Provide Simple Protection for Bluetooth Connection in Wireless Personal Area Network

Mohammed Zaki Hasan Allayla

Assistant Lecture

Abstract

Wireless internet access based on Wireless Local Area Network (WLAN), such as a wireless-Fidelity (Wi-Fi), or Bluetooth networks will become popular with the next few years. New services will be offered that make use of the location and personal profiles to filter internet access. This paper presents security system for indoor location between two devices the mobile device and computer based (Laptop Computer) on Bluetooth technology. The system programmed by visual basic using the Microsoft® Comm (MSComm) control in combination with the others controls to control too many different USB ports. The Bluetooth access points of a network through using the port USB in the laptop computer for the location system and want to access a Global Services Mobile (GSM) Mobile device attached to the computer through a communication Port. It can send, receive a file or write a simple message or long message into input to a textbox and, then perform hash operation through using special algorithm to generate and then send it with systemic key.

الخلاصة

شبكات الانترنيت اللاسلكية المعتمدة على الشبكة اللاسلكية الداخلية التي أصبحت أكثر شيوعا وللسنوات القادمة خدمات جديدة جعلت وضعية الاستخدام من حيث الموقع والدخول الى شبكة الانترنيت مرشحا. هذا البحث يمثل استخدام تقنية البلوتوث لتحقيق الاتصال بين جهازين او جهاز و جهاز موبايل. تمت البرمجة بلغة فيجوال بيسيك باستخدام الأدوات الخاصة والمضافة للسيطرة على الاتصال عن طريق المنافذ التي تعطي امكانية الوصول (خدمة تحديد المواقع) او إرسال الرسائل القصيرة او غيرها من الاستخدامات ولتحقيق الامنية في الاتصال تم ادخال عملية الاعادة او التكرير لزيادة الامنية في الاتصال وارسال البيانات باستخدام مفتاح مشترك.

1. Introduction

The using of the mobile device can increase productivity and responsiveness to costumers. Once equipped with a mobile device, users are no longer limited by the constraints of a work day; anytime, anywhere access to enterprise information that can processed, acted upon, and delivered around the clock is a reality.

In order to begin, it should state a simple different between the Bluetooth and IEEE 802.11b and often their complementary. IEEE 802.11b is largely applied to LAN access, while Bluetooth LAN access is only one of many applications, most of which focus on smaller personal area networks (PANs). Different target applications and technology dictate different security architectures. With the differences between Bluetooth technology and IEEE 802.11b in mind, one may ask about question the validity of comparing the security architectures of the two technologies [1]. The security requirements for Bluetooth applications will vary based on the sensitivity of the information involved, the market, and the needs of the user. There are some applications that do not require any security and others which require extremely high levels of security. Risk analysis and trade studies need to be conducted prior to implementing new applications using Bluetooth wireless technology [8]. As Bluetooth is a radio-based technology, in principle there exists a danger that "unauthorized" Bluetooth-capable devices could listen in to Bluetooth communications and/or actively insert themselves into the communication link. The cryptographic security system which programmed for the Bluetooth connection is aimed at eliminating from these threats. Cryptographic authentication and encryption algorithms are used between two devices portable computer and mobile device. These are implemented on the high layer protocols, called the Application Bluetooth Protocols (ABP). The cryptographic procedures used are based on link keys, which in each case are agreed between two Bluetooth devices during connection. At the application layer define the host controller interface for the user. These keys are computed as a function Personal Indentified Number (PIN), a

random number and then establish the all connection through Bluetooth Device Address (BDA).

2. Bluetooth Networks

Bluetooth technology is a wireless system for short-range communication. It has developed to set up a collection of devices communicating on behalf of client application. The key features of Bluetooth technology are robustness, low power, and low cost, it developed by Ericsson with the assistance of Intel. It provides either point-to-point links, or multipoint without any native IP support, meaning it cannot easily support point to point protocol (PPP). Bluetooth support TCP/IP as one profile implemented through point to point protocol (PPP) on a given conduit [4].

