Man-in-the-Middle Attack and its Countermeasure in Bluetooth Secure Simple Pairing

Thrinatha R Mutchukota, Saroj Kumar Panigrahy, and Sanjay Kumar Jena

Department of Computer Science & Engineering
National Institute of Technology Rourkela, 769 008, Odisha, India
{thrinathr,skp.nitrkl}gmail.com,skjena@nitrkl.ac.in

Abstract. This paper describes the countermeasure of man-in-the-middle attack in Bluetooth secure simple pairing. The attack is based on sending random signals to jam the physical layer of legitimate user and then by falsification of information sent during the input/output capabilities exchange; also the fact that the security of the protocol is likely to be limited by the capabilities of the least powerful or the least secure device type. In addition, a new countermeasure is devised that render the attack impractical, as well as it is an improvement to the existing Bluetooth secure simple pairing in order to make it more secure.

Keywords: Bluetooth, MITM, SSP, Security, NINO

1 Introduction

Bluetooth is a technology for short range wireless data and real time two-way audio/video transfer providing data rates up to 24 Mbps. It operates at 2.4 GHz frequency in the free Industrial, Scientific, and Medical (ISM) band. Bluetooth devices that communicate with each other form a piconet. The device that initiates a connection is the piconet master and all other devices within that piconet are slaves. The radio frequency (RF) waves can penetrate obstacles, because of this reason the use of wireless communication systems have grown rapidly in recent years. The wireless devices can communicate with no direct line-of-sight between them. This makes RF communication easier to use than wired or infrared communication, but it also makes eavesdropping easier. Moreover, it is easier to disrupt and jam wireless RF communication than wired communication. Because wireless RF communication can suffer from these threats, additional countermeasures are needed to protect against them.

The basic Bluetooth security configuration is done by the user who decides how a Bluetooth device will implement its connectability and discoverability options. The different combinations of connectability and discoverability capabilities can be divided into three categories, or security levels: *Silent, Private* and *Public* [1]. In Bluetooth versions up to 2.0+EDR, pairing is based exclusively on the fact that both devices share the same Personal Identification Number (PIN)

or passkey. As the PINs often contain only four decimal digits, the strength of the resulting keys is not enough for protection against passive eavesdropping on communication. It has been shown that MITM attacks on Bluetooth communications (versions up to 2.0+EDR) can be performed [1–5]. Bluetooth versions 2.1+EDR (Enhanced Data Rate) and 3.0+HS (High Speed) add a new specification for the pairing procedure, namely Secure Simple Pairing (SSP) [1]. Its main goal is to improve the security of pairing by providing protection against passive eavesdropping and Man-in-the-Middle attack (MITM) attacks. Instead of using (often short) passkeys as the only source of entropy for building the link keys, SSP employs Elliptic Curve Diffie-Hellman public-key cryptography. To construct the link key, devices use public-private key pairs, a number of nonces, and Bluetooth addresses of the devices. Passive eavesdropping is effectively thwarted by SSP, as running an exhaustive search on a private key with approximately 95 bits of entropy is currently considered to be infeasible in short time. In order to provide protection against MITM attacks, SSP either asks for user's help or uses an Out-Of-Band (OOB) channel. The SSP uses four association models named OOB, Numerical Comparision (NC), Passkey Entry (PE) and Just Works (JW). Figure 1 shows the Bluetooth SSP with NC method. The six phases of SSP are explained below:

