2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)

Network Security Issues of Data Link Layer: An Overview

Shahid Mahmood
Department of Computer Science,
Virtual University of Pakistan,
Lahore, Pakistan
Email: shahid1mahmood_8@yahoo.com

Syed Muhammad Mohsin
Department of Computer Science,
COMSATS University Islamabad,
Islamabad, 45550, Pakistan
Email: syedmmohsin9@yahoo.com

Syed Muhammad Abrar Akber
School of Computer Science and
Technology, Huazhong University of Science
and Technology, Wuhan, 430074, China
Email: abrar@hust.edu.cn

***Abstract*—There is a cardinal infrastructure of application software's, protocols, and physical devices over different sort of wired and wireless networks, that need to communicate with each other, whether located not only on earth but also in the space. OSI seven-layers model has become an international standard to communicate securely and confidently among different kinds of the corporate networks while keeping the other OSI layers unfamiliar with the current layer of communication. This secrecy among the layers results in vulnerability to attack in a way that if one layer is compromised to attack, the other layers will not be able to detect it properly. This individuality of OSI layers makes the whole network severely vulnerable to attack particularly due to the data link layer as compared to other layers. Generally network security problems at layer 2 are not properly addressed as compared to other layers, rather the people focus on the device's security for the whole management system instead. This paper encompasses network security problems faced due to lack of hardening the layer 2 and it also describes, how it makes a LAN or the system of networks more vulnerable to attacks, especially for the MAC flooding, ARP spoofing, VLAN hopping, DHCP attacks, Denial-of-Service (DoS) and Spanning Tree Protocol in a very concise manner.**

***Index Terms*—OSI model, Security, DoS attack, ARP, STA**

I. Introduction

In the recent era, we have occasionally listened about the hacking events occurred in a government portal, research institute security center, hacked the sensitive information from an oil company, jammed the power station or an airport. As the Information Technology (IT) and communication equipment such as cellular phones and the tabs are gradually becoming an essential part of our daily life, the probability of such attacks is rapidly increasing correspondingly. These devices are making the life more convenient and getting our trust rapidly, as well. For instance, these devices are performing functions of perception control. The convenience got by human is not cost-free, as they are putting our lives, our country, and even the educational institutions on risk. The attackers getting access not only to the private lives of humans but also to the critical infrastructures of industries and the country [1]–[4].

Mostly, network layer in the OSI model is considered the weakest section. While the layer 2 (data link layer) is ignored and not handled properly, that can be the possible weakest layer among all the OSI model [3]. Researchers have devised the techniques to prevent trojans, malicious emails, infected documents, and the application from the transport layer or the network layer. But they ignore the data link layer and mostly focus on the security of the device itself, rather focusing on the whole management systems of an enterprise [5]. However, to attack the data link layer is not an easy task, and most of the times, network administrators think it is safe, but they underestimate the attackers.

Usually, an attacker can affect the IP and Wireless LANs in the following ways.

- Denial of Service Attack on the LAN
- Eavesdrop the electronic transmission
- Analyzing and manipulating the flowing data
- Two or more than two of above attacks in combination

If an attacker is able to apply any of the above attacks at the LAN or network of systems, he can affect the comprehensive security strategy of an organization, critical infrastructure of electronic communication, government management systems and/or the public institutions seriously. Usually, a critical infrastructure within a country is monitored via internet security service providers and mobile communication companies. There are pros and cons of information transmission through the local area network and/or internet. For instance, control information, sometimes can't be successfully transmitted to the end devices due to denial-of-services (DoS) attack. DoS attack is easy to be implemented in the Wireless LANs as the frequency jamming equipment are easily available commercially. In last few years, the Wi-Fi technology has flourished very rapidly, and Wi-Fi 6 has achieved its theoretical speed of

978-1-7281-4970-7/20/$31.00

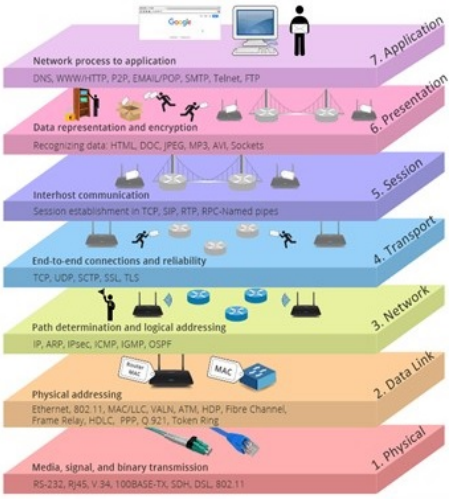

Fig. 1: OSI seven-layer model [1], [3], [10]

