International Journal of Networks and Communications 2022, 12(2): 47-54
DOI: 10.5923/j.ijnc.20221202.01

Effects of DoS Attack in Wi-Fi Broadband Network

Akende Y. Nalukui*, Charles S. Lubobya

Department of Electrical and Electronic Engineering, University of Zambia, Lusaka, Zambia

Abstract This paper investigates the effect of Denial-of-Service (DoS) attacks in broadband-Wi-Fi networks involving public sector networks. Public Sector Networks are home to hundreds of services that have profound influences on citizen's lives and work in Zambia. However, the availability of these networks are constantly threatened by DoS attacks as wireless extensions are generally susceptible to cyber-attacks and may serve as entry points to attacks that might negatively affect and pose unnecessary risks to the entire network and organization. In this paper, we describe DoS attacks at every layer of the OSI Model; simulate the DoS Attack, and analyse the effects of this attack on Wi-Fi supplemented broadband networks also referred to in this paper as Wi-Fi Broadband Networks using OPNET Modeller. Simulation results show that a network under DoS attack drops on average 10Mbps more packets at the access point, than one without this attack. Further, the end to end delay is 0.2s more on network under DoS than one without and that a network under DoS attack experience more queued packets than one without dos attack. The server response time also tends to take long as the number of malicious nodes increases. These results indicate that DoS attack has a serious effect of slowing down the upload and download time of resources and in even more important can cause drop in packets thereby denying services to users as well as threating the integrity of data and availability of the much needed resources.

Keywords Wi-Fi Networks, Broadband Networks, DoS attacks, Wi-Fi Attacks, Access point

1. Introduction

Over the past years, the world has become increasingly mobile. As a result, traditional networks have proven inadequate to meet the challenges posed in this new era [1]. Public sector organizations are now under increasing pressure to enhance operational efficiency and upgrade technology to support the adoption of industry trends like the Internet of Things (IoT), as people use more of mobile devices in addition to computers [2]. As a result, wireless technologies have encroached on the traditional realm of Traditional "wired" networks and has led to the widespread adoption of WLAN technology as a supplement to wired networking infrastructure in the enterprise office environment [3].

Public sector organization are now extending substantial parts of its traditionally wired network infrastructure to wireless technologies to benefit from the mobility, flexibility, scalability and low cost of wireless networks [2] [1] in order to support industry trends like the Internet of Things (IoT), and improve operational efficiency. The generation of wireless communications technologies has opened countless possibilities of use in the Public Sector. As the cost of their deployment is very low, they perfectly complement traditional communication systems, and they have wide bandwidth and wide coverage that enable the deployment of new generation services in this area, some of them directly related to the end user, in order to provide a high quality transport service [4]. Today, remote employees, citizens and other stakeholder organizations can connect to public sector Networks with ease through the internet from anywhere, anytime under different environments and technology platforms using wireless communications.

However, the successful deployment of Wi-Fi technologies to supplement wired (broadband) networks has made public sector networks an attractive target for potential attackers [5] simply because Wireless networks are generally susceptible to adversarial and non-adversarial threats and attacks and can serve as entry points to attacks. Amongst the various security risks posed by IEEE 802.11-based networks, Denial-of-Service (DoS) attacks are constantly threatening the availability of IEEE 802.11-based networks. Unfortunately, these DoS threats and attacks cannot be adequately addressed via cryptographic methods [6] [7], therefore can unnecessary pose security risks to the entire network and organization. DoS attacks do often breach the availability of IEEE 802.11-based networks and prevent legitimate users from accessing the network. Given the nature of today's public sector where business rely heavily on application uptime and availability of resources and services, downtimes can be disruptive and costly and can potentially paralyse organisational operations and in worst cases, even cause irreparable damages. Therefore, protecting

* Corresponding author:
nalukuiyakende@gmail.com (Akende Y. Nalukui)
Received: Oct. 26, 2022; Accepted: Nov. 16, 2022; Published: Dec. 6, 2022
Published online at http://journal.sapub.org/ijnc

public sector data and its networks from cyber-attacks is, now more than ever, a need and not just a concern.

In this paper, we present simulation results that show how IEEE 802.11 supplemented broadband network will perform under DoS attack scenarios. A public sector LAN environment of fifty (50) wired LAN PCs and forty-five (45) wireless nodes connected to form a Wi-Fi broadband network is replicated and simulated in OPNET modeler. The rest of the paper is divided as follows: section two (2) gives the related work, section three (3) outlines the overview of the Wi-Fi networks while attacks on these Wi-Fi networks are given in section four (4). Sections five (5) and six (6) discusses the methodology and results respectively while the conclusion is given in section seven (7).