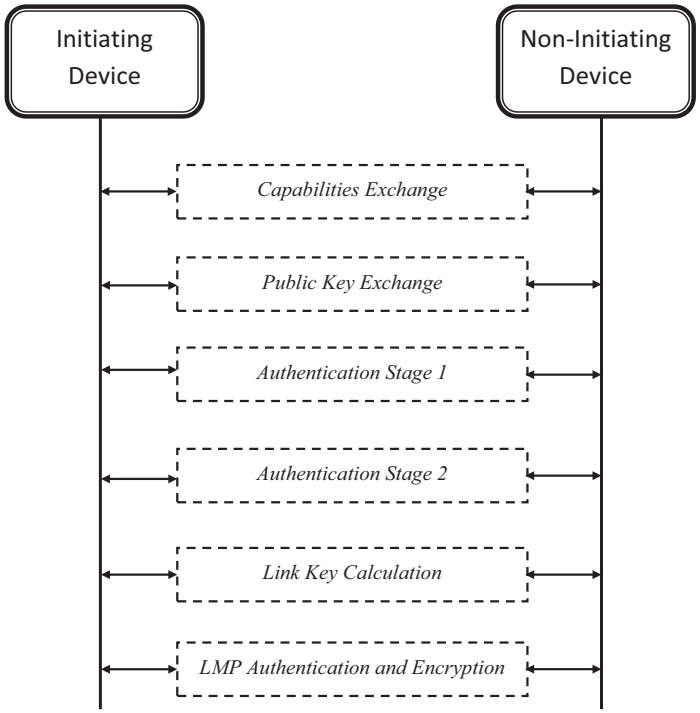

Fig. 1. Bluetooth Secure Simple Pairing with Numerical Comparision

- **Capabilities Exchange:** The devices that have never met before or want to perform re-pairing for some reason, first exchange their Input/Output (IO) capabilities to determine the proper association model to be used.
- **Public Key Exchange:** The devices generate their public private key pairs and send the public keys to each other. They also compute the Diffie-Hellman key.
- **Authentication Stage-1:** The protocol that is run at this stage depends on the association model. One of the goals of this stage is to ensure that there is no MITM in the communication between the devices. This is achieved by using a series of nonces, commitments to the nonces, and a final check of integrity checksums performed either through the OOB channel or with the help of user.
- **Authentication Stage-2:** The devices complete the exchange of values (public keys and nonces) and verify the integrity of them.
- **Link Key Calculation:** The parties compute the link key using their Bluetooth addresses, the previously exchanged values and the Diffie-Hellman key constructed in public key exchange phase.
- **Link Management Protocol Authentication and Encryption:** Encryption keys are generated in this phase, which is the same as the final steps of pairing in Bluetooth versions up to 2.0+EDR.

The rest of the paper is organized as follows. The reported literature on various MITM attacks on Bluetooth are summarized in Section 2. Existing countermeasures and proposed countermeasure against MITM attacks are discussed in Section 3 and 4 respectively. Section 5 provides the concluding remarks.

2 MITM Attacks on Bluetooth

The First MITM attack on Bluetooth assumes that the link key used by two victim devices is known to the attacker was devised by Jakobsson and Wetzel [2]. This attack will work for the version 1.0B and as well as all versions upto 2.0+EDR, because of no security improvements were implemented in those specifications. The authors also showed how to obtain the link key using offline PIN crunching, by passive eavesdropping on the initialization key establishment protocol.

By manipulating with the clock settings, the attacker forces both victim devices to use the same channel hopping sequence but different clocks. This is an improvement of the attack of [2] by Kugler [3]. In addition, Kugler shows how a MITM attack can be performed during the paging procedure. The attacker responds to the page request of the master victim faster than the slave victim, and restarts the paging procedure with the slave using a different clock.

Reflection (relay) attacks aim at impersonating the victim devices [4]. The attacker does not need to know any secret information, because she only relays (reflects) the received information from one victim device to another during the authentication.

The versions 2.1+EDR and 3.0+HS of Bluetooth provide protection against the MITM attacks described above, by the means of SSP. However, it has been shown that MITM attacks against Bluetooth 2.1+EDR and 3.0+HS devices are also possible [5–9]. Because SSP supports several association models, selection of which depends on the capabilities of the target devices, the attacker can force the devices into the use of a less secure mode by changing the capabilities information.

Haataja and Toivanen proposed two new MITM attacks on Bluetooth SSP [1]. The first attack is based on the falsification of information sent during the IO capabilities exchange. The second attack requires some kind of visual contact to the victim devices in order to mislead the user to select a less secure option instead of using a more secure OOB channel. Now the situation has changed— Bluetooth devices with an adjustable Bluetooth device addresses are readily available and techniques for finding hidden (non-discoverable) Bluetooth devices have been invented. Therefore, the danger of MITM attacks has recently increased.

