Implementation of Security Mechanism for Bluetooth Communication

[1]D. Hema Latha, [2]D. Rama Krishna Reddy, [3]K. Sudha, [4]T.S. Savita, [5]Azmath Mubeen

[1]Dept of Computer Science, Osmania University College for Women,Hyderabad,Telangana,India
[2]Dept of Mathematics, Osmania University, Hyderabad,Telangana,India
[3]Dept of Computer Science, osmania University, Hyderabad,Telagana,India
[4]Dept of Computer Science, Osmania University College for Women,Hyderabad,Telangana,India
[5]Dept of Computer Science, Osmania University College for Women,Hyderabad,Telangana,India

Abstract - **Bluetooth is a low cost and low power radio communication technology which uses 2.4 GHz.. the Industrial, Scientific *and* Medical (ISM) unlicensed frequency bands. It is mainly used to interconnect small hand held devices and other electronic equipment that may use infra-red communication. Bluetooth communication does not require line-of sight and can be used to form small ad-hoc networks of devices, the network is formed spontaneously. Bluetooth supports a single connectionless data channel of 789 k bits/sec and up to three synchronous PCM encoded voice channels.**

In this paper, mainly the focus is on the implementation of security mechanism for Bluetooth communication. It is personal area network (PAN), one kind of wireless Ad-hoc network. Bluetooth communication range is categorized as high, medium and low.. depending upon level of the power. High range of Bluetooth communication is up to 91 meters, middle range distance is up to 9 meters and minimum range is up to 1 meter. In Bluetooth communication at the link level, Authentication and Encryption are the main security features. A secret link key is used to achieve these security features that are shared between two Bluetooth devices.

Keywords— **Bluetooth security; E0 key stream; encryption; authentication; key generation and key initialization.**

I. INTRODUCTION

Bluetooth was first started by Ericsson Company and named for the nickname of the Danish King Harald Blatland. Depending upon the power consumption of the device, the communication range of the Bluetooth may vary from 1 meter to 100 meters and version 2 with enhanced data rate (EDR) can operate up to 3 M bits/sec. It shares this in common with IEEE 802.11 Wi-Fi local area network technology but whereas IEEE802.11 has a range of 100 meters and a speed of 11 M bits/sec, Bluetooth performance [1] has a range of 10 meters and a speed of 1 M bits/sec. Bluetooth supports a single connectionless data channel of 789 k bits/sec and up to three synchronous Pulse Code Modulation (PCM) encoded voice channels.

Three strategies are used to connect Bluetooth devices. 1) Voice/ Data Access Points: In this strategy the computing device is connected to a communication device or a wireless channel to share the communication connection with a non-peripheral device. 2) Peripheral Interconnect: In this approach peripheral devices such as the keyboard, mouse and headsets are connected to other type of devices. 3) Personal Area Networking (PAN): This model provides a method for connecting devices with each other in an ad hoc fashion which makes the data transmission fast and easy. PAN model can be implemented for Wireless sensor Networks.

A. Bluetooth Architecture and Protocols

Bluetooth architecture is divided into several layers, based on their functions, as shown in the Figures 1, 2 and 3

