The Journal of Applied Sciences Research

Journal homepage: http://www.journals.wsrpublishing.com/index.php/tjasr

Online ISSN: 2383-2215 Print ISSN: 2423-4400

Review Article

Attacks on Bluetooth and its Security: A Comprehensive Literature Review

Samta Gajbhiye [1], Sanjeev Karmakar [2,*], Monisha Sharma[1], and Sanjay Sharma[2]

[1] Shri Shankaracharaya College of Engineering Technology, Junwani, Bhilai, 490020 Chattisgarh, India
[2] Bhilai Institute of Technology, Bhilai, Chattisgarh, India

ARTICLE INFO

Corresponding Author:
Sanjeev Karmakar
dr.karmakars@gmail.com

How to Cite this Article:
Gajbhiye, S., Karmakar, S., Sharma, M., and Sharma, S. (2015). Attacks on Bluetooth and its Security: A Comprehensive Literature Review. *The Journal of Applied Sciences Research,* 2(1): 58-69.

Article History:
Received: 13 March 2015
Revised: 14 May 2015
Accepted: 16 May 2015

ABSTRACT

Bluetooth technology is used primarily to establish wireless personal area networks. Exponential growth of the volume of Bluetooth-enabled devices indicates that it has become a popular way of wireless interconnections for exchanging information. However, man in the middle attacks against unsecured Bluetooth implementations can provide attackers with unauthorized access to sensitive information. It is a challenging task for researchers to provide a complete secure Bluetooth device. However, extensive contributions have been achieved. A comprehensive literature review of worldwide contributions from 1999 to 2014 has been carried out to analyze the Bluetooth attacks in real scenario and to identify the security feature of Secure Simple Pairing protocol in of Bluetooth v4.0+ low energy device. It has been found that the SSP introduced Elliptic Curve Cryptosystems in Bluetooth which are more secure than the previous mathematical technique based on discrete logarithm problem. The complete security analysis of Bluetooth 4.0+ low energy, man in the middle attacks on Bluetooth enabled devices, applications of elliptic curve cryptographic technique & its hardness is presented through this broad review article.

Keywords: Man in the middle, Secure Simple Pairing, Elliptic Curve Cryptography, Low Energy, Elliptic Curve Diffee Hellman.

INTRODUCTION

One of the most important issues to any communication technique is security. For wireless transmission like in Bluetooth this problem is more severe. A Bluetooth device communicates with each other by pairing and thus establishes link key which is used in later sessions. In Bluetooth versions up to 2.0+ Enhanced Data Rate (EDR) (*Bluetooth SIG Park. W et al., 2004*), paired devices share the same PIN (Personal Identification Number) code or passkey and uses challenge-response scheme for authentication. Secure Simple Pairing (SSP) was introduced in Bluetooth version 2.1+EDR *(Bluetooth SIG Park. W et al., 2007)* new pairing technique. The main idea was to improve protection against passive eavesdropping and Man-in the-Middle (MITM) attacks. SSP employs Elliptic Curve Diffie- Hellman (ECDH) public-key cryptography (Miller, 1987). To make it more

secure and user-friendly, each release of Bluetooth version upgraded different aspects of this technology. The last version Bluetooth4.0 *(Bluetooth SIG Park. W et al.*, 2010*)* focused on low power usage. Bluetooth technology has some security 'loop-holes' that make it vulnerable. Various types of attacks can be performed well before pairing is complete as well as after the pairing is complete. Although SSP paid much attention on security issues, several security weaknesses are discovered, including passive off-line guessing attack and active on-line guessing attack. Also elliptic curves have been utilized in devising algorithms in public-key cryptography. These Elliptic Curve Cryptography (ECC) are more secure, as compared to the Discrete Logarithm Problem (DLP).

The objective of this review is to analyze the Bluetooth attacks in real scenario and to identify the security feature of Secure SSP protocol in of Bluetooth v4.0+ LE devices.

The paper has been constructed with the sections discussing security specification of Bluetooth 4.0 + LE (Low Energy), discussing comprehensive review of world-wide contributions (1999-2014) to analyze the Bluetooth attacks in real scenario and to identify the security feature of SSP protocol in Bluetooth v4.0+LE device followed by results and discussions and finally ending with conclusion.

Security Specification of Bluetooth 4.0 + Le

Four different entities are used for maintaining security at the link layer of Bluetooth protocol stack: a BluetoothS device address (48 bits), two secret keys (128 bits each), and a pseudo-random number (128 bits). Four types of link keys are identified based on different types of applications: Combination key, Unit key, Temporary key, Initialization key and an additional encryption key. Functionally the combination key and the unit key are indistinguishable; the difference lies in the way they are generated. The Personal Identification Number (PIN) may be a fixed number provided with the device or can be selected by the user. Default PIN value of zero may be used. The length of this default PIN is one byte, PIN (default) = 0x00 *(Bluetooth SIG Park. W, et al., 2010)*

Secure Simple Pairing

SSP operates in either of four modes *(Bluetooth SIG Park. W et al., 2010)*:

Numeric comparison: In this mode pairing devices displays 6 digit numbers.

Just works*:* In this mode two devices automatically gets paired without any comparison when discovered nearby. It can be used together with Near Field Communication (NFC) to make it harder for an active attack.

Out of band**:** In this mode pairing devices have another channel that is used to reliably pass information between devices.

Passkey entry: In this mode pairing devices must have the same password. There are five phases of Secure Simple Pairing as illustrated in Fig. 1.

Working of SSP in different phases

Phase 1: Public Key Exchange

Initially initiating device sends its Elliptic Curve Diffie-Hellman (ECDH) public key the device wants to pair. The counterpart then replies with its own ECDH public key *(Bluetooth SIG Park. W, et al., 2010)*

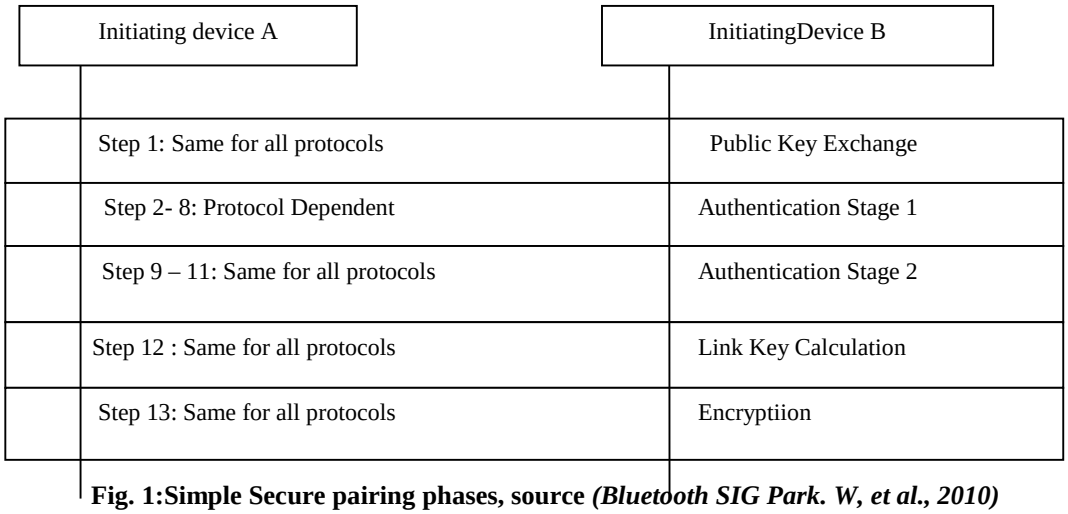

Fig. 1:Simple Secure pairing phases, source *(Bluetooth SIG Park. W, et al., 2010)*

