



Department of Electronics and Communications Engineering

Wireless Security

Prepared By

Shams Ahmed Ayat

ID: 2015-2-55-016

Shusmita Sarkar

ID: 2015-2-55-026

Fariha Kabir

ID: 2015-2-55-014

Supervised By

Mohammad Rafsun Islam

Department of Electronics and Communications Engineering

Letter of Transmittal

To
Department of Electronics and Communication Engineering
East West University

Subject: Submission of Project Work Report on Wireless Security (ETE-498)

Dear Sir,

We are pleased to let you know that we have completed our Project work program on Wireless Security. The attaché contains the Project work report that has prepared for your evaluation and consideration. The Project work has given us a great opportunity to work with the Wireless Security and allowed us the opportunity to apply the theoretical knowledge in the real-life situation, which we have acquired since last four years from you and the other faculty of EWU, which would be a great help for us in future.

We are very grateful to you for your guidance throughout the Thesis period, which helped us a lot to acquire knowledge.

Thanking you.

Shams Ahmed Ayat

2015-2-55-016

Shusmita Sarkar

2015-2-55-026

Fariha Kabir

2015-2-55-014

Declaration

We, therefore, announce that this Project work was done under ETE 498 and has not been submitted somewhere else for the necessity of any degree or diploma or any reason but publication.

Shams Ahmed Ayat
2015-2-55-016

Shusmita Sarkar
2015-2-55-026

Fariha Kabir
2015-2-55-014

Acceptance

We hereby declare that this thesis is from the student's work and best effort of us, and all other sources of information users have been acknowledged. This Project work has been submitted with our approval.

Supervisor:

Mohammad Rafsun Islam

Department of Electronics and Communications Engineering

Chairperson:

Dr. Mohammed Moseur Rahman

Department of Electronics and Communications Engineering

East West University

Acknowledgment

Firstly, our most heartfelt gratitude goes to our beloved parents for their endless support, continuous inspiration, great contribution and, perfect guidance from the beginning to end. We owe our thankfulness to our supervisors for their skilled, almost direction, encouragement, and care to prepare ourselves. Our sincere gratefulness for the faculty of Electronics and Communications Engineering whose friendly attitude and enthusiastic support has given us for four years. We are very grateful for the motivation and stimulation of our good friends and seniors. We also thank the researchers for their works that help us to learn Wireless Security

Abstract

In this project, we described wireless attacks and security protocols briefly. As security for a wireless network is a very important issue, attacks faced by a wireless network should be analyzed. Our research aims to understand the security issues in a Wireless Sensor Networks system and protocols that can be used to combat the issues. This paper will give an idea about past security issues and vulnerabilities as well as present issues and vulnerabilities in different cases and the security protocols that can be considered. Some common attacks and attack issues in Ad-hoc Mobile network with 4G and 5G wireless network systems are analyzed in terms of security challenges and combating ideas both established and proposed. This paper describes the security protocols based on network fields like Ad-hoc Mobile network systems, 4G & 5G cellular networks and, helps with solutions to the vulnerabilities of the common and special attacks in such fields.

Keywords— Wireless Security, Wireless Sensor Network, Ad-hoc mobile network, Vulnerabilities.

Table of Contents

Chapter 1 INTRODUCTION	1
1.1 Overview.....	1
Chapter 2 LITERATURE REVIEW	5
2.1 GENERAL.....	5
2.2 SURVEY ON WIRELESS NETWORK SECURITY	5
Chapter 3 CLASSIFICATION OF COMMON ATTACKS ON WIRELESS SYSTEM	10
3.1 Rogue access point.....	10
3.2 Interference or Jamming	11
3.3 Evil twin.....	12
3.4 WarDriving	14
3.5 Blue-jacking.....	15
3.6 Bluesnarfing.....	15
3.7 IV attack.....	16
3.8 Packet sniffing:	16
3.9 Replay attack.....	18
3.10 WEP/WPA attacks	19
3.11 WPS attacks	19
Chapter 4 SECURITY FOR MOBILE AD-HOC SENSOR NETWORK	21
4.1 Mobile Ad-hoc Network (MANET)	21
4.2 Security Issues with Ad-hoc Network	21
4.2.1 Internal attacks	22
4.2.2 External attacks.....	22
4.3 Security attacks	23
4.3.1 Passive Attack.....	25
4.3.1 Active attack	25
Chapter 5 SECURITY FOR 4G AND 5G CELLULAR NETWORK.....	29
5.1 Existing cellular network issues and 5G.....	30

5.2 Threat models and classification.....	30
5.2.1 Attacks against privacy	31
5.2.2 Attacks against the integrity.....	32
5.2.3 Attacks against availability	32
5.2.4 Attacks against authentication	32
5.3 Countermeasures.....	33
5.3.1 Cryptography method	33
5.3.2 Human Factors	34
5.3.3 Intrusion detection method.....	34
5.4 Authentication and privacy-preserving schemes for 4G and 5G	35
5.4.1 Handover authentication with Privacy	36
5.4.2 Mutual authentication with Privacy	38
5.4.3 RFID authentication with privacy.....	40
5.4.4 Deniable authentication with Privacy	42
5.4.5 Authentication with mutual anonymity.....	42
5.4.6 Authentication and key agreement with Privacy	43
5.4.7 Three-factor authentication with privacy.....	44
Chapter 6 DATA SECURITY IN WIRELESS NETWORKS	47
6.1 How It Works.....	47
6.2 Analysis.....	48
6.3 Security Challenges of WSN	50
6.4 Security in Wireless Sensor Networks (WSN)	51
6.5 Security Goals.....	52
6.5.1 Primary Goals	52
6.5.2 Secondary Goals	53
Chapter 7 Conclusion	55

Table of Figures

Fig 3.1: Rogue access point is introduced by the attacker that weakens the real AP and opens an opportunity to get information	11
Fig 3.2: Connecting SSID free wifi user opens a gate for an Evil twin to get encrypted data.....	13
Fig 3.3: Evil ting attack procedure.....	14
Fig 3.4: Packet sniffing within networks	17
Fig 3.5: Illustration of replay attack.....	18
Fig 3.6: Guessing possible combination of a PIN with WPS PIN	20
Fig 4.1: MANET(within-cluster nodes are transmitting data by routing to destination) Error! Bookmark not defined.	
Fig 4.2: a) passive attack(Darth pretends to be Alice), b) active attack(Darth observes the messages transmitted between Bob and Alice).....	24
Fig 5.1: comparison of 4G and 5G in terms of characteristics.....	29
Fig 5.2: Classification of attacks in 4G and 5G cellular network	31
Fig 5.3: Classification of countermeasures used in authentication and privacy-preserving scheme in 4G and 5G.....	33
Fig 5.4: Classification of authentication and privacy-preserving schemes for 4G and 5G cellular network	36
Fig 5.5: Categorization of authentication and privacy models	38
Fig 5.6: Classification of mutual authentication with privacy	39
Fig 5.7: Classification of RFID authentication protocols	41
Fig 5.8: Different models offered by the Kerberos protocol.....	43
Fig 5.9: Classification of three-factor authentication schemes with privacy	45

Acronyms

WWAN = Wireless Wide Area Networks

WLAN = Wireless Local Area Network

WPAN = Wireless Personal Area Network

SSID = Service Set Identifiers

WEP = Wired Equivalent Privacy

MAC =Media Access Control

SBKH = State-Based Key Hop

WNIC = wide area network interface coprocessor

MANETS = Mobile Ad-hoc networks

DoS = Denial of Service

AODV= Ad-hoc On-demand Distance Vector

QOS = Quality of Service

CoMP = Coordinated Multi-Point

MITM = Man-In-The-Middle

FIFO = First in First out

AES = Advanced encryption standard

RFID = Radio-frequency identification

ECC = Error Correction Codes

Chapter 1

INTRODUCTION

1.1 Overview

Wireless and mobile networks are rapidly extending their capabilities. Wireless communication is changing into in style today due to its immovability, versatility, convenience, adaptability, and consistent network. Wireless communication allows a user the capability of conducting commerce at any time, with close to anyone, from anywhere, using a mobile communication channel. This can also be operated as an entry form to the Internet. Wireless network protection is the mechanism by which protection on a wireless computer network is planned, enforced, and maintained. It is a subset of network security that adds safety to a network of wireless computers. Wireless network security mostly defends a network from unauthorized and malicious attempts to access it. Wireless network security is usually accomplished by wireless devices that encrypt and protect all wireless communication by default. Wireless communication is the transfer of information between two or more points without the connection by an electrical conductor or cables. Applications might including point-to-point communication, point-to-multipoint communication, broadcasting, cellular networks, and other wireless networks. There are three different types of wireless networks.

- **Wireless Wide Area Networks (WWAN):** WWANs are created through the use of mobile phone signals typically provided and maintained by specific mobile phone (cellular) service providers. WWANs can provide a way to stay connected even when away from other forms of network access.
- **Wireless Local Area Network (WLAN):** WLAN are wireless networks that use radio waves. The range of a WLAN can be anywhere from a single room to an entire campus.
- **Wireless Personal Area Network (WPAN):** WPANs are short-range networks that use Bluetooth technology. They are commonly used to interconnect compatible devices.

To access the internet in a wireless network, the clients are connected with the Access Point and that AP is connected to the wireless router. The function of the wireless router is to broadcast a signal through the air and all the wireless clients within the range can connect to the wireless network. Within the broad organization of the Institute of Electrical and Electronics Engineers (IEEE), the 802 group is the section that deals with network operations and technologies.

Despite the benefits that wireless communications provide networks like portability, greater flexibility, productivity, roaming ability, low setup expenses, and much more, wireless network security is the issue and the concern continued to be great. The quality of wireless networks conjointly introduces issues. The quality of users, the transmission of signals through the outside, and also the low power consumption of the mobile user wake a wireless network an oversized variety of options distinctively completely different from those seen in a very wireline network. Problems with security and privacy become a lot of distinguished with wireless networks. Recent safety standards have said the increasing use of wireless technology does not catch up with security. Wireless communications vulnerabilities are currently on the rise due to the massive demand for higher data rates, the need for sophisticated and roaming services, and the huge deployment of services around the world. With the increasing reliance on technology, it is becoming more and more essential to secure every aspect of online information and data. As the internet grows and computer networks become bigger, data integrity has become one of the most important aspects for organizations to consider. This has thus generated serious challenges to the safety of wireless networks and wireless applications. Wireless networks and mobile devices are, unfortunately, subject to the same degree of vulnerabilities and threats as traditional wired networks. A good network security system helps businesses reduce the risk of falling victim to data theft and sabotage. Network security helps protect your workstations from harmful spyware. It also ensures that shared data is kept secure. The present era, however, the dangers and threats associated with wireless networks have found a new aspect, primarily because the means of contact, the airwave, of wireless networks are freely exposed to intruders who take over profit from that to start malicious attacks such as Rogue access point, Evil twin, WarDriving, Blue-jacking, denial-of-service attacks, identity theft, Bluesnarfing, IV attack, active jamming attacks to disrupt legitimate transmissions. Again, firewall-protection intruders also bypass access to sensitive data communicated between two wireless devices. [1]

To combat these risks, you will make every effort to properly configure your WLAN. The wireless security issues are very hard to solve because the outsiders can see wireless network transmission waves which pose many security risks. A new vulnerability to existing wireless standards comes into existence now and then. The problem with having the signal broadcast though is that it is difficult to contain where that signal may travel. If it can get from upstairs to your office in the basement then it can also go that same 100 feet to your neighbors living room. Or, a hacker searching for insecure wireless connections can get into your systems from a car parked on the street. By their very nature, wireless networks are difficult to roll out, secure, and manage, even for the savviest network administrators. When wireless technology was first adopted, there were very few hazards. But with wireless access, the hacking methods have become far more advanced and innovative. Hackers identified wireless networks relatively easy o break

into, and have even used wireless technology to crack into wired networking. As we know Wireless signals are electromagnetic waves traveling through the air. The problem with having the signal broadcast though is that it is difficult to contain where that signal may travel. If it can get from upstairs to your office in the basement then it can also go that same 100 feet to your neighbors living room. Or, a hacker searching for insecure wireless connections can get into your systems from a car parked on the street. And also with easy-to-use Windows or Linux-based software made available free of charge on the internet, cracking has become much simpler and more affordable.

WEP system offers WLAN protection by encrypting the information transmitted over the air so that the information can only be decrypted by the receivers with the right encryption key. But WEP, unfortunately, has limited support and significant design flaws and vulnerabilities which make breaking easier in comparison with other security implementations. Because of these security flaws, WEP has been deprecated in favor of WPA developed by the Wi-Fi Alliance. But it also has weaknesses like (collision avoidance implementation can be broken, vulnerable to denial of service attacks). WPA2 is the Wireless network protection approach applied to WPA. WPA uses TKIP (Temporal Key Integrity Protocol) while WPA2 can use TKIP or the more advanced algorithm of AES. Moreover, WPA3 is usable on new, Wi-Fi Alliance-certified routers. WPA3 replaces WPA2. Although WPA3 is more secure and concise than WPA2, Wi-Fi Alliance will continue to assist and update the WPA2 protocol for the foreseeable future. While not flawless, WPA2 and WPA3 is the most secure choice at present.

We know wireless security is best approached by looking at external and internal policies, management, and security design that deliver high levels of security and flexibility to adapt to changing threats. These policies can help you decide how you can handle access to your wireless network and how you can keep approved users safe and protected, and prevent unauthorized users. Several of these approaches are best practices for any networking environment, while others are unique approaches for addressing threats to wireless health. Anyone can protect his/her wireless network with an inclusive approach. Through the use of WPA on access points and wireless and RADIUS cards as an authentication system, with a specific selection of the authentication process, the level of protection is now achieved as high as possible. [2] Then again, a VPN can be a viable alternative. This is a slightly different technique which allows us to obtain a safe process of authentication as well as the integrity of the data transmitted. In this thesis, we are using SSID (Service Set Identifiers), WEP(Wired Equivalent Privacy), Address Validation MAC (Media Access Control) as a better solution for basic security.

The paper is divided into seven parts. The introduction chapter deals with the general viewpoints and the main inspiration behind the analysis. Literature Review presented in chapter 2, while chapter 3 presents the Classification of Attacks on Wireless System. In chapter 4 briefly presents Security for Mobile Ad-hoc Network, while chapter 5 described Security for 4G and 5G cellular network, and in chapter 6 we discussed Data Security in Wireless Networks. Finally, chapter 7 concludes the conclusion.

Chapter 2

LITERATURE REVIEW

2.1 GENERAL

As we know wireless networks have broadcast nature so there are various security issues in wireless communication. Security is a common concern for any network system. A wireless network is a vigorous research domain.

To attain precise strategy and procedures to carry out the study, the next step of the researcher to undertook and give a review of the literature. Literature and review are some of the basic tasks of any researcher. It assists, leads the researcher to as below,

- Understand where who and how to research relevant to the present study was carried out,
- How the terms, variables were defined and measured,
- What were the measures, outcomes/findings of the earlier research?

The literature review also assists the researcher in recognizing the space that exists between past research, present framework and possible outcomes of the study

This chapter will review the current literature on the relevant area of this research. These areas include all the vast literature collected related to the performance improvement of WSN, IEEE 802.11 WLAN, WPA, WPA2, WEP, WEP2, IEEE 802.15.4 LR-WPAN, EAP-TLS, Wireless Communication in Process Automation, power utilization, WSN, key setting mechanism, SBKH protocol. Earlier contemplateable work has been carried out to enhance the diminishing performance. Network attacks were found to be as complex as the system they are trying to infiltrate. Attacks are might be planned or unplanned. For preventing attackers, the network experts are deriving a large number of plans of action as the intruders increase.

2.2 SURVEY ON WIRELESS NETWORK SECURITY

Jyh-Cheng Chen and Yu-Ping Wang at (2007) have mentioned the execution of the different type of EAP (Extensible Authentication Protocol) techniques and also a comparison for four separate short-range wireless communications protocol (Bluetooth, ultra-wideband, ZigBee and Wi-Fi (over IEEE 802.11))

specifications with low power consumption was presented Implementation of these techniques is very composite but it is shown in this paper that we can easily do it with the aid of WIRE 1x. It's a client-side OPEN SOURCE execution and the communication is more reliable and remains safe and unthreatened If the client-side is more well built. These WIRE 1x work easily with windows and bear almost all the authentication methods specified in EAP. On the other hand, it is also useful in some secure manner of communication using WLAN. He also proposed a review of these common wireless communication standards, analyzing their key characteristics and behaviors in terms of different metrics, including transmission time, data coding performance, complexity, and as we write previously power consumption. He believed that the differentiation presented in this paper might convenience application engineers in selecting an appropriate protocol. It also covers various open-source libraries like WinPcap, Libnet, Openssl. [3]

This hash value has been encrypted with dual RSA and also sent to the destination. And then at the receiving end hash value of decrypted decoded is calculated with MD5 and differentiated with the hash value of original plaintext which is calculated at the sending end for its integrity. This helps us to know whether the original text is modified or not during transmission in the contact medium.

In this survey WEP protocol types, enhancements, weaknesses, WPA protocol types, WPA improvements such as new IV sequencing discipline, MIC, per-packet key mixing function, and rekeying mechanisms and explanation of major problems on WPA which occur in PSK part of the algorithm. And at the last, it presents the wireless security protocol of third-generation known as WPA2/802.11.