MITM attacks can be possible on these Bluetooth connection methods— (i) SSP with just works, (ii) if one of the devices does not have IO devices or the MITM impersonates as legitimate user and tells "no-input and no-output" as its capabilities to connect and (iii) by creating Jam in physical layer (PHY) when legitimate users know each other. Table 1 shows the bluetooth connection methods and the possibility of the MITM attacks on those methods. Possible solutions to the above attacks are presented in Table 2.

The various jammers used for jamming the PHY layer of Bluetooth devices are— constant jammer, deceptive jammer, random jammer, reactive jammer [10, 11]. The jamming activities of various jammers are given in Table 3. There exist different intrusion detection schemes (IDS) are— Signal Strength Measurements, Carrier Sensing Time, Measuring the PDR and Consistency Checks [10–12]. Discoverability of different types of jammers using different intrusion detection schemes (IDS) are shown in Table 4. With these IDS, one can be able to

Table 1. The Bluetooth connection methods and possibility of the MITM attacks

Sl. No.	Bluetooth Connection Methods	Possibility of MITM Attacks
1	SSP with Just Works	YES
2	SSP-OOB as mandatory	NO
3	SSP- Numeric comparison with both devices have IO capabilities	NO
4	One of the devices does not have IO devices or the MITM impersonates as legitimate user and tells "no-input and no-output" as its capabilities to connect.	YES
5	By creating Jam in PHY when legitimate users know each other	YES
6	By using RF fingerprints as Keys	NO
7	By Adding an additional window at the user interface level	NO

detect all types of jammers and overcome the problem of distinguishing between network dynamics and jamming attacks. However, there are still open issues. For example, the frequency of the location advertisements can significantly affect the performance of the location consistency check system. In addition, wireless propagation effects (e.g., Fading) should be taken into consideration for accurately computing the false alarm rate of the IDS.

There exist also various intrusion prevention schemes— simple PHY layer techniques [10], directional antennas [15], spread spectrum [16], cyber mines and FEC (Forward Error Correction) [13, 14], and use of covert channels in the

Table 2. The possible solutions to the attacks which are presented in Table 1

Sl. No.	Problems	Solutions
1	SSP with Just Works	By not allowing the devices for the JW option association model (the users should have key sharing) OR by allowing the devices by adding an additional window at the user interface level.
2	One of the devices don't have IO devices OR The MITM impersonates as legitimate user and tells "no-input and no-output" as its capabilities to connect.	OOB as a mandatory association model (i.e., the communication will be very secure by using near field communication like infrared).
3	By creating Jam in PHY layer when legitimate users know each other	By using one of Anti-Jamming techniques like frequency hopping, direct sequence spread spectrum and uncoordinated spread spectrum.

Table 3. The types of jammers and their activities

Sl. No	Type of Jammers	Activity
1	Constant Jammer	A jammer continually emits radio signals on the wireless medium. The signals can consist of a completely random sequence of bits.
2	Deceptive Jammer	Similar to the constant jammer. Their similarity is due to the fact that both constantly transmit bits. The main difference is that with the deceptive jammer, the transmitted bits are not random. The deceptive jammer continually injects regular packets on the channel without any gaps between the transmissions.
3	Random Jammer	An attacker employing random jamming, jams for t_j seconds and then sleeps for t_s seconds. During the jamming intervals, the jammer can follow any of the approaches.
4	Reactive Jammer	This jammer is constantly sensing the channel and upon sensing a packet transmission immediately transmits a radio signal in order to cause a collision at the receiver.

Table 4. Discoverability of various jammers using different intrusion detection schemes

Sl. No.	Intrusion Detection Schemes [10–12]	Constant Jammer	Deceptive Jammer	Random Jammer	Reactive Jammer
1	Signal Strength Measurements	Yes	Yes	No	No
2	Carrier Sensing Time	Yes	Yes	No	No
3	Measuring the PDR*	Yes	Yes	Yes	Yes
4	Consistency Checks**	Yes	Yes	Yes	Yes

* PDR measurements can not always distinguish between jamming and network failures and/or poor link conditions.
** Consistency Checks introduce two detection techniques:
(a) Signal Strength Consistency Check
(b) Location Consistency Check

