Bluetooth enabling device for physically challenged using actuators and sensor

Lokesh Kumar Gaurav[1], Mantu Kumar Mishra[2], Mr. K.Kumar[3]

[123] Dept of MCA., Veltech Technical University Chennai, India

[1]sylokesh@gmail.com, [2]mishra.mantu8@gmail.com, [3] hellokumar@gmail.com

Abstract—

This paper illustrates Bluetooth enabling device for physically challenged using actuators and sensor for providing robust security and reliability. In it we have written how Bluetooth is useful for we people in present era with high security as well as performance. We have used different types of protocol which is more suitable for Bluetooth device[1] like IP Secure (IPsec) and Secure Shell (SSH).Bluetooth abbreviations out as the most averring for use in low-power sensor networks. This paper also addresses the difficulty of scatter net for singe hope Bluetooth based personal area and ad hoc networks with minimal communication overhead.Bluetooth iscriticized for various vulnerabilities and security as its designers are trying to balance wisely between performance and complementary services including security. Over all it is used for short range and it creates Personal Area Network (PAN)application.

Index terms :- Bluetooth, IPsecr, SSH,scatter net,security,vulnerbilities.

I. INTRODUCTION

Bluetooth is most attractive which is used to createPersonal Area Network (PAN). Using Bluetooth we can construct a network that is being used for establishing a local area network or other small area network which is often formed of wireless devices. At this time Bluetooth devices are directlyused for sending data or information which are very secret therefore we are using actuators and sensor. As we know bluetooth device will be capable to connect up to eight devices including master device in which seven devices will be active slaves and one will be master device.Bluetooth is a most beautiful technology that can be used for ad hoc networking. Bluetooth denotes us to take the facility of computing and communications industry specification which illustrate how e.g. mobile phones, computers and personal digital assistants (PDAs) can cordiality interconnect and communicate with us using wireless transition in limited range. The main goal of Bluetooth device[2] is to eliminate the cable connection for transferring data in a short area. This technology is very useful for laptop, cellular phone or mobile phone, PDA, etc. user for sharing the data or information with each other for wonderful example conference in a room by using ad hoc network. The maximum usage range is between 10 to 100 meters.

As we know that none of protocol focuses on performance evaluation comparing Bluetooth's native security[3] method or technique with suitable, strong security protocols like IPsec and SSH. Like it, this paper focuses on the performance issue of existing security protocols and mechanisms for controlling devices. We mapped the performance of both the built-in Bluetooth security mechanisms which is known as security modes and two otherstandard security protocols operating at different layers of theTCP/IP protocol suite that is called SSH and IPsec. By using thelast two protocols, applications can communicate securelycreating a secure tunnel or Virtual Private Network(VPN).Bluetooth provides three different security modes namely security modes I, II and III, but in our tests we have decided to use only two modes which are security mode I, and III. Security mode I apprises no real security as authentication and confidentiality services are disabled. On the other side, security mode II specifies security services after the connection between the two deviceshave been established and only if a given application has requested them. Like it, the security services in mode II dependon the application running. The last security mode is one of the powerful among the three modes, because it uses both authentication and confidentiality built-in mechanisms independently of the application running.

This research shows the importance of implementing actuators and sensor for making enable Bluetooth with excellent performance and security. In order to make reliable connection for creating PAN. The major advantage of this paper to protect from hacker of bluetooth as well as easy to use like user friendly. This will illustrating some of basic information of bluetooth that is very needed to know if we are working with Bluetooth or taking facility of it. One of the more important matter for us that actuators and sensor is very much useful for providing both performance and security in Bluetooth.

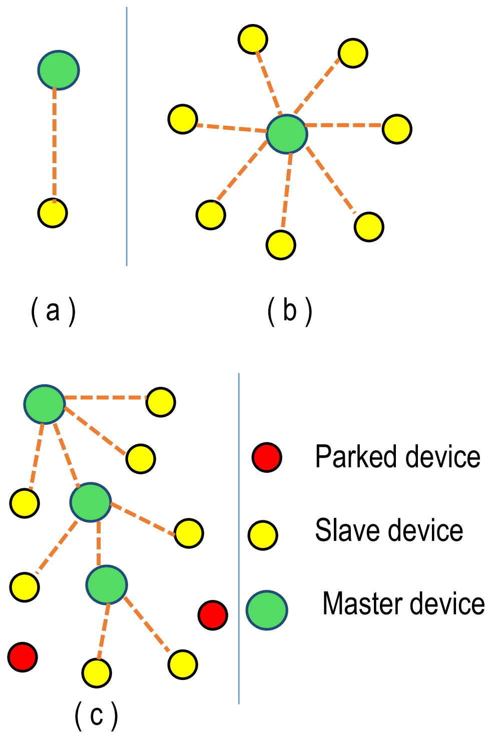

Fig.1 a) Piconet with single slave connection, b)Piconet with Multi-slave connection and c) Scatternet connection.