They also offer a new mechanism called a multiple slot system named MSS which makes use of the key selector, slot selector, and MIC shuffle selector. [4] [5] [6]

Bahareh Shojaie, Iman Saberi, and Seyyed MortezaAlavi have conducted an EAP-TLS survey to differentiate two forms of Extensible Authentication Protocol – transport layer security (EAP-TLS) so that using cryptographic methods, another technique can be given [7]. This new technique used Elliptical Curve Digital Signature Algorithm (ECDSA) and also contrasts it with the current EAP-TLS system and shows that by using the same memory level as opposed to EAP-TLS the new techniques provide good security, high speed, and more performance. New methods allow a compromise between security and efficient resource and time utilization.

Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong SeonHong described numerous wireless sensor network problems and challenges. This paper clarified dual forms of wireless security threats. One is the assault on protection mechanisms and the other against simple mechanisms such as routing mechanisms Significant

attacks described include denial of service attacks, transit information attacks, Sybil attacks, black hole/sinkhole attack, wormhole attack. There's also a holistic view of defense in wireless sensor networks.

Howitt, Jose A. Gutierrez in the year 2003 has initiated that IEEE 802.15.4 is standard addressing which demands of Low-Rate Wireless Personal Area Networks or LR-WPAN which also works for a focus on enabling wireless sensor networks. The standard is identified by keeping up with a top-level of simplicity, as well as permitting for low cost and low power implementations. the 2.4 GHz is the operational frequency band including industrial, scientific, and medical band providing nearly world wide handy. So far this band is also used by other IEEE 802 wireless standards. He moreover proposed a brief specialized presentation of the IEEE 802.15.4 standard and analyzes the coexistence effect of an IEEE 802.15.4 arrange on the IEEE 802.11b devices. [8] [9]

Lifeng Sang and Anish Arora proposed a shared secret free wireless network security infrastructure based on two physical protocols named as cooperative jamming and enforcement of spatial signals. Cooperative jamming is for wireless confidentiality and Spatial signal enforcement is there for the authenticity of messages. The proposed infrastructure offers confidentiality, identity verification, verification of the message, privacy, non-repudiation of the sender, non-repudiation of the recipient, and anonymity [10].

In 2004 Michell and Srinivasan identified a State-Based Key Hop (SBKH) protocol intended to replace all these WEP and WPA of battery-operated devices, like sensors in a wireless sensor network, along with users of small offices, home offices (SOHO) as well as WSN nodes. State-based key hope protocol provides cryptography in a new state-based manner to ensure low-cost and robust security without additional encryption overheads. Implementing SBKH on real hardware represents a challenge

Anthony DeJoie, Bhagyavati, C. Summers provide a survey of the different techniques for strengthening security in WLAN. They explain first-generation WLANS, second-generation WLANs, and discussed their issues and securities. [11] [12]

Chan. Chan. Perrig, H. in 2005 Presented a key setting mechanism between two sensor nodes that are based on the common confidence of a third node somewhere within the sensor network. The nodes and their shared keys are distributed across the network, so that there is a node C sharing a key in both A and B for any two nodes A and B. Hence the key protocol of establishment from A to B could be routed securely via C [13].

Bahareh Gholamzadeh, HoomanNabovati in 2008 addressed various sources of power utilization in wireless sensor networks and introduced multiple design principles that decrease the power consumed and thus increase the network's lifespan [14].

Wireless Communication in Process Automation introduced by In 2010. The growth of wireless networking technology, particularly in wireless short-range networking technology, offers a tremendous opportunity for wireless connectivity of network elements in both gas and oil and other chemical processing plants. In a harsh industrial context, the precondition of a field network requires real-time support for congested traffic, capacity, security, reliability as well as usability. Any wireless network must meet these requirements to be able to function. He also offers a detailed overview of the requirements for wireless process automation, the relative status of existing wireless short-range technologies based on the rules outlined, and the related deficiencies. [15]

Andrew Gin and Ray Hunt contrasted the emerging wireless 802.11 security architecture performance analysis. Paper clarified the security measures for wireless networks. Research clarified security layers such as WEP shared key authentication and 104-bit encryption, WEP shared key authentication and 40-bit encryption, WPA with EAP TLS authentication and RC4 encryption, WPA with PSK authentication and RC4 encryption, WPA2 with PSK authentication and AES encryption and WPA2 with EAP-TLS authentication and AES encryption. The impact on the passage is also debated in this paper [16].

From the literature review, it is obvious that many researchers have already done an extensive research to enhance the efficiency of wireless networks. The security solutions are often isolated and incapable of being integrated or of inter-operating with one another. The authors mentioned above recommended several methods for efficient and secure fusion of the data. The variety of security technologies contributes to greater complexity and maintenance costs, which in particular could lead to a bursting administrative and managerial workload. It is found in the research work that many organizations currently deploy wireless networks usually to use IEEE 802.11b protocols, but the technology chosen is not reliable and is therefore highly vulnerable to active attacks and passive intrusions. Previously existing security protocols such as WEP, WPA, and WPA2 provide some pros and cons, and these security protocols also contain some vulnerability.

For example, In Gamal Selim, Dr. Hesham, Abdul Salam's article, they gave a comparison between WEP2, WPA2, and MSS and not cover all known attacks and protocols. The research teams also did not provide for the implementation of the attacks but instead gave a short description of them. And in Bahareh Shojaie, Iman Saberi, and SeyyedMortezaAlavi's article they only talk about an alternative technique of EAP-TLS, not for EAP-TTLS. Furthermore, WSNs brings a whole host of novel research challenges to the scientific community. Anthony DeJoie, Bhagyavati, C. Summers provides an overview of WLAN, cataloged it according to generation but did not provide any implementation, execution of the

threats and solutions of the issues are identified without any explanation. They must be tackled at multiple levels through different protocols and mechanisms. There is lots of research still to be done.

To assure the security of wireless network Data Confidentiality, Data Authentication, Network Availability is our primary goal. Data Integrity, Non-Repudiation, Modifications, Masquerading, and Replaying are within the part of data confidentiality. Our secondary goal is to be accomplished Data Freshness, Route Freshness, Self-Organization, Time Synchronization, Power Management, and most importantly Secure Localization. In this regard, we have developed and proposed this efficient mechanism that can provide almost the same level of security guarantee both in the home network and in a foreign network.

Chapter 3

CLASSIFICATION OF COMMON ATTACKS ON WIRELESS SYSTEM

In terms of wireless system wireless attack is the most common issue among issues faced by the organizations, working for wireless connection. The reason behind it is the information that can create a risk for the users if any of the personal information that comes to the internet and is broadcasted to an entire world. It helps criminals to spread their crimes and can cause a huge pay for a personal or a company or the country. It is, therefore getting very important to know about such attacks in terms of a wireless system. Some common attacks that can be mentioned here. [17]

3.1 Rogue access point

The Rogue access point is an access point that is added to an encrypted wireless network system without any authorization from the authentication organization that opens a path for the attackers on the network with data or information. That person may have no idea about the accessibility. This happens to somebody who has private information about any private project or company that is confidential. With the access point, it opens a back door to get the information. Using this anyone can get access to anyone's personal information.

If authentication is not enabled in the network system it becomes very easy to grab his/her data with the help of the access point.

One can combat it by using some techniques, for example, MAC address filtering, disable unused ports, using Roguescanner like Airmagnet and AirDefence, that secure the wireless data connection and do not let others have it. [18] [19]

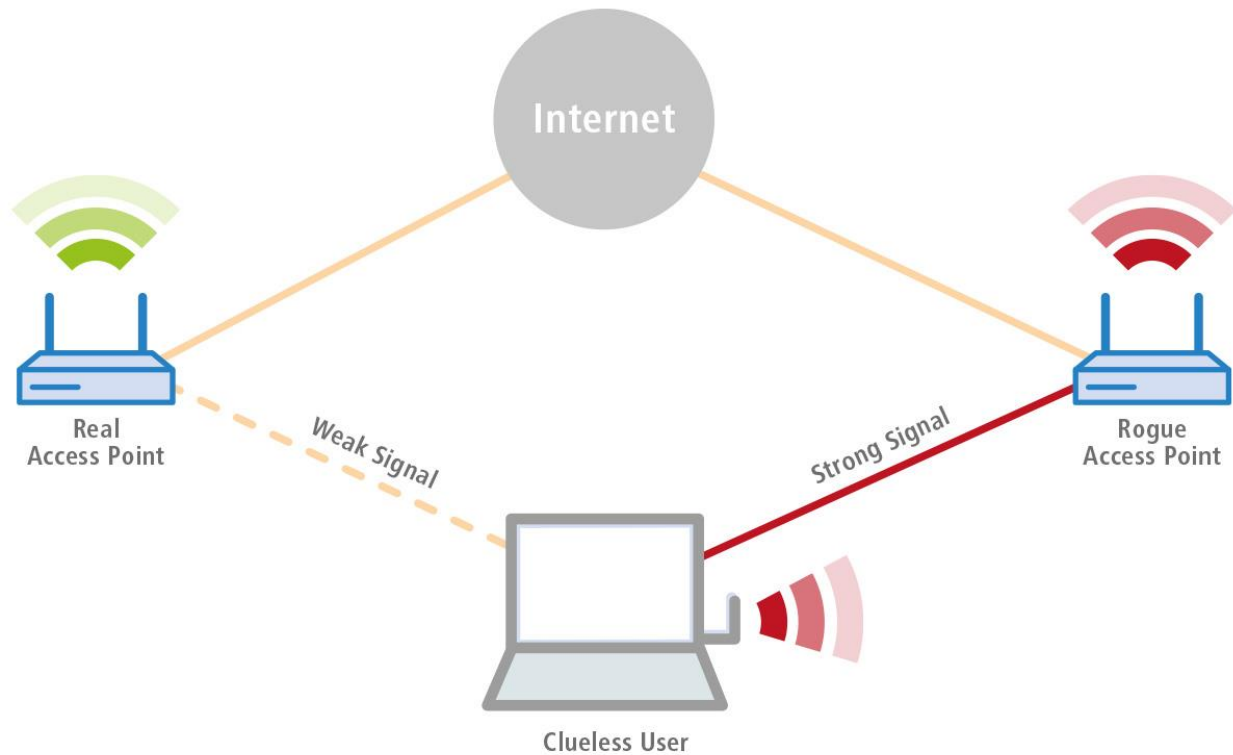


Fig 3.1: Rogue access point is introduced by the attacker that weakens the real AP and opens an opportunity to get information

In this type of attack, an intruder creates a Software-enabled Access Point (SoftAP), also known as a rogue access point, to lure these IoT devices to associate with this unauthorized access point to sniff transmitted data (as shown in [Figure 3.1](#))

Examples: Soft access point: Wifi adapter using windows virtual wifi or Intel's My Wifi can be set up as soft access point. It does not need any physical Wifi router to get access to ones' device.

3.2 Interference or Jamming

Interference is a very big challenge to deal with for a wireless system. It becomes very obvious that signals will interfere and owing to the fact it becomes very hard to stop the interference of the signals. Interference creates huge difficulties in transmitting and receiving signals. Mostly this sort of problem is created by Bluetooth handset, microwave oven, and cordless phones. It can be created in other ways too. In Evil twin, it is created too.

Combating Interference or jamming is the first goal to deal with. If interference happens, spectrum analysis can be a helpful way. Simple software like AJAX using plus can also be used to detect one's

traffic. Power boosting can be used if the interference is caused by other devices. Using a different range of frequencies can be considered as another solution. [20]

For instance, the technique of weak cooperation among base stations proposed by some authors offers significant network performance when employed as it provides a framework for optimal performances of adjacent base stations under some performance objectives. Also, an evolutionary strategy approach employed by some other authors shows proficiency in the management of channel allocation aimed at minimizing the problems of interference, which can manifest as call blocking or dropping.

3.3 Evil twin

In a wireless communication system, an Evil Twin is a rogue access point masquerade as a legitimate Wifi access point that opens a way for attackers to gather personal and corporate Data or Information without the knowledge of the end-user.

An evil twin can be created easily using a smartphone or any internet-capable device or some simple software. With the evil twin access point, the attacker opens a position for himself that can be used as a legitimate hot spot and to discover what service set ID and radio frequency the legitimate access point uses. [21]

An Evil twin is not a new phenomenon in a wireless system, historically it was called clones or honeypots. The difference is now most businesses or industrial organizations using wireless devices in public places that make it easier to create an evil twin. [22]

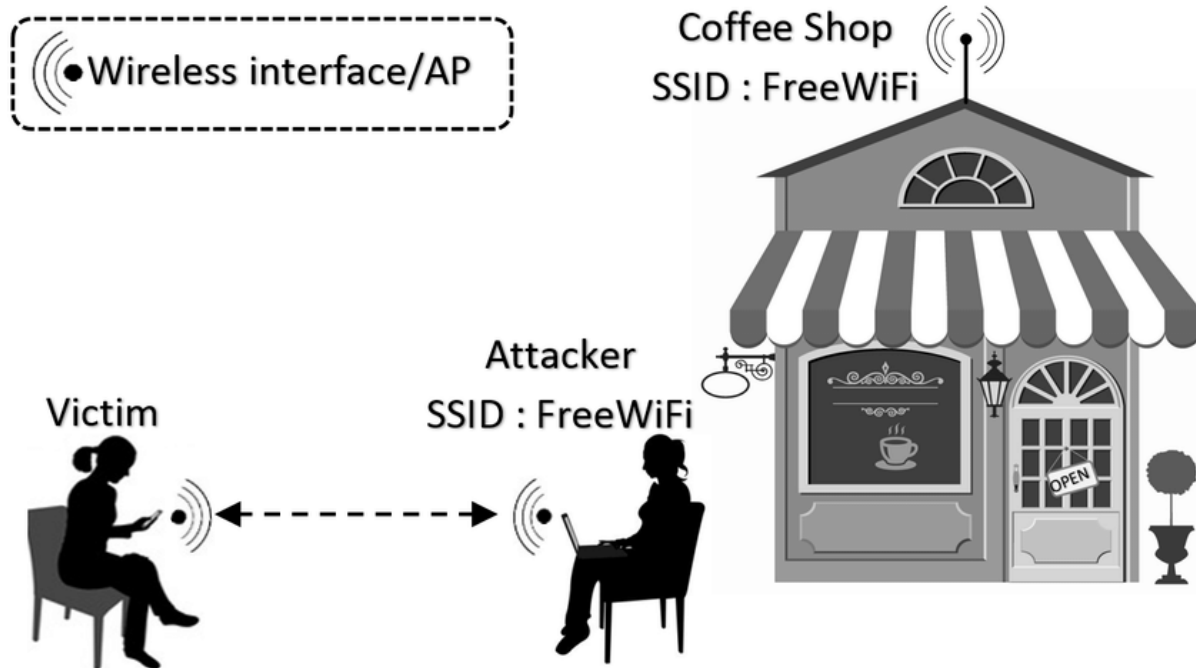


Fig 3.2: Connecting SSID free wifi user opens a gate for an Evil twin to get encrypted data

Illustration of an Evil Twin Attack. The attacker can successfully lure a victim into connecting to a fake access point instead of the legitimate access point when it provides a stronger/better signal to those customers(fig 3.2).

One of the solutions of an evil twin that one can rid of it is encrypting data. It will help create a barrier for one who tries to involve in evil twin thing. End-users should use public hot spots only for internet browsing and try to refrain from banking or online purchase. Employees use wireless devices should connect to the internet through a VPN to protect corporate data. [19]

Following is an example of an Evil twin attack.

Step 1: Setting up a software access point on a laptop on a different channel by the attacker that will mimic the hot spot network and makes sure it is just like the free hot spot network.

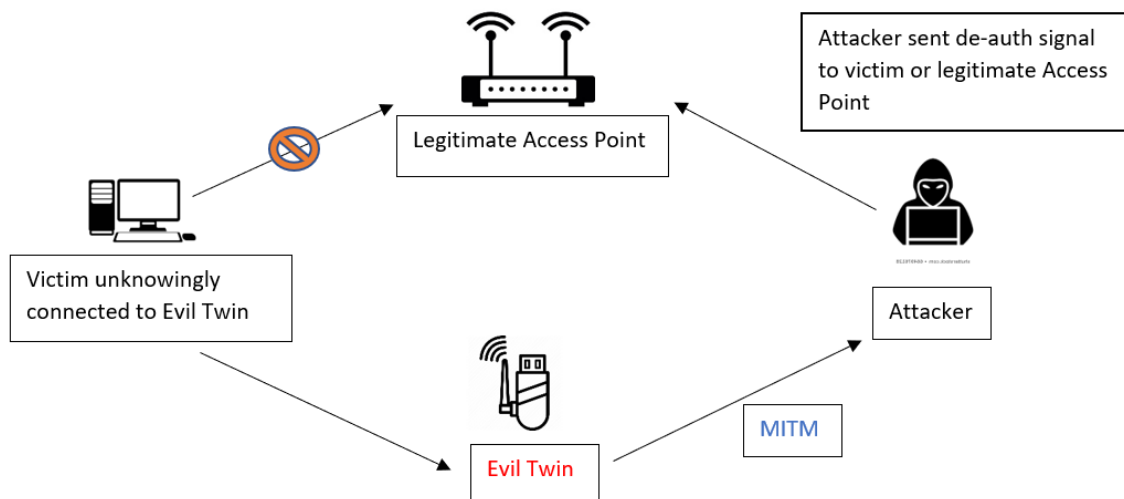


Fig 0.1: Evil ting attack procedure

Step 2: The attacker will jam the hot spot AP wireless signal and block physical radio-frequency.

