Abstract: Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, building personal area networks (PANs). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization [7]. Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 19,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. Bluetooth was standardized as IEEE 802.15.1, but the standard is no longer maintained. The SIG oversees the development of the specification, manages the qualification program, and protects the trademarks. To be marketed as a Bluetooth device, it must be qualified to standards defined by the SIG. A network of patents is required to implement the technology, which is licensed only for that qualifying device [8].

I. INTRODUCTION

Bluetooth (BT) wireless technology provides an easy way for a wide range of devices to communicate with each other and connect to the Internet without the need for wires, cables and connectors. It is supported and used in products by over 3000 companies, including large corporations such as Sony Ericsson, Nokia, Motorola, Intel, IBM, Toshiba, Motorola, Apple, Microsoft, and even Toyota, Lexus and BMW. A variety of products available on the market have short range Bluetooth radios installed, including printers, laptops, keyboards, cars and the most popular type of Bluetooth enabled devices - mobile phones, driving 60% of the Bluetooth market. The technology has already gained enormous popularity, with more than 3 million Bluetooth-enabled products shipping every week. According to IDC, there will be over 922 million Bluetooth enabled devices worldwide by 2008. The technology seems to be very interesting and beneficial, yet it can also be a high threat for the privacy and security of Bluetooth users[2].

The idea behind Bluetooth technology was born in 1994, when a team of researchers at Ericsson Mobile Communications, led by Dr. Jaap Haartsen and Dr. Sven Mattisson, initiated a feasibility study of universal short-range, low-power wireless connectivity as a way of eliminating cables between mobile phones and computers, headsets and other devices. It was later developed into the Bluetooth technology we know today by the Bluetooth Special Interest Group (SIG), an industry association which was announced in May 1998 and formally founded in September 1998. The founding members were Ericsson, IBM, Intel, Nokia and Toshiba, and later in December 1999, 3Com Corporation, Lucent Technologies, Microsoft Corporation and Motorola Inc. joined the Bluetooth SIG.

After years of development the final Bluetooth technology uses the free and globally available 2.4GHz Industrial-Scientific-Medical (ISM) radio band, unlicensed for low-power use, and allows two Bluetooth devices within 10-100 m range to share data with throughput up to 723.2 Kbps, or 2.1Mbps with the new Enhanced Data Rate specification already released in 2005. Each device can simultaneously communicate with up to seven other devices per piconet. Bluetooth technology is also intended to be secure by providing authentication, encryption, quality of service (QoS) control and other security features. However, it will be shown that Bluetooth is vulnerable in a number of ways, opening the door for many malicious attacks now and in the future.

[Source: Mettala, 1999]

<table>
<thead>
<tr>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCS, SDP, RFCOMM</td>
</tr>
<tr>
<td>L2CAP</td>
</tr>
<tr>
<td>HCI</td>
</tr>
<tr>
<td>LMP</td>
</tr>
<tr>
<td>Baseband</td>
</tr>
<tr>
<td>Radio</td>
</tr>
</tbody>
</table>

Bluetooth protocol stack [9]
The common uses of BT technology nowadays include:

- Using a wireless mobile phone headset during a call while keeping a phone in the bag
- Synchronizing a calendar, phone book and other information between a PDA and a PC
- Connecting a printer, keyboard, or mouse to a PC without cables
- Transferring photos or ring tones between mobile phones

The technology is also constantly being examined and updated in order to make it faster, more secure, and cheaper with additional functionality.

Bluetooth allows a maximum of one master and seven active slaves to communicate together in one network called a piconet. A piconet can also support 256 „parked” slaves that maintain contact with the master but do not participate actively in network communication. These slaves can become active members if requested by the master when an available active slave resource becomes available. This allows a large number of devices to communicate successfully within a given range. Bluetooth also supports communication between piconets to form what is known as a scatternet. In scatternet formation, a master in one piconet can be a slave in another piconet. It will then split its network time between both networks.  

II. BLUETOOTH ARCHITECTURE

The architecture of the Bluetooth technology is divided into several layers, varying in their functions and illustrated.

**Radio Frequency (RF) Layers**

The radio layer is the physical wireless connection. In order to reduce collisions with other devices using the ISM range, the radio uses frequency mapping to separate the range into 79MHz bands, starting at 2.402GHz and stopping at 2.480Hz and uses this spread spectrum to hop from one channel to another, up to 1600 times per second.

