Security Issues in Bluetooth Technology - A Review

Menal Dr.*
Sumeet Gill**

Abstract

Bluetooth is a recently proposed standard for short range, low power wireless communication.Bluetooth Technology has become a popular way of wireless interconnection for exchanging messages, data and other information. Security concern is one of the most important problems behind the mass adoption of this technology. This paper provides a brief overview of security issues and weaknesses faced by the Bluetooth technology.

Keywords: Bluetooth technology, Bluetooth security, wireless communication

Introduction

Now a days the use of mobile computing networking increases day by day. People use mobile communication technology more than any other technology. Mobile networking is a pervasive communication platform where users obtain the desired information in seconds and increase the efficiency of work. Smartphones have a number of connectivity features like Bluetooth, wi-fi, RFIDetc. Currently Bluetooth is one of the most commonly uses wireless networking technology that quickly share information with each other at a speed of 1Mbps in basic mode within a 50 m range. Bluetooth is a short range, low power wireless communication technology, mostly integrated into mobiles and other devices. This technology combines the features of packet switching and circuit switching thereby supporting both connectionless and connection-oriented links. It was developed by Ericsson in 1994.The Bluetooth standard is managed and maintained by Bluetooth Special Interest Group. [1] IEEE has also adapted as the 802.15.1a standard. Bluetooth uses the unlicensed 2.4 GHz ISM (Industrial Scientific and Medical) frequency band. Bluetooth operates on 79 channels in the 2.4 GHz band with 1MHz carrier spacing. To make the link robust to interference, it employs a Frequency Hopping technique, in which the carrier frequency is changed at every packet transmission.Like any other wireless technology Bluetooth uses open air medium for transferring data that makes it involved with the security issues. There are several authentication, access control and encryption algorithm that plays major role in the security of wireless technology. Some devices have biometric access control while others have strong password protected systems. But there is no standard access control technique that makes data secure over air.

Bluetooth supports both unicast and mlulticast connections. Bluetooth protocol uses the concept of master and slave.In a master slave protocol a device cannot talk as when they desire. They need to wait till the time the master allows them to talk. The master and slaves together form a *piconet*. Up to seven "slave" devices can be set to communicate with a "master". Several of these piconets can be linked together to form a larger network in an ad hoc manner. The topology can be thought as a flexible, multiple piconet structure. This network of piconets is called *scatternet*.Figure 1 shows the basic piconet topologies.A scatternet is formed when a device from one piconet also acts as a member of another piconet. In this scheme, a device being master in one piconet can simultaneously be a slave in the other one. [2]

This paper is organized as follows. Section I describes the features of Bluetooth technology. Section

Menal Dr.*
Department of Computer Science
Maharaja Surajmal Institute
Janakpuri, New Delhi

Sumeet Gill**
Department of Mathematics
Maharashi Dayanand University
Rohtak, Haryana

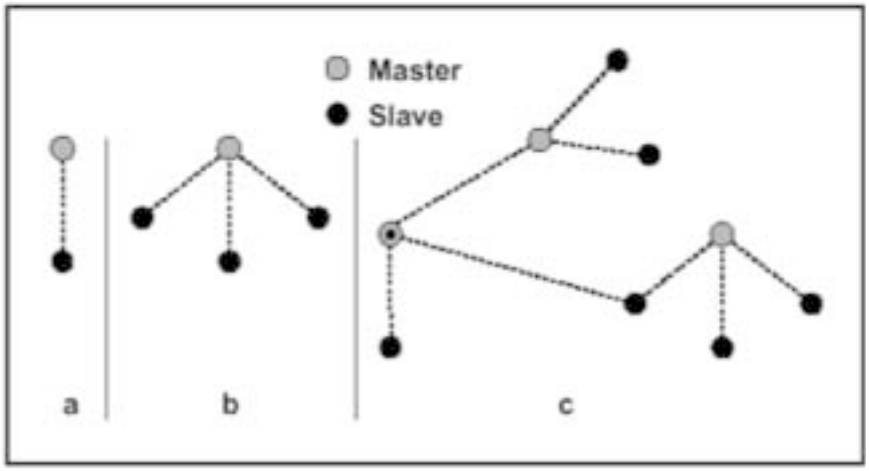

Fig.1 Piconets with master slave operations

IIexplains the Bluetooth architecture and protocols. In Section III,we discuss the security issues and challenges involved in Bluetooth technology. Section IV concludes the paper.