Phase 2: Authentication Stage 1

After pairing, two devices validate each other using challenge response scheme. The sequence diagram of Authentication Stage 1 for the Numeric Comparison protocol, from the cryptographic point of view is shown in Fig. 2 where C_x is commitment value from device X, N_x is nonce from device X, r_x is random value generated by device X, f1( ) is used to generate the 128 bit commitment values C_a & C_b *(Bluetooth SIG Park. W, et al., 2010).*

Phase 3: Authentication Stage 2

The second stage of authentication then substantiates that both devices have effectively completed the exchange. This stage is indistinguishable in all three protocols and is illustrated in Fig 3, where E_x is check value from device X, , IOCapA & IOCapB is IO capabilities of device A & B, f3( ) is function used to compute check values Ex *(Bluetooth SIG Park. W, et al., 2010).*

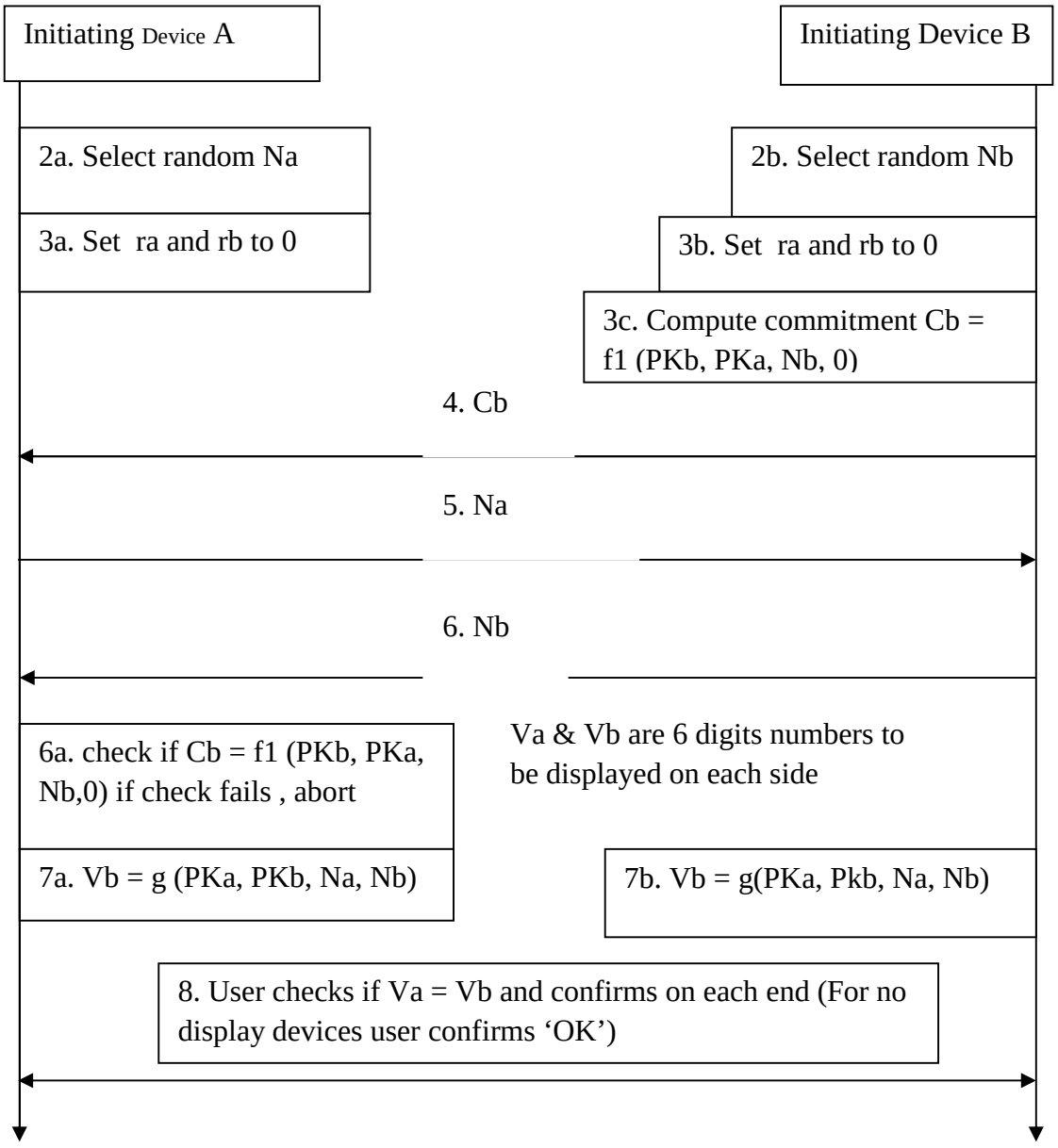

Fig. 2: Authentication Stage 1: Numeric comparisons protocol, source *(Bluetooth SIG Park. W, et. al., 2010)*

Phase 4: Link Key Calculation

After the confirmation of pairing and authentication, a link key is calculated from the derived shared key and the publicly exchanged data (step 12 of Fig. 1) and is used to maintain the pairing. Link key calculation is illustrated Fig. 4. Where DHKey is Diffie Hellman key, f2( ) is used to compute the linkkey and possible other keys from the DHKey and random nonce's, LK is Link Key, PK_x is Public Key of X *(Bluetooth SIG Park. W, et al., 2010).*

