RESEARCH ARTICLE OPEN ACCESS

A Design Approach for Wireless Communication Security in Bluetooth Network

C.Suresh [1], V.Vidhya [2], E.Shamli [3], R.Muthulakshmi [4], S.Menaka [5]
B.Tech Information Technology (Final year) [1]
B.E Computer Science Engineering (Final year) [2] & [3]
B.E Computer Science Engineering (third year) [4] & [5]
Mailam Engineering College
Mailam - India

ABSTRACT

Exponential growth of the volume of Bluetooth-enabled devices indicates that it has turned into a mainstream method for remote interconnections for trading data. Bluetooth technology has turned into a vital piece of this advanced society. The accessibility of cellular telephones, diversion controllers, Personal Digital Assistant (PDA) and Personal computers has made Bluetooth a popular technology for short range wireless communication. However, as the Bluetooth technology becomes wide spread boundless, vulnerabilities in its security protocols are expanding which can be possibly hazardous to the protection of individual data of client. It is the sort of remote Ad hoc system. Ease, low power, low many-sided quality and strength are the fundamental gimmicks of Bluetooth. It takes a shot at Radio recurrence. Bluetooth correspondence extent is sorted as high, medium and low relying on force level. High scope of Bluetooth correspondence is dependent upon 91 meter, medium extent is dependent upon 9 meter and low range is dependent upon 1 meter. Bluetooth is an as of late proposed convention for nearby remote correspondence and has turned into a true standard for short-extend impromptu radio associations. Security concern is a standout amongst the most imperative issues deferring the mass selection of Bluetooth. This article gives a study on the security issues behind the Bluetooth standard. After an outline of the general Bluetooth convention, a security system is presented for the depiction of the Bluetooth security design. At that point both connection level and administration level security plans are talked about in subtle element on the premise of the system. A few shortcomings of the Bluetooth security systems are investigated, together with potential dangers and conceivable assaults against the vulnerabilities. Comparing countermeasures are additionally proposed so as to enhance the Bluetooth security.

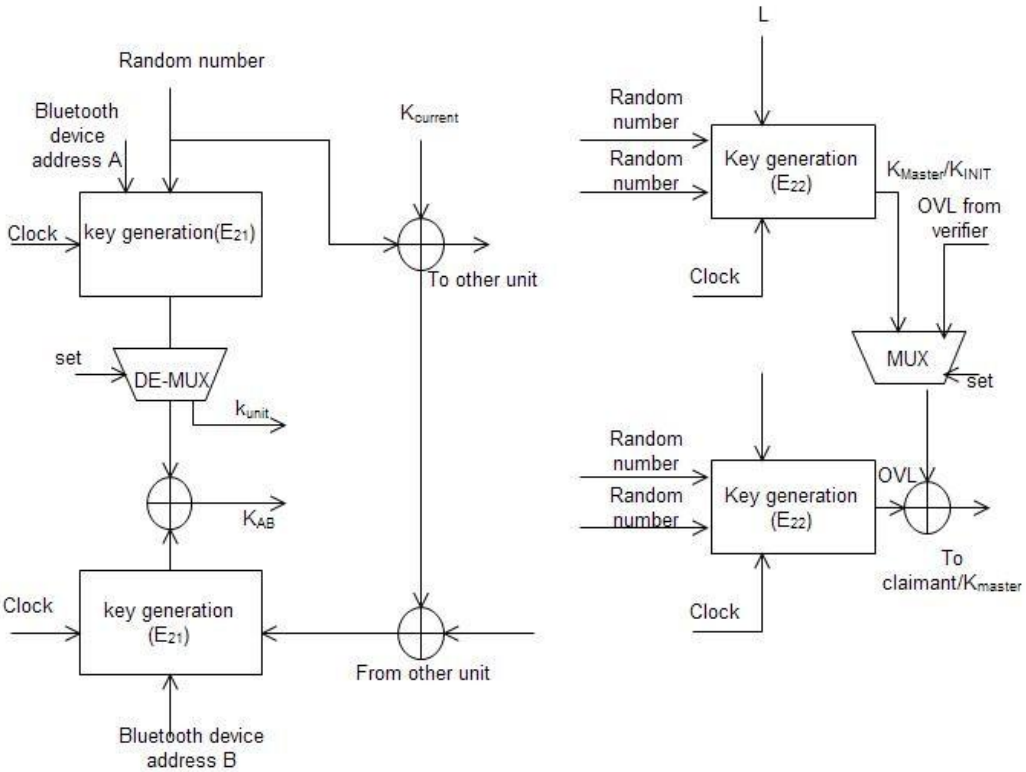
Keywords:- Bluetooth Security, WPAN, PDA, Bluetooth Protocol, RF, L2CAP, RFCOMM, LMP.

