Proposal of an Intelligent Surveillance Algorithm for Scatternet Network

R.Kanthavel
Dept. of Computer Science & Engineering
Government College of Engineering
Tirunelveli

R.Dhaya
Dept. of Information technology
National Engineering College
Kovilpatti

ABSTRACT
Bluetooth, a short range communication technology to replace peripheral cables, has grown steadily and includes a variety of wireless applications. The Bluetooth protocol operates on a wide variety of mobile and wireless devices and is nearly present everywhere. Several attacks exist that successfully target and exploit Bluetooth enabled devices. This paper presents the design of a network intrusion detection system using Bluetooth scatternet for discovering malicious traffic for surveillance. Several Bluetooth enabled devices are internet worked to form scatternet and developing the secure network is an important issue in the scatternet formation. This paper also proposes an Intelligent Surveillance algorithm (ISA) to make the scatternet network secure. The aim of the proposed network is to present a security integrated system that ensures the detection of the intruder which enters the scatternet network. The experimental results show that the system can significantly improve the overall security of the scatternet network.

Key words
Piconet, Scatternet, Surveillance, intelligence algorithm.

1. INTRODUCTION
Bluetooth is a short range wireless technology for exchanging data over static and mobile devices, creating personal area networks (PANs). Bluetooth uses a radio technology called frequency-hopping spread spectrum, which hops up the data being sents and transmits chunks up to 79 frequencies [3,8] with a gross data rate of 1 Mb/s.

On the other hand, a Piconet is the type of Bluetooth connection that is formed between two or more Bluetooth-enabled devices, which has the maximum size of a Piconet to 8 devices with the ratio of 1 master and 7 slaves [15]. But a Scatternet is a number of interconnected Piconets that supports communication between more than 8 devices and is a type of ad-hoc network consisting of two or more piconets. A Several Bluetooth enabled devices are internetworked to form scatternet and developing the secure network is an important issue in the scatternet formation.This paper discusses some of these issues and highlights a number of vulnerabilities in the current generation of Bluetooth enabled devices also introduced a solution to the security problem by generating an algorithm to detect the intruder [13].

Some commonly used Bluetooth enabled devices are vulnerable to exploitation using a range of methods including Bluesnarf, Backdoor and Bluebug[14]. These vulnerabilities can expose the user to a range of issues relating to privacy and security and are explored as follows.

- Bluesnarf attacks are the use of Bluetooth technology to access restricted areas of a user's device without their knowledge or approval for the purpose of capturing data. This vulnerability did not require authentication from other Bluetooth devices attempting to communicate with it[3].

- The Backdoor attack involves in creating a trust relationship through a devices pairing mechanism and also ensuring that the established relationship no longer appears in the user's register of paired devices. The only time the owner can be aware of the connection is if they are observing their device at the precise moment a connection is established. Once the pairing has being established, the attacker could be able to utilize any resource on the target that the device allows access to without the owner's knowledge or consent [2].

- The Bluebug attack creates a serial profile connection to a device. Using this exploit it is possible to use the device to initiate calls, send and read SMS messages, connect to data services and monitor conversations without the knowledge of the device owner [1].

2. EXISTING PROBLEM IN BLUETOOTH SECURITY
As the widespread use and acceptance of Bluetooth continues concerns are being raised related to security vulnerabilities and privacy issues inherent in the use of this technology [10]. Inadequate device resources and lack of user awareness has compounded this issue where the emphasis on design constraints, functionality and ease of use sometimes outweigh security concerns [9]. Recently some concerns have being highlighted relating to the possible security vulnerabilities in commonly used devices, and also the possibility of the imperceptible tracking of device users through the use of distributed and connected Bluetooth sensor nodes[5]. Network developers are looking into different means of remotely controlling the devices comprising such networks, so as to have the flexibility to change various parameters of these

devices without actually being present near these devices [11]. Nowadays Bluetooth vulnerabilities and hacking is improved extraordinarily. In Remote controlled Bluetooth enabled environment security plays a vital role[6]. Still now, security based Remote control Bluetooth enabled environment was not implemented. In particular, the current method being used to exploit these drawbacks is discussed [12].