Bluetooth Networks (BNs) are made up of piconets, which are loosely fashioned or ad-hoc networks piconets are made up of one master node and seven simultaneously active slaves or an almost limitless number of virtually attached but not active (standby) nodes. Master nodes communicate with slaves in a hopping pattern determined by a 3-bit Active Member Address (AMA). Parked nodes are addressed with an 8-bit Parked Member Address, (PMA). Up to ten piconets can be collocated and linked into what is called scatter nets. A node can be both a master in one piconet and a slave in another piconet at the same time, or a slave in both piconets at the same time. The range of a Bluetooth standard piconet is 10 meters, relative to the location of the master. Bluetooth signals pass through walls, people, and furniture, so it is not a line-of-sight technology [2]. Figure 1 provides a logical depiction of several piconets linked together as a scatter net.

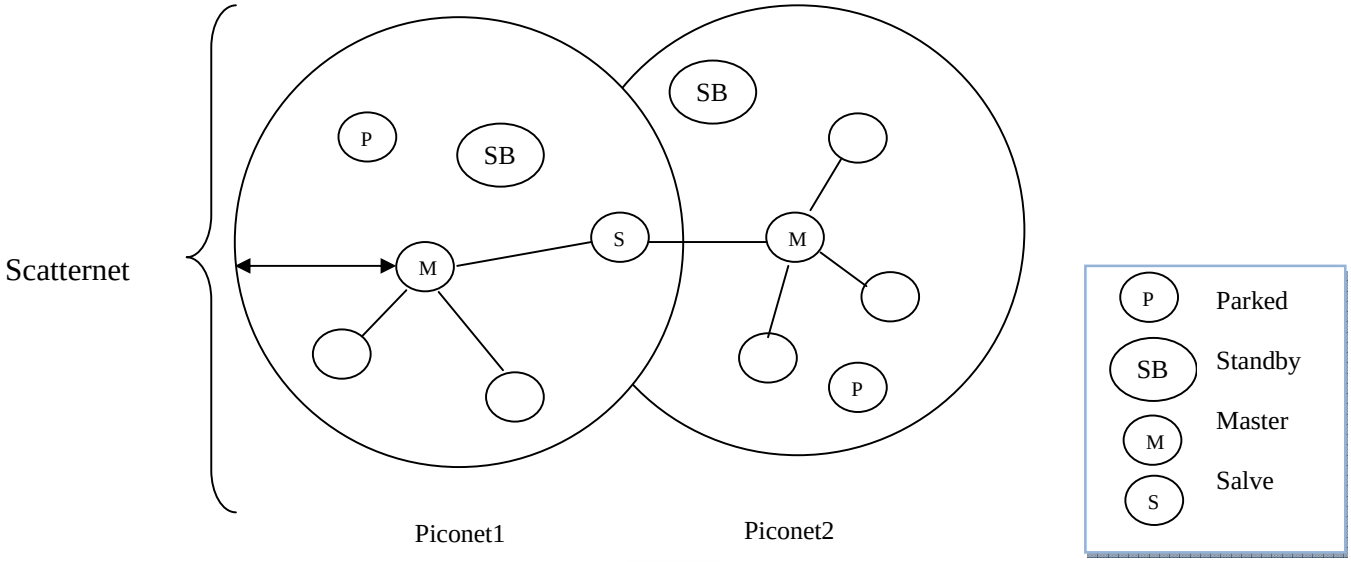

Figure 1 Bluetooth Piconet and Scatternet Configuration

Bluetooth certification is achieved by devices that pass interoperability testing by the Bluetooth Special Internet Group (SIG), an entity which makes certain that these products satisfy the standard. Bluetooth is based around a 9mm by 9mm microchip that operates as an inexpensive means of forming a short-range radio link that provides security for fixed wireless workstations as well as mobile computing devices one of the most advantageous features that Bluetooth has to offer is that it can network devices "ad hoc." This means you can link your laptop computer, and phone with one centralized Bluetooth interface. It can transfer files, names, and addresses with one unified connection protocol, essentially breaking the barrier of sharing information from one device to another [3].

