OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

A review of Network Layer and Transport Layer Attacks on Wireless Networks.

Edvald Sula
[1]*Instructor,Team Leader of Computer and Network Systems, Departamant, „American College of the Middle East, Kuwait".*

Abstract: *Wireless Networks are implemented from many companies in the last years. The main reasons to implement the wireless networks are: (i) easy to deploy, (ii) lower cost comparing to wired networks, (iii) mobility. A wireless network use high frequency radio waves to transmit the data. This nature of the wireless networks makes them more vulnerable against different attacks compared with wired networks. During this study, we are going to make a review about different attacks on Network Layer and Transport Layer of Wireless Networks.*
KEY WARDS*: Wireless Network, Network Layer Attacks, Transport Layer Attacks, Hijacking, IP Spoofing.*

Date of Submission: 26-01-2019 Date of acceptance: 09-02-2019

I. INTRODUCTION

The latest statistics shows that the wireless networks are used as the only way of connecting to the internet from many households in U.S. According "National Center for Health Statistics" latest Wireless Substitution report, at the end of the year 2017, 61.8 % of children living in households use only wireless service. According to this report, 53.3 % of the adults living in households have wireless service only. Because of this fast growing of the wireless networks, is very important to have high security to prevent the attacks that can happen to these networks.

There are many advantages of using wireless networks such as low cost, easy to setup, high scalability, and high mobility.

Even though there are many encryption methods and security mechanisms applied from the network administrators to have a secure communication, hackers are successfully attacking the devices of the wireless network. There are two types of attacks: passive and active.

A passive attack does not disrupt the communication between devices on the network. The attacker is interested on sniffing the data transmitted on the wireless network. One method of passive attack is the man in the middle attack. To detect these methods of attacks is very difficult, as the network, it will not be implicated.

Active attacks are severe attacks of the wireless networks. The focus of these attacks is to destroy the performance of the wireless networks. These attacks can block completely the services of the wireless network. Also, they can modify or fabricate the packets transmitted between devices on the network. Well-known active attacks are Denial of Service attacks or Wormhole attacks.

During this study, we will review the attacks on the network layer and transport layer of the wireless networks. The attacks we will review during this paper are the most important attacks that the network administrators should protect their network. The attacks of the network layer are: IP spoofing, hijacking, smurf, wormhole, blackhole, sybil and sinkhole. The attacks of the transport layer are: TCP sequence prediction, UDP &TCP flooding. During this study it was observed that are many other attacks that effectes physical layer such as eavesdropping, jamming and network injection. Also, are many attacks that effects the application layer such as SQL injection, SMTP attack, Malware attacks and FTP bounce. But, it is observed that the attacks of the network layer are very dangerous and can destroy the performance of the wirless network.

In Section II of the paper we will review the attacks of network layer. Section III reviews attacks of transport layer. The conclusions are in Section IV.

II. ATTACKS ON THE NETWORK LAYER

The main responsibility of the network layer is to transmit the packets from the source to the destination by finding the best route, which is the route that has the lowest cost and shortest path from the source to the destination.

The goal of the attacks on the Network Layer is to disrupt the path between the source and destination that is chosen from the routing protocols. [3].

Some of the most used methods to attack the network layer are below:

2.1 IP spoofing attack [4]

This technique is used from the attackers to gain unauthorized access to the servers. The attacker will send messages to the server not with his own IP address, but with a "trusted" IP address. In this way the server will not understand that it is getting traffic from an attacker. After the attacker will find the "trusted IP" address, will modify the headers of the packets in the way that the attacked server will think the packets are coming from "trusted" IP. The main route cause of DDoS (Distributed Denial of Service) attacks is IP spoofing.

