Research Challenges & Security Concerns Of Wireless Networks: A Review

Priya[1], Kamalpreet[2], Sonika[3]
[1, 2, 3] ECE, DKTGI Rahon (Pb)

Abstract- *Wireless networking technology is quickly changing the way of communication of networked computers. The advent of wireless technology has lessen the human efforts for accessing data at various locations by replacing wired infrastructure with wireless infrastructure. It also provides access to devices having mobility. Since wireless devices need to be small and bandwidth restricted, some of the key challenges in wireless networks are Signal fading, data rate enhancements, mobility, minimizing size and cost, user security and (Quality of service) QoS. Wireless security is the prevention of unauthorized access or damage to computers using wireless network. The security measures we believed in the past to secure our networks are now obsolete with this new technology. This paper introduces the research challenges and security issues in wireless networks.*

Keywords- Department of Defence (DoD), Denial of Service (DoS), Extensible Authentication Protocol (EAP), Payment Card Industry (PCI).

I. INTRODUCTION

"Wireless" as the name implies is the network which is not connected by wires. During the past decades, wireless communications infrastructure and services have been proliferating with the goal of meeting rapidly increasing demands [1]-[3]. Use of wireless networks avoid the costly process of introducing wires or cables for connecting different devices at different locations and into buildings. Wireless network is based on radio waves. Wireless networks use radio waves to connect device such as laptops to the internet. When laptops connected to the Wi-Fi hotspots in public places the connection established is wireless network [4]. As this network is wireless and use radio waves thus many security issues and challenges arises in this network. It has been reported in [5] that an increasing number of wireless devices are abused for illicit cyber-criminal activities, including malicious attacks ,computer hacking, radio jamming, DoS and so on. Some of those are discussed in this paper.

II. TYPES OF WIRELESS NETWORKS [4]

- **Wireless Local Area Network (LAN):-** Links two or more devices using a wireless distribution method, providing a connection through access points to the wider Internet.
- **Wireless Metropolitan Area Networks (MAN):-** Connects several wireless LANs.

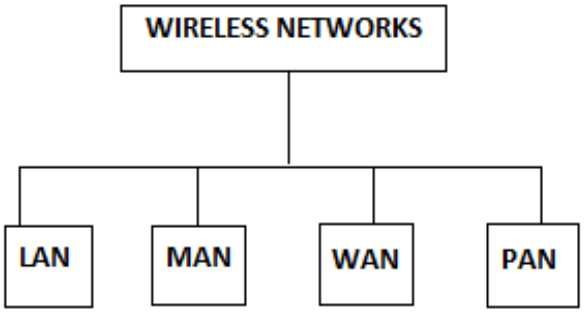

Fig 1: Types of Wireless Networks

- **Wireless Wide Area Network (WAN):-** Covers large areas such as neighboring towns and cities.
- **Wireless Personal Area Network (PAN):-** Interconnects devices in a short span, generally within a person's reach.

III. RESEARCH CHALLENGES IN WIRELESS NETWORKS

3.1 Signal Fading:- In wireless communications ,the variation of the attenuation of a signal due to various variables (including time, geographical position and radio frequency) is called fading. Fading is sometimes referred to as a random process. Communication channel that experiences fading is called fading channel. Fading may also due to multipath propagation (multipath induced fading), weather (particularly rain), or shadowing from obstacles affecting the wave propagation (shadow fading). Unlike wired media, signals transmitted over a wireless medium may change their medium due to reflection, diffraction, and scattering caused by obstacles. Before arriving at the receiver it may be distorted or weakened because they are propagated over an open, unprotected medium.

3.2 Mobility : Without the limitations introduced by the wired connections among devices, all devices in a wireless network are free to move. For supporting mobility, an ongoing connection should be kept alive as a user roams around. In an infrastructure network, a handoff occurs when a mobile host moves from the coverage of a base station or access point to that of another one [6].However, mobility places a few requirements on the network:

- They must have the ability to locate subscribers.
- They must monitor the movement of the subscribers.
- They must enable handoffs seamlessly as the user moves across cells while sessions are kept alive [7].

3.3 Power and Energy : Power is the basic problem in wireless networks. As mobile device is generally small in size, handy and committed to perform a certain set of functions so its power source may not be able to deliver as much power as the one installed in a fixed device [6]. Wireless devices are allowed to move freely thus it would generally be hard to receive a continuous power supply.

3.4 Data Rate: The data rate is a term to denote the transmission speed, or the number of bits per second transferred. The useful data rate for the user is usually less than the actual data rate transported on the network. One reason for this is that additional bits are transferred for signaling the address, the recovery of timing information at the receiver or error correction to compensate for possible transmission errors [8]. It is essential to improve the current data rates to support future high speed applications especially, if multimedia services are to be provided. Data rate is a function of various factors such as the data compression algorithm, interference mitigation through error-resilient coding, power control.