The Bluetooth wireless technology system contains a set of profiles. A profile defines a selection of messages and procedures from the Bluetooth SIG specifications. This gives an unambiguous description of the air interface for specified services and use cases. Working groups within the Bluetooth SIG define these profiles. The Security Expert Group (BSEG) provides the Bluetooth SIG and

associated working groups with expertise regarding all aspects of Bluetooth security [4].

From these reasons, and the attack on the Bluetooth security that describe later, a new profile has been added in order to increase the security level. This profile differ from other setting profiles in hashing the pairing mode for both connected devices each others.

3. Create the alternative point-to-point networking scenario

The scenario that created included all the configuration status of Bluetooth Network, but just one status has been performed. Which it is point-to-point connection, such as two devices the mobile device and computer based (Laptop Computer), or between two computers. Figure 2 illustrate the Bluetooth technology connection scenario.

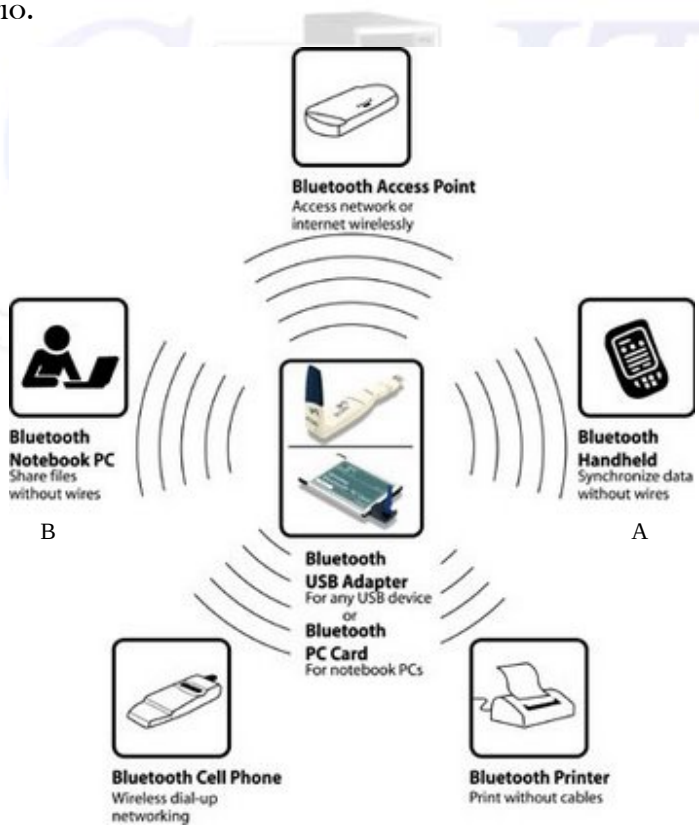

Figure 2 The Bluetooth technology connection scenarios
(A): Two devices laptop and mobile – (B): Two laptops devices

A Bluetooth device has three base modes. The user can switch on or off every mode independent from the other modes [4].

- First, there is the Discoverable Mode. If the device is "discoverable", it listens and answers to inquiries. If it is "non-discoverable"no inquiry scan is accomplished. This is non-secure mode.
- Second, there is the Connectable Mode, which affects that a Page Scan is accomplished to open a connection. If the device is switched over to "non-connectable", no Page Scan is done. This is not secure mode until a channel establishment has been initiated.
- Third, there is the Pairing Mode. If the device is "pairable "the Personal Indentified Number (PIN) is used for authentication, if it is "non pair able "the Personal Indentified Number (PIN) is not entered. Link level enforced security; the security process is executed before the link is established.