3. OVERALL VIEW OF THE PROPOSED NETWORK

The figure 1 illustrates the overall view of the scatternet network which comprises 2 piconets

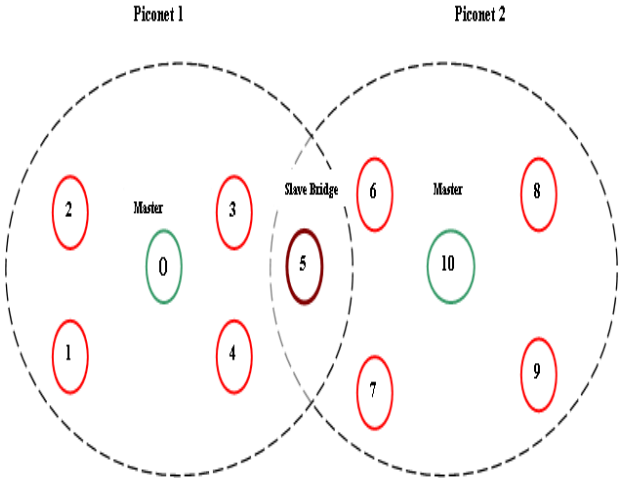

Figure 1: Overall view of the scatternet network

Scatternet is formed by two piconets namely piconet1 and piconet2. Piconet1 has one master and five slaves. In piconet1 node '0 ' acts as master and nodes '1','2','3','4','5' act as slaves. Similarly, piconet2 also has one master and five slaves. In piconet2 node '10 ' acts as master and nodes '6','7','8','9','5' act as slaves. Node '5' acts as a slave of both the piconets, so it is known as slave-bridge. Slave bridge interconnects two piconets (piconet1 and piconet2) to form the scatternet network and it can relay data between members of both piconets. Any updated information of one piconet is send to other piconet via slave-bridge. Each node has the information about all other nodes in the scattenet network such as mobile id, ip address etc[15].

4. PROPOSED ALGORITHM

The proposed algorithm called Intelligent Surveillance Algorithm (ISA) analyzes the external object for Bluetooth vulnerabilities.

4.1 Intelligent Surveillance Algorithm

Procedure Main

Step1: Initialize The Scatternet Network.
Step 2: Get the mobile id of the external object (xmid)
Step 3: If mobile id of the external object (xmid) differs from the mobile id of all the devices in the network (mid) then the same is said to be an "intruder".

Else if the mobile id of the external object (xmid) is same as any one of the mobile id of devices in the network (mid) then, call procedure sub.

```
If
    xmid # mid
    then
        X is an Intruder
        Goto Step 4.
Else if
    xmid == mid
    then
        Call sub ()
```

Step 4: Final intimation (Information about the Intruder) is send to all the nodes in the scatternet network via masters.

PROCEDURE SUB:

Step 1: Get the ip address of the external object (xip).
Step 2: If ip address of the external object (xip) differs from the ip address of all the devices in the network (ip) then the same is said to be an "intruder".

Else if the ip address of the external object (xip) is same as any one of ip address of devices in the network (ip) then the same is said to be one of the object in the proposed network.

```
If

xip # ip
then
        X is an Intruder
         return
Else if
    xip == ip
    then
        X is an internal object.
```

The following figure 2 shows the configuration flow of the Intelligent Surveillance Algorithm**.** Where

xmid - The mobile id of the external object
mid - Mobile id of any one of the devices in the network
xip - ip address of the external object
ip - ip address of any one of the devices in the network

