2) Literature Review

Hypponen and Haataja (2007) have described how man in the middle attack is possible on secure simple pairing. With the help of 2 additional Bluetooth device (can be 1 device also) which clones bd_addr of either parties and then jam their physical layer. So due to frustration user will delete (link key) after few attempts and then secure simple pairing will be initiated by attacker. They just described attack only and how this problem can solved is not covered here.

Pasanen et al. (2010), have presented Novel RF Fingerprint-Based Security Solution for Bluetooth pairing. It is on the fact that each Bluetooth device operates via radio waves and each device has unique RF signal which can be termed as its fingerprint, what they have proposed a use of sensor/server for initiating pairing. It can be useful in offices where there can be a presence of 3rd party server or sensor is possible. Their proposed algorithm is difficult to implement when only 2 devices are paired.

Haataja and Hypponen (2010) have described that MITM attack is possible on SSP. They have talked of a “Bluesnifer” which is easily available in market. This tool can be utilized for MITM attack. It is easily available. They have proposed a new attack on Just works association model used with Bluetooth printer. They have also suggested countermeasures one is using NFC channel. Initial non secure public key exchange in SSP allows attacker to succeed.

Haataja and Toivanen (2010) have proposed 2 new attacks on SSP. 1) bt-ssp-oob-mitm: Here Attacker starts pairing just before user starts. Off course attacker impersonates other real user. Attacker also uses OOB.2) bt-ssp-hs/hf-mitm. Here Attacker again jams physical channel, compels user to delete previously stored link keys. Then again pairing is restarted with victim’s device. Strong cryptography is needed to avoid these.
Kumar and Saxena (2009) have studied perhaps all pairing methods available today. Their conclusion was, Results show that some simple methods (e.g., Visual Number and Image Comparison) are quite attractive overall, being fast and secure as well as acceptable by users. They naturally appeal to settings where devices have appropriate-quality displays. What is important that they clearly stated that a single cryptographic module can be utilized with all pairing methods.

Soriente et.al. (2009) have stated that the human body has some constantly changing variables (such as pH level, odour, humidity, temperature and other chemical properties) those are hard to predict for a (non-invasive) adversary. Thus, a combination of such variables could be used to obtain a short secret. Their usability experiments showed that the relatively short 300ms interval used with the synchronous button press. Users often show very unpredictable behavior when it comes to press the button for pairing.

Saxena (2006) proposed several improvements and extensions to the recently proposed approach of using a visual channel to implement secure pairing. They showed how strong mutual authentication can be achieved using just a unidirectional visual channel, which could also improve the usability of the pairing process. But it is difficult to have a light sensor on each wireless device.

Kainda et.al. (2009) have concluded that currently proposed methods of pairing require rethinking not only from usability perspective but also from a security standpoint: compare & Confirm, compare & select are not suitable methods for the out-of-band channel because of security failures. I agree with the conclusion and suggest that some cryptography module should be added for all methods that are using oob.

Kumar et.al. (2009) have concluded that simple Number Comparison is quite attractive overall, being fast and secure as well as readily acceptable by users. It naturally suits settings where devices have appropriate-quality displays. HAPADEP variant seems to be preferable in scenarios where one device has a speaker and the other microphone.
Vibrate Button or LED Button is best-suited for devices lacking screens, speakers and microphones. According to me number comparison methods require more security then other 2 class of methods.

**Barnickel et.al. (2012)** and all described an attack where once SSP starts, attacker will wait till N20 exchanged and then will jam the channel. Attacker use all information collected till N20 (nounce 20) is transferred, when both users forced to restart pairing. Attacker will impersonate both A and B for each other. They suggest that DHkey should be used in authentication phase 1 when Passkey Entry is used. Transmitting Nai=Nbi only encrypted with DHkey would prevent the attack discussed. My view is that when public keys are exchanged and DHKey are generated, some cryptography should be added.

**Boneh and Franklin (2001)** defined chosen cipher text security for identity-based systems and proposed a fully functional IBE (identity based encryption) system. The system has chosen cipher text security in the random oracle model assuming BDH (Bilinear Diffie-Hellman), a natural analogue of the computational Diffe-Hellman problem. It is already proved that this model is not so strong as claimed.

