ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Bluetooth Hotspot

Pooja Abnave[1], Priyanka Patil[2], P.L.Himabindu[3], Prashant Dukare[4], S.S.Vanjire[5]

Student, Department Of Computer Engineering, University of Pune, Pune, India[1]

Student, Department Of Computer Engineering, University of Pune, Pune, India[2]

Student, Department Of Computer Engineering, University of Pune, Pune, India[3]

Student, Department Of Computer Engineering, University of Pune, Pune, India[4]

Assistant Professor, Department Of Computer Engineering, University of Pune, Pune, India[5]

Abstract: Bluetooth is a technology for short range wireless real-time data transfer between devices. It is becoming increasingly more prevalent in modern society, with technical gadgets now ranging from mobile phones and game controllers to PDAs and personal computers. Bluetooth hotspot is a technology which allows Bluetooth enabled mobiles (clients) to access the internet. With this technology mobile phones need not have a GPRS connection in it. Before accessing the internet Bluetooth mobiles (devices) need to be discoverable. The Bluetooth server discovers all devices in its range and sends a message for pairing. The connection link is established when an appropriate message is sent by the discovered device for pairing in response to the servers message. In this paper we will study how communication links are established, what are the security issues and how they are handled in Bluetooth and the data packet format.

Keywords: Eavesdropping; Ad-hoc network; Bluetooth Network; Bluetooth Security; Media Access

I. INTRODUCTION

Ad hoc networks today are based primarily on Bluetooth technology. Bluetooth is an open standard for short-range digital radio. It is touted as a low-cost, low-power, and low profile technology that provide a mechanism for creating small wireless networks on an ad hoc basis. Bluetooth is considered a wireless PAN technology that offers fast and reliable transmission for both voice and data. Untethered Bluetooth devices will eliminate the need for cables and provide a bridge to existing networks.

Two devices must have the same type of link in order to establish communication. The concept behind a Bluetooth communication is the use of "masters" and "slaves". The master device works as the moderator in the communication between itself and the slave devices as well as between the slave devices themselves. Bluetooth hotspot uses this master slave architecture were Bluetooth server acts as the master and other Bluetooth enabled mobile devices as slaves.

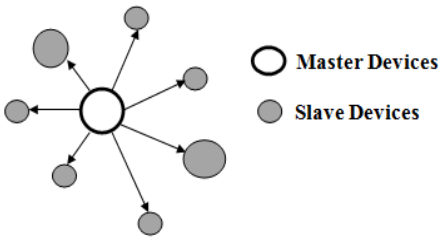

Fig. 1. Piconet master slave Bluetooth architecture

II. NEED

As the number of Bluetooth products increases each year, it is important to develop applications and services to take full advantage of their potential and capabilities. A broadband hotspot is one application where Bluetooth has a value in providing Internet access to mobile users. Consumers owning a Bluetooth enabled mobile phone can easily access a Bluetooth hotspot to browse the Internet without having to carry a PDA or a laptop.

Today, the majority of people are in possession of a mobile phone. The number of mobile phone users is increasing each year. Mobile phone creates more possibilities for social networking. The deployment of Bluetooth hotspots will widen access to broadband services using mobile phones not only to professionals and mobile workers but more importantly, to other segments of consumers who want to go on-line for non-business related and sociable purposes, and to consumers who do not own PCs.

III. BASIC STEPS

Steps to be followed in Bluetooth hotspot are:

- Connectivity
- Authentication and security
- Data transfer

In Bluetooth hotspot we require a Bluetooth server with internet connection in it, Any Bluetooth enabled mobile

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

which wants to be connected to Bluetooth server and use the services provided by it.

The process starts with connectivity process in which Bluetooth server sending a message of pairing to all the discoverable mobile devices in its range. As the services of Bluetooth hotspot are to be provided to authorized users various security issues like eavesdropping and false authentication are considered. The devices receiving the message need to send an appropriate response (passkey) to the server back to complete the authentication.

Now the connection link is established and the data/ file transfer can take place. Now the server sends the client program which needs to be installed on the mobile devices. After installation client requests for the web page which is queued at the server site and maintained by hotspot manager which keeps tracks of what request is made and who requests it. Now the request is taken out from queue one by one and requested page is fetched from internet. This page is now converted into mobile format by the HTML parser and sent to the appropriate client who requested it.

Now we will see in detail the connectivity, security and data transfer mechanisms in Bluetooth.

