Wireless Communication, Network Security & Cryptography

Clinton Joshi
BSc. Computer Science
Don Bosco College
Mannuthy, Thrissur 680 651

Joel C Johnson
BSc. Computer Science
Don Bosco College Mannuthy
Thrissur 680 651

Abstract **-- Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. A wireless network enables people to communicate and access applications and information without wires.Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.The main aim of this article is to communicate the concept of Wirelesscommunication, Network security andCryptography.**

Keywords – Wireless, Network, Cryptography, Security, Communication

I. INTRODUCTION

Wireless communications[1] is by any measure,the fastest growing segment of the communications industry. As such it has captured the attention of the media and the imagination of the public.Cellular phones
have become a critical business tool and part of everyday life in most developed countries, and are rapidly supplanting antiquated wireline systems in many developing countries. In addition, wireless local area networks are currently poised to supplement or replace wired networks in many businesses and campuses. Many new applications, including wireless sensor networks, automated highways and factories, smart homes and appliances, and remote telemedicine, are emerging from research ideas to concrete systems. The explosive growth of wireless systems coupled with the proliferation of laptop and palmtop computers indicate a bright future for wireless networks, both as stand-alone systems and as part of the larger networking infrastructure.

A specialized field in computer networking involves securing a computer network infrastructure. Network security is typically handled by a network administrator or system administrator who implements the security policy, network software and hardwareneeded to protect a network and the resources accessed through the network from unauthorized access and also ensure that employees have adequate access to the network and resources to work.A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is *Pretty Good Privacy* because it's effective and free.Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and *public-key*systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

II. WIRELESS COMMUNICATION

Heinrich Herz discovered and first produced radio waves in 1888 and by 1894 the modern way to send a message over telegraph wires was first conducted. Marconi sent and received signals up to two miles using radio waves. Marconi became known as the “father of radio”. By 1899, Marconi sent a signal nine miles across the Bristol Channel and 31 miles across the English Channel to France. In 1901 he was able to transmit across the Atlantic Ocean.

During World War II, the United States Army first used radio signals for data transmission. This inspired a group of researchers in 1971 at the University of Hawaii to create the first packet based radio communications network called ALOHNET. ALOHNET was the very first wireless local area network (WLAN). This first WLAN consisted of 7 computers that communicated in a bi-directional star topology.

The first generation of WLAN technology used an unlicensed band (902-928 MHz ISM), which later became crowded with interference from small appliances and industrial machinery. A spread spectrum was used to minimize this interference, which operated at 500 kilobits per second. The second generation of WLAN technology was four times faster and operating at 2Mbps per second. Third generation WLAN technology operates on the same band as the second generation and we currently use it today.

In 1990, the IEEE 802 Executive Committee established the 802.11 Working Group to create a wireless local area network (WLAN) standard. The standard specified an operating frequency in the 2.4GHz ISM band. In 1997 the group approved IEEE 802.11 as the world's first WLAN standard with data rates of 1 and 2 Mbps.

A. WPANS: Wireless Personal Area Networks

A wireless personal areanetwork (WPAN) is a personal, short distance area wireless network for interconnecting devices centered around an individual person's workspace.(Fig 1) WPANs address wireless networking and mobile computing devices such as Personal Computers, Personal Digital Assistants, peripherals, cell phones, pagers and consumer electronics. WPANs are also called short wireless distance networks. The two current technologies for wireless personal area networks are Infra Red (IR) and Bluetooth (IEEE 802.15). These will allow the connectivity of personal devices within an area of about 30 feet. However, IR requires a direct line of site and the range is less.

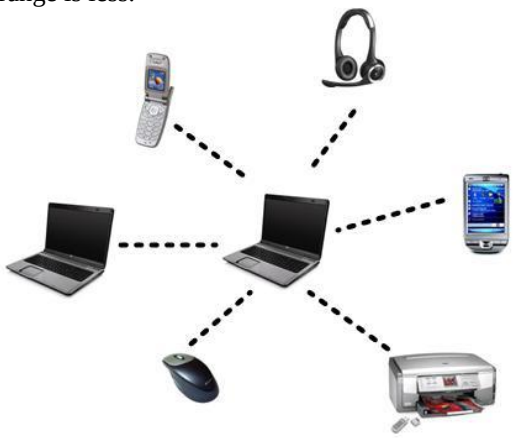

Fig 1: ***w**ireless **p**ersonal **a**rea network*

B. WLANS: Wireless Local Area Networks

WLANS allow users in a local area, such as a university campus or library, to form a network or gain access to the internet(Fig 2). A temporary network can be formed by a small number of users without the need of an access point; given that they do not need access to network resources. It implements a flexible data communication system frequently augmenting rather than replacing a wired LAN within a building or campus. WLANs use radio frequency to transmit and receive data over the air, minimizing the need for wired connections. A wireless local area network (WLAN) is a wireless distribution method for two or more devices that use high-frequency radio waves and often include an access point to the Internet. A WLAN allows users to move around the coverage area, often a home or small office, while maintaining a network connection.

