Analysis of the Existing and Emerging Security Issues of Wireless Communication Networks

Pradeep Kumar Shah, Assistant Professor,
College of Computing Sciences and Information Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- pradeep.rdndj@gmail.com

ABSTRACT*: *Over the past few decades, wireless mobile communications has expanded significantly. The use of wireless networks and communication in daily life has expanded, and as a result, society is now much more vulnerable to attacks and activities related to cyber security. This study gives a brief introduction of security challenges, such as attacks, loopholes, and challenges in wireless networks, to serve as a foundation for a more in-depth discussion on security techniques and attacks in this difficult environment. Based on the review, it is possible to draw the conclusion that further work in this area should focus on thoroughly examining security issues in all network systems that have been discussed and classifying them uniformly according to where they occur, the type of damage they cause, the network level at which they take place, and the extent of breach of security, etc., along with a characterization of the proposed classes.

KEYWORDS: 3G, Communication, Network, Wireless Networks, Security.

1. INTRODUCTION

Wireless communication technologies have undergone some interesting breakthroughs recently, and they will remain to be a quickly expanding industry in the foreseeable future. Third-generation (3G) wireless carriers of today allow broadband transfer with rates of up to 2Mbps in various locations around the world, improving on the backbone of existing wireless systems. Although three out of the five conflicting 3G wireless technologies defined by IMT2000, the worldwide 3G networks standard, are now in various stages of implementation, this complicates the well-known challenge of wireless network compatibility[1]–[3].

Mobile commerce is a new field that involves doing commercial operations utilising portable devices through wireless and mobile networks [4], [5]. It contains not only mobile versions of current e-commerce implementations, and also innovative and new applications that have become increasingly feasible as a result of mobile and wireless networks, such as location-based services and products which typically require users' attention, such as mobile multi-party dynamic games. The prospective effect of mobile ecommerce has caught the attention of consumers, telecommunications companies, suppliers, content creators, companies, and researchers. It brings numerous distinct aspects that distinguish it from e-commerce and wireless technology, such as geolocation and situational awareness, consumer-centric approach and customization, and transaction support. It will play a growing role as a 3rd-party supplier since cellular carriers may be unable to generate and maintain complex and inputs for a huge number of consumers. Mobile commerce has the ability to revolutionise the way enterprises are done from a variety of perspectives. Several B2B (Company to Business) m-commerce solutions can increase the effectiveness of business operations, the level of services provided to users as well as other businesses, and the creation of numerous new prospects and markets. Many European countries with significant thresholds of wireless adaptation, in which m-commerce is producing billions of dollars in revenues from mobile coupons, mobile parking, mobile advertising, mobile tickets, and online purchases, are among those where DoCoMo endorses mobile shopping payouts by scanning mobile phones as well as other hand-held gadgets.

1.1. Evolution of Wireless Networks

With much more than 1.7 billion wireless subscribers, Personal Communications System (PCS), worldwide overall number of cellular, as well as other wireless users is likely to exceed two billion by the end of 2006, if not sooner. Several distinct specifications exist around the world nowadays to satisfy existing subscribers. First and second gen (1G and 2G) networks are built solely on a single or even more variants of wireless connectivity procedures such as Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), 3G via cdma2000 or Wide-band Code Division Multiple Access (WCDMA), Frequency Division Multiple Access (FDMA). It should be emphasised that 3G specifications enable the speed and flexibility both by current providers to transition existing 1G and 2G networks to 3G services and satellites or ground providers to establish new 3G networks. The radio standards include five distinct options, each carefully intended to assist existing 1G and 2G wireless systems in interoperating with or evolving into 3G systems[6], [7]. Nevertheless, the globalisation to 3rd generation has been slower than expected due to operators' perceptions of restricted market requirements, a lack of incentives for carriers and companies, massive investment in extant first and second generation wireless communication systems, and wireless carriers' monopolistic practices in several countries.

1.2. Security Issues in Wireless Networks

1.2.1. Eavesdropping to intercept data

This involves improperly receiving and getting information sent across wireless communication networks which might also jeopardise the integrity of information or data in question. An attacker may take over the message over the air from a specific range since the airwave is not safe[8], [9].

