BLUETOOTH TECHNOLOGY IN WIRELESS NETWORK USING BLUESOLEIL

BLUETOOTH TECHNOLOGY IN WIRELESS NETWORK USING BLUESOLEIL

ABSTRACT

In recent days, wireless communications play a vital role in data transmission; recent trends like **BLUETOOTH** are used to enhance voice and data sharing. The IEEE standards such as Ethernet does not provide reliable and efficient transactions in the network field because the implementation and the maintenance costs are very high. But **BLUETOOTH** makes it possible because it is a communication standard for short distance wireless communications, connecting electronic devices such as computers, peripherals and mobile and fixed-line telecommunications devices at speeds up to 1 mbps and distances up to 10 meters. The technology in its current iteration seeks to remove the need for cabling in office environments, an innovation that will have large benefits for commercial and home users of information technology equipment. The network connection can be made easily in bluetooth, in effect creates a piconet around a given user connection up to eight compatible appliances within a dynamic and mobile personal network. The **Network security** will also be high in it. So implementing Bluetooth in computer network is challenging technique.

In this paper we have implemented **BLUESOLEIL**-a software which describes the operation and functions of the Bluetooth device based on the network security with a small demonstration.

INTRODUCTION:

Authentication and security have been major issues right from the beginning of the computer age. At first the IEEE standards such as Ethernet are provided for the data transmission with the help of cables. In the Ethernet the implementation of network connections is very complex. So we go for the wireless communications. In the wireless communications security and the authentication is very important so we give more importance to security. The emerging and efficient technique for implementing network security in wireless communications is BLUETOOTH. It is one of the devices which can be used recently in the all communication areas. Bluetooth is a short-range radio technology aimed at simplifying communications among Internet devices and between devices and the Internet. The technology allows users to make effortless, instant connections between a wide range of communication devices.

DRAWBACKS OF IEEE802.11:

- Several attacks on IEEE802.11 have been described in media.
- WEP security framework used in IEEE802.11 is susceptible to both attacks on data content and user authentication.
- These exposures allow an attacker to both inappropriately intercept data and also gain access to a network by impersonating a valid user.
- Implementation of Ethernet is complex when compared to Bluetooth.
- The passwords can be guessed, stolen, or cracked.
- In some environments, users deliberately share passwords for their own convenience. So passwords may not be secured in such cases.
- Unlike 802.11b, Bluetooth is not intended to be solely an Ethernet wire replacement, but a general cable replacement technology.

BLUETOOTH DEFINITION:

Bluetooth is a communication standard for short distance wireless communications, connecting electronic devices such as computers, peripherals and mobile and fixed-line telecommunications devices at speeds up to 1 mbps and distances up to 10 meters.

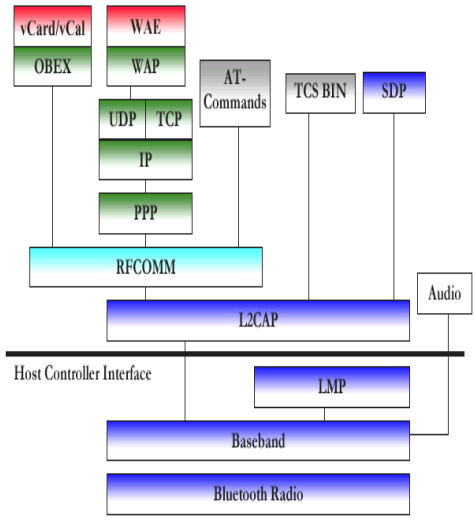
It is the name Bluetooth is the name for a short-range radio frequency (RF) technology that operates at 2.4 GHz and is capable of transmitting voice and data.

Bluetooth will facilitate wireless Local Area Networks in which networks of different handheld computing terminals and mobile terminals can communicate and exchange data, even on the move and when there is no line-of-sight between those terminals.

