Review Paper On Security issues in Wireless LAN

Varsha Rani
School of Engineering & Sciences, B.P.S.M.V, Khanpur Kalan, Sonipat-131305
Email: varsha.ghanghas07@gmail.com

ABSTRACT

Wireless LAN is the most commonly used everywhere nowadays. Wireless LAN is commonly used only because it is easy to use and maintain. We can access it easily ad work effectively with it. But because of higher availability of wireless LAN means its increased attacks, errors and challenges for any organization. In this paper we will discuss about various security issues and threats. In order to study about various security threats this paper will examine about the various attacks such as DOS attack, session hijacking, man-in-middle etc. attacks. This will also explain various securities like confidentiality, availability and access controls. This will help to humans to understand that how actually it is.

KEYWORDS: LAN, Wireless LAN, Attacks, Security threats, Standards.

1. Introduction:

LAN as the name specifies the Local Area Network, means it is a network which works in a limited area or a place. LAN works only within limited area such as a building, companies, colleges, enterprises etc. which comes under only limited space. The users connected through a network in a LAN. Every individual user uses configuration to access the network. LAN mainly consists of a central point which is called as an Access Point. It is analogy to a hub or a switch in traditional star topology based wired local area networks[4].

A NIC normally connects a wireless station to the AP in the Wireless LAN [5]. This Access Point works as a Hub which provides the connections. LAN commonly works as like Star topology in which only one system contains the whole connection while other nodes only share that connection to access the internet. This network is also works as like as the client server architecture or model in which the server contains the whole connection and it provides the connection to the client nodes while they are requesting for the connection. All 802.11 stations operate in two ways, either in ad-hoc mode, where stations are connected to each other, or in infrastructure mode, where stations are communicating with each other via the access points to reach some other network [6]. The above given Fig. shows the wireless LAN in which the

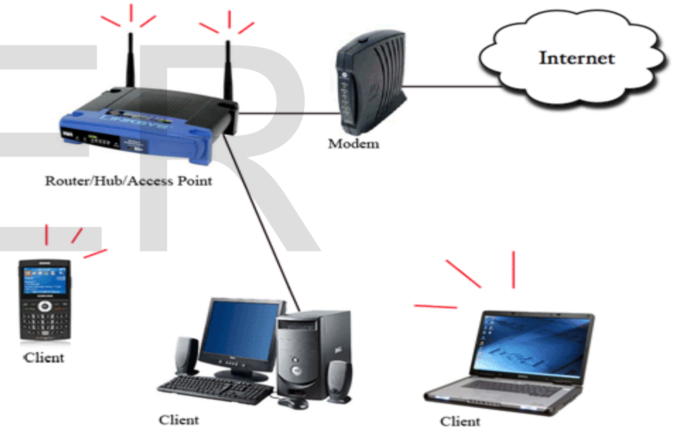


Figure 1. Wireless LAN

client nodes are accessing the connection through the Access Point or Hub.

Wireless LAN means connecting the two or more nodes through a wireless connection method in which each nodes connected through without any connection or wireless). This is all about the wireless local area network.

2. ATTACKs on Wireless LAN:

2.1 Man-in-middle attack: Man-in-middle attack is the most popular attack in the world of wired as well as wireless communication. Man-in-middle attack as its name says there is a third party or third person which sits between the two parties which are communicating with one another and interpret/hacks their personal conversation without the knowledge of the legal parties.

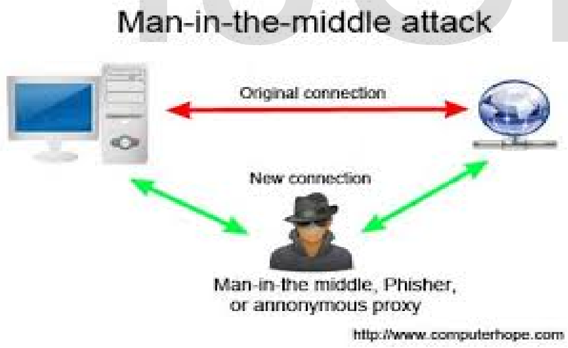

Man-in-the-middle attack
Original connection
New connection
Man-in-the middle, Phisher, or annonymous proxy
http://www.computerhope.com

Figure 2(a). Man-in-middle attack.