Fig 2: ***w**ireless local **a**rea network*

C. WMANS: Wireless Metropolitan Area Networks

This technology allows the connection of multiple networks in a metropolitan area such as different buildings in a city, which can be an alternative or backup to laying copper or fiber cabling(Fig 3). A *Wireless Metropolitan Area Network* (**WMAN**) is also known as a **Wireless Local Loop** (*WLL*).WMANs are based on the *IEEE 802.16* standard. Wireless local loop can reach effective transfer speeds of 1 to 10 Mbps within a range of 4 to 10 kilometres, which makes it useful mainly for telecommunications companies.

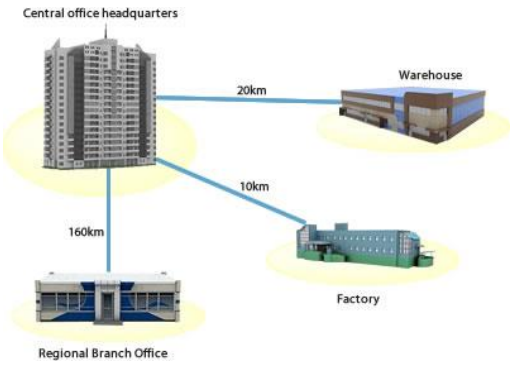

Fig 3: ***w**ireless metropolitan **a**rea network*

D. WWANS: Wireless Wide Area Networks

These types of networks can be maintained over large areas, such as cities or countries, via multiple satellite systems or antenna sites looked after by an Internet Service Provider(Fig 4). These types of systems are referred to as 2G (2nd Generation) systems. The three families of WWAN technologies are GSM/UMTS, CDMA One/CDMA2000 and WiMAX. In the United States, service providers include AT&T, Clearwire, Sprint and Verizon. Wireless WAN services are expected to become increasingly available as 4G technologies mature.

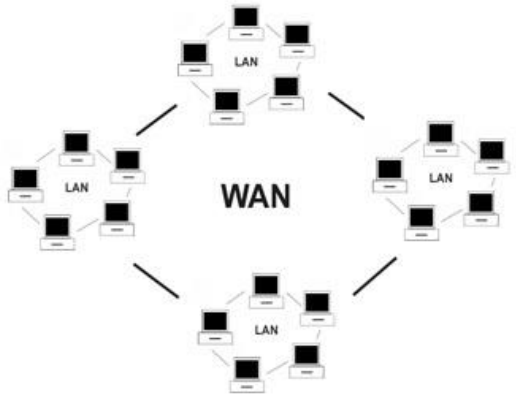

Fig 4: ***w**ireless wide **a**rea network*

E. Cellular Networks

A cellular network or mobile network is a wireless network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station(Fig 5). In a cellular network, each cell uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed bandwidth within each cell.When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

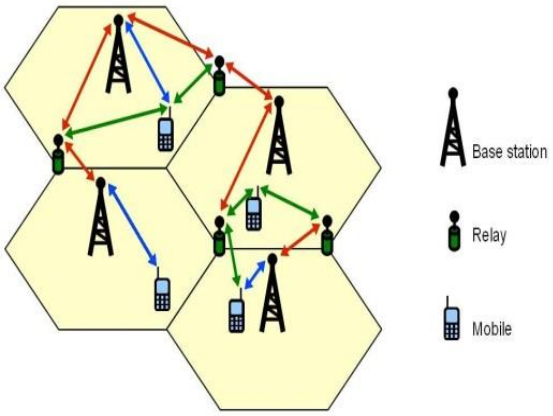

Fig 5:*cellular networks*

F. VPN:virtual private network

A virtual private network (VPN) extends a private network across a public network, such as the Internet(Fig 6). It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions. Major implementations of VPNs include OpenVPN and IPsec.

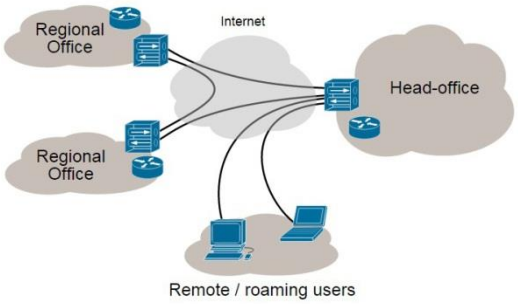

Fig 6:*virtual private network*

III. NETWORK SECURITY

A network is a group of two or more computer systems linked together. Networks can interconnect with other networks and contain subnetworks.

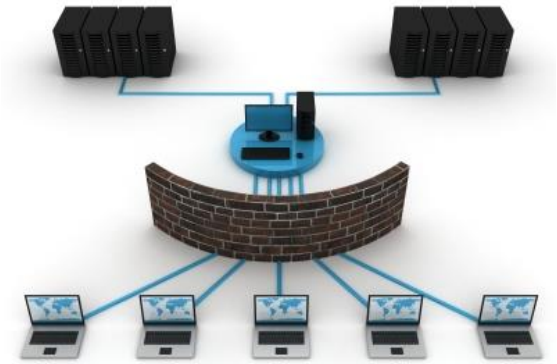

Fig 7: *network security*

Types of Network Security threats [3] are classified into passive and active security threats.