**Lalis et.al. (2014)** have proposed Securing Bluetooth Communication with Hybrid Pairing Protocol. They say that, to address the current vulnerabilities of Bluetooth technology, a hybrid pairing protocol has been presented in this study. The combination of Diffie-Hellman Key Agreement Protocol, MD5 and Hummingbird-2 encryption algorithm. Already ssp is good, we can add some functionality before pairing starts, instead writing everything from scratch, or proposing a separate algorithm altogether.

**Mishra P. (2013)** has proposed an algorithm that we can detect man-in-the middle attack during the second stage of simple secure pairing. Well, he has proposed that some cryptography should be there before ssp starts, But which cryptographic function should be used is not specified.
Mutchukota et.al. (2011) have proposed a PHY layer anti jamming technique, but anti jamming technique can be applied. Without additional Hardware, without software, how it can be implemented is not specified. This is a costly solution for the user.

Sethi et.al. (2014) have proposed, Commitment-based device pairing with synchronized drawing. First, they presented a secure key-establishment protocol for device pairing, which was motivated by the requirements of the synchronized drawings. Second, they discuss potential metrics for comparing the drawings and show that both location metrics and an easier-to-compute LURD string distance measure are suitable for the task. But we cannot expect user to draw a figure on android screen, to establish a Bluetooth Connection.

Yeh et.al. (2012) have proposed an easy, convenient and improved protocol which applies the familiar authentication method of entering the same PIN number on both connecting devices, as an alternative to confirming displayed numbers. This protocol not only secures consumer privacy, but also increases the efficiency of the operation. But it is Compromise with existing standard. At present no user enters any numeric pin. User friendliness is compromised here and it is like older v2 protocols.

Mishra and Gupta (2012) have suggested few possible counter measures against Bluetooth security attacks are suggested. But not a single measure which is full proof and can provide solid security as none is based on any technical concept, all are generalized suggestions.

Maple et. al. (2007) have highlighted a number of weaknesses in existing protocols and configurations of wireless networks and also written about how these weaknesses can be exploited. They have presented a number of recommendations that can ensure the greater security of wireless networks. But again not any technical solution, just generalized suggestions.
Choi et.al. (2008) have suggested that in networking, it is possible to achieve a reasonable level of overall security by systematic approach to assessing and managing risk, but Wireless security should be partitioned into wlan security, Wi-Fi security, infrared security, wireless communication security and then a comprehensive security should be looked into that. But they have left on the readers to devise a comprehensive security mechanism for each segment. It is a direction to researchers that separate security mechanism should be for each.

Alsoufi et.al. (2012) suggested an improvement to existing leap protocol. The LEAP protocol is implemented and simulated using one base station and fifty sensor nodes situated randomly. Initially, an individual key was generated for each node from a randomly generated master key. Then a cluster key was generated by each node and published to their neighboring nodes using the pair-wise keys. Finally, the global key was generated in order to enable public broadcasts. What they have suggested is a concept of individual key, group key and pair key, which can be useful in improving Bluetooth security.

Khanna (2009) focused on Current State of Research in the problem of the home mobile security. Different devices using for home security, their goal is to use only device that is mobile which covers all the functionality and capability. Integration of different parts and their solution can be developed with current devices and applications. Bluetooth, Infrared and Wi-Fi access security have been discussed. In next decade wireless home will be a reality. But in such system Bluetooth, infrared and wifi all require separate level of security and as all they use different kind of waves, it is not possible to devise a same mechanism for each of them.

Ijeh et.al.(2009) taken a holistic approach for understanding the development and management of protocols for wireless security and privacy locations, the study ascertained how the location of key data transmitted over the wireless network could be restricted to defined areas in order to enhance security. More emphasis on user's smartness or eagerness to achieve security. Main focus on wap, but today even wap2
has been cracked. More so, security mechanism should not depend on user's smartness or eagerness, but should be provided by some strong cryptographic mechanism.