**Base band layer**

The base band allows the physical connection between devices. It is responsible for controlling and sending data packets over the radio link. When a Bluetooth device connects to another Bluetooth device, they form a small network called a piconet. A piconet is a small network of Bluetooth devices, where every device in the network can be in one of the following states.

**Master:** The Bluetooth device that initiates communication. The master sets the time and broadcasts its clock to all slaves providing the hopping pattern, in which they hop frequency at the same time.

**Slaves:** The state given to all devices that are connected to another. The device can be an active slave if it natively transmits or receives data from the master, or a passive slave if it is not currently sending or receiving any information. The passive slaves check if there is a connection request from the master by enabling their RF receivers periodically.
Standby: All devices that are not connected to a master (i.e. not slave) are called standby devices. When searching for other devices, a device enters the inquiry state. When a device starts creating a Bluetooth link, it enters the page state. Also a device can go to a low power mode to save power.

**Link 2 Manager Protocol (LMP)**

The LMP protocol uses the links set up between devices by the base band to establish logical connection responsibilities of the LMP. It also includes security aspects and device authentication.

**Logical Link Control and Adaptation Protocol (L2CAP)**

The L2CAP is responsible for receiving applicative data from the upper layers and translates it to the Bluetooth format so that it can be transmitted to the higher layer protocol over the base band.

**Radio Frequency Communication Protocol (RFCOMM)**

The RFCOMM is used to emulate serial connections over the base band layer to provide transport capabilities for upper level services and avoiding direct interface of the application layer with L2CAP.

**Service Discovery Protocol (SDP)**

The SDP protocol is used to discover services, providing the basis for all the usage models.

**Telephony Control and Signaling layer (TCS)**

The TCS protocol defines the call control signaling for the establishment of speech and data calls between Bluetooth devices. TCS signaling messages are carried over L2CAP.

**Application Layer**

The application layer contains the user application. The applications interact with the RFCOMM protocol layer to establish an emulated serial connection\[6\].

![Functional architecture of the interpiconet scheduling function (IPSF) and its relation to other functions in a generic Bluetooth unit.](image)
III. BLUETOOTH OPERATION

Nodes are organized in small groups called piconets. Every piconet has a leading node called master,” and other nodes in a piconet are referred to as “slaves.” A node may belong to multiple piconets, and we refer to such a node as a “bridge.” A piconet can have at most 7 members. Every communication in a piconet involves the master, so that slaves do not directly communicate with each other but instead rely on the master as a transit node. In other words, Bluetooth provides a half-duplex communication channel. Communication between nodes in different piconets must involve the bridge nodes. A bridge node cannot be simultaneously active in multiple piconets. It is active in one piconet and “parked” in others. Bluetooth allows different activity states for the nodes: active, idle, parked, sniffing. Data exchange takes place between two nodes only when both are active. Activity states of nodes change periodically.

The nodes are organized into 3 piconets. The masters of these piconets are M1; M2; M3 respectively. The remaining nodes are the slave nodes or bridge nodes. Slave nodes S1 and S2 can communicate via master M1: Nodes S1 and S3 can communicate via master M1; bridge B and master M2[1]. Bluetooth uses frequency hopping spread spectrum in the physical layer. Different piconets use different frequency hopping sequences. The frequency hopping sequence of a piconet is derived from the node id and the clock information of the master. A node thus needs to know the identities and the clock information of the masters of all the piconets it participates in. It acquires this information from the master when it joins the piconet. Synchronization information is also exchanged periodically.

The bandwidth of the Bluetooth communication channel is currently 1 Mbps. Nodes in different piconets can transmit simultaneously even if they are within transmission range of each other. This is because they use different frequency hopping patterns. However, there can be only one communication at a time within a piconet and this communication involves the master and one slave. The master decides the communication order (and duration) for the slaves.