Table 5. Intrusion prevention schemes

Sl. No.	Intrusion Prevention Schemes	Activities [10, 13, 14]
1	Simple PHY Layer Techniques	By reducing the distance between legitimate transceiver pair or by increasing the transmission power, we can reduce the jamming-to-signal ratio and make the link more robust to jamming attacks.
2	Directional Antennas [15]	Jamming interference coming from directions other than the direction of transmission does not stimulate transmission deferrals due to carrier sensing.
3	Spread Spectrum [16]	The most well known techniques are based on the use of Spread Spectrum communications. Here signal processing techniques used as jamming countermeasures.
4	Cyber Mines and FEC (Forward Error Correction) [13, 14]	Low energy long-lived jamming units are called cyber-mines. For handing these there are some methods like Low Density Parity Codes (LDPC) and Turbo-Codes etc.
5	Use of covert channels in the presence of a jammer [17, 18]	When the reception of a packet is affected by jammer, the receiver can identify the reception of a (corrupted) packet. By encoding data based on the inter-arrival times between received corrupted packets, a low rate channel under jamming can be established.

Schemes 1 and 2 do not perform any processing of the transmitted signal while, Schemes 3-5 perform processing of transmitted signal.

presence of a jammer [17, 18]. Table 5 shows the prevention schemes for the jamming attacks.

2.1 MITM Attack in Bluetooth SSP

The MITM first disrupts (jams) the PHY by hopping along with the victim devices and sending random data in every time slot. In this way, the MITM shuts

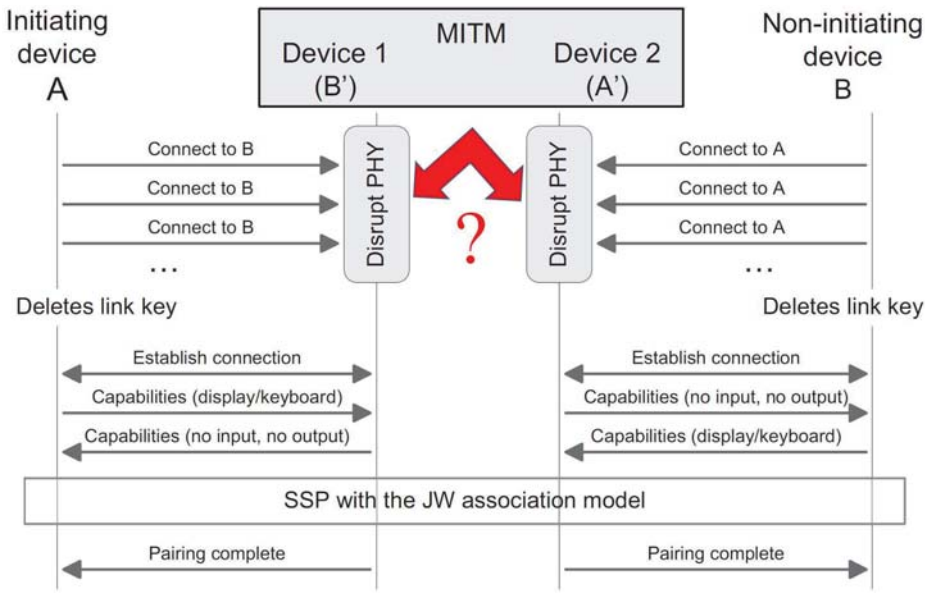

Fig. 2. MITM Attack on Bluetooth SSP

down all piconets within the range of susceptibility and there is no need to use a Bluetooth chipset to generate hopping patterns. Finally, a frustrated user thinks that something is wrong with his/her Bluetooth devices and deletes previously stored link keys. After that the user initiates a new pairing process by using SSP, and the MITM can forge messages exchanged during the I/O capabilities exchange phase by pretending as legitimate user, because the legitimate user's information is deleted. While using the SSP, also the MITM attacks are going to be possible by using the PHY layer jamming and falsification of information. Figure 2 shows the problem of MITM attacks on physical layer of bluetooth devices.

3 Existing Countermeasures

3.1 By Adding an Additional Window at the User Interface Level

It is recommend that an additional window, "The second device has no display and keyboard! Is this true?", should be displayed at the user interface level of SSP when the JW association model is to be used. The user is asked to choose either "Proceed" or "Stop". The advantage of this approach is that the JW association model can still be a part of the future Bluetooth SSP specifications without any changes [1].

