ISSN-2230-9659

BLUETOOTH & WIRELESS LAN

Neha Gupta

Assistant Professor in Bharti Vidyapeeth College of Engineering,

neha.06.gupta@gmail.com

Abstract: Wireless networking is the preferred method for establishing new computer networks, more and more organizations and users are switching over to wireless communication because of its benefits such as flexibility and portability, increased productivity and low installation cost over wired networks. As the popularity of wireless network increases, the need to make them secure also increases. Wireless networks cover a broad range of different networking options with different needs and uses like Bluetooth is used in communication between two devices and 802.11 is used for providing a secure communication. In this paper we do the study of various security issues in Bluetooth and wireless LAN and also compare them.

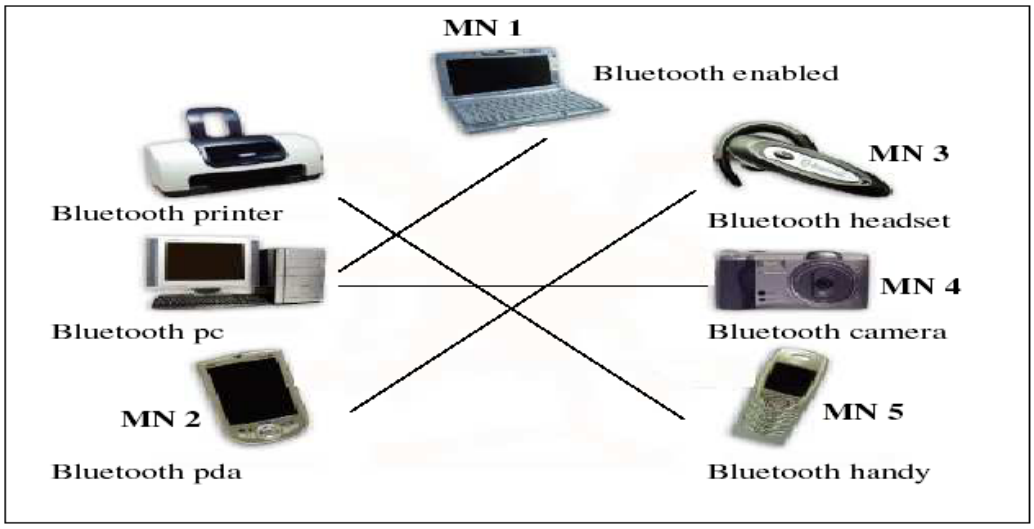
Keywords: skill-orientation, decision making, positional advantage, International market.

BLUETOOTH (802.15)

Introduction:

ISSN-2230-9659

The term Bluetooth refers to an open specification which enables short range peer-to-peer wireless communication of voice and data based on proximity network. Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices called gadgets finds each other and forms a network called piconet. A Bluetooth LAN can also be connected to internet if one of he gadget has this capability. Bluetooth technology has several applications i.e., peripheral devices can communicate with each other by using this technology, monitoring devices can communicate with sensor devices in a small health care center, home security devices can us this technology to connect different security sensors to main security controller and the conference attendees can synchronize their palmtop computers at a conference.



Bluetooth Network

Bluetooth Security

Security has played a major role in the invention of Bluetooth. The Bluetooth SIG has put a large effort to make Bluetooth a secure technology. Generally the security in Bluetooth s divided into three modes:

ISSN-2230-9659

1. **Non secure:** The device does not automatically initiate any security procedure.
2. **Service level enforced security:** The device does not automatically initiate the security procedure until L2CAP layer establishes a channel. The level provides an easy interaction with applications that have varied security requirements.
3. **Link level enforced security:** This device initiates security procedure before the link is established at the LMP layer.

Security Services

The need of security services such as authentication and encryption is of paramount importance, especially in an RF based ad hoc setting.

- **Device Authentication:** The unidirectional or mutual authentication of Bluetooth enabled device is carried out by the link manager.
- **Confidentiality:** Encryption of payloads of packets at the link layer is carried out by using a stream cipher with four linear feedback shift registers. It is based on a secret key of 8-bits to 128-bits that is a shared by a pair of devices. The variable length of the key is intended to accommodate the security requirements of different applications.

Device Authentication Protocol:

Authentication of a Bluetooth enabled device i.e. slave by another i.e. master is based on a challenge-response mechanism, which requires the following parameters:

- Address of a Bluetooth enabled device, 48-bits unique to each Bluetooth device.
- Shared secret key or link key-128 bits.
- Random number(RAND)-128 bits

There could be two cases:

Case I: Link key is not available:

ISSN-2230-9659

If slave and master have never communicated with one another, a shared key must be established. Steps to generate a link key:

1. **Pairing process:** To generate a link key the devices undergo a pairing process. At the end of this process an initialization key (Kinit) is produced which is used by both the devices to encrypt data during link key generation.
2. **Link key generation process:** After successful completion of pairing process a Kinit is available to both devices. Now link key can be generated using either of two options:
    - Link key generation using unit key: If one of two devices is memory constrained then the unit key i.e. 128 bits long private key of slave is use as the link key between slave and master. Then this unit key is encrypted by Kinit and transmitted to master.
    - Link key generation using combination key: It permits the generation of link key based on the properties of both devices.