Step 3: The clients' laptop searching for a better connection, will see the evil twin AP advertising the same SSID as a hot spot and connect.

Step 4: The attacker is to have the software running on the laptop to assign the IP of the client that just connected to the evil twin to route properly.

3.4 WarDriving

WarDriving is a way to find an access point to others' devices with the wrong intention. With the help of free WI-FI or other GPS functionalities, driving around, they can gather a huge amount of information. Special types of software are also used sometimes in such cases. With the data, the person controlling can get more information on how he/she can get more data.

The term was originated from a phone-hacking technique used in the 1980's-war dialing. War dialing is consist of every dialing phone number in a specific sequence in search of modems. Since the strategy was so effective even in today's life many professionals and crackers employ it maliciously. Wardriving is likely war dialing and eventually to aid to immodest attackers.

Wardriving got popularity in 2001. The initial wardriving tools consisted of simple software coupled with WNIC(wide area network interface coprocessor). As these programs were not designed by professionals, the inefficiency needed some useful solutions. However, it is still relevant to use WNIC nowadays in modern programs. [23] [24]

As technology advances, more security professionals are likely to implement a form of wardriving as a part of their regular management regime. At the same time, more attackers are liable to enhance detection and develop better ways to exploit a network.

3.5 Blue-jacking

This is hacking using Bluetooth. Blue-jacking refers to some kind of crime where one hacks another one's device via Bluetooth and publishes unsolicited messages. This is considered spam for what one might not be able to get pop-up notifications. It doesn't depend on an antenna, Bluetooth is the way of Bluejacking. As there is no authentication one can easily pass messages via Bluetooth and can use it further

There is a variety of tools that are available for Bluejacking. Such tools can bypass the entire manual procedure for implementing Bluejacking. These software tools can be downloaded, installed, and run on a Bluetooth configured device to send any anonymous, unsolicited message to another Bluetooth enabled device. This software searches for all discoverable Bluetooth devices and sends a file to them. A small text is sent to spam the other Bluetooth enabled device. To customize the message to be sent, the file or the message to be sent need to be put into a directory specific to the device and the software. This message or file will then be sent when Bluejacking is done. [25]

3.6 Bluesnarfing

It is more severe than Bluejacking since it is used to steal one's information. It enables the Bluetooth for Mobile device for one to steal the whole information like contacts or images that can carry a serious security issue and be harmful to any individual. It is permeability that exposes the individual's weakness via Bluetooth.

Bluesnarfing allows attackers or hackers to get access to users' calendars, contacts, emails, and text messages which are personal data of the user.

In discoverable, mode Bluetooth-enabled devices are more vulnerable to bluesnarfing attacks. As a result, hackers can have access to Bluetooth-enabled devices and respond to queries from other devices and thus the attacker gets unauthorized access to information. [25]

Mobile discovery mode is generally activated by default in most mobile devices. Unless the mode is deactivated the device is vulnerable to bluesnarfing attacks. Turning off is the only solution to protect devices from such attacks. Keeping the device invisible can also protect from bluesnarfing.

3.7 IV attack

IV attacks refer to an Initialization Vector attack. It can be a severe threat to wireless communication. It causes some modifications at the initialization vector of an encrypted transmitting data in a wireless communication data packet. Afterward, the attacker can have access to much information about the plaintext of a packet and generate a new encryption key, and using the same initialization vector the attacker can decrypt others packets.

With the decrypt table, the attacker can decrypt other packets of the network and get information on a plain text of the network. [26]

3.8 Packet sniffing:

Packet sniffing or capturing is possible when the packet is not encrypted and the person is in a position that can see the type of data is sending to an individual. So, packet sniffing is a tough job to do.

Identifying the type of sniffer can depend on how sophisticated the attack is. It is possible sniffers to hide for a long time in the network [27]. Some anti-sniffing applications can be used to catch the intruders. A sniffer can be software installed onto your system, a hardware device plugged in, sniffer at a DNS level or other network nodes, etc. Practical networks are complex and so it becomes difficult to identify sniffers. As network follows layered protocol and each has to perform defined tasks to do, sniffers can attack at any layer. Though sniffing depends on the purpose of attack but the layer 3(network) and layer 7(application) is the main concern for such attacks. Secured versions of protocols are also available but if some systems are still using the unsecured versions then the risk of information leakage becomes considerable. [28]

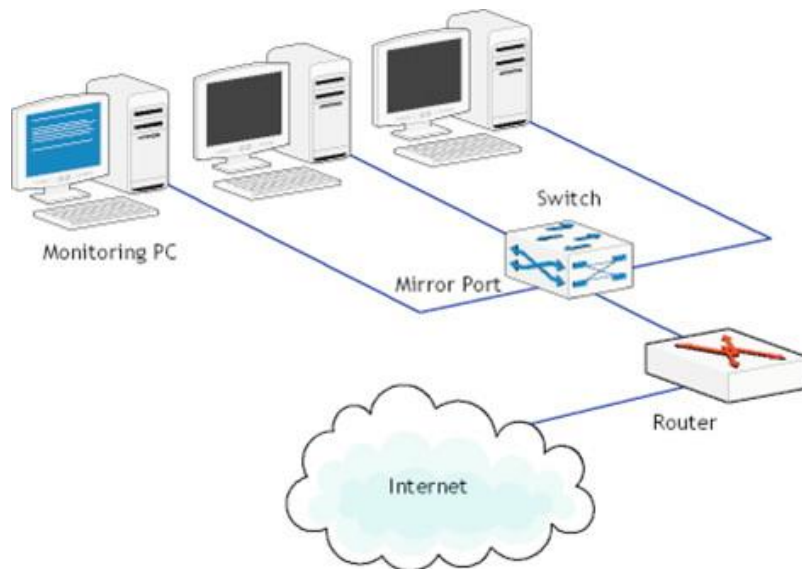


Fig 0.2: Packet sniffing within networks

In the primitive form, a packet sniffer (also referred to as network sniffer) captures all of the packets of data that pass through a given network interface. To capture these packets, your network interface must be in Promiscuous Mode and the interface needs to be connected to a port that has visibility to all of the packets. For example, if you are interested in a specific subnet, you would connect the sniffer to a switch or hub on that subnet. Most modern switches today support port mirroring via a Switched Port Analyzer (SPAN) or Remote Switched Port Analyzer as shown in Figure 3.4. These ports are typically connected to IPS, network monitoring devices, or performance measurement devices that can detect network loading. [29]

If packet sniffing is done it becomes very easy to what is going on the network and information can be used for any-where.

One must make sure that one's network card is silent to be successful in packet sniffing which means one's card is not sending information to the network if the network is busy.

So due to get rid of the attack one has to ensure that the data is sending across the network is encrypted. WPA2 or WPA can be used to encrypt data. With this encryption, it becomes very difficult for one to decrypt the data and see.

Organizations and individual users should keep away from applications that are using insecure protocols, like basic HTTP authentication, File Transfer Protocol (FTP), and Telnet to prevent the network from the attack. Instead, secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be preferred. In case there is a necessity for using any insecure protocol in any application,

all the data transmission should be encrypted. If required, VPN (Virtual Private Networks) can be used to provide secure access to users. [30]

3.9 Replay attack

It is a network attack. A Replay attack is repeating valid data transmission again and again to cause malicious actions. Here an individual spies on information that are sent between a sender and a receiver. That individual can also spy on the conversation of two people and also can intercept and retransmit it and leading some delay in transmission. This is such an attack in which an attacker can use the data to fool around to the computer so that they can get access without detection. Sometimes attackers get the encryption key and use it to get authentication to a packet.

One of the best techniques to avert replay attacks is by using strong digital signatures with timestamps. Another technique that could be used to avoid a replay attack is by creating random session keys that are time-bound and process bound. A one-time password for each request also helps in preventing replay attacks and is frequently used in banking operations. Other techniques used against replay attacks include the sequencing of messages and non-acceptance of duplicated messages. [31] Replay attack can happen the following way-

- B sends a one-time token to A, which A uses to transform the password and send the result to B. For example, she would use the token to compute a hash function of the session token and append it to the password to be used.
- On his side, B performs the same computation with the session token.
- If and only if both A's and B's values match, the login is successful.
- Now suppose an attacker E has captured this value and tries to use it in another session. B would send a different session token, and when E replies with her captured value it will be different from B's computation so he will know it is not A. [32]

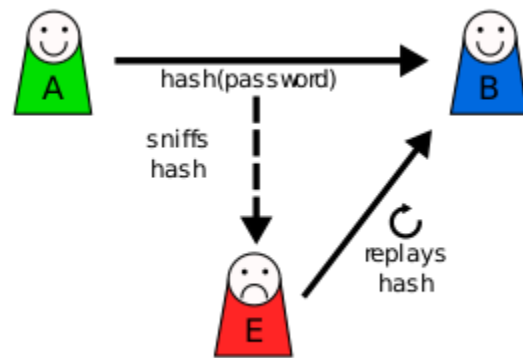


Fig 0.3: Illustration of replay attack

3.10 WEP/WPA attacks

The general weakness of the WEP encryption of system is the reason behind this WEP/WPA attacks in a wireless communication system. Since it's a very poor encryption technique, sometimes one's access point might not allow the WEP method of encryption. Owing to that, the encryption method is very poor, if anyone notices encryption using WEP that shouldn't be trusted as safe from attacks. [24] These access points become very vulnerable. Here are the basic steps we will be going through:

1. Start the wireless interface in monitor mode on the specific AP channel
2. Test the injection capability of the wireless device to the AP
3. Use airplay-ng to do a fake authentication with the access point
4. Start air dump-ng on AP channel with a filter to collect the new unique IVs
5. Start air play-ng in ARP request replay mode to inject packets
6. Run air crack-ng to crack key using the IVs collected

3.11 WPS attacks

WPS attacks are some forms of attacks in a wireless network that can be very dangerously harmful with a WPS password guessing tool by an individual is in a position to launch an attack in an individual network. Using the password tool attacker can reclaim the wireless network password and with the help of this password, an attacker can gain data and information from one's network.

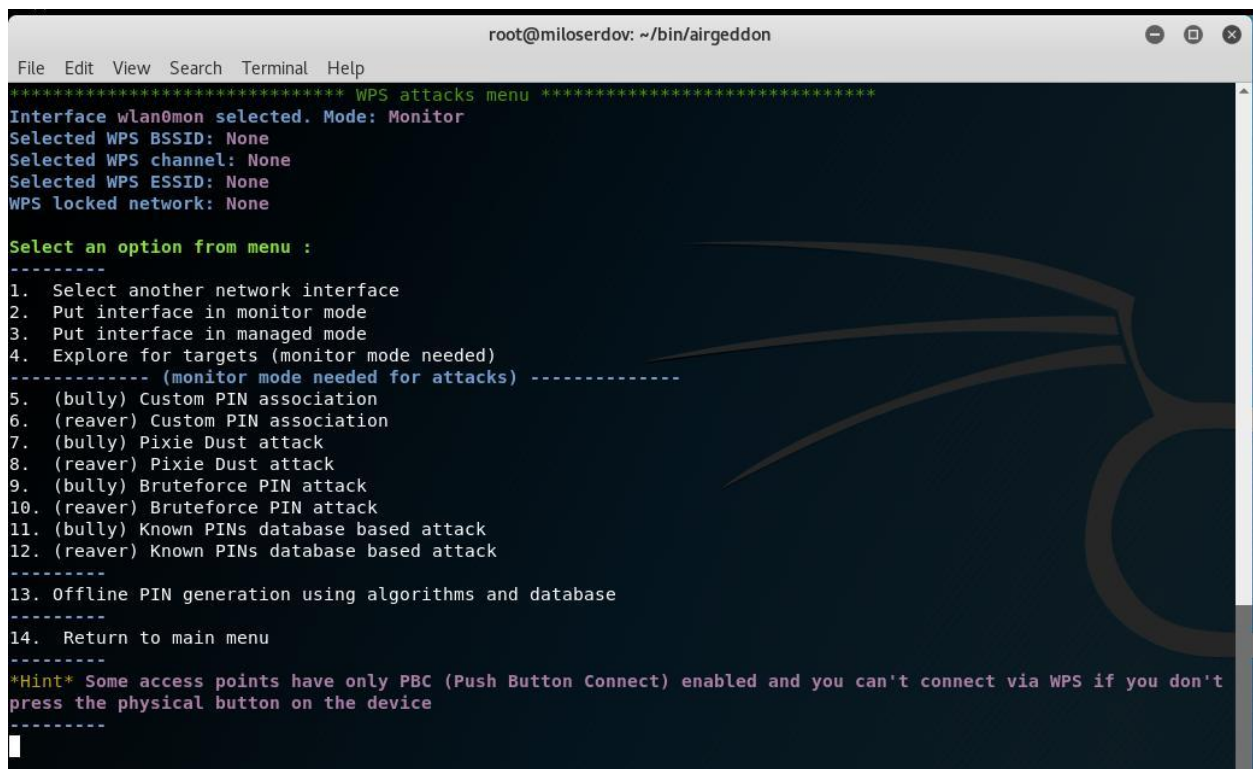
To avoid such attacks one's security protocol is needed to be very strong so that using the password tool the encrypted password can't be retrieved.

WPS Pin stands for "Wi-Fi Protected Setup" and it is 8 digit PIN. WPS Pin is used for making connections between a router and wireless printers and other devices.

Because of the poor design when creating WPS it was left vulnerable to a brute force attack. This is where an attacker simply guesses all possible combinations of the PIN until they find the correct one. With an 8 digit PIN using the numbers 0-9 that would present 100,000,000 possible combinations (10^8). If you could guess at a rate of 1 PIN per second (there is a delay waiting for a response from the AP) it would take 1,157.4 days to test all possible combinations. Statistically speaking you could expect to crack the PIN in roughly half that which would be 578.7 days. This isn't a viable attack vector. [33]

The 8th digit of the PIN isn't used as part of the PIN but is instead a checksum for the prior 7 digits. This reduces the possible combinations from 100,000,000 to 10,000,000 (10^7). This instantly reduces the attack

to 115.7 days to try all possible combinations or 57.8 days to try 50% based on a rate of 1 PIN per second. [34] [35]

A terminal window titled 'root@miloserdov: ~/bin/airgeddon' displays a 'WPS attacks menu'. The menu lists 14 options for WPS attacks, including custom PIN association, Pixie Dust attack, Bruteforce PIN attack, and Known PINs database based attack. A hint at the bottom states: '*Hint* Some access points have only PBC (Push Button Connect) enabled and you can't connect via WPS if you don't press the physical button on the device'.

```
root@miloserdov: ~/bin/airgeddon
File Edit View Search Terminal Help
***** WPS attacks menu *****
Interface wlan0mon selected. Mode: Monitor
Selected WPS BSSID: None
Selected WPS channel: None
Selected WPS ESSID: None
WPS locked network: None

Select an option from menu :
-----
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
----- (monitor mode needed for attacks) -----
5. (bully) Custom PIN association
6. (reaver) Custom PIN association
7. (bully) Pixie Dust attack
8. (reaver) Pixie Dust attack
9. (bully) Bruteforce PIN attack
10. (reaver) Bruteforce PIN attack
11. (bully) Known PINs database based attack
12. (reaver) Known PINs database based attack
-----
13. Offline PIN generation using algorithms and database
-----
14. Return to main menu
-----
*Hint* Some access points have only PBC (Push Button Connect) enabled and you can't connect via WPS if you don't
press the physical button on the device
-----
```

Fig 0.4: Guessing possible combination of a PIN with WPS PIN

When presenting the PIN for verification it is sent in 2 halves. The first 4 digits and the last 4 digits. These separate halves are then verified independently. This presents a huge weakness as it would be a much stronger key but the effective keyspace has now been reduced considerably. The first half of the PIN only has 10,000 (10^4) possible combinations and at our rate of 1 PIN per second would only take 2.7 hours to guess all possible combinations. The second half of the PIN, due to the checksum value, only has 1,000 (10^3) combinations and would take a meager 16 minutes to guess all possible combinations. To go from a total time of 4 months down to 3 hours to try all possible combinations. WPS PIN can be a very easy way to attack WPS protocol and get access to the network. [36] [37]

Chapter 4

SECURITY FOR MOBILE AD-HOC SENSOR NETWORK

4.1 Mobile Ad-hoc Network (MANET)

The word ad-hoc means 'not pre-planned' before it happens. In Mobile Ad-hoc networks (MANETS) the word carries the same connotation.

MANET is more like a scrabble game since any player(user) can place tiles(node) to any place as long as they are connected to one existing tile.

A mobile Ad-hoc network is defined as a network that is designed without a planned structure configuration.