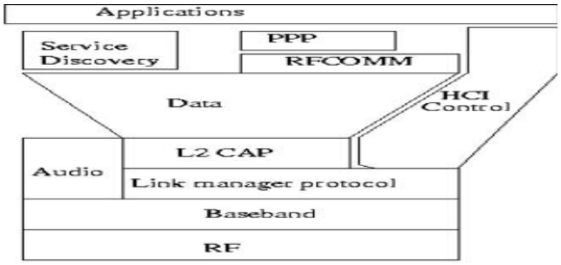

Fig. 1 Bluetooth architecture

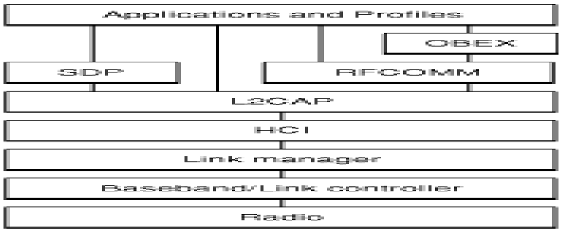

Fig. 2 Bluetooth architecture

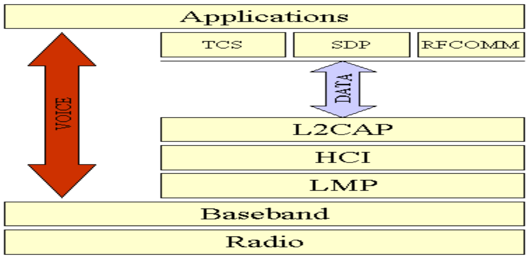

Fig. 3 Bluetooth architecture

1.1 *Radio Frequency (RF) Layers*: The radio layer provides physical wireless connection between the communicating devices. It uses ISM frequency band range in order to reduce collisions with other devices. This layer uses frequency mapping to separate the range into 79 MHz bands, which starts at 2.402 GHz and ends at 2.480 Hz and uses this spread spectrum to hop from one channel to another, up to 1600 times per second. This layer also performs frequency hopping at the rate of 1600 hops/sec which makes eavesdropping difficult. Devices implement one of following three security modes:

- Mode 1 - insecure, here no security measures are used.
- Mode 2 - service-level security, here security is not provided before channel is established.
- Mode 3 - link-level security, here security measures are established before a link setup.

Different security polices can be used in parallel.

1.2 Base *band layer*: The base band layer 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 it forms a small network called a piconet, shown in fig. 4. Bluetooth enabled devices can be either in a master or a slave mode. A group of devices in which one device is designated as master and the remaining as slaves which builds a network called a **piconet** [2], shown in Fig. 4. At the same time the device can be a slave in several piconets. And also a device can also be a slave in one piconet and a master in another. This type of a network topology is called a scatter net.

Master: It's the Bluetooth device that initiates communication. The master sets up the time and broadcasts its clock to all slaves providing with the hopping pattern, in which the same hop frequency is maintained.

Slaves: All the devices will be in slave state if they are connected to one another. The device can be an active slave if it transmits or receives data from the master actively or a passive slave if it is not currently sending or receiving any information. By enabling their RF receivers periodically, the passive slaves check if there is a connection request from the master.

Standby: All devices which are not connected to a master (i.e., not slave), will be in standby mode A device enters the inquiry state, when it is searching for other devices. A device enters the page state, when it starts creating a Bluetooth link. Sometimes the device may go to low power mode to save power.

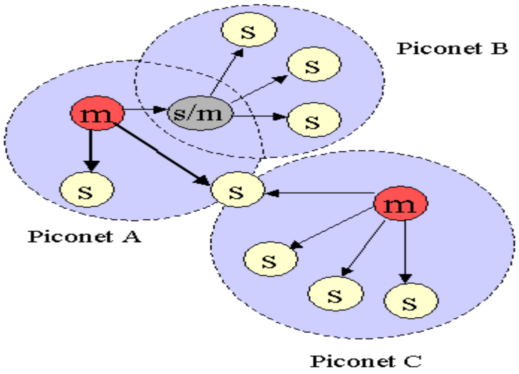

Fig. 4. Piconet

1.3 *Link 2 Manager Protocol (LMP):* The LMP protocol utilizes the connections established between devices with the help of base band layer to create logical connection responsibilities of the LMP. Security aspects and device authentication are also taken care by this layer.

1.4 *Logical Link Control and Adaptation Protocol (L 2CAP) :* The main function of L2CAP is to receive applicative data from higher layers and convert it to the Bluetooth format so that it can be transmitted to the higher layer protocol over the base band.

1.5 *Radio Frequency Communication Protocol (RFCOMM):* The RFCOMM is follows the serial connections over the base band layer to provide transport capabilities for higher level services and avoid direct interface with the application layer with L2CAP.

1.6 *Service Discovery Protocol (SDP):* This protocol is used to discover services and provides the basis for all the usage models.

1.7 *Telephony Control and Signaling layer (TCS):* This protocol supports call control signaling in order to establish speech and data calls between Bluetooth devices. TCS signaling messages are carried over L2CAP.