BLUETOOTH ARCHITECTURE AND PROTOCOLS

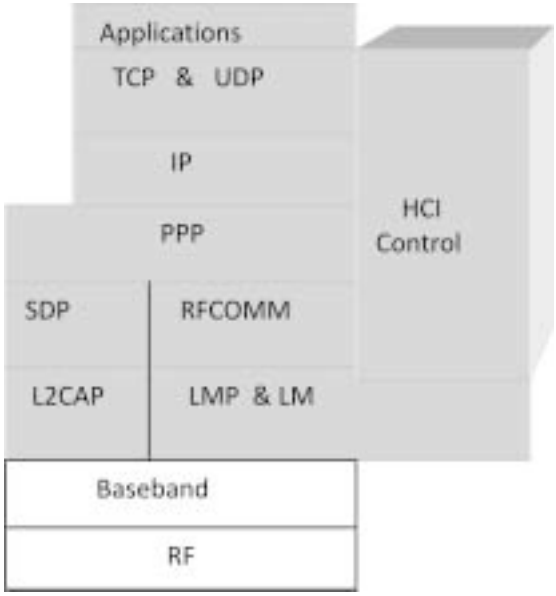

Fig. 2 Bluetooth Architecture

Personal Networking Hardware and the Protocol Stack Layers:

The Bluetooth Baseband Layer: The baseband layer performs functions like Bluetooth packet assembly, forward error correction (FEC), automatic repeat request (ARQ), data whitening, Bluetooth clock synchronization, and frequency hopping control.

The Bluetooth Link Manager Layer: The Link Manager forms the piconet by inquiring what other Bluetooth radios are in the area, establishing connection and maintaining the piconet. The Link Manager also handles security issues like authentication and encryption.

Radio: The Radio layer defines the requirements for a Bluetooth transceiver operating in the 2.4 GHz ISM band.

Baseband: This layer describes the specification of the Bluetooth Link Controller (LC) which carries out the baseband protocols and other low-level link routines. The Link Manager Protocol (LMP) is used by the Link Managers (on either side) for link set-up and control. The Host Controller Interface (HCI) provides a command interface to the Baseband Link Controller and Link Manager, and access to hardware status and control registers.

Logical Link Control and Adaption Protocol (L2CAP)

Supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.L2CAP, which adapts upper layerprotocols over the baseband, provides data services to the high layer protocols with group abstractions. The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol.

The protocol is based on the ETSI standard TS 07.10. The Service Discovery Protocol (SDP) provides a means for applications to discover which services are provided by or available through a Bluetooth device. Device information, services and the characteristics of the services can be queried using the SDP [2]. Fig 2 shows Bluetooth architecture

Bluetooth Security Issues

Attack to a wireless network is easier because information is zapping back and forth through the open air. In a wireless environment where every bit is on the air, security concerns are high.Security can be defined by three fundamental elements[4]:

Authentication: This service is used for verifying the identity of the communicating devices before being able to connect to the application. Native user authentication does not provided by the Bluetooth.

*Authorization:*This service allows the resources which are connected to Bluetooth for transmitting the data after an authorization procedure. Only the trusted devices allow to do so.

*Confidentiality:*This service ensures that only the authorized devices can share the application and then prevent from all kinds of eavesdropping.

Bluetooth does not address other security services such as audit, integrity, and non-repudiation.

Bluetooth Security Modes

Cumulatively, the BT versions up to 2.1 define four modes of security. Each of these versions supports some of these modes but none of them supports all four.

Security Mode 1

This mode is non-secure. It has the lowest security level. Mode 1 is only supported in earlier versions.

Security Mode 2 (Service-level Enforced)

Mode 2 is designed as a *service-level enforced security-mode*. In this mode communication is initiated after the establishment of the channel at L2CAP level. Security Mode 2 is supported by all Bluetooth devices.