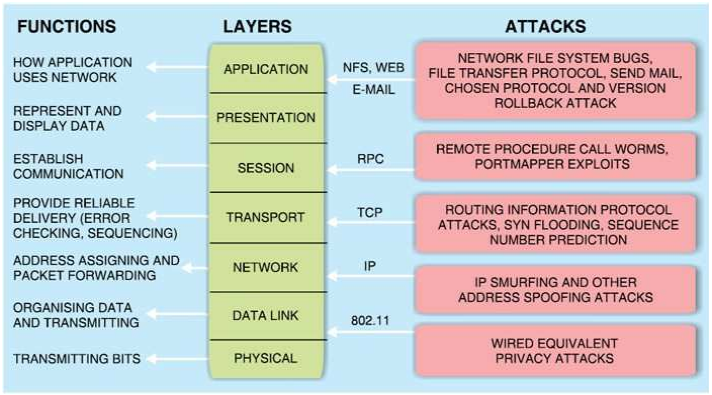

Fig. 2: Functions and attacks at each layer of OSI model

about 9.6 Gbps. By this development in data transmission, one can imagine the future of Wi-Fi technology [4], [13], [17].

In summary, above-mentioned attacks are likely to attain the IDs and user passwords, which is a threat to wireless local area networks. On the other hand, the manufactures are also aware of the attacking techniques, so they also do every possible effort to mitigate these threats. For e.g., the efforts made by the manufacturers to mitigate the Layer 2 CAM overflow attack, Cisco has introduced new technology into iOS called port security. In this paper, we are particularly focusing on the security problems and potential back-doors in the data link layer of the OSI model.

Section 2 of this study elaborates the background of the topic while prominent security attacks on data link layer are discussed in section 3 of this study. Section 4 is composed of conclusion and the future work.

II. Background

To comprehensively understand the network security problems and issues in the data link layer, we need a brief introduction to this layer. The OSI seven-layer model was developed according to the International Organization for Standards (ISO), so that different kind of devices having a variety of software applications installed, distinct physical characteristics, and interfaces can communicate with each other securely and confidently. Each layer above the current layer is served by the current layer and each above layers rely on the functionality of its attached downward layer. But the functionality of each layer is contrasting from each above and below the attached layer [6]. Fig. 1 of this study shows the OSI reference model having a short description of each layer. Whereas, role and responsibility along with potential threats at any specific layer are shown in Fig. 2.

Data link layer establishes the communication among the variety of devices in the system of networks, identifying their peculiar MAC address, corrects the errors occurred at the physical layer and transfers data on the functional and procedural bases. Data link layer consists of two sub-layers, Logical Link Layer (LLC) and MAC layers. Layer 2 of the OSI model is responsible to provide the following functionalities [7]–[9].

- Framing
- Access control
- MAC addressing
- Data rate control
- Media access control (MAC sublayer)
- Error correction received from the physical layer

III. Security attacks at data link layer

Considering the importance and criticality of data link layer in OSI model, we have selected it for comprehensive survey related to its security issues. Following section encompasses the detailed description of security threats of data link layer.

A. Spanning tree protocol

There can be multiple paths among the client and server to provide a backup path, while the original path is not available. Due to multiple paths among a server and a client's system, three types of frames can loop forever in the network that is uni-cast, broadcast, and multi-cast. It is the spanning tree protocol (STP) that detects these looping frames and prevent them from being forwarded to the next switch or bridge in the network, having multiple paths. Spanning tree protocol uses a spanning tree algorithm (STA) called 802.1D IEEE and it is designed to run on the switches and/or bridges that are compatible with standard 802.1D IEEE [11]. STP ensures that there are no loops while having redundant links in the network. In case of failure of the original link, these are the redundant links that provide the connectivity on the local area network. If we don't employ a single STP at a time on the switch of a local area network (LAN), then in case of failure of the original path, there will be several paths having loop messages in the intended network.