IP spoofing attack can further cause the below attacks:

1. Blind Spoofing.
2. Non-Blind Spoofing.
3. Man in the middle attack.

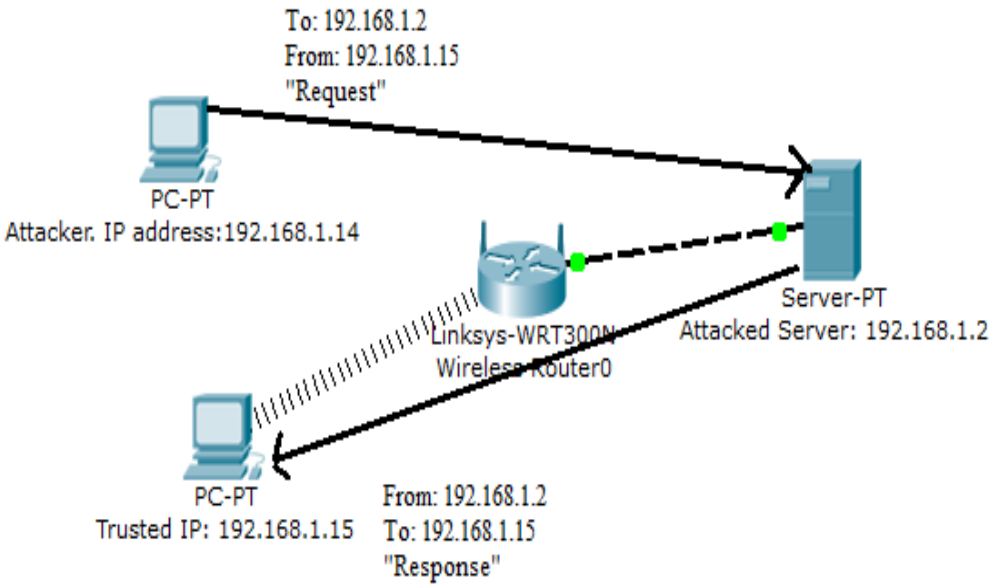

Figure 1: IP Spoofing

Figure 1 demonstrates how IP spoofing attack happens.

2.2 Hijacking attack [4] [5]

Another method used to attack the network layer is hijacking. These attacks are easy to implement, but difficult to detect. The basic idea of the attack is to disrupt a session between client and server and take over the IP address of the trusted client. The next step of the attacker is to discontinue the communication between the server and the trusted client and to create a new session with server by pretending to be the trusted client. After the new connection is created, the attacker can take the data he wants from server until this attack will be detect from the victim client (trusted IP) or from the server.

These attacks happens when the server is unware for a certain amount of time of the existence of an attacker on the network and the legitimate client that is disconnected from the network (from the attacker), the attacker will make sure to keep it unaware of the attack.

The attackers usually use different tools to monitor the victim's network, such as WirelessMon, Ethereal, Netstumbler.

If the wireless network will not use advanced encryption methods, and different authentication mechanism, the possibilities to be attacked using hijacking will be high.