1.8 *Application Layer:* The application layer provides user applications. The applications interact with the RFCOMM protocol layer to establish an emulated serial connection. [3].
Related work on protocols assessment for wireless sensor networks (WSN) [4] was carried out and the security mechanism discussed, for implementation to Wireless Sensor Networks.

II. BLUETOOTH SECURITY

Security for Bluetooth [5] is provided on the radio paths, link authentication and encryption can be provided, however, true end-to-end security is not possible without providing security solutions for the upper layers of Bluetooth. Basically, Bluetooth security architecture [6] mainly focuses on the following three security services:
Confidentiality: The main goal of Bluetooth is confidentiality or privacy. This service prevents an Eavesdropper from hacking crucial and critical information. With this security service, only the authorized user can access the data.
Authentication: The second goal of the Bluetooth is providing identity verification of the communicating devices. Authentication allows the communicating devices to recognize authorized user, if the user is not authorized user communication is aborted.
Authorization: Access control of the resources is the third goal of the Bluetooth. This is accomplished by deciding the authorized users to use the resources.

III. KEY MANAGEMENT

Bluetooth system provides various types of keys to ensure secure transmission. The main important key is the link key that is used between two Bluetooth devices for authentication. An encryption key is derived from the link key. This provides security for the data in the packet and is regenerated for all new transmissions.

A. *Link key*

To cover various applications four types of link keys are defined. All the keys are 128-bit random numbers and are either temporary or semi-permanent. Unit key, KA, is extracted at the installation of the Bluetooth device from a unit A. The storage of KA needs very less memory space and used when device has less memory or when the large group of users has to access the device. Combination key, KAB, is derived from two pair of devices A and B. When more security is needed, combination key is generated and used for each pair of devices. This requires more memory, as the device has to store one combination key separately for each connection it has. The master key, K is used when the master device wants to transmit to several devices simultaneously. It over rides the current link key for one session only. The initialization key- K init, used in the initialization process. This key protects initialization parameters when they are transmitted. This key is formed from a random number, an L-octet PIN code, and the BD_ADDR of the applicant unit.

B. Encryption key

Encryption key is extracted from the current link key. Encryption key will be changed automatically when ever encryption is required. The purpose of separating the authentication key and encryption key is to facilitate the use of a shorter encryption key without weakening the strength of the authentication procedure.

C. PIN code

PIN is a number, which can be chosen or fixed by the user. Its length usually 4 digits, but it can also be between 1 - 16 octets. And it can be changed by the user when required and this adds security to the system. The PIN is used by entering into one device (fixed PIN), but it will be safe to enter into both units. Example, the later one can be used for laptop and phone communication. Encryption and key control in shown in Figure 5

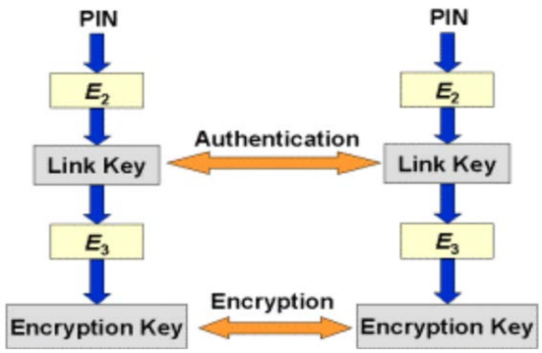

Figure 5. Encryption and key control

3.4 Key Generation and Initialization

During an initialization phase keys exchange takes place that is carried out separately for each two units that needs to implement authentication and encryption. The initialization procedure consist of five parts: Generation of an initialization key, Authentication, Generation of link key, Link key exchange and Generating of encryption key in each unit.