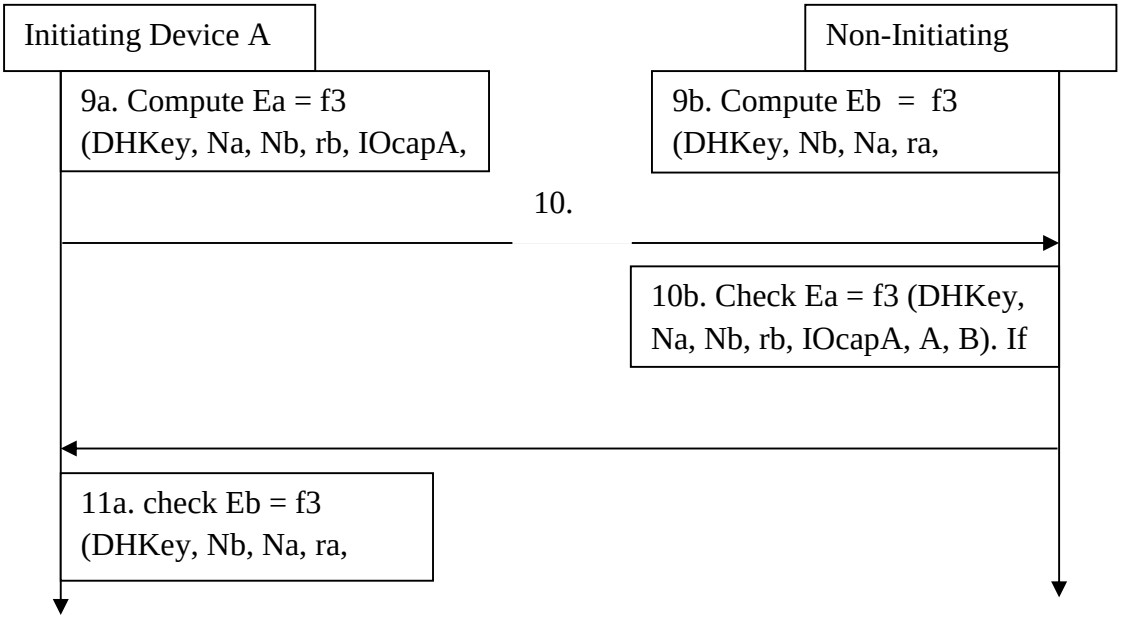

Fig. 3: Authentication Stage 2, Source *(Bluetooth SIG Park. W, et al., 2010)*

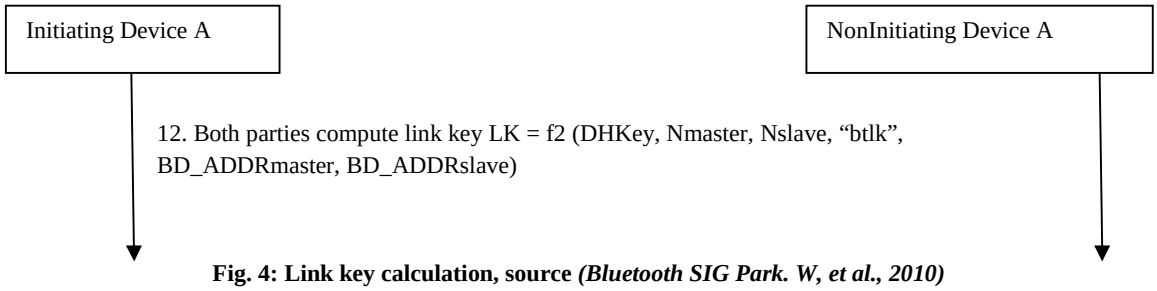

Fig. 4: Link key calculation, source *(Bluetooth SIG Park. W, et al., 2010)*

Security of Bluetooth LE

Instead of Link Key, Long-Term Key (LTK) is generated by one of the device and sent over to other, rather than both devices generating the same key separately. The association models are alike as SSP apart from quality of protection provided. ECDH could not be used here because of its inadequate resources and hence no safeguard from passive eavesdropping. Thus an attacker may determine LTK, once he captures LE pairing frames *(Bluetooth SIG Park. W, et al., 2010)***.**

LE uses Advanced Encryption Standard-Counter with CBC-MAC (AES-CCM). Two new keys were introduced called Identity Resolving Key (IRK) and Connection Signature Resolving Key (CSRK). The IRK lets a trusted device to resolve another device's private device address from a public (random) device address. The advantage of this feature is, if the device remains discoverable, the challenger cannot track its location over the time. The CSRK verifies cryptographically signed data frames from a

particular device and lets Bluetooth connection to use data signing (providing integrity and authentication) to protect the connection *(Bluetooth SIG Park. W, et al., 2010)*

LE do not make use of authentication challenge/response scheme. Instead successful encryption using LTK provides implicit authentication. Similarly, successful data signing offers inherent authentication that the remote device holds the correct CSRK, although privacy is not granted *(Bluetooth SIG Park. W, et al., 2010)*.LE pairing and key distribution is illustrated in Fig 5.

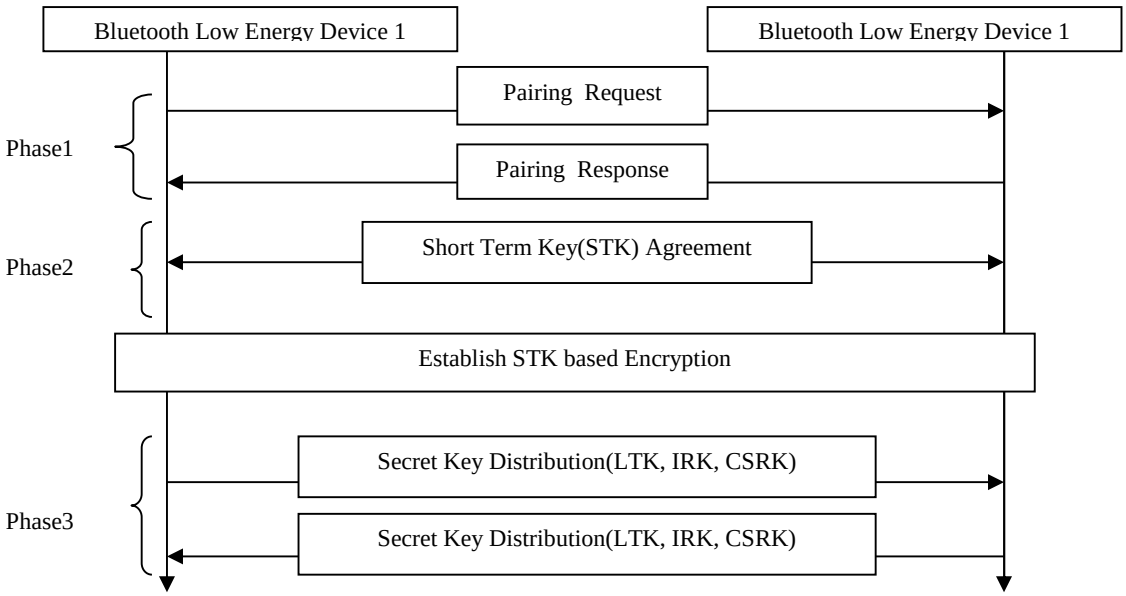

Figure 5 : LE Pairing and Key Distribution scheme

REVIEW OF LITERATURE

Attacks on Bluetooth Devices

Several papers as well as official reports pointed the security problem in Bluetooth. Given an output key stream segment of length *O* (2^{64}), (Hermelin. M. and Nyberg. K., 1999) theoretically proved that Bluetooth stream cipher with 128 bit key can be wrecked in O (2^{64}) steps (Canniere, *et al*, 2001) had proved that E0 stream cipher of Bluetooth has some security imperfections. (Jakobsson. M. and Wetzel. S., 2001) for the first time formulated MITM attack on Bluetooth for version 1.0B. By passive eavesdropping on the initialization key establishment protocol they also developed a technique to acquire the link key using an "Off-Line PIN crunching attack". They pointed few limitations of version1.0B like usage of the unit key, the short Bluetooth PIN and the confidentiality problem caused by site tracking (Fluhrer S. and Lucks S., 2001). used public information of the encryption mechanism in E0 and examined keystream to compute the encryption key.