There are several types of STPs. It is recommended to use a single type of STP at a time, to avoid the timing problems on the switched networks. These timing issues may result in blocking and forwarding problems in virtual local area

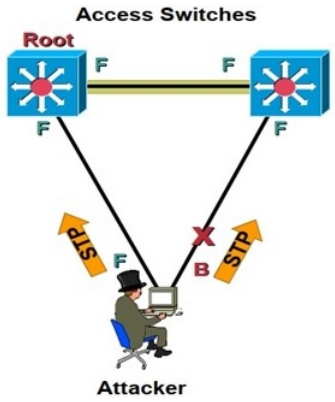

Fig. 3: Spanning tree protocol before root privileges [8], [12]

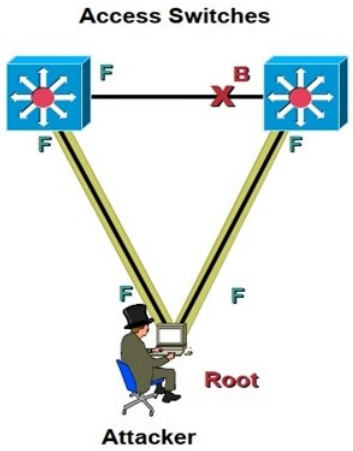

Fig. 4: Attacker is able to illegally listen the traffic [8], [12]

networks (VLANs). Because at a time, a single switch can handle a single flavor of STP. There is a main control unit in the network called root bridge, responsible for doing decisions related to the network, for example, it decides about the port, either to put it into a forwarding or blocking mode etc. On the bases of the network devices, VLAN is classified into two environments, one is switched environment and other is the bridge environment. In the switched environment, usually, the root switch is considered the root bridge of the network. As each VLAN has its domain, so each VLAN must have its separate root bridge as well. However, a single switch may serve as the root of a single or all the VLANs simultaneously.

In bridge environment, decision of root can be made automatically or manually, however,the wrong selection of the root bridge can result in sub-optional paths in the networks. For the selection of a switch or a port as a root switch or a trunk port accordingly, we use the multi-cast messages called bridge protocol data units (BPDUs). This BPDU is considered the configuration messages in the VLANs. Root Bridges are responsible to multi-cast the BPDUs to the other switches that use a formula to determine which one the needed to be disabled and which one allowed to forward traffic on to the VLAN, as show in Fig. 3. The bridge having the least cost or smaller root ID is selected as the root bridge and all other switches not allowed to forward the traffic and/or not to become a root bridges due to their higher root ID. Other switches do not advertise their ID anymore due to the root ID.

The attacking technique in this scenario is that an attacker multi-casts the falsely configured BPDUs to the switches on a VLAN. Devices on the corporate network consider the attacker's switch as the root bridge. To make the attack successful, the attacker needs two bridges, two switches or two wireless local area network (WLAN) connections to influence the network effectively. After becoming root, the attacker can listen to all the traffic of the victim's network and even can insert new frames. The attacker being the root can do a man-in-the-middle attack (MITM) while being in the middle position of the server and the client [12]. This scenario is shown in Fig. 4 of this study.

B. Basic VLAN hopping attack

According to IEEE 802.1Q, a root bridge is allowed to carry all the VLAN's traffic from one switch to the other switch, while the access link switch connects the end-users to access their particular VLAN. There can be many open ports over a VLAN to allow the request of a new connection from the members of the network. Anyone can connect his laptop to the local area network through these open ports. To automate the discovery of trunk links between the switches, Cisco has devised a protocol called dynamic trunking protocol (DTP). The DTP can be used to negotiate as well as for the formation of new trunk links in a VLAN. Furthermore, DTP can also be used to discover the encapsulation used, either Cisco ISL (Inter-Switch Link) or IEEE 802.1Q. [1], [13]–[15].

An attacker sends the false DTP messages over a VLAN to turn an access link into a trunk link to access all the traffic that is normally filtered from the access links. In this way an attacker can view all communicating information of a trunk link.

