Advancement in Bluetooth Technology

ANIKET JAIN [1], DURGESH KUMAR [2]
[1,2]*Dept. of Electronics & Communication Engineering, Poornima College of Engineering, Jaipur*

Abstract -- Bluetooth is broadly utilized as a short range information interchanges stage for associating numerous gadgets from cell phones to earphones, and PC mice to PCs for some, applications including music and sound spilling. It helps in trading information over short separations utilizing short-wavelength UHF radio waves from settled and cell phones. This is in the all-around unlicensed industrial, scientific and medical (ISM) 2.4 GHz short-go radio recurrence band. It additionally depicts the practical review and utilization of Bluetooth and manages the improvement of a model for recording, printing, checking, and controlling of eight process factors in the meantime, utilizing an appropriated control framework. The gadgets utilize a radio communicate correspondences framework, they don't need to be in the visual observable pathway of each other.

Indexed Terms -- Bluetooth, Network, Wireless Communication, Gadgets, Media, Radio Bands, Frequency, Equipment, Transmission, Piconet, Scatternets, and Technology.

I. INTRODUCTION

We as a whole have encountered the bother that emerges when we begin associating peripherals to a PC, or when we interface other electronic gadgets, with a lot of links that ends up hard to control. At that point, we begin to figure how simple it would be if every one of these associations was finished utilizing an alternate route from the physical links, as infrared, radio or microwaves. The organizations of software engineering and broadcast communications expected to create an opened, ease interface to make less demanding the correspondence between gadgets without utilizing links. This is the starting point of the innovation which key name is "Bluetooth". This is a reality these days, yet now another issue emerges and is that there is a considerable measure of norms and innovations, inconsistent between them. What we require now is an all-inclusive, substantial gadget for the association of a wide range of fringe, and that works straightforwardly for the client. This is Bluetooth. Inverse to other current innovations, similar to infrared advanced by the IrDA (Infrared Data Association) or DECT, Bluetooth has the help of the business of software engineering and broadcast communications, which somehow ensures the achievement. In spite of the fact that there is a high number of makers who consolidate the interface IrDA in their phones, including Ericsson, Motorola, and Nokia, the utilization ends up being baffling for some clients who treat without progress to download data from their PC or PDAs to their cell phones, or the other way around. The gadgets that Bluetooth fuses are perceived and talk each other similarly as a PC does with the printer. The low cost of these items implies that the joining in any gadget assumes a minimal effort for the maker and the client.

II. BLUETOOTH HISTORY

In the year 1994, the organization of media communications ERICSSON, started a concentrate to explore the suitability of a radio minimal effort interface between cell phones, what's more, the embellishments. The goal was to dispense with the links between the portable phones and cards of PCs, headsets, work area gadgets, and so on. Toward the start of 1997, Ericsson comes nearer different producers of compact gadgets to build the enthusiasm for this innovation. The rationale was basic: all together that the framework was fruitful and extremely usable, a basic amount of compact gadgets should utilize a similar innovation, five associations, Ericsson, Nokia, IBM, Toshiba, and Intel forms a Group of Special Interest (SIG) in the year 1998. This gathering contains the ideal blend in the business territory: two pioneers of the market in versatile communication, two pioneers of the showcase in PCs PC and a pioneer of the market in innovation of preparing of computerized signs.

a) How Bluetooth Got its Name:

Every one of the general population has a cell phone with the Bluetooth framework yet few of them know the reason for the name, yet it is an exceptional name: Blue-tooth. Does somebody have a tooth with blue shading? Indeed, the name originates from a lord, Harald I Bluetooth: Harald I Bluetooth (Danish Harald Blåtand) was the King of Denmark between 940 and 985 AD. The name "Blåtand" was likely taken from two old Danish words,'blå' which means dull cleaned and 'tan' which means incredible man. He was conceived in 910 as the child of King GromThe Old (King of Jutland, the primary landmass of Denmark) and his significant other There Diebold (little girl of King Ethelred of England). In the same way as other Vikings, Harald thought of it as fair to battle for treasure in outside terrains. At the point when Harald's sister Gunhild was widowed after the passing of the vicious Norwegian ruler Erik Blood Ax, she came to Denmark to look for Harald's assistance in securing control of Norway. Harald took the chance to seize control himself. By 960 he was at the stature of his forces, administering over both Denmark and Norway. He was absolved by a minister named Poppo, sent by the German ruler. He at that point made a landmark that read: "Ruler Harald raised this landmark to the memory of Grom his dad and Thyre his mom. Harald prevailed all of Denmark and Norway and made the Danes Christian". These words were too cut in stone called rune stones. Harald was murdered in a fight in 985. Harald finished the nation's unification started by his dad, changed over the Danes to Christianity, and vanquished Norway. The development started by Harald in Norway was proceeded by his child Sweyn I, who vanquished England in 1013. Under Sweyn's child, Canute there grew up an awesome Anglo-Scandinavian kingdom that included parts of Sweden.