2. Related Works

A lot of research works have been done relating to IEEE 802.11 networks and their security. Most of these research works focus on the confidentiality and integrity of 802.11 networks more than availability of the 802.11 networks. The IEEE 802.11 standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol whose primary goal was to protect the confidentiality of link-layer communications from eavesdropping and other attacks. [7] Discovered that WEP had several serious security flaws emerging from misapplication of cryptographic primitives. They further demonstrated a number of attacks against the Wired Equivalent Privacy (WEP) protocol, which was employed to provide network confidentiality, and it was discovered that WEP failed to achieve its security goals. Furthermore, [7] identified a number of vulnerability that can be used by attackers to modify and spoof WEP-protected frames without knowing the shared secret key. A number of DoS attacks against availability of IEEE 802.11 networks have also been widely discussed by several authors [3] [7] [5] [8] [9] [10] [11] [12] [13] [14]. While [14] examined such DoS attacks in IEEE 802.11 ad hoc networks and indicated that traditional wireline-based detection and prevention approaches do not work in wireless LANs, [13] presented DoS attack issues in broadband wireless networks, along with possible defenses. [5] Identified some identity-based DoS attacks which exploit the vulnerability that the management frames in IEEE 802.11 are unauthenticated also demonstrated the DoS attack against the IEEE 802.11 DCF through a simulation study. To address the jamming attacks, [5] further proposed two enhanced detection protocols. One scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, and the other employs location information to serve as the consistency check. [3] identified a trivial but highly effective DoS based on commonly available IEEE 802.11 hardware and freely available software. This attack targets at the Direct Sequence Spread Spectrum (DSSS) Wireless LANs. However, very limited work has been done on investigating the vulnerabilities of IEEE 802.11 DCF mechanism using actual practical set ups.

This paper focuses on Denial-of-service (DoS) attacks against IEEE 802.11 based Networks. And because Wireless networks are generally susceptible to adversarial and non-adversarial threats that can breach the availability of wireless networks, such attacks do prevent legitimate users from accessing the network.

3. Overview of Wi-Fi Networks

"Wi-Fi" stands for Wireless Fidelity, and is generally used as synonym for wireless Local Area Network (LAN) and stems from IEEE 802.11 family of standard [15]. Wireless networks are based on the Institute of Electrical and Electronics Engineers IEEE 802.11 set of standards for WLANs [1] [16]. Wireless devices are constrained to operate in a certain frequency band namely 2.4 GHz and 5 GHz. Wi-Fi routers that come with 2.4 GHz or 5 GHz are called the single-band routers but a lot of new routers support both 2.4 GHz and 5 GHz frequency and are called dual-band routers [17] [18] [19]. Figure 3.1 shows a Wi-Fi network

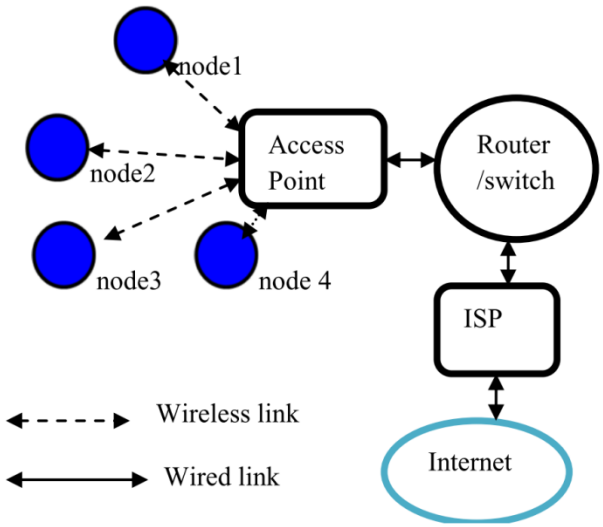

Figure 3.1. Wi-Fi networks [15]

Several Wi-Fi nodes are connected using a wireless link to the access point to which they are identified and registered. These wireless nodes can transmit and receive data, voice or video signals to and from the access point. The access point has wired connection point to which broadband internet connection is terminated. The wired link can connect to the nearest switch, router and the Internet Service Provider (ISP). The aim is to investigate and analyse the effects of the DoS attack on network performance of IEEE 802.11 supplemented Broadband networks using various performance metrics such as number of data dropped in bits per second, packet queue size, packet delivery ratio, Server Response time and end to end delay.