C. Double tagging VLAN hopping attack

To operate the VLANs, the messages containing additional 802.1Q header rotate among the backbone and end access point in the entire network. The 802.1Q header contains two tags, one for the end-user that is outer tag and other is the service provider that is the inner tag of the message rotating in the VLAN. The double tags header allowed only to the root switches allowed to send while the access links are not allowed in the VLAN. The outer tag is stripped out as the frame enters the trunk links of a VLAN (dynamic desirable option enabled switch), while the other tag contains the victim's related information delivered to the victim, as shown in Fig. 5. Cisco supports two types of ports to connect with devices either to a single or multiple VLANs i.e., trunk port and access port. A Trunk port is usually a link connecting two switches or one router and one switch or two routers forming a backbone of the VLAN, while the access ports are used to connect the end-users. An attacker usually lies on the access port, wants to access a victim host from the same VLAN but on the other

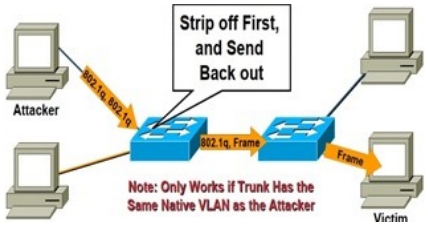

Fig. 5: Double tagging VLAN hopping attack

TABLE I: Summary of critical security attacks at data link layer

Attack Name	Description
MAC Attacks (CAM Table Flooding)	A switch is flooded with random MAC address. This makes the switch's table to become filled. The switch is the forced to operate like a hub (i.e. frames are forwarded out to all the ports)
STP Attacks	Wrong BPDU frames are sent to switches to change the spanning-tree topology. DoS attacks can be launched if the topology is frequently changed.
CDP Attacks	Wrong CDP information is sent to switch or routers to interfere with their operations.
VLAN Attacks	By sending wrong VLAN information to switches, either i) configurations of networks are changed, or ii) operation of network are severely affected.
DHCP	Networks are attacks by interfering DHCP operations. Attacks like a man in the middle can be launched.
ARP Attacks	Networks are attacks by interfering ARP operations. In these attacks, network operation can be severely affected (e.g. a rogue router can become the default gateway of a network)

access port, traversing through the trunk port in its way. Cisco switches use the 802.1Q tag enabled on the trunk ports. There are four states in which Cisco switches can operate, as stated below.

- Trunk
- Dynamic auto
- Dynamic desirable
- No-negotiate

Three modes of Cisco switches, trunk, dynamic auto and dynamic desirable permit changing an access port into trunk port, while the other mode do not allow an access port to be a trunk port. This sort of attack can be performed only in one direction while being on the same VLAN, as shown in Fig. 5 of this study.

Now, we are going to briefly discuss the attacks that can affect the development of system-security policy and are the hot topics for the implementation of basic safety operations. These attacks are more common as compared to the first ones mentioned in the earlier sections as given in Table 1 of this study [14], [16].

D. Cisco Discovery Protocol attack

Cisco discovery protocol (CDP) is a network-independent and media-independent protocol, enabled by default in the Cisco switches and routers hence, can send the CDP announcements over the corporate network. Cisco switches for their configuration rely on the CDP announcements that consist of the version of the operating system, hostname, port ID, device type, duplex setting, virtual trunking protocol (VTP) domain, the power drawn, source and destination addresses and time-to-live. However, these frames are highly extensible due to the use of type-length-value (TLV) format. So, further information can be added to these announcement frames due to the TLV features.

To avoid the mis-configuration of dynamic routing protocols, CDP uses a method of operation called on-demand routing. In which CDP announcements provide the routing information on demand. The devices in a corporate network can update their CDP database from the headers of the packet received accordingly and new devices can be added to the corporate network. However, Cisco devices can't propagate the CDP messages. Cisco switches use dynamic trunking protocol (DTP) that supports four modes of operation, mentioned above. If a Cisco switch is in the first two modes of operations i.e., dynamic desirable and dynamic auto, an attacker will be able to convert an access link into a trunk link. In the first mode of operation, Cisco root routers and switches can send the CDP messages to other devices on a corporate network, while the other devices can configure themselves accordingly for their connectivity to the network. The information sent through these messages consist of sender/receiver IP address, Cisco IOS, software version used in Cisco devices, time to live a packet, the model number of switches and routers and their capabilities, etc. The time-to-live information is used to define the life of packet in a corporate network. When the routers and switches are in first two modes of operations, an attacker not only can get the information related to the network but also can over-flow device's memory and can potentially crash the root switches by sending false numerous CDP frames.