The reason of the name is that in the tenth century the lord Harald II of Denmark, nicknamed " blue tooth " in light of an illness that was giving him this hue to his denture, reunified under his rule various little kingdoms that existed in Denmark and Norway and that were working with various principles, … the same thing that does the innovation Bluetooth, advanced by Ericsson (Sweden) and Nokia (Finland), two Scandinavian nations.

Fig. 1: - King Harald II

b) How it Work?

Every device should have an inbuilt microchip (handset) that transmits and gets in the frequency of 2.4 GHz that can be accessible anywhere in the world. Thereare three channels of voice accessible. The data can be traded to velocities of up to 1 megabit for a second &2 megabits for second in the 2nd generation of the Technology. A plan of "recurrence bounce" (hops of recurrence) permits to the gadgets to convey comprehensive in zones where an awesome electromagnetic obstruction exists. Other than that is given plans of encryption and check.

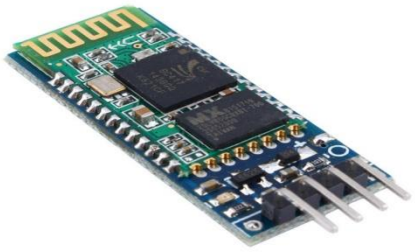

Fig. 2: - Bluetooth hardware

c) Frequency Bands:

The basic Bluetooth versions work in the ISM band of 2.4 GHz. Despite the fact that around the world, this band is accessible, the width of the band can contrast in various nations. This is the frequency of the band of the logical and therapeutic enterprises 2.45 GHz (ISM*). The extents of the transfer speed in The United States and Europe are between 2.400 to 2.483,5 MHz, it covers some portion of France and Spain. The

scopes of the transmission capacity in Japan are between 2.471 to 2.497 MHz. The transmitters of radio spreads over 2.400 and 2.500 MHz of frequencyand so the framework can be used worldwide and it is conceivable to choose the fitting frequency. This free licensed band can be opened for any arrangement of radio and should deal with the impedances of screens for infant, the controls for entryways of carports, the remote phones and the microwave stoves.

The industrial, scientific and medical bands for radio were initially owned by the world for using the RF electromagnetic fields for medical, industrial and scientific purposes. By and large, interchanges hardware must acknowledge any obstruction created by ISM gear.

Country	Frequency Range	RF Channels	
Europe* & USA	2400 - 2483.5 MHz	f = 2402 + k MHz	k= 0,...,78
Japan	2471 - 2497 MHz	f = 2473 + k MHz	k= 0,...,22
Spain	2445 - 2475 MHz	f = 2449 + k MHz	k= 0,...,22
France	2446.5 - 2483.5 MHz	f = 2454 + k MHz	k= 0,...,22

Fig. 3: - Frequency Ranges of Different Countries

d) Power:

The equipment of transmission is categorized into 3 groups according to the level of power emission, as we can see in the table in figure 4. The receiver's arrangement must possess a sensitivity greater than 70 dBm, and the rate of admissible mistake must be a minor or equal to 0.1 %.