IV. SECURITY ISSUES OF WIRELESS NETWORKS

Security is a big concern in wireless networking, especially in m-commerce and e-commerce applications. Mobility of users increases the security concerns in a wireless network. Current wireless networks use authentication and data encryption techniques on the air interface to provide security to its users [9]. Network security issues, whether wired or wireless, fall into three main categories [10]: availability, confidentiality and integrity.

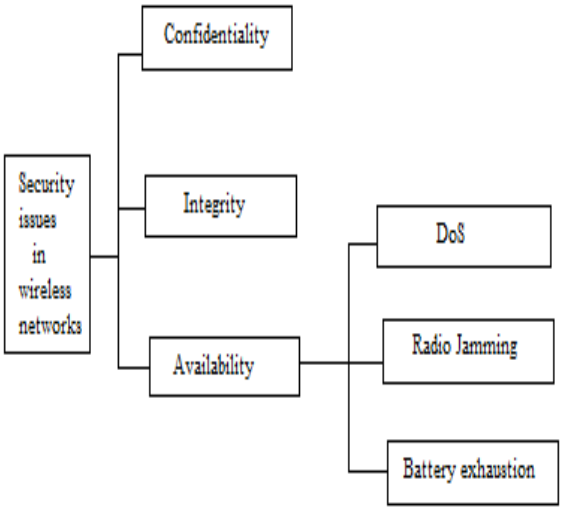

Fig 2: Security Issues in Wireless Networks

- **Confidentiality:** is the information being sent across the network transmitted in such a way that only the intended recipient(s) can read it.
- **Integrity:** is the information reaching the recipient intact, not intercepted and changed.
- **Availability:** is the network available to users whenever it is supposed to be. No jamming, adaptability to abrupt topologies [15].

4.1 Confidentiality

The confidentiality refers to limiting the data access to intended users only, while preventing the disclosure of the information to unauthorized entities [17].Considering the symmetric key encryption technique. Encryption is the method to make sure the data is not revealed to unauthorized user, wireless networks are able to do the same. Encryption is nothing without authentication. An unauthenticated user could authenticate and then be given the key used to decrypt the data. The standard method for authorization is to have some form of centralised system which is used to store access control list and this method is used in networks which have a static set of users. So this method is suitable for WI-FI but in other networks which are more ad-hoc in nature such as blue tooth networks. It becomes unsuitable. To tackle such types of problems of the system, a better solution is a form of secure transient association between the devices. In this approach the decision on how to behave or who to trust is made by one master device. Which commands the slave devices or either by each device [15].

4.2 Integrity

The integrity of information transmitted in a wireless network means the information should be accurate and reliable during its entire life-cycle. Which means it could represent the source-information without any falsification and modification by unauthorized users. The data integrity may be violated by so called insider attacks, for example node compromise attacks [18]-[20].In wireless network information sent through the air, thus it can be easily interrupted and altered by harmful user. The integrity of data in wireless networks is broken or damaged. The existing methods used by wired networks are perfectly adequate for protecting the integrity of data [16].

4.3 Availability

The availability implies that the authorized users are indeed capable of accessing a wireless network anytime and anywhere upon request. The violation of availability, referred to as denial of service, will result in the authorized users to become unable to access the wireless network, which in turn results in unsatisfactory user experience [21], [22].

There are many ways in which one can restrict the availability of the network. Some of these are:-

- DoS (Denial of Service)
- Radio Jamming
- Battery exhaustion

4.3.1 DoS : Wireless networks are particularly susceptible to DoS attacks. DoS is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack , the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy. Wired networks require the attacker to be physically connected to the network in some way before they can launch such an attack but in wireless networks an attacker only has to be within a certain range of the network (usually 100m) to be able to launch such an attack. These kind of attacks are very difficult to stop since network providers want to allow legal users to begin communications with the network, and cannot stop evil users from exploiting this to cause a DoS attack . These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP) [12].

4.3.2 Radio Jamming: Another way in which the evil users can potentially restrict the availability of the wireless networks is through radio jamming. This involves sending out a lot of noise on the same frequency as the network uses. However, there are techniques, such as frequency hopping which can make this kind of attack more difficult. Also, this threat is less relevant in the non-military world since the 'jammer' could be reported to the police and arrested.

4.3.3 Battery exhaustion: One kind of attack on the availability of wireless networks which has arisen in the last few years is battery exhaustion attacks. Because many wireless network devices are portable and therefore battery powered, evil users can repeatedly send messages to the device. This prevents it from going into its sleep mode, and the battery runs down much faster [10].

V. THREATS TO WIRELESS SECURITY

5.1 Misconfigured access points: The misconfigured access points are a type of security surface, that are the easiest to break, if its detected. The place, where you will most likely meet misconfigured access points are home wireless network or very small businesses. Large wireless environments are mostly use centralized management platforms that control hundreds or thousands of access points and keep them synchronized, therefore it is less chance of any configuration error there[13].