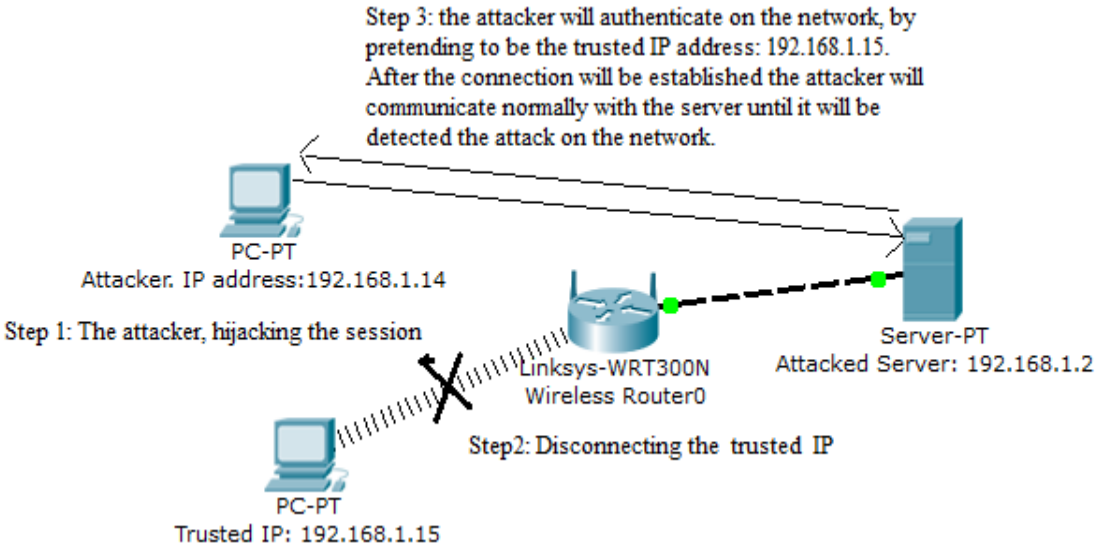

Figure 2: Hijacking
Figure 2 demonstrates how hijacking attack happens.

2.3 The Smurf attack [5] [6]

This attacking technique is a DoS (Denial of Service) attack that happen on the network layer. These attacks are very easy to implement.

The idea of this attack is to overload a server with packets. The attacker will send a high number of packets from a spoofed IP address to the server. The main goal of these attacks is to disable the service the network is providing. Many techniques of attacking are used to achieve this goal. When the attacker wants to realize a Smurf attack, he will transmit to the intended victim a large number of Internet Control Message Protocol (ICMP) by using an IP broadcast address. To achieve this, the attackers use a program called "smurf" that builds a network packet which appears at the attacked server as it is coming from the trusted IP address. When the attacked server will receive this ICMP packets, by default the server will response to the request. The "smurf" program will generate the necessary amount of ICMP requests to overload the victim with ICMP requests and responses until this device will not be able to provide the necessary services on the network. [7]

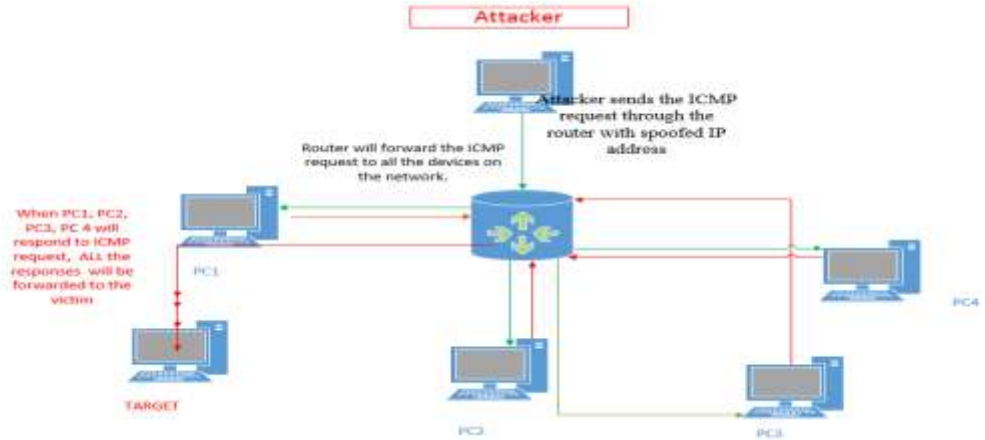

Figure 3: The smurf attack
Figure 3 demostrates a smurf attack.

2.1 Wormhole attacks

These attacks are the most severe attacks and complicated attacks in wireless network. Wormhole attacks are very hard to detect and to protect from them. Even when all the communication on the wireless network provides authenticity and confidentiality, a wormhole attack can happen. The attackers will record the packets at one point of the network and retransmits them to another point of the network using private high-speed network, and then replays them into the network from that point. These kind of attacks are a serious threat against network routing protocols.