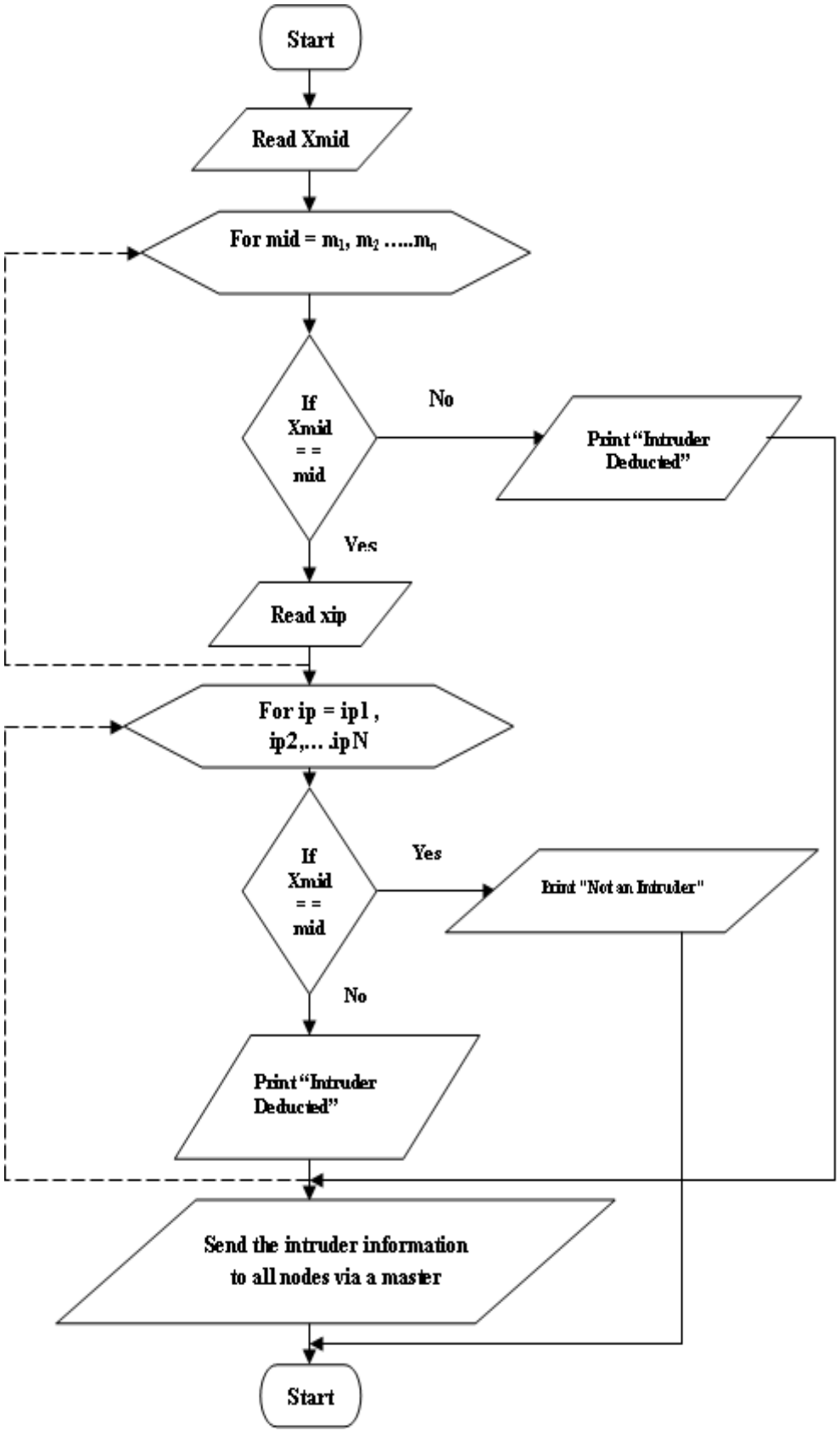

Figure 2: Configuration Flow

5. EXPERIMENTAL WORKS

As discussed earlier, the proposed network has two piconets. Piconet1 has node-0 as master-1. Master-1 controls five slaves namely node-1, node-2, node-3, node-4, and node-5. Piconet2 has node-10 as master-2. Master-2 controls five slaves namely node-5, node-6, node-7, node-8, and node-9. Each master performs the inquiry process to collect the information about all the nodes in the network such as mobile-id (48-bit unique address) and ip-address. So each node in the network has the information such as mobile-id and ip-address of all other nodes.

The intruder may replace the device in the proposed network with the duplicate id of the original device. So, each node is assigned with an individual ip-address in addition with mobile-id. This ip-address is provided by the network administrator to each device that cannot be duplicated or hacked by others. We propose an Intelligent Surveillance Algorithm (ISA) to make the scatternet network secure. Any attack such as blue-snarf can be blocked and identified by ISA.

5.2. DETECTION OF EXTERNAL OBJECT

There are two possible cases one may be the normal intruder which can be identified by its mobile id and the other intruder with hacked mobile-id using blue-snarf or other attack can be identified by its different ip-address. If an external object enters the proposed scatternet network, the near-by device of the intruder in the network performs inquiry scan. As a result of inquiry scan, the mobile id, ip address and other security parameters are received. The received mobile id is checked with mobile id's of each of the devices in the proposed network. If mobile id of the external object (xmid) differs from the mobile id of all the devices in the network (mid) then the external object is said to be an "intruder". The information about the detected intruder will be sent to all other devices in the network including piconets with the help of masters in the network[16].

