New Efficient Bluetooth Authentication Scheme

Mustafa S. Kadhm[1], Suphian Mohammed Tariq[2], Hayder Ayad[3], [4]Fouad Abdulrazak

[1]Computer Engineering Techniques, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq.

[2,4]Department of Computer Engineering, College of Engineering, Al-Iraqia University, Baghdad, Iraq.

[3]Department College of Business Administration, AL-Bayan University, Baghdad, Iraq.

Abstract

Bluetooth can be described as a wireless connection used for transferring data from ten to one hundred meters distance with transfer speed around 720kbps. The current validated Bluetooth network process, consists of four stages, key generations for launching key, link key, combining and encrypting key has been included. Small authenticated process will be needed due to the limitation of resources that Bluetooth equipments own. A new authenticated scheme has been suggested for the net of the Bluetooth. Diffie-Hellman Algorithm was used to enhance the authentication process of Bluetooth. This creative authentication process eliminates the effect of the SNARF attacks which stem from the preface of Diffie Hellman algorithm.

Keywords: Bluetooth, Authentication Scheme.

1- Introduction

Bluetooth is a modern technology created to be applied in Personal Area Networks (PAN) and to be used with nearby devices[1]. Bluetooth is a method that depends on the concept of connecting devices wirelessly. By using Bluetooth technology, eight devices can be linked by establishing Piconet, one of these eight devices will be the dominant and the others will be the slaves[1]. This Piconet can be connected to another Piconets to establish what is called Scatternet. The most familiar protocols to create Scatternet are Blue Tree, Blue Net and Blue Star. Radio radiation with range about 2.4 GHz frequencies is the kind of radiation that Bluetooth depends on to transfer the data from point A to point B. Bluetooth utilizes more than 79 various bandwidth frequencies to avoid any interference with other Bluetooth devices [1]. Recently, amplifiers have been trying to increase the Bluetooth range from ten to one hundred meters.

Ericsson is considered to be the pioneer in developing Bluetooth system in 1994. The idea came when he tried to find alternative way to replace cables for data transformation from different devices such as mobile phone, and computers with wireless connections. In 1998, Ericsson, IBM and Nokia and Toshiba have invented the Bluetooth SIG. In 1999 Microsoft and Motorola started to use this technology with their devices.

The authentication measurement of Bluetooth is rather sophisticated and requires many messages exchange. This method is, to some extent, inactive due to the fact that many resources are needed in the authentication process. Using complicated algorithms for Bluetooth authentication affects the performance because of the limited resources in the portable devices.

To improve the performance of the equipments relates to Bluetooth, a new authentication method is required with less messages exchange and minimal computation. The PIN key in Bluetooth connection is saved at the time of mutual authentication in each device reference. There is a possibility of SNARF attack on Bluetooth devices when the stored PIN key might be stolen from the device. A hacker could then control and manipulate the stolen date from other devices and leaves the victim hopeless. In return, to face such a dramatic situation, Diffie Hellman exchanging key algorithm is considered as an effective solution against SNARF strike. The mechanism of this algorithm avoids storing or exchanging the PIN key, therefore it save the Bluetooth device from attack.

1.1- Bluetooth in the networks

There are two types of nets when associated with Bluetooth technology;

The first one is Piconet: in the Piconet, there are up to eight devices can be engaged. Piconet is central form which manages the Bluetooth devices in a one Piconet. The layout of the Piconet, one device is considered to be the master and the others are slaves. The whole system contact with each other through the central (master) device. The Piconet system works and communicates through one channel. All working devices are tied altogether to a common timer and frequency hopping manner. The synchronized system is presented by the master slave approach. Fig. (1) illustrates a basic two devices connected using Piconet system , the first one is the master and the other one is the slave.

Fig.(1) Simplest Piconet

Fig. (2) illustrates a Piconet system with eight devices. One main device connected with slave devices. In this figure, ‘m’ represents master and ‘s’ represents slave devices.