1.2.2. Electromagnetic Interference

In broadcast, interference/interruption is particularly prevalent since a radio receiver could simultaneously take up two or even more messages. This frequently causes signal weakening and interferes with smooth broadcasts.

1.2.3. Bandwidth Congestion

Piggybacking, or gaining unauthorized access to a wireless System, results in bandwidth congestion. It entails the action of utilizing another user's personal wireless broadband service without that user's explicit knowledge or permission in order to obtain a wireless connectivity. Piggybacking can also result in direct computer attacks, service violations, and unlawful activity by unscrupulous users that may be connected to you.

1.2.4. Wireless Network Sniffing

A wireless sniffer is a software program or technology that intercepts data as it is transferred across a system and decodes it into a human-readable form. Wireless intrusion detection systems are packet analyzers that collect data transferred across wireless networks. Although wireless packet sniffers are useful for network maintenance, their characteristics also render them appealing tools for hostile operations. Such tools can be used by hackers to steal information and snoop on networks. Predators can use sniffer tools to track sensitive data such as banking data, bank accounts, passwords, credit card details, logins, and so on. Wireless sniffer vulnerabilities can be addressed by employing secure protocols such as SFTP, HTTPS, and Secure Shell (SSH). These secure methods ensure that every data sent is immediately encrypted.

1.2.5. Denial-of Service Attacks

In this case, a malevolent hacker deprives a wireless user unlawfully of the benefits of the channel's services. In order to capture the passwords with just some cracking tools as during channel's recovery, the intruder overflows the network with pointless communications to render it inaccessible. This compromises the protection and grants the attacker unauthorised access to information.

1.2.6. Wireless Spoofing attacks

Spoofing is a kind of attack in which an attacker impersonates another computer on the network using data collected by a wireless sniffer. Spoofing attacks frequently target company network and are capable of man-in-the-middle attacks against network hosts or the theft of critical data. By using firewalls with deep packet sniffing capabilities or by taking steps to confirm the sender's or user's identity, spoofing attacks can be reduced (Figure 1).

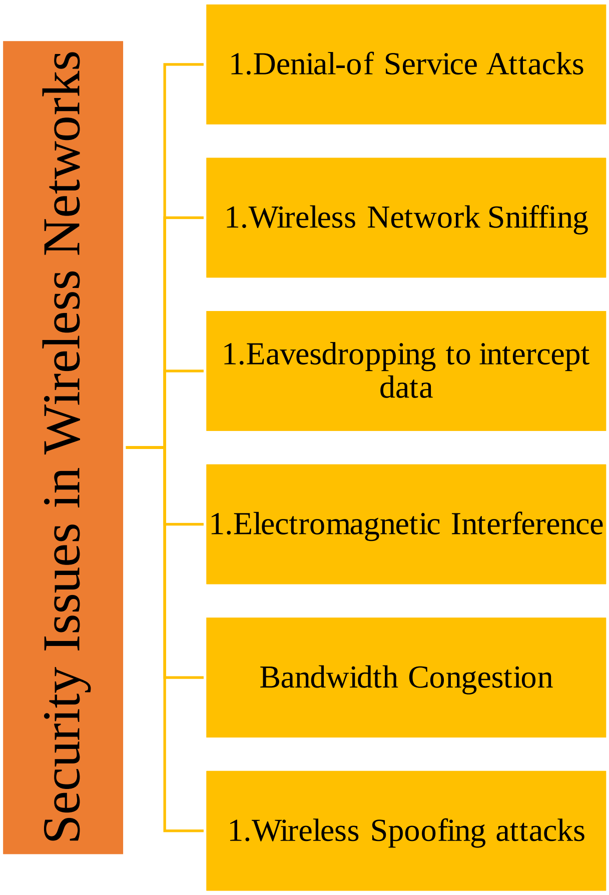
Security Issues in Wireless Networks
1.Denial-of Service Attacks
1.Wireless Network Sniffing
1.Eavesdropping to intercept data
1.Electromagnetic Interference
Bandwidth Congestion
1.Wireless Spoofing attacks

Figure 1: Illustrating the Security Issues of Wireless Networks.

