International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 4 Issue 10, October -2015

An Approach to Enhance the Security Lapses in Bluetooth Wireless Network Communication

Payel Majumder[1], Suparbhat Mondal[2], Bijoy Kumar Mandal[3]

[1,2,3]Computer Science & Engineering, NSHM Knowledge Campus, Durgapur, India

ABSTRACT

This work proposes an approach to enhance the security lapses that are present in data exchange process of Bluetooth. The paper begins with analyzing both the advantages and risks of mobile devices and wireless networks that can be brought to today's businesses. The paper continues the analysis who in an organization should take on the responsibility to mitigate the risks related to mobile devices and wireless networks. Bluetooth technology is widely used for transmission of data over short range distances. E0 algorithm is being currently used for data transfer. E0 stream cipher algorithm has many shortcomings and can be easily broken down. AES algorithm is highly secure with very few published attacks against it. Also the difficulty of factoring large integers ensures the security of RSA algorithm. We propose a hybrid algorithm taking the benefits of RSA algorithm and AES algorithm that is an efficient way to eliminate the security lapses.

Keywords: AES, E0, Client-Server Model, PDA.

I. INTRODUCTION

Bluetooth, a new technology named after the 10th century Danish king Harald Bluetooth, is a recently proposed standard for local wireless communication and is becoming hotter and hotter a topic. A wireless sensor network consists of sensor nodes deployed over a geographical area for monitoring physical phenomena like temperature, humidity, vibrations, seismic events, and so on[1]. Bluetooth is the new emerging technology for wireless communication. It was developed by a group called Bluetooth Special Interest Group (SIG), formed in May 1998. The founding members were Ericsson, Nokia, Intel, IBM and Toshiba. Since then, almost all of the biggest companies in the telecommunications business (e.g. 3Com, Microsoft, Motorola) have joined the Bluetooth SIG and the number of the participating companies is now over 1,500. The version 1.0 of the Bluetooth speciation was approved in the summer of 1999, and the latest version (at the time of writing) 1.0B in December 1999. . Bluetooth can be used to connect almost any device to another device. The traditional example is to link a Personal Digital Assistant (PDA) or a laptop to a mobile phone. That way you can easily take remote connections with your PDA or laptop without getting your mobile phone from your pocket or messing around with cables. Bluetooth can also be used to form ad hoc networks of several (up to eight) devices, called piconets. This can be useful for example in a meeting, where all participants have their own Bluetooth compatible laptops, and want to share files with each other.

To minimize complexity and to reduce the cost of the transceiver, a simple binary Gaussian frequency shift keying modulation is adopted. In order to allow efficient wideband data transmission the bit rate is 1 Mbps. Two or more Bluetooth units sharing the same channel form a piconet. Within a piconet a Bluetooth unit can be either master or slave. Within each piconet there may be only one master and up to seven active slaves. Any Bluetooth unit can become a master in a piconet. Furthermore, two or more piconets can be interconnected, forming what is called a Scatternet. The connection point between two piconets consists of a Bluetooth unit that is a member of both piconets. A Bluetooth unit can simultaneously be a slave member of multiple piconets, but a master in only one, and can only transmit and receive data in one piconet at a time, so participation in multiple piconets has to be on a time division multiplex basis [2] and also, communication bandwidth is extremely dear: each bit transmitted consumes about as much power as executing 800– 1000 instructions, and as a consequence, any message expansion caused by security mechanisms comes at significant cost [3]. How can security possibly be provided under such tight constraints? But security is critical. With sensor networks being envisioned for use in critical applications such as building monitoring, burglar alarms, and emergency response, with the attendant lack of physical security for hundreds of exposed devices, and with the use of wireless links for communications, these networks are at risk[4].

II. BLUETOOTH SECURITY

Security for Bluetooth is provided on the various wireless links, in other words, link authentication and encryption may be provided, but true end-to-end security is not possible without providing higher layer security solutions on top of Bluetooth. Briefly, the three basic security services defined by the Bluetooth specifications are the following:

- Authentication: A goal of Bluetooth is the identity verification of communicating devices. This service provides an abort mechanism if a device cannot authenticate properly.
- Confidentiality: Confidentiality, or privacy, is another security goal of Bluetooth. The intent is to prevent information compromise caused by eavesdropping (passive attack).
- Authorization: A third goal of Bluetooth is a security service developed to allow the control of resources. This service addresses the question "Has this device been authorized to use this service?"