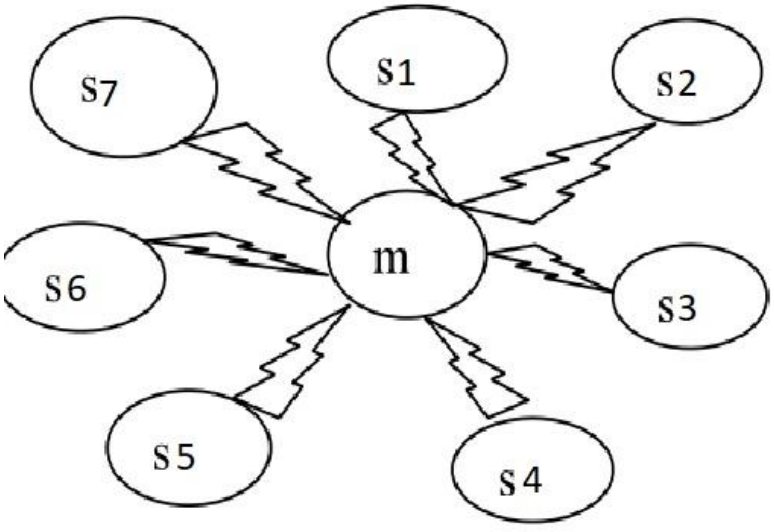


Fig.(2) Piconet with eight devices

The Second one is Scatternet as in fig. (3),which is a sophisticated network consists of two or more Piconets nodes and could be up to ten connected together at the same time. Scatternet is the solution for the dilemma of low bandwidth interference when large number of units are connected.

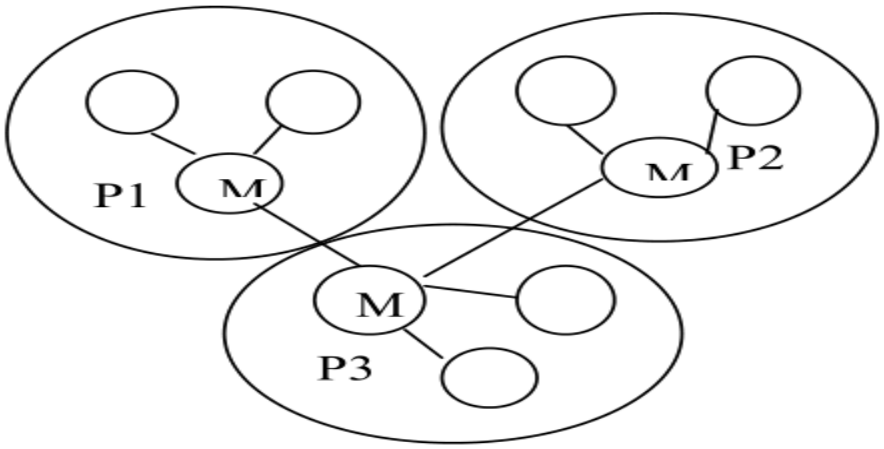


Fig. (3) Scatternet

2- Literature Review

As Jonghun Park and Yongsuk has suggested a blue star island algorithm for net construction. Forming of the network in terms of establishing and maintaining the Bluetooth system technology has been achieved with much better accurate performance. The multiple Piconets jointed with slave turn out to be a blue star island [2]. Some others such as John D. Padgett, Booz Allen Hamilton, and Herndon have argued about the Bluetooth security mechanism and discussed some technological information to support this mechanism. Necessities accompanied with network design, deployment, and Bluetooth fundamental justify the using of the DOD. Level of services and forms of securities have been gone through beside discussing the types 1,2, and 3 of security levels. In security type one, the odds of starting a connection of pairs will be nil. In second type, the distant device has launched a demand to the device for safety measurements. In the last type, rational connection in this mode will never be established unless a security initiation starts in the first place. This last type, and due to this advantage, is indicated as a connection level of security type. Some drawbacks have been investigated for better security patterns [3].

Harmful detrimental aggressions against Bluetooth nets have been examined in detailed in terms of security background of the Bluetooth system by Pushpa R.Suri, Sona Rani. A Non-symmetrical key replacement technique has been presented by them to overcome this issue that mentioned before. In this way the risk of setting off eavesdropping on coupling process and predicting the Personal Identification Number (PIN) have been minimized. In this, a reciprocal verification and key patterns have been applied in the work and studied carefully [4].

The possibility of implementing cable alteration technology, this issue has been debated by Mostafa Akhavan-E-saffar 1,and Vahid Tabataba Vakily because of the regular attacks happen against Bluetooth networks. Assaults against Bluetooth can be classified into active and passive patterns. They stated that there is a steady relationship between the architecture of the network and the rate of attacks. More weakness in architecture design means more security risk and more exposure to be attacked[5]. Deepak Jayanna ,and Gergely V. Záruba have worked on different kind of Piconet and Scatternet system topologies. They came up with a new process or technique to tackle the negative impact of the attacks. They suggested a firm regulations to be followed for this purpose [6]. Zhifang Wang, Robert J. Thomas, and Zygmunt Haas dealt with the Bluetooth topology named blue network. They suggested a method contributed to eliminate the negative impact of blue tree topology [7].

