AN INTELLIGENCE ENCRYPTION ALGORITHM FOR REINFORCING SECURITY IN BLUETOOTH COMMUNICATION

P.Prem Priya[1], J. Sherine Glory[2], R. Preethi[3]

*[1, 2, 3] Department Of Information Technology, RMK College of Engineering and Technology
Puduvoyal Chennai, (India)*

ABSTRACT

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. To enhance the security of data transmission in Bluetooth technology, the design of a network intrusion detection system using Bluetooth scatternet for discovering malicious traffic for surveillance and encryption algorithm of DES and RSA is proposed. The paper focuses to present a security integrated system that ensures the detection of the intruder which enters the scatternet network and also ensuring secure transmission of data. The experimental results show that the system can significantly improve the overall security of the scatternet network.

Keywords- Piconet, Surveillance, Intelligence Algorithm, E0 Key Stream, Triple DES, RSA

I. 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 sent and transmits chunks up to 79 frequencies [5, 10] with a gross data rate of 1 Mb/s. 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 [11]. 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. Encryption is an essential process to assure confidentiality and security. Over transmission channels and scatternet Network because channels are an open medium to intruders in which they can intercept and alter the contents of any transmitted information. Well known standardized encryption algorithms such as DES and AES were designed to achieve security against intruders. The Encryption algorithm using in Bluetooth encryption process is the E0 stream cipher [6]. However, this algorithm has some shortcomings, 128-bit E0 stream ciphers in some cases can be cracked by 0 (264) mode in some cases. Some commonly used Bluetooth enabled devices are vulnerable to exploitation using a range of methods including Bluesnarf, Backdoor and Bluebug [10]. These vulnerabilities can expose the user to a range of issues relating to privacy and security and are explored as follows.

1) 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].

2) 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].

3) 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.

II. VIEW OF THE PROPOSED NETWORK

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

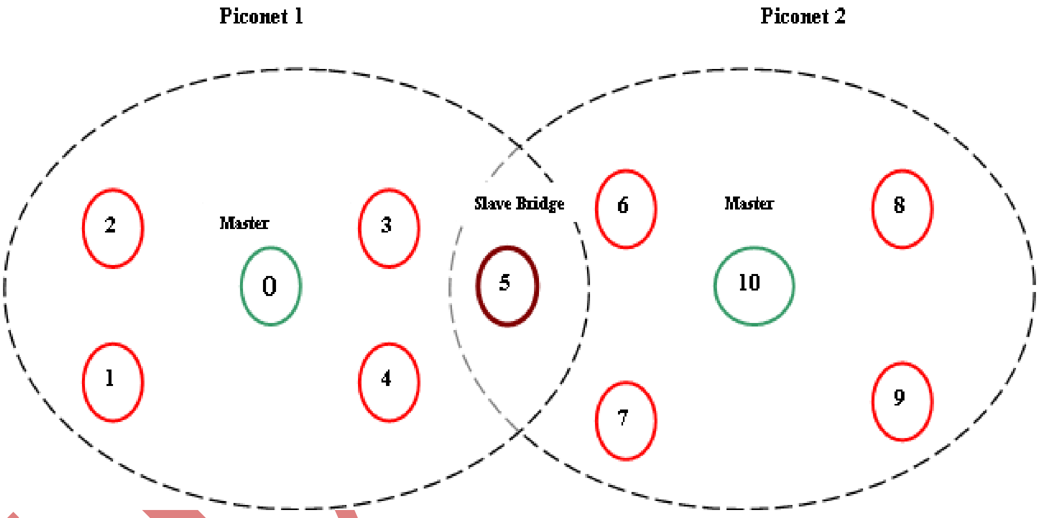

Fig1. Overall View of Network

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**].**

III. DESIGN OF DES ALGORITHM

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

3.1 Intelligence 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".

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

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.