Case II: Link key is available

For any future authentication purposes both devices stores the link key. Hence the pairing process becomes unnecessary. Te device simply performs the mutual authentication process

Security threats to Bluetooth Devices:

- **Blue jacking:** In this attacking process the unsolicited messages are sent to Bluetooth enabled devices. This method is most widely used for promotional purposes. Blue jacking works when the sending device and receiving devices are within the range of 10 meters of one another. The owners of the Bluetooth devices should be careful when adding contacts to their address book. Blue jacking is not usually done with malicious intent.
- **Blue snarfing:** In this method of hacking into a Bluetooth enabled device and copying its entire contacts , calendars or anything that is stored in the memory. By setting devices to the undiscoverable mode, it becomes difficult to find and attack the device. But these days there

ISSN-2230-9659

are so many soft wares available on the web to steal information from Bluetooth enabled devices.

- **The Back door attack:** it involves the establishment of a trust relationship through the pairing mechanism. In this way, when the owner is not noticing he devices at the precise moment a connection is established and attacker may be free to continue to use resources that a trusted relationship with that device grant access to. This means that not only the data can be accessed from the phone but services such as modem or internet, WAP, GPRS may be accessed without the knowledge of the owner.
- **The Cabir worm:** It is a malicious software that uses Bluetooth technology for seeking out the Bluetooth devices and sending itself to them.
- **Man In The Middle Attack:** In this attack the intruder seeking the access to Bluetooth device, inserts itself in between the two authorized devices. The two devices communicate with each other through the man in the middle, who intercepts and manipulates the data packets.
- **Blue bagging:** In this attack, the intruder access the phone's commands se that he can make calls, add or delete information, or eaves drop on the phone owner's conversation. The manufactures have addressed this vulnerability, so that the users of the Bluetooth enabled device keep their soft wares upgraded to latest phone models.
- **Denial of Service Attack:** Bluetooth devices are also vulnerable to this attack , typically by bombarding the device with requests to point that it causes the battery degrade.

Wireless LAN(802.11)

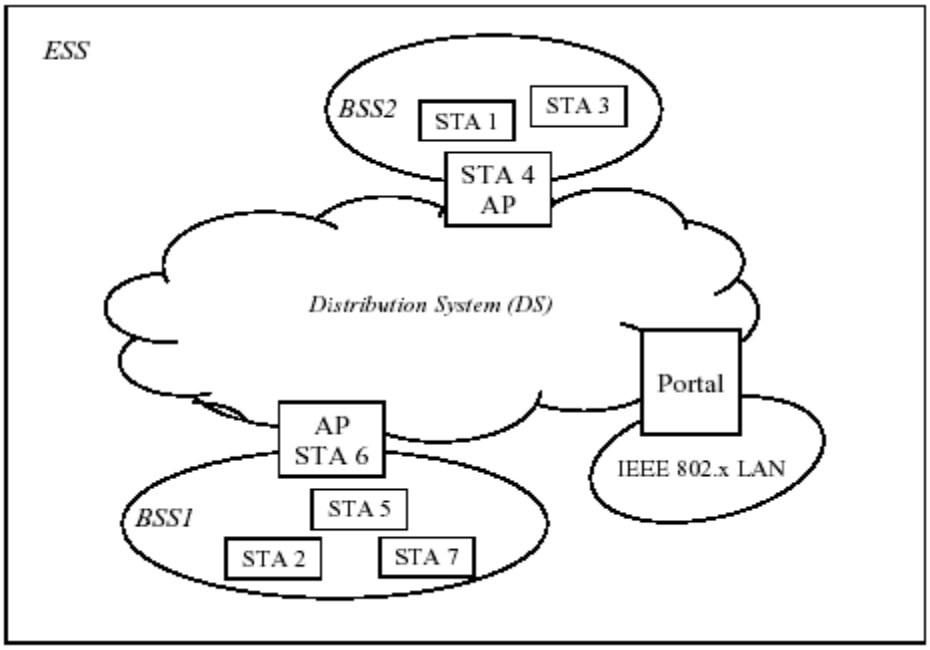
Introduction

The 802.11 is a standard that uses the CSMA with collision avoidance. The IEEE standard in 1997 specifies the MAC and PHY layers. The PHY standard allows both direct sequence and frequency hop spread spectrum transmissions in the 2.4 GHz ISM band. Whereas MAC layer is responsible

ISSN-2230-9659

for medium access control and management component supports the association of the mobile node at an AP, roaming between APs, authentication, encryption and power management.

The maximum data rate initially offered by wireless LAN was 2 megabits per second. A higher version, with a physical layer definition under 802.11 specifications allows a data rate of up to 11 megabits per second using direct sequence spread spectrum transmission.