That third person will access the private information of the two parties and modify their conversation without the knowledge of legal parties. The man-in-middle accesses the correct information and than save that information in their own database and provides/forwards the interpreted information to the next legal member of the conversation. The legal parties think that they are communicating in a secure manner but there is the insecure conversation is done between both of them. The whole process is done without knowing them as shows in Fig. given below:

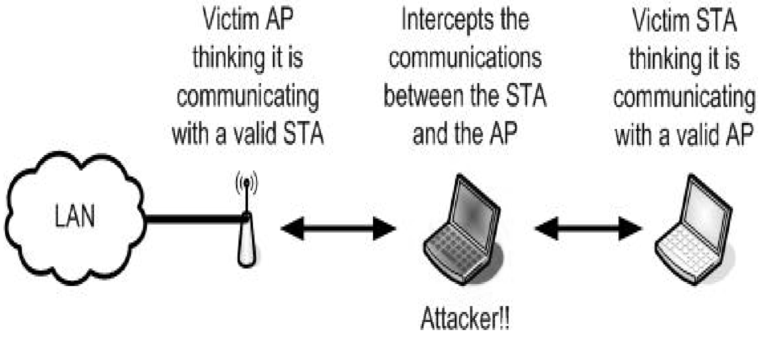

Victim AP thinking it is communicating with a valid STA
Intercepts the communications between the STA and the AP
Victim STA thinking it is communicating with a valid AP
LAN
Attacker!!

Figure 3(b). Man-in-middle attack.

2.2 DOS attack: Denial of Service attacks or DOS is a serious threat on both wired and wireless networks. This attack aims to disable the availability of the network and the services it provides [1]. In Wireless LANs, DOS is conducted in several ways like interfering the frequency spectrum by external RF sources hence denying access to the WLAN or, in best cases, granting access with lower data rates [2]. In DOS attack the main focus of this attack is disable or discarding the originality of the data or network so that the services can not be accessed by any node in the given network. Its main aim to loose the connectivity of the connections between various nodes.

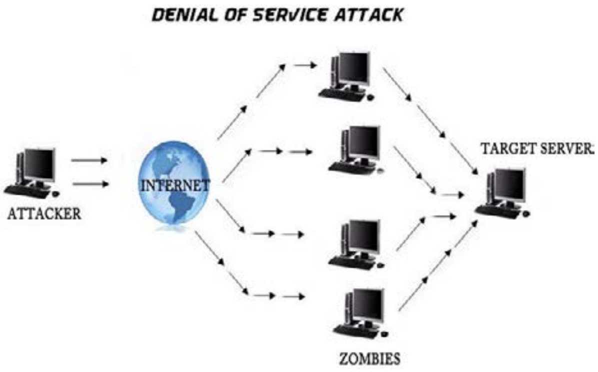


Figure 4. DOS attack.

2.3 Hijacking the session attack: This is also named as session hijacking attack in which when any unauthorized user access the information as well as the whole access to the network then that unauthorized user not only access the private information about the network while it also changes the network connection as well as the configuration of the network is called that the session is hijacked.

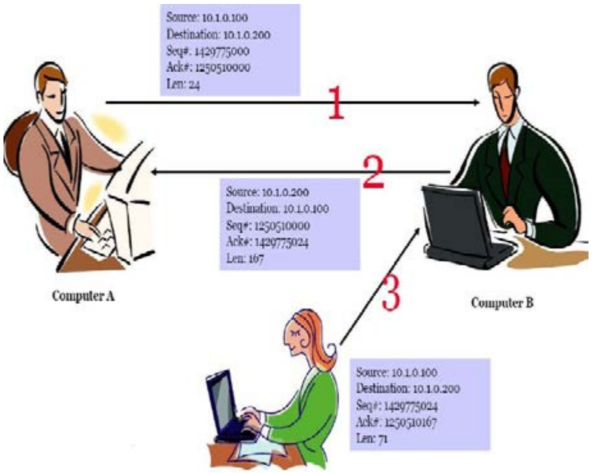
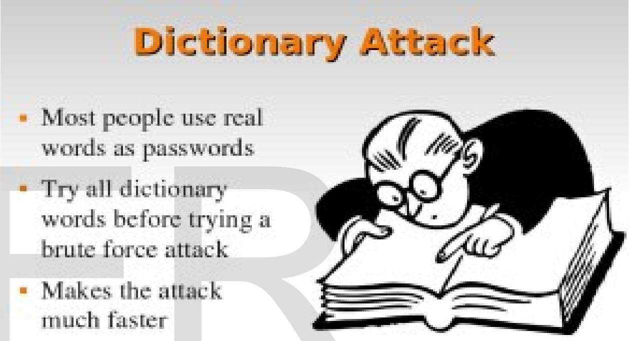


Figure 5. Way to Hijacking the Session.