IV. CONNECTIVITY

Identification and authorization are the two important steps for having trusted connection between two Bluetooth devices. Connectivity is the first step for establishing any connection[5].This can be achieved by using two methods namely,

- Inquiry method (Inquiry function of Bluetooth)
- Communication link method (Monitoring communication link)

A. Inquiry method:

The inquiry method detects the user's presence by using the inquiry function. The Bluetooth device of the PC (master) gets the slave information of surrounding Bluetooth devices by running the inquiry function regularly. The PC then judges that the user is sitting in front of the PC if the acquired slave information indicates that the user's Bluetooth device is specified as an authentication key[5].

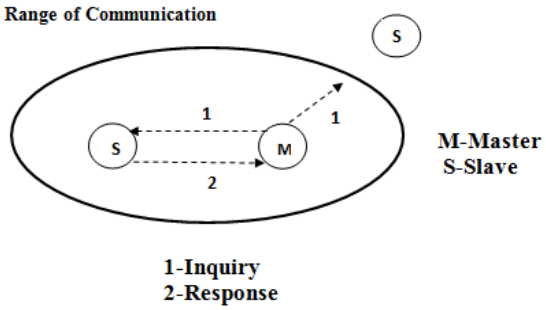

Fig. 2. Inquiry Method

B. Communication link method:

A communication link is data transmission connection between a master and slave for sending and receiving data packets.

The master sets up a communication link to a slave by using slave information when the master establishes a connection with the slave, and it controls data transmission to confirm whether the slave can communicate with it[5].

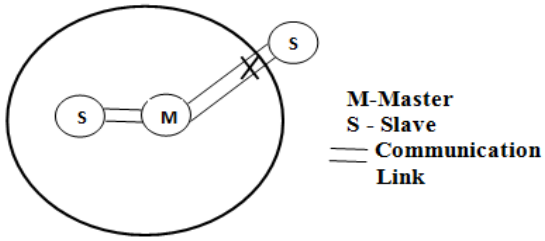

Fig. 3. Communication link Method

Due to some erroneous detection in the above methods they were improved and were renamed as:

- Advanced inquiry method,
- RSSI method.

A. Advanced inquiry method:

If the Bluetooth function of the PC (master) gets the slave information of the authentication key once within a set period of time, the advanced inquiry method judges that the user is sitting in front of the PC[5].

B. RSSI method:

RSSI (Received Signal Strength Indication): In telecommunications, RSSI is a measure of the power of a received radio signal; that is, RSSI quantifies the strength of a radio signal. In general, the value of RSSI decreases as the relative distance with a communication partner increases. RSSI can therefore be used as a measure for expressing relative distance with a communication partner[5].

In this method the PC begins to compare the RSSI value and the threshold value that was set for user. The PC judges that the user is sitting in front of the PC if the RSSI value is higher than the threshold value The communication link method can be finely controlled by comparing the RSSI and threshold values.

To develop a presence-detection system with high detection accuracy at modest cost, a presence-detection method using the received signal strength indication (RSSI) function of a Bluetooth device was developed. The performance of this method under various environmental conditions was evaluated by a simulator[5].

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

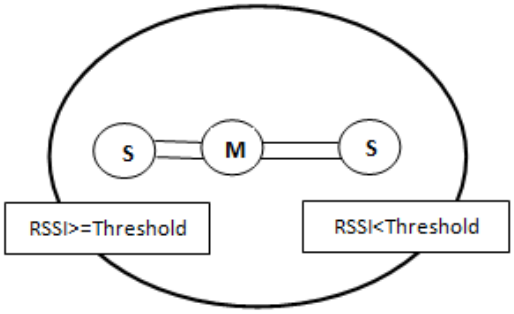

Fig. 4. RSSI Method

V. SECURITY

When a user sends data over a wireless network, he has a reasonable expectation that such data is not easily readable by unauthorized persons. Unlike a wired network, which requires a physical intrusion, wireless data packets can be received by anyone nearby with an appropriate receiver, potentially outside the physical security barriers of an organization.

There are basically two main security issues in wireless technology which are needed to be considered for trust building between two devices.

- Eavesdropping

Eavesdropping is the act of secretly listening to the private conversation of others without their consent.

- False authentication

The present system WI-FI hotspot has both these security issues. Now let us see how these issues are handled in Bluetooth technology.