2. DISCUSSION

There are some important techniques to avoid hackers.

- Use of encryption: Scrambling or encrypting network traffic is one of the greatest ways to protect wireless networks from hackers. The majority of wireless routers, access points, and base stations come with an encryption system already installed. Consider purchasing an encryption feature-equipped wireless router if your current model does not. Wireless routers are frequently shipped by manufacturers with the encryption option disabled.
- Use anti-spyware, anti-virus, and firewalls: Devices linked to wireless networks require the same security measures as those connected to the Internet to prevent virus infection. Download and keep up-to-date anti-spyware and anti-virus programmes. The firewall setting should always be on[10].
- Disable identification broadcasting: An essential feature in wireless routers is identifier broadcasting. It broadcasts a signal to any nearby device, alerting it to its existence. One should avoid broadcasting this data if the individual utilising the network is already aware of its presence. Intruders can target insecure wireless networks by using identifier broadcasting. If our wireless router enables it, disable the identification broadcasting technique.
- Change the router's standard admin password: Hackers are aware of the factory default passwords for every new wireless router. They should update such

credentials and stick to lengthier ones from a security standpoint. Longer passwords are more difficult to crack.

- Limit the computers that can connect to the wireless network: Each Media Access Control (MAC) address on a system is unique. Routers offer a unique feature that restricts the network's access to units with certain MAC addresses. Don't depend only on this step because some hackers have been known to mimic MAC addresses.

3. CONCLUSION

Wireless networking is rapidly evolving, as indicated by widespread installations of several wireless networks of various sizes, including wireless personal area networks (WPANs), metropolitan area networks (WMANs), local area networks (WLANs), and wide area networks (WANs). These mobile systems can take many forms, including ad hoc networks, mesh networks, cellular networks as well as domain-specific networks like automotive communications systems and sensor systems. Yet, because of fundamental communication are conducted out via electromagnetic radiations in open area, wireless communication lack security measures. Wireless communication present a distinct challenge to the computer and network security communities. Many technological problems are associated with the attempt to enhance wireless network encryption, including compatibility with current wireless networks, complexity in execution, and practical values in the actual market. The purpose for this special issue is the necessity to tackle wireless communication security and give timely strong technological contributions.

REFERENCES:

[1] C. M. G. Gussen, P. S. R. Diniz, M. L. R. Campos, W. A. Martins, F. M. Costa, and J. N. Gois, “A Survey of Underwater Wireless Communication Technologies,” *J. Commun. Inf. Syst.*, 2016, doi: 10.14209/jcis.2016.22.

[2] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, “Opportunities and challenges of wireless communication technologies for smart grid applications,” 2010. doi: 10.1109/PES.2010.5589988.

[3] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, “Survey of wireless communication technologies for public safety,” *IEEE Communications Surveys and Tutorials*. 2014. doi: 10.1109/SURV.2013.082713.00034.

[4] K. Moorthy *et al.*, “Barriers of mobile commerce adoption intention: Perceptions of generation X in Malaysia,” *J. Theor. Appl. Electron. Commer. Res.*, 2017, doi: 10.4067/S0718-18762017000200004.

[5] J. J. Hew, “Hall of fame for mobile commerce and its applications: A bibliometric evaluation of a decade and a half (2000-2015),” *Telemat. Informatics*, 2017, doi: 10.1016/j.tele.2016.04.003.

[6] M. Dahiya, “Evolution of Wireless LAN in Wireless Networks,” *Int. J. Comput. Sci. Eng.*, 2017.

[7] G. Smilarubavathy, N. V Abiramy, D. Pavithra, and R. Nidhya, “The Survey on Evolution of Wireless Network Generations,” *Int. J. Sci. Technol. Eng.*, 2016.

[8] I. Kartvelishvili and T. Todua, “Security issues in wireless network,” *Glob. Bus.*, 2017, doi: 10.35945/gb.2017.03.023.

[9] F. Vakil, “Wireless Networks and Security Issues,” *Rev. Bus.*, 2005.

[10] M. Hasan and N. Prajapati, “An attack vector for deception through persuasion used by hackers and crakers,” 2009. doi: 10.1109/NetCoM.2009.59.