Singh et.al. (2012) identified and described the various research issues and challenges available in the wireless domain. They first presented an overview of the taxonomy of wireless network. We presented an overview of a comprehensive list of research issues and challenges of the wireless network like signal fading problem, mobility problem, power and energy, data rate enhancement, security and the quality of service issues problems of the wireless networks. Good analysis of all Present problems but it is something survey type, no suggestion for enhancing security is given.

VamsiRam and Venkateswarlu (2012) proposed a new security model which addresses three important types of active attacks, MITM attack, Clone attack and Replay attack. By using 3-round Zero knowledge protocol they implemented this model. Requirement of base station is there. Not a case with adhoc network and Bluetooth. However when more than 2 devices are paired, in Bluetooth or mobile adhoc network, one device can be made surrogate base station and then zero knowledge proof can be utilized. What is limitation here that you require at least 3 devices, but in most cases only 2 devices are paired.

Jacob and Hutchinson et.al. (2011) said that While Wireless networks have enabled a greater amount of accessibility to end users; they have also opened many security flaws for potential hackers and cyber criminals. If addressed properly networking wirelessly can be secure, however this study confirms the need for security to be addressed. All wep and wpa discussed. It is proved all are non secure, TKIP is secure but not preferable as it is similar to wap and vulnerable to a number of similar attacks taken place on wep.

Saravanan et.al. (2012) have devised A Novel Bluetooth Man-In-The-Middle Attack Based on SSP using OOB Association model. They proposed a novel Man-In The-
Middle (MITM) attack against Bluetooth enabled mobile phone that supports Simple Secure Pairing (SSP). From the literature it was proved that the SSP association models such as Numeric comparison, Just works and passkey Entry are not more secure. They have suggested OOB channel to overcome this problem. Presently visual confirmation by user is OOB in Bluetooth, Which is not so secure so can’t we have some additional mechanism?

Kumar et.al. (2012) have inspected the security threats in the mobile adhoc networks, Due to nature of mobility and open media wireless Ad-hoc network are much more prone to all kind of security risks as covered. As a result, the security needs in the wireless Ad-hoc network are much higher than those in the traditional wired networks. They have surveyed active attack, passive attack, routing attack, transport layer attack etc. A whole framework is required to handle all such attacks in wireless networks in my view.

Arafat et.al. (2009) have devised a research tool that tests 4 different pairing approach 1) Button-to-Button (B-to-B) 2)Display-to-Button (D-to-B) 3)LED-to-Button (LED-to-B) 4)Beep-to-Button (Beep-to-B). The development of this simulator include Bouncy Castle Cryptographic library, and Chart2D library. Bouncy Castle is a lightweight collection of APIs used in cryptography. It can be tool to check any proposed pairing variant.

Soriente et.al. (2009) have presented a BEDA protocol for pairing devices. They have used a human factor for designing protocol. They claim it is more secure. BEDA protocols or their variants are still in research & testing phase. No comprehensive framework has been developed for them.

Kumar et.al. (2012) have proposed a key distribution scheme which authenticates users identity for each message. Their scheme forces prior authentication before key exchange begins. They have suggested double encryption using public key of both the parties ,and devised a way that even if attacker decrypts public key, It will be too time
consuming for him to crack it[8]. But only theoretical explanation has been given. Whether this scheme works practically needs to be tested.

**Kumar et.al. (2009)** have tested all available pairing testing methods. They presented the first experimental evaluation of prominent device pairing methods. They pursued a thorough analysis of these methods in terms of both security and usability. Results show that simple Number Comparison is quite attractive overall, being fast and secure as well as readily acceptable by users. HAPADEP variant seems to be preferable in scenarios where one device has a speaker and the other a microphone: it is fast, error-free and requires very little user intervention. Very good study of existing protocols from all perspective. As number comparison is most suitable, focus should be on how it can be made more compact.