Bluetooth technology provides a method for authenticating devices. Device authentication is provided using a shared secret between the two devices. The common shared secret is called a link key. This link key is established in a special communications session called pairing. All paired devices share a common link key. There are two types of link keys: unit keys and combination keys[1].

A device using a unit key uses the same secret for all of its connections. Unit keys are appropriate for devices with limited memory or a limited user interface. During the pairing procedure the unit key is transferred (encrypted) to the other unit. Note that only one of the two paired units is allowed to use a unit key.

Combination keys are link keys that are unique to a particular pair of devices. The combination key is only used to protect the communication between these two devices. Clearly a device that uses a unit key is not as secure as a device that uses a combination key. Since the unit key is common to all devices with which the device has been paired, all such devices have knowledge of the unit key. Consequently they are able to eavesdrop on any traffic based on this key[1].

Authentication is performed with a challenge response scheme utilizing the E1 algorithm. E1 is a modification of the block cipher SAFER+. The scheme operates as follows: The verifier issues a 128 bit long challenge. The claimant then applies E1 using the challenge, its 48-bit Bluetooth address, and the current link key. He then returns the 32 most significant bits of the128 bit result. The verifier confirms the response, in which case the authentication has succeeded. In this case, the roles are switched and the same procedure is applied again, there by accomplishing mutual authentication[1].

The Bluetooth challenge response algorithm differs from that used in 802.11b in very important ways. In 802.11b the challenge and response form a plaintext/cipher text pair. This fact, combined with the simplicity of the encryption method (XOR), allow an intruder to easily determine the authentication key string by listening to one authentication procedure. In contrast, the Bluetooth authentication method never transmits the complete challenge response pair. In addition, the E1 algorithm is not easily invertible. Thus even if an attacker has recorded an authentication challenge response session, he cannot (directly) use this data to compute the authentication key[1].

The known attacks on the E0 cipher used in Bluetooth are far more computationally complex then corresponding attacks on RC4 used in 802.11b. As yet, no practical direct attack has been reported[1].

The known attacks on 802.11b security have been discussed and found not to apply to Bluetooth wireless technology. In particular

i) 802.11b authentication is highly susceptible to impersonation by recording only one authentication procedure. This is facilitated because a plaintext/cipher text pair is transmitted. Bluetooth communications do not share this limitation.

ii) 802.11b encryption is not very secure. The RC4 implementation used in 802.11b has several well-known direct attacks. Currently known direct attacks on the Bluetooth encryption are computationally complex and of little practical value.

VI. DATA TRANSFER

Data is transferred using packets. To transfer data, a link needs to be established between the devices. i.e establishing a packet transport mechanism. One can start adding higher-level protocols such as the familiar Internet protocols IP, TCP, UDP and, on top of that, to name a few, HTTP and FTP. This eventually leads us back to the automatic file transfer implied by the scenario[4].

Between two (or more) Bluetooth devices two types of links can be established, namely:

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

- Synchronous Connection-Oriented (SCO) link

The SCO link is typically used for time-bounded data, such as voice. An SCO link is implemented by reserving time slots at a regular interval for data exchange.

- Asynchronous Connectionless Link (ACL)

The ACL link works as a traditional packet switched network. Packets are transmitted only when necessary.

A. Bluetooth Packet Format

The standard Bluetooth packet consists of three parts: the access code, the header and the payload

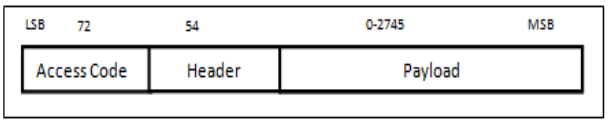

Fig.5 . Bluetooth packet format

i) *The Access Code:*

The 72-bit access code is mainly used to identify packets transmitted over a Bluetooth channel. All data packets sent on the channel share the same access code. In addition, the access code is used for device paging (finding out if a specific device is in range) and inquiries (used to discover new devices). A Bluetooth device monitors the access code of each packet; if the device is not directly or indirectly addressed, the rest of the packet is ignored .The access code is very fault-tolerant, so up to 6 bit errors can be corrected. The access code is also used to determine receiver timing[4].

ii)The Packet Header

The 18-bit packet header contains the following Information:

