Analysis of the Data Link and Network Layer Attacks and Defence Mechanisms

Resul DAŞ, Abubakar KARABADE
Department of Software Engineering, Technology Faculty
Firat University, 23119 Elazig, Turkey
resuldas@gmail.com karabadeabubakar@gmail.com

Abstract - Data link and network layer are the OSI reference model of the network component that handled both frame and packet of a data unit. The objective of these layers to transfer a packet from source to its destination in the network system. The traditional architecture of these layers, the adversary considered these layers are the weakest layers in network security. The Attackers are able to compromise these layers and exploited their vulnerabilities. This thread result by attackers received much attention in the field of network security. Because in network system having a secured network is the first priority to reach their requirement. A network is said to be secured if it can sustain from compromised. In order to secure the network, the network administrator must have a good knowledge of understanding the techniques used by attackers and their mitigation. In this paper, we analyse different types of data link and network layer attacks and techniques of these attacks and their countermeasures such as Prevention, Detection and defend mechanisms.

Keywords- Network Attack, Network layers, Detection and Prevention

I. INTRODUCTION

The computer networks are developed to support human network communication such as a person to person exchange information, knowledge, idea, opinion, and advice. Computer networks are mostly connected via Ethernet cable or wireless through radio waves. The computer network is configured base of two types, peer to peer and client/server network. The peer to peer network is implemented on less than ten computers. The client/server network is more suitable for larger area network consists of centralized computer or server act as a storage location of file and application for communication within the network.

The computer networks are designed as stack of layers, each layer builds upon the one below it and each layer do its job separately and pass to the next layer. These layers also provide an interior service above it and correct error that occur on below it [1]. The network layers are organized into two international standard, OSI reference model and TCP/IP model [2].

The OSI reference model is a network stack consists of seven layers. Each layer performs a well-defined function. In the OSI model of the network system, the data link layer is a second layer of the OSI model that provides a reliable link between two directly connected nodes and correct the errors that occurs in the physical layer. However, data link layer consists of device such as switch, Ethernet token ring etc. [3]. The layer above the data link layer is the network layer, the network layer is designed to determine how packet are forward from source to destination. The network layer consists of a router, IP and IPV6 [4] etc. These two layers are used to deliver frame in local network and guide packet to end point.

The TCP/IP model was developed under sponsorship of defence advanced research project agency (DARPA). The TCP/IP model defining the internet protocol consists of four layers and each layer is responsible for difference phase of commutation. Despite the importance of the network and information that it shared, send etc. Secured of this network becoming more a threat with the expansion of network users. Attackers are trying to exploit and compromise and get access to sensitive data [5]. The techniques that attackers used are so efficient and hard to visualise. Because of this reason now majority of organizations are concerned about how they will protect their data against these attackers. This paper will analyse data link and network layer attacks and their defence mechanism.

II. DATA LINK LAYER ATTACKS

The data link layer of a network is a second layer in the OSI reference model that provides forward of data and error correction that happen in physical layer. It also provides a service interface to the network layer. Generally, most of systems administrators of networks do not monitor the data link layer unless there is connectivity issue. Most intrusion detections are applied in high layer of the OSI reference model [5, 6]. However, due to lack of external security control in data link layer security threat become challenging.

The security challenges of data link layer have now received greater attention of many organizations. The attacker used malicious program to exploit system network. However, if the data link layer is hacked, the integrity, essential communication and availability of service to the network layer are exploited. This section will analyse data link layer attacks and their defence mechanism, are listed below.

A. CAM Table Overflow Attack

The CAM table stand for content address memory table. The CAM table is a dynamic table in computer network switch that maps the MAC address to a specify switch port [7]. It maintains all switch ports of their MAC address, allowed uniquely distribution of an information to assign physical addresses. The switch maintains database of MAC address and guide the received frame.

