**CHAPTER-1**

**INTRODUCTION**

Over the past decade, mobility of the world has been increased drastically, due to which our traditional methods of networking the world is proving inadequate based on the challenges that our new lifestyle has been posed. Earlier the users were connected to the network by wires or cables and the thinking that is overpowering in that people move but the networks do not. Wireless connectivity has now reincarnated the world of networking and allows the network user with a vast deal of free movement. Now the wireless technologies are overpowering the realms of wired networks. Today’s wireless networks have several advantages over wired networks in terms of mobility, flexibility and cost.

In wireless networks, data is stored centrally but the user is moving which enable users to easily access data in motion without wires. This could increase the gains in terms of output or productivity. Due to traditional wired local area networks, there is a problem of deployment of wires in an older building and it is very costly and time consuming to implement them in new building also. Wired networking has decreased the flexibility of the network. If we have to increase its range, or location then we have to face certain challenges. But wireless networking has now removed the problem of ease of deployment and flexibility. Since a wireless router has been installed anywhere in the building and there is no need of wires to do that since wireless network is available everywhere. Hotspot technology has now increased the flexibility of the network as it can be installed everywhere, including train stations, airports, hotels, libraries and even in our houses.

Earlier if a new user is being added to the network, there arises a need of running cables, installing new terminal and maintaining it in a new jack but wireless networking removes all this and now to offer services to a new user we only have to configure it to the existing infrastructure and not the whole process of installation and wiring is required. Due to an upper limit in available bandwidth, the speed of wireless network is restricted. Another challenge from which wireless networking is affected is that the radio waves suffer from propagation losses such as multipath interference, fading, reflection, refraction and ring. But the prime area of concern on any wireless network is about security. Since the wireless network transmitter is available to everyone which is in the range of a transmitter and have appropriate antenna. In a wired network, signal transmission will be through wires which can be protected by strong and full proof physical access control.

Wireless Local Area Networks (WLAN) are increasing in popularity. They are being installed by businesses of all types, educational institutions, governments, and the military. WLANs provide users a significant mobility advantage as users can access their information in many locations, some of which are more conducive to collaboration. The freedom and mobility that WLANs promise, however, also present some serious security challenges. In the military domain, the department of Défense’s (DoD) transition from industrial-age to network-centric warfare brings with it technical challenges that are highly dependent and revolve around the successful implementation of a robust and secure wireless network of systems.

These networks must address the threats described here. WLANs are not limited by network jacks nor are they limited by geography. WLANs provide unprecedented flexibility in that an area not originally intended as a collaborative workspace can accommodate a large number of wireless clients. Auditoriums now accommodate hundreds of networked computers just by plugging a few Wireless Access Points (WAPs) into the network. The radio waves used for WLAN propagate quite well. The advertised ranges for wireless network interface cards range up to 300 feet. In reality, 802.1 1 b networks can be accessed over one-half mile away in an urban environment. In this addressees known security threats to IEEE 802.1 1 networks focusing specifically on 802.1 1 a because that is the standard we implemented. However, the difference between 802.1 la and other protocols in the 802.1 1 family is trivial with respect to security. 802.1 1 ISBN 0-7803-7808-3/03/$17.00 0 2003 IEEE 76 WLANs all use the same layer 2 packets; the difference is in the physical layer. 802.1 la uses a higher frequency than 802.1 lb or one of the possible flavours of 802.1 Ig. This higher frequency means that the radio transmission will not travel as far and will not propagate through solid objects as well the low frequency standard.

This tends to help limit eavesdropping, but in no way eliminates the threat. Also 802.1 la has about 5 times the bandwidth that 802.1 Ib does. This higher bandwidth means that attacks that require data collection can be executed faster on an 802.1 la WLAN than on an 802.1 Ib WLAN. Most of the attack techniques highlighted here can be applied to other wireless network protocols, such as IEEE 802.15, a wireless personal area network specification similar to Bluetooth.

**CHAPTER-2**

**LITERATURE SURVEY**

**2.1 EXISTING SYSTEM**

In earlier security system Wireless Equivalent Privacy (WEP) was used. But, WEP got many drawbacks. WEP Plus (WEP+) provide better security by avoiding Week Initialization Vectors drawbacks. To obtain complete effectiveness of WEP+, it is necessary to use it at both ends of wireless connections, Moreover, it is vender specific. It is quite possible that strong threats like replay attacks can break it. WEP+ uses four different types of the base keys. In 64-bit encryption, only 40 bits are encrypted and the remaining 24 bits are system generated bits. This thing is big drawback for WEP+.

**2.2 PROPOSED SYSTEM**

Wi-Fi Protected Access 2 (WPA2) provides authentication, confidentiality and integrity to the wireless network. It uses Counter-Mode with Cipher Block Chaining-MAC Protocol (CCMP). For better protection against threats, it is necessary to use WPA2 for encryption and authentication.