3.2 SSP-OOB as Mandatory

Future Bluetooth specifications should make OOB a mandatory association model in order to radically improve the security and usability of SSP. Therefore, future Bluetooth specifications should at least strongly recommend the use of an OOB channel (e.g., NFC) to all Bluetooth device manufacturers [1].

4 Proposed Countermeasure

The proposed approach is as follows. While one of the initiating or non-initiating devices is trying to connect with each other, the attacker will send wrong signals which leads to the corruption of the original signal. So, the legitimate users thinks that, there may be some sort of genuine jam in the network and gets frustrated, and deletes all the information about the other devices. We have to stop these jamming attacks which are attacking PHY layer. By considering the prevention schemes of jamming attack explained in Table 5, we can avoid the MITM attack. After that, the process of SSP will be followed for the secure communication. The prevention schemes of PHY layer are also called anti-jamming techniques. Figure 3 shows the solution for the countermeasure against MITM attack.

5 Conclusion

It is shown that the MITM attack on PHY layer can be avoided by applying the anti-jamming techniques on SSP model. That will give MITM-attack-free

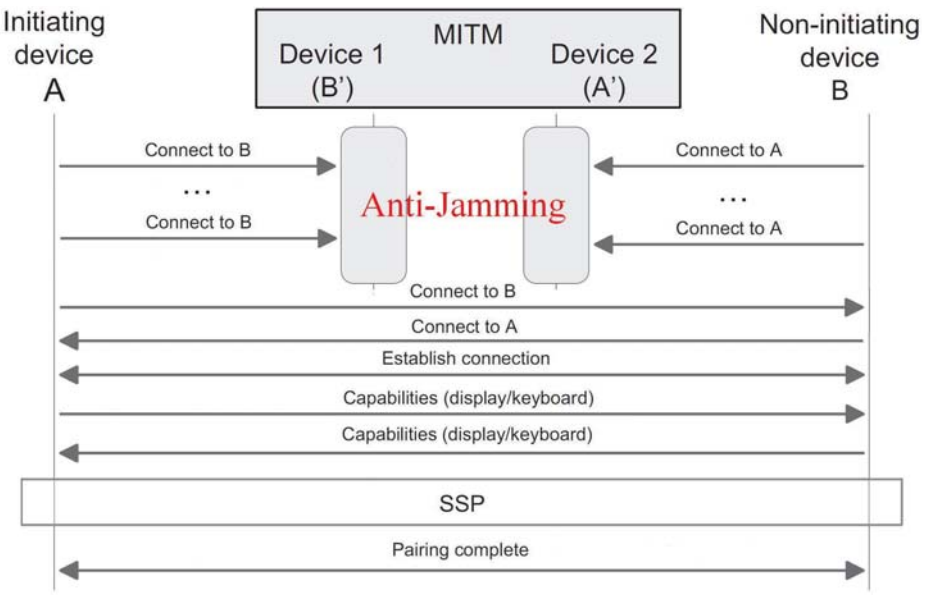

Fig. 3. Countermeasure to MITM Attack

method for secure communication. Still the problem area is open for more research on how to make Bluetooth connections more secure.

Acknowledgment

The authors are indebted to Information Security Education and Awareness (ISEA) Project, Department of Information Technology, Ministry of Communication and Information Technology, Government of India, for sponsoring this research and development activity.