The CAM table overflow attack is an attack in data link layer on a switch. It is a technique employed to compromise the security vulnerabilities of data link layer. The CAM table overflow turns a switch into a hub. The attackers succeed by floods the CAM table with the new MAC address of the switch port by filling a CAM table beyond the capacity of its memory, the table will not long deliver packet base on the MAC address of the switch. The switch is unable to learn the new Mac address and relative path, behaviour like hub begin, start broadcasting Ethernet frames to the flow traffic and every connected attacker can hear the traffic flow through the switch.

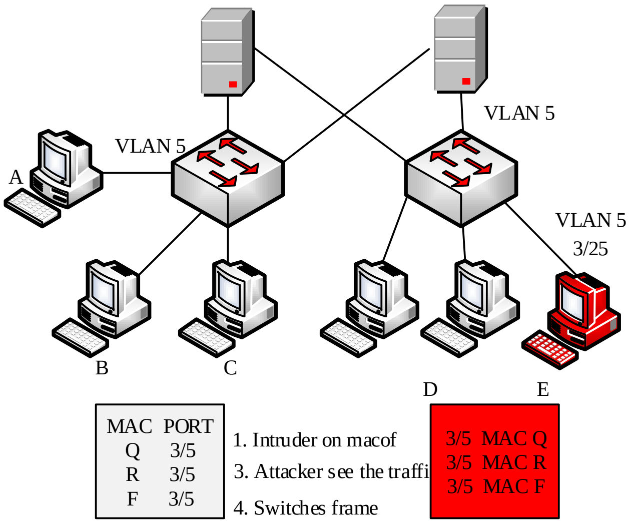

Figure 1 CAM table overflow Attack

The figure 1 described how MAC addresses overflow transpire. The attacker used Macof program tool to compromise the host packet. These tools contain randomly MAC and IP addresses that generate switch from source to destination. The Macof tool fills up CAM table memory with aim of consuming the amount of memory, until the CAM table could not accept the new MAC address. As long the Macof tools remain running the CAM table remain full, the attackers are exploiting the network.

Defence Mechanism: The CAM table overflow attacks, hacker succeed because there is no authentication when client broadcast the MAC addressed, this result the hacker pretend to be thousands of users, providing authentication will prevent the CAM table overflow attack. Moreover, CAM table overflow attack prevents by limiting the number of hosts to switch port [8]. Some big organizations prevent the CAM table overflow attacks by configuring port security of the switch or by specifying the MAC address of a specific switch port. Also can be prevented by allowing switch dynamically learn and fixed the problem.

B. VLAN Hopping Attack

The VLAN stand for virtual local area network. The VLAN is the process of separating a switch into broadcast domains? Allow logically segment of LAN into different network department.

The VLAN hopping attacks occur when the attacker send a packet to a switch port to generate traffic with a VLAN ID of an endpoint [7]. The attacker in VLAN hopping is trying to imitate switch to agree Trunking and send receive traffic between VLANS. The attacker also used a tang to send a double tang. In tagging, the attacker insert a second 802.1q tag near the existing tag, this result the existing tag to strip off by the first switch. Remain tag contains a difference LAN to which the packet will be sent [9]. The figure 2 diagram illustrates how the VLAN hopping occur.

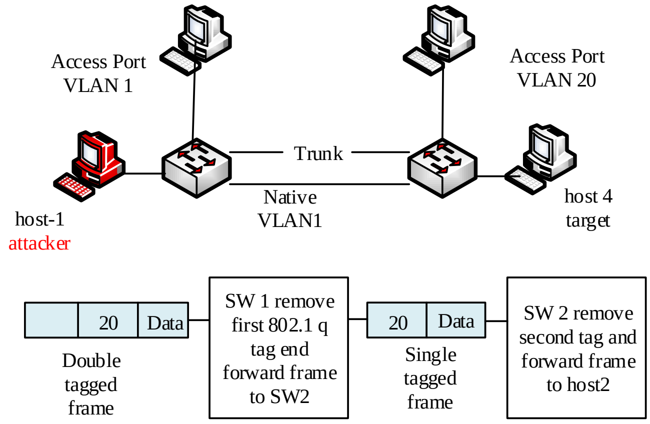

Figure 2. VLAN hopping attack

Defence Mechanism: VLAN hopping attacks, to ensure data link layer did not fall under this attack, all user ports should be assigned as access port and not used port should be switched off or using dedicated VLAN ID for all trunk [10].

C. STP Manipulation Attack

The switch topology of a network redundant link is always hopping and cause loops. This result the Time to Live (TTL) of sending packet already exists in the network layer. The TTL number only magnifies when the packet passing through the router while in data link layer no way to destroy the packet that is in loops and result broadcast storm. The STP is used in data link layer in the switch of network to prevent creation of loops bridging in Ethernet network topology. It provided switch to have redundant link and loop free topology. The STP prevents broadcast storm, identifies one switch as Root Bridge and block all remain data pathway.

The STP manipulation attack occurs when the attacker compromise spanning tree protocol Root Bridge by spoofing. The spoofing of Root Bridge is done by broadcasting out STP configuration and changing bridge protocol data unit (BPDU) force STP to recalculate again and if the attacker can compromise the root bridge, traffic is easy to redact and sniff it [1, 11]. The figure 3 illustrates how STP manipulation happed.

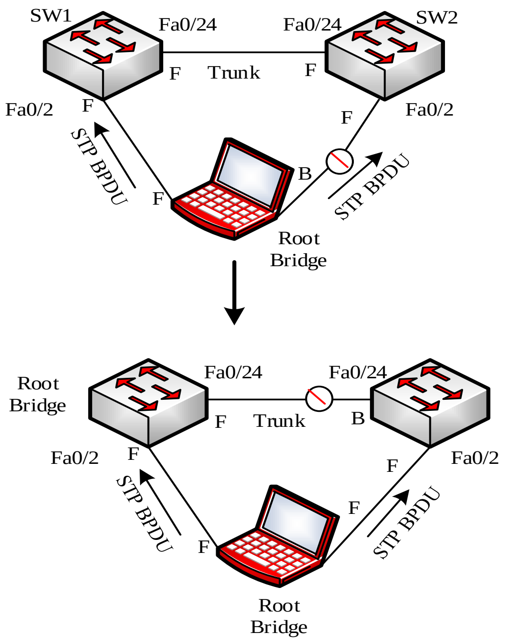

Figure 3. STP manipulation attack

Defence Mechanism: The method to mitigate against the manipulation of STP by using root bridge guards and BPDU guard. These guards are enrichment command that enforces root bridge placement. The STP manipulation also can be prevented by disabling the usage of priority zero [11].

D. ARP Spoofing (ARP Poisoning) Attack

The ARP stand for address resolution protocols. The ARP is a protocol in a network that maps the protocol addresses of internet to sensible machine addresses in local area network [12].

The ARP spoofing occurs when the attacker used to know the ARP address of the host and attempted compromised the network. In ARP spoofing the attacker targets forward a packet to a destination by sending a packet with another host Ethernet address with an aim to compromise the entry of CAM table. When the attacker sends out a request of broadcast ARP address in order to find the MAC address of a specified host and ARP response request by sending the address [13].

The ARP spoofing attack allowed gratuitous reply even ARP request did not receive a response. The figure 4 described how hacker spoofing IP addresses.

Defence Mechanism: ARP spoofing can be defended using timer hold down by setting the length of time entry during ARP cache. The ARP spoofing can also mitigate with intrusion detection tools. In IDS fake ARP message detects and maintain the stability of MAC table. Some small organizations used strength authentication for protection instead of IP address [14].