At the application layer in Bluetooth stacks, an option security style has add at this layer to perform more authentication through used the Personal Indentified Number (PIN) symmetrical encryption. Both users deal with symmetrical Personal Indentified Number (PIN) for sending the file in encrypts form and decrypts with same Personal Indentified Number (PIN) at once the connection occur, where addition is capable with the all modes above. Beginning from the listening, connection occur, and that moment the authentication through the entering the Personal Indentified Number (PIN) ask, and the user must answer with the Symmetric Identifier Key (SIK), which also encrypted by hash function to decrypt the original file, otherwise the file still in unreadable form to user.

After describe the scenarios of connect one Bluetooth device to another. It is necessary to know how to transfer data between the two devices .There is no need to go into the specifics of the algorithms that Bluetooth devices use to choose on their radio frequencies. The Bluetooth is no more than just a replacement for a USB port. First operation let

assume that beginning searching from deceives started, at once the connection occur both the authentication and encryption/decryption started for sending or/and receiving the files between two devices. The authentication covers only the knowledge of a common secret key and the knowledge of the device addresses.

4. The propose of the creation of the security

First step it must describes the Bluetooth attack mechanism from the attacker, which called passive attack. The Bluetooth technology has a significant security component, which includes key management, authentication and secrecy. However, the security of the whole system relies on the user's choice of secret Personal Indentified Number (PIN). In normal cases the user enters the must often too short, for example (12345) or just one digit. Which get the attack the capability to attack such as: -

- First attack: - the stealing keys, link keys and encryption keys from victim of his/her choice. This can be done either by exhaustively searching through Personal Indentified Number (PIN), or mounting a middle- person attack.
- Second attack: - mapping the physical whereabouts of users carrying Bluetooth-enable devices by planting "Bluetooth detecting devices" at locations of interest.
- Third attack: - final attack is on the cipher, that the attacker can break the security. [6]

So it must take any consideration for these types of attacks, to protect the connection, data. Through present security system for indoor location between two devices the mobile device and computer based (Laptop Computer) on Bluetooth technology.

5. The sequence steps for implementation of connection operation & the aim consideration of security:-

Nearly all major cryptographic protocols depend on the security of hashing operation. Which it means that the protocols must programmed in the application

layer in Bluetooth stack. The connection in Bluetooth wireless personal area network through takes the secret key, which request from the user to enter to success the pairing and shared between two or more than one devices, as shown in figure 3 below.

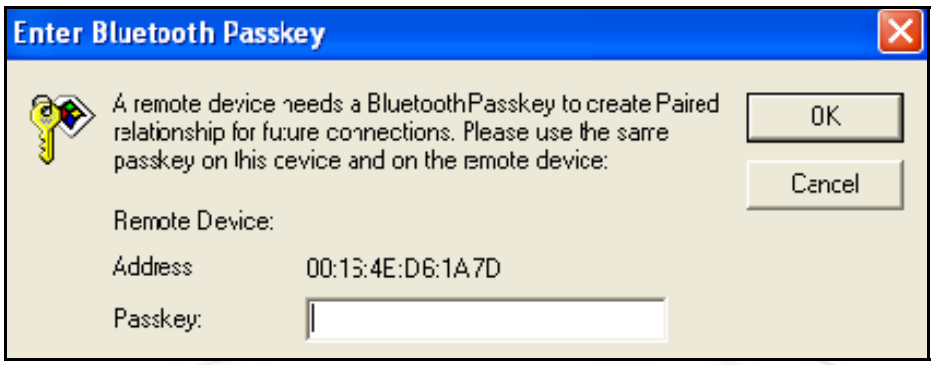

Figure 3: requesting from user to enter the secret key in order to the pair and share

In the same moment the second device, or other devices, must enter the secret key, to acceptance the connection. This is the first authentication between the users based on the one unit keys which are the same. However, a unit that uses a unit key is only able to use one key for all its secure connections. Hence, it has to share this key with all other units that it trusts. Consequently all trusted devices are able to eavesdrop on any traffic based on this key. A trusted unit that has been modified or tampered with could also be able to impersonate the unit distributing the unit key. Thus, when using a unit key there is no protection against attacks from trusted devices.