Besides the operation and constraints associated with the Bluetooth communication channel, another key aspect in the context of adhoc networking is the piconet formation process. A node discovers the nodes in its vicinity through the periodic use of an inquiry process that involves transmission using a well-known frequency hopping sequence. The inquiry process has two main states: A transmit state and a scan state. In the transmit state, a node continuously transmits its identity as it hops on the different frequencies of the inquiry hopping pattern. Transmission on each frequency is followed by a short listening period to determine if any node is responding to the inquiry. Nodes will be able to respond if at the time they have their receiver tuned to the frequency of the hopping sequence currently used by the transmitter. However, because there is no coordination between nodes, there is no guarantee that two nodes engaged in the inquiry process will be able to hear each other. For one, they could both be in either transmit or scan mode. Furthermore, even when one is transmitting and the other listening, their lack of clock synchronization means that they may not be using the same frequency at the same time. Thus, in order to facilitate synchronization, the sender hops through the frequencies of the frequency hopping sequence faster than the receiver. Once the receiver has learned the identity of a new node as a result of the inquiry process, it transmits its own identity. Subsequently, if either one of the two nodes decides to involve the other in a piconet in which it is the master, it pages for the other node. The paging message is transmitted on a frequency hopping sequence intended for paging, and is derived from the address of the desired recipient. If the paged node is scanning the same frequency as that on which the paging node is transmitting, then the two synchronize and the recipient receives the information required to join the piconet. Once again the transmitter switches frequencies at a faster rate than the receiver to facilitate the synchronization. Once two nodes belong to the same piconet, their clocks are synchronized and they use the same frequency hopping sequence to exchange information[7].
IV. CHALLENGES

The usage models described above require various system requirements to be met. In this section, we review several requirements and the challenges they offer.

A. Support for both voice and data

The air protocol must support good quality real-time voice, where “good” is considered to be wired phone line quality. Voice quality is important to both end-users who are accustomed to it, and for speech recognition engines whose accuracy depends on it.

B. Able to establish ad hoc connections

The dynamic nature of mobility makes it difficult to make any assumptions about the operating environment. Bluetooth units must be able to detect other compatible units and establish connections to them. A single unit must be able to establish multiple connections in addition to accepting new connections while connected. Ignoring a new connection request while connected is confusing to the user and deemed unacceptable, especially if we want to support unconscious computing while retaining the ability to perform interactive operations.

C. Able to withstand interference from other sources in an unlicensed band.

The Bluetooth radio operates in the unlicensed 2.4 GHz band where many other RF radiators are expected to exist. The fact that microwave ovens operating at this frequency is one reason why this band is unlicensed in most countries. The challenge is to avoid significant degradation in performance when other RF radiators, including other personal area networks in nearby use, are in operation.

D. Worldwide use

Not only are “standard” cables equipped with a variety of connectors, different standards exist in different geographical locations throughout the world. Experienced mobile travelers are accustomed to carrying around a number of different power, phone, and network connectors. The challenge here is very regulatory in nature with many governments having their own set of restrictions on RF technology. And while the 2.4 GHz band is unlicensed through most parts of the world, it varies in range and offset in a number of different countries.

E. Similar amount of protection compared to a cable

In addition to the radio’s short-range nature and spread spectrum techniques. Bluetooth link protocols also provide authentication and privacy mechanisms. Users certainly don’t want others listening in on their conversations, snooping their data transmissions, or using their cellular phones for Internet access.

F. Small size to accommodate integration into a variety of devices
The Bluetooth radio module must be small enough to permit integration into portable devices. Wearable devices in particular, such as mobile phones, headsets, and smart badges have little space to spare for a radio module.

**G. Negligible power consumption compared with the device in which the radio is used.**

Many Bluetooth devices will be battery powered. This requirement implies the integration of the Bluetooth radio should not significantly compromise the battery lifetime of the device.

**H. Encourage ubiquitous deployment of the technology.**

To achieve this goal, the SIG is designing an open specification defining the radio, physical, link, and higher level protocols and services necessary to support the usage models in the vision. The Specification will be made available under favourable adoption terms, including royalty free, to SIG members. Thus, the major challenges before Bluetooth technology are robust and efficient security system, vendor independence and application interoperability and quality of service.

**V. BLUETOOTH SECURITY**

Security for Bluetooth is provided on the radio paths, which means that link authentication and encryption may be provided, but true end-to-end security is not possible without providing security solutions for the higher layers of Bluetooth. Basically, Bluetooth addresses the three security services:

**A. Confidentiality:**

The first goal of Bluetooth is confidentiality or privacy. This service prevents an eavesdropper from reading critical information. In general, with this security service only the authorized user can access the data.

**B. Authentication:**

Providing identity verification of the communicating devices is the second goal of Bluetooth. Authentication allows the communicating devices able to recognize each other; hence communication aborts if the user is not authorized.

**C. Authorization:**

The third goal of Bluetooth is to control access to the resources. This is achieved by determining the users who are authorized to use the resources.

**Keys used in Bluetooth security**

**A. Unit Keys:**

The authentication and encryption mechanisms based on unit keys are the same as those based on combination keys. However, a unit that uses a unit key is only able to use one key for all its secure connections. Hence, it has to share this key with all other units that it trusts. Consequently, all trusted devices are able to eavesdrop on any traffic based on this key. A trusted unit that has been modified or tampered with could also be able to impersonate the unit distributing the unit key. Thus, when using a unit key there is no protection against attacks from trusted devices [15].