After this key generation and initialization procedure, the connection is established or the link can be aborted, as shown in the following figures 6 and 7

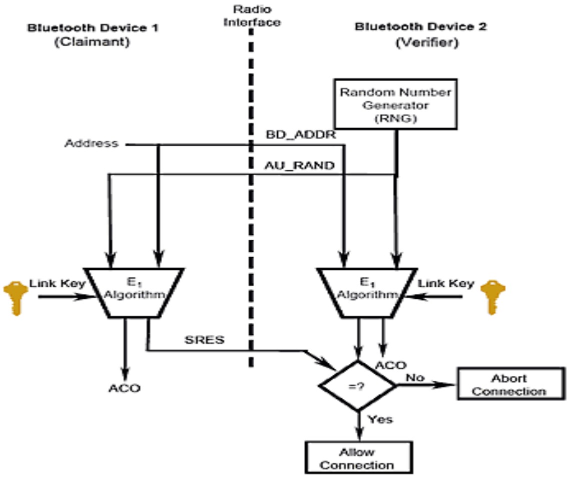

Fig. 6. Key generation and initialization process

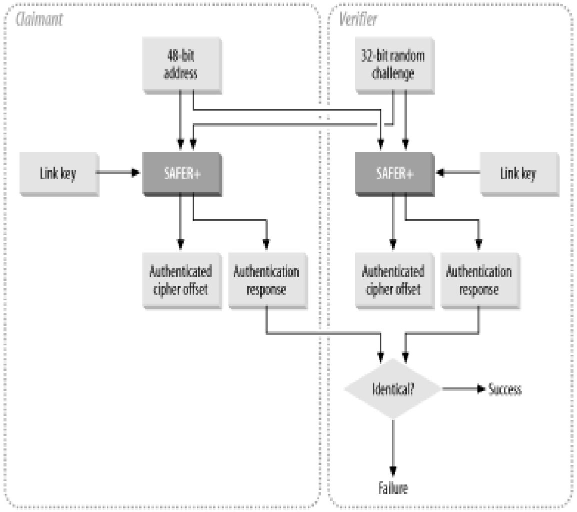

Fig. 7. Key generation and initialization process

Bluetooth security keys

The security keys used in Bluetooth are: *Unit Keys, Combination Keys* and *Encryption Keys.*

a) Unit Key: The authentication and encryption techniques which are based on unit keys are the same as those based on combination keys. But, a unit that uses a unit key is able to use only one key for all of its secure connections as it has to share this key with all other units that it trusts. For all these trusted devices there may be chance of eavesdrop on any traffic based on this key. A trusted unit which is modified or tampered may also be able to imitate the unit by distributing the unit key. So, unit key may not provide security against attacks from trusted devices.[7]

b) Combination Key: This key is generated during the initialization process if the devices decide to use. At the same time the combination key is generated by both the communicating devices. First, both devices generate a random number. Both devices generate a key with the key generating algorithm E21, combining the random number and their Bluetooth device addresses. After that, the devices exchange random numbers securely and calculate the combination key (Kab) that is to be used between them as shown in Fig 8

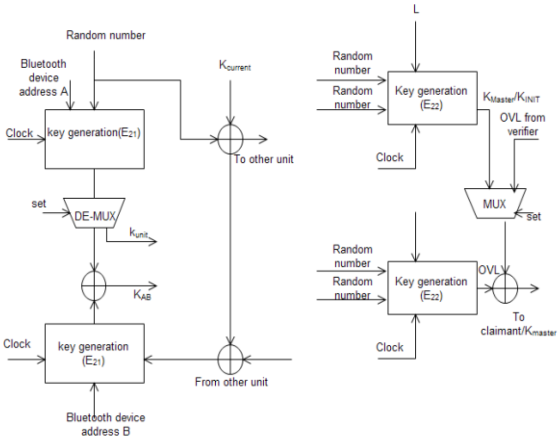

Fig 8: Link Key generation

c) Encryption key: This key is generated from the present link key, that is, a 96-bit Ciphering Offset Number (CON) and a 128-bit random number. The Ciphering Offset Number is based on the Authenticated Ciphering Offset (ACO) that is generated during the authentication process. The encryption key is generated, when the Link Manager (LM) activates encryption and it is changed automatically every time when the Bluetooth device enters the encryption mode [8]. All security transactions are made ready between two or more communicating devices and are handled by the link key. The link key is a 128- bit random number and is used in the authentication process and as a parameter when extracting the encryption key. The link key life span depends on whether it is a semi-permanent or a temporary key. A semi-permanent key can be used after the current session is completed authenticate Bluetooth devices that share it. A temporary key will be available only till the current session and cannot be reused. In multipoint connections temporary keys are used, where the same information is transmitted to more than one recipient. The length of the Personal Identification Number (PIN) code used in Bluetooth devices and can vary between 1 and 16 octets. The regular 4-digit code will be sufficient for some applications, but for higher security applications it may need lengthy codes. The PIN code of the device can be made permanent, so that it requires to be entered only to the device willing to communicate or connect. During the initialization process the PIN code must be entered to the both devices.