Wireless LAN Architecture

Security services:

In the 802.11 the MAC layer is responsible for security services. It provides the following services:

1. **Authentication:** The authentication function is provided by using the open authentication and shared key authentication. The function of authentication is to verify the identity of users and to assure the recipient that the message is from the source it claims to

ISSN-2230-9659

2. **Confidentiality:** The WEP specifications provide the need for user confidentiality. A pseudo random number generator, which take 40 bits secret key as input is used to create a sequences that is XORed with the payload of each frame. The goal of WEP is to prevent eaves dropping. Confidentiality ensures that the data/information transmitted over the network is disclosed to the unauthorized users.
3. **Data Integrity:** Through the use of the integrity checksum field data integrity can be validated. The function of integrity is to assure that the data received are exactly as sent by an authorized party.

Security Threats in Wireless LANs:

1. **Passive attacks :** An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.

- **Eavesdropping—**The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.

- **Traffic analysis—**The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

2. **Active attacks:** An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks can be divided into internal attacks and external attacks:

ISSN-2230-9659

- **Internal attacks** from the compromise nodes that once legitimate art of the network. These attacks are difficult to prevent as legitimate users executes this type of attacks.
- **External attacks:** These types of attacks are carried out by nodes that are not legitimate part of the network. Such attacks can be prevented by using authentication, firewalls and encryption.

In wireless LANs the attacks can be classified into four categories:

- **Attack using impersonation:** In impersonation attacks, an intruder assumes the identity and privileges of another node in order to consume resources or to disturb normal network operation. An intruder device achieves impersonation by misrepresenting its identity. Strong authentication procedure is used to prevent this attack. There are two types of impersonation attacks:
  i. **Man In the Middle Attack:** in this attack the intruder ca impersonate the receiver with respect to the sender and sender with respect to the receiver without having either realize they have been attacked.
  ii. **Session Hijacking:** it consists of taking control of user's session after obtaining or generating an authentication session ID.

- **Attacks using modification:** the attacker illegally modifies the content of messages traveling from the source to destination. These attacks breaks the integrity control security function.

- **Attack using fabrication:** an attacker generate false messages in order to disturb network operation or to consume resources.
  i. **Reaction attack:** the attacker monitors the reaction of recipient to its forgeries

ISSN-2230-9659

ii. **Replay attack:** an attacker retransmits the same data to produce an unauthorized affect.

❖ **Denial of Service attack:** An attacker explicitly attempts to prevent legitimate user from using the system services. This type of attack affects the availability of the system.

Comparison of Bluetooth and Wireless LAN(802.11)

Comparison of characteristics:

Characteristics and issues	Bluetooth	Wireless LAN(802.11)
Communication Medium	Radio waves	Radio waves
Coverage range	10-90 meters	20-100 meters
Band	2.4 GHz ISM band	2.3 GHz ISM band
Network size	Maximum 8 devices	Dozens of devices
Maximum data rate	3 Mb/s	54 Mb/s

Comparison of security issues:

ISSN-2230-9659

Security Issues	Bluetooth	Wireless LAN(802.11)
Architecture	FHSS at 1600 hops/s	DSSS, FHSS
Authentication	Optional, enabled with WEP	Optional, enabled with link level or service level security
Encryption	40-bit RSA	128-bit (SAFER)
Error Handling	CRC-16 or CRC-32 with retransmission	Optional, FEC

Reference:

1. **C.E. Perkin and P.Bhagwat, "**High dynamic Destination sequence Distance Vector Routing**".**
2. **C.E. Perkin and P.Bhagwat "**Ad hoc On Demand Distance Vector Routing(AODV) Routing**",** IETF MANET working group INTERNET DRAFT. June 2002
3. **D.B Johnson, D.A Maltz, Y.C Hu, J.G Jacobson Jetcheva**, " Dynamic Source Routing for Mobile Ad hocc Networks(DSR). IETF MANET working group INTERNET DRAFT. February 2002

ISSN-2230-9659

4. **Eitan Altman and Tania Jimenez**, "NS Simulator For Beginners, Lecture Notes 2003-2004". Univ de Los Andes Merida Venezuela and ESSI, Sophia-Antipolis, France. December 4, 2003.
5. **William Stallings** [2000], *Network Security Essentials*: Security Attacks. Prentice Hall. (pp. 2-17)
6. **Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang** "Resisting Flooding Attacks in Ad Hoc Networks". Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (ITCC'05). 2005
7. **Anand Patwardhan, Jim Parker and Anupam Joshi.** "Secure Routing and Intrusion Detection in Ad Hoc Networks". [On-line] accessed on 6th November, 2005
8. **Yih-Chun Hu, David B. Johnson and Adrian Perrig. "**Secure Efficient Ad hoc Distance vector routing" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02). 2002
9. **Kimaya Sanzgir, Bridget Dahilly, Brian Neil Levine, Clay Shields, Elizabeth M and Belding-Royer** "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02). 2002
10. **Shahul Ahamed Ali Mohammad, Dr. Anca-Juliana, "**Evaluation of Mobile Ad hoc Secure Routing Protocols". February 2006