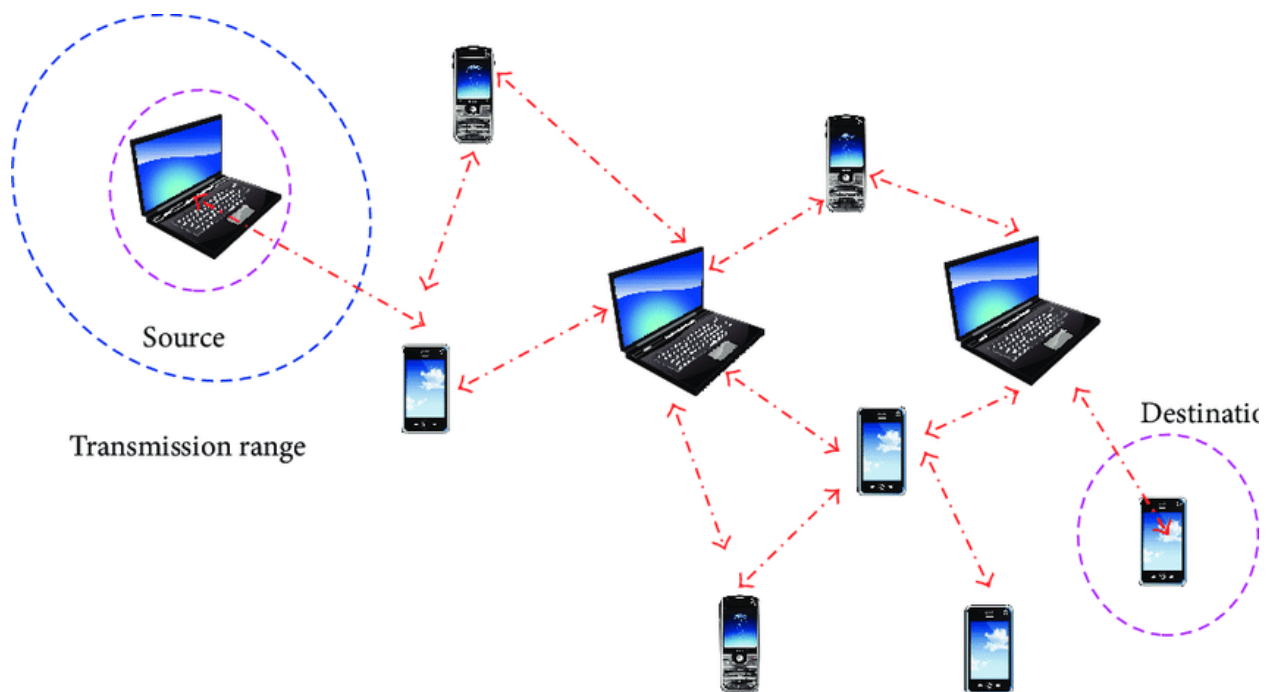


Fig 4.1: MANET(within-cluster nodes are transmitting data by routing to destination)

From a source node, a message is transmitted to the destination within the shortest hop number. Nodes advertise the routing table and find the destination hop with the upgraded sequence number.

Nodes can be connected dynamically without following any previous any conventional architecture. Nodes are rather configured in an autonomous. The general 'non-structure' is a decentralized arrangement of nodes.

4.2 Security Issues with Ad-hoc Network

The constantly changing structure protocol of MANET makes it vulnerable to security attacks. Like conventional networks security of data confidentiality, availability of system and applications, authentication, system integrity are threatening. Vulnerabilities can lead to message eavesdropping, injection of fake messages, denial of service attack or, poor monitoring of routing information. [38]MANETs are susceptible to both internal and external attacks.

4.2.1 Internal attacks

Nodes as well as the network interface links that simplify seamless transformation are the target if internal attack. The prime target is the routing tables that are the core of direct node communication. Detecting attacks for each node containing a routing table is very tough. Once the corrupted routing table information is transmitted to other routing tables it becomes very difficult to find the culprit and isolation.

Confidentiality is the protection of any information from being exposed. In an ad-hoc network, this is more difficult to achieve because intermediates nodes receive the packets for other recipients.

The Internal attack also known as insider attacks is more dangerous than the external attacks because the compromised or malicious nodes are originally the legitimate users of the Ad hoc network. They can easily pass the authentication and get protection from the security mechanisms. As a result, the adversaries can make use of them to gain normal access to the services.

Packet dropping, node isolation, route disruption, etc. are some internal attack criteria that can be launched against an Ad-hoc network. [39] [40]

4.2.2 External attacks

External attacks target the performance of the network. These include network congestions, denial of service(DoS) attacks and, corrupt routing information. Examples can be given over an external attack.

This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service.

Authentication assures that an entity of concern or the origin of communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.

Integrity guarantee of messages when they are transmitting shows the identity of the messages. Integrity can be compromised through malicious and accidental altering. If the message is lost the malicious node can alter the message and attempt to drop messages, replay and, revise by advertising as an authentic node. It can even change the content that can cause a transmission failure or hardware error like hard disk failure.

It is just like normal other attacks that are launched in network protocol to get encrypted information and disturbing nodes for providing transmission. [40]

4.3 Security attacks

Security attacks that can be launched against mobile ad hoc networks are generally divided into two classes: passive and active attacks.

Even though attacks can be propelled at various layers of the protocol stack, we examine mostly the attacks that can be propelled at the network layer.

The attacker does not disturb the routing protocol during performing passive attacks. On the other hand, during an active attack, the attacking node has to invest some of its energy to launch this attack. In active-attacks, malicious nodes can disturb the correct functionality of the routing protocol by modifying routing information, by redirecting network traffic or launching denial-of-service attacks (DoS). This is done by altering control message fields or by forwarding routing messages with falsified values.

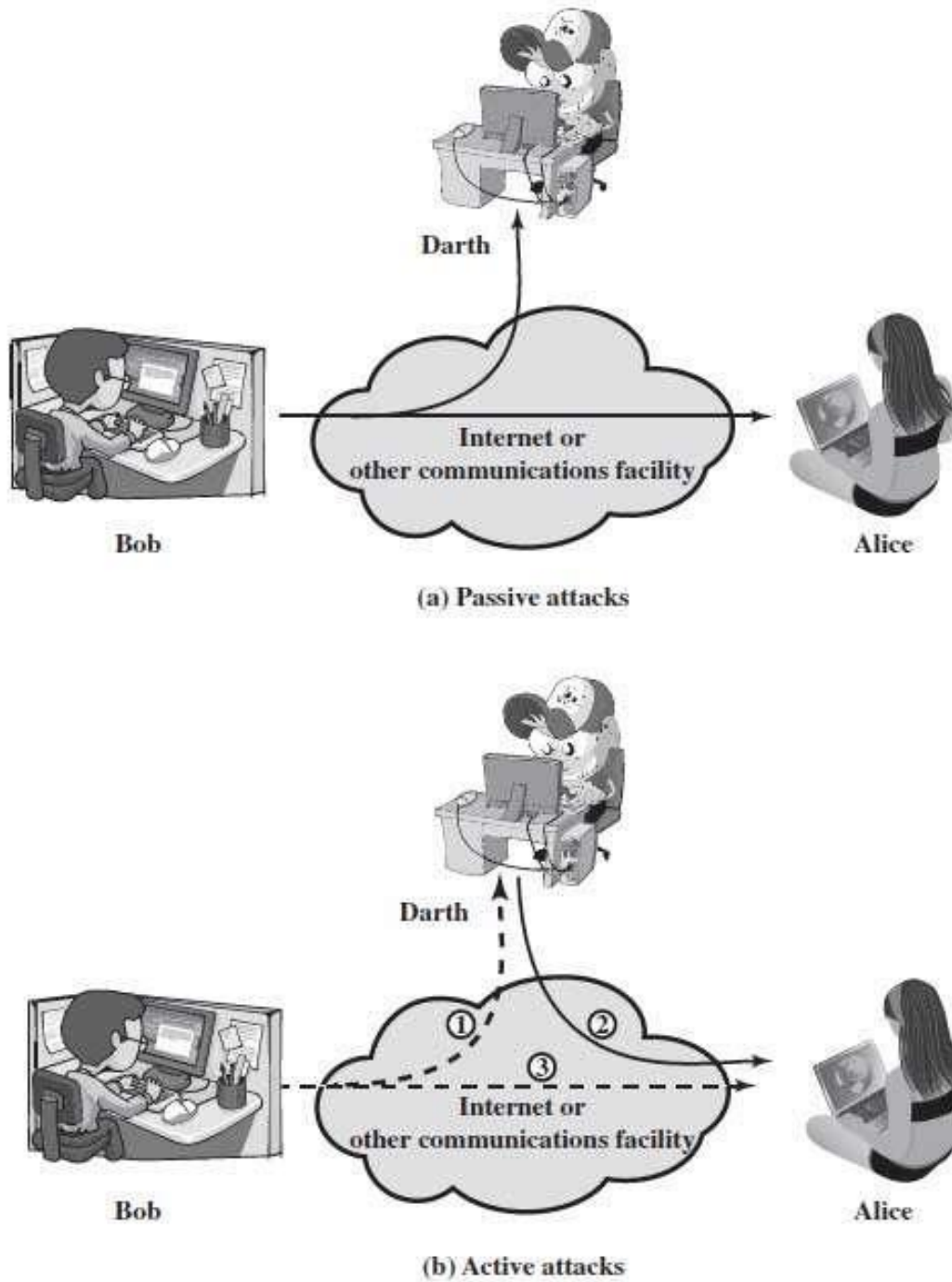


Fig 4.1: a) passive attack(Darth pretends to be Alice), b) active attack(Darth observes the messages transmitted between Bob and Alice)

In an active attack involves some modification of data transmission or creation of a false stream. A masquerade takes place when one entity pretends to be a different entity (path 2 of Figure 4.2b is active).

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (paths 1 and 2 active).

Passive attacks (Figure 4.2a) are like eavesdropping on, or monitoring of, transmissions. The common technique for masking content is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place. Here Darth is determining the location of Bob and getting information.

4.3.1 Passive Attack:

A malicious node in MANET executes a passive attack, without actively initiating malicious actions. In traffic analysis, the malevolent node endeavors to take in significant data from the system by observing and tuning in on the communication between nodes inside the MANET.

For example, if the malicious node sees that the connection with a specific node is mentioned more often as possible than to different nodes, the passive attacker would have the option to perceive that this node is significant for special functions inside the MANET, for instance, routing. The attacker may then change its job from passive to active, and endeavor to dispatch a functioning attack to put the vital node out of activity. It could do as such, for instance, by performing a DoS attack, to collapse parts of or even the total MANET. Then again, it might give the data to an accomplice, which dispatches the attack. [40]

At other times, a passive attacker might attempt to eavesdrop on traffic between nodes communicating in a MANET to extract information. For instance, the enemy could try to launch such an attack to spy on secret information flowing in a MANET deployed on a battlefield.

4.3.2 Active attack

Due to the lack of infrastructure and the vulnerability of wireless links, the current routing protocols for MANETs allow the launching of different types of attacks. Contrasted and passive attacks, malicious nodes running a functioning attack can effectively take part to disrupt the typical activity of network service. It intrudes on the precise execution of the routing protocol by altering routing information, by

creating fabricated routing data, or by imitating different nodes. Active security attacks against ad hoc routing protocols can be classified into different groups. [41] [42] [43]

- a. Attacks by dropping packets
- b. Attacks using a modification of protocol messages field
- c. Attacks using impersonation
- d. Attacks using fabrication
- e. Wormhole attacks

4.3.2.a Attacks by dropping packets

In this kind of attack, an attacker attempt to drop packets either selectively or completely to get successful in disrupting the operation of the network. With the pattern of the packet that has been dropped by the attacker, this attack can be classified into two types.

- **Black Hole:** At the start, the attacker drops all types of packet both like control or data. The malicious node analyzes the routing protocol performing passive attacks like eavesdropping information on the network traffic. Subsequently, during the route discovery phase of a routing protocol, this node lies and announces itself as knowing an accurate path to the requested target node, to be able to intercept packets. When transferring the packets is done he discards all of them.
- **Gray Hole:** Unlike a black hole process, the attacker drops packet selectively. This time the malicious node can switch its action from forwarding routing table or discarding others. The packet dropping behavior depends on the intention of the attack. The node in the established routing topology drops packet selectively to disrupt network which is difficult to detect. Depending on the drop rate and dropped data, detecting this type of attack is challenging.

4.3.2.b Attacks using a modification of protocol message

Routing protocol packets carry important control information that governs the behavior of data transmission in ad hoc networks. Malicious nodes can directly participate in routing discovery and filter routing protocol packets to disrupt communication by simply altering the fields.

The attack can be classified as remote redirection attacks and denial-of-service attacks.

- **Remote redirection with modified sequence numbers:** Protocols such as AODV instantiate and maintain routes by assigning monotonically increasing sequence numbers to routes toward a

specific destination. By advertising a route to a node with a destination sequence number any node can divert traffic through itself. The sequence number is greater than the authentic sequence number. This is how a malicious node modifies the routing protocol message advertising itself as the shortest route in remote redirection attacks.

- Remote redirection modified hop count: The route distance is described with hop count in AODV protocol. A malicious node can divert all the traffic to a particular destination by advertising the shortest route. Once it is inserted between two communicating nodes, it becomes able to do anything with the passing packet between them. It can choose to drop a packet on the route to perform as the first step of man-in-the-middle.
- Denial-of-service: Routing protocols such as DSR explicitly state routes in data packets referred to as the source route. In the absence of any integrity checks on this source route, a malicious node can modify this source route and thereby succeed in creating loops in the network or launching a simple denial-of-service attack.

4.3.2.c Attacks using impersonation

This type of attack is launched performing masquerading node to another node. The attacker misrepresents its identity by changing the IP or MAC address to that of some belonging node and masquerading as the node which refers to spoofing. Doing this attacker gets a chance to operate as a trustworthy node and can advertise incorrect routing information to the participants within the network. The creation of loops in the routing computation is one famous example of this exploit and results in unreachable nodes or a partitioned network.

Another variant of the spoofing attack is the Sybil attack. In this, malicious nodes may not only impersonate one node but can even represent multiple identities by maintaining false identities. The malicious node generates fake recommendations about the trustworthiness of a particular node to attract more network traffic to it. This offers the attacker an ideal starting point for subsequent attacks.

4.3.2.d Attacks using fabrication

Such type of attacks can be broadly classified into the following three types:

- Falsifying routing error message: When any individual move or fail both AODV and DSR need to measure the broken nodes. If the destination node or any intermediate node moves or fails then the immediate previous node of the failed node broadcast an error message to other nodes that of broken link node. After getting these information nodes then invalid the route

the destination. The attacker can easily broadcast an error message with the malicious node against the benign node.

- **Route cache poisoning in DSR:** Without being a constituent, a node can get the routing information by overhearing transmissions on routing in DSR. The node adds this routing information to its' Own cache. Using this method an attacker can gather routing information and poison route cache. If a malicious node wants to launch a denial-of-service attack on another node, it would simply broadcast spoofed packets with source routes to that node via itself. Any neighboring nodes that overhear the packet transmission may add the route to their route cache.
- **Routing table overflow attack:** A malicious node may endeavor to overpower the protocol by starting route discovery to nonexistent nodes. The basis behind this attack is to make such a large number of nodes that no further nodes could be made as the routing tables of nodes overflowing. Proactive routing algorithms endeavor to find routing information even before they are required, while receptive algorithms make just when they are required. This makes proactive algorithms more vulnerable to table overflow attacks.

4.3.2.e WarmHoleattacks

In wormhole attacks, the attacker receives packets at one point in the network and tunnels them to another part of the network and replays them into the network from that point onward. In the case of reactive protocols like DSR and AODV, this attack could be launched by tunneling every REQUEST to the target destination node directly. When the destination's neighboring nodes hear this REQUEST packet, they follow normal protocol operation to rebroadcast that REQUEST packet and then discard any other REQUESTS for the same route discovery. Thus, this prevents the discovery of any routes other than those through the wormhole. This puts the attacker in a position where any attack can be launched on the network as it. Practically routes all the discovers after a warm hole. [44]

Chapter 5

SECURITY FOR 4G AND 5G CELLULAR NETWORK

The fifth-generation mobile networks (5G) will soon supersede 4G in most countries of the world. The next generation of a cellular network is organized based on new advantages and security solutions. Compared to a 4G network system, 5G is characterized by a higher bit rate with more than 10GBps with more capacity and very low latency.

In a 5G environment, the blend of different wireless technologies and service providers that share an IP-based core network will offer the possibility to the mobile devices of switching between providers and technologies, for maintaining a high level of Quality of Service (QoS). Maintaining a high level of QoS in terms of delay, when a huge volume of data is transferred inside a 5G network while keeping at the same time high security and privacy level, is critical to prevent malicious files from penetrating the system and propagating fast among mobile devices.