Rohit Pandharkar and M. A. Joshi debated about the algorithm of Diffie-Hellman algorithm. This algorithm is useful to establish a secured communicating channel. Many different types of attacks might happen with the using of this algorithm. To block all these assaults, an improvement to Diffie-Hellman algorithm has been achieved [8]. Lein Harn, Manish Mehta ,and Wen-Jung Hsin have improved this algorithm. They combined digital signature plot with diffie-Hellman to secure data integration and secrecy [9].

3- Attacks on Bluetooth

Bluetooth coupling is a crucial element of the authentication. PIN will be swapped as two devices linked together and this PIN will be kept into Bluetooth apparatus. The pairing device will share a secret key created by them to be used for upcoming connections. PIN might be 8-128 digital bit. Small decimal PIN could be cracked in less than seconds depends on how much complicated the PIN is by the time, the attacks are getting more and more sophisticated and varied due to the advancing in technology. Some of these kinds of attacks are illustrated in the next section.

3.1 PIN Cracking Attack

Utilizing protocol analyzer and acquirement of a FHS package, attacker could try to obtain IN_RAND, LK_RAND and the initializing key through the whole pairing and authenticating process. The attacker might move forward listing to all of probable alternatives of the PIN. Utilizing the obtained IN_RAND and BD_ADDR, they might require attempting probable alternatives as data entering in the E22 algorithm. Finally, they might be capable to uncover the right initializing key. The following step is to assume and examine the odds of the contributed session connection key utilizing all the prior information. Postulating the correct data is gathered, the appropriate gear is utilized, and sufficient time is permissible, PIN cracking turn into a quite simple mission.

3.2. Backdoor Attack:

In this assault, an attacker build a reliable link with the aimed device during the pairing process. When the two devices are linked together, a Connection is formed and recognized successfully an attacker get rid of attacking device from coupling registry. This link might once more permits a way in allowable data on the phone or phone calls and immediate communication like messages. Nevertheless, as this attack barely awards admission to data flagged for reliable communication, it is further restricted than the SNARF attack [13].

3.3 MAC Spoofing Attack

Amongst every passive attacks, the most commonly stated attacks are categorized as MAC spoofing and PIN cracking attacks. Nasty attackers can carry out MAC spoofing through the connection key creation whilst Piconets are being shaped. Guessing the attack is prepared before successful coupling and prior to encryption is formed, attackers could effortlessly interrupt information planned for other devices. Attackers, with particular hardware, could easily utilize spoofing to eliminate valid communication or detain and/or control information whilst in transit. Bluetooth SIG couldn't offer an excellent resolution to stop this kind of attack.

3.4 SNARF attack:

This type can be occurred without any previous knowledge from owner to connection request, and the attacker can get the access of the intended device. The attacker is able to connect to all parts of the memory phone [13] such as pictures, vCards, settings, messages, PIN, Etc. This type of attack including phone cloning, could take place if the phone in 'discovery' and 'visible' status.

4. Bluetooth coupling or Pairing Mechanism

Bluetooth's Generic contact Profile describes the following three diverse security patterns for a Bluetooth device:
Mode 1: is ingrained insecure and not permit authentication and encryption at any rate.

Mode 2: Enforces security after establishing a link between the devices, and required devices are authenticated and encrypted using one time channel that requires security is established.

Mode 3: security is forced down to the connection level and the authentication is achieved through communication establishment. Therefore, the link between devices in security pattern 3 could be limited to devices that have been earlier paired altogether. Through pairing process devices swap link keys and are assumed to be

bonded. Here we clarify Bluetooth's coupling Mechanism [8],[11] when a couple of devices have adequate memory and they produce combination key utilizing each other's connection key. The pairing mechanism indicates the producing and exchanging of keys between devices. The pairing mechanism carries on as follows:

i) Both devices calculate Kinit utilizing E22 algorithm.
ii) E22 algorithm uses as entered data the address of a single Bluetooth elements, BD_ADDR_A, RAND, also the PIN.
iii) RAND is launched in the plain text between the two elements over the Bluetooth Radio guide or channel.
IV) Initializing key is then utilized to encrypt arbitrary values, RAND_A also RAND_B that are applied to obtain the combination of key utilizing the connection keys of two devices.