4. Attacks on Wi-Fi Networks

Denial-of-Service (DoS) attacks are attacks against availability, attempting to prevent legitimate or authorized users from accessing the network [20] [21]. Wireless networks are highly susceptible to DoS attacks [5] because mobile nodes share the same physical media for transmitting and receiving signals. As a result, network and computing resources such as TCP connection buffers, application/service buffer, bandwidth, CPU and power are usually more constrained compared to wired nodes [9]. DoS attack target different layers of OSI model [22] and can impact resources, radio signals, network protocols, and even wireless applications [23].

4.1. Wireless Systems are Vulnerable to DoS

Denial of Service attacks deny service by preventing legitimate users and systems from performing typical tasks such as connecting to the wireless network, staying connected to the wireless network, serving up various network requests and managing network communications. Disruption of these types of network services can wreak havoc on usability and can even threaten data integrity, confidentiality and availability. There are two main reasons that IEEE 802.11-based wireless systems are vulnerable to DoS attacks:

i. *Lack of frame authentication.*

IEEE 802.11 based networks lack frame authentication in management frames such as beacons, association requests, and probe responses. The functionality in the MAC layer of IEEE 802.11-based network is all about access. It allows wireless systems to discover, join, and basically roam free on the network, completely exposed to the elements. This implicit trust among wireless systems makes it easy for attackers to spoof authentic devices and bring down individual nodes or even an entire wireless network all at once.

ii. *Lack of physical boundaries for radio waves.*

Lack of physical boundaries for radio waves makes attacks simpler and reduces the likelihood that an attacker will be identified. Additionally, APs and other wireless infrastructure equipment are often exposed in easy-to-access areas where they’re more susceptible to tampering and theft.

4.2. Physical Layer Attacks

Physical Layer DoS attacks are generally known as Jamming Attacks. Jamming attacks are attacks in which attacker sends radio frequencies which interfere with the frequencies of wireless network. The aim is to prevent a station as well as an AP from successfully transmitting or receiving frames in the physical layer so that frames cannot be passed on to higher layers. Jamming attack is a type of DoS attack at physical layer [11] [20]. Low throughput, low packet delivery ratio (PDR) and high packet latency are indicators of a jamming attack [11]. Some of the attacks are described below

4.2.1. Resource Unlimited Attack (RUA)

Wireless networks are built upon a shared medium that makes it easy for adversaries to conduct radio interference, or jamming attacks, which effectively cause a denial of service (DoS) of either transmission or reception functionalities [9]. If the jammer has virtually unlimited resources (i.e. energy, power, and bandwidth) then it can maintain a high level of signal strength at any receiver continuously in a wide frequency range. In such jamming cases all wireless devices in the effective range and jamming bandwidth will be blocked off as long as the attack continues.

4.2.2. Reactive Attack

Continuous transmission drains the jammer's energy resources. An energy-efficient jamming technique is reactive jamming. In this kind of attack a jammer passively monitors the channel until it senses a frame transmission. Upon detection of an ongoing frame transmission the jammer starts to send interfering signals to corrupt the ongoing frame transmission [10]. Alternatively, when the jammer detects the start of an ongoing DCF handshake, it can create interference signal without the need to detect an ongoing transmission. Jamming opportunity is present at all the stages of a handshake.

4.2.3. HR (Hit and Run) Attack

If the jammer station continuously transmits jamming signals, then its energy consumption will be high. Furthermore, detection of such a station will be easy. However, if jamming signals are turned on and off periodically or randomly, then both the energy consumption will be less and the identification of such a node will be harder.

4.2.4. Symbol Attack

IEEE 802.11 and IEEE 802.11b frames do not include any Forward Error Correction (FEC) schemes. Thus, creating an error in a single symbol will render the whole frame useless. Similar to the reactive attack, during an ongoing transmission a jammer transmits a strong signal for the duration of a single symbol [9] and can succeed in destroying the whole frame.

4.3. Data Link Layer

DoS attacks at Data Link Layer benefit from a central basic vulnerability, known as MAC-address spoofing. Wireless networks are particularly vulnerable to these attacks due to the use a shared medium [12]. MAC protocol allows an attacker to selectively or completely disrupt the network access using relatively few packets and lower power consumption [20] [5]. In “selective Mac Layer Attacks, the attacker targets an individual station not the whole network. Whilst in complete MAC layer attacks, the attacks can be generalized to block the network access to all the stations served by an AP. However, there are more efficient

resource-depletion attacks for complete disruption. The attacker can simply target the AP and exhaust its finite computation and/or memory resources so that it can no longer give service to any other station [20] [12].

