Enhancing Bluetooth Authentication using Diffie Hellman Algorithm

Rajveer Kaur
Department of Computer Science Engineering
Lovely Professional University
Jalandhar, Punjab, India

Rupinder Kaur Cheema
Department of Computer Science Engineering
Lovely Professional University
Jalandhar, Punjab, India

ABSTRACT
Bluetooth is a technology for connecting devices wirelessly to achieve data transfer at the rate of 720 kbps within a range of 10 to 100 meters. In existing authentication procedure for Bluetooth networks, four levels of key generation viz initialization key , combination key, link key, encryption key were incorporated. Bluetooth devices have limited resources, so we need a small authentication procedure. We proposed a new authentication scheme for Bluetooth networks. We presented enhancement in the authentication procedure of Bluetooth by using Diffie-Hellman Algorithm. This novel authentication procedure acts as the countermeasure against SNARF attack by the introduction of Diffie Hellman algorithm.

Keywords: Authentication, Algorithm, Diffie-Hellman, SNARF

1. INTRODUCTION
Bluetooth is a wireless networking technology which is specifically developed for Personal Area Networking (PAN) and other short range applications [1]. Bluetooth is a technology for connecting devices to each other without cables and any other physical medium. Up to eight Bluetooth devices are networked together by forming piconet, where a single device is the master and rest seven devices are slaves [1]. These piconets are further interconnected to other piconets and create a scatternet. The most common formation protocols for scatternet are Blue Tree, Blue Net and Blue star. Bluetooth uses the radio waves for transferring the data between two devices. It operates on 2.4GHz frequency in the free ISM band (Industrial Scientific and Medical). It uses the frequency hopping. To avoid the channel interference Bluetooth frequency hopping uses 79 different baseband frequencies [1]. Bluetooth devices are connected in maximum 10 meter range, but it will be increased up to 100 meter by using amplifiers. By increasing the range of devices it created some distortion interferences.

Bluetooth technology is developed by Ericsson in 1994, when Ericsson starts researching the possible ways of replacing cables between mobile phones, laptops, printers, etc with wireless links. The Bluetooth SIG was founded in 1998 by Ericsson, Nokia, IBM, Intel and Toshiba 3Com, Microsoft and Motorola joined the Bluetooth SIG in 1999December [1]

The authentication Procedure of Bluetooth is quite complex and need much number of message exchange. This approach is inefficient as large numbers of resources are required at the time of authentication. As Bluetooth are used in handheld devices like PDA's and mobile phone. Resources of these handheld devices are limited and with the current authentication procedure performance of the handheld devices degrades. To enhance the

performance of the Bluetooth devices, we require a new authentication procedure in which less number of messages are exchanged at the time of authentication and less computation needs to be performed by the handheld devices for successful authentication. In Bluetooth devices PIN key is stored when they authenticate to each other for future reference. SNARF attack is possible in Bluetooth devices, it stole your saved PIN key from your device. An attacker can use your PIN key and he/she will get your data from other devices on the behalf of you. Diffie Hellman key exchange algorithm provides the safety against SNARF attack. In Diffie -Hellman algorithm, there has not been the provision for the storage or exchange of the PIN key. So it protects Bluetooth devices from attacks.

1.1 Bluetooth in the nets
In Bluetooth technology there are two types of networks.

1) **Piconet:** In a piconet up to eight devices are considered. Piconet is basic form that handles the Bluetooth devices in a one piconet. In a piconet one device is a mater and rest is the slaves. All devices in a piconet could communication through the master device. All the devices in a piconet share the same channel during typical operations and that devices are synchronized to a common clock and frequency hopping pattern. The synchronization is provided by the master slave. Fig: 1(a) shows a simplest piconet, which is considered only two devices one is master and other is slave. The communication is take place between these two devices.

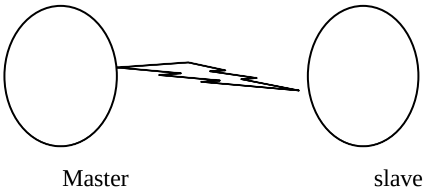

Fig: 1(a) simplest piconet

Fig: 1(b) shows a piconet in which up to eight devices. One is the master and rest seven devices are slaves. In this figure 'm' is master device and 's' is slave devices.