Device Power Class	Maximum Permitted Power mW(dBm)	Range (approximate)
Class 1	100 mW (20 dBm)	~100 meters
Class 2	2.5 mW (4 dBm)	~10 meters
Class 3	1 mW (0 dBm)	~1 meter

Fig. 4: - Power Classification

The microchip is going to be attached with the portable devices and powered by phone batteries, that´s why it must have a very less consumption of power i.e. up to 97 % less than a mobile telephone. If the devices does not exchange information, then they establish the way of "wait" to preserve energy. The power of transmission that is used as the specification is of 100 mW for a scope of up to 100 m.*E and*1 mW for a scope of 10 m.

e) Scope:

The connections made by Bluetooth has a maximum range of about 10 meters, if we use amplifiers it may come up to 100 meters, creating some distortion and interferences. It is necessary to remember that these devices were created by the intention of using them in closed environments and little distances.

f) Protocols:

Different protocols help to operate different sets of applications and all of them have a link to information and a physical cap common Bluetooth. The figure in the next column will show the sets of protocols.

Protocol Layer	Protocols in the stack
Bluetooth Core Protocols	Baseband, LMP, L2CAP, SDP
Cable Replacement Protocol	RFCOMM
Telephony Control Protocol	TCS Binary, AT-commands
Adopted Protocols	PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC, WAE

Table 1: - Protocol layers

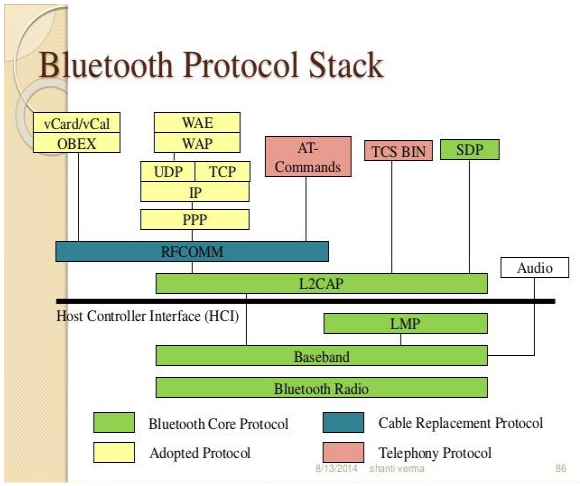

Fig. 5: - Protocol Flow Chart

III. BLUETOOTH NETWORK

The biggest advantages where we can see the versatility of the design of the Bluetooth technology, is in the easy confection and arrangement of nets i.e. Piconet & Scatternets between different devices carryingBluetooth. It has been designed to operate in a multi-user environment. It showcases 2types of possible configuration of Bluetooth network, which can be expand to a considerable number of elements to expand the subnetworks andnetworks. The network, that runs this technology is consists of Piconet anda more complex network which is named asScatternet. Up to eight devices can form a "piconet" and even ten "piconets" can coexist in the same area of coverage. If we know that every link is protected andcodifiedagainst interference and loss of link, Bluetooth can be considered to be a wireless very sure short scope network.

The Piconet are several devices that are on the same radio of coverage where they share the same channel and that is constituted between two and eight of these units. Each & every device has its unique direction, wireless LAN will become the base for the standard IEEE 802.11, where the Scatternet formed by the connection of a Piconet to another Piconet, with a maximum of interconnections often Piconets. In the following figure it is possible toobserve and understand with major facility these two configurations.

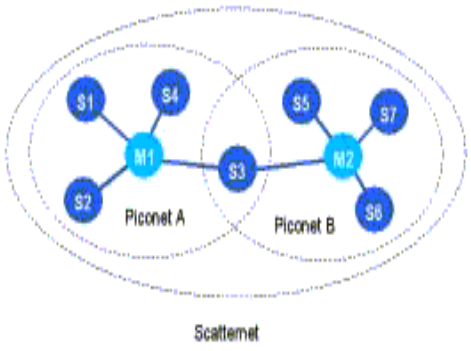

Fig. 6: - Scatternet with Piconets

The equipment's that share the same channel will divide the resources and the capacity of this one. Though the channels have a bandwidth of one 1Mhz, as more users join the Piconet, minor resources they will have for each user, because of the lesser available resources the Scatternet was came into existence to solve the problem of the low bandwidth that every user of a Piconet has if they find the great number of connected units. The Scatternet is crucial, as an individual user or whole, its performance counts when one out of every user takes part in the same channel of 1 MHz.