In the above fig.1 slave device is nothing but it is a Bluetooth enable device, which is sharing data for slave device to master device or vice-versa. Master device is also a device that provides facility to make connection among slaves. Master device of one piconetcan be slave of other piconet. And parked is one of the device which is not connected in network of bluetooth. Parked device can be unlimited in any Bluetooth network.If one slave device is connected with one master device is known as “piconet with single connection”. When we people connect one master device with multiple slaves(less than seven slaves) device are called “piconet with multi-slaves”. And we use more than one master device is called scatternet. In other way we can say that two or more piconet is often called scatternet. An indefinite number of parked devices can be appear in network of Bluetooth.

II. PROBLEM STATEMENT

Anyway the Bluetooth technology has a limited scope, this characteristic of limited scope presents a great disadvantage and bellow is some disadvantages.

Disadvantages

- Bluetoothnetwork has no considerable security by that we people feel secure transferring of data.
- In existing bluetooth performance[4][5] is big issue it take large time for searching new device and sending data for certain device.
- Bluetooth PC (master device) dialer is for both a stand-alone system application and a Bluetooth external look plug in. It means master device can easily connect or access data of outlook device via a single click.

III. MOTIVATION

At present era the most common features of the Bluetooth devices are low complexity, low power, robustness, low cost, easy configuration, lack chance of data hacking.

Advantages

- One of the biggest attractions of the implementation of this technology is the creation of networks, with the Bluetooth technology for high performance using actuators and sensor.
- Using fast recovery mechanism protect from the loss of data. For it we need to increase suddenly transmission rate.
- It can be used anywhere where is need for transfer of small amount of data on shorter ranges (synchronization, for example) and it can be also used as a cable replacement technology.
- Bluetooth can make personal area network at any place without any extra device. This is very much useful where there is no network there we can also establish own network.

IV. BLUETOOTH PERFORMANCE

As we know, the experimental procedure consistsof three main parts: evaluation of Bluetooth built-in securitymodes I (no security), and III (strong security), and estimationof the performance of IPsec (IP secure) and SSH (Secure Shell) mechanisms over bluetooth links. In all scenarios we people assemble measurements for subsequent network performance parameters absolute. File Transfer time (TT), Achieved Transfer Rate (ART) and Throughput. All measurements have taken place at the server node because of its processing power.

- The transfer time is represented actual duration of transfers during a transaction of any data.
- The achieved transfer rate is represented the actual transfer rate achieved during a transaction. In an idea scenario, a constant data rate should be motioned between two communication end-points[6]. However due to various reason, mainly concerned with the wireless medium nature, this parameter modifying over time. We should underline the fact bytes sent and bytes received could also keep retransmitted bytes.

  achieved_transfer_rate(Kbps) = ((bytes_sent +bytes_received) * 8)/ TT.
- Throughput represents the percentage of achieved_transfer_rate over the practical maximum_transfer_rate of link,which in our case is 723 Kbps:

  Throughput(%)=achieved_transfer_rate/maximum_transfer_rate*100.

Over all, ‘*achieved transfer rate improvement*’is acomparison metric that shows the improvement of theachieved_transfer_rate with respect to the Bluetooth mode lachieved transfer rate achieved_transfer_rate_B_land iscalculated as:*achieved_transfer_rate_improvement*(%)=(*achieved_transfer_rate-achieved_transfer_rate_B_I*)/ *achieved_transfer_rate_B_I** 100.

A positive value implies that the performance or channel throughput has increased in orderto compare with Bluetooth mode we achieved transfer rate, while a negative one means that the performance has decreased[7]. Measurements were assemble during repeated FTP (File Transfer Protocol) file transfers, between the laptop server and the PDA client. Each file was transferred twelve times and only average values were recorded. Over allscenarios, the ping response times between client and server were varying among 19.7 and 21.8 msecs.

Bluetooth security modes I and III Evaluation

Measurements for resulting Bluetooth modes I and III were assembled by transferring four different files between the client and the server. The size of files were 5.26, 7.0, 10.5 and 15 Mbytes respectively. Figure 2 shows a graphical representation of these values. As we can normally notice the results are generally as expected. At first, the TT metric is little bit higher for mode III, as well as the ATR is higher for mode I. This occurs because mode III mandates authentication or handshake at the beginning of each transaction. Remember that the handshake time is combined in TT too.