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.
```

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.

3.2 DES and RSA Encryption Algorithm

3.2.1 Public Key Cryptography

Now, X being an external object and wishes to join a network and transmit data securely by standard encryption methods.

The public key is typically used for encryption, while the private or secret key is used for decryption.

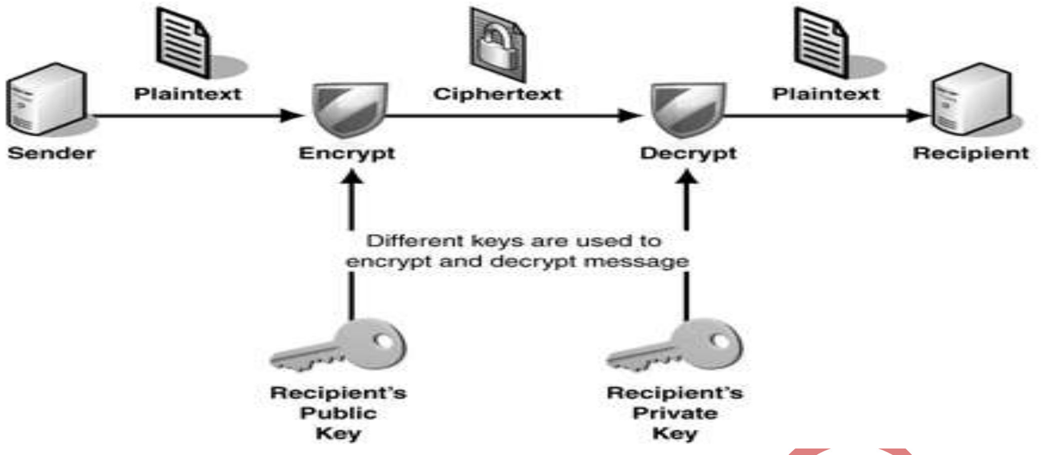

Fig 2.Public Key Cryptography

3.2.2 The ideas of proposed Algorithm

RSA algorithm is the first relatively complete public key algorithm. It can be used for data encryption, also can be used for digital signature algorithms. RSA cryptosystem is on the difficulty of integer factorization in the group ,and its security establishes in the assumption that constructed by almost all the important mathematicians, it is still a theorem that does not permit, which is lack of proof, but Mathematicians believe it is existent.DES is a group cipher algorithm, which encrypts data by a group of 64-bit. A group of 64-bit plaintext is entered from one beginning of the algorithm; 64-bit cipher text is exported from the other side. DES is a symmetric algorithm, encryption and decryption use the same algorithm (e the different key arrangement), the key can be any 56-bit value (the key is usually 64-bit binary number, but every number that is a multiple of 8-bit used for parity are ignored). This algorithm uses two basic encryption techniques, make