I. INTRODUCTION

Bluetooth [1, 2] is a wireless communication technology for short range communication. It was developed by Ericsson in 1994. It uses short wavelength radio transmissions from mobile or fixed devices. The Bluetooth system operates in the worldwide unlicensed 2.4 Ghz ISM frequency band. To make the link robust to interference, it employees a Frequency Hopping (FH) technique, in which the carrier frequency is changed at every packet transmission. Tominimize complexity and to reduce the expense of the transceiver a simple binary Gaussian frequency shift keying modulation is adopted. With a specific end goal to permit effective wideband information transmission the bit rate is 1 Mbps. Two or more Bluetooth units having the same channel structure a piconet. Inside a piconet a Bluetooth unit can be either ace or slave. Inside every piconet there may be stand out expert and up to seven dynamic slaves. Any Bluetooth unit can turn into an expert in a piconet. Besides, two or more piconets can be interconnected, framing what is known as a Scatter net. The association point between two piconets comprises of a Bluetooth unit that is a part of both piconets. A Bluetooth unit can all the while be a slave part of numerous piconets, yet an expert in stand out, and can just transmit and get information in one piconet at once, so investment in various piconets must be on a period division multiplex basis.

The primary design goal of Bluetooth is a cable replacement protocol for wireless connectivity. Presently it has reached out to incorporate the application situations of both voice/data access points and personal ad hoc networks. A diverse set of wired and wireless devices are Bluetooth connectable, including office appliances, *e.g.*, desktop PCS, printers, projectors, laptops, and PDAS; communication appliances, *e.g.*, speakers, handsets, pagers, and cellular telephones; home machines, *e.g.*, DVD players, computerized cams, cooking stoves, clothes washers, iceboxes, and indoor regulators. Bluetooth is suitable for an extensive variety of uses, *e.g.*, wireless office and

gathering room, savvy home and vehicle, insightful stopping, electrical paying and managing an account. Bluetooth is an accepted standard for pervasive devices to attain to the pervasive integration by low-power, short-range, minimal effort installed radio. The typical transmitting force is 1mw (0dbm) and the alternative is 100mw (-30 to +20dbm). The typical extent is 10m and the noncompulsory one 100m. Power utilization is from 20ma to 30ma on diverse working states. The expense of a solitary chip Bluetooth arrangement hopes to be around $5 every gadget. Bluetooth embraces an expert slave construction modeling to structure a specially appointed remote system named piconet. An expert in a piconet may correspond with up to seven dynamic slaves. A few joined piconets can further structure a scatter net. Bluetooth particular is a free open standard and the most recent adaptation 1.1 was endorsed in February 2001 [3, 4]. The Wireless Personal Area Network (WPAN) standard, created by the IEEE 802.15 Working Group [5], is focused around the Bluetooth. Security is constantly a standout amongst the most critical issues to any correspondence procedure. In a remote situation, for example, the Bluetooth, this issue gets to be more serious for the completely outside transmission. The point of this paper is to give a study on Bluetooth security, including a diagram of the essentials, a presentation of execution issues, and an examination of potential vulnerabilities. The Bluetooth framework gives full-duplex transmission utilizing an opened time division duplex (TDD) plan where each one opening is 0.625 ms in length. Expert to-slave transmissions dependably begin in an even-numbered time opening, while slave-to-ace transmissions dependably begin in an odd-numbered time space. An even-numbered time space and its ensuing odd-numbered time opening together are known as a casing. There is no immediate transmission between slaves in a Bluetooth piconet; transmission is just between an expert and a slave, and the other way around. The correspondence inside a piconet is sorted out such that the expert surveys each one slave.