Comparing 4G and 5G

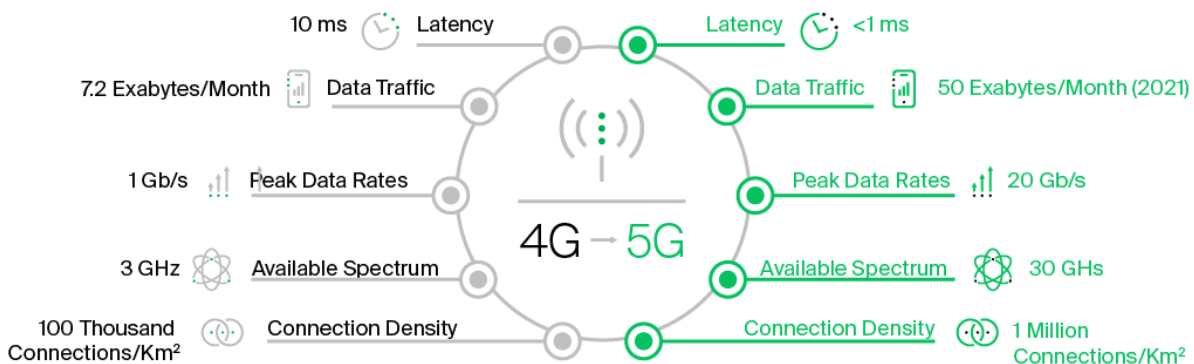


Fig 5.1: comparison of 4G and 5G in terms of characteristics

Firstly, only proposed authentication and privacy-preserving schemes for 4G and 5G cellular networks were collected. Secondly, each collected source was evaluated against the following criteria: 1) reputation, 2) relevance, 3) originality, 4) date of publication (between 2005 and 2017), and 5) most influential papers in the field. The final pool of papers consists of the most important papers in the field of 4G and 5G cellular networks that focus on authentication and privacy-preserving as their objective.

5.1 Existing cellular network issues and 5G

A quick look into recent wireless network statistics reveals that global mobile traffic experienced around 70% growth in 2014. Only 26% of smartphones (of the total global mobile devices) are responsible for 88% of total mobile data traffic. Cisco's Visual Networking Index (VNI) forecasts that mobile networks will have more than half of connected devices like smart devices by 2019. Increasing smartphone usage is resulting in an exponential growth in mobile video (multimedia) traffic. In fact, since 2012 video traffic is more than half of the global mobile traffic. An average mobile user is expected to download around 1 terabyte of data annually by 2020. Moreover, researchers are exploring new applications in directions of augmented reality, Internet of Things (IoT), Internet of Vehicles (IoV), Device to Device (D2D) communications, e-healthcare, Machine to Machine (M2M) communications and Financial Technology (FinTech). Supporting this enormous and rapid increase in data usage and connectivity is an extremely daunting task in present 4G LTE cellular systems [45]. For example, with a theoretical 150 Mbps maximum downlink data rate, traditional LTE systems, with 2×2 MIMO can support only up to (150/4) simultaneous full HD (@ 4 Mbps rate) video streaming. Furthermore, while standard LTE networks were originally designed to support up to 600 RCC-connected users per cell M2M communications and IoT require supporting tens of thousands of connected devices in a single cell. LTE cellular network is exploring avenues of different research and development, like, MIMO, small cells, Coordinated Multi-Point (CoMP) transmission, HetNets and, multiple antennas to enhance capacity and data rates. However, it is unlikely to sustain this ongoing traffic explosion in the long run. Hence, the primary concern is to satisfy the exponential rise in user and traffic capacity in mobile broadband communications. [46]

Capacity for wireless communication depends on spectral efficiency and bandwidth. It is also related to cell size. The key essence of next-generation 5G wireless networks lies in exploring this unused, high-frequency mm-wave band, ranging from 3 ~ 300 GHz. The availability of a big chunk of mm-wave spectrum is opening up a new horizon for spectrum constrained future wireless communications. [45]

5.2 Threat models and classification

In this section, we will be discussing threat models in a cellular network system in 4G and 5G. Thirty – five attacks were found analyzing the authentication and prevention schemes for 4G and 5G networks. Based on the behavior of the attacks in 4G and 5G, in a cellular system attacks can be classified into four categories. [47] They are-

- Attacks against privacy

- Attacks against integrity
- Attacks against availability
- Attacks against authentication

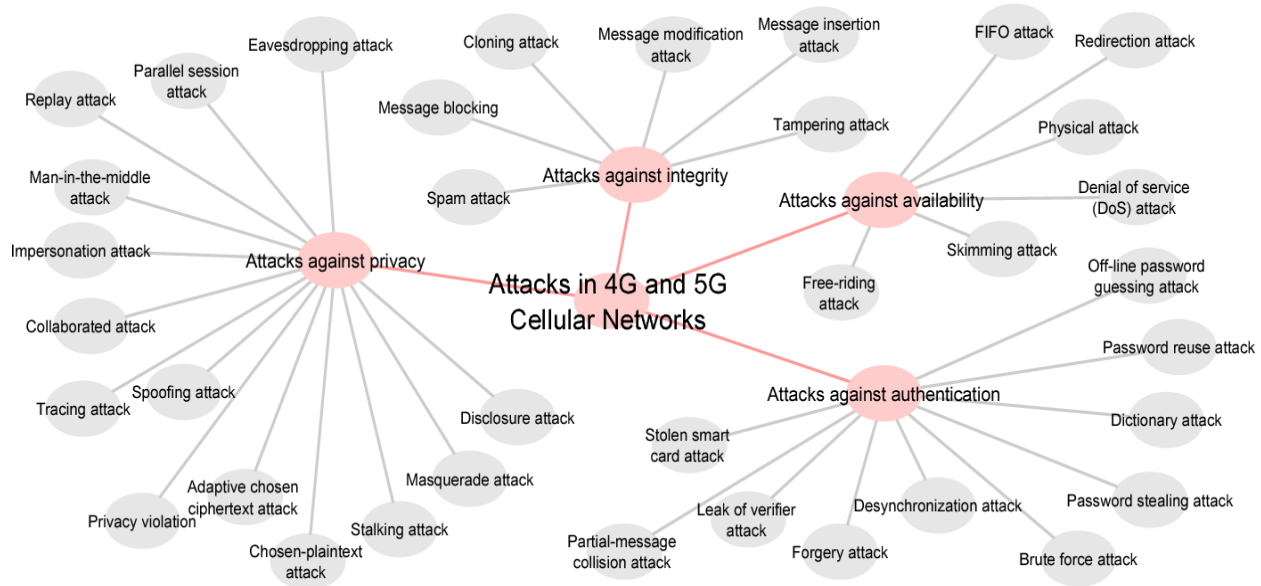


Fig 5.2: Classification of attacks in 4G and 5G cellular network

5.2.1 Attacks against privacy

It consists of eavesdropping attack, parallel session attack, replay attack, Man-In-The-Middle (MITM) attack, impersonation attack, collaborated attack, tracing attack, spoofing attack, privacy violation, adaptive chosen ciphertext attack, chosen-plaintext attack, stalking attack, masquerade attack, and disclosure attack. The most serious attack among them is the MITM attack. When a malicious third party masquerades its Base Transceiver Station (BTS) as a real network's BTS, MITM attack occurs. It is a base station based attack. [46]

Mayrhofer proposed a unified cryptographic authentication protocol framework to use with arbitrary auxiliary channels to detect the MITM attack in cellular networks. Based on the combination of learning parity with noise, circulant matrix, and multivariate quadratic, Lichman in 2016, introduced an entity authentication model that proved the security against all probabilistic polynomial adversaries under a MITM attack. The idea of checking the timestamp to detect the MITM attack is not sufficient, but it is necessary to use the private keys that are not known to the attackers. Yao proposed a group based secure authentication scheme, named, GBS-AKA, which can detect the MITM attack using the session keys.

Through the MITM attack, the attacker can launch the other attacks of this category such as eavesdropping attacks to intercept keys and messages by unintended receivers.

5.2.2 Attacks against the integrity

It includes spam attack, message blocking, cloning attack, message modification attack, message insertion attack, and tampering attack. An attack on integrity mainly based on the modification of data exchanging between mobile users. The hash function of assuring the integrity of transmitted data is used in 4G and 5G cellular network systems. The SHA-1 and MD5 algorithms are used in the hash function. It can easily detect an attack against integrity with hash function by observing wrong hash keys.

5.2.3 Attacks against availability

It includes First In First Out (FIFO) attack, redirection attack, physical attack, skimming attack, and freeriding attack. The main objective of such attacks is to make a service unavailable. By gathering entering time and exiting time intervals, the FIFO attack can be launched by a strong adversary. In the 4G and 5G cellular networks, the redirection attack is easily possible when an adversary gets the correct user entity information by increasing its signal strength to redirect or by impersonating abase station. Using a MAC to maintain the integrity of tracking area identity, to protect the network from a redirection attack is an idea introduced by Saxena and Lichman. The free-riding attack can cause a serious threat and reduces the system availability of D2D communication in the 4G and 5Gcellular networks. Keeping a record of the current status of the user equipment and realize reception non-repudiation by key hint transmission can detect the free-riding attack.

5.2.4 Attacks against authentication

It is consists of a password reuse attack, password stealing attack, dictionary attack, brute force attack, desynchronization attack, forgery attack, leak of verifier attack,partial-message collision attack, and stolen smart card attack. The goal of an attack against authentication is to disrupt the client-to-server authentication and server-to-client authentication. The password reuse attack and password stealing attack disrupt the password-based authentication schemes, which the attacker pretends to be legitimate user and attempts to login on to the server by guessing different words as a password from a dictionary. The stolen smart card attack and off-line guessing attack disrupt the smart-card-based remote user password authentication schemes, which if a user's smartcard is stolen, the attacker can extract the stored information without knowing any passwords.

5.3 Countermeasures

The countermeasures used by the authentication and security preserving schemes for 4G and 5G cellular networks can be classified into three categories.

- Cryptography method
- Human Factors
- Intrusion detection method

Classification can be shown with a diagram.

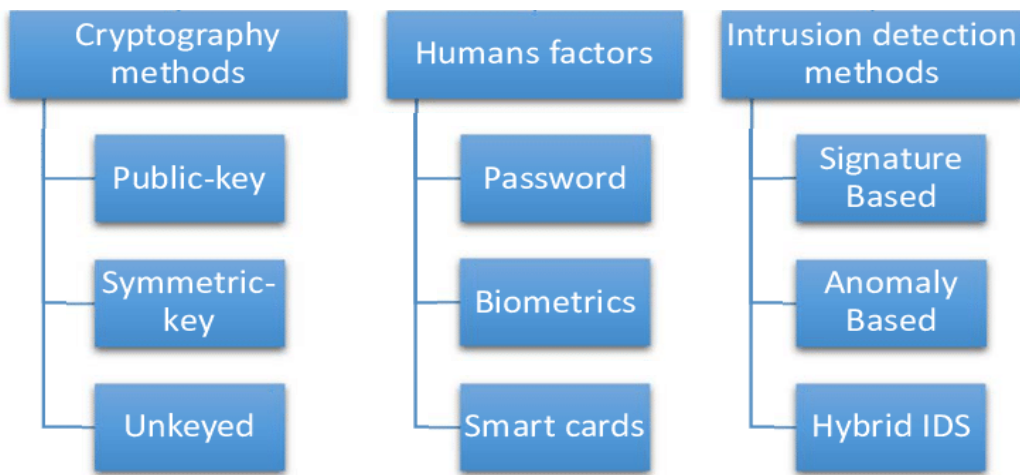


Fig 5.3: Classification of countermeasures used in authentication and privacy-preserving scheme in 4G and 5G

5.3.1 Cryptography method

It is the most used method used in authentication and privacy-preserving scheme in 4G and 5G cellular system. This method can be classified into three categories including public-key cryptography, symmetric-key cryptography, and unkeyed cryptography.

This key method used public-key infrastructure to identify the genuine access point (AP) or Base station (BS) and this Pailier cryptosystem based on three algorithms that are the generation of keys, encryption, and decryption. The generation of keys is based on two large, independent, and random prime numbers: p and q . Let m be a message to be encrypted. So the encryption algorithm stands as $= (1 + N)^m \cdot r^N \text{ mod } N^2$ where $0 \leq m < N$, r is a random integer $0 < r < N$, and the public key $N = p \cdot q$. To find the clear text m , the decryption algorithm stands as $m = \frac{(c \cdot r^{-N \text{ mod } N^2}) - 1}{N}$ [46]. The scheme uses both

Blind signature and Rabin's public-key cryptosystem. The Blind signature requires a signer and a signature requester. The content of a message is disguised in it. Rabin's public key cryptosystem is characterized by its asymmetric computational cost and requires a large amount of computation effort.

Symmetric encryption is used to provide user anonymity. Advanced encryption standard (AES) is used as the symmetric encryption algorithm for mobile devices. As symmetric encryption is faster than asymmetric encryption, the symmetric-key cryptosystem for IoT-enabled LTE networks can improve a privacy-preserving authentication scheme. Using symmetric-key techniques to achieve user anonymity is intrinsically infeasible. Hash functions are used almost in all the authentication and privacy-preserving schemes to provide data integrity for the encrypted messages. The scheme uses three popular methods that are the Message Authentication Code (MAC), the Keyed-Hash Message Authentication Code (HMAC), and the Aggregate Message Authentication Codes (AMAC).

5.3.2 Human Factors

The goal of this method is to ensure authentication. The research community has proposed three factors, 1) what you know (e.g., passwords, personal identification number (PIN)), 2) what you have (e.g., token, smart cards, passcodes, RFID), and 3) who are you (e.g., biometrics like fingerprints and iris scan, signature or voice). The methods based on what you know (e.g., passwords) might be divulged or forgotten, and the methods based on what you have (e.g., smart cards) might be shared, lost, or stolen. In contrast, the methods based on who are you (e.g., fingerprints or iris scans) have no such drawbacks. These three factors can be used together or alone.

5.3.3 Intrusion detection method

An Intrusion detection system(IDS) is the second stage of defense. When an intruder has already managed to bypass all existing countermeasures and has already taken control of a legal entity of the network, an IDS must spot misbehavior fast enough to be efficient. Lots of new methods have been introduced in the last few years to detect intruders in 4G and 5G cellular systems. Based on the observation that network traffic variables are non-stationary and exhibit 24 h periodicity, the proposed anomaly detection approach based on Bayesian Robust Principal Component Analysis (BRPCA) represents network traffic as a sequence of traffic variable vectors. The method was evaluated against two synthetic datasets that represent a DOS and femtocell-based attack respectively [20]. A novel hybrid NIDS based Dempster-Shafer theory of evidence was proposed to combat such attack or a virtual jamming attack. The performance of the method, which combines a signature-based and an anomaly-based IDS, was evaluated on an experimental IEEE 802.11 network testbed. During bandwidth spoofing attack, the attacker tries to

acquire the bandwidth that is going to be assigned from the BS to the SCA, thus blocking its communication. The method is proved to be capable of detecting and removing the intruder which is executing a bandwidth spoofing attack on the SCA (small cell access) in a 5G WCN. An RNN-based (Random Neural Network) approach for detecting large scale Internet anomalies based on the analysis of captured network data was proposed.

Dealing with attacks in LTE networks, a random packet inspection scheme was introduced. The proposed scheme has an inspection rate that can be dynamically adjusted based on the perceived intrusion period of the session. This way the IDS performs a deep packet inspection, that ensures the presence of signatures or malicious codes at the same time inspecting efficiently and quickly. This method provides an effective tool for balancing induced inspection costs with detection latency in LTE core networks.

5.4 Authentication and privacy-preserving schemes for 4G and 5G

In this part, the comparison of authentication and privacy-preserving schemes for 4G and 5G will be discussed. Based on categorization the scheme can be classified into seven types.