**CHAPTER-3**

**WIRELESS NETWORK THREATS**

The wireless technology uses air as medium to communicate with each other. This medium made the wireless network susceptible to threats by attackers.There are two types of attacks in wireless security:

• Active Attacks

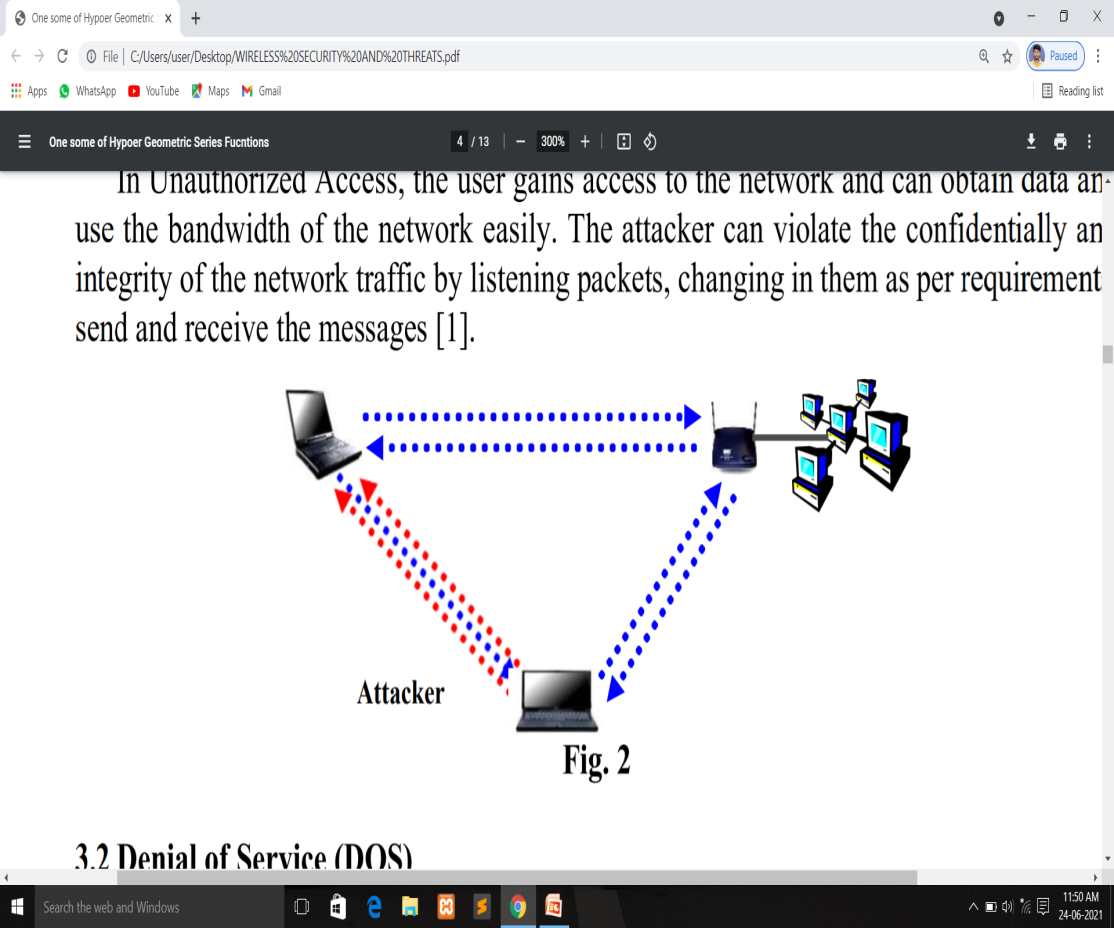
• Passive Attacks

In Active Attacks, the attackers change the contents of the information and generate

fake information in the network to destroy network security like Unauthorized Access, Active Eavesdropping, Man in the Middle Attack (MITM), Session Hijacking, Denial of Service (DoS), Replay, while in Passive Attacks, the attacker just listens to the traffic of the network, obtain information from the packets without changing it like passive Eavesdropping and Traffic Analysis. These types of attacks are very hard to detect.

**3.1 Unauthorized Access**

In Unauthorized Access, the user gains access to the network and can obtain data and use the bandwidth of the network easily. The attacker can violate the confidentially and integrity of the network traffic by listening packets, changing in them as per requirements, send and receive the messages.