**B. Combination Keys:**

The combination key is generated during the initialization process if the devices have decided to use one. Both devices generate it at the same time. First, both of the units generate a random number. With the key generating algorithm E21, both devices generate a key, combining the random number and their Bluetooth device addresses. After that, the devices exchange securely their random numbers and calculate the combination key (Kab ) to be used between them as shown in Fig 2.
C. Encryption keys:

The encryption key is generated from the current link key, a 96-bit Ciphering Offset Number (COF) and a 128-bit random number. The COF is based on the Authenticated Ciphering Offset (ACO), which is generated during the authentication process. When the Link Manager (LM) activates the encryption, the encryption key is generated. It is automatically changed every time the Bluetooth device enters the encryption mode.[3]

VI. BLUETOOTH THREATS

A. Bluesnarfing

It is a method of hacking into a Bluetooth-enabled mobile phone and copying its entire contactbook, calendar or anything else stored in the phone’s memory.

B. Man in the Middle Attacks

In a man in the middle attack, an attacker seeking (unauthorized) access to a Bluetooth device inserts himself “in between” two authorized devices. Communications between the two devices then pass through the man in the middle, who intercepts and manipulates data packets.

First Bluetooth virus, Series 60 affected Jun 15 2004: Symantec warns of a worm for Series 60 mobile phones that transmits itself through Bluetooth. It's just a proof-of-concept (doesn't do any damage), but it's a scary concept.

C. Virus:

METAL Gear.a for Series 60 Dec 21 2004: Another new security notice for Series 60 owners--avoid a file claiming to be the game Metal Gear Solid with the file name METAL Gear.sis[3].

VII. CONCLUSION

By developing the Specification for a low-cost, low-power radio-based cable replacement, the Bluetooth SIG hopes to drive an evolution in personal networking. A very key characteristic of Bluetooth that differentiates it from other wireless technologies is that it enables combined usability models based on functions provided by different devices[11]. Some telecommunication sector Bluetooth implementations have exhibited fundamental flaws discovered and highlighted by common users. Bluetooth’s security may be considered adequate for small ad-hoc networks, such as a connecting a...
PDA to a mobile phone, but for larger ad-hoc networks, carrying sensitive information like in-vehicle messages relating to ignition systems, lock systems and immobiliser systems, Bluetooth security is insufficient on its own. Even after the basic Bluetooth security issues have been corrected, more sophisticated security methods need to be implemented on the upper levels of software that run on the Bluetooth stack. The security specification only considers Bluetooth device authentication and not the more functional, user authentication. Security must be built above the defined Bluetooth security measures. This includes the use of better authentication systems using possible distributed secret PIN schemes, predefined trust relationships, defined and known only by the automotive designers and engineers, allowing Bluetooth to be a securely integrated wireless automotive technology of the future.

VIII. SECURITY TIPS

- Enable Bluetooth only when you need it.
- Keep the device in non-discoverable (hidden) mode.
- Use long and difficult to guess PIN key when pairing the device.
- Reject all unexpected pairing requests.
- Update your mobile phone firmware to a latest version.
- Enable encryption when establishing BT connection to your PC.
- Update your mobile antivirus time to time to keep pace with the new emerging viruses and Trojans.

IX. ACKNOWLEDGEMENT

I would like to thank Mr. Sukhwinder sir for showing us the right directions to move forward giving us valuable ideas, Suggestions and giving me the opportunity to present the review paper. I would also like to thank my parents and friends for their invaluable assistance.

REFERENCES

[4]. Pauric Doherty, Alan Molloy, Martin Glavin, Fearghal Morgan Department Of Electronic Engineering, National University Of Ireland, Galway Galway,ISSC 2004, Belfast, IRELAND.
[5]. (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (2) Trishna Panse, Vivek Kapoor Department of Information Technology, Devi Ahilya Vishwavidyalaya Institute of Engineering & Technology, Indore, India.
[6]. Per Johansson Ericsson Research Manthos Kazantzidis, Rohit Kapoor, Mario Gerla Computer Science Department, UCLA
[8]. https://www.bluetooth.org/About/bluetooth_sag.htm Retrieved 2011-05-03
[9]. Naveen Erasala, David C. Yen, Department of Decision Sciences and Management Information System, Miami University, Oxford, OH 45056, USA.