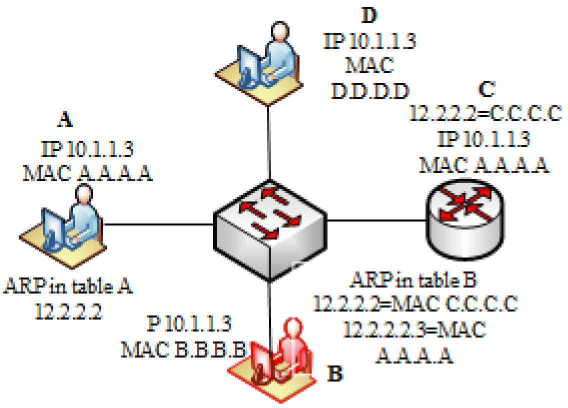

Figure 4. ARP Spoofing (ARP Poisoning) Attack

E. DHCP Starvation Attack

DHCP (dynamic host control protocol) is a client/server protocol that allowed a computer to have their IP address without a pre configure of the original IP address. The server is dynamically giving the IP address to network host.

The DHCP starvation attacks occurs when the attacker request broadcast DHCP with the aim of spoofed the MAC address. The DHCP server some time runs out of IP addresses this result DOS (Daniel service attack) attack [15]. Figure 5 illustrated the behaviours of DHCP attack

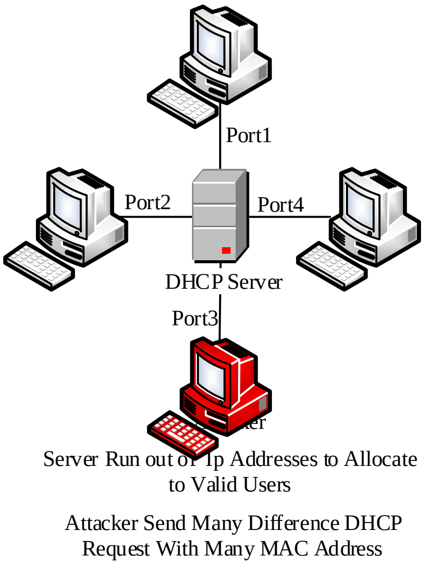
Port1
Port2
Port4
DHCP Server
Port3
Server Run out of Ip Addresses to Allocate
to Valid Users
Attacker Send Many Difference DHCP
Request With Many MAC Address

Figure 5. DHCP Starvation Attack

Defences Mechanism: The DHCP starvation attack is mitigate by reduce number of MAC address of switch port or by implementing port security on the switch.

III. Network Layer Attacks

The network layer is one of the most crucial parts in the OSI reference model of a network. The layer 3 of a network contains main protocol that provided packet service from source to destination for example router, IPV6, IP and Proxy etc. In terms of security the network layer is particularly vulnerable to attack both external and internal sources. This section will explain the types of attacks in the network layer.

A. *IP Spoofing Attack*

The IP stand for internet protocol, is a well-known popular protocol that used for communication across any interconnect network such as VLAN and WAN. The IP has two types of protocol, TCP (transmission control protocol) and IP (internet protocol). The IP is also used in application like electronic mail and file transfer. The network layers of the OSI reference model information packets are routed via their IP addresses.

The IP spoofing is a type of attack in the network layer. The attacker spoofing IP by forging a packet that have an IP source and hide their anonymity with an aim to the compromised the network system. When the attacker forges packet with source IP address, then router will forward the packet to the destination, then router will not check the validity of the packet source address [16]. The goal of spoofing IP to establish a connection that will allow attackers have root access to a destination host and enable them to create a backdoor in the target system. The figure 6 diagram illustrate IP spoofing attacks.

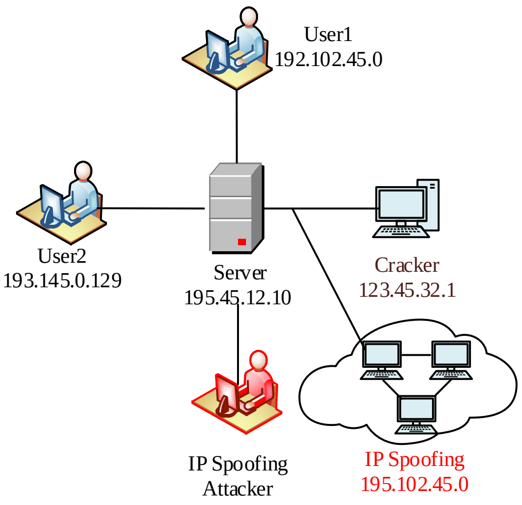

Figure 6. IP Spoofing attacks

Defence Mechanism: The IP spoofing can be defended using router based filter by detecting the compromised packet. The router filter is done by comparing each coming packet interface with the associated expected interface of the IP source packet in MAC table. The IP spoofing can also be prevented by avoiding all applications that used IP address for authentication or by disable the source routing [17].