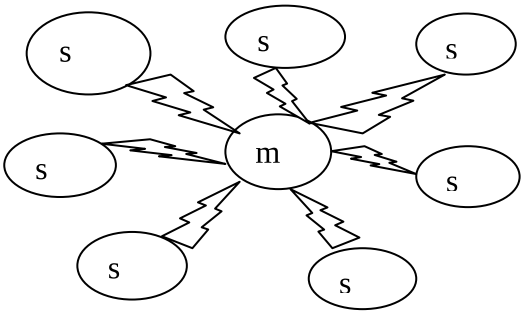

Fig: 1(b) piconet with eight devices

2) **Scatternet**: A bit more complex network is scatternet. When two or more piconets are together it becomes a scatternet. Up to ten piconets at a time is connected to a scatternet. Scatternet is solved the problem of the low bandwidth that every user of a Piconet has if they find great quantity of connected units [1]. Fig 1(c) shows the scatternet. P1, P2, P3 are the piconets in scatternet.

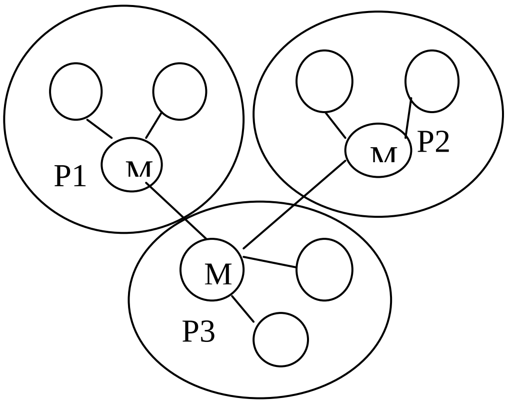

Fig:1(c) Scatternet

1.2 Security Modes

There are three security modes in Bluetooth that describe the Bluetooth specifications. They are defined as follow:

- **Mode 1**: In security mode1 the device will never initiate pairing in a connection.
- **Mode 2**: In security mode2 a remote device will request to device for security requirements to use of an application or a service.
- **Mode 3**: In security mode3 the device will always initiate the security to logical link establishment so this mode referred as a link level security mode.

Two trust levels are specified, that are given below:

- Trusted devices: Those devices are trustily paired they marked as trusted devices and store in device database.
- Untrusted devices: These devices may be paired or unknown, these are not marked as trusted devices and not store in device database.

2. LITERATURE REVIEW

Bin Zhen, Jonghun Park and Yongsuk proposed a blue star island algorithm for network formation. Network formation is done for establishment and maintenance of Bluetooth network topology with better performance. The two piconets with a joint slave becomes a blue star island [2]. John D. Padgett, Booz Allen Hamilton, Herndon, VA, discussed a technical background on how Bluetooth security works, requirements associated with designing and deploying and Bluetooth based solutions for use in the DOD. Services level security modes are discussed security mode1, security mode2 and security mode3. In security mode1 the device will never initiate pairing in a connection. In security mode2, a remote device has sent request to device for security requirements. In security mode3, the device will always initiate the security to logical link establishment. So this mode is referred to as a link level security mode. In this, solutions are also discussed for security modes [3]. Pushpa R.Suri, Sona Rani had discussed some background information about Bluetooth system and security issues to isolate various attacks in the Bluetooth network. They had proposed asymmetric key exchange method. This has reduced the risk of triggering eavesdropping on pairing process and finding the Personal Identifier Number (PIN) used. In this pairing process, mutual authentication and key types are discussed along with their working [4]. Mostafa Akhavan-E-saffar 1, Vahid Tabataba Vakily discussed about the cable replacement technology called Bluetooth and various attacks which are possible in Bluetooth. These attacks are broadly classified into active and passive attacks. Author also discussed, that if Bluetooth architecture is poorly implemented then Bluetooth network is more vulnerable to security attacks [5]. Deepak Jayanna, Gergely V. Záruba discussed various piconet and scatternet formation network topologies. These topologies are like Bluetree, Bluestar, blue net . They had proposed a new piconet formation protocol by following strict rules of protocol development [6]. Zhifang Wang, Robert J. Thomas, Zygmunt Haas discussed the Bluetooth topology called blue net topology. This topology removes the disadvantage of blue tree topology [7]. Rohit Pandharkar and M. A. Joshi discussed about the Diffie-Hellman algorithm which is used to set a secure communication channel .In Diffie-Hellman algorithm various type of attacks are possible. To prevent these attacks, they made enhancement in the Diffie-Hellman algorithm.[8]. Lein Harn, Manish Mehta, Wen-Jung Hsin made enhancement in the Diffie-Hellman algorithm. In this they have integrated digital signature scheme and diffie-Hellman to ensure data integrity and confidentially [9].