BLUETOOTH PROTOCOL ARCHITECTURE:

Bluetooth technology is designed for and optimized for use in mobile devices. Mobile computers, cellular handsets, network access points, printers, PDA's, desktops, keyboards, joysticks and virtually any other device can have short range. It uses Frequency Hop (FH) spread spectrum, which divides the frequency band into a number of hop channels.

The following figure shows the protocol architecture of the Bluetooth.



The complete Bluetooth protocol stack has been designed to include the existing protocols as much as possible (like TCP, UDP, OBEX) as well as Bluetooth specific protocols like LMP and L2CAP. The protocol reuse ensures smooth interoperability between existing applications and hardware. The Specification is also open, thereby allowing vendors to build proprietary applications. Although different applications may run over different protocol stacks, they all use the Bluetooth data link and physical layers. The Applications layer lies on top of the vCard (internal object representation convention) layer.

Baseband: The Baseband and Link Control Layer enables the RF link Bluetooth units in a piconet. This layer uses inquiry and paging procedures to synchronize the transmission between different Bluetooth devices.

Link Manager Protocol (LMP): The link manager protocol is responsible for setting up link channels between Bluetooth devices after performing security methods like authentication and encryption by generating, exchanging and verifying linking and encryption keys and negotiating base band packet size.

Logical Link Control and Adaptation Protocol (L2CAP): L2CAP packets carry payloads which are carried to the upper layer protocols.

Service Discovery Protocol (SDP): Using SDP, device information, services allowed and characteristics of the services are queried between Bluetooth enabled devices.

Cable Replacement Protocol (RFCOMM): RFCOMM is a serial line emulation protocol.

Telephony Control Protocol: The Telephony Control - Binary (TCS Binary) and Telephony Control - AT Commands are used to establish speech and data calls between devices and control mobile phones and modems respectively.

Adopted Protocols: Bluetooth also supports PPP, TCP/UDP/IP, and OBEX and WAP protocols to maximize interoperability.

The some of the features of the Bluetooth is as follows,

Topology	Supports up to 8 simultaneous links in a piconet
Flexibility	Goes through walls, bodies, clothes, ...
Data Rate	1 MSPS, 721 Kbps
Power	0.1 Watts active power
Size/Weight	25 mm × 13 mm × 2 mm, several grams
Cost	Long term $5 per endpoint
Range	10 meters or less; up to 100 meters with PA
Universal	Intended to work worldwide
Security	Very, link layer security, SS radio

BLUETOOTH NETWORK:

The network implementation is very easy when compared to the Ethernet because Bluetooth provides a wireless communication. The bandwidth of the Bluetooth is 2.9 GHz which is capable for transmitting data as well as voice. The Bluetooth hardware supports point to point as multipoint communications. One master and seven slaves can be active in a piconet. Piconet is a network which is termed in the Bluetooth for connecting eight devices such as laptop or mobiles in a single connection.

BLUETOOTH SECURITY:

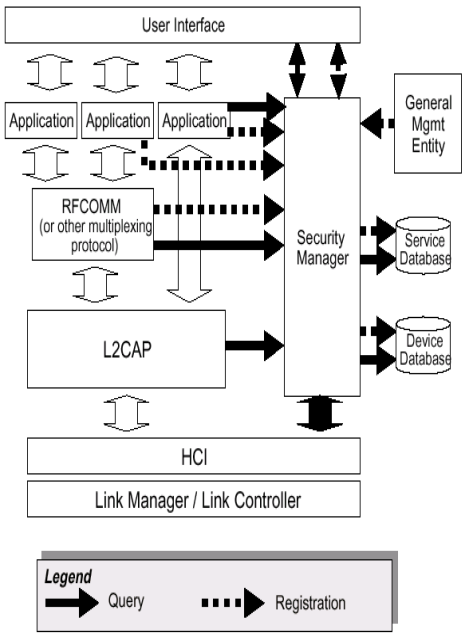
Security is a challenge faced by every communications standard. Wireless communications present special security challenges. Bluetooth builds security into its model on several different levels, beginning with the security inherent in its frequency-hopping scheme. At the lowest levels of the protocol stack, Bluetooth uses the publicly available cipher algorithm known as SAFER+ to authenticate a device's identity. The generic-access profile depends on this authentication for its device-pairing process. This process involves creating a special link to create and exchange a link