In the generation and during transmission of CDP frame no authentication is provided. Hence, a false CDP frame can easily be crafted and sent over the network to the connected devices. If an attacker gets access via Telnet, he can collect the CDPs and hence the necessary information of entire topology of the network running at layer 2 and 3. CDP attack scenario is shown in Fig. 6. This useful information makes him able to craft a very effective attack against the network, for instance, man-in-the-middle attack [4], [13].

E. CAM table overflow attack

CAM stands for content addressable memory (CAM) table that is system memory construct. Ethernet switches are vulnerable to CAM table overflow attack. For instance, Cisco switches store the MAC addresses, corresponding physical port and VLAN ID on which end-user is located.

Usually, Cisco CAM table is designed to store 100 to 10000 MAC addresses simultaneously. If the new MAC addresses are being received continuously at the respective port from client of a particular corporate network, then it may lead to CAM table overflow attack. Each entry remains about 300 seconds in the CAM table of the ethernet switch. CAM table stores the MAC addresses for the respective port number for each entry made in the CAM table. If an address already exists in

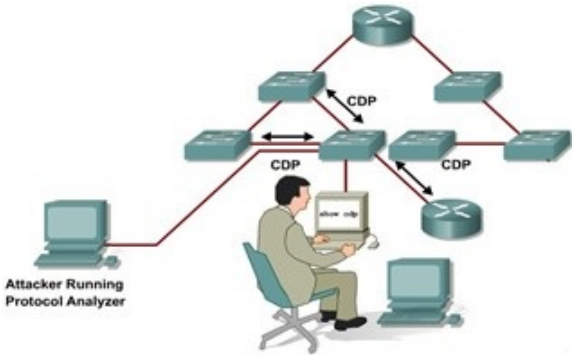

Fig. 6: CDP attack [2], [17], [18]

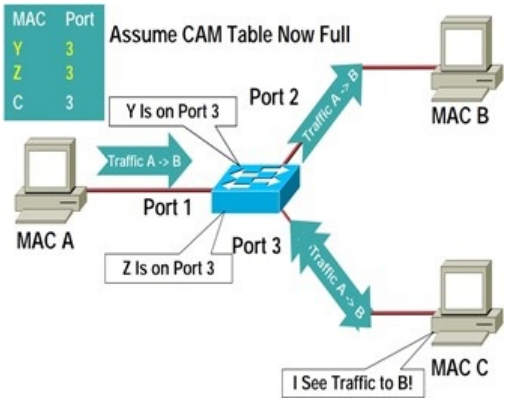

Fig. 7: CAM table over-flow attack [2], [16], [17]

the table, then only the time-stamp is updated otherwise new entry is made in the table for a new address that is a new connection from the member of a VLAN.

Attackers take advantage of the max size of the CAM table and send numerous packets containing false MAC addresses. So, the received number of MAC addresses exceeds the max table capacity. In this situation, the switch turns into a hub and enables the attacker to access every client in a corporate network or a virtual local area network (VLAN). Attackers take the desired exact information of the hosts and the structure of a local area network (LAN) and perform a man-in-the-middle (MITM) attacks more effectively in the corporate network as shown in Fig. 7 [4], [13], [17].

F. MAC spoofing attack / ARP poisoning

The address resolution protocol (ARP) is a protocol that normally works on the network layer, however, MAC address spoofing is performed on the data link layer. In the spoofing process, gratuitous ARP (GARP) packet is sent over the network. The GARP is sent to announce the combination of spoofed MAC and IP addresses. The devices connected to the local area network or virtual local area network (VLAN), maintain a cache containing the IP addresses and their corresponding MAC addresses for each entry. Because there is no authentication system for received ARP packets, a device can send false frames containing false MAC addresses. So,