(Gehrmann. C. and Nyberg. K. ,2002) dealt with the problems identified by Jakobsson & Wetzel and demonstrated that by broadening the current link key concept and by exploiting the enhanced private-public key pairing procedure, secure and convenient access point roaming can be accomplished via Bluetooth Baseband security. Also introduced a new anonymity mode to avoid location tracking .(Sun. J., *et al.,* 2002) explored flaws of Bluetooth1.1 protocols is because of its wireless nature, adhoc nature, device address scheme, methods for PIN code, random number generation, unchangeable unit key, and security manager. (Bagini *et. al.*, 2002) have found an attack on the Bluetooth stream cipher that can reconstruct the 128-bit secret key with complexity of about 2^{70} from 45 initializations. *(*Luand Yi and Vaudenay Serge. 2002) *recommended* a new attack against E0 called Maximum Likelihood Decoding (MLD) algorithm based on fast Walsh transform to recover the closest codeword for any linear code and was considered to be the best attack.

(Singelee and Preneel, 2004). Reported that intruder can acquire the random number at some stage in initialization phase and hence PIN and all keys. And suggested to avoid use of unit keys since it is stored in non-volatile memory and almost never changed. Based on the weakness reported by (Vainio. And Juha, 2000), (Jakobssonand Wetzel, 2001) and (Karygiannis and Owen, 2002), (Aissi *et al.*, 2004) made passive wire tapping and off-line attacks impossible and presented strong shield against active MITM attacks by proposing modified Diffie-Hellman (DH) key exchange pairing mechanism that uses cryptographic one-way functions to toughen the security of the link key using relatively short and user-friendly PIN values. Also suggested for PIN size between 5-12 decimal digits and ECDH key exchange protocol for the next version. (Levi A. *et al.,* 2004) simulated attacks and showed that current Bluetooth specifications do not have protective means for relay attacks.

Since Secure Remote Protocol was found to be dictionary attacks by both in a passive and active approach, Bluetooth SIG recommended change in the length of the Personal Identification Number (PIN) used. Another solution to dictionary attack was proposed by (Sayegh and El-Hadidi, 2005) by recommending a protocol BT-EC-SRP and succeeded in creating a strong initialization key from a weak human memorable PIN.

(Giousouf, *et al, 2005)* pointed out few weakness in Bluetooth like PIN length is too short , unit key sharing can direct to eaves dropping, device address are not validated hence addresses may be spoofed , Encryption key length and E0 stream cipher algorithm is flexible and weak, End-To–End security is not carried out, security services are limited, strength of the challenge response Pseudorandom generator is not known . (Shaked and Wool, 2005) captured the advantage of short PIN and implemented an attack during pairing to decode PIN in no time. (Haataja, 2005) in his report recommended that: encryption should be enabled by default by the manufacture, long PIN codes should always be used, security level of Bluetooth device should never be public as default , private security level should be set as compulsory and Bluetooth device address(BD_ADDR) must be printed in every instruction manual. This also requires minor changes to the Bluetooth specification. Bypassing security model proposed by (Kim *et al.,* 2005) on power-limited devices for protecting communications between peer devices proved to be faster than a certificate-based Diffie-Hellman method. (Lu *et al.,* 2005) encashed flaws in resynchronization of E0 and showed the fastest plaintext attack on Bluetooth encryption.

BT2.0 + EDR0 (Bluetooth SIG Park. W *et al.,* 2004). Provides faster transmission speeds than previous versions whereas SSP introduced in BT 2.1 + EDR0 (Bluetooth SIG Park. W *et al.,* 2007). Provides a noteworthy security improvement for link key generation and management such as Encryption Pause Resume, Extended Inquiry Response, NFC (Near Field Communication), Sniff Subrating, Qualityof-service(QoS). SSP considerably simplified the pairing process from the user's point of view. SSP either uses NFC as an Out-of-Band (OOB) channel or asks the user to compare two six-digit numbers in order to provide protection against MITM attacks and to ruin passive eavesdropping attacks Secure Simple Pairing uses Elliptic Curve Diffie Hellman (ECDH) public key cryptography. ECDH provides a very high degree of security against passive eavesdropping attacks but it may be exposed to MITM attacks, which however, are much harder to perform in practice than the passive eavesdropping attack. This attack remains in Bluetooth4.0 (Bluetooth SIG Park. W *et al*., 2010).

Since the release of BT2.1+EDR, many researchers proposed modified key Agreement protocol to minimize eavesdropping and MITM attacks in SSP. There after (Hyppönen & Haataja, 2007), in their paper on Nino MITM attack on SSP exploited that the devices exchange information about their IO capabilities during the first phase of the SSP. They reported that it is the point where intruder gets control over an unauthenticated channel, modify the information about devices capabilities and force the devices to use the Just Works association model. (Chang and Shmatikov, 2007) study demonstrated that authentication can fail when the same device is involved in concurrent Simple Pairing sessions and refined authentication scheme to integrate session identifiers still holding the properties of Simple Pairing

By integrating ECC and interlock protocol (Bin. YU. and Haiyan, 2008) efficiently defended MITM attack in the encryption key negotiating process and provided integrity authentication for the keys by designing an

encryption key agreement scheme. Haataja *et al.*, proposed four novel attacks respectively: Bluetooth BT-SSP-Printer-attack (Haataja and Hypponen, 2008) against Bluetooth enabled printers that support SSP , BT-SSP-OOB-MITM attack (Haataja and Toivanen, 2008) which exploited the fact that valid users are misled to select a less secure option instead of using a more secure OOB channel (e.g., USB cable, IrDA or NFC), BT-SSP-HS/HFMITM attack (Haataja and Toivanen, 2008) in which he pointed that all Bluetooth-enabled headsets and hands-free devices that support SSP uses the Just Works association model in order to make pairing process user-friendly, Man-In-The-Middle (MITM) attacks on Bluetooth Secure Simple Pairing (SSP) named BT-Nino-MITM (Hyppönen and Haataja, 2007) and efficient RF fingerprint-based (Haataja *et al.*, 2010) security solution for Bluetooth SSP. He observed that disclosure and integrity attacks usually compromise some sensitive information and can be very hazardous, whereas DoS attacks only irritate Bluetooth network users and are less dangerous. He suggested few changes at specification level like an additional window at the user interface level, Just Works as a voluntary and OOB as a obligatory association model.