B. *Teardrop Attack*

The teardrop attack is a type of DOS attack that compromise computer system. This type of attack is done by sending a fragmented IP datagram pair to target a system. The teardrop attack result system to crash in order to create backdoor or get access to sensitive data [18, 19].

Defence mechanism*:* The teardrop attack can be defended by main tools such IDS, Cisco Security program etc. [19].

C. *ICMP Attack*

ICMP standard for internet control message protocol. ICMP is most used protocol in the field of network topology. The aim of ICMP for query error and report to network administrator. The ICMP found on any integral part of the IP address to determine if the system is responding [20].

The ICMP attack happened because of ICMP does not have authentication. This allowed the attacker to use ICMP to target system and intercept packet. The ICMP attack is easy to intercept packets, the attacker only needs to send spoofed ICMP message just like is coming from the original host gateway. Compromised ICMP massage cause overwhelming to network system and create a back door [21].

Defence Mechanism: The ICMP attack can be defended by using IDS, firewall and limiting the network across the component of the network [19, 21].

D. *Ping Flood Attack*

Ping is a command used by network administrator to test computer connectivity. The ping flood attack is another category of ICMP attack; the attacker compromised the bandwidth connection of the network in order to slow the flow of traffic [22]. The ping flood also can be done by sending frequent messages of the ICMP request packet with the aim to target network host, the combination of request and replay cause the network to crash and create a back door [23].

Defence Mechanism: The ping flood is mitigated by reconfigure of the router component or disable the ICMP echo message request of the network [24].

E. *Smurf Attack*

The Smurf attack of network layer involved exploit internet protocol to create denial of service attack [25]. The attacker used malicious program that is called Smurf. These Smurf grogram cause part of the network to be inaccessible. This attack performs by sending ICMP echo request to broadcast network address all the systems will receive the echo request and send a response to adversary source.

Defence Mechanism: the Smurf attack can defended using intrusion detection and vulnerability software [26]**.**

F. *DDOS/DOS Attack*

The denial of Service (DOS) attack is a type of attack in the network layer. DOS attack occurs when the attackers send a packet of the message with an aim to compromise vulnerabilities of the network service [27]. It prevents legitimate of user from getting access of network component by exhaust the functionality of the service and capacity of bandwidth connection. The DOS attack exploits website of large organizations and resulted a business system failure [28].

The distributed denial of service (DDOS) attack is a new type of large scale attack in the network layer. The Distributed denial of service attacks results a victim to denial of service request [29]. The attacks are launched indirectly with large amount of compromised computer system on the network [30]. Before performing distributed denial of service the attacker takes control of many computers over a network and all the computers are vulnerable. In a distributed denial of service attack the attacker used denial of service attack to weaken the computer and inserts malicious code then launches the attack.

The distributed denial of service attack increase frequently and disturbance the global network and take down a popular website like yahoo, CNN and amazon etc. The DDOS attack is hard to defend because they do not target specifies system; they use a large number of zombies and distribute them to a different location, then launch attacks [31]. Figure 7 illustrated the DDOS attack.