IV. BLUETOOTH ARCHITECTURE

The Bluetooth connection occurs between a master and a slave radio. The radios of Bluetooth are similar irrespective of the same device may operate as a master and also the slave. Each radio has unique device address (BD_ADDR) that is fixed. The fixed address is of 48-bit.

Two or more radio devices together form ad-hoc networks called Piconets. All units within a Piconet share the same channel. Each Piconet has one master device and one or more slaves. There may be up to seven active slaves at a time within a Piconet. That is why, each active device within a Piconet network is identified by a 3-bit active device address. Inactive slaves in unconnected modes may continue to reside within the Piconet.

A master in the Piconet or Scatternetcan only initiate However, once a link is established, the slave may request a master/slave switch to become the master. Slaves cannot interact with each other directly according to the protocols. Every type of communication happens within the slave and the master. Slaves within a Piconet must also synchronize their internal clocks and frequency jumps with that of the master. Each Piconet uses a unique frequency hopping sequence. Radio devices used Time Division Multiplexing (TDM). A master device in a Piconet network sends the data on even numbered slots and the slaves may send on odd numbered slots.

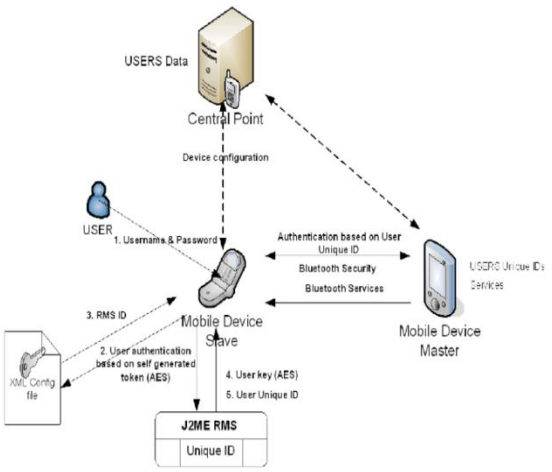

Fig. 7: - Bluetooth Architecture

V. SECURITY

As you all know it is an open system so it can have some risks like data loss that directly questions its security. Nowadays a lot of smartphones and other different devices contains pre-installed Bluetooth and in some cases, the people who buy those devices don´t know even that the Bluetooth is operating in the system. There are some opinions which comments that Bluetooth is secure in the encryption and some other technical aspects but most of the information I found about Bluetooth security is quite technical. Anyway, I think that some description about security of Bluetooth must be included in this information because security is a very crucial part of any entity. So I decided to include the clearer and simple text I found about Bluetooth security, with the link given in references.

Today's wireless world means that data is being sent invisibly from device to device through air. This data, in the form of contacts, emails, addresses, photos, and more needs to be sent securely. Bluetooth wireless technology has put stress on security while making connections between the devices. The SIG, made up of more than 8,000 members, has a Security Expert Group. It includes technical engineer from its member companies who provide critical security requirementsand information as the Bluetooth wireless specification grows. Bluetooth wireless technology that is used by the developers in their products have several security options. And there are 3 modes of security for Bluetooth access between two devices:

a) Security Mode 1: non-secure.
b) Security Mode 2: service level enforced security.
c) Security Mode 3: link level enforced security.

The manufacturer of each product finds these security modes. Services and Devices have different security levels. For devices, there are 2 levels: "untrusted device" and "trusted device." A trusted device has already been paired with one of your other devices and has unrestricted access to all services. Services have 3 security levels:

Services that require authentication and authorization.
1. Services that require authentication only.
2. Services that are open to all devices.

a) Security Features:

The security supports encryption and authentication. Authentication verifies who is on the other end of the linked side. Encryption ensures data should not leak. Even if a third party hacks the data, it is in encrypted form and not in original form.

1. Pairing:

When 2 devices interact for the first time, there is a pairing procedure. In this, a secret key is generated by the device. This key is shared to both the devices. It is stored in each device. When the devices want to communicate in future, there will be no pairing procedure.

2. Security modes of a device:

There are 3 security modes in a device.

- Non-secure: A device will not start any security steps.
- Service level enforced security: A device does not start security steps before channel establishment at the L2CAP level.
- Link level enforced security: A device starts security steps before link set up at LMP is completed.

b) Security Levels:

There are 2 kinds of security levels:

- Authentication
- Authorization

1. Authentication:
"It is performed after finding out the type of service. It cannot be performed when ACL link is established. It is performed only when connecting the request to service is submitted. It can be performed bi-directionally: client authenticates the server and vice versa."