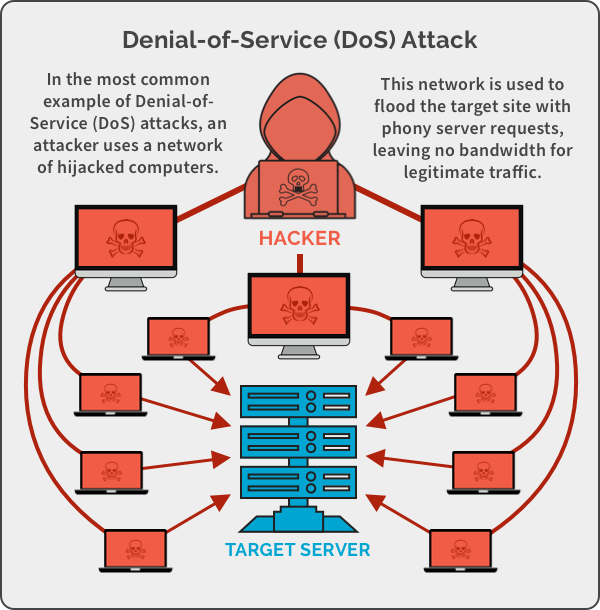


**Fig3.1: The Unauthorized attack**

**3.2 Denial of Service**

Denial of Service (DoS) is very famous attack to break down the wireless as well as

wired network. To breakdown the network, it sends huge traffic on the Access Point make it unable to respond.

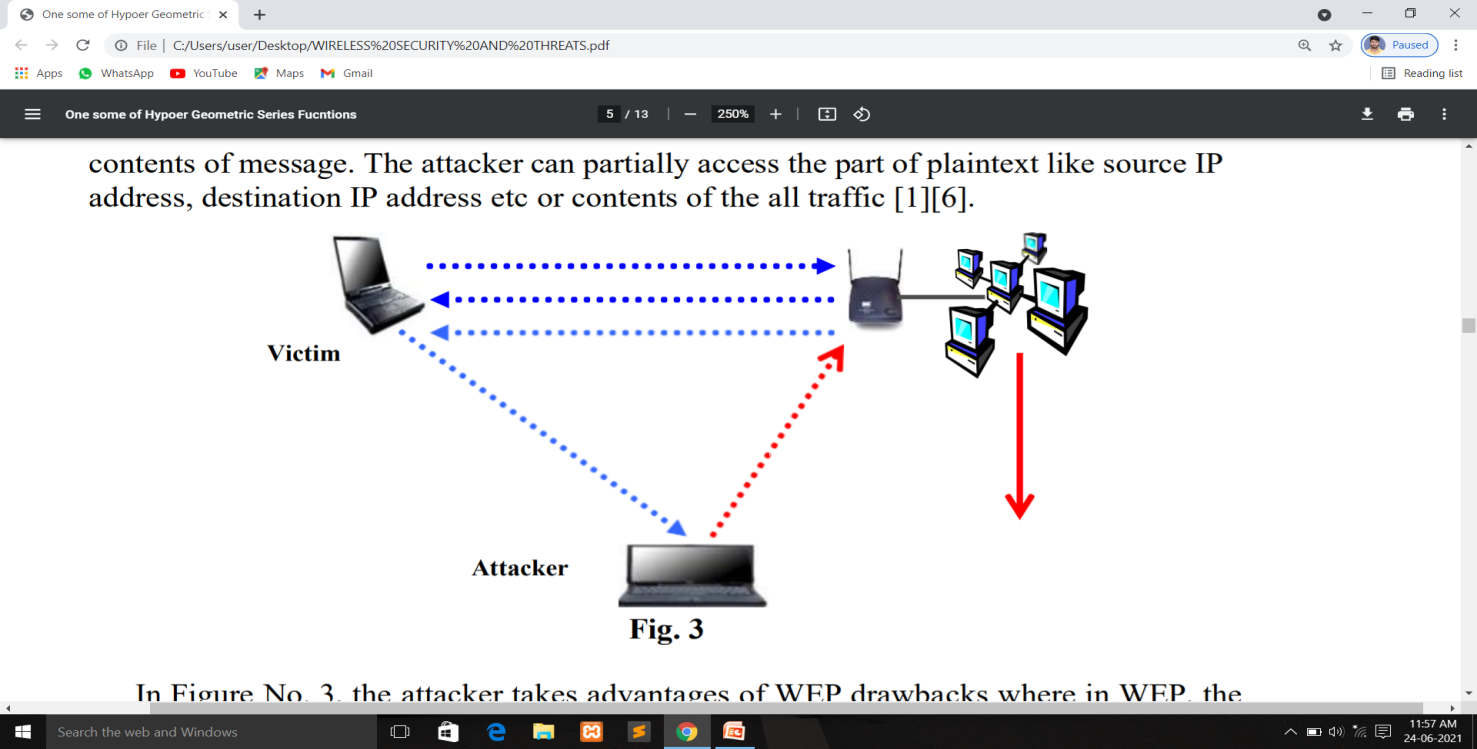


**Fig 3.2: Denial of service attack**

In Wireless network, the DoS attack is just carried out by using a powerful enough transceiver, interference in shape of noise is generated to jam to the network. Denial of Service (Dos) attack uses forged Disassociation technique to break network security. The attacker flood large number of disassociation frames to the client computer to break its connection with access point. After break-up of connection, the client computer again attempts to establish its connection with access point. It is pertinent to mention that client computer is already authenticated and only need association. To prevent reassociation, the attacker continues to send Disassociation frames up to desired period. Similarly, the attacker can use forged De-authentication technique to breakup network security. The attacker flood De-authentication frames to client computer and resulted, client computer unauthenticated with access point and will try to again authenticate itself with access point. To prevent again authentication, the attacker continues to send De-authentication frames up to desired period. Several tools are available over the internet like LAN Jack. Hunter-killer that can be used to launch DoS attack.

**3.3 Active Eavesdropping**

The core threat of the wireless network is eavesdropping in which data in shape of signals is transferred from client workstation to access point. In Active Eavesdropping, the attacker injects its data into the network signals to crack the secret key as shown in Figure No.3. The goal of this attack is to determine the contents of message. The attacker can partially access the part of plaintext like source IP address, destination IP address etc or contents of the all traffic.

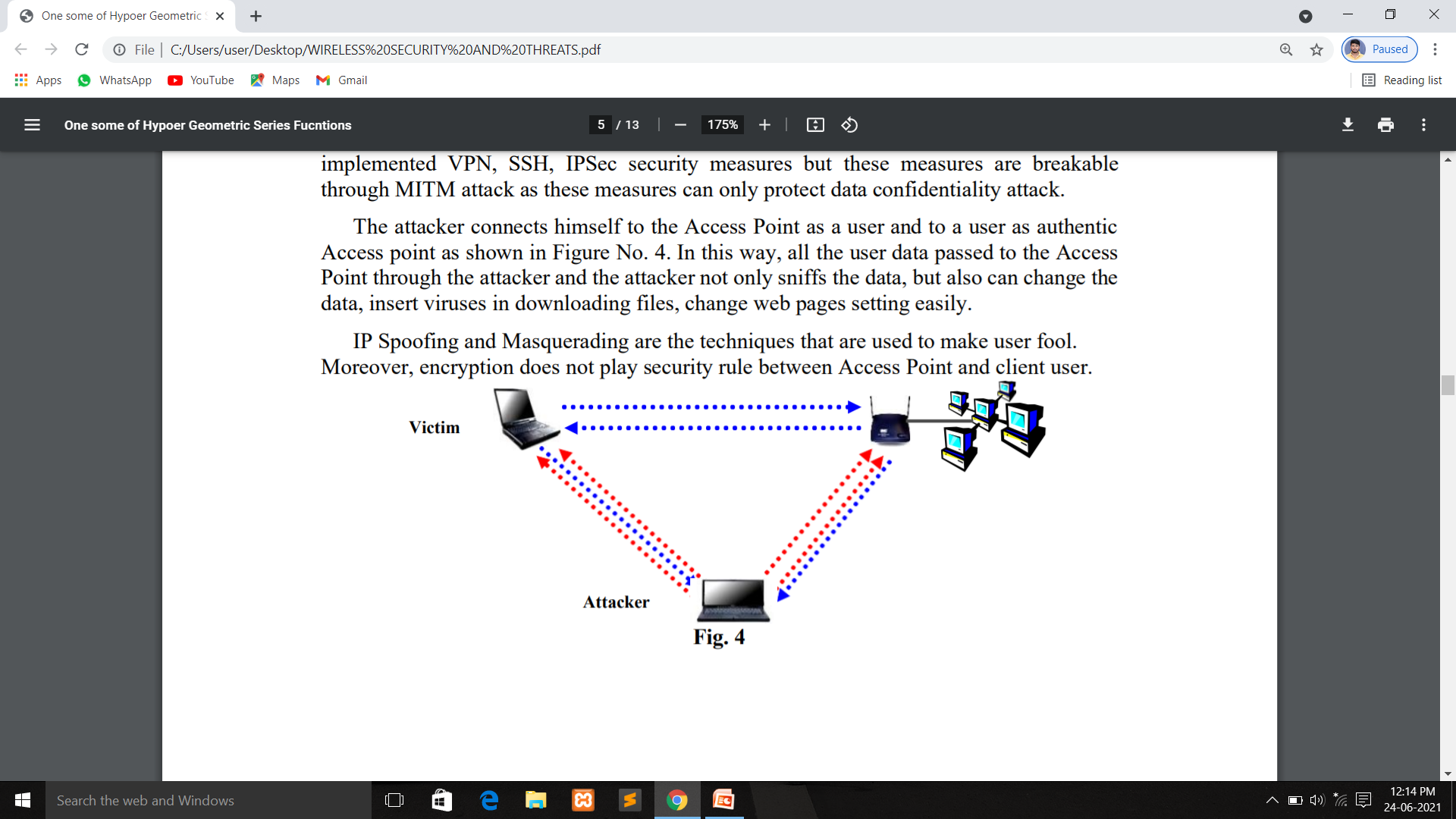


**Fig3.3: The Active Eavesdropping.**

**3.4 Man in the Middle Attack**

The Man in the Middle is very dangerous attack wherein the attacker eavesdropping

the communication and modifies it before sending [6]. Although, organization implemented VPN, SSH, IPSec security measures but these measures are breakable through MITM attack as these measures can only protect data confidentiality attack. The attacker connects himself to the Access Point as a user and to a user as authentic Access point as shown in Figure No. 4. In this way, all the user data passed to the Access Point through the attacker and the attacker not only sniffs the data, but also can change the data, insert viruses in downloading files, change web pages setting easily. IP Spoofing and Masquerading are the techniques that are used to make user fool. Moreover, encryption does not play security rule between Access Point and client user.



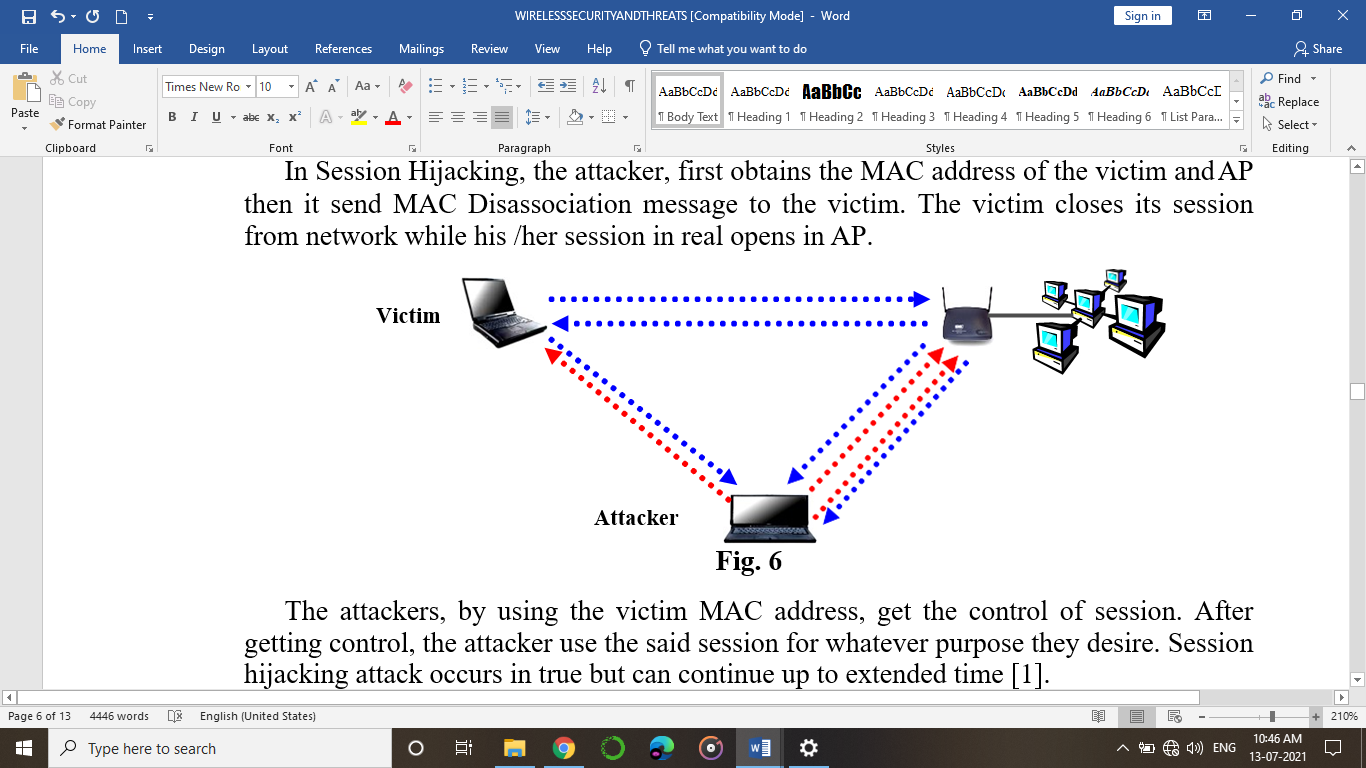
**Fig3.4: The Man in the Middle Attack.**

Address Resolution Protocol (ARP) poison is technique that is used in Man in the Middle Attack. ARP enables the user to find users MAC address. When network receives a packet, whose destination IP address is missing or unknown, it caches the packet by sending this packet on network and ask to every client about it, if any machine match with it, then machine reply with ARP Reply packet and in this packet MAC address is available. Once the cache has been updated, the attacker can act as MITM.

**3.5 Session Hijacking**

Session Hijacking indirectly resembles to the Man in the Middle Attack (MITM)

wherein the attacker captures the session of the victim client [8] [11]. The victim just supposes that his/her session was expired due to whatever reasons while his/her session was handed over to attacker and he/she can exploit it as per his desire. In Session Hijacking, the attacker, first obtains the MAC address of the victim and AP then it sends MAC Disassociation message to the victim. The victim closes its session from network while his /her session in real opens in AP.