**Uzun and Karvonen (2007)** focused on 2 questions 1) “how to implement pairing protocol so that it is easy to use?” 2) “Is it still secure when used by a non-technical person?” In their study Users perceived “Compare-and-Confirm” and “Select-and-Confirm” as easy to use, and considered “Copy” difficult. However, they considered Compare-and-Confirm and Select-and-Confirm to be less secure and less professional than Copy. They concluded that Copy is inherently resistant to fatal errors. The Users clearly differentiated among the methods in terms of ease-of-use and perceived level of security. Again a research proves that user-friendliness is as important as its security.

**Soriente et.al. (2008)** introduced HAPADEP – an approach to secure device pairing. HAPADEP can be viewed as an extension of the previously proposed Loud-and-Clear technique where all communication is conducted over the user perceptible audio channel. It works for very short distance (30-60 cm) and unsuitable for noisy environments. Protection against MITM also is not very powerful. Here they convert cryptographic data to human-verifiable audio. For deaf people, this scheme is not usable at all. And there can be an alternative way of generating cryptographic pattern also.
**Mandal et.al. (2014)** proposed a new architecture for generating pin. Present system uses DH key for calculating link key. However, there are more layers in the present model, then the model they have presented. Whatever they proposed is simple but as they said it is to be tested in future and needs to be more strengthened.

![Diagram of key exchange](image)

**Momani et.al. (2011)** have proposed enhanced SSP architecture (ESSP). They have added few steps before actual SSP starts. They claim, that intruder will be caught if he tries to attack. Well, claims must be verified. Again which cryptography module can be utilized here is not specified here.

**Nazir et.al. (2012)** presented an overview of some of the major attacks that Bluetooth has faced over the years along with some possible solutions. Some safety tips for the users have also been provided to instantly create awareness among them to be more cautious about their personal information. Although a vast majority of devices now communicate using this technology, the risks are far greater if the security threats are overlooked by peers in this industry. A good document for understanding how pairing works as per existing specifications. But onus is on users again on how to secure it.
Mishra and Gupta (2012) have proposed solution for MITM attacks and what they proposed that before ssp starts, some cryptographic method can be utilized. Again they are missing exactly which cryptographic module should be used for this.

Reddy and Jena (2011) have tried to solve mitm problem by storing keys in database. They have also advised use of cryptography before pairing starts. But again which cryptography method should be used is not specified. They have advised this approach for piconet (A group of NFO objects), can’t be utilized for pairing 2 devices.

Aissi et.al. (2004) made a proposal for enhancing Bluetooth Security Using an improved pairing Mechanism. They have 1st presented a current pairing scheme and its variant is being used today. They have suggested Two-stage approach, Registration Stage and key establishment stage. Registration stage comprises of initial key generation by one of the devices and exchange of identities and Cryptographic verification values. Cryptographic verification value (PIN) can be entered and stored in the devices after the first stage. Intention was to make short range financial transaction more secure but it was lacking enough security, Today its variant SSP is used.

Musale and Apte (2012) have concluded that Bluetooth is a WPAN standard that is moderately secure but still has weaknesses in its security architecture, making it vulnerable to attacks by malicious intruders. They have listed many types of attacks and advised user to be vigilant while using Bluetooth. They haven’t suggested any mechanism for Bluetooth security. Onus on users for being more secure is not advisable.

Metagar et.al. (2013) have given guidance for establishing secure wireless networks keeping in mind a layman. They have given listing of a combination key (generation) algorithm which is used in pairing. Their opinion about present state is for now, Bluetooth offers convenience and access to a broader base of information, but one must remember that there are people out there with malicious intent, and they can
violate Bluetooth security. Their proposed solution can be compared with ssp, but can’t
ssp be made stronger.

Kumar (2009) Emphasized that the problem of pin guessing attack on the Bluetooth
system. He has not suggested any measures to stop guessing effective, or how that can
be tackled. Guessing here is made with sniffer (by machine) so countering that is bit
more difficult.

Chang et.al. (2012) have proposed Securing Bluetooth Communications; which
applies the familiar authentication method of entering the same PIN number on both
connecting devices, as an alter-native to confirming displayed numbers. This increases
the efficiency of the operation. Well but it is Compromise with existing standard. At
present no user enters any numeric pin. User friendliness is compromised here and it is
like older v2 protocols