- A 3-bit target device address, which addresses an active device on the Bluetooth channel. A broadcast address is also provided.
- A 4-bit type code. Identifies the type of data or control packet.
- Fields for flow control, sequencing and packet acknowledgement.
- An 8-bit header CRC. To protect the header from transmission errors each bit is repeated three times in row (the Bluetooth spec refers to this as 1/3 FEC encoding) yielding a total length of 54 bits[4].

iii)The Packet Payload:

The payload part (0 to 2745 bits) of the packet carries the actual data. For ACL links, the payload begins with an 8-or 16-bit header, which indicates the length of the data packet and provides fields for logical channels and flow control. The header also supports fragmentation of data packets. The careful reader notices that during the Bluetooth time slot of 6.25mS you can send a maximum of 625 bits; how are then 2745 bit packets possible? The answer is that a packet may span up to five time slots, during which the channel frequency is kept constant[4].

B. Packet Types

Bluetooth supports a wide variety of packet type depending on the type of link, throughput and bit fault tolerance. On SCO links packets for low, medium and high quality voice as well as combined data and voice are supported. For ACL links 1, 3 and 5 slot packets using medium (5 check bits for each 10 bits) and high (no additional check bits) data rates are supported[4].

C. Media Access

With the term "media access" one understands the means and procedures used by a device to gain access to the transmission medium. On a Bluetooth channel media access is handled by dividing the time slots into two groups: master-to-slave and slave-to-master slots.

The master can only initiate transfer in even-numbered slots (the slots being numbered by the Bluetooth channel clock) and replies from the slave can only be transmitted in odd numbered slots. A slave may only transmit in the slave-to-master slot if it was addressed in the previous master-to-slave slot. It is up to the master to reserve enough slave-to-master channel capacity[4].

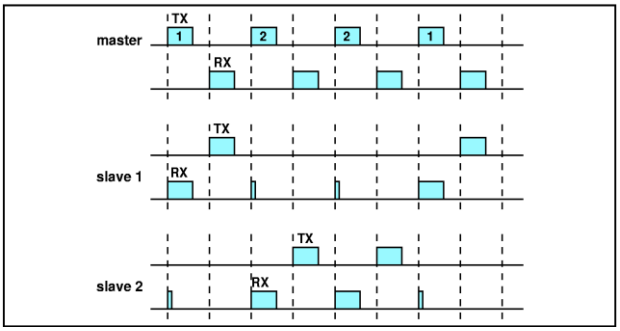

Fig. 6. Master/Slave transmits and receives timings

D. Packet Acknowledgement and Flow Control

When transmitting data or data/voice packets an unnumbered ARQ (Automatic Repeat Request) scheme is used. Such packets are retransmitted until an acknowledgement of successful reception is received, or a timeout occurs. The acknowledgement (either positive or negative) is piggy-backed onto the header of the return packet. A missing acknowledgement (e.g. the return packet was lost) is treated as a negative acknowledgement. In case of master-to-slave transmission, the return packet is sent in the subsequent time slot. When the slave transmits the return packet is received the next time the master addresses the slave[4].

In order to distinguish the cases when a packet was successfully received, but the acknowledgement was lost and successful acknowledgement, a 1-bit sequencing number is used. If a packet it resent, the sequence number is held; this way the recipient will detect duplicate packets. If the receive buffer fills up, a Bluetooth device may stop the transmission by resetting the FLOW field in the return packet. This "stop" signal does not affect control packets. If the return packet is not received, a "go" signal is assumed[4].

REFERENCES

[1] Thomas G. Xydis Ph.D, Simon Blake-Wilson. "Security Comparison: Bluetooth™ Communications vs. 802.11". Bluetooth Security Experts Group. 11-10-2001 revised 2-1-2002

[2] Bluetooth Special Interest Group.
https://www.bluetooth.org/About/bluetooth_sig.htm

[3] Nateq Be-Nazir Ibn Minar and Mohammed Tarique. "A Secured Bluetooth Based Social Network" published in International Journal of Computer Applications (0975 – 8887) Volume 26– No.1, July 2011.

[4] Tancred Lindholm. "Setting up a Bluetooth Packet Transport Link" Department of Computer Science,Helsinki University of Technology.

[5] Masataka Kikawa, Takashi Yoshikawa, Shinzo Ohkubo, Atsushi Takeshita, Yoh Shiraishi, and Osamu Takahashi. "A Presence-detection Method using RSSI of a Bluetooth Device". International Journal of Informatics Society, VOL. 2, NO. 1 (2010) 23-31.