**Fig 3.5: Session Hijacking attack**

The attackers, by using the victim MAC address, get the control of session. After

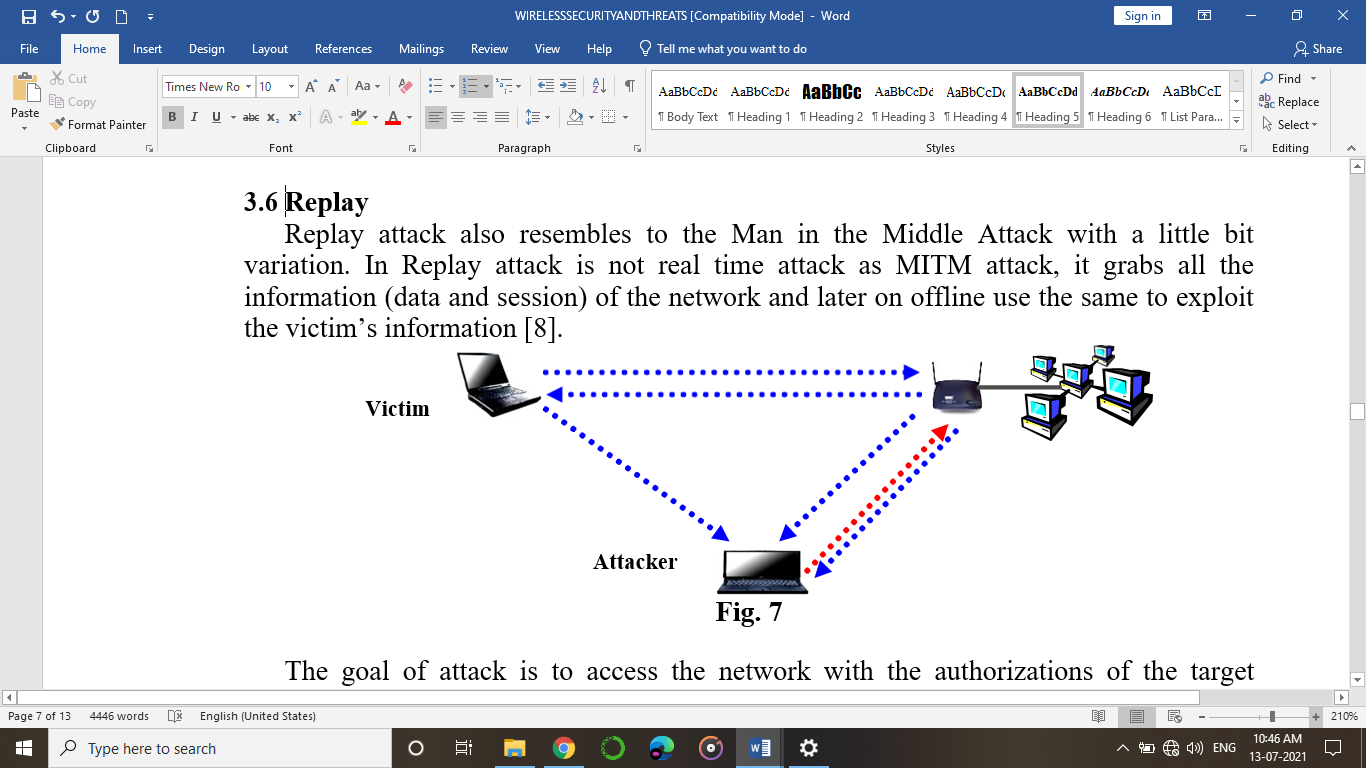
getting control, the attacker uses the said session for whatever purpose they desire. Session

hijacking attack occurs in true but can continue up to extended time.

**3.6 Replay**

Replay attack also resembles to the Man in the Middle Attack with a little bit variation. In Replay attack is not real time attack as MITM attack, it grabs all the information (data and session) of the network and later on offline use the same to exploit the victim’s

Information.



**Fig 3.6: replay attack**

The goal of attack is to access the network with the authorizations of the target without

secret key. Moreover, the attacker may use resources of the network by using target client authorization and permission. This attack is real and often used to exploit the security of the wireless network.

**3.7 Traffic Analysis**

The Traffic Analysis is very simple and easy technique in which the attacker just notes

the number and size of the packets transmitted over the air, protocols used by the network

and active access point.

If packets are encrypted, then the attacker can get partial or full information from packet of the message. The attacker, before starting an active attack should get preliminary

information about the network properties.