IV. ENCRYPTION PROCESS

In Bluetooth encryption system, the user data or user payload is encrypted, which is shown in Fig. 9. This is accomplished with a stream cipher E0 that is re-synchronized for every user data or payload. The E0 stream cipher is composed of user payload key generator, the key stream generator and the encryption/decryption portion. The payload key generator combines and arranges the input bits in an appropriate order and transfers them to the four Linear Feedback Shift Registers (LFSR) of the key stream generator. The payload key generator combines and arranges the input bits in an appropriate order and transfers them, based on whether a device uses a semi-permanent link key or a master key; there are various encryption approaches available. The broadcast traffic is not encrypted properly if the unit key or a combination key is used, means separately addressed traffic may be encrypted or may not be encrypted. When a master key is used, there are three possible approaches. In encryption approach 1, data or traffic encryption is not performed. In encryption approach 2, the encryption of broadcast traffic is not performed, but the independently addressed traffic is encrypted with the help of master key. And in encryption approach 3, all the traffic encryption is done with the master key [9]. The size of the encryption key used between two devices must be discussed and adjusted, as the encryption key size varies from 8 bits – 128 bits. In each and every device, there will be a parameter that defines the maximum allowed key length. In the negotiation for key length, the master sends its suggestions to the slave about the encryption key length. The slave device may either accept and acknowledge it, or send another suggestion. This is continued, until an agreement is reached or any one of the devices aborts the negotiation. The used application aborts the negotiation. Every application defines minimum acceptable key size, and if the requirement is not met by either of the devices or participants, the application aborts the negotiation and the encryption is not performed. This is essential to avoid a malicious device which forces the encryption to be low in order to do some harm [10].

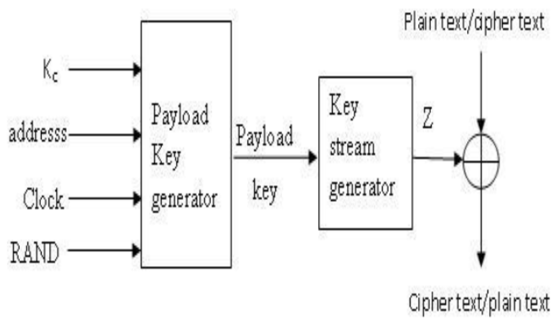

Fig 9: The Stream Cipher System E0

V. AUTHENTICATION

The Bluetooth authentication strategy makes use of challenge response method that is illustrated in the Fig. 10. In this method a two - move protocol is used to enquire whether the other party knows about the secret key. This two – move protocol use symmetric keys, means the successful authentication is based on the fact that both participants share the same key. The Authenticated Ciphering Offset (ACO) is computed and stored in both devices and is used for cipher key generation later on. The verifier sends the applicant a random number for authentication. Then, both the participants use the authentication function E1 with the random number, the applicants Bluetooth Device Address and the present link key to get a response. The applicant sends the acknowledgement or response to the verifier, who makes sure that the acknowledgements or responses match. The used application notifies which user is to be authenticated. So the master may not be compulsorily the verifier. Few applications may need only one-way authentication, such that only one party is authenticated. This is not being true in all situations due to mutual authentication sometimes, where both parties are authenticated in turn. When an authentication fails, there will be certain time period until a new attempt for authentication is made. The time period is increased twice for each consequent failed attempt from the same address, until the maximum waiting time is attained. The waiting time may decrease to a minimum when no failed authentication attempts are made [11].