- Handover authentication with privacy
- Mutual authentication with privacy
- RFID authentication with privacy
- Deniable authentication with privacy
- Authentication and mutual anonymity
- Authentication and key agreement with Privacy
- Three-Factor authentication and privacy

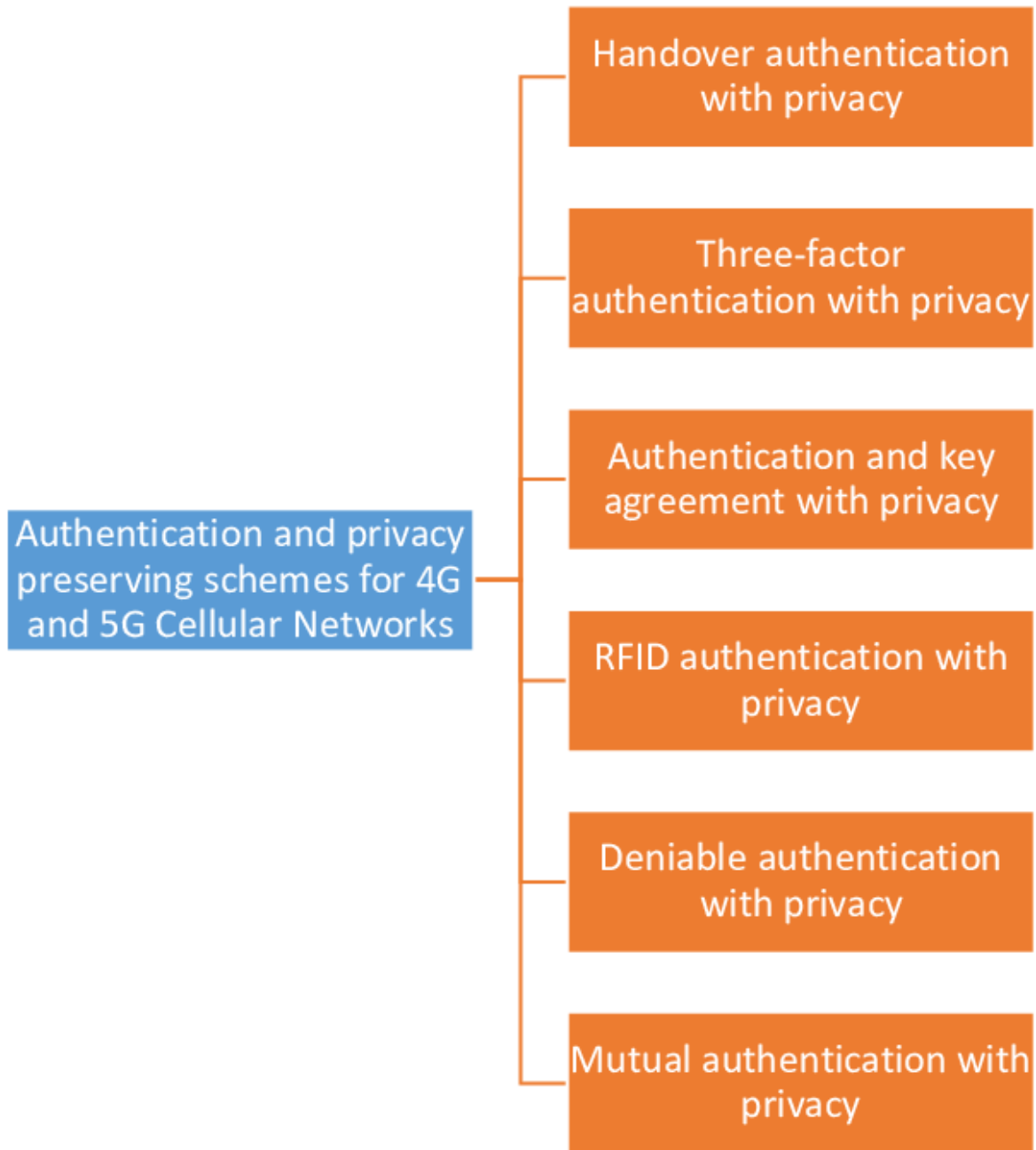


Fig 5.4: Classification of authentication and privacy-preserving schemes for 4G and 5G cellular network

5.4.1 Handover authentication with Privacy

The existing handover authentication schemes for LTE wireless networks can be classified into three classes based on the cryptographic primitives. The classes are included with i) Symmetric-key based scheme, ii) Public-key based scheme, and iii) Hybrid scheme. In LTE wireless networks, there are two types of base stations, namely, Home eNodeB (HeNB) and eNodeB (eNB). The 3GPP project suggested

handover from an eNB/HeNB to a new eNB/HeNB cannot achieve backward security in handover procedures. Specifically, a handover scheme is proposed for mobile scenarios in the LTE networks. The scheme can provide strong security guarantees including perfect forward secrecy, master key forward secrecy, and user anonymity. It is efficient in terms of computational cost, communication cost, and storage cost. But the scheme does not consider identity and location privacy.

IEEE 802.16m is proposed as an advanced air interface to meet the requirements of the fourth generation (4G) systems [47]. To preserve the identity privacy for the IEEE 802.16m network, a privacy-preserving fast handover authentication scheme based on the pseudonym was proposed. Based on the 3-way handshake procedure, the scheme achieves three objectives that are i) Fast Handover, ii) Mutual authentication and key agreement, and iii) Privacy preservation. This adds a benefit is users can improve location privacy significantly by applying the idea of pseudo-location swapping.

To provide the security key derivation and anonymity for all of the mobility scenarios in LTE-A networks, a group-based anonymity handover protocol, named NAHAP is proposed. The NAHAP protocol is efficient in terms of the signaling cost, the communication cost, and the computational cost compared with the LTE-A handover mechanism. Similar to the NAHAP scheme, another uniform group-based handover authentication protocol, named UGHA, is proposed which is efficient in terms of computational cost. Using software-defined networking, Duan and Wang proposed an authentication handover scheme with privacy protection in 5G heterogeneous network communications [48]. A novel group authentication protocol with privacy-preserving to provide unlinkability and traceability in 4G/5G communications is launched. This scheme is efficient in terms of signaling overhead and computation overhead. With all of the mobility scenarios in the LTA/LTA-A networks, a privacy-preserving with no frame ability authentication protocol, called Nframe is proposed to guarantee users' privacy, unlinkability, and traceability. The N-frame protocol uses a pseudonym-based scheme. To achieve a simple authentication process without complex key management and minimize message exchange time, the Nframe protocol uses pairing-free identity-based cryptography. The N-frame protocol is efficient in terms of computation cost and communication overhead compared to three schemes, namely, HALP scheme, Pair-Hand scheme, and UHAEN scheme, but the perfect forward and backward secrecy are not considered [48]

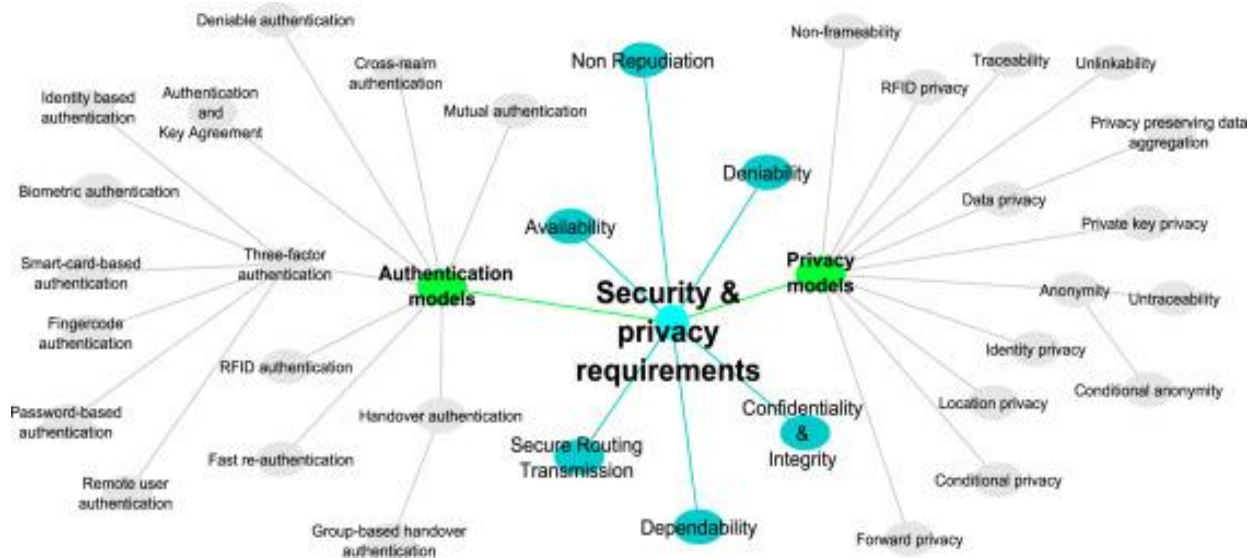


Fig 5.5: Categorization of authentication and privacy models

5.4.2 Mutual authentication with Privacy

To achieve mutual authentication with privacy, the proposed security schemes for 4G/5G networks need to preserve the Location privacy, Identity Privacy, Data Integrity, and Authenticity.

Dimitriadis and Polemi (2006) proposed a protocol, named, IDM3G, to achieving mutual authentication and identity privacy in 3G [46]The IDM3G protocol used two phases, namely, 1) the authentication of the UMTS Subscriber Identity Module (USIM) by providing a personal identification number and 2) the mutual authentication between the USIM and the mobile operator.

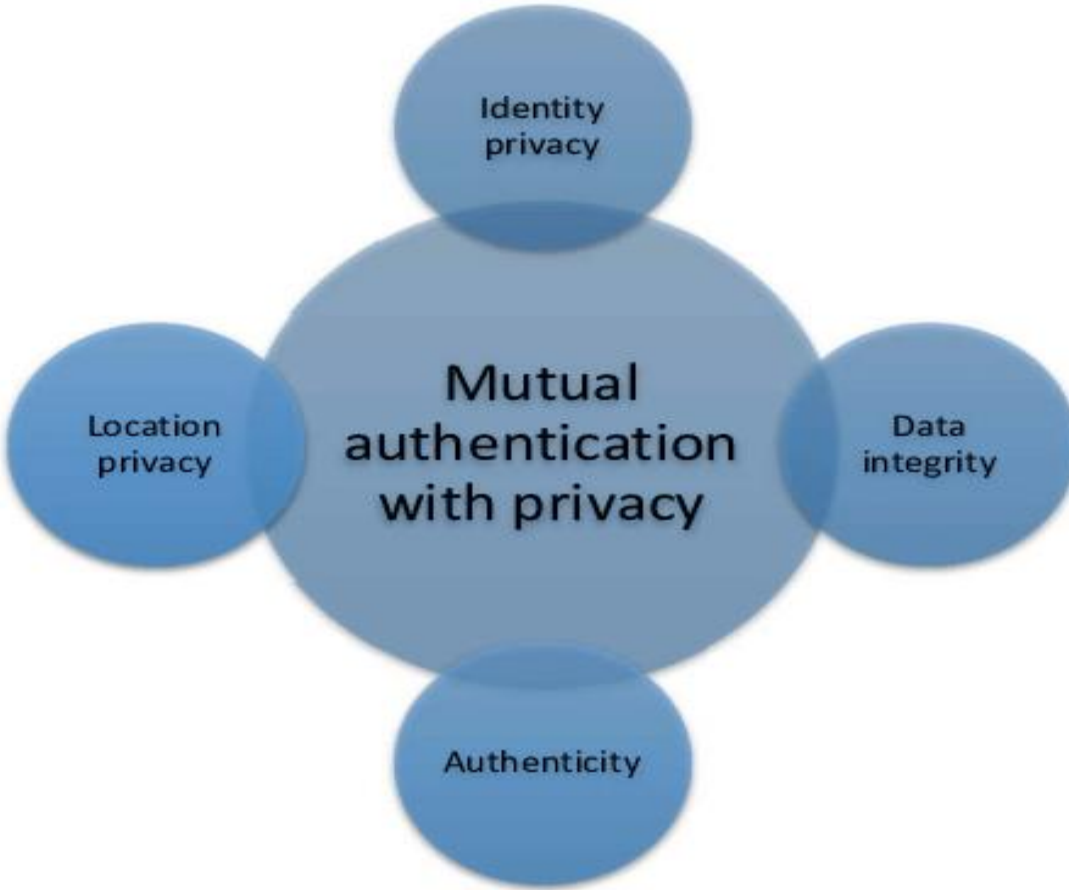


Fig 5.6: Classification of mutual authentication with privacy

By using the authentication request based on HTTP, the IDM3G 13 is efficient in terms of the number of messages exchanged in the path, which is lower compared to both protocols, but the location privacy is not considered. Similar to the IDM3G protocol, Dimitriadis and Shaikh (2007) proposed a protocol, called BIO3G, for establishing secure and privacy-friendly biometric authentication in 3G mobile environments [32]. Since BIO3G can not resist locations and Identity, they proposed a protocol with three categories for the 4G cellular network system. The main idea of the protocol is to use self-certified public-key. The advantage of the protocol is it considers identity privacy but the disadvantage is it does not consider locations secrecy. Ensuring location privacy in a cellular network is an effort to prevent any other party from learning mobile users' current and past locations. The recent schemes are planned based on the location privacy in 4G and 5G network systems.

Location privacy is one of the most important models for privacy. With the help of the Preset in Idle technique, the proposed novel mutual authentication protocol with provable link-layer location privacy protocol is efficient in terms of the packet delay time and the total packet time cost. An advanced

Identity Management scheme, called AIM, to guarantee mutual authentication, privacy, and tracking avoidance for 4G networks is proposed by Abdelkader.

For the security of future fifth-generation(5G) telecommunications, a service provider will need to apply the managed security services (MSS) as network security services. According to Ulltveit-Moe, the security services may be required for all mobile terminals such as antivirus, firewalls, Intrusion Detection Systems (IDS), integrity checking, and security profiles. Specifically, a location-aware mobile intrusion prevention system with enhanced privacy, named m-IPS, which is integrated into MSS is a must [46]. Using identification parameters, including, the International Mobile Subscriber Identity (IMSI) and the Radio Network Temporary Identities (RNTI), Jang proposed an authentication protocol to safely transmit identification parameters in different cases of the initial attach under 4G mobile communications. Recently, Mahmoud proposed a privacy-preserving power injection querying scheme over LTE cellular networks, to solve the problem of privacy exposure of storage unit owners. Therefore, the 4G/5G communications can be used by the traffic information systems. This system is based on three main phases, that are i) System initialization, ii) Device authentication and report submission, and iii) Device eviction.

5.4.3 RFID authentication with privacy

The term RFID stands for Radio Frequency Identity. An RFID system is a low cost and convenient in identifying an object without being physical contact. It consists of Radio Frequency(RF) tags or transponders, RF tag readers, or transceivers. According to Sun and Ting, RF technology can provide three functions: item awareness, information searching, and quality control. An RFID application performs three basic roles. [48]

- Tag
- Reader
- Back-end database

An RFID authentication protocol consists of five categories that are i) Generation-2 protocol, ii) CRC-based protocol, iii) Minimalist cryptography, iv) Protocol with substring Function, and v) ECC-based protocol.

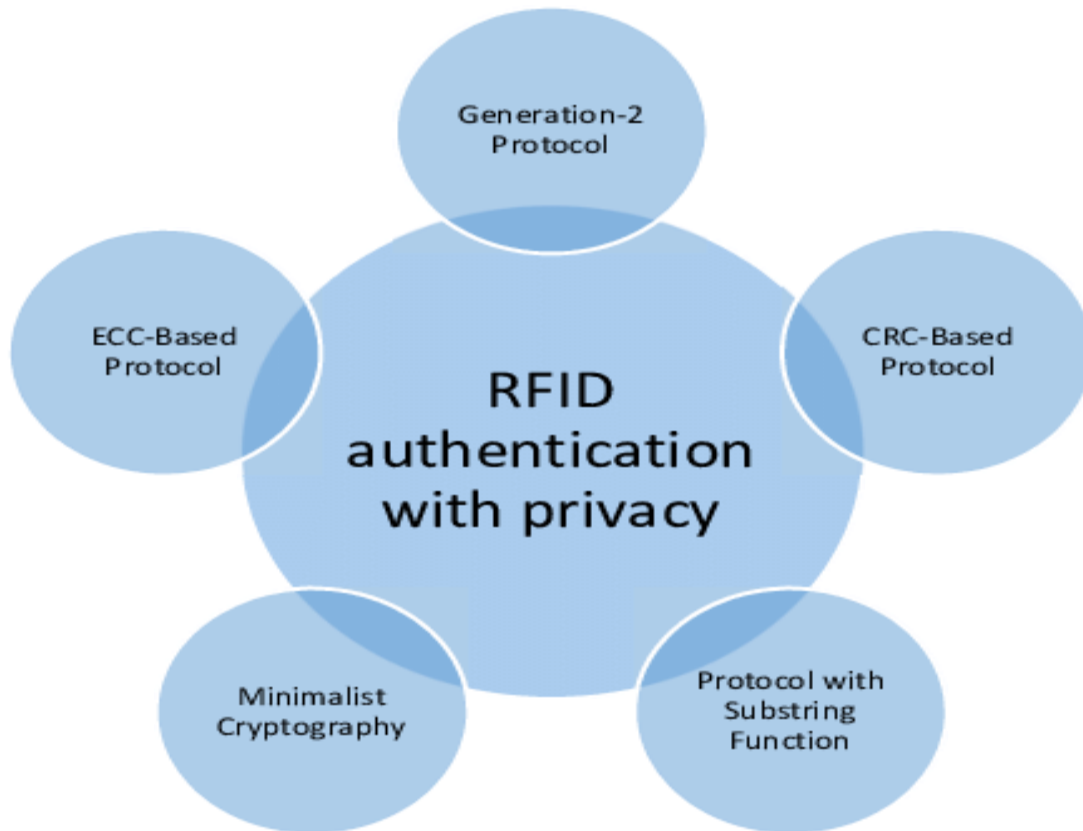


Fig 5.7: Classification of RFID authentication protocols

A message authentication scheme based on Cyclic Redundancy Check (CRC) codes for 5G Mobile Technology and an ultra-lightweight RFID authentication protocol, called SASI are proposed o providing strong authentication and integrity protection. The SASI protocol uses only simple bit-wise operations on the tag. Chien and Chen addressed the weaknesses of these schemes and proposed a mutual authentication scheme for GEN-2 RFID.

A privacy and authentication protocol for passive RFID tags, called PAP, based on four main phases included In-store, checkout, Out-store, and Return, is proposed that can resist against Replay attack but vulnerable to some attacks like desynchronization attack and tracing attack. [49]

To achieve RFID authentication with anonymity, and even availability, Chien and Laigh proposed an RFID authentication protocol based on Error Correction Codes (ECC). The protocol can achieve mutual authentication between the tags and the reader based on the successful verification of the PRNG function applied to the secret key. To detect a Man-in-the-middle attack, an authentication protocol named LCMQ is proposed that secure in a man-in-the-middle attack. Using an ultralightweight RFID mutual

authentication protocol with cache in the reader, the LRMAPC protocol can achieve mutual authentication and provide forward security.