Bluetooth has three different modes of security. Each Bluetooth device can operate in one mode only at aparticular time. The three modes are the following:

- Security Mode 1: Non-secure mode
- Security Mode 2: Service-level enforced security mode
- Security Mode 3: Link-level enforced security mode

III. ATTACKS

- System assumptions: We assume that radio links are insecure, i.e., attackers may eavesdrop on radio transmissions, inject messages, and record and later replay messages. If an attacker is able to interact with the routing protocol, it can also drop messages for which it is responsible. Attackers possess hardware capabilities similar to that of legitimate nodes, and wireless transmissions use the same power levels. Network nodes move only infrequently or slowly once deployed, and know their own locations. They may additionally know that of their neighbors. This may be fulfilled by many different key distribution schemes in the literature [5]. Nodes trust their own clocks, measurements, and storage.

- Routing attacks: Karlof and Wagner [6] have systematically studied attacks on routing protocols. We summarize these attacks below, noting whether they are applicable. Then we discuss those attacks which are not obviously thwarted in greater detail. In an insider attack, a compromised node uses any means available to legitimate nodes to disrupt the protocol or perform a specific attack listed above.

IV. PREVIOUS WORK

At present the E0 stream cipher is being used for encryption of data in Bluetooth Technology as shown in Figure 1. However, 128-bit E0 stream cipher has a few weaknesses. The Bluetooth encryption system uses the stream cipher E0 to encrypt the payloads of the packets which is re-synchronized for every payload. The E0 stream cipher consists of the payload key generator, the key stream genera-tor and the encryption/decryption part. The input bits are combined by the payload key generator and are shifted to the four Linear Feedback Shift Registers (LSFR) of the key stream generator. The key stream bits are then generated which are used for encryption. The Exclusive-OR operation is then performed on the key stream bits and data stream bits to generate the ciphertext. Similarly the Exclusive-OR operation is performed on the ciphertext to get back the plaintext during the decryption process.