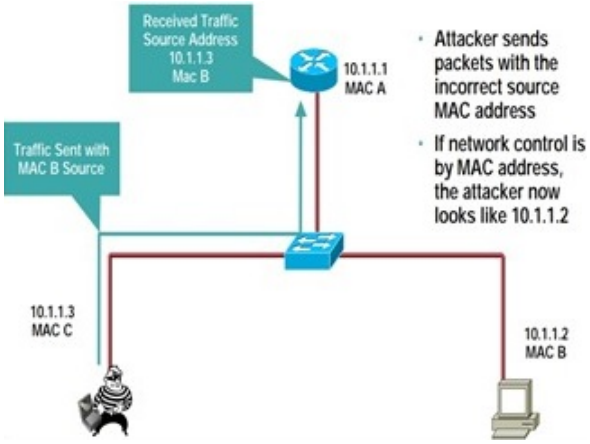

Fig. 8: MAC spoofing attack [10], [16], [17]

the cached entries in the target devices also change upon receiving a false GARP packet. The whole process of making a false entry in the ARP cache of a device is called the ARP poisoning. An attacker can proclaim his access switch as the default gateway for the corporate network. An attacker uses ARP poisoning for this purpose, as shown in Fig. 8. The ARP poisoning enforces all the gateway traffic to pass through the attacker's switch. This scenario makes him able to analyze all the traffic before forwarding to the real gateway device. An attacker can systematize the necessary changes to the packets which he enforces through his false gateway [17].

G. DHCP starvation attack

Dynamic host configuration protocol (DHCP) is used for host configuration in the IP networks to allow communication among the DHCP server and DHCP clients. The DHCP server provides the configuration parameters for an IP-network such as default gateway, host IP addresses, lease time for an IP address and others. A router can also be configured as a DHCP server. A DHCP server provides necessary information automatically upon the request made from a DHCP client. In the DHCP starvation attack, an attacker may send tons of false IP addresses assigning requests so that the total capacity of the DHCP server exhausts and DHCP server can't serve the real clients anymore, as shown in Fig. 9 of this work. In this situation, an attacker can set a false DHCP server, on the IP network which sends the DHCP replies to the clients that are not the replies from actual DHCP server but these are the manipulated replies from illegal DHCP server [10], [17].

H. Wireless 802.11 (Wi-Fi) attack

Wi-Fi is an acronym of the 'wireless fidelity' to provide WLAN services through compatible devices such as Wi-Fi routers. The Wi-Fi networks (WLANs) are easier to establish and maintain as compared to the corporate network consisting of ethernet cables. Wi-Fi cards are most of the time built-in on the computers, others can add external cards to have Wi-Fi network services. While the wired (ethernet) connections require to have the cables to be properly installed. Due to

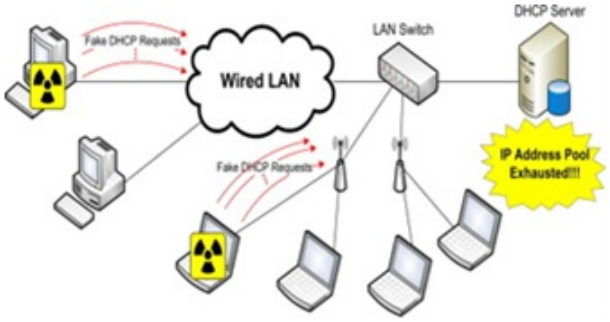

Fig. 9: DHCP starvation attacks [1], [3], [10]

their simple and less costly installation, an attacker can do the following things to the Wi-Fi local area network (WLAN).

- Easily can put himself between the server and the client
- Can do the Denial-of-Service (DoS) attack
- Able to capture all the traffic

Two ways by which an attacker can connect to a Wi-Fi LAN, are given in the following.

- Establish a false access point (AP) having higher intensity signals than the original one and provide a similar configuration as the original one have and wait for the new clients got connected with it.
- De-authenticate the original one or two clients of an AP and create a new client having same credentials as the real AP, so that de-authenticated client got connected with rogue AP.

The denial-of-services attack on a Wireless LAN can be formed by the following two possible ways.

- There can be made numerous requests to the wireless LAN that will over-flow the resources of an AP. Hence, the access point will reject all the original clients' connection request made further.
- Many devices are commercially available that can affect the operational frequency of AP and the access point will be unable to provide the services on the same frequency.

An eavesdropper can capture all the traffic from an AP if he has simply a wireless network card. An attacker may use the following two easy steps to capture the network traffic through NIC.

- Install the wireless network interface card
- Put the wireless NIC into monitoring (promiscuous) mode [4], [18].