Though very easy to implement, these mechanisms are usually based on ad hoc techniques that lack a sound security analysis. Most commonly such a mechanism is based on a secret key shared between the parties and takes the form of a hashing operation map of different length of the Personal Indentified Number (PIN). [7]

a. The implementation of Key Generation:-

The creation of an initialization begin through derived from random number, a Personal Indentified Number (PIN), it may be able to be either a factory value or the user which can enter a maximum of 16 octets. The initialization key is discarded when the link key is exchanged between different units. [5]

So it is only one way used to protect the initial value before the connection occurs. when both two users/devices (A) and (B) wants to transmits a message, file, or other things, it appends to the connection a value called the Hash Authentication Tag (HAT), computed by the hash algorithm as a function of the transmitted information and generate another shared secret key. After the user/device (A) enter the Personal Indentified Number (PIN), must hashing it before the connection done i.e. the pairing and the sharing, at the left side user/device (B) recomputed the authentication tag on the received message using the same mechanism (and key) and checks that the value he obtains equals the hash authentication tag in order to the received message.

b. The implementation of Authentication & hashing operation:-

Hash functions are of fundamental importance in cryptographic protocols and the way that used for achieve the authentication connection between the devices. They compress a string of arbitrary length to a string of fixed length; depend on the entering of PIN [9]. A hashing operation is a function which takes the secret key, which request from the user to enter to success the pairing and shared between two or more than one devices, as shown in figure4 below. At the same time when the Personal Indentified Number (PIN) wills Xoring with secret key, the second device, or other devices, must enter the secret key, to acceptance the connection, must recomputed the results of Xoring operation in order to success the connection (both pairing and sharing). And then finally both begin their different operations of sending and receiving as a Short Message Service (SMS), Video, Multimedia Message Service (MMS) and etc... as shown in Figure 5 below show the system programmed by visual basic using the Microsoft® Comm (MSComm) control in

combination with the others controls to control too many different USB ports. The Bluetooth access points of a network through using the port USB in the laptop computer for the location system and want to access a Global Services Mobile (GSM) Mobile device attached to the computer through a communication Port.

