DATA COMMUNICATION NETWORKS AND SECURITY

ADUSEI PEPRAH EMMANUEL

Nanjing University of Posts and Telecommunications,China
Bachelor Student, Computer Science and Technology
Computer Science Department
E-mail: aduseiea65@yahoo.com

Abstract - The objective of this paper is to evaluate data Communication Networks and Security. This paper introduces data Communication Networks which emphasize on cellular telephony, satellite networks and satellite orbits. Another important aspect of the paper is Network Security which focused on communication network base attacks, principles of cryptography, and basic technologies to prevent vulnerabilities in network security. This paper concludes that, channel is always assigned to the caller by the mobile switching center (MSC), handoff procedure in 4G networks helps signals to be transmitted from one cell to another without the notice of the caller. It was established that the major principle of cryptography was algorithm and secrecy. The algorithm makes sure that the encryption and decryption of a plaintext is not made readable by an intruder or a hacker. The secrecy ensures that the key is not made known to a third party. The basic technologies to prevent vulnerabilities in network security were mainly intrusion detection, firewall, password management, strict security polices, antivirus, and encryption.

Index Terms - Communication, Satellite, Orbit, Network Security, Cryptography.

I. INTRODUCTION

As a result of fast technological advancement, the installation of worldwide telephone networks, the invention of radio and television, the birth and bizarre growth of the computer industry, the launching of communication satellites and the Internet are rapidly converging in the 21st century and the differences between collecting, transporting, storing, and processing information are quickly disappearing. Theeruption of hackers, electronic fraud and virus in this modern age complex world of universal electronic connectivity, necessitate the need to protect oneself. It is therefore necessary to consider networksecurity as a strategy to protect the systems from network-based attacks. This has as a result led to an intensified awareness of the essence to protect data and resources from disclosure, to warrant the authenticity of data and messages, and to protect systems from network-based attacks. Additional, the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security.

II.DATA COMMUNICATION NETWORKS

Data communications are the exchange of data between two devices via someform of transmission medium such as a wire cable, for data communications to occur,the communicating device must be part of a communication system made up of a combinationof hardware (physical equipment) and software (programs)[1].Computer network allows computers in a telecommunication network to exchange data.In general,data communication networks facilitate the efficient use of computers to transmit data by means of wired or wireless communication channels.A lot of topics can be discussed under data communication network but I would like to emphasize on cellular telephony in data communication and satellite networks.

A. Cellular telephony in data communication.

Cellular telephony is designed to provide communications between two movingunits, called mobile stations (MSs), or between one mobile unit and one stationaryunit, often called a land unit [2].The mobile phone is an example of mobile station. Previously, the mobile phones were built with an antenna but currently the size of the antenna has been reduced to the extent the antenna are now built in the mobile phone. Have you ever wondered about how our mobile station work especially when calls are made? Technically and practically, every city or area is divided into cells.A group of cells is called a cluster.As the city or area is divided into small cell, they must be symmetrical in shape. Each cell is assigneda band of frequencies and is served by a base station, consisting of transmitter, receiver, and control unit, adjacent cells are assigned different frequencies to avoidinterference or crosstalk and cells sufficiently distant from each other can usethe same frequency band [3]. Fig 1.1 shows the architecture of the mobile system. In the diagram mobile station (MS) is the mobile phone of the user or a stationery unit. Signal are transmitted to the base transceiver station of the cell when a call is made, and then transferred to the mobile switching center (MSC) which controls the whole system. The mobile switching center (MSC) forwards the data to the public switching office and a connection is made if the called partyis available.

The architecture of a cellular system includes the phone (stationed), public switched telephone network PSTN), mobile switching center (MSC), base station (BS) and mobile station (MS).

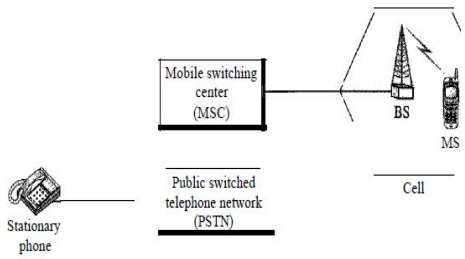


Fig 1.1 Architecture of a cellular system

When a call is made by a user, a separate channel is assigned to the caller by the mobile switching center (MSC). For example, in Fig 1.2 Channel 3 is assigned to the User R.

Channel 1	Channel 2	Channel 3	Channel 4	Channel 5
		User R		

Fig 1.2 Assigned Channel to the User R is 3

If all the channels are engaged by other users in a particular cell as shown in Fig 1.3, then the user has to wait for a channel to be free. In such cases the user receives a replied message as "call can't be completed or network error" depending on the service provider.

Channel 1	Channel 2	Channel 3	Channel 4	Channel 5
User A	User B	User Q	User P	User Y

Fig 1.3 All Channel are used up.

- **Handoff Procedure in 4G network**

Recently, fourth generation (4G) systems have been developing to support greater bandwidth services, higher data rates, improved quality and seamless global mobility as compared to the current 3G systems[4]. Have you analyzed why calls are not disconnected and ended whileslocomotionis made from a coverage area or cell to another coverage. The process of which the call signals are handed over from base station to another base station without the call been dropped is called handoff Procedure. Considering a situation in Fig 1.4 where a caller moves from BS1 to BS2. Signal is obtained from BS1 because the call is made in the territory of the cell of BS1. As the caller approaches BS2, signal strength gradually loses. At the boundary of BS1, the signal strength drops totally as the caller enters BS2. Simultaneously, as the signal strength is lost in BS1, BS2 takes controls of the device as it enters the BS2 cell. Thefourth generation (4G) network system has immensely helped handoff procedure to be successful because of higher and improved quality mobile system.In a typical 4G network scenario, mobile terminals or handsets with multiple interfaces can choose among the appropriate access link between IEEE 802.11 Wireless Local Area Network (WLAN), IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX), Bluetooth and satellite systems in addition to cellular telephony networks and these are reachable globally today[5]. Handoff procedure can be classified into horizontal and vertical handoff in every heterogeneous mobile network system.Horizontal handoff occurs when mobile node (MN) movesbetween similar wireless networks, while vertical handoff occurs when the movement is betweenheterogeneous wireless networks [6].

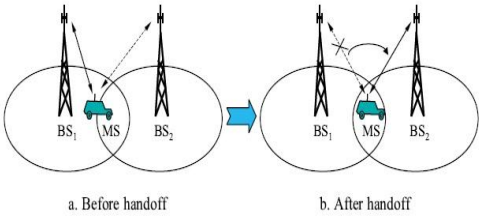


Fig 1.4 Handoff Procedure

B. Satellite Networks

Historically in telephony networks, it provided connections from telephone or private branch exchanges(PBX) to the telephony networks, the user terminals link to the satellite earth terminals toaccess satellite links directly [7].Globally, communication network with earth stations and some connectivity has made transmission of data reach their destination accurately and rapidly. Satellite is the backbone of all these successful communication networks. Arthur C. Clarke in his seminal article "Extra-Terrestrial Relays" described a satellite in synchronous orbit being used for providing communication relay services within any two points on the hemisphere and a constellation of three such satellite for providing global coverage, and further argued that using a satellite in synchronous orbit would be more cost effective and provide much better coverage than alternative terrestrial communication techniques [8].Satellite networks are very effective at broadcasting data over large geographical location, and are an effective means for reaching remote locations lacking in communication infrastructure [8].

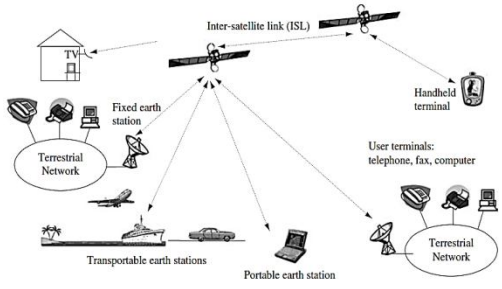
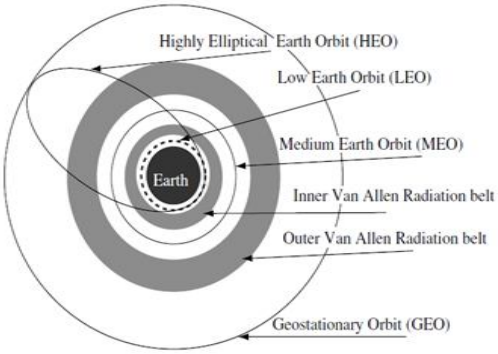


Fig 2.1 Satellite and terrestrial networked system with Applications.

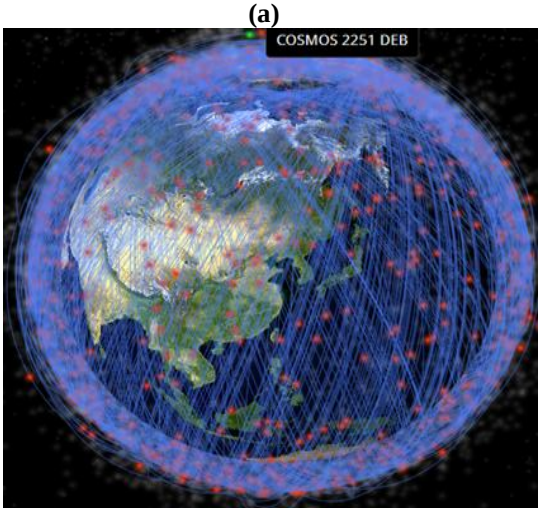
The merging of satellite and terrestrial networks is widely recognized as the foundation for an effectual global information infrastructure.

➢ **Satellite Orbit**

Every satellite designed and launched into its orbit depends on it purpose and application.Most of the communications satellites likewise use a geostationary orbit because it stays in the same spot relativetoEarth.



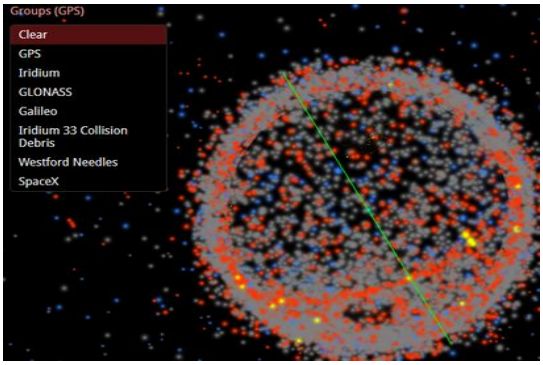
(a)



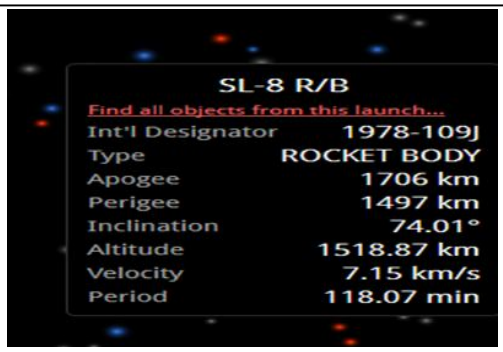
(b)

Fig 2.2 Satellite Orbit

Fig 2.2(a) display the different types of satellites with different altitudes. The geostationary orbit is mostly located above the earth. It travels at about 6,880 miles per hour around the equator and which follow the earth's rotation. Television satellites, Long Distance Communications satellites, Internet, Global Positioning Systems (GPS) uses the geostationary orbit. Fig 2.2(b) display the earth with different satellites in their orbits with different altitude.



(a)



(b)

Fig 2.3 GPS in the geostationary orbit.

Fig 2.3(a) display the satellite SL-8 R/B in the GPS geostationary orbiting around the earth with a speed of 7.15km/s. It has an apogee and perigee with a distance of 1706km and 1497km respectively.

III. NETWORK SECURITY WITH CRYPTOGRAPHY

Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and managementpolicy required to provide an acceptable level of protection for Hardware and Software , and information in a network[9]. Generally, network security is indivisibly related to the confidentiality, integrity, authenticity and reliability of network. Its control and protect our technologies from cyberattacks. Fig 3.1 shows theshows the report on security vulnerabilities of information system by the U.S. security organization CERT / CC.