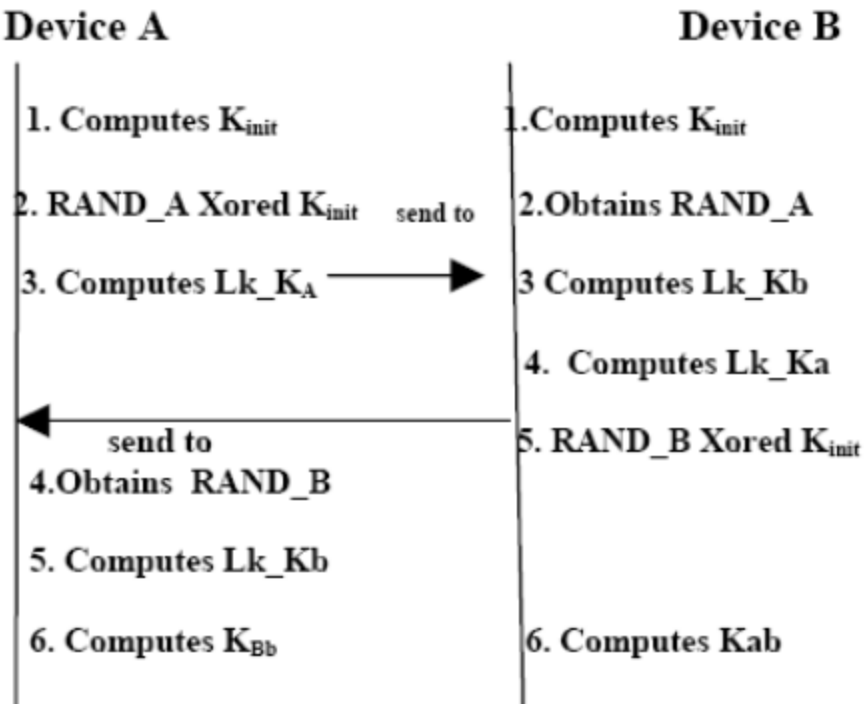


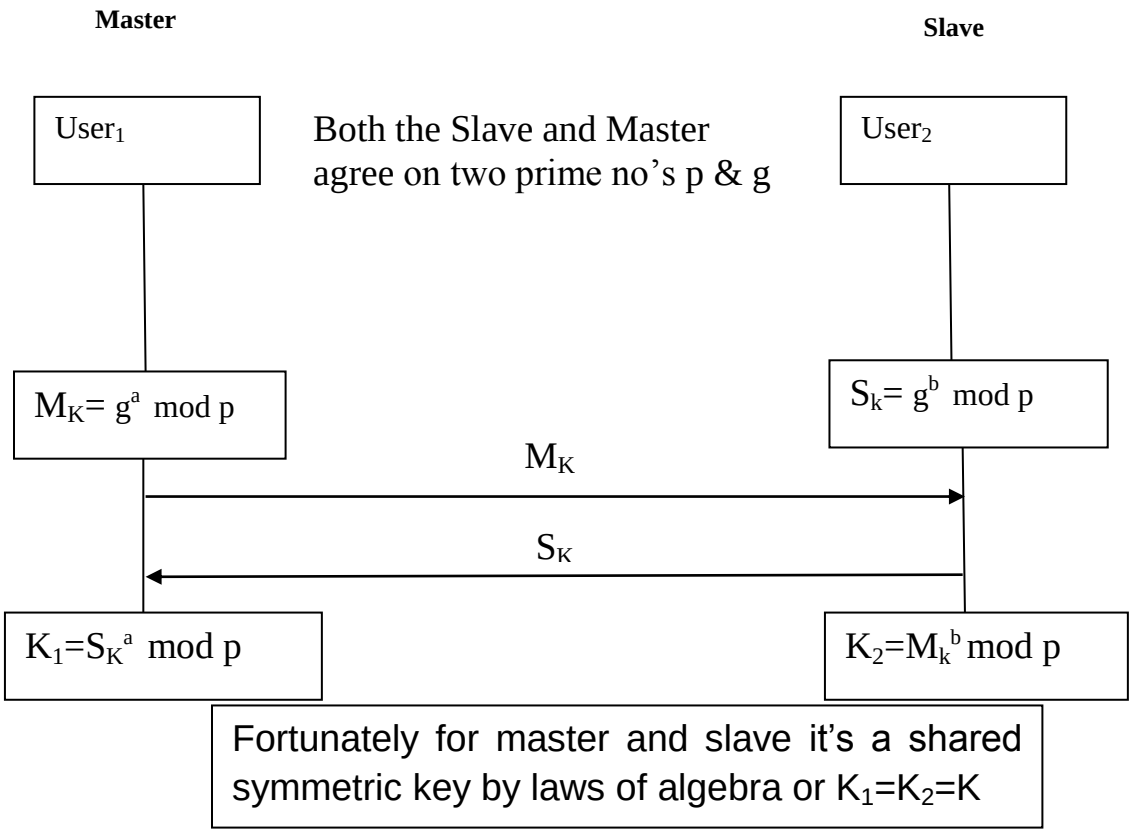
Fig. (4) Bluetooth coupling Mechanism

5- Diffie-Hellman Algorithm

Diffie Hellman is a definite process of exchanging keys. It is considered one of the first practical models of Key switching over achieved within the ground of cryptography. The key could then be utilized to encrypt consequent communications by using of a symmetrical key chipper. The Diffie Hellman Algorithm normally is applied to create the common or public key. Common key algorithm for key exchanging lets users to switch a secret key over an exposed and insecure medium without any former
Secrets [2].

Stages in the algorithm:
1- Both the Slave and Master correspond on a prime and base numbers p and g respectively.
2- Master and Slave calculates public key
2.1- Master selects a classified and unknown number a, and dispatch to Slave
$M_K = g^a \bmod p$
2.2- Slave selects a unknown and secret number b, and dispatch to Master
$S_k = g^b \bmod p$

3- Master and Slave Exchange their public key to both the party
3.1- Master calculates $K_1=S_K^a \bmod p$.
3.2- Slave calculates $K_2=M_K^b \bmod p$.



Fig(5): Diffie-Hellman Key exchange

Each Master and Slave could utilize this number as their own key. Be informed that p and g do not require protection .

In case two sides in, Diffie-Hellman algorithm declares, Master and Slave want to swap data. Prior to initiating the communication, protected channel is formed. Both sides of parties chose their own arbitrary number. On the foundation of the chosen arbitrary numbers, protected channel and joint key is formed.

6- Suggested Scheme

The main point that should be concerned about, in the Bluetooth, is security because Bluetooth is self-organizing system and it is much exposed to security attacks. Designing proficient Bluetooth security protocol is considered a hefty sophisticated task. To stop diverse categories of attacks in Bluetooth net, portable devices in the Bluetooth net should be reciprocally authentic and shared key is swapped over between the portable devices to encrypt connection between