them chaos and spread, and composite them. The entire hybrid encryption process is as follows: Let the sender is A, the receiver is B, B's public key is B, B's private key is dB, K is DES encryption session key(assuming that the two sides of communication know each RSA public key).

The process of Encryption: During the process of sending encrypted information, the random number generator uses 64-bit DES session key only once, it encrypt the plaintext to produce cipher text. On the other hand, the sender get debit's public key from public key management center, and then using RSA to encrypt session key. Finally, the combination of the session key from RSA encryption and the cipher text from DES encryption are sent out.

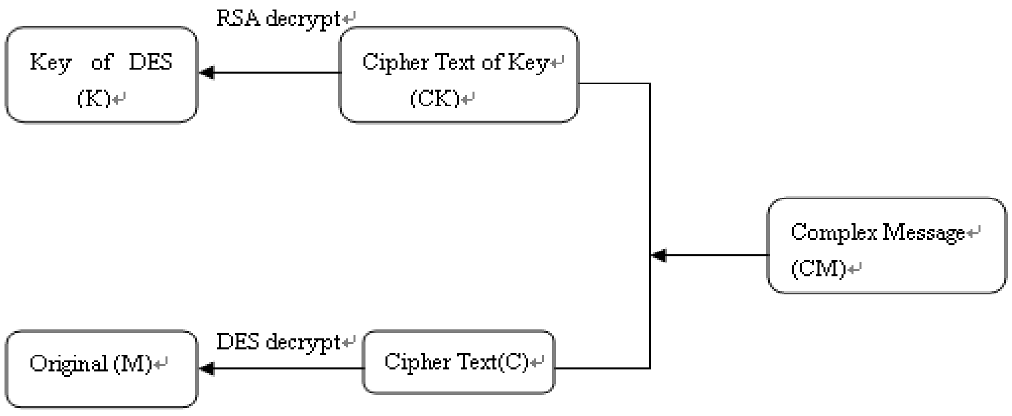

Fig 3.The process of Encryption

The process of Decryption: The decryption of hybrid encryption algorithm is as follows. The first, the receiver B divide received cipher text CM into two parts, one is cipher text CK from the RSA algorithm encryption, and the other is cipher text C from the DES algorithm encryption. The second, the receiver B decrypt cipher text CK by their own private key dB, receive the key K which belongs DES algorithm, then decrypt the cipher text C to the original M by key K. Figure is a decryption of hybrid encryption algorithm of RES and DES.

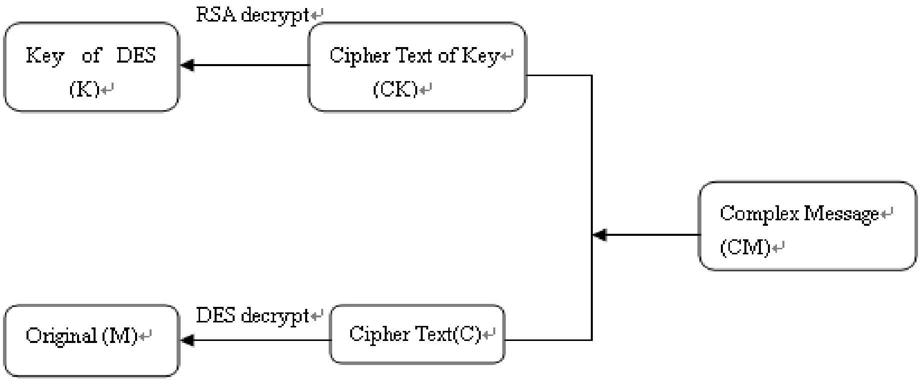

Fig 4.The process of Decryption

IV. IES ALGORITHM