To uncover malicious Bluetooth traffic (Reeves. D., 2008) implemented intrusion detection system using false signatures and identified reconnaissance, denial of service, and information theft attacks on Bluetooth enabled devices. Based on the attack classification it also consists of an intrusion response component to redirect attacks in progress. (Andrew Y. Lindell, 2008) and (Barnickel J. *et al*., 2009) showed that passkey entry mode is not safe for pairing since it reveals the password on the first part of the pairing process. Subsequently, the attacker can mount a man-in-the-middle attack if same PIN is used twice on a new run of the pairing process also suggested to pair in isolated place and recommended to choose the arbitrary and distinct number every time a pairing takes place.

(Saravanan, *et al*., 2009) used Out Of Band technology to show MITM attack against Bluetooth enabled mobile phone that supported Simple Secure Pairing (SSP). (Kumar, 2009) introduced a new parameter called ‘au_id’ (Authentication ID) for pairing and authentication and was accepted by Bluetooth SIG as a method to exchange keys. (Sharmila and Neelaveni, 2009) confirmed TRIPLE DES algorithm better than SAFER+ algorithm. (Soriente *et al.*, 2009) introduced human body either as the communication medium or as the source of the common secret while pairing in Bluetooth. *(*Hay. S. and Harle R. , 2009) found the substitute to inquiry-based Bluetooth tracking in the form of connection-based tracking which allows tracing of a previously identified handset within a field of fixed base stations and concluded that the process is very slow and can be a security and privacy risk.

(Alam and Khan, 2010) encrypted the commitment value calculated by slave based on ECDH Cryptography to enhance the security of pairing and authentication process in SSP of Bluetooth. To secure the exchange of public keys (AL-Moman *et al*., 2011) proposed Enhanced SSP (ESSP) that validates public keys of the communicating devices. ESSP adds a phase before first phase of SSP and is executed only once, when new devices gets into the Personal Area Network (PAN) of the user. This modification to SSP detects the device if it attempts to get into the Bluetooth networks before pairing. By reducing the distance between legitimate transceiver pair or by increasing the transmission power (Mutchukota. T. et al., 2011) presented anti-jamming techniques on SSP model so as to reduce jamming-to-signal ratio to avoid MITM attack on Physical layer.

(Sandhya and Sumithra, 2012; 2013; 2014) covered SSP in Bluetooth4.0 normal mode and low energy mode. And found that it maximizes security by using 16 alphanumeric PIN, ECDH public key cryptography to protect passive eavesdropping attacks and uses numerical comparison or passkey entry user assisted numeric methods to prevent MITM attacks. In another paper replaced Triple DES-Tiger algorithm with AES-Blake algorithm and proved that it works better than the Triple DES-Tiger algorithm. Subsequently replaced Continuing with previous one, again used alternative to AES by PRESENT-Blake. Experimented conducted on Java confirmed that the PRESENT-Blake algorithm gives 15 times better throughput than the AES-Blake algorithm.

In order to find out the major vulnerabilities in modern Bluetooth-enabled mobile devices *(*Nasim, 2012) performed successfully several attacks such as- Surveillance, Obfuscation, Sniffing,

Unauthorized Direct Data Access (UDDA) and Man-in-the-Middle Attack (MITM) on the communicating devices. To avoid man-in-the-middle attacks so as to secure consumers privacy efficiently (Tzu-Chang Yeh, *et al*., 2012) proposed an easy and improved protocol for authentication that requires entering the same PIN number on both connecting devices, instead of confirming displayed numbers. Although (Villegas. J, 2012) reported bluetooth 4.0 to be highly secure. Still the author says that the sensitivity of the problem lays when the devices pair for the first time or when they have to re-establish a link key.

(Padgette *et al.,* 2012) summed up security vulnerabilities associated with Bluetooth in all the versions as follows: Link keys can be stored inappropriately, power of the pseudo-random number generators is unknown, length of Encryption key is flexible, No user certification exists (specification provides only device certification), End-to-end security is not performed (Only individual links are encrypted and authenticated, Data is decrypted at intermediate points), restricted Security services (Audit, non repudiation, and other services are not the part of specification.), Discoverable and/or connectable devices are prone to attack , no eavesdropping protection in LE pairing, no MITM protection against Just Works pairing method. In paper "Performance Analysis and Comparison of Bluetooth Low Energy with IEEE 802.15.4 and SimpliciTI". (Mikhaylov K., 2013) revealed that Bluetooth Low Energy (BLE) provides an inexpensive and power-efficient solution for wireless communication. Nonetheless, radio transceiver and stack of Bluetooth still have many limitations that reduce the throughput and increases communication time. The other serious limitation of the BLE technology is the restrictions regarding its network topology

Security Using ECC

As stated above, SSP technique of Bluetooth2.1+ EDR used ECC for authentication and digital signatures. Based on the initial work of (Miller, 1986) and (Koblitz ,1987), (Robshaw, 1997) proved that ECC offered the opportunity to use shorter keys than with RSA which lead to better storage requirements and improved performance and proved that Elliptic Curve Discrete Logarithm(ECDLP) problem is particularly hard to solve. Thus the smaller key sizes resulted in smaller system parameters, smaller public-key certificates, bandwidth savings, faster implementations, low power requirements, and smaller hardware processors. By the end of year 2000 elliptic curve cryptosystems have been considered as part of various standards bodies like NIST, Certicom Research. There after, many implementations of Elliptic Curve Cryptography were proposed by (Sui, *et al*., 2002), (Aifen, *et al*., 2005), (Tsai, 2009), (Martinez, *et a*l., 2010) , (Senekane, *et al*., 2011) and (Arshad and Ikram, 2011) in cryptographic applications which base their security on the intractability of hard mathematical ECDLP. Over the years, sub-exponential time algorithms were developed to solve these problems. As a result, key sizes grew to more than 1000 bits, so as to attain a reasonable level of security. (Khaled and Kayali, 2004) have embedded ECC in smart cards, (Gupta, *et al, 2004)*. used it for Speeding up Secure Web Transactions, (Lauter, 2004) proposed for wireless security, Lencher *et al*., (2006) implemented in Hardware to accelerate it, (Baktir, *et a, 2007)* used in processor architecture which performs all finite field arithmetic operations in the discrete Fourier domain, (Malan *et al.,* 2008) implemented for sensor networks based on the 8-bit, 7.3828-MHz MICA2 mote in 4KB of primary memory and many more.

SSP has gone through a series of reviews by experts, and the released version generally does good work in improving the security of Bluetooth pairing. However, MITM attacks against SSP are still possible. Therefore, Bluetooth security architecture needs to be further updated to prevent these threats. In general, MITM attacks are hard to prevent in wireless networks. By far the best way to stop such attacks is to use SSP's OOB channel.