5.4.4 Deniable authentication with Privacy

The deniable authentication differs from traditional authentication in a way that the Receiver cannot convince a third party. To provide a lower degree of scalability and security, Bersani and Tschofenig defined an experimental protocol for the Internet community, called EAP-PSK. The Extensible Authentication Protocol (EAP) is an authentication frequently used in wireless networks. According to Pereniguez, if the authentication mechanism does not have an adequate level of privacy, the identity and location can be revealed. Pereniguez proposed a privacy-enhanced fast reauthentication, named 3PFH, for EAP-based 4G of mobile communications. The main idea of 3PFH is defined by a multilayered pseudonym architecture to achieve user anonymity and un-traceability. The 3PFH is applicable when the handoff takes place between different network operators [46].

5.4.5 Authentication with mutual anonymity

Anonymity is an important security aspect of cellular communication since it protects the privacy of the users. Li Lu, Jinsong Han proposed an anonymous zero-knowledge authentication protocol, called PT, for Peer-to-peer (P2P) systems. It can apply as an authentication protocol in 4G and 5G cellular communications. Besides, the PT protocol can support trust management in anonymous environments and scalable in both static and dynamic environments. To provide integrity to data exchanges after authentication, the PT protocol uses a Diffie-Hellman Key Exchange protocol into the authentication procedure to generate a session key [48] [46].

To achieve the privacy-preserving context transfer for 4G, four privacy-preserving schemes for Context transfer protocol (CXTF) is proposed in 2011. These schemes are efficient in terms of application handoff service time compared to CXTF, while at the same time guarantee the privacy of the end-user. To verify the identity of a user or a host over a 4G network, the network authentication protocol, called Kerberos, can be used. The Kerberos protocol is proposed under IETF RFC 4120 where several entities were mentioned including, i) The client, C with its secret key, ii) The server, S with its secret key, iii) Ticket granting service, and iv) key distribution center.

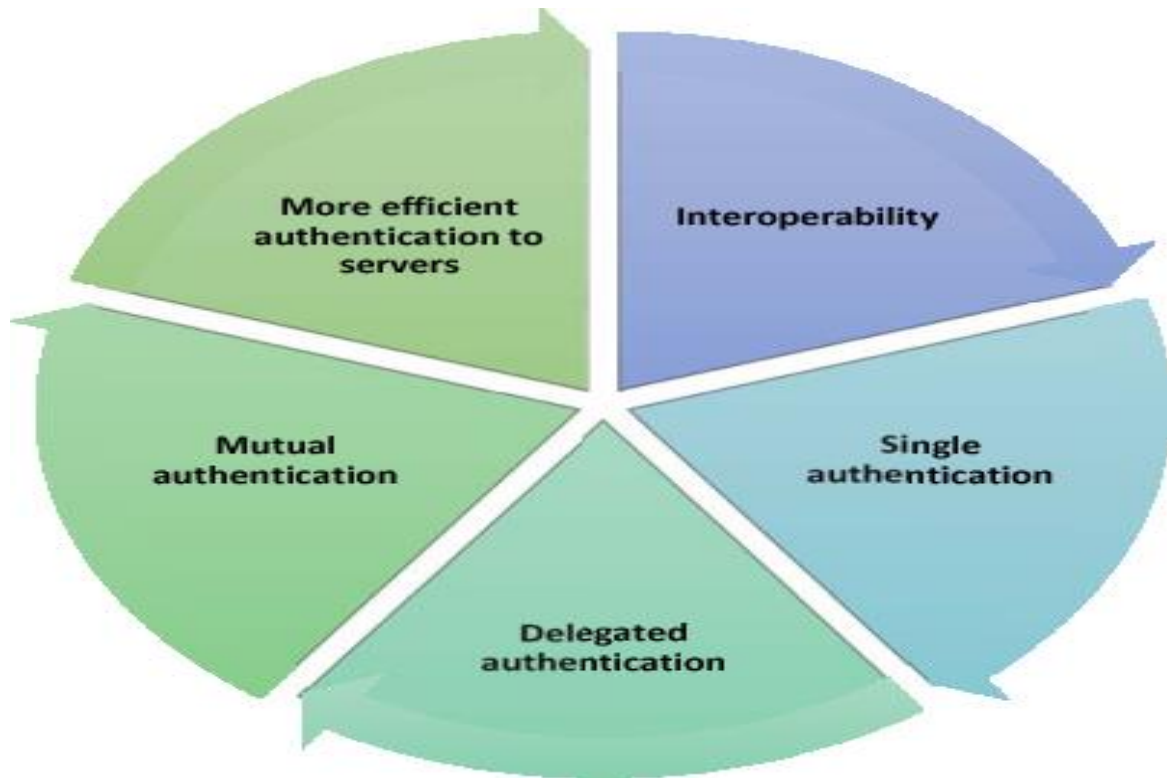


Fig 5.8: Different models offered by the Kerberos protocol

As shown in the figure Kerberos authentication protocol offers some authentication model. The name of the models are 1) More efficient authentication to servers, 2) Interoperability, 3) Single authentication, 4) Delegated authentication, and 5) Mutual authentication. The Kerberos protocol suffers from two issues; anonymity and service access un-traceability. A two-level privacy architecture, named PrivaKERB, to preserves the privacy of the user during activity with Kerberos is proposed. PrivaKERB is efficient in terms of service times, resources, and network utilization compared to the standard Kerberos protocol.

5.4.6 Authentication and key agreement with Privacy

The Authentication and Key Agreement (AKA) protocol is a challenge-response based mechanism that uses symmetric cryptography. The Universal Mobile Telecommunication System (UMTS) has adopted the AKA protocol of 3GPP, known as a standard of 3G with RFC 3310 [48]. Improved authentication and key agreement protocol based on a public-key cryptosystem are vulnerable to some attacks, such as replay attack, man-in-the-middle attack, and DoS attack. A proposed hybrid scheme based on modifications to the LTEAKA scheme, which employs both symmetric and asymmetric key encryption to detect and avoid both insider and outsider attacks. Using an efficient access-policy updating method, a group-based AKA protocol, called GR-AKA is introduced to reduce the communication overhead and alleviates the burden

between machine type communication devices, but the known-key secrecy and the perfect forward secrecy are not considered. To avoid the signal congestion in 3GPP networks a group-based authentication for machine-to-machine (M2M) is proposed which is efficient in terms of bandwidth consumption.

The AKA protocol can easily be extended to provide revocable privacy by adopting the fair blind signature technique called PPAB to achieve scalable, authentication, and billing in the context of interdomain roaming in the wireless metropolitan area sharing networks (WMSNs). The PPAB protocol considers five levels of privacy protection, namely, 1) content privacy, 2) external privacy, 3) internal privacy I, 4) internal privacy II, and 5) internal privacy III. Content privacy is hiding communication content from an external adversary. The external privacy is hiding identity information of mobile users from the external adversary. The internal privacy I hiding identity information of mobile users from the wireless Internet service providers. [48] The internal privacy II is hiding identity information of mobile users from the roaming broker. The internal privacy III is hiding identity information of mobile users from adversary for each handoff event. PPAB is efficient in terms of energy consumption compared but the deniability and completeness are not considered.

5.4.7 Three-factor authentication with privacy

The three-factor authentication schemes with privacy can mainly be classified into three categories: i) Smart cards-based protocol, ii) Passwords-based protocol, and iii) Biometricsbased protocol.

These three different data types can be used together in an authentication protocol, where smart cards show *what you have*, passwords represent *what you know*, and biometrics mean *what you are*. Based on the login and authentication phase, the server accepts only if each factor (password, smart card, and biometric data) passes the authentication. The protocol is efficient in terms of low computation for smart cards. The biometric systems can mainly be classified into three categories: 1) Traditional Biometric Systems (e.g., Windows Hello), 2) Wearable biometric systems (e.g., Using a smartphone), and 3) Hybrid biometric systems (e.g., Hybrid systems arises in telecare services).

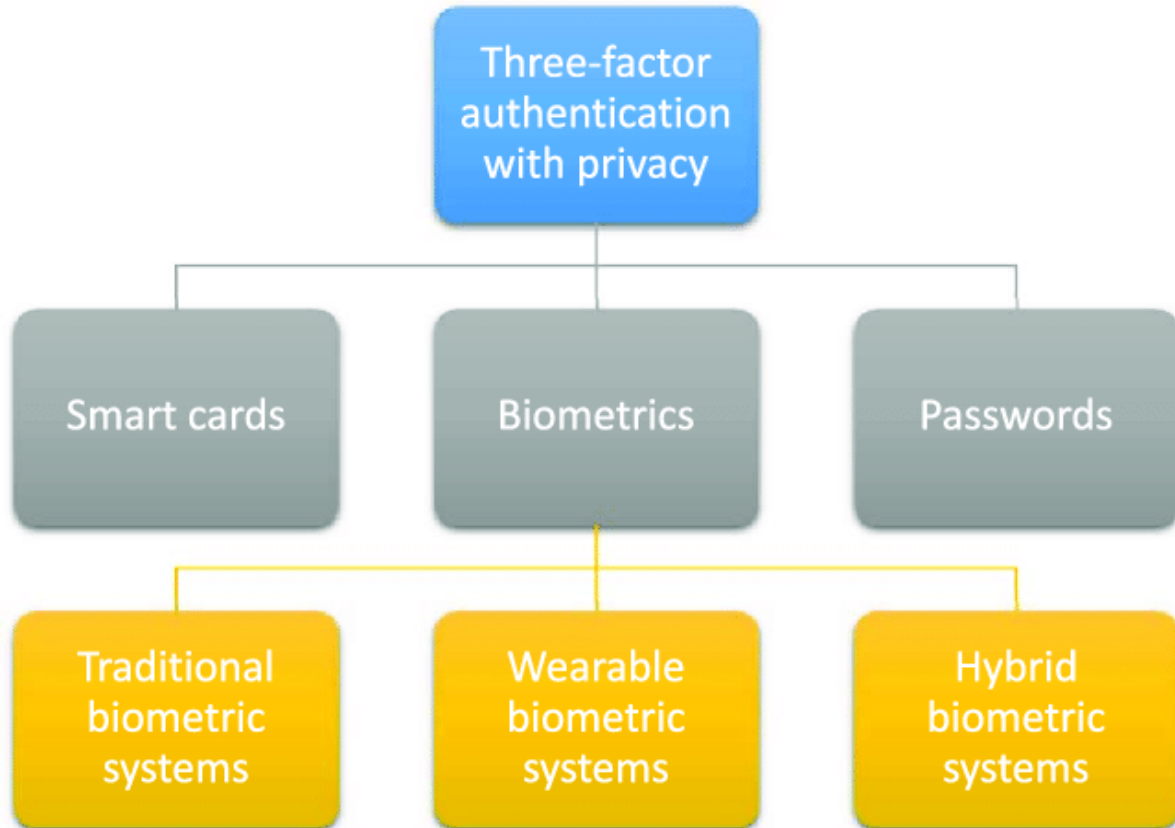


Fig 5.9: Classification of three-factor authentication schemes with privacy

For the security of 4G and 5G networks using Biometric-based identification, it is required that the client does not learn anything on the database. The fingerprint is likely to be used in applications that need higher reliability.

The password-based-authentication protocols are a reliable solution to provide identity protection and satisfy strong mutual authentication in 4G and 5G networks. Cryptanalysis of the Hsiang and Shih protocol can be presented to propose a secure dynamic identity-based authentication protocol for multi-server architecture. The protocol is efficient in terms of computation complexity compared to related smart card-based multi-server authentication protocols.

Many of them are still valid. For example, the 3GPP's approaches for 3G and 4G – which brought the industry highly secure radio and core network protocols, subscriber authentication, and more – are largely still valid. However, there must also be new considerations for 5G security design. Most notably, trust

models must be revisited, and new aspects such as potentially misbehaving entities and devices should be catered for. Greater emphasis also needs to be placed on the assurance side, and it is important to account for completely new stakeholders and the extent to which they and their businesses will be dependent on 5G security design.

Chapter 6

DATA SECURITY IN WIRELESS NETWORKS

Wireless networks are moderately less secure than wired arrange since of less demanding get to of unauthorized people in scope ranges of getting to focus. There's certainly within the usage of wireless systems, distinctive boundaries that frame the so-called fundamental security of remote networks, which prevents unintended get to of outsiders arrange within the scope of an get to point. Security boundaries (essential security) conventions have been given in Wi-Fi networks give a relatively low level of security of these systems, which has moderated improvement.

SSID (Service Set Identifiers), **WEP**(Wired Equivalent Privacy), Address validation **MAC** (Media Access Control) these are the Basic security of a wireless network by implementing these features.

"Service Set Identifier." An SSID may be a one of a kind ID that comprises of 32 characters and is utilized for naming remote systems. When different remote systems cover in a certain area, SSIDs make sure that information gets sent to the right goal

People ordinarily encounter an SSID most regularly when they are employing a gadget to put through to a wireless network. For example, if you take your Gadgets to a coffee shop and endeavor to put through to the nearby Wi-Fi network, your screen will show a list of SSIDs — this can be the names of all the networks that inside extend of your versatile gadget. You'll select the title of the nearby network you need to put through to and after that enter the password to connect. [50]

"Wired Equivalent Privacy." WEP is a security protocol for Wi-Fi networks. But it does not provide more securities. Programmers prepared with observing hardware can receive and record, to challenge absent from the access point, and after that, reply to the customer's encrypted on the premise of processing can decide the key that can at that point be utilized to connect the network.

The MAC address (short for media get to control address) is the unique hardware address of a single network connector. The physical address is utilized to recognize a device in computer networks.

6.1 How It Works

Wireless MAC Filtering is the simplest method for limiting access in a Wireless Network. Only wireless equipment, who has been previously, registered MAC address of the router or Access Point can connect to a wireless network.SSID Hiding (Wireless Broadcast SSID Disabled) is a method for limiting unauthorized access to a wireless network. Securing the network can be done with WEP or WPA.

- **WEP** (Wired Equivalent Protection) is an encryption method:
 - Using 64 bits (10 Hexa characters) or 128 bits (26 Hexa characters). Hexa characters are: 0-9 and A - F

- Authentication: Open or Shared Key Now the 64-bit WEP encryption can be cracked in minutes, and the 128 bits in a few hours, using public applications.
- **WPA-PSK** (WPA Preshared Key or WPA-Personal) is a much safer method such as WEP.
- **WPA2** network provides unique encryption keys for each wireless client that connects to it.
- Also, those encryptions (WPA and WPA2) can be broken in case the watchword contains fewer characters or a word found within the dictionary. To break this encryption makes it inconceivable to utilize long passwords, arbitrarily generated.

6.2 Analysis

We use A 54Mbps Wireless Router. This router provides a dedicated arrangement for Office/Home systems. With our network all connected, our local wired or wireless network can share Web access, records and, fun for multiple PC's through one ISP account. In expansion, this device supports Bridge mode which can make two AP's communicate with each other wirelessly. There are three submenus under the Remote menu. There are three submenus under the Wireless menu (shown in Figure): Wireless Settings, MAC Filtering and, Wireless Measurements. Tap any of them, and we should be able to configure the comparing work. The detailed explanations for each submenu are given below.



System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented.

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack.

When developing a secure network, the following need to be considered:

1. Access: authorized users are provided the means to communicate to and from a particular network.
2. Confidentiality: Information in the network remains private.
3. Authentication: Ensure the users of the network are who they say they are.
4. Integrity: Ensure the message has not been modified in transit.

5. Non-repudiation: Ensure the user does not refute that he used the network.

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack. [49]

SSID

Enter a value of up to 32 characters. The same name (SSID) must be assigned to all wireless devices in our network. The default SSID is TP-LINK, but it is recommended strongly that we change our networks' name (SSID) to a different value. This value is case-sensitive. For example, *TP-LINK* is NOT the same as *tp-link*.

Region

A region is selected from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region. If the country or region is not listed, we can contact the assistance. As the default region in the USA, when we choose our region from the pull-down list the SAVE button is to clicked.

Channel

This determines which operating frequency will be used. It is not necessary to change the wireless channel unless we notice any interference problem within other access points.

Mode

It selects the desired wireless mode and the options are;

- **54Mbps(802.11g):** Both 802.11g and 802.1b can connect to the router.
- **11Mbps(802.11b):** Only 802.11b can connect to the router.

Enable wireless router radio

The wireless radio of this Router can be enabled or disabled to allow wireless stations access. When it is enabled it can access the router otherwise it can not.

Enable SSID broadcast

If we select the Enable SSID Broadcast checkbox, the Wireless Router SSID will broadcast its name (SSID) on the air.

Enable bridges

Selecting enable bridges from checkbox we can input a MAC address of other IPs to communicate with them wirelessly.

There are six entities configured in MAC of IP. The IPs can communicate to other IPS unless knowing each others' MAC addresses.

Enable wireless security

By enabling the function encryption becomes a must for a wireless station to connect to the router. Otherwise without encryption connection is established. This is highly recommended to enable the function of encryption for the sake of security.