The flow of the entire proposed IES algorithm is given in the fig 5.It describes the combination of both techniques discussed above: This is the design of the propose Intelligence Encryption algorithm.

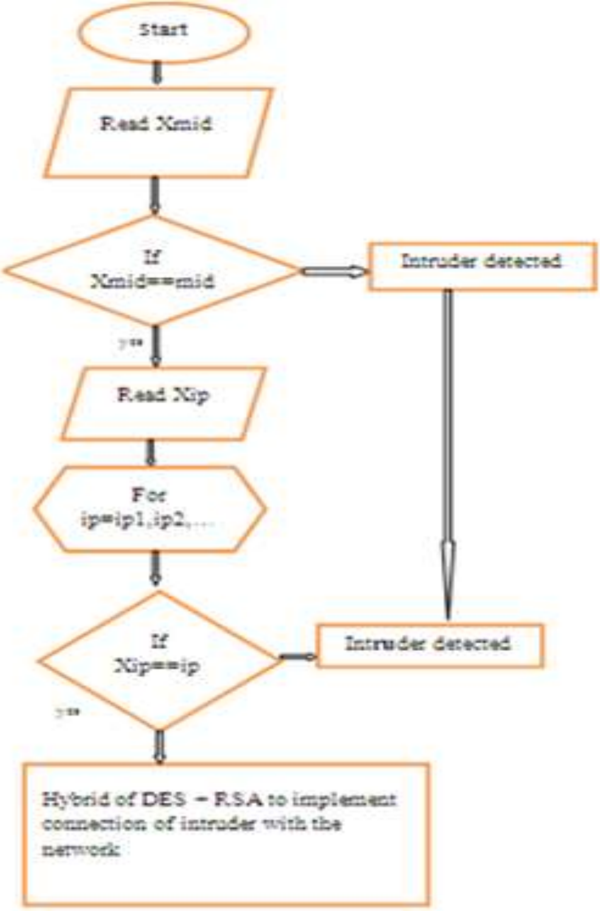

Fig 5: Overall Design Of IES Algorithm

V. RESULTS AND DISCUSSION

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

Table-1: Proposed Scatternet Network Detail

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 4 show 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 7 represents the Node and the Intruder Detection Time 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

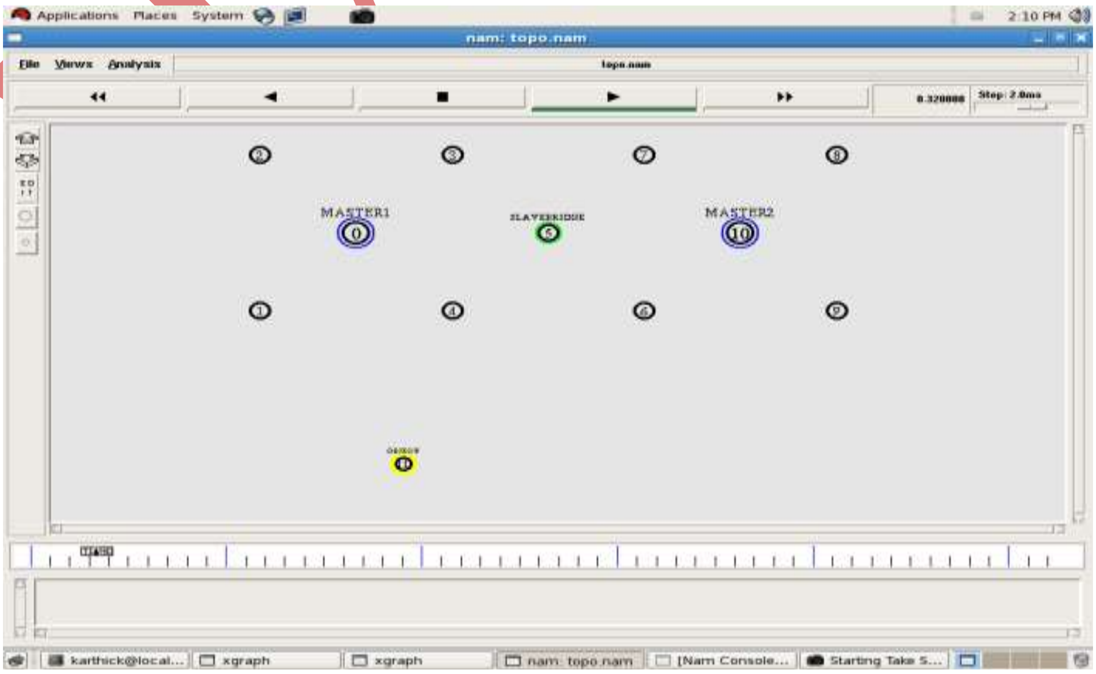

Figure 6: Initial Network Arrangement

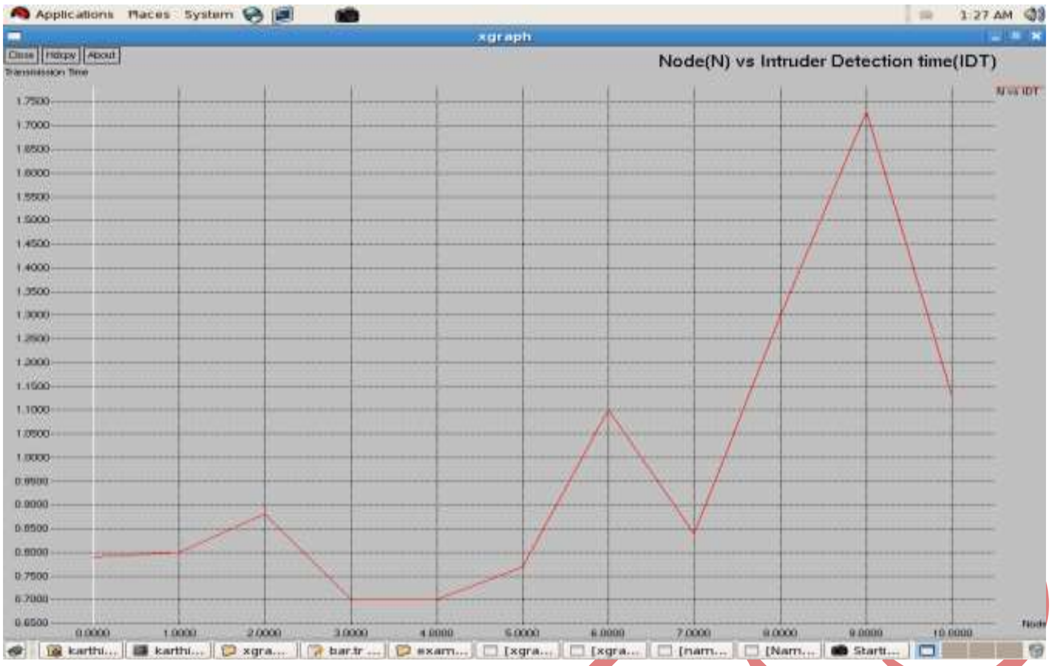

Figure 7: Node Vs. Intruder Detection Time

DES and RSA Encryption Result

- Using RSA algorithm and the DES key for data transmission, so it is no need to transfer DES key secretly before communication.
- Management of RSA key is the same as RS situation, only keep one decryption key secret.
- Using RSA to send keys, so it can also use for digital signature.
- The speed of encryption and decryption is the same as DES. In other words, the time-consuming RSA just do with DES keys.

VI. 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 (IEA). 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, since DES and RSA is more secure and easier to achieve.

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.

REFERENCES