2. Authorization:
Some services require the manual authorization of the device after authentication onlythen, these services can be accessed. This leaconcept of trust. There are two kinds of device trust levels:

- Trusted device: It has fixed relationship (paired) and unrestricted access to all services.
- Untrusted device: This device has been previously authenticated, a link key is stored, but the device is not marked as trusted in the device database.
- An unknown device is also an untrusted device. No security information is available for this device.

c) Security Problems:
The encryption scheme of Bluetooth has some weaknesses. The E0 stream cipher with 128-bit key length can be broken in O (2^64) in handfull circumstances. The proof is in mathematical form and therefore out of the scope of this paper, so it will not be included.
There is also a problem in the usability of the Bluetooth enabled devices. The use of the PIN in the starting process of 2 Bluetooth devices is tacky. When you have to enter the PIN twice every time you connect two devices, it gets problematic even with shorter codes. If theBluetooth devicescontains an ad hoc network and every machine is to be started individually, it is not bearable. And it does not hold the security very easily. The specification makes a suggestion to use application level key agreement software with the longer 16 octets PIN. So the PIN need not be entered physically to each device of the connection but is exchanged.

The generation of the starting key may also be of great concern. The strength of the starting key is based purely on the used PIN. The starting key generation algorithm i.e. E22 derives the key from the PIN, the length of the PIN and a random number, which is transmitted over the air. The output is highly questionable, as the only secret is the PIN. When using 4 digit codes there are only 10,000 different possibilities. Adding the fact that 50% of used PINs are "0000", the trustworthiness of the initialization key is quite lower.

The Device Address, which is different for every Bluetooth device, introduces another problem. When it recognizes the connection is made to a certain Bluetooth device, it is easy to monitor andtrack the behavior of this person. Logs can be made on all Bluetooth transactions and privacy is compromised. Profiling and other questionable ways of categorizing can take place.

Another problem with Bluetooth is the battery draining denial of service scheme, against which it has no protection. If this is going to be a big problem, I suspect some preventation will be taken by the Bluetooth SIG. There are several problems still in the security of Bluetooth. It seems to be sufficient for smaller applications, but any type of sensitive or otherwise problematic data should not be send via Bluetooth

VI. APPLICATION

Bluetooth's applications are very varied and allow changing radically the formthat the users interact with the mobile telephones and other devices. Inside the field ofthe technology, the application is immediate because it allows an easy, instantaneous communication, in any place and low cost. We cannot forget the impact in the way of realizing the processes, on having replaced the conventional means and having made new business and applications possible.

More prevalent applications of Bluetooth:

- Wireless control of and communication between a mobile phone and a hands-free headset. This was one of the earliest applications to become popular.
- Wireless networking between PCs in a confined space and where little bandwidth is required.

- Wireless communications with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of files between devices with OBEX (a kind of communications protocol).
- Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- For controls where infrared was traditionally used.
- Sending small advertisements from Bluetooth enabled advertising hoardings to other, discoverable, Bluetooth devices.

VII. INTRODUCTION TO BLUETOOTH 5

The Bluetooth SIG officially announces Bluetooth 5 as the latest version of the Bluetooth. Important updates to Bluetooth 5 include larger broadcast message capacity, faster speed, and longer range, as well as improved coexistence and interoperability with other wireless technologies. It continues to evolve the IoT experience by enabling effortless and simple interactions across the long range of connected devices.

This concludes whole-home and building coverage, as well as new use cases for outdoor, industrial, and commercial applications, will be a reality. We continue to evolve to meet the needs of IoT consumers and developers while staying true to what Bluetooth is at its core: the global wireless standard for secure, connectivity and simplicity.

There are very exciting new features present that promise to revolutionize the scope, appeal, and spread of Bluetooth as the primary connectivity solution on the market. The important introductions are given below:

- Improved co-existence
- Errata
- Long range
- Advertising extensions
- High throughput
- Increased broadcast capacity

The new Bluetooth features for long range, high throughput, and advertising extensions offer truly exciting possibilities for home, industry and commerce as well as the more traditional areas of wearables and personal devices historically associated with Bluetooth.