Confidentiality: The first objective of Bluetooth is secrecy or security. This administration keeps a spy from perusing discriminating data. When all is said in done, with this security benefit just the approved client can get to the information. The methodology of changing information into a structure that it can't be comprehended without a key. Both information and control data can be scrambled.

Authentication: Providing personality confirmation of the imparting gadgets is the second objective of Bluetooth. Validation permits the conveying gadgets ready to perceive one another; henceforth correspondence prematurely ends if the client is not approved. The procedure of checking "who" is at the flip side of the connection. Verification is performed for both gadgets and clients.

Authorization: The third objective of Bluetooth is to control access to the assets. This is attained to by deciding the clients who are approved to utilize the assets The methodology of choosing if a gadget is permitted to have entry to an administration. Approval dependably incorporates valid.

II. MODES OF SECURITY

Every Bluetooth device can work on one of the 3 security modes. Mode 1 is a non secure mode in which a Bluetooth gadget should never launch any security technique. Mode 2 is administration level implemented security where a gadget does not start security systems before channel foundation at L2cap level, and whether to launch or not relies on upon the security prerequisites of the asked for channel or administration. Mode 3 is a connection level authorized security in which a Bluetooth gadget might start security methodology before the connection set-up at the LMP level is finished. Likewise, two levels of Bluetooth security plan can be distinguished, as takes after:

•Link-level security, relating to security mode 3. The Bluetooth gadget starts security techniques before the channel is built. This is the inherent security instrument and it is not mindful of administration/application layer security.

•Service-level security, relating to security mode 2. The Bluetooth gadget starts security techniques after the channel is built, *i.e.*, at the higher layers. This is a kind of add-in mechanism and is regarded as a practical issue.

III. LEVELS OF SECURITY

Bluetooth allows different security levels to be defined for devices and services. Two security levels can be defined for a device. A trusted device has unrestricted access to all or some specific services. Essentially this means that the device has been beforehand verified and stamped as "trusted". A depended device has confined access to administrations. Typically the gadget has been already validated however has not been checked as "trusted". An obscure device is additionally an endowed devices. Three levels of administration security are permitted to be characterized so that the prerequisites for approval, confirmation, and encryption can be set freely, including administrations that oblige approval and verification, benefits that oblige validation just, and administrations open to all devices. These three security levels can be described by using the accompanying three attributes.

Authorization Required: access is just allowed after an approval method. Just trusted devices would get programmed access.

Authentication Required: the remote devices must be verified before having the capacity to associate with the application.

Encryption Required: the connection between the two devices must be encrypted before the application can be accessed.

IV. LINK LEVEL SECURITY

Figure 2 illustrates the link-level security framework of Bluetooth. In the figure, one of the two Bluetooth devices (the claimant) tries to reach the other one (the verifier). Generally four parts exist in the whole scheme as shown top down in the Figure 2.