4.3.1. Probe Request Flood

Probe request frames are used by stations to actively scan an area in order to discover existing wireless networks. The basic idea is to send a burst of probe requests having different source MAC addresses [22] (MAC's Spoofing) to induce a heavy workload on the AP so that it cannot give service to legitimate stations [12].

4.3.2. Authentication or Association Request Flood

Similarly, the attacker can waste the AP's resources by sending a burst of authentication or association requests. By sending a burst of authentication request frames, using MAC spoofing, it should be possible to bring AP's resources close to the saturation level [12]. If IEEE 802.11i is implemented, the attacker can also exhaust the space of the EAP packet identifier, which is only 8-bits long, by association request flooding [3].

4.3.3. De-authentication or De-association Request Flood

Cryptographic protection is not implemented yet for management frames in the IEEE 802.11 standard. Therefore, by listening to the traffic and learning the MAC addresses of the station and the AP, an attacker can forge a de-authentication or a de-association frame and transmit it either to the station or to the AP to knock the station off the network. De-authentication attacks are more efficient than de-association attacks because they require more work for the station to return back to the associated state. If the attack is repeated persistently, the station is kept from accessing the network indefinitely and disables the ability of the hosts to access the local network [5].

4.4. Network Layer Attacks

Network Layer DoS attacks in the network layer mainly focus on exploiting routing and forwarding protocols in wireless networks. DoS attacks can be achieved by sending a large amount of IP data to a wireless network and are also possible due to the bandwidth limitations of wireless networks as compared to wired networks [20].

4.4.1. ICMP Ping Flooding

Internet Control Message Protocol (ICMP) is an error reporting and diagnostic utility and it is considered as a part of Internet Protocol (IP) suite. Although this protocol is very important for ensuring correct data distribution, it can be exploited by malicious users and cause Denial of Service (DoS) attacks. Due to the broadcast nature of wireless communication, exploitation of this kind of attack is even easier. An attacker sends huge number of ping packets, usually using "ping" command to either disrupt or intercept communication from a wireless access point [24]. In this way attacked system cannot respond to legitimate traffic.

4.5. Transport Layer Attacks

Transport Layer DoS attacks involve sending many TCP connection requests to a host. It is very effective and extremely difficult to trace back to the attacker because of IP spoofing techniques used. The following are some of the Transport Layer attacks.

4.5.1. TCP Sync Flooding

TCP Sync Flooding is one of the most common DoS attacks is the SYN Flooding Attack [17]. TCP implementations are designed with a small limit on the maximum number of half-open connections per port that are possible at any given time. An attacker initiates a SYN flooding attack by sending many connection requests with spoofed source addresses to the target machine which in turn allocates required resources. When the limit of half open connections is hit, all successive connection establishment attempts are denied, regardless of whether they are legitimate or not, causing DoS effects. In other cases the attacker will allow the DoS attack to last longer than the timeout period by continuously requesting the target machine for new connections. The amount of CPU and network bandwidth required by an attacker for a sustained attack is negligible [25].

4.6. Application Layer Attacks

Application Layer DoS attacks attempt to exploit a weakness of an application protocol at Layer Seven (7) of the OSI Model. It is achieved by sending large amounts of legitimate requests to an application.

4.6.1. HTTP Flood Attack

HTTP flooding Attack is a Layer Seven (7) attack which is really dangerous and harmful. It is a form of Distributed Denial of Service (DDoS) where an HTTP flood attack makes use of 'HTTP GET' and 'HTTP POST' requests to carry out the cyberattack. The main purpose is to bring down a target site or server by flooding it with a huge number of HTTP requests which will make it unresponsive and thus become inaccessible for use. Similar to routing attacks, attackers can also exploit forwarding behavior. Typical attacking approaches include injecting junk packets, dropping packets, and disorder packets in legitimate packets. Attackers can use spoofed packets to disguise their attacking behavior, or find partners to deceive defenders. The objective is to exhaust bandwidth or disrupt connection so that service cannot be delivered [10].