This study explicitly concentrated on pairing mechanism in Bluetooth devices and by broad literature review it is concluded that because of defects in the link key establishment protocol and encryption (optional to the user) process that starts at the end of the pairing process Bluetooth devices are exposed to malicious intrusion. It is found that Elliptic Curve technique was used in wide range of cryptographic application and till date it is the best cryptography technique to improve the new pairing scheme in Bluetooth devices.

RESULTS

Following outcomes have been observed:

1. Normally, PIN size is 4 decimal digits and is flexible from 1 to 16 octets.
2. Master may use separate encryption keys for each slave in a point-to-multipoint configuration.
3. A link key based on a unit key can be changed. And it requires re-initialization of all devices connecting.
4. Correlation attacks are possible because of weakness in summation generator.
5. The high re-synchronization frequency can disrupts correlation attacks.
6. Application decides whether to accept or reject a suggested key size that fails in setting up a secure link.
7. To prevent an intruder from repeating the authentication procedure with a large number of different keys, for each subsequent authentication failure, the waiting interval is increased exponentially.
8. Simple Secure Pairing:

8.1. To avoid replay attacks a pseudo-random 128-bit nonce is used which is generated after the exchange of public keys and must be newly generated for each fresh session of pairing.

8.2. An active MITM may inject its own key material into pairing process to have any effect other than denial-of-service.

8.3. Out of Band protocol can be more secure the other three association models provided both devices have matching OOB interfaces.

8.4. The "gradual disclosure" technique prevents leakage of more than 1 bit of un-guessed Passkey information in the case of a MITM attack.

9. Security issues in Bluetooth V4.0

9.1. LE pairing provides no eavesdropping protection.

9.2. LE Security Mode 1 level 1 does not require any security mechanisms (i.e. no authentication or encryption).

10. Security issues in all versions

10.1. Link keys can be stored improperly. And can be modified by attacker.

10.2. Strength of the pseudo- random number generators (PRNG) are not known and may produce static or periodic numbers that may reduce the effectiveness of security mechanism.

10.3. Encryption Key length is negotiable. Bluetooth LE requires a minimum key size of seven bytes

10.4. No user authentication exixts , only device authentication is provided by the specification.

10.5. End-to-End security security is not performed. Only individual links are encrypted and authenticated. Data is decrypted at intemediate points. End-to-End security on top of Bluetooth stack can be provided by use of additional security controls.

10.6. Security services are limited. Audit, Non-repudiation , and other services are not part of the standard. If needed, these services can be incorporated in an overlay fashion by the application developer.

10.7. Discoverable and/or connectable devices are prone to attack.

CONCLUSIONS

Bluetooth security is critical and as such it should still be considered not strong enough for sensitive and privacy invasive applications. It is important that mobile application developers should provide appropriate security controls that offer identity-level security features.

By broad literature review it is concluded that during pairing process Bluetooth enabled devices are exposed to malicious interference because of two reasons: faults in the link key establishment protocol, the encryption of a session is voluntary and is done at the end of the pairing process. Also it is found that till date Elliptic Curve Method is best suitable cryptography techniques to improve the new pairing scheme.

Although LE uses similar pairing method names to BR/EDR SSP, LE pairing does not use ECDH-based cryptography and provides no eavesdropping protection. An attacker may calculate LTK if he captures the LE pairing frames.

REFERENCES

Aifen., S., Hui., L. ,Yixian., Y. and Chow. K.P. (2005). Elliptic Curve Cryptography Based Aauthenticated Key Agreement with pre-shared Password. *Journal of electronics (china)*. 22(3):268-272.

Aissi., S., Gehrmann., C. & Nyberg., K. (2004). Proposal for Enhancing Bluetooth Security Using an Improved Pairing Mechanism. *Bluetooth Architecture Review Board at the Bluetooth All-Hands Meeting*.

Alam., A. &Ibrahim, K. I. (2010). Security Enhancement of Pairing and Authentication Process of Bluetooth. *International Journal of Computer Science and Network Security*, 10(6):243-249.

ALMomani., I., AI-Saruri.& AL-Akhras. M. (2011). Secure Public Key Exchange Against MITM During SSP in Bluetooth. *World Applied Science Journal*. 13(4):769-780.

Andrew., Y. & Lindell. (2008). Attacks on the Pairing Protocol of Bluetooth v2.1, June 25, pp: 1-10, *www.blackhat.com* , USA (browsing date: 24/07/14)

Arshad. R. and Ikram. N. 2011. Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. Multimed Tools Appl. Springer Science+Business Media. DOI: 10.1007/s11042-011-0787-0, LLC 2011.

Bagini., V., Golic., J. & Morgari., G. (2002). Linear Cryptanalysis of Bluetooth Stream Cipher. Advances in Cryptology – EUROCRYPT. *Lecture Notes in Computer Science, Springer- Verlag*. 2332:238–255.

Baktr., S., Kumar., Christofpaa., S. & Sunar., B. (2007). A State-of-the-art Elliptic Curve Cryptographic Processor Operating in the Frequency Domain. *Springer Science + Business Media. Mobile Netw App*l . 12: 259–270.

Barnickel., J., Wang., J. & Meyer., U. (2009). Implementing an Attack on Bluetooth 2.1+ Secure Simple Pairing in Passkey Entry Mode. *IT Security Research Group RWTH Aachen University*.

Bellardo., J. & Savage., S. (2003). 802.11 Denial–of–Service Attacks: Real Vulnerabilities and Practical Solutions. *In Proceedings of the 12th USENIX Security Symposium*. pp:15–28.

Bin., YU. & Haiyan. (2008). Research and Design of one Key Agreement Scheme in Bluetooth. *International Conference on Computer Science and Software Engineering. IEEE Computer Society. Wuhan*, Hubei. 3:665 – 668.

Canniere., C., Johansson., T & Preneel., B. (2001). Cryptoanalysis of the bluetooth stream cipher. *COSIC Internal Report. http://www.cosic.esat.kuleuven.be/publications /article-22.pdf* (Browsing Date: 22nd Jun 2013.)

Certicom Research: Standards of efficient Cryptography. (2000). SEC1: Elliptic Curve Cryptography, Ver1.0. *www.secg.org/collateral/sec1_final.pdf.*(Browsing Date: 27th Jan 2011).

Certicom Research: Standards of efficient Cryptography. (2000). SEC2: Recommended Elliptic Curve Domain Parameters , Ver1.0. *www.secg.org/collateral/sec2_final.pdf.*(Browsing Date: 27th Jan 2011).