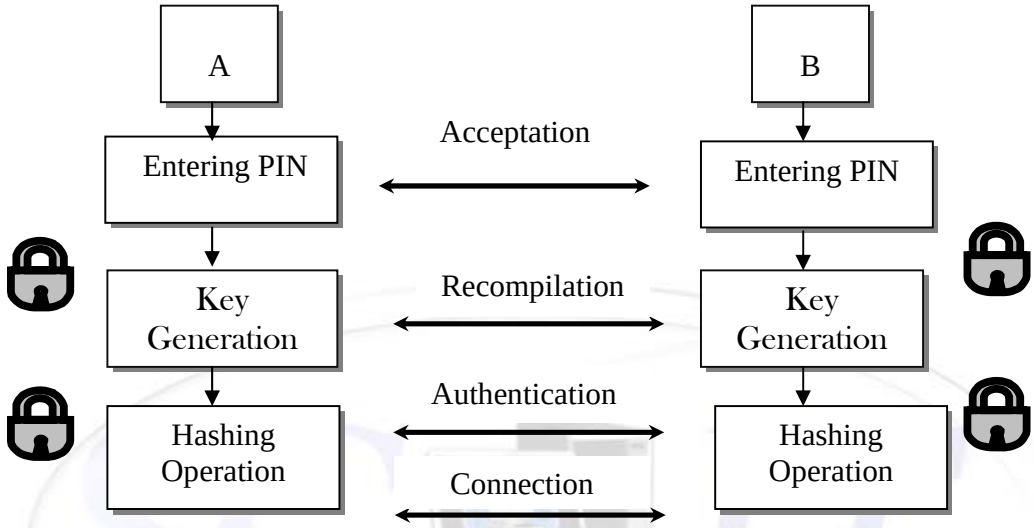

Figure 4: The Authentication & Hashing operation

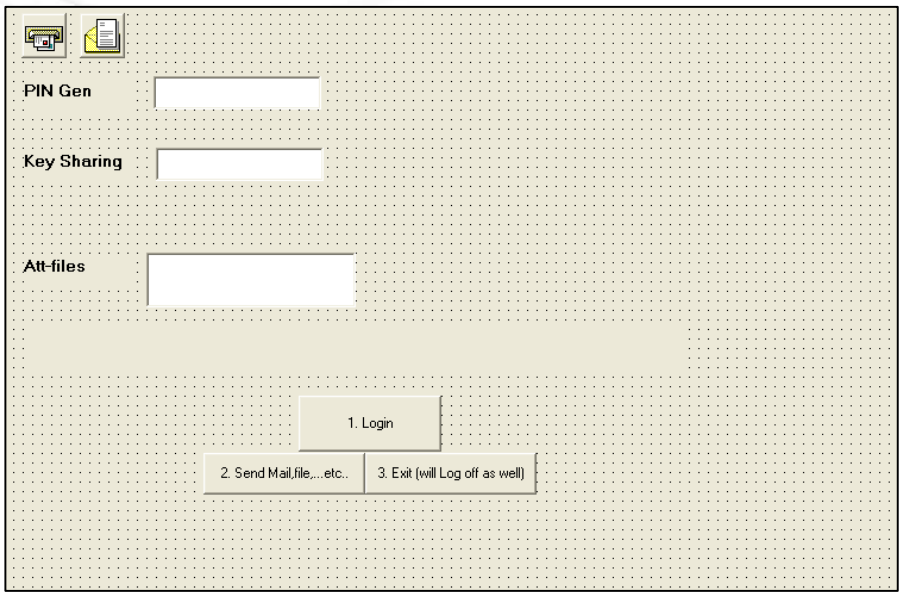

Figure 5: The Development Integrated Environment of the system

6. Conclusion

Although the hashing operation may be a simple operation for the encryption or for authentication but provide protection for user against the hacker, intruder, and etc. for many reasons. it is appends to the connection a value called the Hash Authentication Tag (HAT), computed by the hash algorithm, or operation as a function of the transmitted information and generate another shared secret key. This value it compresses a string of arbitrary length to a string of fixed length. In this paper a string is summary from Xoring operation with systemic key to success the first pairing between devices. It can use for one way encryption to add more complexity against the hacking tool.

7. References

1. Bluetooth SIG, Specification of the Bluetooth system, Core, Part B, "Bluetooth™ Security White Paper", Version 1.1, 19 April 2002.
2. David Kammer, Bluetooth Application Developer's Guide: The Short Range Interconnect Solution" , Copyright © 2002 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America.
3. Donghoon Chang, Kishan Chand Gupta, and Mridul Nandi,"RC4-Hash: A New Hash Function based on RC4", Korea University, Korea, University of Waterloo, 2002, Canada.
4. Keijo M.J.Haataja, "Security in Bluetooth, WLAN and IrDA: a comparison", university of Kuopio, Dept. of computer science, Finland, 2006.
5. Markus Jakobsson and Susanne Wetzal, "Security Weaknesses in Bluetooth", lucent technologies, bell labs information sciences research center, Murray Hill, 2004, USA.
6. Markus Swenson & Tanawat Tatiyavoranat, "Bluetooth 15C", 2G1704, internet security and privacy KTH, 24-11-2005.
7. Mihir Bellare, Ran Canetti, Hugo Krawczyk,"Keying Hash Functions for Message Authentication", Department of Computer Science & Engineering, Mail Code 0114, University of California at San Diego, 9500. Email & website: mihir@cs.ucsd.edu. http://www-cse.ucsd.edu/users/mihir.
8. Thomas G. Xydis Ph.D.,"Security Comparison: Bluetooth TM Communications vs. 802.11", Simon Blake-Wilson, Bluetooth Security Experts Group, 2001.
9. Yaniv Shaked and Avishai Wool, "Cracking the Bluetooth PIN", supported in part by a grant from Intel corporation , school of electrical engineering systems, the website http://www.eng.tau.ac.il, 2008.