[1] R.Kanthavel and R.Dhaya, 'Proposal of an Intelligent Surveillance Algorithm for ScatternetNetwork", International Journal of Computer Applications, vol no.6.pp. 0975-887, 2012.

[2] Trinh Minh Tri,Gatica-Peerz and Daniel,"Contextual Grouping: Discovering Real Life Interaction Types from Longitudinal Bluetooth Data",IEEE Conference on Mobile Data Management, vol no.3,pp. *256*-265,2011.

[3] Han Bin,"Reasearch of Cluster Based Intrusion System Wireless Sensor Networks",IEEE *Conference on Internet Technology and Applications*,pp. *1-4*,2011.

[4] Isniguro .K and RunheHuang,"Implementation of a Wireless Communication Technology Based Home Security System",*IEEE Conference on Computer Research and Development* ,vol no.4,pp.394-398,2011.

[5] M. Roesch," SNORT - lightweight intrusion detection for networks", *LISA Conference ,1999*.

[6] Juha T. Vainio. "Bluetooth Security", *Helsinki University of Technology*,pp.410-560,2000.

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

[8] C.Law and K.Y.Siu,".A Bluetooth Scatternet Formation Algorithm.",*IEEE Symposium on Ad Hoc Wireless Networks*,vol no.13.pp..*3519-3522,2000.*.

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

[10] Satyajit Chakrabarti,"Bluetooth Scatternet Formation and Internetworking with 802.11 and GPRS ", *University of Kalyani*,pp.1-109, 2002.

[11] Guotao Zhao, Huadong Ma, Yan Sun, Hong Luo and Xufei ".Enhanced surveillance platform with low-power wireless audio sensor networks", *IEEE Symposium on World of Wireless, Mobile and Multimedia Networks* ,pp.1-9, 1999.