key. Once verified, the link key is used to negotiate an encryption mode the devices will use for their communication. Bluetooth is extremely secure in that it employs several layers of data encryption and user authentication measures. Bluetooth devices use a combination of the Personal Identification Number (PIN) and a Bluetooth address to identify other Bluetooth devices. Data encryption (i.e., 128-bit) can be used to further enhance the degree of Bluetooth security. The transmission scheme (FHSS) provides another level of security in itself. Instead of transmitting over one frequency within the 2.4 GHz band, Bluetooth radios use a fast frequency-hopping spread spectrum (FHSS) technique, allowing only synchronized receivers to access the transmitted data.

SECURITY ARCHITECTURE:

The general Bluetooth security architecture is shown in Figure.

Bluetooth security implementation is based on a challenge-response system using the passkey (PIN) as the secret key. The Security Manager (key unit) performs the following tasks:



Bluetooth Security Architecture

- Stores security related information for services (Service Database);
- Stores security related information for all available devices in range (Device Database);
- Processes access requests by protocol implementations or applications (grants access or denies connection);

- Enforces authentication and/or encryption before connection can be established;
- Initiates and processes input from a device user (called External Security Control Entity (ESCE) - a human operating a device) to setup trusted relationship;
- Initiates pairing and queries PIN (PIN entry may be done by an ESCE or an application).

For connection-oriented L2CAP data (setup to connect to the next higher protocol or application) security check is performed at the onset of the request while for connectionless data packets the Security Manager checks the Service Database (for services that does not allow connectionless packets) to decide whether the packet will be allowed or denied.

SECURITY LEVELS:

Bluetooth specifications include authentication (uni- and bi-directional) and encryption services at the link level using the Link Manager Protocol (LMP). Authentication between a pair of devices is based on a secret link key that is generated by a pairing procedure when the two devices communicate for the first time. There are three security modes defined:

- Security Mode 1 (non-secure): No security procedures are performed;
- Security Mode 2 (service level security): Security procedures initiated after channel establishment request has been received at L2CAP level. Whether security procedure is initiated or not depends on the service type. Service (or application) level security implementation allows different access policies for different applications which may run in parallel.

- Security Mode 3 (link level security): Security procedures are performed and authenticated at the LMP level before a channel is created for communication. A Bluetooth device in security mode 3 may reject a host connection request best on host settings

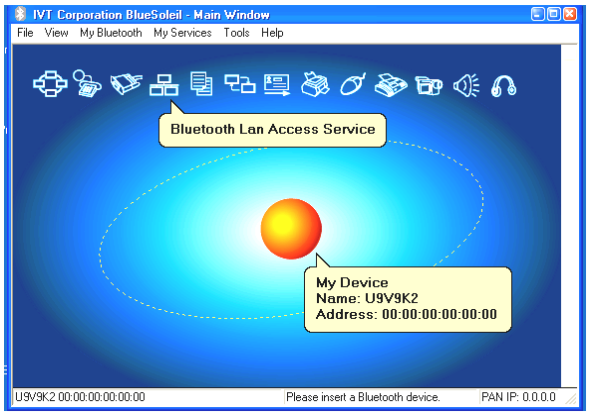
Services are also classified as - (1) services that are open to all devices; (2) services that require authentication only; and (3) services that require both authentication and authorization. While automatic access is only granted to trusted devices, all other

devices need manual authorization. A link may be changed to encrypted mode if required by the service or application.

BLUESOLEIL:

Bluesoleil is window based software that allows your *Bluetooth*® enabled desktop or notebook computer to wirelessly connect to other Bluetooth enabled devices. BlueSoleil allows MS Windows users to wirelessly access a wide variety of Bluetooth enabled digital devices, such as cameras, mobile phones, and headsets, printers, and GPS receivers. You can also form networks and exchange data with other Bluetooth enabled computers or PDAs.