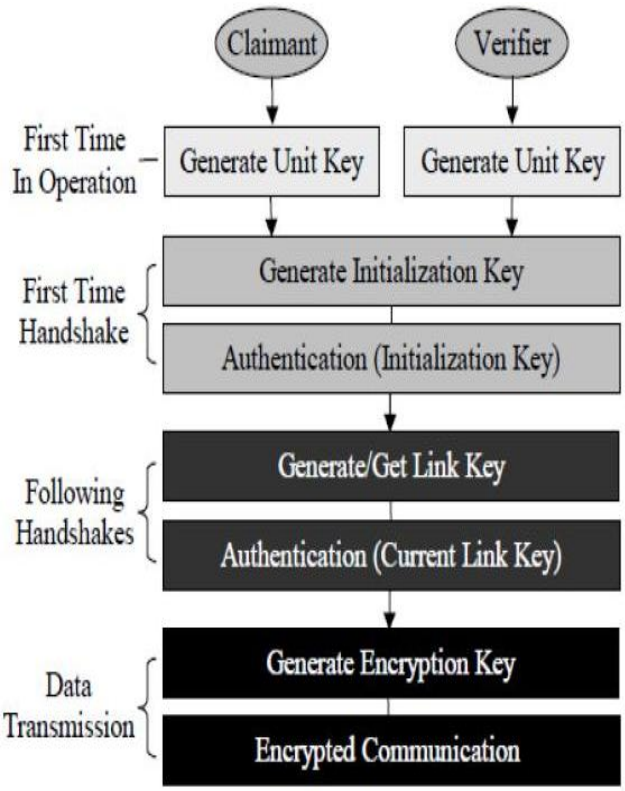


Figure. 2. Bluetooth Link-level Security Scheme

4.1. Key Management Scheme:

Key management schema is used to generate, store, and distribute keys, which compasses the first step of each of the four parts in Figure 2. Basically, Bluetooth security schema is based around symmetric key cryptography, *i.e.*, a private key called link key is shared between two or more parties. The link keys can have diverse lifetimes. A semi-lasting key can be utilized after the current session is ended, while a brief key is substantial just until the current session is over. A sum of four sorts of links keys have been characterized, as demonstrated in Figure 3. The initialized key is utilized just amid the initialized process. The unit key is produced once at the establishment of the unit. The mix key is inferred by both units for administrations that require more security. The expert key, created by the expert devices, is utilized when the expert needs to show messages. There is additionally a Bluetooth PIN utilized for confirmation and to create the initialization key before trading link keys.

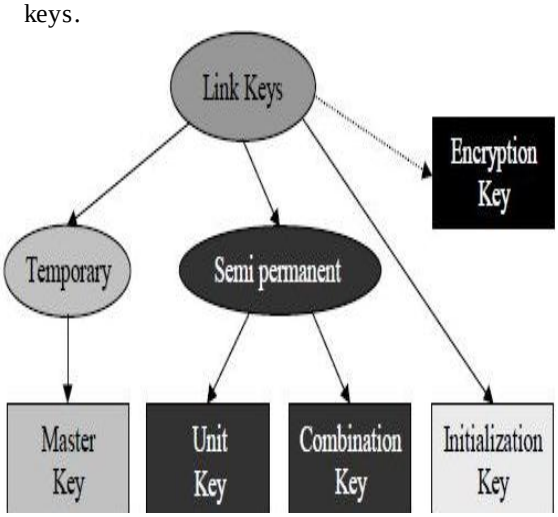


Figure. 3. Bluetooth Key Structure

4.2. Authentication Scheme:

The Bluetooth authentication schema uses a test reaction system in which a 2-move protocol is employed to check an claimant's knowledge of a mystery key, as demonstrated in Figure 4. In the event that confirmation falls flat, a certain waiting up interim must pass before another endeavor can be made. The holding up interim will increment exponentially. This is to keep an interloper to repeat the authentication procedure with different keys.

4.3. Encryption Scheme:

Figure 5 shows the encryption procedure. The encryption key (KC) is generated from the current link key. There are a several encryption modes in which show messages and individually addressed to can be either scrambled or not, contingent upon whether a gadget utilizes a semi-changeless connection key or an master key.

V. SECURITY LEVEL OF SERVICE

This section describes the pratical issues involed in the implementation of security mechanisms, i.e. an approach for an adaptable security structural planning based on top of the connection level security peculiarities of Bluetooth. More data can be found in [6]. Figure 6 represents the general security structural planning. The key part in the structural engineering is a security supervisor, with the accompanying capacities. Store security-related data on both service and device into relating service and device databases.

- Grant or refuse access requested for by protocol implementations or applications.
- Command the link manager to enforce authentication and/or encryption before interfacing with the application, utilizing the HCI.
- Query PIN entry to set-up trusted device relationship.

Employing such a centralized security manager is flexible to implement different access strategies and simple to include new arrangements without influencing different parts. Additionally, the security director goes about as an extension to join application level and link level security controls together and in this manner helps in giving end-to-end security.

