Proc. 5th Int. Conf. Inven. Comput. Technol. ICICT 2020*, pp. 396–402, 2020, doi: 10.1109/ICICT48043.2020.9112588.

[20] M. Mavani and L. Ragha, "Security Implication and Detection of Threats due to manipulatingIPv6 Extension Headers," *Annu. IEEE India Conf.*, 2013.

[21] A. S. Ahmed, R. Hassan, and N. E. Othman, "Security threats for IPv6 transition strategies: A review," *2014 4th Int. Conf. Eng. Technol. Technopreneuship, ICE2T 2014*, vol. 2014-Augus, no. July 2020, pp. 83–88, 2015, doi: 10.1109/ICE2T.2014.7006224.

[22] A. S. Ahmed, R. Hassan, and N. E. Othman, "Secure neighbor discovery (SeND): Attacks and challenges," *Proc. 2017 6th Int. Conf. Electr. Eng. Informatics Sustain. Soc. Through Digit. Innov. ICEEI 2017*, vol. 2017-Novem, pp. 1–6, 2018, doi: 10.1109/ICEEI.2017.8312422.

[23] D. Felsch, M. Grothe, J. Schwenk, A. Czubak, and M. Szymanek, "the Dangers of Key Reuse: Practical Attacks on Ipsec Ike 27 Th Usenix Security Symposium," *Proc. 27th USENIX Secur. Symp.*, pp. 1–25, 2018.

[24] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, no. January, pp. 25–37, 2017, doi: 10.1016/j.jnca.2017.02.009.

Authorized licensed use limited to: UNIVERSITY OF STRATHCLYDE. Downloaded on May 24,2021 at 22:31:03 UTC from IEEE Xplore. Restrictions apply.