We can select one of the following authentication types:

- **WEP** - Select the WEP authentication type based on 802.11 authentications.
- **WPA-PSK/WPA2-PSK** - Select WPA/WPA2 authentication type based on pre-shared passphrase.
- **WPA /WPA2** - Select WPA/WPA2 authentication type based on Radius Server.

Security Options - We can select one of the following Security options:

When we select **WEP** for authentication type we can select the following authentication options: [49]

- **Automatic** - Select Shared Key or Open System authentication type automatically based on the wireless station request.
- **Shared Key** - Select 802.11 Shared Key authentication.
- **Open System** - Select 802.11 Open System authentication.

6.3 Security Challenges of WSN

The WSN faces a significant number of security challenges some of which are mentioned below:-

(a) **Wireless Medium.** The passive attacks like eavesdropping are quite simple to launch because WSN uses a wireless medium for communication purposes which is inherently less secure. The adversary can very easily intercept, alter, or replay the transmission when desired.

(b) **Ad-Hoc Deployment.** The Ad-Hoc communication environment of WSN demands the security solution to facilitate the uninterrupted operation of sensor nodes in case of a node failure, addition, or mobility. The security solutions must have the potential to support self-configuration in case a node fails or is replaced by some adversary.

(c) **Hostile Environment.** The sensor nodes of WSN are most likely to be deployed in an unattended and hostile environment that creates a possibility that an attacker or adversary can get physical access to these devices. These nodes can be physically captured by an adversary for retrieving important security parameters like cryptographic keys by an attacker [5].

(d) **Resource Scarcity.** As the nodes of WSN can be deployed in remote and hostile environments without further attendance, the importance of energy conservation and hardware resource utilization increases manifold. The security solution for WSN must be efficient in terms of bandwidth consumption, computational capability, memory utilization, and energy consumed for secure communication protocol (transmission and reception) to achieve these WSN targets.

(e) **Immense Scale Deployment.** Scalability is a major requirement of WSN and nodes number can range from a few dozens to thousands. However, where scalability can be a major requirement the security model for such a huge network has to be designed thoughtfully, such that with scalability the WSN can achieve high computation and communication efficiency.

6.4 Security in Wireless Sensor Networks (WSN)

- The security design of WSN needs to be robust and effective for which it has to cover WSN security goals, security threats, and security classes.
- (a) **Security Threat.** An event that has the potential to adversely affect the systems' performance by under security breach is known as a security threat.
- (b) **Security Threat Classification.** The attacks on WSN can be largely classified as interception, interruption, modification, and fabrication.
- **Interception.** A type of attack that can harm the confidentiality by attempting to have unauthorized access of the sensor node and its stored data/keys.
- **Interruption** A type of attack that prevents legitimate communication between the communicating parties. Interruption can harm the availability of the network, by corrupting messages, injection of malicious code or physically capturing of nodes, etc.
- **Modification** A type of attack that harms the integrity of the network. In this attack, the adversary not only attempts to have access to the data but also attempts to tamper it, for example, the adversary can alter the contents of the data that is in transition.

- **Fabrication** harms the authentication of the data that is being transmitted as the adversary injects the false data packets into the network.

6.5 Security Goals

There are two categorized goals to perform. i) primary goals ii) secondary goals.

6.5.1 Primary Goals

Data Confidentiality

Data Confidentiality refers to the concealment of messages in transition so that the messages communicated or transmitted via sensor nodes and networks remain aloof or confidential from the passive attacker. It is more difficult to maintain data confidentiality in a wireless network than a wired network. Since WSN neighboring nodes of a transmitting node also listen to the communication it can easily accomplish eavesdropping on the information being routed.

- **Data Integrity** Data Integrity refers to the message being transmitted to remain unaltered. Data Integrity in a sensor network is critical because the messages from the source node to the destination node must pass through intermediate nodes. The attacks on the integrity of the network are further categorized as follows:-
- **Non-Repudiation** refers to a condition in which both sending and receiving parties must not deny that they have not sent/received the data message/control message. The WSNs are the most vulnerable networks to these types of attacks because they lack the centralized controlling infrastructure.
- **Modifications.** After intercepting or accessing information, the attacker modifies the information to make it beneficial to itself.
- **Masquerading.** Masquerading or spoofing happens when the attacker impersonates somebody else.
- **Replaying.** In this attack, the attacker acquires a copy or duplicate of the message transmitted by the node and afterward tries to replay that message.

Data Authentication

Data Authentication relates to the identification of the sending origin of the received message and also its reliability. The Wireless Sensor Networks involve both modifications of packets attack and insertion of additional or false packets attack.

Node or Network Availability

Node Availability means that whether the node has the can operate its assets and/or the accessibility of a network is ensured for the communicating nodes. There should be an assurance of the availability of the node/network under any critical situation like DoS attacks.

6.5.2 Secondary Goals

Data Freshness

The freshness of each data packet needs to be ensured even the confidentiality and integrity of data has been assured. Informally speaking, data freshness depicts that the data is latest, as well as data freshness, must ensure that no previous messages will be replayed.

Route Freshness

Even if we ensure the data freshness there is still a need to ensure freshness of the network route. As we know that the nodes of WSNs are inherently facing resource scarcity in terms of limited processing, storage, and energy capacities, an attacker could impersonate nodes and restrict them to update their routing tables.

Self-Organization

A WSN is a typical form of an ad-hoc network that has no fixed or centralized infrastructure that exists for the reason for network management. This inherent constraint in the network architecture of WSN poses an immense challenge to its security aspect.

Time Synchronization

The wireless sensor network is a distributed system, and in such distributed systems each node has its clock and own time domain. However, a common scale among sensor nodes is important to identify a

causal relationship between events in the physical world and to support the elimination of redundant sensor data.

Secure Localization

Localization is the task of determining the physical coordinates of sensor nodes (or a group of sensor nodes) or spatial relationships among objects. The utility of a wireless sensor network depends on the ability of its sensor nodes to accurately, precisely, and automatically determine/trace the current location of the intended sensor nodes to which it wants to communicate.

Power Management

The power consumption of a WSN is of key concern due to the inherent energy constraints of sensor nodes as they are generally operated with batteries and it may be impractical to change the depleted batteries in the deployed area. It is pertinent to mention here that those attacks launched to exhaust the power of the nodes' batteries can adversely affect the performance of the entire setup if the attacker launches this attack on the "critical node".

During the past few years, a substantial amount of work has been done in the WSN security domain as security has become a key focus for energy-constrained WSN due to diverse critical security applications [5]. Keeping in view this fact, the key objective of our work is to encompass several security facets of WSN that help in analyzing the nature and complexities of WSN security-attacks.

Chapter 7

Conclusion

Wireless networks continue to develop in many market sectors, such as telecommunications, industrial applications, M2 M (machine-to-machine), and home automation, despite the essential security issues. In this paper, we have analyzed the security threats and the security objectives that need to be achieved. Most security strategies fail because the solution has to handle so many types of potential customers. Ad hoc network security-sensitive procedures involve a high degree of safety; ad hoc networks, on the other hand, are inherently vulnerable to security attacks. Consequently, safety mechanisms are essential for ad hoc networks. Stable routing and setting up of a secure key management service in an around ad hoc networking, These two issues are essential if our safety goals are to be achieved. Also in this study, we surveyed privacy schemes for cellular 4 G and 5 G networks and state-of-the-art authentication. We were able to identify the vulnerability models in cellular networks into attacks on privacy, attacks on integrity, attacks on availability, and attacks on authentication through thorough study and analysis that was carried out as well as we've been able to describe security measures into methods of cryptography, human factors and methods of intrusion detection. We have to realize, that there can be no single security solution to all. This is due to the very different threat accumulation in a given setting around a given asset, but primarily due to the growing sophistication of ISs. Additionally, the advancement of new technologies and devices introduces new vulnerabilities, whose magnitude can not be determined in advance because it depends on the size of deployment among other factors. Safety remains a mechanism that has to go hand in hand with designing an information system. Security concerns are likely to worsen in the future as the world becomes more globalized and more communicative. Privacy protection is a critical issue in that context. Although it may be impossible to fully eliminate all the vulnerabilities associated with wireless networking, maintaining an overall degree of protection becomes much simpler if a comprehensive approach is implemented in risk evaluation and management.

The paper reflects our research's first step in evaluating security risks, recognizing safety standards, and defining current techniques. More research is required to implement these protection mechanisms in a network and analyze the effect on the network efficiency of those security mechanisms.

To stay protected, wireless networks must be protected against both external and internal security threats. A notable best practice of securing a wireless network is to have accurate knowledge of security, wireless network access control, proper authentication, and encryption of wireless network, accurate implementation, and sustained maintenance. These could help adjust to the new demands for speed and security being put on the network.

References

- [1] D. S. P. K. S. A. M. Sri Lakshmi, "A Review on Wireless Network Attacks," (*IJCSIT*) *International Journal of Computer Science and Information Technologies*, 2014.
- [2] S. K. ., M. Elankayer Sithirasenan, "An EAP Framework for Unified Authentication in Wireless Networks," *IEEE*, 2011.
- [3] J.-C. C. A. Y.-P. WANG, "Extensible Authentication Protocol (EAP)," pp. supl.26 - supl.32, 2005.
- [4] P. A. S. Kirtiraj Bhatele, "A Novel Approach to the Design of a New Hybrid Security Protocol," 2012.
- [5] M. M. S. D. ARASH HABIBI LASHKARI, "A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)," *2009 2nd IEEE International Conference on Computer Science and Information Technology*, 2009.
- [6] P. D. G. S. D. H. M. E. B. E. M. A. Salam, "NEW PROTOCOL DESIGN FOR WIRELESS NETWORKS SECURITY," *IEEE Xplore, 8th International Conference Advanced Communication Technology*, 2006 .
- [7] I. S. M. S. M. N. S. M. A. Bahareh Shojaie, "Improving EAP-TLS Performance Using Cryptographic Methods," *IEEE*, 2012.
- [8] H.-W. L. S. H. Al-Sakib Khan Pathan, "Security in Wireless Sensor Networks: Issues and Challenges," *IEEE*, 2006.
- [9] J. A. G. Ivan Howitt, "IEEE 802.15.4 Low Rate –Wireless Personal Area Network Coexistence Issues," *IEEE*, 2003.
- [10] A. A. Lifeng Sang, "A Shared-Secret Free Security Infrastructure for Wireless Networks," *DBLP*, 2012.
- [11] M. S. Srinivasan. K, "Performance of State Based Key Hop (SBKH) Protocol for Security on Wireless Networks," *IEEE*, 2004.

- [12] W. C. S. D. Bhagyavati B, "Wireless security techniques: an overview," *InfoSecCD '04 Proceedings of the 1st annual conference on Information security curriculum development*, pp. 82-87, 2004.
- [13] H. Chan. Chan. Perrig, "Peer intermediaries for key establishment in sensor networks.," *IEEE*, pp. 524-535, 2005.
- [14] B. G. a. H. Nabovati, "Concepts for Designing Low Power Wireless Sensor Network," *IEEE*, 2008.
- [15] W. I. a. N. F. Thornhill, "Wireless communication in process automation: A survey of opportunities, requirements, concerns and challenges," *Conference: Control 2010, UKACC International Conference*, 2010.
- [16] R. H. Andrew Gin, "Performance analysis of evolving wireless IEEE 802.11 security architectures," *DBLP*, 2008.
- [17] A. Neu, "Types of Wireless Network Attacks," *CYBER SECURITY*, 2016.
- [18] J. J. K. G. S. K. Justice Owusu Agyemang, "Information Security and Computer Fraud," *A Lightweight Rogue Access Point Detection Algorithm for Embedded Internet of Things (IoT) Devices*, pp. 7-12, 2019.
- [19] S. B. S. N. Mayank Agarwal, "International Journal of Wireless Information Networks," *An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks*, pp. 1-16, 2018.
- [20] I. F. L. ., Y. S. L. S. S. C. C. C. a. M. L. Weidong Fang, "Recent Advances in Security and Privacy for Wireless Sensor Networks," *Information Security of PHY Layer in Wireless Networks*, p. 10, 2016 .
- [21] C. S. H. Smith, *Cryptology and Network Security*, vol. 7712, J. P. S. Manulis, Ed., Germany: 11th International Conference, CANS 2012, 2012.
- [22] Y. s. G. Chao Yang, " IEEE Transactions on Information Forensics and Security," *Active User-Side Evil Twin Access Point Detection Using Statistical Techniques*, pp. 1638-1651, 2012.
- [23] D. L. A. M. Biju Issac, "DATA COMMUNICATIONS & NETWORK SECURITY," *War Driving and WLAN Security Issues—Attacks, Security Design and Remedies*, pp. 289-298, 2007.

- [24] S. U. T. S. Ch.Sai Priya, The Impact of War Driving On Wireless Networks, INDIA. : IJCSET, 2013.
- [25] A. Joseph, "Bluejacking Technology," in *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY*, India, 2018.
- [26] A. T. S. N. B. B. Mini Sharma, "Classification and analysis of security attacks in WSNs and IEEE 802.15.4 standards : A survey," in *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall)*, India, 2017.
- [27] S. R. Ellis, Computer and information Security, Canada: ELSEVIER, 2013.
- [28] A. V. S. Rupam, "An Approach to Detect Packets Using Packet," IEEE, India, 2013.
- [29] A. A. Habib, Analysis of various wireless network packet-sniffing tools for network monitoring and analysis, Bangladesh, 2017.
- [30] S. R. C. S. Ansari, "Packet sniffing: A brief introduction," pp. 17 - 19, 2003.
- [31] Z. Feng, J. Ning, I. Broustis, K. Pelechrinis and S. V. Krishnamurthy, "Coping with packet replay attacks in wireless networks," in *2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, Salt Lake City, UT, USA, 2011.
- [32] A. D. M. F. M. Dragoni, Detecting and Preventing Beacon Replay Attacks in Receiver-Initiated MAC Protocols for Energy Efficient WSNs, Greenland: 18th Nordic Conference, NordSec 2013, Ilulissat, Greenland, October 18-21, 2013, Proceedings, 2013.
- [33] M. K. K. A. Althubyani, A Survey on Wi-Fi Protocols: WPA and WPA2, Canada: Springer, 2014.
- [34] A. LONG, "Hack WPA WiFi Passwords by Cracking the WPS PIN," pluralsight, 2012.
- [35] I. D. Rianto, Binus University , Jakarta Barat.
- [36] F. T. Sheldon, J. M. Weber and S.-M. Yoo, "The Insecurity of Wireless Networks," *IEEE Security & Privacy*, pp. 54-61, 2012.
- [37] s. p. Kanawat, "Attacks in Wireless Networks," *International journal of smart sensor and ad hoc*

network, pp. 114-116, 2011.

- [38] V. S. S. M. S. Athulya, "Security in Mobile Ad-Hoc Networks," in *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*, Coimbatore, 2012.
- [39] B. S. A. Goyal Priyanka, "A Literature Review of Security Attack in Mobile Ad-hoc Networks," *International Journal of Computer Applications*, 2010.
- [40] D. P. S. Priti1*, "A Review: Security Issues in Mobile," *A Monthly Journal of Computer Science and Information Technology*, pp. 365-370, 2014.
- [41] B. W. C. W. Cardei, *A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks*, Boston: Springer, Boston, MA, 2007.
- [42] A. B. B. Aniruddha Bhattacharyya, "Different types of attacks in Mobile ADHOC Network:Prevention and mitigation techniques," Department of Computer Science & Engineering, Institute Of Engineering & Management, Saltlake.
- [43] S. H. a. C. J. M. PO-WAH YAU, *Malicious attacks on ad hoc network routing protocols*, UK: Information Security Group,.
- [44] H. M. a. V. K. B. Majid Khabbazian, *Wormhole Attack in Wireless Ad Hoc Networks*., Canada: Department of Electrical and Computer Engineering.
- [45] A. R. a. N. S. Mamta Agiwal, "Next Generation 5G Wireless Networks:A Comprehensive Survey," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, india, 2016.
- [46] L. M. A. K. Mohamed Amine Ferrag, "Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-preserving Schemes," *Journal of Network and Computer Applications* , 2017.
- [47] G. M. C.-W. P. A. A. Lasebae, *Providing Security in 4G Systems: Unveiling the Challenges*, Spain: Sixth Advanced International Conference on Telecommunications, AICT 2010, 9-15 May 2010, Barcelona,, 2010.

- [48] S. S. K. O. G. Y. I. Ahmad, "Security for 5G and Beyond," *IEEE Communications Surveys & Tutorials*, pp. 3682-3722, 2019.
- [49] C. V. Anghel Drugarin, "Data security in wireless network," *ACTA TECHNICA CORVININESIS-BULETIN OF ENGINEERING*, pp. 133-136, 2010.
- [50] A. B. A. M. Muhammad Noman Riaza, "Classification of Attacks on Wireless Sensor Networks: A Survey," Department of Computer Science, Virtual University of Pakistan, Lahore, 54000, Lahore, 2018.
- [51] Stamatios and V. Kartalopoulos, "Differentiating Data security and Network Security," in *IEEE International Conference on Communications*, Beijing, 2008.
- [52] M. U. A. Q. A. Naeem Raza, "Mobile Ad-Hoc Networks Applications and Its Challenges," *Communications and Network*, pp. 131-136, 2016.