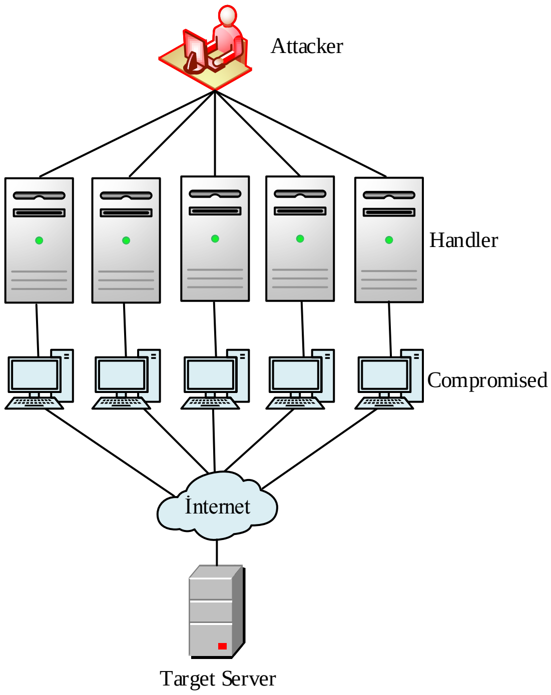

Figure 7. DDOS attack

Defence Mechanism: The DDOS attack is mitigated using a firewall, though the firewall plays crucial role in organizing the security solution and provided complete protection against DDOS attack. It can also be mitigated using intrusion detection to offer anomaly-based capabilities [32,33].

IV. Comparison of Data Link and Network Layer Attack and Defences

The data link and network layer of OSI model are developed to support communication within the network system. The table 1 compared the data link and network layer. This comparison offers generic means to explain network attacks and their functions into multiple phases. If proper security measure is not implemented an attacker can compromise the security holes by using different attack techniques. We address common data link and network attacks and their solutions. The comparison shows that these attacks are productive.

The attack techniques on the data link and network layers are efficient and sometimes are invisible [34-35]. If one layer is attacking the whole communications are interrupted. The below table 1 also describe some techniques for detecting and defends against attackers such as Intrusion Detection Systems (IDS), Packet filtering, access list, firewall and Encryption techniques that can be implemented to secure data link and network layer of a network. In addition, also we described the tool for understanding the data communications between two networked systems.

Table 1. Comparison of Data Link and Network Layer Attack and Defences

Type of the Attack	Attack Agent	Defence and Detection
CAM table overflow	The attacker fills the memory of the MAC table cause to overflow	IDS, switch dynamically fixed the problem
VLAN hopping attack	The attacker trunked the switch	IDS, switch off unused port
STP manipulation	Manipulate the STP cause link layer to loop	IDS, Root bridge guard
ARP Spoofing attacks	The attacker sends a request of ARP	Used Timer Hold Down, filtering, IDS
DHCP starvation attack	Spoofing the MAC address	IDS, reduce the number MAC address
IP spoofing attacks	The attacker spoofing IP addresses	IDS, Authentication, router base filter
Teardrop attacks	Send fragment IP datagram pair cause system to crash	IDS, Cisco security software
ICMP attacks	Spoofed the ICMP message	Provide authentication, IDS
Ping flood attack	Compromised the bandwidth of a network	By reconfigure of the router
Smurf attack	Exploit internet protocol to create denial of service attack	IDS, vulnerability software
DDOS/DOS attack	Result victim to denial of service request	IDS, firewall etc.

V. CONCLUSION AND SUGGESTIONS

Network security is never an easy subject. Many methods are developed to mitigate network infrastructure and communication over an Internet, but these mitigation techniques some are critical to defend the network against intrusion. In order to eliminate all these attack techniques, critical designation of network infrastructures must improve. The network security most provide a secure access to the network from virtually any endpoint and protect against viruses, zombies, spam, phishing and other attacks with multiple threat-detection techniques.

This paper analysis the most well-known attacks techniques of data link and network layer. These network attacks are most prompted problem that a design to compromise the network resources like server, bandwidth, and disk space etc. There are many different types of these attacks include CAM table overflow, VLAN hopping, STP manipulation, ARP spoofing, DHCP starvation, IP spoofing teardrop, ICMP, Ping flooding, Smurf, and DDOS attacks. In addition, we analysed some of these attack mitigation techniques such as IDS, IPS, and IP trace back. These mitigation techniques overcome these attack problems by configuring a switch and router.