IV. Conclusion and future work

Until last decade of the 19th century, traditional networking consisted of the hubs, switches and ethernet cables. The technology of today is based on light waves and electromagnetic waves for connectivity such as the Wi-Fi 6, rather relying on the ethernet cables [19]. In current era, about 61 percent of the employees within an organization have access to the Wi-Fi networks in their offices. This ease of access has put our secrecy on risk and has introduced new vulnerabilities such as unauthorized access to the critical infrastructure of an organization, company records and even solidarity of a country.

Focusing on the importance and criticality of network security issues at data link layer, we have presented a detailed overview of the security problems related to network layer 2 (data link layer), and briefly consolidated on the techniques through which a network administrator conceives vulnerabilities that may occur at other layers of OSI model due to the data link layer. We emphasized on developing a general understanding of the network security problems at layer 2 of OSI model. However, the developers and manufacturers are also on their way to perform their role in the prevention of network hacks for example techniques developed by the developers to overcome the CAM overflow attacks is named as the port security provided by the Cisco manufacturers. Protection systems exist to prevent the network security problems such as the host-based intrusion protection (HIP), firewalls, intrusion protection systems (IPS), host-based intrusion protection (HIPS) etc. In future we will devise a comprehensive framework to counter security threats of data link layer.

References

[1] A. Annapurna, S. Mohammed, D. Madhuri, Data Link Layer-Security Issues, International Journal of Computer Science & Engineering Technology (IJCSET), vol. 4, p. 4, 1009 - 1012.
[2] J. szombat, Hackerek támadták meg az Európai Bizottságot, [Online]. Available: https://www.origo.hu/nagyvilag/20121110-hackerek-tamadtak-meg-az-europai-bizottsagot-azerbajdzsanban.html.
[3] GReAT, The "Red October" Campaign, 14 January 2013. [Online]. Available: https://securelist.com/the-red-october-campaign/57647/.
[4] Wi-Fi, 2019. [Online]. Available: http://en/Wikipedia.org/wiki/Wi-Fi.
[5] M. LAJOS, Az informatikai biztonság egy lehetséges rendszertana, 2008.
[6] B. T. B. Risteski, Simulation Analysis of DoS, MITM and CDP Security Attacks and Countermeasures, Future Access Enablers of Ubiquitous and Intelligent Infrastructures, p. 197 - 203, 2015.
[7] Data Link Layer, July 2019. [Online]. Available: http://www.ee.surrey.ac.uk/Projects/CAL/networks/Data Link Layer.
[8] Hacking Layer 2: Fun with Ethernet switches, Cisco, 2013. [Online]. Available: https://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.
[9] A. O'Keeffe, The difference between Layer 3 and Layer 2 networks, 2019. [Online]. Available: https://www.aussiebroadband.com.au/blog/difference-layer-3-layer-2-networks/.
[10] OSI model, Wikipedia, 2019. [Online]. Available: https://en.wikipedia.org/wiki/OSI model.
[11] M. Sanchez, Encyclopedia of Parallel Computing, 2011, p. 12 - 40.
[12] Spanning Tree Protocol, Cisco, 2019. [Online]. Available: https://www.cisco.com/c/en/us/tech/lan-switching/spanning-tree-protocol/index.html.
[13] D. F. a. K.-Y. W. Kai-Hau Yeung, Tools for Attacking Layer 2 Network Infrastructure, 2008.
[14] VLAN hopping, wikipeida, 2019. [Online]. Available: https://en.Wikipedia.org/wiki/VLAN hopping.
[15] What is Spanning Tree Protocol (STP), 2019. [Online]. Available: http://www.omnisecu.com/cisco-certified-network-associate-ccna/what-is-spanning-tree-protocol-stp.php.
[16] G. Marro, Attacks at the Data Link Layer, Master thesis, The University of California at Davis, 2003.
[17] IEEE 802.11ax, Wikipedia, 2019. [Online]. Available: https://en.wikipedia.org/wiki/IEEE 802.11ax
[18] Wi-Fi 6, tp-link, 2019. [Online]. Available: http://www.tp-link.com/us/wifi6.
[19] M. S. Y. I. Husameldin, Mitigation of DHCP starvation attack, Computers & Electrical Engineering, vol. 38, no. 5, p. 1115 - 1128, 2012.