4.6.2. AP Overloading

IEEE 802.11-based wireless access points can only handle a limited amount of traffic before their memory fills up and their processors become overloaded. This type of DoS attack overloads both the wireless medium and the actual wireless infrastructure. Attackers can exploit a weakness in the way

access points queue incoming client requests beginning with the Client Association Identifier (AID) tables. Once this memory fills up, most APs will no longer accept incoming association requests and may lead to some APs to crash. These types of DoS attacks can typically be accomplished by using either Association Flooding or Authentication Flooding. When APs are set up to use "open" as the default authentication type, it allows any client whether trusted or untrusted to connect to the AP. This is one of those fundamental IEEE 802.11 security flaws deemed necessary to keep wireless-connectivity headaches to a minimum.

5. Research Methodology

The Network Topology implementation of the Wireless Local Area Networks (WLAN) was done by designing the network that included the Server, Access Point (AP), IP-Cloud, Gateway Router (Ethernet4_slip_gtwy), forty-five (45) Wireless Workstations, Applications, Profiles, Task and IP Attribute Config object as shown in Figure 5.1 WLAN Topology. The 100base-T cable was used to connect the devices from Access Point (AP) to the Gateway router and from Gateway router to the IP cloud PPP_DS3 was used. Similarly, from IP Cloud to PPP Server, PPP_DS3 cable was used. It is important to note that the 100Base-T link represents an Ethernet connection operating at 100Mbps (i.e. 10 times faster than standard Ethernet). The Basic Service Set Identifier (BSSID) was set to 1 for all the nodes and Access Point (AP). The BSSID is the Media Access Control (MAC) physical address of the Access Point or wireless router which was used to connect to the Wi-Fi and that the term is used in wireless network. The Basic Service Set (BSS) is the cornerstone topology of any IEEE 802.11 network.

5.1. Simulation Set-up

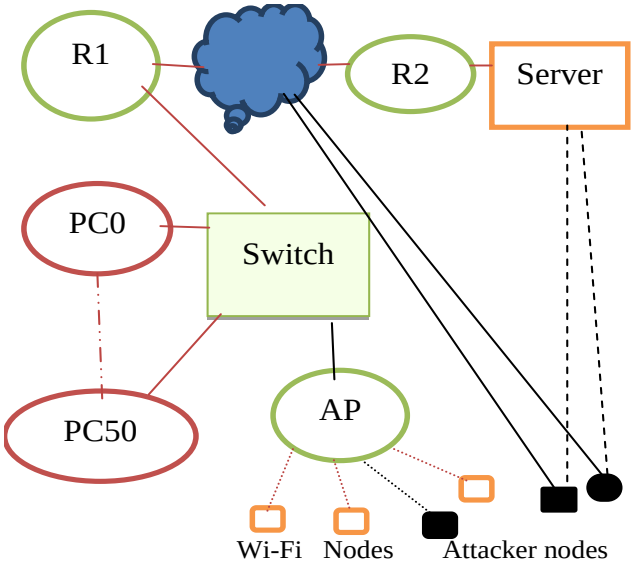

Figure 5.1. Configuration of the Wi-Fi broadband Network

The simulation was set in such a way that a number of Wi-Fi nodes were connected to the Wi-Fi broadband network via the access point AP. The access point was then connected to the switch from which also was connected a number of wire LAN computers. The switch was then linked to the IP cloud and the server via the routers R1 and R2. Figure 5.1 shows the configuration of the network used in simulation.

The pulsed jamming attack was also configured in the wireless LAN environment with the base frequency of the pulse jammer set at 2401MHz and the bandwidth set at 22MHz. With these frequencies the wireless channels 1 and 5 were affected. For the HTTP flooding attack the target was to flood the server with a huge number of GET and POST requests in order to bring it down by making it unresponsive and thus become inaccessible for use to the other nodes.

Other simulation parameters were set as shown in table 1:

Table 1. Simulated parameter set up

Number of Wi-Fi nodes	45
Number of LAN computers	50
Data simulated	Data base, ftp, video
Malicious node	Maximum 4
Wi-Fi data rate	54Mbps
Access point buffer size	256000 bits
Transmit power	0.005 W
Ping packet size	65527 bytes

6. Results and Discussions

Figure 6.1 shows the data dropped in bits per second at the access point with one Wi-Fi malicious nodes and one broadband connected malicious nodes. The effect of the malicious Wi-Fi node was to broadcast huge numbers of malicious messages that eventually will overload the access point thereby limiting or completely denying legitimate access to the AP. Furthermore, access to server resources was also limited. In the figure we see substantial amount of data being dropped at the access point before attack but that this effect becomes more when malicious nodes are introduced.