Wardriving is freeware tool that is available over the internet is very useful tool for

traffic analysis. To find out target Access Point, the attacker moves from one place to

another to find out active access points of the network. Every Access Point (AP)

broadcast its Service Set Identifier (SSID) over the air to recognize itself to the wireless

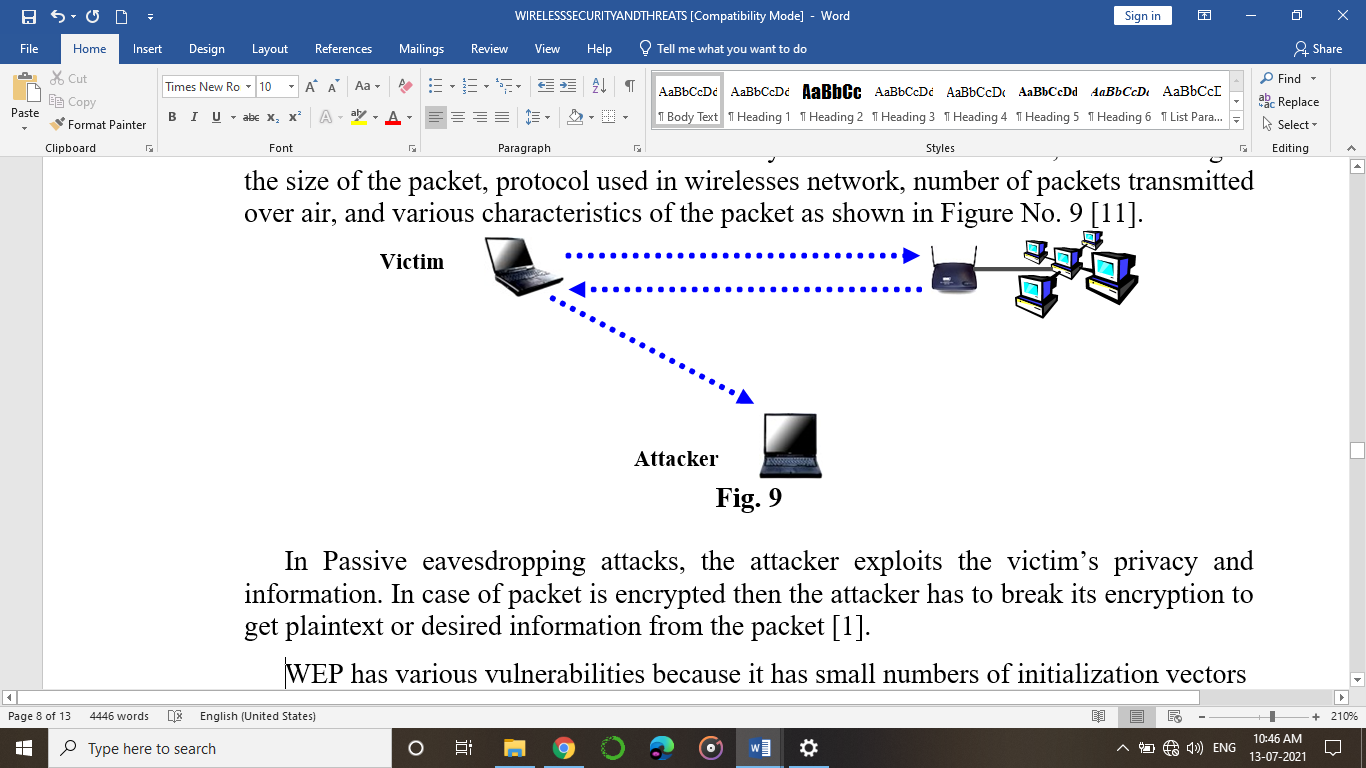
notes desired to connect to network. Through this broadcasting information, access points

allow everyone in its domain to identify them.

**3.8 Passive Eavesdropping**

This attack much resembles to traffic analysis attack. In this attack, the attacker gets

the size of the packet, protocol used in wirelesses network, number of packets transmitted

over air, and various characteristics of the packet.

**Fig 3.8: Passive eavesdropping**

In Passive eavesdropping attacks, the attacker exploits the victim’s privacy and

information. In case of packet is encrypted then the attacker has to break its encryption to

get plaintext or desired information from the packet.

WEP has various vulnerabilities because it has small numbers of initialization vectors

(IV) sequences and this thing made it susceptible to attack. Rapidly reusing the same IV

and made stream less vulnerable but can be cracked.

WPA2 use AES and 3DES strong encryption algorithms to ciphertext and in presence

of these algorithms, passive eavesdropping is very hard. It can only be possible, if the

packets are not encrypted.

**CHAPTER- 4**

**COUNTERMEASURES**

Although, there are various flaws in WEP algorithm but still it is possible for users to secure their respective wireless networks. To deal with above mentioned security threats, the following techniques are recommended to minimize the security risks involved in wireless network.

**4.1 Training and Educating Users**

The first step in wireless network security is to educate the users about how to secure network. It is often observed that end users do not know how to implement security and leaves various loopholes for attackers. If users will well aware about wireless tools configurations/settings and how to secure their respective network, then it is quite possible to reduce security risks.