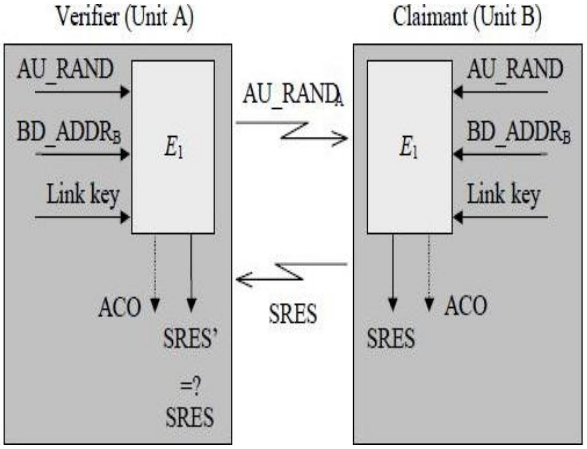


Figure. 4. Challenge-response for the Bluetooth Authentication

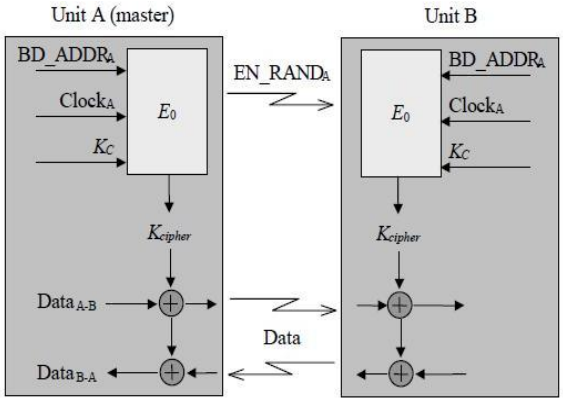


Figure. 5. Encryption Procedure

Verification ought to be performed in the wake of figuring out what the security level of the administration is. That is to say, the verification must be performed when an association appeal to an administration (SCO link) is submitted.

VI. VULNERABILITY

Although the Bluetooth network system is relatively secure, by employing the schemes described above, there are still a number of weaknesses in the standard. Several pieces of research on addressing security flaws present in Bluetooth networks have been carried out. Table 1 lists the detailed description and analysis of Bluetooth vulnerabilities, together with possible attacks/risks and countermeasures corresponding to each of the weakness issues.