Usually in the wireless network, routing protocols have implemented different mechanisms to defend against wormhole attacks; otherwise, the routing protocols will not be able to route more than one hop. [8]

2.2 Blackhole attack

This attack is a type of Denial of Service attack. The main idea of this attack is to drop the incoming and outgoing information between the receiver and the source. In blackhole attack, the attacker will capture all the packets and discard them instead of forwarding them to the destination. The effectiveness of the network will be decreased during this attack, while important packets will not reach the destination. Network parameters such as delay and throughput will be changed during the blackhole attack. The delay will be increased because the packets will not be delivered to the destination. The throughput will be become very less, while it will be used from the blackhole attacker. [10] [11]

2.3 Sybil attack

Sybil attack is a method of attacking by stealing or fabricating the identities of other devices on the network. The attacker will use these identities to operate as multiple identities to other network devices. Usually, this method of attack is used against routing algorithms. There are two types of Sybil attacks: external and internal. Using different security mechanisms, external attack can be prevented. To stop an internal attack is used the method of mapping between identity and entity by one to one. Unfortunately, this attack is able to overlap the mapping by creating multiple identities. [12]

2.4 Sinkhole attack

Malicious device on the network advertises itself to the routing protocols as having the best path to the destination. Some protocols will try to verify if this path is the shortest path to communicate with the destination by using acknowledgment packets. Using these packets, the protocol will understand if this path has reliability, and if the latency is low. The sinkhole attack can transmit false report attacks or reply route messages, making in this way the malicious device look attractive path to forward their packets to the destination[13] [14]

III. ATTACKS ON THE TRANSORT LAYER

During this section we will review attacks which occur in the transport layer. During this section we will review the TCP and UDP attacks. TCP and UDP are protocols of the transport layer. The main characteristics of TCP are: reliable transmission, connection oriented, and confirmed service. This protocol is used to transmit information that request reliable transmission, such as e-mails and file sharing.

Characteristics of the UDP protocol are: connectionless, reduced overhead and latency and does not guarantee reliability. It is used by application which does not require high reliability, such as video streaming, VoIP, IPTV and online games. [4]

TCP and UDP protocols have security vulnerabilities; below we will mention these vulnerabilities:

3.1 TCP flooding attacks.

This method of attacking the transport layer is known also as ping flooding. This attack is denial of service (DoS) attack. Attacker sends to the victim a huge number of ping requests. The victim will respond to these ICMP echo requests by sending ping replies. This process will continue until the victim will be blocked replying this ping requests and responses.

This attack is one of the oldest attacks of the wireless networks. The method of attacking is not effective as before, because it requires a high bandwidth to saturate the network with ping requests and replies. [4]

3.2 UDP flooding attacks.

UDP protocol of the transport layer will be attacked, also by flooding attacks. Before the attacking the victim, the attacker will spoof the IP address of other legitimate devices, to hide his identity. The attacker will send to a random or specified port of the victim system a high number of UDP packets. After this request, victim system will analyze the request and determine what response to reply for this request. If the requested application cannot be offered from the system, the system will reply with the message: "Destination Unreachable". The attacker will send UDP packets to the victim to deplete the network bandwidth, crash the system of the victim, or at least to degrade the performance of the system attacked. [15]

3.1 TCP sequence prediction attack.

To deliver the packets ordered at the destination, TCP transport protocol uses a sequence number for each packet transmitted. At beginning, the attacker will listen the communications between two hosts (host 1

and host 2). One of this hosts is the victim of the attack, let's suppose that the victim will be host 1. Then, the attacker will send request packets to host 2 with the spoofed IP address of the trusted device. The attacker will flood host 2 until a Denial of Service attack will happen and the communication between host 1 and host 2 will stop. After this step, the attacker can issue the packets with correct sequence number, which host 1 is expecting from host 2. Attacker will send the packet with correct sequence number to host A with the spoofed IP address of host B. This packet can damage the network by asking the victim to run malicious scripts or to execute different commands. [16]

IV. CONCLUSIONS AND FUTURE WORK

During the last years, wireless networks are used from many companies. Security remains the main problem and the biggest threat of the wireless networks.

During this study, we reviewed different attacks on the network layer and transport layer that degrade the performance of the wireless networks. The attacks we reviewed on the network layer are IP spoofing, hijacking, smurf, wormhole, blackhole, sybil and sinkhole.

Attacks of the transport layer of the wireless networks that we reviewed are: TCP sequence prediction, UDP &TCP flooding.