3. ATTACKS ON BLUETOOTH

In Bluetooth pairing is an important part of the authentication. When two devices paired to each other they exchange the PIN and PIN stored in Bluetooth devices. They generate a shared secret key that they use for all future communication. PIN can be 8-128 bit long. Some uses only 4 decimal-digit PIN it can be creaked in to 0.3 sec. As technology improves, these attackers could take more advantage. Some of the attacks in Bluetooth are given below:

3.1 SNARF attack: This attack is launched without any knowledge of owner to connection request. In this an attacker connects to the targeted device and this gain the access of the device. All portions of memory are available for the attacker including contacts, pictures, vCards, settings, messages, PIN, etc since the attacker is able to connect without permission from the owner of the phone [13]. This attack is only possible when the phone is set in ‘discovery’ and ‘visible’ mode on the network. Phone cloning is also this type of attack.

3.2 BACKDOOR attack: In this attack an attacker make a trust connection to the target device through the pairing procedure. When both devices are connected to each other, a connection is established successfully an attacker remove attacking device from pairing registry. This connection would again allow access permitted data on the phone as well as phone calls and instant messages. However, since this attack only grants access to information flagged for trusted connections, it is more limited than the SNARF attack [13].

3.3 BLUEBUG attack: An attacker hack your phone to use it like make a call, send and read messages, connect to internet data services. An attacker can monitor conversation in the surrounding area of the phone it is possible when the phone is on a GSM network. This attack is launched within 2 to 3 seconds if all the process is correctly implemented and it not leaves any trace for intrusion. An attacker can then route incoming calls to other devices [13]. Through an AT command this attack give the full control of the device to an attacker.

4. BLUETOOTH AUTHENICATION SCHEME

In this section, we are discussing the current Bluetooth authentication scheme. Following are the various messages which need to be exchanged for successful authentication:

4.1 Pairing procedure

Initialization key generation: The initialization key (I.K) is the first key which generated in the pairing process. It is used to derive combination key later on in the pairing process. Once a combination key is derived, the initialization key will be discarded. The strength of this key relies solely on 4 to 16 bytes Pnumber [5]. To generate a I.K we need a device address (D.A), pass key(PassK) and length (LengthK, in octets), and a 128-bit random value (RANDOM). Following equation

I.K= E33 (PassK', RANDOM, LengthK)........... (1)

PassK' is the concatenation of PassK and D.A.

LengthK= min (LengthK+6, 16)

Fig 2: shows the pairing authentication procedure between master and slave.

Link key generation: combination key is used for link key generation instead of unit key. The combination key is generated with the collaboration of both pairing parties (i.e. device M and S). CK is the combination key of both devices KeyM and KeyS. Each key is generated locally by the device itself.

KeyM= E31 ((RANDOM for M), D.A of M)…….. (2)

KeyS= E31 ((RANDOM for S), D.A of S)………. (3)

The combination key is generated using:

CK= KeyM XOR KeyS…………………………… (4)

Link key exchange: The link key exchange procedure should be done before each party calculates the combination key. This

is to enable the nodes to get each other's random value . To calculate the combination key CK, random value of both the devices is used. For later communication, the combination key will become the link key. The link key exchange procedure is indicated using (5), (6).

Value sent from M to S:

KM= (RANDOM for M) XOR (I.K)……….. (5)

Value sent from S to M:

KS= (RANDOM for S) XOR (I.K) …………(6)

When each party receives the above values equation 5 and 6, to obtain the other parties random value (RANDOM) equation (7), (8) are used. Device M computes:

RANDOM for M= (KS) XOR (K.I)……….. (7)

Device S computes:

RANDOM for S= (KM) XOR (K.I) ………..(8)

The K.I is discarded when the link key is successfully exchanged. After this, each device is able to generate the link key (combination key CK) locally and utilise it for the future secure communication [10].

KEYS	NOTATIONS
Initialization Key	I.K
PIN	Pnumber
Device address	D.A
Pass key	PassK
Length	LengthK
Random Value	RANDOM
Combination Key of two devices (Master & Slave)	CK
Key Master	KM
Key Slave	KS
M	Master
S	Slave