portable devices by utilizing shared key. In current Bluetooth validation, initializing key is formed in the first place and on the beginning of starting key, the communication key is formed. When communication key is successfully formed, the secure channel is formed and common key is formed. Accordingly, information exchanged between the portable devices are encrypted by common key. An algorithm was suggested for sharing key formation and secure channel formed in Bluetooth authentication. Diffie-Hellman algorithm is used for validation in Bluetooth appliances. This algorithm formed a common key and a safe channel is installed

among Bluetooth appliances and in Bluetooth network. Table 1 , shows a detailed comparison between the current authenticated scheme and the suggested one.

Table 1: Comparison between existing and suggested authentication schemes

Existing Authentication Scheme	Suggested Authentication Scheme
NARF Easy to be attacked	NARF attack is not allowed
xchanging plenty of messages comply with uccessful authentication	ess messages can lead to uccessful authentication
lenty of processes are necessary for shared ey generation	w number of processes are sufficient
onsuming huge energy	nergy saving
ong waiting time in authenticated condition.	hort waiting time in authenticated condition.
lot of attacks are expected due to storing of n number at the devices	evices are not storing any pin number .

7- Conclusion & Future Work

In brief, the current Bluetooth scheme needs plenty of exchanged numbers of messages. Bluetooth are applied extensively in portable devices that work with inadequate resources. Proficient Authenticated scheme with few numbers of exchanged messages will be needed for successful validation. Current authentication of the Bluetooth scheme, SNAEF attack is probable. To tackle this issue, a new suggested authentication scheme by utilizing Diffie Hellman swap protocol was suggested. For future plan, the new Bluetooth validation scheme will be used and the results will be compared with the current authentication scheme.

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.