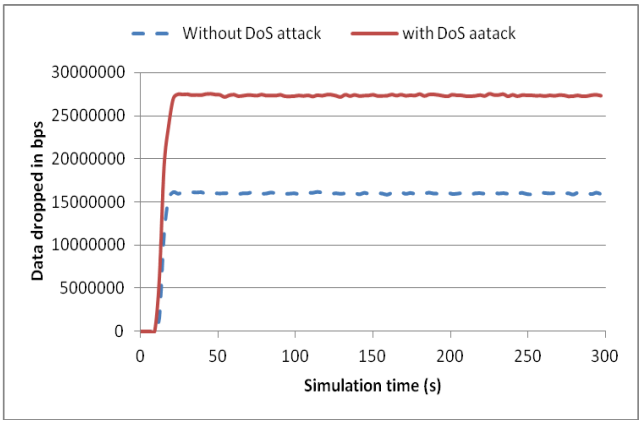

Figure 6.1. Data dropped in bps at the access point

And because attackers can exploit a weakness in the way access points queue incoming client, we see in figure 6.2 an increase in packets queued at the access point which results in some of these packets being dropped as discussed in figure 6.1. The queued packets are more, about 120 on average, in a network under DoS attack than one without these attacks which averages 115 packets. Such queues tends to frustrate users during upload and download activities.

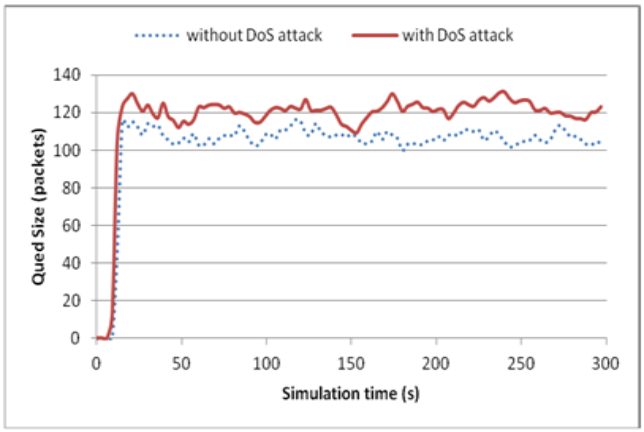

Figure 6.2. Queued packets at the access point

The Wi-Fi-broadband network also experiences an increased performance in terms of end-to-end delay when attacked by malicious nodes. This is illustrated by results illustrated in figure 6.3.

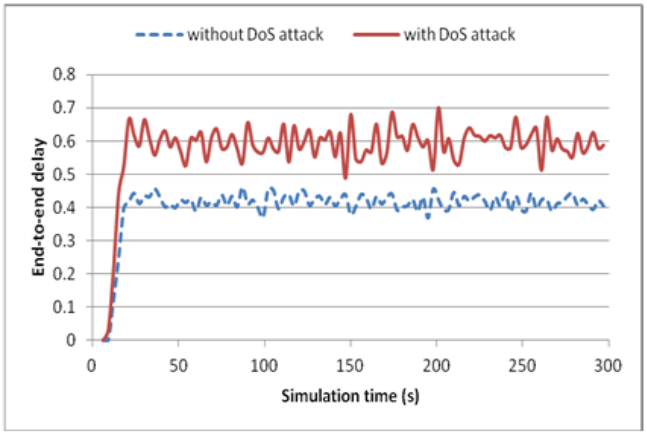

Figure 6.3. Traffic end-to-end delay measured between end nodes

From these results we note an average end to end delay of 0.6s for a network under attack compared to an average of 0.4s for a network without DoS attack. This arises on account that the traffic movement from the end nodes to the server is greatly affected and slowed by these DoS attacks.

Figure 6.4, finally shows the effect of increasing number of malicious nodes on server response time. The server response time tends to increase linearly with increase in number of malicious nodes. The response time increase from 0.49s without malicious nodes or DoS attack to 0.56s as malicious nodes increase to 4. This increase is occasioned by the increase in malicious messages sent to the server which then delays time needed by users to access resources.

Figure 6.5 shows the effect on throughput at the access point when the wireless network is under different DoS attacks. From the results obtained, jamming attacks and the flooding attacks contribute to the highest reduction in throughput with the ICMP ping flooding attack having the least reduction in throughput.