Table1: Notations

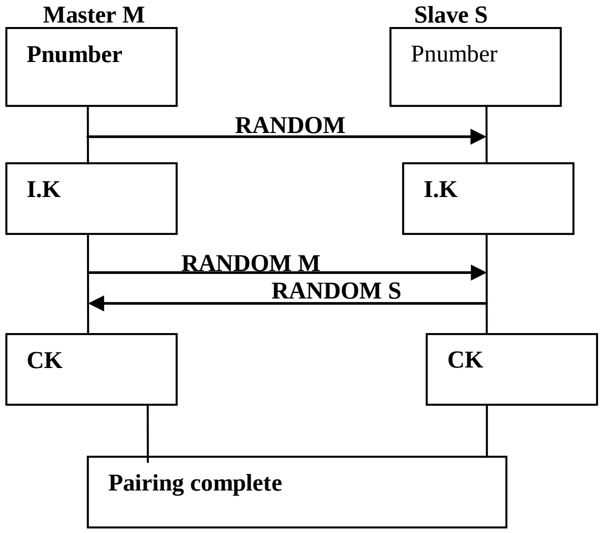

Fig 2: Pairing authentication procedure

4.2 Diffie-Hellman Algorithm

Definition of Diffie Hellman : Let n be a prime number and p be an integer. The Diffie Hellman Problem (DHP) is the problem of computing the value of p^{ab}(mod n) from the known values of p^{a} (mod n) and p^{b}(mod n).

The setup of Diffie Hellman algorithm

1. Suppose we have two parties Master and Slave, they want to communicate to each other.
2. They do not want the eavesdropper to know their message.
3. Alice and Bob agree upon and make public two numbers n and p, where n is a prime number and p

is a primitive root mod n. Anyone has access to these numbers [11].

Master	Slave
Choose a secret number a. Compute M≡ p^a (mod n)	Choose a secret number b Compute S≡ p^b(mod n).

Table 2: Private computations

4. Public exchange of values.
    - Master sends M to Slave ==M
    - S= Slave sends S to Master
5. Master compute the number K≡ $S^a \equiv (P^a)^b$ (mod n).
   Bob compute the number K≡$M^b \equiv (p^b)^a$ (mod n).
   Here Master and Slave have the same key that is K=p^{ab} (mod n).

In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to exchange data. Before starting the communication, secure channel is established. Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established.

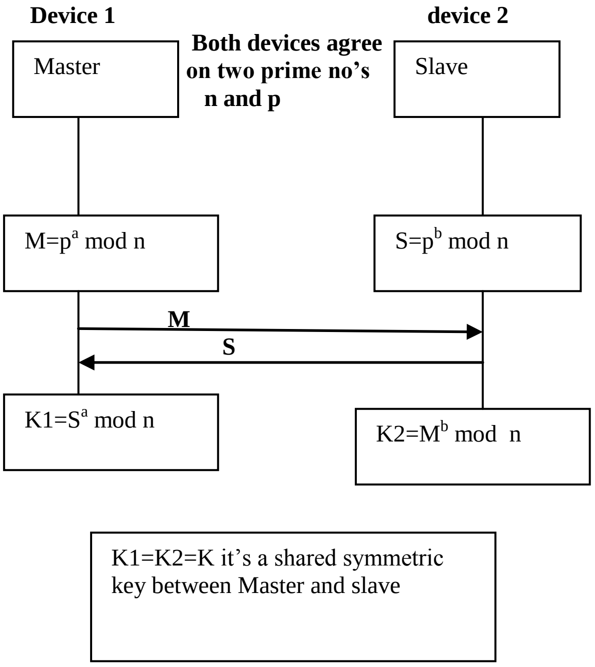
Device 1
device 2
Master
Both devices agree on two prime no's n and p
Slave
M=p^a mod n
S=p^b mod n
M
S
K1=S^a mod n
K2=M^b mod n
K1=K2=K it's a shared symmetric key between Master and slave

Fig3: Diffie-Hellman Key exchange

Fig3, shows that Master and Slave wants to communicate with each other .To start communication both parties need to establish secure channel .To establish secure channel both parties select a random prime number g and n these two number are public. Both parties, Master and Slave now need to select their private numbers respectively these numbers are 'a' and 'b'. As, illustrated in the figure both parties calculated the two numbers M and S from the public and private selected random numbers. After, calculating M and S both parties exchange M and S. When Slave receives M and Master receives S both parties will calculate mode inverse; If both parties have same mode inverse values, secure channel is established between Master and Slave.

To encrypt the packets we used the public key or shared key (K) of both parties. For decryption of packets we use the private key of both parties which is randomly chosen by the users i.e. 'a' and 'b'.

6. PROPOSED SCHEME

In Bluetooth, security is the main concern because Bluetooth is the self configuring network and it is much vulnerable to security attacks. To design an efficient security protocol for Bluetooth is a challenging task. To prevent various types of attacks in Bluetooth network, mobile devices in the Bluetooth network should be mutually authenticated and shared key is exchanged between the mobile devices to encrypt communication between mobile devices by using shared key. In existing Bluetooth authentication initialization key is established firstly and on the basis of initialization key, link key is established. When link key is successful established, secure channel is established and shared key is established. Consequently, data exchanged between the mobile devices are encrypted with shared key. We proposed an algorithm for key shared establishment and secure channel establishment in Bluetooth authentication. We are using the Diffie-Hellman algorithm for authentication in Bluetooth devices. This algorithm established a shared key and a secure channel is setup between Bluetooth devices and in Bluetooth network. In table3 ,we show the comparison between the existing authentication scheme and proposed authentication scheme.