If the received mobile id is same as the mobile id's of the existing devices then the received ip address is checked with the ip addresses of all the devices in the network. If ip address of the external object (xip) differs from the ip address of all the devices in the network (ip) then the same is said to be an "intruder with hacked mobile-id"[17]. The information about the detected intruder will be sent to all other devices in the network including piconets with the help of masters in the network. In both the cases the detected intruder is in dead state through out the network because the information about the intruder is present in every node in the proposed scatternet network.If the received mobile id and ip address are identical with any one of the proposed device in the network then the external object is confirmed to be one of the device in the proposed network.

A device in the network identifies the intruder. The device sends the information about the intruder to its respective master in the piconet[18]. The master sends the intruder information to the other piconet master via slave-bridge. Finally, masters of both piconets send the intruder information to all its slaves in the scatternet network.

6. EXPERIMENTAL OUTPUT

Table-1: Proposed Scatternet Network Details

NODE	MOBILE ID	TYPE	IP ADDRESS
0	0	MASTER	100
1	1	SLAVE	101
2	2	SLAVE	102
3	3	SLAVE	103
4	4	SLAVE	104
5	5	SLAVE BRIDGE	105
6	6	SLAVE	106
7	7	SLAVE	107
8	8	SLAVE	108
9	9	SLAVE	109
10	10	MASTER	110

The table 1 represents the proposed scatternet network details. The details include node number, mobile id of the node, and type of the node and ip address of the node.

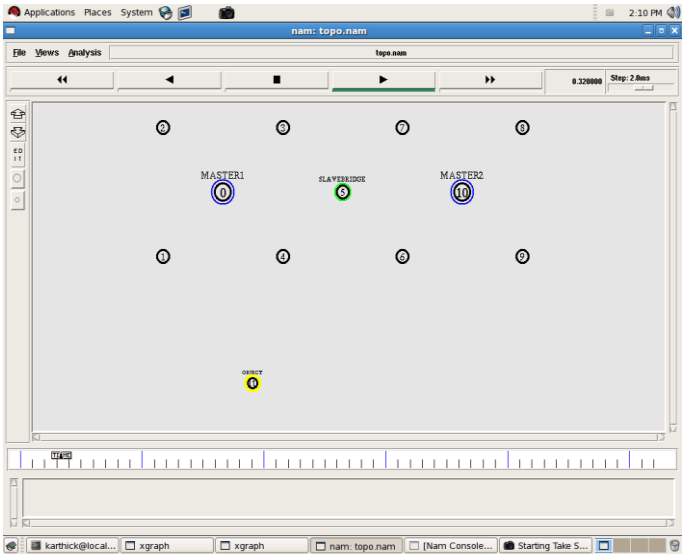

Figure 3: Initial network arrangement

Figure 3 shows the external object enters the proposed scatternet network. The node-0 and node-10 are masters and node-5 is slave-bridge. The external object is detected by the node 4 using Intelligent Surveillance Algorithm when it reaches the range of ten meters. The node 4 sends the information about the external object to its master 0. The Master-0 sends the information about the external object to slave bridge denoted by node 5.The acknowledgement for the data transfer is received from slave-bridge to Master 0.The slave-bridge sends the information about the external object to Master 10 and the acknowledgement is received from the Master 10.The Master 0 sends final intimation to its slave's

node 1, node 2, node 3, and node 4 so that the entire slave's in the piconet get alert about the external object.

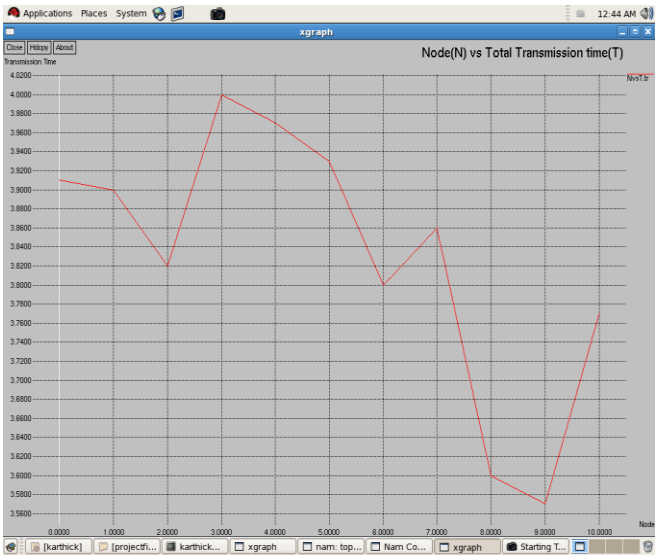

Figure 4: Node (N) Vs. Total Transmission Time (T)