Here we are going to explain about the LAN (Local Area Network) connection with the help of Bluesoleil. The main window of the bluesoleil software is as shown below.



LAN ACCESS:

The Bluetooth LAN Access Profile (LAP) allows users to access a Local Area Network (LAN) via a Bluetooth enabled LAN access point.

Typical Usage:

- Accesses a Local Area Networking via a Bluetooth enabled LAN access point.
- Use your computer as a LAN Access Point.

Access a LAN via a Bluetooth enabled Access Point (AP)

- Connect to the LAN AP's LAP service.
- In the **Connect Bluetooth LAP Connection** dialog, enter the user name and password if necessary. Click **Connect**.

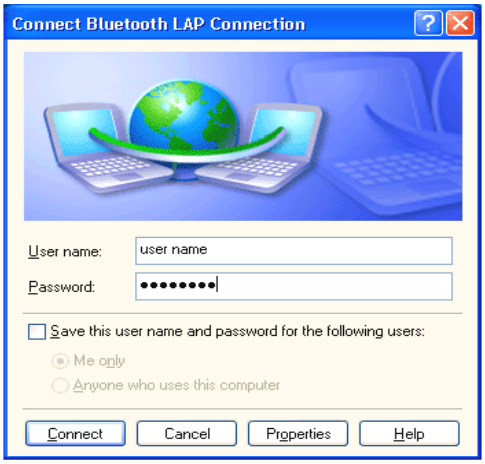


Figure 1 Connect Bluetoot*h* LAP Connection

Use your computer as a LAN Access Point (Advanced Users Only)

- Start the Bluetooth LAP Access service on BlueSoleil.
- Specify any static IP addresses for LAP clients (Alternatively, you can use DHCP to have the system dynamically assign IP addresses).

  (1) In the **Network Connections** window, right click **Incoming Connection**, then select **Properties on the popup menu.**

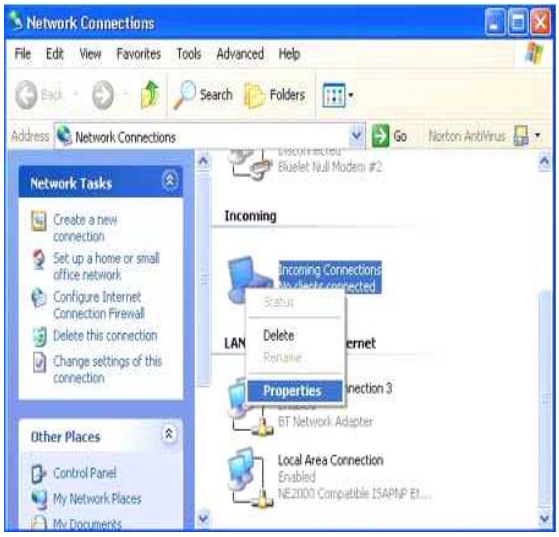
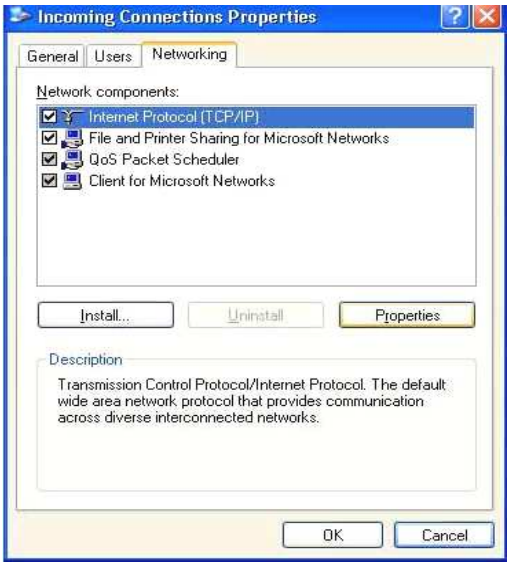


Figure 2 : Select Properties On the Pop-up Menu

(2) Select **Incoming Connections Properties | Networking** -> **Internet Protocol (TCP/IP)**, and click on the **Properties** button. (Figure 3)

Figure 3 : Internet Protocol (TCP/IP) Network Component



3) Select **Specify TCP/IP addresses** and enter the range of IP addresses assigned to LAP clients.