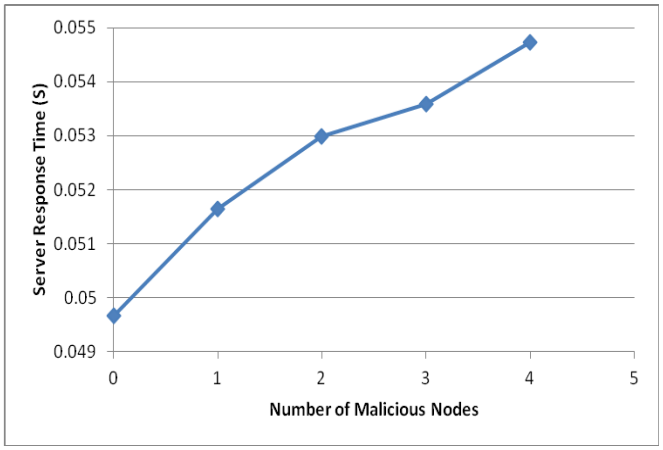

Figure 6.4. Server response time in second

The jamming and HTTP flooding attacks tend to drop a lot of traffic thereby minimizing throughput.

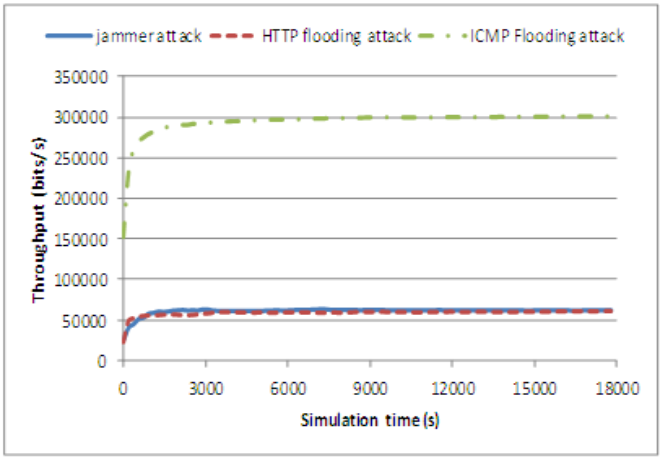

Figure 6.5. Effect on access point throughput under different DoS attacks

7. Conclusions

Wireless Networks are mostly susceptible to Denial of Service attacks like jamming and flooding. Given the nature of today's public sector where business rely heavily on application uptime and availability of resources and services, we cannot afford to compromise the availability and security of such networks. And when considering the application of IEEE 802.11 technology in safety-critical environments which typically have stringent availability requirements like Public Sector Organizations, adequate strategies must be put in place to mitigate the significant threat of Denial of Service in current IEEE 802.11 because attacks on these networks can be disruptive and costly and can potentially paralyze organizational operations and in worst cases, even cause

irreparable damages. Therefore, protecting public sector data and its networks from DoS attacks is, now more than ever, a need and not just a concern.

In this paper, we have described some of the common DoS attacks at every layer of the OSI Model. We have also demonstrated and discussed the effects of DoS attack on Wi-Fi broadband networks. DoS attacks can increase the number of dropped data packets at the AP in a network, increase packet queue size, increase end to end delay and increase server response time. Further, we have noted that Jamming and Flooding attacks contribute to the highest reduction in throughput and can wreak havoc on usability and can even threaten data integrity, confidentiality and availability. Comparatively, jamming attacks and HTTP flooding attacks affect throughput more than ICMP Ping flooding attacks and thus can be considered high risk attacks. Lastly, attacks launched by multiple attackers also known as DDoS attacks that send large traffics to the network is able to bring the entire network or services down as well as affecting the server response times.

REFERENCES

[1] Matthew S. Gast, "802.11 Wireless Networks; The definitive Guide, Second Edition," *O'Reilly Media, Inc., 2005 Gra?enstein Highw. North, Sebastopol, CA 95472.*, no. ISBN: 0-596-?0052-?, 2005.

[2] E. Sula, "Wireless Networks.," vol. 8, no. December, pp. 23–27, 2018.

[3] K. Tham, J. Smith, and M. Looi, "QUT Digital Repository: Spectrum Wireless LANs. In: Wireless Telecommunications Symposium, 2004, A Trivial Denial of Service Attack on IEEE 802. 11 Direct Sequence Spread Spectrum Wireless LANs," *System*, no. May, pp. 14–15, 2004.

[4] U. Gutiérrez, I. Salaberria, A. Perallos, and R. Carballedo, "Towards a broadband communications manager to regulate train-to-earth communications," *Proc. Mediterr. Electrotech. Conf. - MELECON*, pp. 1600–1605, 2010, doi: 10.1109/MELCON.2010.5476304.