In figure 4, Node (N) and Total Transmission Time is represented. The total transmission time by each node to send the information about the external object that enters the proposed scatternet network. The maximum time taken to send the information is four seconds. From the figure it is clear that the total transmission for every node in the network is approximately equal

Table 1: Node Vs Transmission time

Node(N)	Total Transmission time (T)
0	3.91
1	3.9
2	3.82
3	4
4	3.97
5	3.93
6	3.8
7	3.86
8	3.6
9	3.57
10	3.77

The Table 1 represents the parameters that are Node (N), Total Transmission Time (IDT).

.

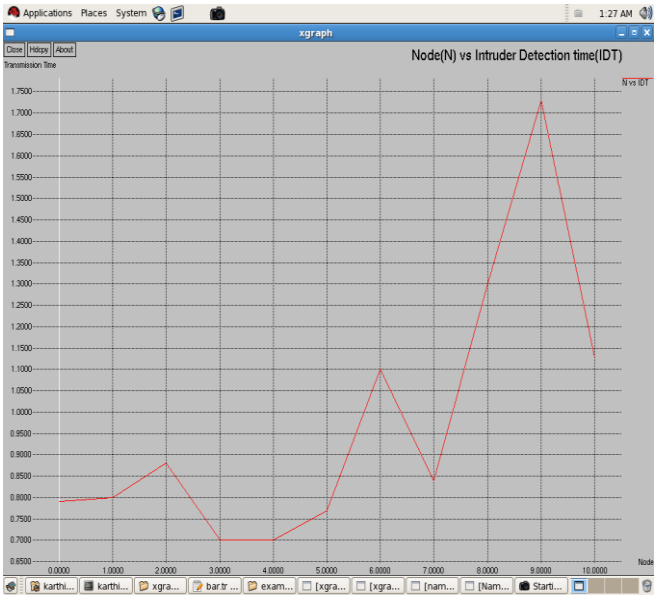

Figure 5: Node Vs. Intruder Detection Time

Figure 5 represents the Node and the Intruder Detection Time .

Table 2: N Vs IDT

Node(N)	Intruder Detection Time (IDT)
0	0.79
1	0.8
2	0.88
3	0.7
4	0.7
5	0.77
6	1.1
7	0.84
8	1.3
9	1.73
10	1.13

The table 2 represents the parameters that are Node (N), Intruder Detection Time (IDT).The figure illustrates that the time taken by each node to detect the intruder that enters the proposed scatternet network. We have assumed that the external object comes from the particular distance. So the time taken for intruder detection increases, when the distance between the node and external object increases.

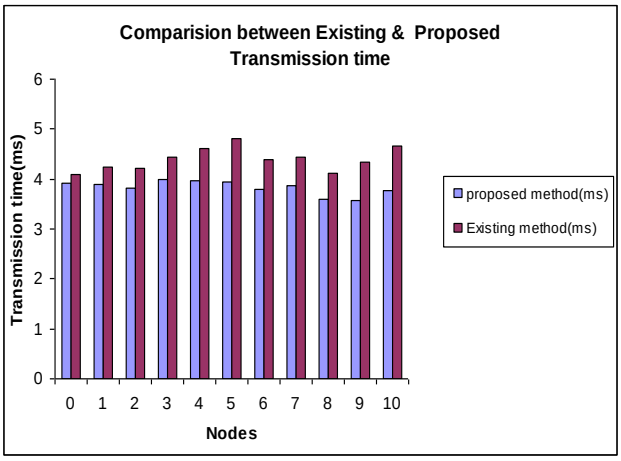

Figure 6:Comparison between existing & proposed transmission time(ms)

Figure 6 shows the Comparative analysis between existing and Proposed transmission time(ms). It is clearly found that the transmission time of the proposed method is lower than that of the existing method.