**4.2 Wireless Network Auditing**

It is powerful technique to secure wireless network. The user should scan his/her

network through network scanner to know about the activities of network [6]. Several free

network scanning software’s like Net-stumbler and Kismet are available over the internet.

**4.3 Turn Off AP When You Would Not Use It**

If the user turns off his/her wireless network router/access point, when he/she is not

using it then we can limit the time that it is susceptible to hack [6].

**4.4 Change Router’s Pre-Set Password**

Every manufacture of the wireless router/access point set default user name and

password. If the user does not change it, then it is very sweet cake for the attacker as the

attacker simply scans access point and accesses it through its default username and

password. Therefore, it is strongly recommended that in first instance, the user should to change

by default, username and password.

**4.5 Change SSID**

Every access point has by default ID and attacker can easily find access point by

entering default ID. All the devices that connect to wireless network use same SSID. If

user does not change default SSID, then it is like to leave default password. Moreover, it

is also best practice to change SSID within 30 days or before.

**4.6 Turn Off SSID Broadcasting**

Access Point uses SSID broadcasting technique to show its presence in the environment

in which it is working. By turning off SSID broadcasting function, it is very hard for the

attacker to scan the network [6]. Therefore, it is recommended to turn off this function if

router allows this.

**4.7 Utilize Virtual Private Network**

In securing wireless network, it is very best security technique to put behind wireless

access point to Virtual Private Network (VPN). A Virtual Private Network is very good

solution to authenticate unauthorized users who try to connect themselves to the network

and encrypt their respective communication.

If an organization has more than one access points, then it is strongly recommended

that connect all of them with one common switch and connect this switch to VPN server.

**4.8 Location of Access Point**

During designing of wireless network, it is suggested to always place access point in

the middle of the network place to avoid its unnecessary signal broadcasting outside the

network place. For better security, the signal strength and power level should to set as per

boundary of the network.

**4.9 Use of Antivirus, Firewall and Anti Spyware**

To exploit the security, viruses and Malwares play their roles accordingly. For better

security, it is recommended that the client must install updated firewall, antivirus, antimalware and Anti Spyware software’s on his computers.

**4.10 Encryption**

The best way to secure wireless network from unauthorized users/attackers is to use

encryption for ciphertext. WEP algorithm has various vulnerabilities and it is not

recommended to use it for encryption purpose. IEEE 802.11i use Advance Encryption

Standard (AES) and Triple Data Encryption standard (3DES).

**REFERENCES**

1. Welch, D. and Lathrop, S. (2003). Wireless Security Threat Taxonomy. IEEE Workshop on information assurance, 76-83.

2. Arbaugh, W., Shankar, N. and Wan, Y.C.J. (2002). Your 802.11 wireless network has no cloths. Wireless Communications, IEEE, 9, 44-51.

3. Bittau, A., Handley, M. and Lackey, J. (2006). The final nail in WEP's coffin. Security and Privacy, 2006 IEEE Symposium.

4. Hassan, H.R. and Challal, Y. (2005). Enhanced WEP: An efficient solution to WEP threats, Wireless and Optical Communications Networks, 2005. WOCN 2005. Second IFIP International Conference, 594-599.

5. Fluhrer, S., Mantin, I. and Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. Lecture Notes in Computer Science, 2259/2001, 1-24.

6. Choi, M.K., Robles, R.J., Hong, C. and Kim, T. (2005). Wireless Network Security: Vulnerabilities, Threats and Countermeasures. International Journal of Multimedia and Ubiquitous Engineering, 3, 77-86.

7. Berghel, H. and Uecker, J. (2004). Wireless Infidelity II: Airjacking. Communications of the ACM, 47,15-20

8. Malekzadeh, M., Azim, A., Ghani, A., and Subramaniam, S. (2010). Design of Cyberwar Laboratory Exercises to Implement Common Security Attacks against IEEE 802.11 Wireless Networks. Journal of Computer Systems, Networks, and Communications, 2010.

9. He, C. and Mitchell, J.C. (2005). Security Analysis and Improvements for IEEE 802.11i. The 12th Annual Network and Distributed System Security Symposium (NDSS'05), 90-110.

10. Khakurel, S., Tiwary, P.K., Maskey, N., Sachdeva, G. (2010). Security vulnerabilities in IEEE 802.11 and adaptive encryption for better performance. Industrial Electronics & Applications (ISIEA), 2010 IEEE Symposium, 207-210.

11. Yuan, X., Archer, R.L., Xu, J. and Yu, H. (2008). A Visualization Tool for Wireless Network Attacks. Journal of Education, Informatics and Cybernetics, 1.

12. Beaton, A.E. and Tukey, J.W. (1974). The fitting of power series, meaning polynomials, illustrated on band-spectroscopic data. Technometrics, 16, 147-186.