[5] J. Bellardo and S. Savage, "802.11 Denial-of-service attacks: Real vulnerabilities and practical solutions," *Proc. 12th USENIX Secur. Symp.*, pp. 15–27, 2003.

[6] W. Xu, "Defending Wireless Networks from Radio Interference Attacks," pp. 101–195, 2007.

[7] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," *Proc. Annu. Int. Conf. Mob. Comput. Networking, MOBICOM*, pp. 180–188, 2001.

[8] K. Bicakci and B. Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks," *Comput. Stand. Interfaces*, vol. 31, no. 5, pp. 931–941, 2009, doi: 10.1016/j.csi.2008.09.038.

[9] Q. Gu and S. Marcos, "Denial of Service Attacks Department of Computer Science Texas State University – San Marcos School of Information Sciences and TechnologyPennsylvani a State University Denial of Service Attacks Outline," pp. 1–28, 2007, [Online]. Available: https://s2.ist.psu.edu/ist451/DDoS-Chap-Gu-June-07.pdf.

[10] M. Tyagi, S. Narvare, and C. Agrawal, "A Survey of Different Dos Attacks on Wireless Network," vol. 9, no. 5, pp. 23–32, 2018.

[11] L. Arockiam, "A Survey of Denial of Service Attacks and it ' s Countermeasures on Wireless Network," *Int. J.*, vol. 02, no. 05, pp. 1563–1571, 2010.

[12] F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks," *2004 IEEE Wirel. Commun. Netw. Conf. WCNC 2004*, vol. 1, pp. 634–638, 2004, doi: 10.1109/wcnc.2004.1311620.

[13] S. Khan, K. K. Loo, T. Naeem, and M. a Khan, "Denial of service attacks and challenges in broadband wireless networks," *J. Comput. Sci.*, vol. 8, no. 7, pp. 1–6, 2010, [Online]. Available: http://bura.brunel.ac.uk/handle/2438/4027.

[14] C. Gupta, P. Singh, and R. Tiwari, "Network and Transport Layer Attacks in Ad-hoc Network," pp. 38–42, 2017, doi: 10.17148/IJARCCE.

[15] S. C. Lubobya, M. E. Dlodlo, and G. De Jager, "Performance evaluation of the wireless tree Wi-Fi video surveillance system," *Proc. - UKSim-AMSS 16th Int. Conf. Comput. Model. Simulation, UKSim 2014*, pp. 511–516, 2014, doi: 10.1109/UKSim.2014.40.

[16] A. Sheikh, *Hacking Wireless Networks*. 2021.

[17] L. Seno and S. Vitturi, "Wireless extension of Ethernet Powerlink networks based on the IEEE 802.11 wireless LAN," *IEEE Int. Work. Fact. Commun. Syst. - Proceedings, WFCS*, pp. 55–63, 2008, doi: 10.1109/WFCS.2008.4638726.

[18] G. Fleishman, "TAKE CONTROL OF WI-FI NETWORKING and SECURITY."

[19] S. Song and B. Issac, "Analysis of Wifi and Wimax and Wireless Network Coexistence," *Int. J. Comput. Networks Commun.*, vol. 6, no. 6, pp. 63–77, 2014, doi: 10.5121/ijcnc.2014.6605.

[20] K. Bicakci and B. Tavli, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks," *Comput. Stand. Interfaces*, vol. 31, no. 5, pp. 931–941, 2009, doi: 10.1016/j.csi.2008.09.038.

[21] M. Manisha and D. M. Kumar, "Network Layer Attacks and Their Countermeasures in Manet: A Review," *IOSR J. Comput. Eng.*, vol. 16, no. 2, pp. 113–116, 2014, doi: 10.9790/0661-1625113116.

[22] B. Need and F. O. R. Security, "BUSINESS NEED FOR SECURITY Denial of Service Attacks in Wireless Networks."

[23] A. Joshi and R. H. Goudar, *Advanced Computing, Networking and Informatics- Volume 2*, vol. 28, no. VOLUME 2. 2014.

[24] M. Bogdanoski and A. Risteski, "Wireless network behavior under ICMP ping flood DoS attack and mitigation techniques," *Int. J. Commun. Networks Inf. Secur.*, vol. 3, no. 1, pp. 17–24, 2011.

[25] M. Alkasassbeh, G. Al-Naymat, A. B.A, and M. Almseidin, "Detecting Distributed Denial of Service Attacks Using Data Mining Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, pp. 436–445, 2016, doi: 10.14569/ijacsa.2016.070159.