Beside this, encryption algorithms are implemented during the transaction for mode III and as a result the overall it increases the time of transferring data. We can also understand that the larger the file size is the longer TT difference between mode I and mode III is to be. This situation is also portrayed in the respective plot of fig2

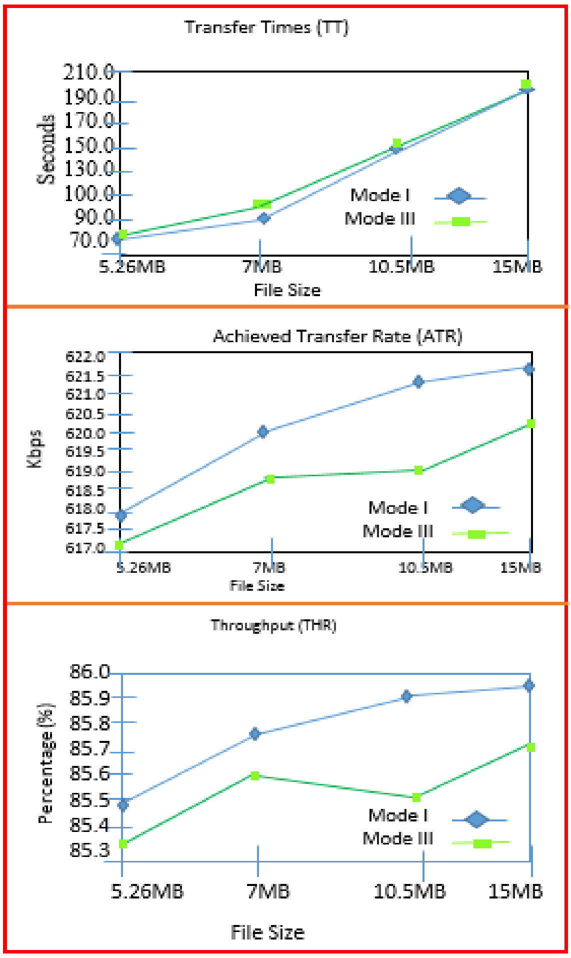

Fig.2 Average metric values for network parameters measured/Bluetooth Modes I &III.

The above diagram shows the graphical performance and bellow we have made table of it to understand mode value in a better way.

Table 1 Standard deviation for all Bluetooth Scenarios

	MODE I		
File Size (MB)	TT (sec)	ATR (Kbps)	THR (%)
5.26	0.5	2.6	0.4
7	0.1	0.9	0.1
10.5	0.4	1.6	0.2
15	0.2	0.5	0.1
	MODE III		
5.26	0.1	1.3	0.2
7	0.5	3.2	0.4
10.5	0.1	0.5	0.1
15	0.6	2.2	0.3

In simple, these measurements advocate that mode I uses the network better than mode III.Due to volatile nature of the wireless link, we also get standard deviation (SD) for the measured values in Table 1.

V. BLUETOOTH SYSTEM ARCHITECTURE

In order to explain Bluetooth technology which is used to show the protocol of Bluetooth in a network. Here we have drawn a Bluetooth architecture.

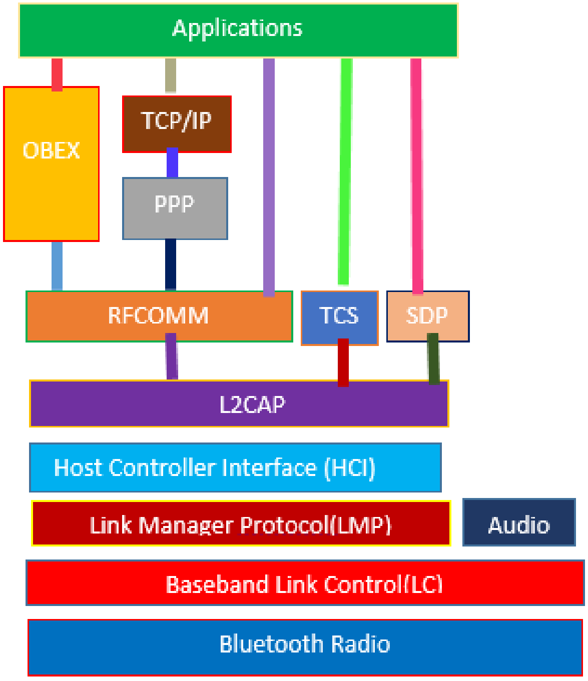
Applications
OBEX
TCP/IP
PPP
RFCOMM
TCS
SDP
L2CAP
Host Controller Interface (HCI)
Link Manager Protocol(LMP)
Audio
Baseband Link Control(LC)
Bluetooth Radio