FEATURES:

a) 2x Speed:

- 2M PHY
- Up to 1400 kbps throughput
- 15 to 50% lower power

b) 4x Range

- 2x range at 125 kbps PHY
- 2x range at +20 dBm TX

c) 8x Advertisement Capacity

- Up to 255 B of data per packet
- Chaining of multiple advertisement packets
- Offload advertisement packets to data channels

VIII. CONCLUSION

From the above data we get to know about how the Bluetooth technology came into existence, how Bluetooth got its name from the historical novel about Vikings and King Harald Blåtand at that time. He was also the reason for the adaptation of the symbol of Bluetooth technology. We had also discussed about the year 1994 when Ericsson, the telecommunications company OF Sweden, came up with the idea of replacing that were then commonly used to communicate between instruments with an RF-based 'wireless' alternative by the tangle of RS-232 cables.

Further, we had given the idea of Bluetooth architecture, how Piconet and scatternet forms and affect the topology of Bluetooth network. We had included the protocol section that was formed by the alliance of companies Ericsson, IBM, Intel, Toshiba and Nokia, and later joined by many other companies, they were named as Bluetooth special interest group(SIG).

Bluetooth uses ISM band i.e. the industrial, scientific and medical band that was free of license from that time that is why we does not have to pay for the

transmission of data over Bluetooth carrying devices. It made the successful connection by using the steps like inquiry, paging, link establishment, service discovery, L2CAP channel, RFCOMM channel, security, PPP, network protocols.

ACKNOWLEDGMENT

I am thankful to Mr. Omprakash Sharma, Director Poornima College of Engineering, Jaipur(Raj.) for giving me the opportunity to be the part of his college and providing the necessary guidance through his faculty team of Electronics and Communication Engineering.I am also thankful to Mrs. Garima Mathur, H.O.D Electronics and Communication Engineering for proving me proper working area and timings in spite of our regular classes. She also grants access to the resources of the department required for making my seminar report.

REFERENCES

[1] A Modern Study of Bluetooth Wireless Technology Mrs. PratibhaSingh, Mr. DipeshSharma,Mr.Sonu AgrawalRIT, Raipur, Dept. of Computer science & Eng., RIT,Dept. of inf. Tech.,SSCET, durg, Dept. of Computer sci. & Eng. Raipur, (Chhattisgarh)

[2] Bluetooth Technology Key Challenges and Initial Research RochGu´erinEnyoung Kim Saswati Sarkarguerin@ee.upenn.edu ekim@lucent.comswati@ee.upenn.eduU. Pennsylvania Lucent Technologies U. PennsylvaniaPhiladelphia, PA Holmdel, NJ Philadelphia, PAot

[3] Bluetooth: Vision, Goals, and Architecture JaapHaartsen Mahmoud NaghshinehJon InouyeEricsson IBMWatson Research Center Intel Corporation Enschede, The Netherlands Hawthorne, NY, U.S.A. Chandler, AZ, U.S.A.Olaf J. Joeressen Warren AllenNokia Mobile Phones Toshiba Corporation Bochum, Germany Irvine, CA, U.S.A

[4] Das, A. Ghose, A. Razdan, H. Saran, and R. Shorey. Enhancing performance of asynchronous data traffic over the Bluetooth wireless ad-hoc network. In *Proceedings of INFOCOM'2001*, Anchorage, AK, April 2001.

[5] A Bluetooth Routing Protocol Using Evolving Fuzzy Neural Networks presented by Chenn-Jung Huang, Wei-Kuang Lai, Sheng-Yu Hsiao and Hao-Yu Liu.

[6] Miller and C. Bisdikian. Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications. Prentice-Hall,2000.

[7] IEEE. Standard for Wireless LAN Medium AccessControl (MAC) and Physical Layer (PHY) specifications,1997.

[8] Bluetooth Security Analysis and Solution U.L.MuhammedRijah, S.Mosharani, S.Amuthapriya, M.M.M Mufthas, MalikberdiHezretov and DhishanDhammearatchi Faculty of Computing, Sri Lankan Institute of Information Technology.