2.4 Type of Dictionary attack: This attack focuses on the username and passwords. In this type of dictionary attack the hacker try to access the username and on the basis of username it try to access the password and it makes a number of word combinations using the dictionary. It tries until it accesses the password of the network. Dictionary attacks will be unsuccessful if the password is not in the dictionary [11]. The main aim of this attack is to make the unwanted changes into the network to slow down the network or any other.



Dictionary Attack

- Most people use real words as passwords
- Try all dictionary words before trying a brute force attack
- Makes the attack much faster

Figure 6. Dictionary attack basics.

2.5 Eavesdropping Attack: Eavesdropping is mainly focus on attack against the confidentiality of data usage over the network. When this attack is applied on the network then the wireless LAN radiates the network signals/traffics on to the space. This makes the sense impossible to get that who is controlling the network that who is accessing the data over the network or who is not. It is so complicated to identify that which party receives the signals while we are installing any Wireless LAN. The main risk is that 802.11 do not provide a way to secure data in transit against eavesdropping [12]. Hence, eavesdropping by the third parties enables the attacker to intercept the transmission over the air from a distance [3]. This is an attack that cannot be easily prevented using adequate physical security measures[8]. Besides, this attack can be done far away from the premises of any organizations [9][10].

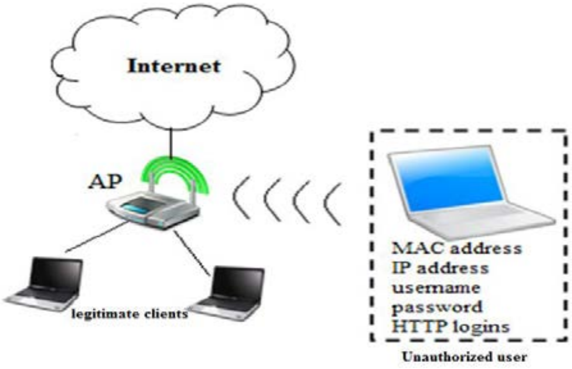
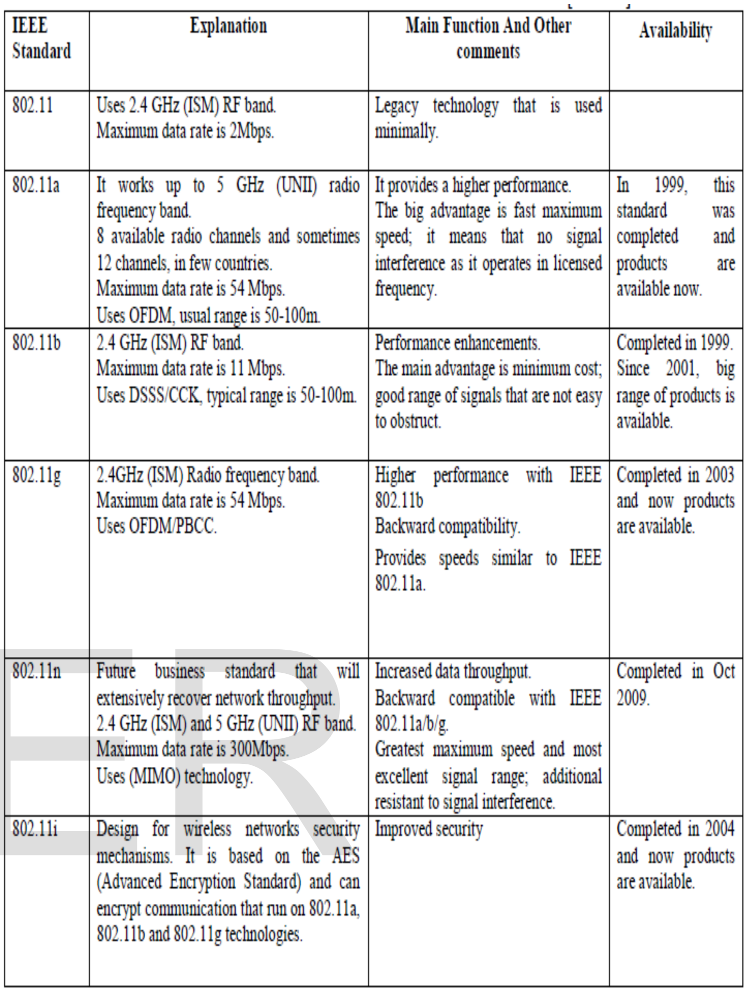


Figure 7. WLAN Eavesdropping.

Examples of passive attacks are Eavesdropping, Man-in-the-Middle attack, Traffic Analysis etc. Active attack categories are WEP Key Cracking, Evil Twin AP and AP Phishing etc. [7].