Also we compare all these types of attacks and their mitigation techniques. The comparison shows the behaviour of the attacker that used to eavesdrop traffic, manipulate data and deny the flow of information in the network system and we have given some trick to mitigate against most common attacks, also the limitation of the existing solution. These attackers are mostly attacking switch and router of the network.

We can suggest that a new environment that will suit a network security system in data link and network layer, using threat monitor. The threat monitor will be distributed across the router and switch. Will capture all the traffic in log file. This log file will contain information about every transferred response and request. By applying specifies technique to a log file can quickly record a broadcast storm and analysis using machine learning and data mining techniques. After analysis and identify the cause of the broadcast storm, the threat monitor will develop a solution to the problem and reports to system users.

REFERENCES

[1] Simoneau, P. (2006). "The OSI Model: Understanding the Seven Layers of Computer Networks", "Global Knowledge Training LLC.", 1-11.

[2] Yang, G. (2010). "Introduction to TCP/IP Network Attacks", 1-10.

[3] Larmo, A., Lindström M., Meyer M., Pelletier G., Torsner J., and Wiemann H. (2009). "The LTE Link-Layer Design", "IEEE Communications Magazine", Vol. 47, 1-8.

[4] Waichal, S., Meshram, B. B. (2013). " Router Attacks-Detection And Defense Mechanisms", "International Journal of Scientific & Technology Research", Vol. 2, 1-5.

[5] Futoransky, A., Notarfrancesco, L., Richarte, G., Sarraute C. (2003) "Building Computer Network Attacks", "Core Security Technologies" 1-10

[6] Altunbasak, H., Owen H. (2007). "An Architectural Framework for Data Link Layer Security with Security Interlayering", "SoutheastCon, 2007. Proceedings. IEEE", 1-8.

[7] Buhr, A., Lindskog, D., Zavarsky, P., Ruhl R.(2011). "Media Access Control Address Spoofing Attacks against Port Security", 1-8.

[8] Kh., A. W, Cai, Dr. L., Alyawe, S. A. (2012). "A new verification method to prevent security threads of unsolicited message in IP over ethernet networks", "International Journal of Computer Networks & Communications", Vol. 4, 1-11

[9] Nanak, G. (2013). "Effective Remote Management for Inter-VLAN Routing Networks", "pecial Issue for National Conference On Recent Advances in Technology and Management for Integrated Growth 2013 (RATMIG 2013)", ISSN 2319 - 4847, 1-6.

[10] Lundberg, S. (2014). "VLAN Hopping", "Advanced LAN Technologie" 1-8

[11] Maj, S. P., Veal, D., Makasiranondh, W. (2010). "Using State Model Diagrams to Manage Secure Layer 2 Switches", "International Journal of Computer Science and Network Security", Vol. 10, 1-4.

[12] Abdur Rahman, Md. F., Kamal, P. (2014). "Holistic Approach to ARP Poisoning and Countermeasures by Using Practical Examples and Paradigm", "International Journal of Advancements in Technology",Vol. 5, 1-10.

[13] Bruschi, D., Ornaghi, A., Rosti, E(2013). "S-ARP: A Secure Address Resolution Protocol∗", "Italian Dept. of Education and Research F.I.R.S.T. project.", 1-9.

[14] Hofer, C., Wampfler, R. 2010, "IP SPOOFING", 1-7.

[15] Mukhtar, H., Salah, H., Iraq, Y. (2012). "Mitigation of DHCP Starvation Attack", "Journal of Computers and Electrical Engineering", Vol. 38, 1-10.

[16] Duany, Z., Yuan, X., Chandrashekar, J. (2006). "Controlling IP Spoong Based DDoS Attacks Through Inter-Domain Packet Filters", "IEEE INFOCOM 2006", Vol. 5, 1-30.