Chang., R. & Shmatikov V. 2007. Formal Analysis of Authentication In Bluetooth Device Pairing, *www.us.utexas.edu*. (browsing date: 06_12_2013)

D., Sharmila & R, .Neelaveni. (2009). Performance Analysis of SAFER+ and Triple DES security algorithms for Bluetooth Security Systems . *IJCSNS International Journal of Computer Science and Network Security*, 9(2):395-404.

Fluhrer S. and Lucks S. 2001. Analysis of the E0 Encryption System" available from S. Lucks. *http://th.informatik.unimannheim.de/People/Lucks/papers/e0.ps.gz* , a gnu-zipped Postscript file.

Gehrmann. C. (2002) . Bluetooth Security White paper Version 1. Bluetooth SIG Security Expert Group. *http://grouper.ieee.org/ groups/1451/5/ Comparison %20of% 20PHY /Bluetooth _ 24 Security _Paper .pdf* (Browsing date: 23rd July 2013).

Gehrmann. C. and Nyberg. K. 2002. Enhancement to the Bluetooth Baseband Security. *http:// research. nokia.com/publication/7851*. (Browsing date: 20th Feb 2013).

Ghossoon. M. W. Al-Saadoon. (2009). Applying Packets Analysis as New Approach for Discovering Bluetooth Intrusion . *www.icics.info/icics/proceeding/icics.paper/81.pdf* , pp:1-7

Giousouf. A. (2005). Bluetooth Security, Communication Security Department, Ruhr University, Bochum. *http://www.emsec.rub.de/media/crypto/attachments /files/2011/ 04 / seminar_giousof _ bluetooth.pdf*.. (Browsing date:6th Oct 2011).

Gupta.V., Stebil., D.& Fung., S. (2004). Speeding up Secure Web Transactions Using Elliptic Curve Cryptography. *http://research.sun.com/projects/crypto*,(Browsing date: 21st Sep 2011).

Haataja. K. (2005). Bluetooth network vulnerability to Disclosure, Integrity and DenialofService attacks. *Proceedings of the annual Finnish Data Processsing Week at the University of Petrozavodsk (FDPW'2005). Advances in Methods of Modern Technology*. 7:63-103

Haataja. K. (2009). Security Threats and Countermeasures in Bluetooth-Enabled Systems. *Ph.D Thesis. University of Kuopio*.

Haataja., K. & Hypponen., K. (2008). Man-In-The-Middle Attacks on Bluetooth: a Comparative Analysis,a Novel Attack, and Countermeasures. *Malta 12-14 March 2008, ISCCSP 2008*, pp:1096-1102

Haataja., K. & Toivanen. P. (2010). Two practical man-in-the-middle attacks on Bluetooth secure simple pairing and countermeasures. *Wireless Communications, IEEE Transactions*, 9(1): 384–392. *http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber = 7693*.

Haataja., K. & Toivanen., P. (2008). Practical Man-in-the-Middle Attacks Against Bluetooth Secure Simple Pairing. *4th International Conference on Wireless Communications, Networking and Mobile Computing*. pp:1 – 5. *http://ieeexplore.ieee.org/xpl/mos tRecent Issue. jsp ?punum ber=4677908*.

Hay. S. & Harle. R. (2009). Bluetooth Tracking without Discoverability, (Eds.): LoCA 2009, *LNCS* 5561, pp. 120–137, *Springer-Verlag Berlin Heidelberg 2009.*

Hermelin., M. & Nyberg., K. (1999). Correlation Properties of the Bluetooth Combiner Generator. *In Proceedings of the 2nd International Conference on Information Security and Cryptolog. Springer-Verlag. Lecture Notes in Computer Science*. 1787:17–29.

Hyppönen K. & Haataja K.(September 26-28, 2007). Niño Man-In-The-Middle Attack on Bluetooth Secure Simple Pairing. *Proceedings of the IEEE Third International Conference in Central Asia on Internet, The Next Generation of Mobile, Wireless and Optical Communications Networks (ICI'2007). Tashkent. Uzbekistan. DOI: 10.1109/CANET.2007.4401672,*. pp:1-5.

Jakobsson. M. & Wetzel. S. (2001). Security Weakness in Bluetooth.. *RSA Security Conference ,San Francisco, USA. Springer Lecture Notes in Computer Science*, 2020:176-191.

Karygiannis. T. & Owen. L. (2002). Wireless Network Security: 802.11, Bluetooth and handheld devices, *NIST special publication 800-48. http://m.tech.uh.edu/faculty/ conklin/ IS7033Web /7033/Week9/NIST_SP_800-48.pdf.* (Browsing Date: 22nd July 2013).

Khaled., M. & Kayali., AL. (2004). Elliptic Curve Cryptography and Smart Cards, *SANS Institute Reading Room. http://www.sans.org/reading_room/whitepapers/vpns/ elliptic -curve-cryptography-smart-cards_1378* (Browsing date: 21st Sep 2011)

Kim., H., Dabbous., W. & Afifi H. (2005). A Bypassing Security Model for Anonymous Bluetooth Peers. , 0-7803-9305-8/05/$20.00 © *2005 IEEE*.

Koblitz. N. (1987). Elliptic Curve Cryptosystems. *Mathematics of Computation*. 48 (177): 203-209.

Kumar. T. (2009). Improving Pairing Mechanism in Bluetooth Security, *International Journal of Recent Trends in Engineering*. 2(2):165-169

Lauter. K. (2004). The Advantages of Elliptic Curve Cryptography for Wireless Security. *IEEE Wireless Communications*. 11(7) :62-67.

Lechner., J., Weitzer., A., Grosch., J.,Szekely., A., (2006), Tillich., S. & Wolkerstorfer. J.. Hardware/Software Co-Design of Elliptic Curve Cryptography on an 8051 Microcontroller. *Proceedings of 8th international conference on Cryptographic hardware and Embedded Systems, Springer-Verlag Berlin. Heidelberg*. pp:430-444.

Levi., A., Cetintas E., Aydos M, Kaya Koc C & Caglayan M. U. S. (2004) , Relay Attacks on Bluetooth Authentication and Solutions. *Computer and Information Sciences ISCIS 2000. LNCS*. 3280:278-288.

Lu., Y., Meier., W. & Vaudenay S. (2005). The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption. *Advances in Cryptology- CRYPTO-2005.LNCS*.3621:95-117.

Luand. Yi. & Vaudenay. Serge. (2002). Faster Correlation Attack on Bluetooth Keystream Generator E0, *EPFL http://lasecwww.epfl.ch* .

Malan., D., Welsh., M. & Smith., M. (2008). Implementing Public-Key Infrastructure for Sensor Networks. *ACM Transactions on Sensor Networks*. 4(4):22.1-22.23.

Martínez., V., Encinas., L., & Avila. S. (2010). A Survey of the Elliptic Curve Integrated Encryption Scheme. *Journal Of Computer Science And Engineering*. 2(2):7-13

Mikhaylov., K.., Plevritakis., N. & Tervonen J. 2013 , Performance Analysis and Comparison of Bluetooth Low Energy with IEEE 802.15.4 and SimpliciTI., J. *Sens. Actuator Netw. 2*:589-613, doi:10.3390/jsan2030589.