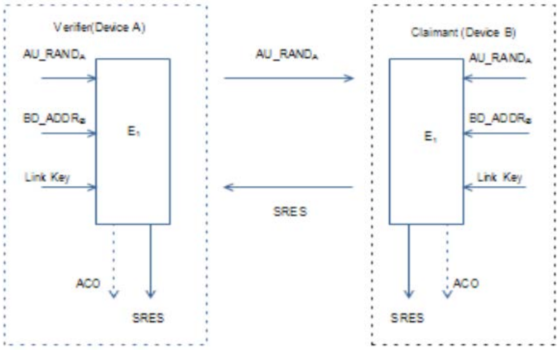

Fig 10: Challenge response for Bluetooth

VI. SECURITY METHODS FOR BLUETOOTH

Security Method 1- In this security method the Bluetooth device does not initiate any security operation, allowing other Bluetooth devices to initiate connections with it. This is the most insecure method

Security Method 2- In this method security is provided after the establishment of the link between the devices at the L2CAP layer. This method provides flexible security guidelines which involves application layer controls that function in parallel with the below protocols.

Security Mode 3- This method carry out security controls such as authentication and encryption at the Baseband layer itself, before the connection is established. The security manager usually imposes this onto the LMP layer. Bluetooth [12] allows security levels to be defined for both devices and services. For devices there are two possible security levels. A remote device can be a trusted or un trusted device. Trusted device will have access to all services for which the trust relationship has been established. An untrusted device will have restricted access to services. Typically such devices would not share a permanent relationship with the other device.

Comparative study on Intrusion Detection System in Mobile Ad-hoc Networks (MANETs) [13] work is worth mentioning.

VII. CONCLUSIONS

Discussed the Bluetooth Architecture and Functions of each layer. Proposed a secret link key generation to provide security for Bluetooth systems. Generation and initialization process of Secret key is discussed. Described the Encryption, authentication processes and security methods. Further, Bluetooth security can be enhanced with other mechanisms like key pairing function.

VIII. REFERENCES

[1] Yujin Lim, Jesung Kim, Sang Lyul Min and Joong Soo Ma, “Performance evaluation of the Bluetooth-based public Internet access point”, in proceedings of the 15th International Conference on Information Networking, pp. 643 – 648, 2001.

[2] Wang Feng, Arumugam, N. and Krishna, G.H., “Performance of a Bluetooth piconet in the presence of IEEE 802.11 WLANs”, in proc of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1742 - 1746 vol. 4, 2002.

[3] Christian Gehrmann, Bluetooth™ Security White Paper, Bluetooth SIG Security Expert Group.

[4] D.Hema Latha, D.Rama Krishna Reddy and K.Sudha, “Assessment of Medium Access Control Protocols in Wireless Sensor Networks” 3rd National Conference on Computer Networks and Information Security (NCCNIS 2014), *Vasavi College of Engineering, Hyderabad, India.*

[5] Antnan ,Bluetooth Security, Communication security Department,Ruhr University,Bochum.

[6] Kent, S. & Atkinson, R., “Security Architecture for the Internet Protocol”, IETF RFC 2401, 1998.

[7] Paraskevas Kitsos, Nicolas Sklavos,Kyriakos Papadomanolakis, and Odysseas Koufopavlou, Hardware Implementation of Bluetooth Security,*University of Patras, Greece.*

[8] Daniele Miorandi,Carlo Caimi, Andrea Zanella, Performance Characterization of a Bluetooth Piconetwith Multi Slot Packets.

[9] R. C. Merkle. Secure communications over insecure channels. Communications of the ACM, 21(4):294–299, 1978.

[10] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.

[11]BluetoothSIGSpecifications:https://www.bluetooth.org/Technical/Specifications/adopted.htm.

[12]Trifinite Group(Bluetooth security Research) - http://trifinite.org/

[13] Azmath Mubeen, D. Hema Latha, D.Rama Krishna Reddy, “A comparative study on Intrusion detection systems I mobile ad-hoc networks”,
IJRDTM – Kailash | ISBN No. 978-1-63041-994-3| Vol.20 | Issue 08 2013, http:// www.ijrdtm.com | http://journal.rtmonline.in, Published by: Modern Rohini Education Society (Regd.) | Paper Id: IJRDTM-05256 Page 1, International Journal of Research & Development in Technology and Management Sciences.