References

1. Haataja, K., Toivanen, P.: Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures. Wireless Communications, IEEE Transactions on 9(1), 384–392 (Jan 2010), http://dx.doi.org/10.1109/TWC.2010.01.090935
2. Jakobsson, M., Wetzel, S.: Security weaknesses in bluetooth. In: Naccache, D. (ed.) Topics in Cryptology, CT-RSA 2001, Lecture Notes in Computer Science, vol. 2020, pp. 176–191. Springer Berlin/Heidelberg (2001), http://dx.doi.org/10.1007/3-540-45353-9_14
3. Kugler, Dennis: "man in the middle" attacks on bluetooth. In: Financial Cryptography, Lecture Notes in Computer Science, vol. 2742, pp. 149–161. Springer Berlin/Heidelberg (2003), http://dx.doi.org/10.1007/978-3-540-45126-6_11
4. Levi, A., Çetintaş, E., Aydos, M., Koç, c.K., Çağlayan, M.U.: Relay attacks on bluetooth authentication and solutions. In: Aykanat, C., Dayar, T., Körpeoglu, I. (eds.) Computer and Information Sciences - ISCIS 2004, Lecture Notes in Computer Science, vol. 3280, pp. 278–288. Springer Berlin/Heidelberg (2004), http://dx.doi.org/10.1007/978-3-540-30182-0_29
5. Haataja, K.: Security threats and countermeasures in Bluetooth-enabled systems. Ph.D. thesis, University of Kuopio, Department of Computer Science (Feb 2009)
6. Suomalainen, J., Valkonen, J., Asokan, N.: Security associations in personal networks: A comparative analysis. In: Stajano, F., Meadows, C., Capkun, S., Moore, T. (eds.) Security and Privacy in Ad-hoc and Sensor Networks, Lecture Notes in Computer Science, vol. 4572, pp. 43–57. Springer Berlin/ Heidelberg (2007), http://dx.doi.org/10.1007/978-3-540-73275-4_4
7. Hypponen, K., Haataja, K.: Nino: man-in-the-middle attack on bluetooth secure simple pairing. In: 3rd IEEE/IFIP International Conference in Central Asia on Internet, 2007, ICI-2007. pp. 1–5 (Sep 2007), http://dx.doi.org/10.1109/CANET.2007.4401672
8. Haataja, K., Hypponen, K.: Man-in-the-middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures. In: Proc. IEEE Third International Symposium on Communications, Control and Signal Processing (ISCCSP-2008). St. Julians, Malta (Mar 2008)
9. Haataja, K., Toivanen, P.: Practical man-in-the-middle attacks against bluetooth secure simple pairing. In: Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on. pp. 1 –5 (Oct 2008), http://dx.doi.org/10.1109/WiCom.2008.1153

10. Pelechrinis, K., Iliofotou, M., Krishnamurthy, V.: Denial of service attacks in wireless networks: The case of jammers. Communications Surveys Tutorials, IEEE 99, 1–13 (2010), http://dx.doi.org/10.1109/SURV.2011.041110.00022
11. Xu, W., Trappe, W., Zhang, Y., Wood, T.: The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing. pp. 46–57. MobiHoc'05, ACM, New York, NY, USA (2005), http://doi.acm.org/10.1145/1062689.1062697
12. Xu, W., Ma, K., Trappe, W., Zhang, Y.: Jamming sensor networks: attack and defense strategies. Network, IEEE 20(3), 41 – 47 (May-Jun 2006), http://dx.doi.org/10.1109/MNET.2006.1637931
13. Noubir, G., Lin, G.: Low-power dos attacks in data wireless lans and countermeasures. SIGMOBILE Mob. Comput. Commun. Rev. 7, 29–30 (Jul 2003), http://doi.acm.org/10.1145/961268.961277
14. Lin, G., Noubir, G.: On link layer denial of service in data wireless lans: Research articles. Wirel. Commun. Mob. Comput. 5, 273–284 (May 2005), http://portal.acm.org/citation.cfm?id=1072503.1072505
15. Noubir, Guevara: On connectivity in ad hoc networks under jamming using directional antennas and mobility. In: Langendoerfer, P., Liu, M., Matta, I., Tsaoussidis, V. (eds.) Wired/Wireless Internet Communications, Lecture Notes in Computer Science, vol. 2957, pp. 521–532. Springer Berlin/Heidelberg (2004), http://dx.doi.org/10.1007/978-3-540-24643-5_17
16. Viterbi, A.J.: Principles of Spread Spectrum Communication. Addison-Wesley Wireless Communications Series, Addison-Wesley (1995)
17. Xu, W., Trappe, W., Zhang, Y.: Anti-jamming timing channels for wireless networks. In: Proceedings of the first ACM conference on Wireless network security. pp. 203–213. WiSec'08, ACM, New York, NY, USA (2008), http://doi.acm.org/10.1145/1352533.1352567
18. Chung, F., Salehi, J., Wei, V.: Optical orthogonal codes: design, analysis and applications. Information Theory, IEEE Transactions on 35(3), 595 –604 (May 1989), http://dx.doi.org/10.1109/18.30982