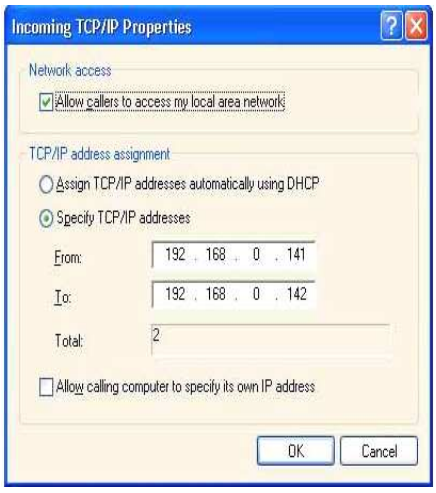


Figure 4 : Enter the IP Addresses Thus we can get the LAN connection in wireless communication using Bluetooth with the help of Bluesoleil.

BLUETOOTH ADVANTAGES:

- The synchronization and exchange of data are Bluetooth's major applications, as are electronic commerce applications such as electronically paying for parking meters, bus tickets, shopping bills, movie tickets and so on.
- Smart offices are envisaged in which an employee with a Bluetooth device is automatically checked in when entering the building and this triggers a series of actions such as lights and PCs being switched on.
- Home equipments, automotive components and entertainment devices can be interfaced together using Bluetooth technology.
- According to the Bluetooth partners one of its main advantages is the feature that it does not need to be set up.

BLUETOOTH APPLICATIONS:

- Wireless networking between desktops and laptops, or desktops in a confined space and where little bandwidth is required
- Bluetooth cell phones have been sold in large numbers, and are able to connect to computers, personal digital assistants (PDAs), certain automobile handsfree systems and various other devices. The standard also includes support for more powerful, longer-range devices suitable for constructing wireless LANs.
- Transfer of files (images, mp3s, etc) between mobile phones, Personal digital assistants (PDAs) and computers via OBEX nes
- Bluetooth car kits — Acura, with the 2004 Acura TL, was the first motor vehicle manufacturer to install handsfree Bluetooth technology Companies like Parrot or Motorola manufacture Bluetooth hands-free car kits for well-known brand car manufacturers.

The Future of Bluetooth:

The next version of Bluetooth, currently code named Lisbon, includes a number of features to increase security, usability and value of Bluetooth. The following features are defined:

- **Atomic Encryption Change** - allows encrypted links to change their encryption keys periodically, increasing security, and also allowing role switches on an encrypted link.
- **Sniff Sub rating** - reducing the power consumption when devices are in the sniff low power mode, especially on links with asymmetric data flows. HId devices are expected to benefit the most with mice and keyboards increasing the battery life from 3 to 10 times those currently used.
- **QoS Improvements** - these will enable auto and video data to be transmitted at a higher quality, especially when best effort traffic is being transmitted in the same piconet.
- **Simple Pairing** - this improvement will radically improve the pairing experience for Bluetooth devices, while at the same time increasing the use and strength of security. It is expected that this feature will be significantly increase the use of Bluetooth.

CONCLUSION:

Bluetooth offers a very high network security in the wireless communications. So when compared to the Ethernet the cost and the implementation is very low in it. The future can give highly advanced technology with large coverage area in the communication field. So the usage of bluetooth can be raised heavily than any other devices in the wireless communication. Bluesoleil is one of the important software to access the bluetooth device operations. The usage of this software is raised because of it’s high security in the voice and data transmission. The passkeys which are provided by this software cannot be easily deleted or cracked by the hackers. So inorder to provide LAN connection will be secured in it

REFERENCES: