International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

A Literature Survey on Security Management Policies used in Wireless Domain

K. Senthil Kumar[1], P. Supraja[2], V. Sridharshini[2]

[1]Assistant Professor, [2]UG Student
[1,2]Department of Computer Science and Engineering, Knowledge Institute of Technology, Salem, Tamilnadu, India

How to cite this paper: K. Senthil Kumar | P. Supraja | V. Sridharshini "A Literature Survey on Security Management Policies used in Wireless Domain" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.4-7, URL: https://www.ijtsrd.com/papers/ijtsrd22854.pdf

IJTSRD22854

ABSTRACT

Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless. Wireless network security is the process of designing, implementing and ensuring security on a wireless computer network. Nowadays wireless networks are the most popular way of communication. For example, internet services in companies, cafes, e-markets and in homes. This paper will highlight the drawbacks and their proposed system to give continuous growth of new technologies in wireless domain, both for application and basic research. Papers should emphasize original results relating to the theory and/or applications of wireless communications and networking.

Keywords: *Wireless, frequencies, networks, internet-services, security, communication*

INTRODUCTION

Wireless Communications and low cost manufacturing technologies have resulted in a heterogeneous network system called Wireless Sensor Network (WSN).There are several technologies in wireless domain which are listed out below:

1. Bluetooth
2. Wi-Fi
3. Wimax
4. Zigbee
5. Satellite Communication

Here we created a proposed system to secure the confidential information; it also prevents users from unauthorized access to the network and prevents malicious elements within a pre-existing network in each of the above mentioned technology.

1. BLUETOOTH

Bluetooth is an ad hoc network was designed to connect devices to one another. It connects the device directly so it is known as peer-to-peer network.

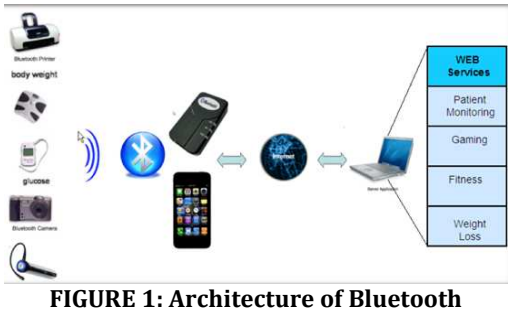


FIGURE 1: Architecture of Bluetooth

WORKING

Each Bluetooth device works with a microchip embedded in it that can send receive radio signals. It can send both data and voice. The radio signals are sent and received in the 2.4GHZ radio band, in the industrial, scientific, and medical (ISM) band. Inside the chip is software called a link controller that does the actual work of identifying other Bluetooth devices and sending and receiving data.

When a Bluetooth device finds one or more other devices within its range they go throw a series of communications that should establish whether they should communicate with one another. The connection of two or more Bluetooth devices is called piconet.

SECURITY ISSUES

- **Blue jacking**-This is the process where an attacker sends unsolicited messages or business cards to a Bluetooth-enabled device, mostly for advertising purposes.

- **Bluesnarfing**-This is a method to force a connection with a Bluetooth-enabled device to gain access to data such as contact list, calendar, emails, text messages, pictures, videos and the international mobile equipment identity (IMEI) stored in the memory.

- **Blue bugging**-This method was developed after the onset of blue jacking and bluesnarfing where it allows attackers to remotely access a Bluetooth-enabled device and use its features, such as read phone books, examine calendars, connect to the Internet, place phone calls, eavesdrop on phone calls through call forwarding and send messages without the user's knowledge.

- **Blue smack**-This is a Bluetooth Denial Of Service (DOS) attack where the Bluetooth-enabled device is overwhelmed by malicious requests from an attacker, causing it to be inoperable by its owner and draining the device's battery, affecting the continued operation of the device after the attack.

2. WI-FI

Wireless technology is shortly called as Wi-Fi. By its very nature Wi-Fi is an open technology. A facility allowing computers, smart phones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area. It is not a single standard. It refers to an entire family of standard based on the 802.11 networking protocol. There are multiple 802.11 standards based on their speed performance.

FIGURE 2: Wi-Fi

WORKING

A key component of wi-fi network is an access Point (or) router. The access point consists of radio transmitter and receiver as well as a interface to the wire network such as Ethernet network or directly to the internet. The access point serves as a base station and a router between the wireless network and large Ethernet network or an internet.

When a station is first turned on or enters an area near the access point, it scans the area to look for an access point to sending out packets of information called probe request frames. Before a station transmits information's or a request it sends a short packet of information called request to send(RTS).

SECURITY ISSUES

- Data sent over Wi-Fi can be captured by eavesdroppers – easily, within a few hundred feet; even farther with directional antennas.
- WLANs are inherently vulnerable to DoS. Everyone shares the same unlicensed frequencies, making competition inevitable in populated areas.
- Business network penetration by unknown, unauthorized APs has long been a top worry. Fortunately, most enterprise WLANs now use legitimate APs to scan channels for possible rogues in their spare time.
- Wireless IPS products like Motorola Air Defense, Air Magnet, and Airtight can also detect malicious Wi-Fi clients operating in or near a business' airspace. However, truly effective defense requires up-to-date, properly deployed WIPS sensors.
- Clients that form unauthorized Wi-Fi connections of any type, whether accidentally or intentionally, put themselves and corporate data at risk.
- Wi-Fi laptops have long been able to establish peer-to-peer ad hoc connections that pose risk because they circumvent network security policies.
- Fraudulent APs can easily advertise the same network name (SSID) as a legitimate hotspot or business WLAN, causing nearby Wi-Fi clients to connect to them.
- Addition to the above man-in-the-middle application attacks, hackers continue to develop new methods to phish Wi-Fi users.

3. WIMAX

WIMAX stands for worldwide interoperability for microwave access. Wimax refers to broadband wireless networks that are based on the IEEE 802.16 standard, which ensures compatibility and interoperability between broadband wireless access equipment. Wimax, which will have a range of up to 31 miles, is primarily aimed at making broadband network access widely available without the expense of stringing wires (as in cable access broadband) or the distance limitations of digital subscriber line. A wimax system consists of two major system:

- Wimax tower
- Wimax receiver

WORKING

WiMAX technology providers build a network with the help of towers that enable communication access over many miles.The broadband service of WiMAX technology is available in coverage areas. The coverage areas of WiMAX technology separated in series of over lied areas called channel.

When a user sends data from one location to another the wireless connection is transferred from one cell to another cell. When signal transmit form user to WiMAX base

station or base to user (WiMAX receiver) the wireless channel faces many attenuation such as fraction, reflection, refraction, wall obstruction etc. These all attenuation may cause of distorted, and split toward multi path. The target of WiMAX receiver is to rebuild the transmitted data perfectly to make possible reliable data transmission. Transmitted data divided into numerous data stream where everyone is owed to another sub carrier and then transmitted at the same broadcast interval. At the downlink path the base station broadcast the data for different user professionally over uninterrupted sub-carriers.

SECURITY ISSUES

- The security issues, include despite the good intentions for WiMAX security level, there are several potential attacks including: DoS Attacks replay attack, Man in the Middle attacks, Rogue base stations, etc.
- Traditional wireless technologies such as 2.5G cellular networks are not exposed to DoS attack since they are mainly based on circuit switching.
- A classic threat arises from the water torture Attack, in which an attacker sends a series of frames to drain the receiver's battery. In addition, attacker with a properly positioned RF receiver can intercept messages sent through wireless, and thus a confidentiality mechanism in the design is required.

4. ZIGBEE

Zigbee is a new wireless technology technical standard created for control and sensor networks based on the IEEE 802.15.4 standard. It is created by the zigbee alliance.

WORKING

There are three different zigbee devices types that operate on the layers in any self-organizing application network.

1. Zigbee coordinator node
2. Full function (FFD)
3. Reduced function devices (RFD)

ZIGBEE COORDINATOR NODE

It is the root of network tree and a bridge to another network able to store information about the network. Only One ZCN for a network. It also acts as a coordinator.

THE FULL FUNCTION DEVICE

A intermediary router transmitting data from other devices. It needs lesser memory than Zigbee. It can operate on all topologies.

THE REDUCED FUNCTION DEVICES

A Device capable of talking in the network. It cannot relay data from oZther devices and hassles memory

SECURITY ISSUES

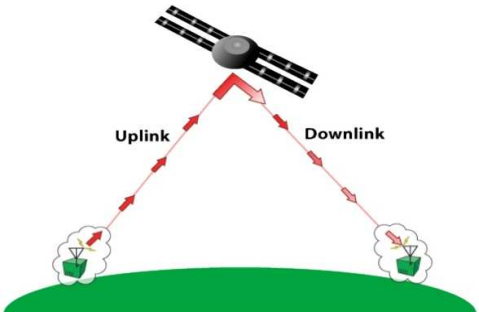
- Sniffing – sniffing attack in a zigbee network generally refers to the process of collecting all the available information in the network, which is possible in a network which implements the standard generic security level protocols for communication.
- Replay attack- A reply attack is a kind of key based attack where the replay attack can be evaded with the use and implements of freshness counter.
- Physical attack- this type of attack is the most common and involves tampering with the devices in the zigbee devices by locating it.
- Denial- of-Services- it disrupt the zigbee network.

5. SATELLITE COMMUNICATION

A communication satellite is a radio relay station in orbit above the earth. It receives, amplifies and redirects analog and digital signals carried on a specific radio frequency.

Two major elements of satellite communications systems are

- Space segment
- Ground segment



WORKING

Two stations on earth want to communicate through radio broadcast but are too far away to use conventional repeated. The two stations can use a satellite as a relay station for their communication. One earth station transmits the signals to the satellite. Up link frequency at which ground station is communicating with satellite. The satellite transponder converts the signal and sends it down to the second earth station. This frequency is called a downlink frequency.

SECURITY ISSUES

- Satellite communication (SATCOM) networks are critical in aeronautics, the energy and maritime industries, emergency services and the media.
- To exploit the vulnerabilities, an attacker would have to first compromise or gain physical access to a PC connected to one of the above networks.
- Many of the problems were discovered in Broadband Global Area Network satellite receivers.
- Vulnerabilities that IO Active claims to have found in mobile Harris BGAN terminals would allow attackers to install malicious firmware or execute arbitrary code.

DISADVANTAGES OF WIRELESS SYSTEMS

- The bandwidth is lower compare to Wi-Fi
- Battery usage is more compare to the condition when Bluetooth is powered OFF
- Easy to hack a information
- Slower Transmission Than Other Interface
- Limited Operational Range
- Compatibility Issues

REFERENCES

[1] https://www.alienvault.com/blogs/security-essentials/security-issues-of-wifi-how-it-works

[2] https://www.slideshare.net/Naveenmar11/wifi-technology-30347173

[3] https://www.esecurityplanet.com/viws/articlephp/3869221/Top-Ten WiFi-Security-Threats.html

[4] https://techterms.com/definition/wimax

[5] https://www.researchgate.net/publication/

[6] 49281057_Security_issues_of_IEEE_80216

[7] https://www.csoonline.com/article/2146021/cyber-attacks-espionage/major-security-flaws-threaten-satellite-communications.html