During this study, it was observed that attacks which happens on the network layer are many and more dangerous for the wireless network compared with attacks of the other layers especially the transport layer which was studied during this review.

This study, can be further improved by reviewing or proposing different security mechanisms used to prevent these attacks on the network layer and transport layer. Therefore, network administrators can implement these mechanisms and protect or prevent the attacks against the wireless network on the transport and network layer.

REFERENCES

[1]. Simone Soderi, Harri Viittala, Jani Saloranta, Alessandro Mancini, Matti Hämäläinen, Jari Iinatti (2013), " Emulation of Secure Wi- Fi Communication: A Performance Gap Analysis against a Virtual Test-bed ", 13th International Conference on ITS Telecommunications (ITST), IEEE, pp 226-227.

[2]. Priyanka, Harish Mittal, (2016), " A Survey: Attacks on Wireless Networks", Journal of Network Communications and Emerging Technologies, Volume 6, Issue 5, pp 16-21.

[3]. Christiana Ioannou and Vasos Vassiliou (2016),"The Impact of Network Layer Attacks in Wireless Sensor Networks". 2016 International Workshop on Secure Internet of Things (SIoT), IEEE

[4]. Yulong Zou, Jia Zhu, Xianbin Wang, Lajos Hanzo, (2016). "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", Vol. 104, No. 9 Proceedings of the IEEE pp. 1727-1765

[5]. S. S. Manivannan, E. Sathiyamoorthy, (2014)"A Prevention Model for Session Hijack Attacks in Wireless Networks Using Strong and Encrypted Session ID", Cybernetics and Information Technologies, Volume 14, No 3, Sofia.

[6]. Monika Malik, Dr. Yudhvir Singh (2015)"A Review: DoS and DDoS Attacks ", International Journal of Computer Science and Mobile Computing ISSN 2320–088X, Vol. 4, Issue. 6, pp.260 – 265

[7]. Farhan Sajjad, "Denial of Service – The Smurf Attack", University of Windsor, Canada Yih-Chun Hu, Adrian Perrig, and David B. Johnson, 2006"Wormhole Attacks in Wireless Networks", IEEE journal on selected areas in communications, vol. 24, no. 2, pp: 370-380.

[8]. S.Nithya, K.VijayaLakshmi, V.PadmaPriya, (2015), "A Review of Network Layer Attacks and Countermeasures in WSN", Journal of Electronics and Communication Engineering (IOSR-JECE) Volume 10, Issue 6, Ver. I (Nov - Dec .2015), PP 00-00.

[9]. Mohammad Wazid, Avita Katal, Roshan Singh Sachan, R H Goudar and D P Singh , (2013)"Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network", International conference on Communication and Signal Processing, IEEE.

[10]. Rupinder Kaur, Parminder Singh, (2014)" Black Hole and Greyhole Attack in Wireless Mesh Network", American Journal of Engineering Research (AJER), Volume-3, Issue-10, pp-41-47

[11]. RuPurva Sharma (2014)" Survey on Orthogonal Dimensions of Sybil Attack in Wireless Sensor Network", International Journal of Computer Applications, National Conference on Intelligent Systems.

[12]. Sachin Dev Kanawat, Pankaj Singh Parihar, (2011) " Attacks in Wireless Networks", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), Volume-1, Issue-1.

[13]. Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala (2013) " Detection of Sinkhole Attack in Wireless Sensor Networks", Proceeding of the 2013 IEEE International Conference on Space Science and Communication.

[14]. Aarti Singh, Dimple Juneja(2010) "Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks", International Journal of Engineering Science and Technology Vol. 2(8), 2010, 3405-3411.

[15]. Alok Pandey, Jatinderkumar R. Saini (2014) " Attacks & Defense Mechanisms for TCP/ IP Based Protocols", International Journal of Engineering Innovation & Research, Volume 3, Issue 1.

Edvald Sula" A review of Network Layer and Transport Layer Attacks on Wireless Networks. " International Journal of Modern Engineering Research (IJMER), vol. 08, no. 12, 2018, pp 23-27