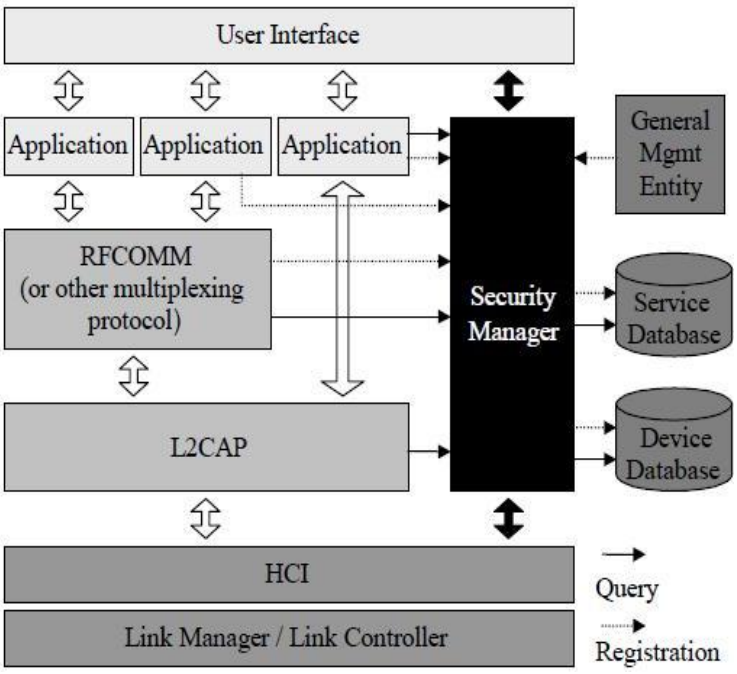


Figure. 6. Bluetooth Security Architecture

Table 1. Vulnerability Analysis of the Bluetooth Standard

Weakness	Attack / Risk	Countermeasure
The quality of pseudorandom number generator is undetermined.	Guess the generator implementation or the generated pseudorandom number.	Statistical tests to detect non-repeating and randomly generated requirements.
PIN key is too short and default PIN is all zero.	Easy to exhaustively search or guess PIN key.	Increase the PIN code length.
Need to physically enter PIN code to devices.	Inconvenient PIN code input.	Application level key agreement software.
Initialization key is too weak.	Depend only on RAND and PIN which are both unsafe.	Employ new strong initialization key generation scheme.
Unit key is reusable, and is public to the other side once used.	Calculate encryption key or impersonate other devices with their unit key.	Use unit key as input to generate a random key. Use a key set instead of only one unit key.
Shared master key.	Impersonating or disclosing.	Change broadcast scheme.
No user authentication.	Device embezzling.	Application level security and employ user authentication.
Repeating attempts for authentication.	Disabling authentication attempts from legitimate devices.	Encrypt device address. Limit the entry number of the list.
Weak E_0 stream cipher.	Shortcut attack: guess the contents of E_0.	Replace the cipher with other advanced scheme.
Negotiable key length.	Encryption abort. Use too short a key.	Globe agreement on minimal key length.
Leak support for legacy applications.	Security manager stands idle, no security for legacy applications.	Add a Bluetooth-aware "adapter" application for the legacy application.
No separately defined authorization for services.	No service-related flexible device trusting assignment.	Modify the security manager and the registration processes.
Unidirectional access check but bi-directional traffic.	Malicious verifier attacks claimant by nasty messages.	Access check at all the phases and mutually. Check-consistent data flow direction.

The table concerns the evaluations on the majority of the Bluetooth security particular conventions, including general security plan, key administration, validation, encryption, and approval. It is qualified to note that the whole system of the Bluetooth security is worthy. The shortcomings of the general Bluetooth conventions originate from the remote nature, specially appointed nature, and gadget location plan. For security particular conventions, shortcomings fall into routines for PIN code, irregular number era, unchangeable unit key, and security supervisor. More security can be normal through the job of abnormal state security conspires by conventions and/or applications upon the Bluetooth.

VII. CONCLUSION

Bluetooth is one of a several new wireless technologies that are changing the enterprise environment. Since it is low power, shorter extent, lower data transfer capacity, utilized for less delicate applications, and more inadequately utilized than alternate remote advances, it is intrinsically lower hazard. Albeit more qualified items rise, at present Bluetooth is still more a research facility engineering to be mulled over than a broadly utilized supporting strategy for innumerable items. The convention is still in its exploration stage somewhat in view of the security issues. Since the Bluetooth security plan is sensibly strong to applications with less security prerequisites, the last peculiarities may depend more on the usage than noteworthy changes to the determination.

Taking into account the first plan objective of link substitution, Bluetooth is more suitable to short-range and little size remote individual region systems than for joining with outside open systems, contrasting to *e.g.*, WLAN. To applications, for example, extensive impromptu systems and outside interconnection access, abnormal state security plans ought to ideally be implemented for complementation. Illustrations incorporate *e.g.*, IPSEC for IP, secure steering conventions, appropriated mystery plans, and so forth.

REFERENCES

[1] The official Bluetooth technology info site, http: //www.bluetooth.com.

[2] C. S. Lee, “Bluetooth Security Protocol Analysis and Improvements”, M.Sc. thesis at San Jose State University, http://www.cs.sjsu.edu/faculty/stamp/students/cs298ReportSteven.pdf.

[3] Bluetooth SIG, Specification of the Bluetooth System: Core, Version 1.1, vol. 1, **(2001)** February 22.

[4] IEEE 802.15 Working Group for WPANs, http://ieee802.org/15/.

[5] J. C. Haartsen, “The Bluetooth Radio System”, IEEE Personal Communications, vol. 7, no. 1, **(2000)** February, pp. 28-36.

[6] T. Muller, “Bluetooth Security Architecture: Version 1.0”, Bluetooth White Paper, Document # 1.C.116/1.0, **(1999)** July 15.

[7] K. Dasgupta, “Bluetooth Protocol and Security Architecture Review”, online report, http://www.cs.utk.edu/~dasgupta/bluetooth/.

[8] J. T. Vainio, “Bluetooth Security”, Online report, **(2000)** May 25, http://www.niksula.cs.hut.fi/~jiitv/bluesec.html.

[9] M. Jakobsson and S. Wetzel, “Security Weaknesses in Bluetooth”, online report, http://www.bell-labs.com/user/markusj/bluetooth.pdf.

[10] C. Candolin, “Security Issues for Wearable Computing and Bluetooth Technology”, Online report, http://www.cs.hut.fi/Opinnot/Tik-86.174/btwearable.pdf

[11] R. Mettala, “Bluetooth Protocol Architecture: Version 1.0”, Bluetooth White Paper, Document #1.C.120/1.0, **(1999)** August 25