[17] Mirkovic, J., Jevtic, N., Reiher, P. (2005). "A Practical IP Spoofing Defense through Route-Based Fltering", 1-14.

[18] Trabelsi, Z., Ibrahim, W. (2013). "A Hands-on Approach for Teaching Denial of Service Attacks: A Case Study" "Journal of Information Technology Education: Innovations in Practice", "Volume 12", 1-9.

[19] Choudhary, K., Shilpa, M. (2010). "Smurf Attacks: Attacks Using ICMP", 1-3.

[20] Prasad, B., K., M., Reddy, A., R., M., Venugopal R., K. (2014). "DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey", "Global Journal of Computer Science and Technology: E Network, Web & Security", Vol. 14, 1-19.

[21] [20]. Choudhary, Kavita, Meenaksh, and Shilpa. Smurf Attacks: Attacks Using ICMP (2011): 1-3.

[22] Kaushik, A., K., Joshi, R., C. (2010). "Network Forensic System for ICMP Attacks", "International Journal of Computer Applications", Vol. 2, 1-8.

[23] Kumar, A., Tilagam, P., S. (2011). "A Novel Approach for Evaluating and Detecting Low Rate SIP Flooding Attack", "International Journal of Computer Applications", Vol. 26, 1-6.

[24] Kumar, A., Sharma, A., S., Singh, A. (2011). "Performance Evaluation of BST Multicasting Network over ICMP Ping Flood for DDoS", "International Journal of Computer Science & Engineering Technology (IJCSET)", Vol. 2, 1-9.

[25] Geneiatakis, D., Vrakas, N., Lambrinoudakis, C. (2009). " Utilizing Bloom Filters for Detecting Flooding Attacks against SIP Based Services", "Computer security", 1-14.

[26] G.R, Z., Kabiri, P. (2011). "Identification of Effective Network Features to Detect Smurf Attacks", 1-6.

[27] gtakhbayar, N., Battulga, D., Sodbileg, Sh. (2012). "CLASSIFICATION OF ARTIFICIAL INTELLIGENCE IDS FOR SMURF ATTACK", "International Journal of Artificial Intelligence & Applications (IJAIA)", Vol. 3, 1-5.

[28] Alomar, E., Gupta, B, B., Ppayah, S., K. (2012). "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art", "International Journal of Computer Applications", Vol. 49, 1-6.

[29] Elleithy, K., M. (2011). "Denial of Service Attack Techniques: Analysis, Implementation and Comparison", "SYSTEMICS, CYBERNETICS AND INFORMATICS", Vol. 3, 1-6.

[30] Alomar, E., Gupta, B., B., Ppayah, S., K. (2012). "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art", 1-6.

[31] Sandeep, Rajneet. (2014). " A Study of DOS & DDOS – Smurf Attack and Preventive Measures", "International Journal of Computer Science and Information Technology Research", Vol. 2, 1-6.

[32] Mirkovic, J., Reiher, P. (2010). " A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", "This work is funded by DARPA under contract number N66001-01-1-8937.",Vol. 34 , 1-10.

[33] Beitollahi, H., Deconinck, G. (2012). "A Four-Step Technique for Tackling DDoS Attacks", "The 3rd International Conference on Ambient Systems, Networks and Technologies (ANT-2012)", Procedia Computer Science 10 (2012) 507 – 516, 1-10.

[34] Gündüz, M.Z., Daş, R., "Yerel Alan Ağları İçin IP Tabanlı Saldırı Tespit Uygulaması ve Güvenlik Önerileri", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (6th International Conference on Information Security and Cryptology - ISCTURKEY 2013), pp.302-307, 20-21 Eylül 2013, ODTÜ, Ankara.

[35] Gündüz, M.Z., Daş, R., "Kablosuz Yerel Alan Ağlarına Sızma Uygulaması ve Temel Güvenlik Önerileri", 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (7th International Conference on Information Security and Cryptology - ISCTURKEY 2014), pp.295-300, 17-18 Ekim 2014, İstanbul Teknik Üniversitesi, İstanbul