3. **Wireless LAN standards of IEEE 802.11:** Various WLAN standards(802.11) are given as shown in Fig-



IEEE Standard	Explanation	Main Function And Other comments	Availability
802.11	Uses 2.4 GHz (ISM) RF band. Maximum data rate is 2Mbps.	Legacy technology that is used minimally.	
802.11a	It works up to 5 GHz (UNII) radio frequency band. 8 available radio channels and sometimes 12 channels, in few countries. Maximum data rate is 54 Mbps. Uses OFDM, usual range is 50-100m.	It provides a higher performance. The big advantage is fast maximum speed; it means that no signal interference as it operates in licensed frequency.	In 1999, this standard was completed and products are available now.
802.11b	2.4 GHz (ISM) RF band. Maximum data rate is 11 Mbps. Uses DSSS/CCK, typical range is 50-100m.	Performance enhancements. The main advantage is minimum cost; good range of signals that are not easy to obstruct.	Completed in 1999. Since 2001, big range of products is available.
802.11g	2.4GHz (ISM) Radio frequency band. Maximum data rate is 54 Mbps. Uses OFDM/PBCC.	Higher performance with IEEE 802.11b Backward compatibility. Provides speeds similar to IEEE 802.11a.	Completed in 2003 and now products are available.
802.11n	Future business standard that will extensively recover network throughput. 2.4 GHz (ISM) and 5 GHz (UNII) RF band. Maximum data rate is 300Mbps. Uses (MIMO) technology.	Increased data throughput. Backward compatible with IEEE 802.11a/b/g. Greatest maximum speed and most excellent signal range; additional resistant to signal interference.	Completed in Oct 2009.
802.11i	Design for wireless networks security mechanisms. It is based on the AES (Advanced Encryption Standard) and can encrypt communication that run on 802.11a, 802.11b and 802.11g technologies.	Improved security	Completed in 2004 and now products are available.

Figure 8. WLAN Standards of IEEE 802.11

4. **WIRELESS security requirements :**

1. Access control
2. Authentication
3. Availability
4. Confidentiality
5. Integrity

We can also secure our connection or network by checking that no unauthorized user can access out wireless network. If we provides the authenticity to our network then there are less chances to lost network connection while transmission over the network.

5. Conclusion: In this paper here we included what are the various security issues which occur in Wireless LAN and affects the security threats. Here are some standards which are useful for it and preventing the security threats occurred in WLAN. There are various security requirements which also prevent the security threats in WLAN. Wireless LAN is most widely used network nowadays. So it should be secure so that users can communicate over this network easily and securely.

REFERENCE:

[1]. William Stallings, "*Cryptography and Network Security Principles and Practices*", 3rd Edition, Prentice Hall 2003.

[2]. Wang Shunman, TaoRan, WmgYue and ZhangJi, *"Wireless LAN and its security problem".* Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT'2003.

[3]. R.A. Hamid, "*Wireless LAN: Security Issues and Solutions*", [Press release], 2003.

[4]. Gurjeet Singh "*Performance and Effectiveness of Secure Routing Protocols in MANET*" Global Journal of Computer Science & Technology, Vol 12, Issue 5, 2012.

[5]. P. Feng, *"Wireless LAN Security Issues and Solutions"*, IEEE Symposium on Robotics and Applications, Kuala Lumpur, Malaysia, pp. 921-924, 3-5 June, 2012.

[6]. L. Phifer, *"Wireless Lunchtime Learning Security School"*, http://searchsecurity.techtarget.com/guides/Wireless-Security-School, [Accessed on: 14/11/12] 2009.

[7]. "*Search Security, Information security tutorials*" [Online], Available at: http://searchsecurity.techtarget.com/tutorial/Information-security-tutorials, [Accessed on: 14/11/12] 2011.

[8]. Md. Waliullah, Diane Gan, *"Wireless LAN Security Threats & Vulnerabilities:
A Literature Review"*, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014

[9]. D. Welch, S. Lathrop, *"Wireless Security Threat Taxonomy"*, Proceeding of the Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, U.S Military Academy, West Point, NY, 18-20 June, 2003, pp. 76-83

[10]. N. Sunday, *"Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures"*, Thesis (MSc), Blekinge Institute of Technology, 2008.

[11]. YouTube, "*Dictionary vs. Brute force Attacks – Explained*", Available at: http://www.youtube.com/watch?v=2hveQ8QZ9MQ, [Accessed on: 14/11/12] 2008.

[12]. BORISOV, N., GOLDBERG, I., AND WAGNER, D., "*Intercepting mobile communications: The insecurity of 802.11*", MOBICOM 2001.