7. CONCLUSION

Though Bluetooth scatternet network is secure, it is susceptible to various attacks such as blue-snarf, blue-bug, and misappropriation of devices, man-in-the-middle attacks and eavesdropping. So, we are providing the security using the Intelligent Surveillance Algorithm (ISA). The presented Bluetooth security integrated system is more useful in confidential areas such as military. Our system is also useful in remote controlled Bluetooth enabled environment to make it more secure. The network laid in remote place can protect from hacking and misappropriation.

As it is known that attacks such as bluesnarf uses brute force approach are time consuming. From the results, it is obvious that the ISA algorithm detects the intruder within the short time and prevents from such attacks quickly. The work has demonstrated that the scatternet network has been successfully secured and monitored by the Intelligent Surveillance Algorithm (ISA) which provides many issues for further investigation and research. The algorithm is implemented based on detecting a single intruder. It can be extended for detecting multiple intruders in the proposed scatternet network. The future work also includes in detecting intruder of various innovative attacks that will also include different strategies for enhancing the work using WIFI, WIMAX.

8. REFERENCES

[1] T. Hodes, M. Newman, S. McCanne, R. Katz, J.Landay.1998. Shared Remote Control of a Video Conferencing Application: Motivation,Design, and Implementation. SPIE Multimedia Computing and Networking (MMCN. vol. 3654. 17-28.

[2] B. Myers, H. Stiel, and R. Gargiulo.1998. Collaboration Using Multiple PDAs Connected to a PC.Proceedings CSCW'98: ACM Conference on Computer-Supported Cooperative Work. 285-294.

[3] M. Roesch.1999. SNORT - lightweight intrusion detection for networks. In 13th LISA Conference.

[4] Juha T. Vainio. 2000. Bluetooth Security., Helsinki University of Technology.

[5] J.Anderson.2001. Computer security threat monitoring and surveillance. James P. Anderson Co., Tech. Report.

[6] C.Law and K.Y.Siu,.2001.A Bluetooth Scatternet Formation Algorithm. IEEE Symposium on Ad Hoc Wireless Networks.3519-3522.

[7] .Jennifer Bray and Charles F Sturman.2001. Bluetooth: Connect Without Cables. Prentice Hall.

[8] Satyajit Chakrabarti.2002. Bluetooth Scatternet Formation and Internetworking with 802.11 and GPRS . University of Kalyani.1-109.

[9] G. Tan and J. Guttang. 2002. A locally coordinated scatternet Scheduling Algorithm. In the 27th Annual IEEE Conference on Local Computer Networks (LCN), Tampa, Florida.1-11.

[10] Chakrabarti, Liyun Wu , Son Vuong, Victor C.M. Leung.2004. A Remotely Controlled Bluetooth Enabled Environment. Satyajit University of British Columbia Vancouver, Canada.77-81.

[11] Mahtab Hossain A.K.M. and Wee-Seng Soh.2007.A comprehensive study of bluetooth signal parameters for localization. IEEE Symposium on Personal, Indoor and Mobile Radio Communications. 1-5.

[12] Karen Scarfone and John Padgette. 2008. Guide to Bluetooth Security (Draft).NIST Special Publication 800-121.2008. 1-43.

[13] MAJ Terrence Oconnor, Dr. Douglas reeves. 2008. Bluetooth network-based misuse detection. Annual computer security applications conference. IEEE Computer Society.377-391.

[14] Barrales-Guadarrama R .,Rodrí guez -Rodrí guez M .E., Barrales-Guadarrama V .R. and Mocholí -Salcedo A.2010.A Bluetooth Development platform for Wireless Sensors. IEEE Conference on Electronics, Robotics and Automotive Mechanics (CERMA).213-219.

[15] Guotao Zhao, Huadong Ma, Yan Sun, Hong Luo and Xufei Mao.2011.Enhanced surveillance platform with low-power wireless audio sensor networks. IEEE Symposium on World of Wireless, Mobile and Multimedia Networks .1-9.

[16] Han Bin.2011.Research of Cluster based Intrusion deduction system in Wireless Sensor Networks.IEEE Conference on Internet Technology and Applications.1-4.

[17] Ishiguro K. and Runhe Huang. 2011.Implementation of a Wireless Communication technology based home Security System. IEEE Conference on Computer Research and Development.394-398.

[18] Trinh Minh Tri, Gatica-Perez and Daniel.2011. Contextual Grouping: Discovering Real-Life Interaction Types from Longitudinal Bluetooth Data. IEEE Conference on Mobile Data Management. 256-265.