Fig. 3 Architecture of Bluetooth

In this diagram there so many of protocol which is being used to establish the connection. Here all part of diagram is define in brief. Object Exchange (OBEX)- is used to exchange the object. Host Controller Interface (HCI) – this is the lowest layer of the Bluetooth Host stack. It interfaces directly with the host controller hardware. Point to point protocol (ppp)-this protocol is responsible to make connection from one point to other point. Logical Link Control and Adaptation Layer (L2CAP) – this layer handles packet segmentation andreassembly (SAR), protocol multiplexing, and provides quality of service information.Service Discovery Protocols (SDP) – as the name implies, applications use this layer to discover Bluetooth services that are available.RFCOMM – this layer provides serial behavior over Bluetooth, similar to using a standard serial (COM) port.TCS This is the Telephony Control Protocol Specification and describes the call control and signaling of voice channels over Bluetooth. Radio Frequency Communications Protocol (RFCOMM).

VI. WORKING PRINCIPLE

When we want to send any image, audio, video, text file, etc then we shall have to first of all we need to search the device then we need for establishing the connection after thatBluetooth device simply takes a security code from the source device (our device) and matches from the destination device (other device)if both security codes are same the connection will be established otherwise connection will be failed. We can connect maximum of sevenBluetooth enable devices with same procedure of connection. In which one device will work as a master device and other will work as slave devices. It provides high security for all devices because without permission of slave device even master device can't access data because here we have implemented security protocol. One of the most important security of Bluetooth is that it is used for limited area so unauthorized people after wishing can't hack the data of Bluetooth. The data is not visible on source device until or unless the last bit of data is not sent from destination device. After taking concept of this paper if Bluetooth will be designed the performance and security would be excellent.

In the below diagram we can see seven device are connected to each other. The device which is in center that will work like a master device and other will work like slaves of piconet total number of slave is seven. Once connection is done then we would send or share data.

Fig.4 A Bluetooth with seven active node

VII. CONCLUSION

In this paper we have successfully developed a Bluetooth based technology which is very muchuseful for security and performance. This Bluetooth technologyprovide the way to operate or perform the task. Here I have implemented the concept for both performance and security to exchange the secret data or normal data in easy way with no risk. In this paper we are providing facility to connect seven nodes for constructing piconnet network. In order to construct a network with several slave we have given the concept of scatternet with excellent performance[8]. This paper provides the fast transmission so that the user can easily send or receive data after implementing the above concept. Over all this paper is very much useful and user friendly for every one which is considered as learner.

VIII.FUTURE ENHANCEMENT

As future work we shall expand this study investigating the performance of asymmetric cryptography technique such as public key certificates and to support authentication services in the context of such protocols that promote automatic keying[9]. On the other side direction is to detect how much energy[10] is required for this sort of secure connections for security, as mobile devices can't afford batteries with actual capacity.

REFERENCES

[1] Hewlett Packard Smart Handheld Group, Bluetoothtechnology overview.

[2] The official Bluetooth wireless info site, http://www.bluetooth.com

[3] Christian Gehramann, JoakimPersson and Ben Smeets, Bluetooth Security

[4] Nikhil Anand, An overview of Bluetooth Security.

[5] The official Bluetooth membership site, https://www.bluetooth.org.

[6] Francia, G., Kilaru, A., Le Phuong and Vashi, M. "Anempirical study of Bluetooth performance", Inproceedings of the 2nd annual conference on Mid-south college computing, ACM International Conference Proceeding Series; Vol. 61, pp. 81 – 93, 2004.

[7] Howitt, I. "Bluetooth performance in the presence of 802.11b WLAN", IEEE Transactions on Vehicular Technology,

[8] Volume: 51 Issue: 6, pp. 1640-1651, 2002.

[9] Wang Feng, Arumugam, N. and Krishna, G.H.,"Performance of a Bluetooth piconet in the presence of IEEE 802.11

[10] WLANs", in proc of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1742 - 1746 vol. 4, 2002.

[11] Yujin Lim, Jesung Kim, Sang Lyul Min andJoongSoo Ma, "Performance evaluation of the Bluetooth-based public Internet access point", in proceedings of the 15thInternational Conference on Information Networking, pp. 643 – 648, 2001.

[12] Karnik, A. Kumar, A., "Performance analysis of the Bluetooth physical layer", in proc. of IEEE International Conference on Personal Wireless Communications, pp. 70 – 74, 2000.

[13] http://www.icta.ufl.edu/gt.htm

[14] Helal et al., "Gator Tech Smart House: A programmablepervasive space," in IEEE Computer, vol. 38, no. 3, pp. 50-60, March 2005.