Existing Authentication Scheme	**Proposed Authentication Scheme**
SNARF Attack is Possible	SNARF attack will be prevented
Much number of message exchange will be required for successful authentication	Less number of message exchange is required for successful authentication
More Computations are required for shared key generation	Less number of Computations are required for shared key generation
More energy consumption	Less energy Consumption
Device more wait in authenticated state.	Less wait at authenticated sate
PIN number is stored at the devices which leads to various type of attacks	No Pin number will store at devices.

Table 3: Comparison between existing and proposed authentication schemes

6. CONCLUSION AND FUTURE WORK

In this paper we conclude that existing Bluetooth scheme requires need much number of messages exchange. Bluetooth will be used in the handheld devices which is having limited resources .We need an efficient authentication scheme with requires less number of message exchange for successful authentication. In existing Bluetooth authentication scheme SNARF attack is possible .To prevent this attack, we proposed an new authentication scheme by using the Diffie Hellman exchange protocol for authentication. In our Future work, we will implement our new Bluetooth authentication scheme and compare the result with the existing authentication scheme.

7. ACKNEWLEDGEMENTS

I wish to thanks to Navjot Singh and my teacher Rupinder Kaur Cheema for their guidance during this work. I thank them for unconditional support, for inspiring me, for their valuable insights, patience and guidance. I am very honoured to have had the opportunity to work with them. I specially thanks to my parents who's helped me a lot for this work.

8. REFERENCES

[1] KEIJO HAATAJA "Security Threats and Countermeasures in Bluetooth-Enabled Systems" Department of Computer Science University of Kuopio 2009

[2] Bin Zhen, Jonghun Park and Yongsuk Kim "Scatternet Formation of Bluetooth Ad Hoc Networks" i-Networking Lab, Samsung Advanced Institute of Technology, YongIn city, 440-600, Korea 2003

[3] John D. Padgette "Bluetooth security in the DOD" Booz Allen Hamilton Herndon, VA, April 19, 2009

[4] Pushpa R S uri Sona Rani "Symmetric Key Insecurity in Bluetooth Communication" Department of Computer Science and Applications, Kurukshetra University, kurukshetra, Haryana,INDIA.

[5] Mostafa Akhavan-E-saffar, Vahid Tabataba Vakily "Improvement Bluetooth Authentication and pairing protocol using Encrypted Key Exchange and Station-to-Station MAC Protocols" 2009 international conference on machine learning and computing

[6] Deepak Jayanna, Gergely V. Záruba "A Dynamic and Distributed Scatternet Formation Protocol for Real-life Bluetooth Scatternets" Department of Computer Science and Engineering, The University of Texas at Arlington 2005

[7] Zhifang Wang, Robert J. Thomas, Zygmunt Haas "Bluenet – a New Scatternet Formation Scheme" ECE Cornell Univ, Ithaca, NY, 14853, Proceedings of the 35th Hawaii International Conference on System Sciences – 2002

[8] Karl E Persson and D. Manivannan "Secure Connections in Bluetooth Scatternets" Computer Science Department University of Kentucky Lexington, KY 40506, 2003

[9] K.E. Persson, D. Manivannan, M. Singhal "Bluetooth scatternets: criteria, models and classification" Laboratory for Advanced Networking, Department of Computer Science, University of Kentucky, Lexington, KY 40506, 2004

[10] Sanif Sentosa Liong, Payam M. Barnaghi "Bluetooth Network Security: A New Approach to Secure Scatternet Formation" School of Computer Science and Information Technology, the University of Nottingham Malaysia Campus Kuala Lumpur, Malaysia

[11] Will Garner "Diffie-Hellman Key Exchange"

[12] Inigo Puy "Bluetooth" 2008

[13] James Lewis "Bluetooth Security" ECE 578 7 March 2005

[14] Pushpa R Suri Sona Rani "Symmetric Key Insecurity in Bluetooth Communication" Department of Computer Science and Applications, Kurukshetra University, kurukshetra, Haryana, INDIA.

[15] Zhifang Wang, Robert J. Thomas, Zygmunt Haas "Bluenet new Scatternet Formation Scheme" ECE Cornell Univ, Ithaca, NY, 14853, Proceedings of the 35th Hawaii International Conference on System Sciences – 2002