Miller., V., S. (1986). Use of elliptic curve in cryptography. *In Advances in Cryptology - Crypto'85. Springer-Verlag*. pp:417-426.

Mutchukota., T., Panigrahy., S, & Jena. S. (2011) , Man-in-the-Middle Attack and its Countermeasure in Bluetooth Secure Simple Pairing, Computer Networking and Intelligent Computing, *Communications in Computer and Information Science*. 157:367-376.

Nasim., R. (2012). SECURITY THREATS ANALYSIS IN BLUETOOTH ENABLED MOBILE DEVICES, *International Journal of Network Security & Its Applications (IJNSA).* 4(3), DOI : 10.5121/ijnsa.2012.4303 41

National Institute of Standards and Technology. (1998) . Digital signature standard. *FIPS Publication 186-1. http://csrc.nist.gov/encryption/* (Browsing Date:20th Jun 2013).

National Institute of Standards and Technology..(2000). Digital Signature Standard. *FIPS Publication 186-2. http://csrc.nist.gov/encryption/* (Browsing Date: 20th Jun 2013).

Padgette,. J., Scarfone., K. & Chen., L. (2012). Guide to Bluetooth Security. *NIST Special Publication. http://csrc.nist.gov/publications/drafts/800-121r1/Draft-SP800-121_Rev1.pdf* (Browsing Date: 19th July 2013).

Pasanen., S., Haataja., K., Paivinen., N. & Toivanen. P. (2010). New Efficient RF

Fingerprint-Based Security Solution for Bluetooth Secure Simple Pairing. *Proceedings of the 43rd Hawaii International Conference on System Sciences. IEEE Computer Society, Honolulu*. pp:1-8.

Reeves., D.(2008). Bluetooth Network-Based Misuse Detection. *Annual Computer Security Applications Conference 2008. IEEE Computer Society*. DOI 10.1109/ACSAC2008.39. pp: 377-391.

Robshaw. M.J.B & Yin. L. (1997). Elliptic Curve Cryptosystems. *A RSA Laboratory Technical Note.*

Sandhya. S. & Sumithra. Devi. K. A. (2013). Performance Evaluation of Crypt Analytical Approaches in Bluetooth Networks. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*. 2(7):403-408. ISSN 2319 – 4847.

Sandhya. S. & Sumithra. Devi. K. A. (2014) . A Lightweight Paradigm for Security in Bluetooth , *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 3(4): 1536-1540.

Sandhya. S. & Sumithra. Devi. K. A. (22-24 Feb 2012). Analysis of Bluetooth Threats and v4.0 Security Features. *International Conference on Computing, Communication and Applications (ICCCA.) Dindigul, Tamilnadu*. pp:1 – 4.

Saravanan., K., Vijayanand., L., & Negesh., R.,K. (2009). A Novel Bluetooth Man-In-The-Middle Attack Based On SSP using OOB Association model. *http://arxiv.org/ftp /arxiv/papers/1203/1203.4649.pdf.* (Browsing Date: 28th Feb 2013).

Sayegh., A. & El-Hadidi., T. (5-6 Sep 2005). A Modified Secure Remote Password (SRP) Protocol for Key Initialization and Exchange in Bluetooth Systems. *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05). IEEE*. pp: 261-269.

Senekane. , Qhobosheane. S. & Taele. B.M. (2011). Elliptic Curve Diffie-Hellman Protocol Implementation Using Picoblaze. *International Journal of Computer Science and Network Security*. 11(6):30-34.

Shaked., Y. & Wool., A. (2005). Cracking the Bluetooth PIN, MobiSys '05: The Third International Conference on Mobile Systems, *Applications, and Services. USENIX Association, New York, NY, USA*. Pp:39-50.

Sharmila., D., Neelaveni., R. &Kiruba. K. (2009). Bluetooth Man-In- The-Middle attack based on Secure Simple Pairing using Out Of Band association model. *International Conference on Control, Automation, Communication and Energy Conservatio.* pp:1-6 .*http:// ieeexplore. ieee.org/xpl/ mostRecentIssue.jsp ?punumber= 5191366*.

Singelee., D., Preneel., B. (2004). Security Overview of Bluetooth. *COSIC Internal Report .http://www.cosic.esat.kuleuven.be/publications/article-565.pdf* (Browsing Date: 22nd May 2012).

Soriente., C, Tsudik., G. &Uzun., E. (2009). Secure pairing of interface constrained devices, *Int. J. Security and Networks*. 4(1/2):17-26.

Specification of the Bluetooth System Version 1.0. (1999*). Bluetooth Special Interest Group. www.bluetooth.com.*

Specification of the Bluetooth System Version 1.1. (2001). *Bluetooth Special Interest Group. www.bluetooth.com*

Specification of the Bluetooth System Version 1.2. (2003). *Bluetooth Special Interest Group. www.bluetooth.com.*

Specification of the Bluetooth System Version 4.0. (2010). *Bluetooth Special Interest Group. www.bluetooth.com.*

Specification of the Bluetooth SystemVersion 2.0 + EDR. (2004). *Bluetooth Special Interest Group. www.bluetooth.com.*

Specification of the Bluetooth SystemVersion 2.1 + EDR. (2007). *Bluetooth Special Interest Group. www.bluetooth.com*

Specification of the Bluetooth SystemVersion 3.0(Seatle). (2009). *Bluetooth Special Interest Group. www.bluetooth.com*

Sui., AF., Yang., YX., Niu.,XX. & Luo., SS. (2004) Research on the authenticated key agreement protocol based on elliptic curve cryptography. *Journal of Beijing University of Posts and Telecommunications*. 27(3):28-32.

Sun., J., Howie., D., Koivisto. A., & Sauvola. J. (2002). Design, Implementation and Evaluation of Bluetooth Security. *www.mediateam.oulu.fi/publications /pdf/87.pdf* .(Browsing date: 22nd May 2012).

T. Wu. (1998). The Secure Remote Password Protocol. *Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, San Diego, Cananda.* pp: 97-111.

Tsai., JL. (2009). Efficient nonce-based authentication scheme for session initiation protocol. *Int J Network Security.* 8(3):312–316.

Tzu-Chang., Y, Jian-Ren., P., Sheng-Shih., W. & Jun-Ping., H. .(July 2012) Securing Bluetooth Communications. *International Journal of Network Security*. 14(4):pp-229-235.

Vainio. & Juha. (2000). Bluetooth Security. *http://www.niksula.cs.hut.fi /~jiitv /bluesec.html* (Browsing Date:4th Jul 2013)

Villegas., J. (2012). Bluetooth Low Energy Version 4.0 *Helping create the "internet of things"* (Browsing Date :19/7/2014).