5.2 Unmanaged use of wireless outside the enterprise : With every major advance in networking technology comes new ways to exploit it. The risks of mobile computing flow in both directions, into and out of an enterprise. People are carrying enterprise information outside, on mobile devices. Policies are needed on laptops and very soon on smart phones also. In the other direction, mobile devices can become infected with malicious software while outside the network area. The harmful devices eventually get inside the enterprise network and infact its network. Agencies need access policies to prevent the network from these harmful devices.

5.3 Hackers: As Wireless networks are very common so it is also very common to find wireless networks that are unsecured .May be the users are lazy or may be they don't have proper knowledge when it comes wireless networks. Whatever the reason, hacker easily break the wireless security, and also use wireless technology to crack into non-wireless network . Active attacks on wireless links are a growing problem as mobile and wireless computing offers increasingly attractive targets to hackers. After a device becomes powerful enough and the information they contain becomes valuable enough, they attract the attention of bad guys and become

victim to exploit. A good defense against hackers is educational and technical. Many organizations are realizing they need to have a 24/7 monitoring system for wireless. As adoption increases, various sensitive markets, such as the DoD and PCI, are becoming more authoritarian in their security, with requirements for best practices to acquire and manage the technology [14].

VI. CONCLUSION

This paper discusses about wireless networks, research challenges in wireless networks, their security issues and threats in wireless networks. As wireless networks are rapidly becoming popular and thus demand for various useful wireless applications is also increasing. So this increase in popularity and demand also increases the network's security issues. This paper covers all those issues at one place which is beneficial for those who wants to go with research on finding solutions on wireless issues.

REFERENCES

[1] Yulong Zou, Senior member, IEEE, Jia Zhu, Xiabin Wang, Senior member, IEEE and Lajos Hanzo, Fellow, IEEE "A Survey on Wireless Network Security:Technical Challenges, Recent Advances and Future Treands",pp. 1-36

[2] http O. Aliu, A. Imran, M. Imran, and B. Evans, "A survey of self organisation in future cellular networks," IEEE Communications Surveys &Tutorials, vol. 15, no. 1, pp. 336-361, February 2013.

[3] H. ElSawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A Survey," IEEE Communications Surveys & Tutorials, vol.PP, no. 99, pp. 1-24, June 2013

[4] www.techopedia.com/definition/26186/wireless-network.

[5] Symantec Norton Department, "The 2012 Norton cybercrime report," September 2012, available on-line at http://www.norton.com/2012cybercrimereport.

[6] Gajender Pal, Kuldeep Kumar, Manish Kumar, "A Review paper on wireless networks" vol.1, pp. 88-90 April,2015

[7] "Getting to Know Wireless Networks and Technology", informit.com, February 2008.

[8] www.telecomabc.com/d/data-rate.html

[9] Aniruddha Singh, Abhishek Vaish, Pankaj Kumar Keserwani ,"Research issues and challenges of Wireless Networks", vol.4, pp. 572-575,2-Feb- 2014.

[10] Rupinder Singh, Dr. Jatinder Singh, Dr. Ravinder Singh, "Security Challenges In Wireless Sensor Networks ",vol.6,pp.1-6,may-june 2016.

[11] Michel Barbean and Jeyanthi Hall, ''Wireless Communications: Security issues, solutions and challenges".

[12] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim School of Multimedia, Hannam University, Daejeon, "Wireless Network security:Vulnerabilities, Threats and Countermeasures",vol.3,pp. 77-86,july 2008

[13] https://www.tutorialspoint.com/wireless_security/wireless_security_misconfigured_access_point_attack.htm

[14] William Jackson, "4 threats to wireless security" .https://gcn.com/articles/2010/04/19/mobile-computing-security.aspx

[15] Akhil Gupta and Rakesh Kumar Jha,"Security Threats Of Wireless Networks: A Survey", 2015,IEEE

[16] M. Gast, "Introduction to Wireless Networks" in 802.11 Wireless Networks: The Definitive Guide, New York:O'Reilly, pp. 01-06, 2002.

[17] W. Stalling, Cryptography and network security: Principles and Practices, Third Edition, NJ: PrenticeCHall, January 2010

[18] D. Dzung, M. Naedele, T. Von Hoff, and M. Crevatin, "Security for industrial communications systems," Proceedings of the IEEE, vol. 93, no. 6, pp. 1152-1177, June 2005.

[19] E. Shi amd A. Perrig, "Designing secure sensor networks," IEEE Wireless Communications, vol. 11, no. 6, pp. 38-43, December 2004.

[20] X. Lin, "CAT: Building couples to early detect node compromise attack in wireless sensor networks," Proceedings of The 2009 IEEE Global Telecommunications Conference, Honolulu, USA, December 2009.

[21] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54-62, October 2002.

[22] H. Huang, N. Ahmed, P. Karthik, "On a new type of denial of service attack in wireless networks: The distributed jammer network," IEEE Transactions on Wireless Communications, wvol. 10, no. 7, pp. 2316-2324, July 2011.