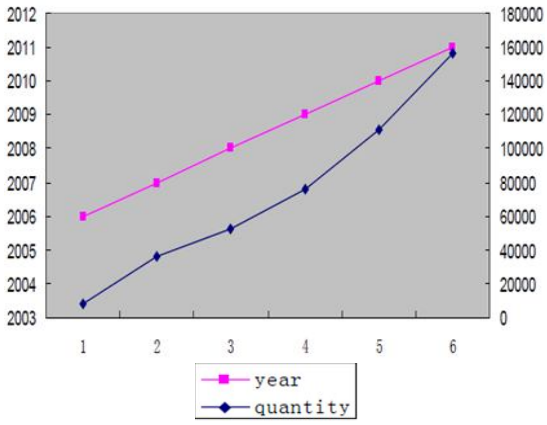


Fig 3.1 2006-2011 The total number of system security vulnerabilities.

IV. COMMUNICATION NETWORK BASE ATTACKS

Different types of attackers (e.g., serious hackers, interested computer novices, dishonest vendors, and disgruntled current or former employees) could pose a potential threat to an institution's information security. The internet provides different sources of information on known security flaws in hardware and

software. Using almost any search engine on the internet, average internet users can quickly find information describing how to break into various systems by exploiting known security weaknesses. Attackers may also breach security by using automated tools to probe network systems, then exploiting any identified security weaknesses to gain unauthorized access to the network. Apart from attacks originated from external parties, many break-ins occur due to poor information security policies and procedures, or internal misuse of information systems. Also, new security risks could arise from evolving attack methods or newly detected holes and bugs in existing software and hardware.Attacks in communication network can be grouped into Passive attacks and Active attack. Two types of passive attacks are the release of message contents and traffic analysis.They are very difficult to detect, because they do not involve any alteration of the data. The emphasis in dealing with passive attacks is on prevention rather than detection [10]. On the other hand, Active attacks are involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, and modification of messages [10].Some types of attacks incommunication network arebrute force cryptanalytic attack, IP spoofing, password sniffing, known plaintext dictionary attack and so on.

V. PRINCIPLES OF CRYPTOGRAPHY

Cryptography plays a major role in the communication network. It plays a vital role in information security as message content are confidentially transmitted.

- Algorithm:Sending a message from computer A to computer B requires an algorithm to be able to encrypt or decrypt the message. Algorithms like data encryption standard (DES), advanced encryption standard (AES), triple DES etc. performs some alteration and substitution in the plaintext.
- Secrecy: It's important to note that the sender and receiver must trust themselves with the secrecy of the Key. If the algorithms together with the key is discover by an intruder, the plaintext now becomes readable by the intruder.Such a key needs to be shared between the two communicants, which basically means you have to give it to the other person through a perfectly secure protocol (e.g.by hand/trusted courier).

VI. BASIC TECHNOLOGIES TO PREVENTVULNERABILITIES IN NETWORK SECURITY

An effective network security plan is developed with theunderstanding of security issues, potential attackers,needed level of security, and factors that make anetwork vulnerable to attack [11]. Some basic technologies are explained below;

- Intrusion detection systems (IDS):As computer networks technology is rapidly advancing, intrusion is inevitable. An IDS can be grouped into host based and network based IDS. Network based IDS filters and cross check network traffic for any sign of intrusion (see Fig 3.2). Host based IDS also performs some statistical tests and use it to check some anomalies from the user on a local machine for signs of intrusion.

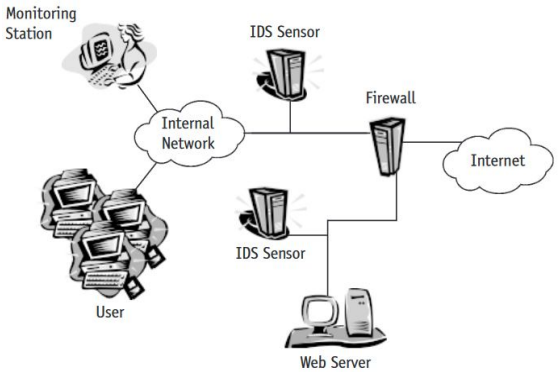


Fig 3.2 Network based IDS communicating with a monitoring station on the internal network with two IDS sensors on separate network segments.