Security Mode 3 (Link-level Enforced)

Mode 3 is designed as a *link-level enforced security-mode*. Here, all security measures take place before the communication link is fully established. Security Mode 3 is only supported in earlier devices.

Security Mode 4 (Service-level Enforced)

Similar to security Mode 2, this mode is enforced on the service level, after the physical link has been established.

Bluetooth Trust and Service Levels

In addition to the four security modes, two *trust levels* and three *service security levels*are provided in the Bluetooth. Two trust levels are *trusted* and *untrusted*. Devices which falls under trusted level have full permission to access all services provided by the connected devices while untrusted devices restricted for limited access.

For achieving authentication, encryption and authorization the three security levels are allowed to be defined . Available Service Security Levels depend on the security mode being used.

Bluetooth Service Security Levels:

Service Level 1

Trusted devices are allowed to connect automatically to all services after the completion of authentication and authorization.Untrusted devices need manual authorization for all services.

Service Level 2

At this level only authentication requires. After the authentication procedure service is accessed by the device.

Service Level 3

This service is open to all devices i.e. access is granted automatically with no authentication required.

Trust and service levels allow the definition of policies to set trust relationships and may also be used to initiate user-based authentication. Bluetooth core protocolsusually only provide device authentication. [3]

Analysis of Security Issues

As technology grows day by day new attacks are also being developed by the attackers. The weakness of the basic Bluetooth protocols involves the pairing process,

Table-1: Key Issues with Bluetooth Security

Security Issues	Description
Initialization key is too weak	Generate new initialization key scheme
PIN key is too short and default is all zero	Increase the length of PIN code
The master key used for broadcast encryption is shared among all piconet devices	Change broadcast scheme
Weak E_0 stream cipher	Replace the cipher with new advance technique
No user authentication	Application level security and employ user authentication
Encryption key length is negotiable encryption	Program each device to initiate 128 bit Bluetooth immediate after manual authentication
End to end security is not performed	End to end security can be provided by use of additional security controls
Security services are limited	Bluetooth does not address audit, integrity, and non-repudiation; if such services are needed, they should be provided through additional means.
The quality of pseudorandom number generators are not known	Bluetooth should use strong PRNGs based on standards
Unit keys are reusable and static for every pairing	Device uses same unit keys and link leys. This should be avoided using strong cryptographic management
Link keys can be stored improperly	Link keys can be modified if they are not securely stored

device address scheme and its wireless nature. Along with weaknesses, the Bluetooth specifications have several design issues also like how to decide which node become master, slave and bridges in a piconet, how many piconets a node should join and many others.

Table 1 provides an overview of some of the known security issues or vulnerabilities [5].

Conclusion

This paper was intended as a brief introduction to Bluetooth technology. It is one of the technologies that can be used for ad hoc networking and it uses widely among people due to its key features that includes robustness, low complexity, low power, and low cost. Since it is a wireless networking communication technology, so security is always a prior issue. This technology is still in research phase due to the security problems.

Bluetooth is by design a peer to peer network technology and typically lacks centralized administration and security enforcement infrastructure. The Bluetooth specification is very complex and includes support for dozens of data services. Because of these complexities and outside interconnection access,high level of security mechanism should be enforced. Various security issues that raises here can be reduced at a certain level using upcoming technologies. The future work would be focused on the improvement in the security schemes.

References

1. The official Bluetooth technology info site,http://www.bluetooth.com.
2. Talukder A,Ahmed H,Yavagal R R, *Mobile Computing*, 2nd edition.McGraw-Hill,2013,pp 84-90.
3. K. Scarfone and J. Padgette. \Guide to bluetooth security,". Tech. Rep., 2008.
4. T. C. Yeh, J. R. Peng, S. S. Wang, and J. P. Hsu, \Securing bluetooth communications," *International Journal of Network Security*, vol. 14, no. 4, pp. 229-235, 2012.
5. Padgette J., Scarfone K., Chen L."Guide to Bluetooth security"NIST Special Publication 800-121,June 2012.
6. Mandal B., Bhattacharyya D., Kim T., "A Design Approach for Wireless Communication Security in Bluetooth Network" Vol.8,No.2(2014), pp. 341-352, *"International Journal of Security and its Application"*