A. Passive Security Threats

These threats involve such activities as wiretapping, eavesdropping, and the collection of private data for traffic analysis. An example of this would be exactly what the NSA is doing with their prism program, wherein they collect all of the private information upstream of the content provider. The job of the system owner in protecting the data is not to detect these attacks but rather to prevent the access to this information by using a durable encryption method.

B. Active Security Threats

Active threats always involve a modification of the data stream. Four main categories of attack: masquerade, replay, modification of methods, and the denial of service attack. A masquerade attack attempts to utilize an alternate identity while threatening a system and almost always uses other forms of attack in conjunction with this method. A replay attack capture information sent by an unwary client and later attempts to reuse, replay, that information in order to gain access to protected data.The attacker utilizes all of the resources of the victim, thus

isolating the systems under attack and making them inaccessible.

Main security devices and technologies used are:

- Firewalls
- Intrusion Detection and Prevention Systems (IDS)
- Virtual Private Networks (VPN)
- Tunneling
- Network Access Control (NAC)
- Security Scanners
- Protocol Analyzers
- Authorization, authentication and accounting (AAA)

IV. CRYPTOGRAPHY

Cryptography[5] is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it.

A message in its original form is known as **plaintext** or **cleartext**. The mangled information is known as **ciphertext**. The process for producing ciphertext from plaintext is known as **encryption**. The reverse of encryption is called **decryption**.

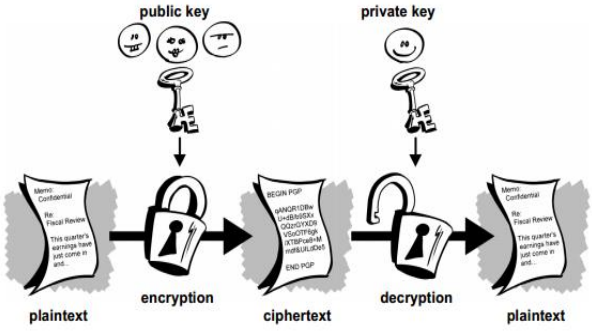

*Fig 8:*cryptograpgy method

Modern cryptography concerns itself with the following four objectives:

1) **Confidentiality :**the information cannot be understood by anyone for whom it was unintended.

2) **Integrity :** the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

3) **Non-repudiation :** the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

4) **Authentication :** the sender and receiver can confirm each others identity and the origin/destination of the information.

A. Caesar's Cipher

An extremely simple example of conventional cryptography is a substitution cipher. For example, if we encode the word "SECRET" using Caesar's key value of 3, we offset the alphabet so that the 3rd letter down (D) begins the alphabet. So starting with ABCDEFGHIJKLMNOPQRSTUVWXYZ and sliding everything up by 3, you get DEFGHIJKLMNOPQRSTUVWXYZABC where D=A, E=B, F=C, and so on.

B. Key management and conventional encryption

Conventional encryption has benefits. It is very fast. It is especially useful for encrypting data that is not going anywhere. However, conventional encryption alone as a means for transmitting secure data can be quite expensive simply due to the difficulty of secure key distribution.

C. Public key cryptography

The problems of key distribution are solved by public key cryptography, the concept of which was introduced by Whitfield Diffie and Martin Hellman in 1975.Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read.

CONCLUSION

Wireless technology is becoming more and more popular because of its low cost and ease-of-use. In many cases wireless has become cheaper than the wired alternative. This technology allows us a faster and more convenient access to the world. XBee technology provides the world with a variety of wireless applications. The direct interfacing of analog sensors and digital i/o, makes Xbee widely acceptable in variety of areas. From a simple domestic application of temperature control to the more complex mesh sensor networks that analyze volcano, XBee devices are gradually becoming an industry standard in wireless communication.

As hackers and many algorithms are there to break passwords and much valuable information, which leads to a great loss. Hence network security provides the remedy by many ways. Hence much more advanced security measures would be more helpful. So always that should be an eye on network security as it is much and more important.

Cryptology presents a difficulty not found in normal academic disciplines: the need for the proper interaction of cryptography and cryptanalysis. This arises out of the fact that in the absence of real communications requirements, it is easy to propose a system that appears unbreakable. Many academic designs are so complex that the would–be cryptanalyst doesn't know where to start; exposing flaws in these designs is far harder than designing them in the first place. The result is that the competitive

process, which is one strong motivation in academic research, cannot take hold.

ACKNOWLEDGEMENT

We would like to thank our honorable Principal Prof. Paulson Chalissery of Don Bosco College and Ms.Chris Aloysius, Head of Department of Computer Science for giving us the facilities and providing us with a propitious environment for working in college.

REFERENCES

[1] T.S. Rappaport. Wireless Communications:Principles and Practice,2nd editon.Prentice Hall, 2002.
[2] "Overview of Wireless Communications". cambridge.org. Retrieved 8 February 2008.
[3] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with JayshreeUllal, senior VP of Cisco.
[4] http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
[5] Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. Handbook of Theoretical Computer Science 1. Elsevier.
[6] http://www.wired.com/images_blogs/threatlevel/2012/01/decrypt.pdf