- Firewall:It's designed to filter internet traffic. It protects our system from network based security attacks. It monitors data transfer and makes sure safety measures are taken between two or more networks.
- Password management:Every networked system with multi users have to be password protected. Password helps to authenticate the authorized user to gain access to the system. It's recommended that strong passwords are created to prevent intruders from easily accessing it.
- Strict security policy:Policies must be enforced to manage and protect information at all cost(e.g. storage, computer data) to prevent unauthorized disclosure or modification of information. Policies must ;

a. govern use of computer, application and communication networks
b. specify on how cryptographic data is protected
c. be programmed so that an automated system can enforce it

- Antivirus:The work of the antivirus is to detect, prevent and remove or delete any malware. It also protect against a wide variety of threats.
- Encryption:The most effective method to protect our data is to encrypt information and data.In cryptography, encryption veils information to make it difficult to read for any intruder. Without the encryption key, a ciphertext can't be decrypted even by the receiver.

CONCLUSION

Communication network together with security has globally succeeded and increasingly gained much

attention as internet is expanding recently. Data communication and network security were analyzed to determine what exactly happens in our cellular communications and necessary measures to protect our network. It was a surprise to understand how the satellite and orbit contributes globally to communications in our networked system. Combined use of algorithm and secrecy proves effectiveness in cryptography. Basic technologies like intrusion detection, firewall, password management, strict security polices, antivirus, and encryption gives a strong assurance of an effective network system as far as communication is concerned.

REFERENCES

[1] Behrouz A. Forouzan, "Data Communications and Networking," McGraw-Hill, 1221 Avenue of the Americas, New York, NY 10020, ED-4, pp. 4, 2007.

[2] Behrouz A. Forouzan, "Data Communications and Networking," McGraw-Hill, 1221 Avenue of the Americas, New York, NY 10020, ED-4, pp. 467, 2007

[3] William Stallings, "Data and Computer Communications," Pearson Education, Inc., publishing as Prentice Hall, 1 Lake Street, Upper Saddle River, NJ 07458, ED-8, pp. 415, 2007.

[4] Xichun Li and Rosli Salleh, "Handoff Techniques for 4G Wireless Mobile Internet," Information Technology Journal, Vol. 6, 745-750, 2007.

[5] Xiaohuan Yan, Y. Ahmet Sekercioğlu and Sathya Narayanan, "A survey of vertical handover decision algorithms in Fourth Generation heterogeneous wireless networks", Elsevier B.V, 2010.

[6] Nirmal Raj T,R.M.Suresh, "Efficient Service time Prediction and Bandwidth Reservation Technique for Vertical Handoff in 4G Networks",International Journal of Scientific & Engineering Research, Vol. 6, March 2014.

[7] [7] Zhili Sun, "Satellite Networking Principles and Protocols",John Wiley & Sons Ltd, the Atrium, Southern Gate, Chichester,pp. 28, 2005.

[8] [8] Eytan Modiano, "Satellite Data Networks", Journal of Aerospace Computing, Information and communication", American Institute of Aeronautics and Astronautics Inc., Vol. 1, October 2004.

[9] Prof. Mukund R. Joshi, Renuka Avinash Karkade,' "Network Security with Cryptography", International Journal of Computer Science and Mobile Computing,Vol. 4, pp 201-204, January 2015.

[10] Stallings W., "Network Security Essentials: Applications And Standards," Pearson Education, Inc., publishing as Prentice Hall, 1 Lake Street, Upper Saddle River, NJ 07458,ED-5, pp. 11,2011.

[11] Dowd, P.W.; McHenry,J.T., "Network security: it's time to take it seriously," Computer, vol.31,no.9, pp.24- 28, September 1998.

★★★