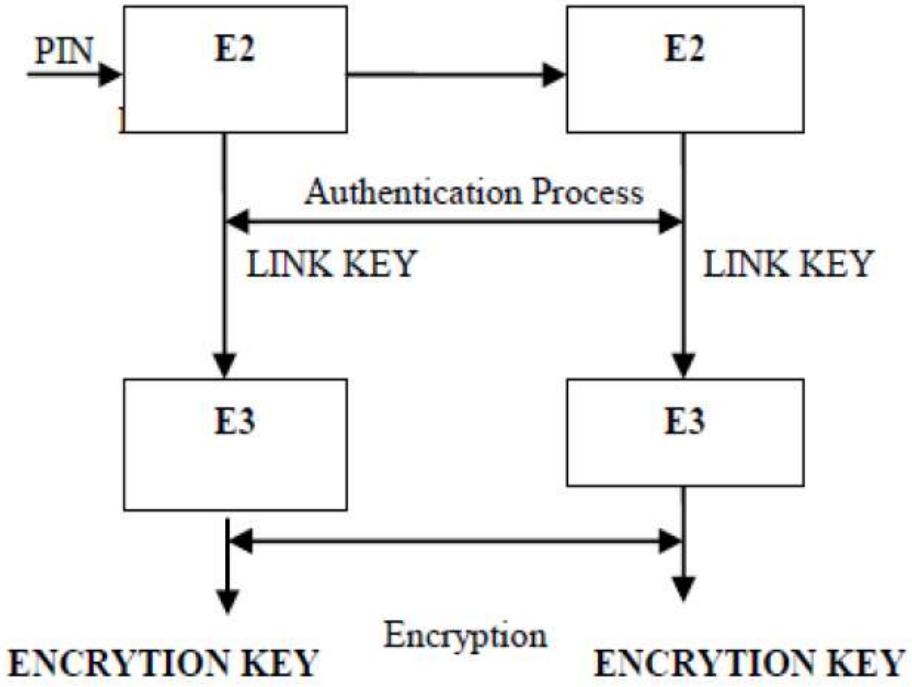

Figure 1: Bluetooth Encryption Process

- Low reliability of PIN: The PIN is the only secret used for the key generation that is not transferred by wireless communication. For many applications, the PIN will be a relatively short string of numbers. Typically, it may consist of only four decimal digits. If the PIN is small then an exhaustive search can derive the initialization of security keys. Therefore, the credibility of the PIN code is lower; 4 bits PIN code only has 10,000 possibilities. This problem can be overcome by using a longer PIN as it becomes difficult for the attacker but at the same time it becomes inconvenient for the user to enter the PIN every time when the connection is established.
- Random Number Generator: Random Number Generator (RNG) may produce static or periodic numbers that may reduce the effectiveness of the authentication scheme. Thus the strength of the pseudo random generator may not be known. If the random number comes out to be a sequence of zeros then the cipher text will be the same as the plaintext and the whole process would be worthless.
- Address Spoofing: Addresses are not validated, so the addresses can be spoofed which is similar to IP address spoofing. If the unique blue-tooth address assigned to each device is known, the user can be tracked. Address spoofing also enables the tracker to monitor the activities of the user if his Bluetooth address is known thus hampering the user's privacy.
- Limited Resource Capacity of LFSR: LFSR (Linear Feedback Shift Register) is used to generate the pseudo random numbers in E0 algorithm. Four LF-SRs are used in E0 stream cipher. If the generated cycle by LFSR is shorter than the key then there can be a threat from the attacker using divide and conquer attack. The probability of the attack however is very low since the divide and conquer technique requires access to the key stream extending over periods of partial input. This, however, has been taken into account in the Bluetooth specifications. The above mentioned divide-and-conquer attack needs access to the key stream extending over periods of partial input. Since the resynchronization frequency of Bluetooth is very high, such an attack is impossible.

V. PROPOSED HYBRID ALGORITHM

RSA algorithm is asymmetric public key cryptography. Data sent using RSA is hard to break without using the private key. But we cannot send a large file using RSA algorithm. So we are using RSA algorithm to send a key (AES) to the receiver. AES algorithm is symmetric in nature and is one of the best ways to send large amount of data as it is very fast. Taking into account the advantages of both AES and RSA and avoiding their shortcomings, hybrid encryption algorithm based on AES and RSA has been proposed.

- Assumptions Made

    a. Device A is sender and device B is receiver.

b. A connection is made between the two interacting device.
c. Both devices are unaware of each other's public keys.

- **Algorithm**

a. Device A sends a "send Data?" request to device B.
b. Device B rejects it by terminating the connection or accepts it by sending its public key.
c. Device A generates an AES key, encrypts it using the public key received (public key of device B) and sends it to device B.
d. Device A encodes the file selected to be sent using the AES key and sends it to device B.
e. Device B decrypts the encrypted data received using the AES key received previously, saves the file and terminates the connection.

CONCLUSION

Bluetooth technology is widely used for transmission of data over short range distances. Bluetooth being a wireless technology is more susceptible to attacks as compared to other fixed networks. So it is important to consider the security of data during transmission. E0 stream cipher algorithm which is currently used in Bluetooth for encryption has many shortcomings and can be easily broken down. AES algorithm is highly secure with very few published attacks against it. Also the difficulty of factoring large integers ensures the security of RSA algorithm. Thus the proposed Hybrid Encryption Algorithm using AES and RSA provides a more secure and convenient technique for secure data trans-mission among Bluetooth devices as compared to the E0 algorithm.

REFERENCE

[1]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: a Survey", Computer Networks, Volume 38, N. 4, March 2002.
[2]. Bluetooth SIG, Specification of the Bluetooth System: Core, Version 1.1, vol. 1, February 22. 2001
[3]. IEEE 802.15 Working Group for WPANs, http://ieee802.org/15/.
[4]. B K Mandal, D Bhattacharyya and Tai-hoon Kim, "A Design Approach for Wireless Communication Security in Bluetooth Network" International Journal of Security and Its Applications, Vol.8, No.2, pp.341-352, 2014.
[5]. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A secure routing protocol for ad hoc networks, In Proceedings of the IEEE International Conference on Network Protocols(ICNP), 2002.
[6]. C. Karlof and D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, In First IEEE International Workshop on Sensor Network Protocols and Applications 2003
[7]. C. Candolin, "Security Issues for Wearable Computing and Bluetooth Technology", Online report, http://www.cs.hut.fi/Opinnot/Tik- 86.174/btwearable.pdf
[8]. J. Dunning, "Taming the Blue Beast: A Survey of Bluetooth Based Threats", IEEE Security & Privacy, vol. 8, no. 2,pp. 20-27, 2010