International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

A survey paper on Bluetooth over mobile phones

B. Karuna Sree , A. Mallikarjuna Reddy , Dr G. Vishnu Murthy
[1]MTech 2nd Year, Dept. of CSE, CVSR College, Hyderabad, Telangana, India
[2,3]Assistant Professor, Dept. of CSE, CVSR College, Hyderabad, Telangana, India

Abstract

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile device and building personal area networks (PANs). The data easily transfer from sender to receiver this leads to attack. To provide security for the mobile phones steganography is used .In this paper we discuss about security issues in Bluetooth over mobile phones.

1. Introduction

Bluetooth is wireless connectivity. In other words, it is a way of connecting mobile phones to other mobiles phones and devices without wires. Using radio waves similar to a remote control toy, Bluetooth has a range of up to 50 meters depending on the particular Bluetooth device and the prevailing conditions [1].

Bluetooth is an industrial standard for wireless specification for wireless Personal Area Network (PAN). In recent years, Bluetooth technology has become a standard in mobile devices such as mobile phones and personal digital assistant (PDA) for short range communication. The Bluetooth standard defines the following requirements [2]:

- The system must operate globally, and the required frequency
- Band must be license-free and open to any radio system.
- The system must provide peer connections.
- The connection must support both voice and data.
- The radio transceiver must be small and operate at low power.

Bluetooth-enabled devices can dynamically discover other devices in their range and their supported services, through an inquiry process.

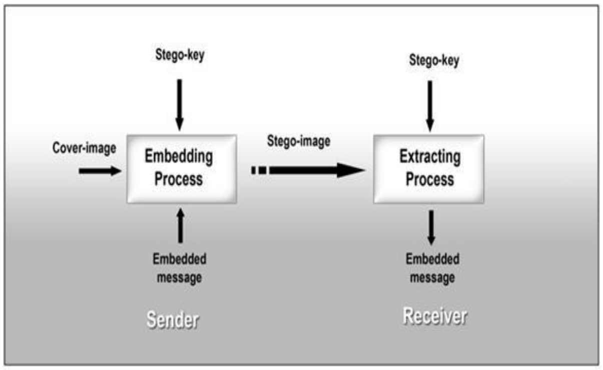
2. Steganography:

After expanding use of mobile phones, establishing hidden communication it an important subject of security that has gained increasing importance. One of the methods for establishing hidden communication is Steganography. Steganography is a powerful security tool that provides a high level of security, it is used for the hidden exchange of information.

Baker S. and Nori A. [3] discuss the Steganography in mobile phones over a Bluetooth implemented on J2ME (Java 2 Micro Edition) platform and has been implemented on Nokia mobile phones. Steganography is the practice in which secret messages are hidden inside a different digital content, such as image, data file, or audio, which is called the cover object. The process of concealing this secret message into the cover image is carried out before the transmission process and the embedded secret message is extracted by the receiver [3-7].The basic concept of steganography is to ensure that secret messages are securely transmitted without any doubts. It differs from cryptography, because in cryptography, the secret message is encrypted, making it unreadable, but steganography ensures that the secret message is hidden completely. Figure 1 illustrates the basic concept of steganography, which consists of two basic processes:

1) Embedding process: It is carried out by the sender. During the embedding process, there is a secret message, which the sender intends to transmit securely. There is also a cover image into which the secret message will be embedded and there is also a stego key, which enables that only the receiver who has the corresponding decoding key can extract the secret message.

2) Extraction process: It is carried out by the receiver. The image generated after the embedding process, called stego image, carries out the secret message



Basic architecture of steganography

Steganography can be implemented using numerous techniques. Some common techniques include transform domain technique and the spatial domain technique. In transform domain technique, the secret message is embedded into the coefficients of the image transform used, while in spatial domain technique, the least significant bits (LSBs) of the cover image is replaced by that of the secret bits [3-7].

3. Least significant bit(LSB)

Rahul Joshi, Lokesh Gagnani in [8], they discussed Least Significant Bit (LSB) method. Using this method the secret message bits are directly replaced with the LSBs of the cover image. To embed one bit from secret image or text by using the stego bit and apply the XOR operation between them and the result put in the Least Significant bit of the cover image. The image is called stego-image which sent over Bluetooth of mobile.

$$\text{LSB} = \text{Stego bit} \oplus \text{Secret bit}$$

When we want to decode the secret image or text by inverting the operation according to the equation:

$$\text{Secret bit} = \text{Stego bit} \oplus \text{LSB}$$

The two sides (sender and receiver) must be agreed together for using the same secret key. The problem least significant bit (LSB) approach simply does not pick up least significant bits of pixel in a sequence but is combined with midpoint circle approach to choose which pixels are used to hide message.

Mohammad Shirali Shahreza[9], he presented method, instead of sending of information directly , information is hidden in a picture with password over a site. Then the address of the picture is sent to the user. After receiving the address of the picture through SMS, the user downloads the picture by a special program. After entering the password, the user can witness the information extracted from the picture if the password is entered correctly. Shiladitya Pujari & Sripati Mukhopadhyay [10], they presented a new scheme of image based Steganography where the secret message is divided or segmented into random number of units holding equal number of characters and the cover image is logically divided into a random number of squire blocks. Each logical block of image is used to hide each unit of message in a pseudo-random fashion. Ge Huayong & Huang Mingsheng [11], they have explain concept and principle of Steganography and steganalysis, spatial domain and transform domain embedding method are generalized. Then the performance specification of image Steganography is discussed. Marwan ali albahar & Olayemi [12], they presented two solutions in data security field for ensuring that only legitimate recipients will have access to the intended data: Steganography and cryptography. These solutions can be used for providing a high level of security. With the exponential growth of challenges in the field of computer security, the use of Bluetooth technology is expanding rapidly to expose many of these challenges on the surface. One of these challenges is the MITM attack during Bluetooth pairing process.

4. Conclusion

In this paper we have discussed about Bluetooth security issues in mobile phones and discussed different algorithms that are used to keep mobile phone secure during communication of messages from sender to receiver. Steganography is a powerful security tool that provides a high level of security, it is used for the hidden exchange of information.

5. References

1. U.Sarwar, S.Ramadass, and R. Budiarto,” A framework for detecting Bluetooth mobile worms”, International Conference on Telecommunications and Malaysia International Conference on Communications, IEEE, pp 343-347, 2007.

2. G. Sarswat and J. Noida. “Bluetooth Hacking”, http://cnss.wordpress.com /2007/09/11/bluetooth-hacking1, 2007.

3. Baker S. and Nori A., Steganography in Mobile Phone over Bluetooth, International Journal of Information Technology and Business Management (JITBM), 1(vol.16), 2013, pp.111–117.

4. Sekhar A., Kumar M., and Rahiman M., A Novel Approach for Hiding Data in Videos Using Network Steganography Methods, Procedia Computer Science, (vol.70), 2015, pp. 764–768.

5. Artz D., Digital Steganography: Hiding Data Within Data, IEEE Internet Computing, 3 (vol.5), 2001, pp.75–80.

6. Joseph A. and Sundaram V., Cryptography and Steganography: A Survey, International Journal of Computer Technology and Applications (IJCTA), 3 (vol.2), 2001, pp. 626–630.

7. Saraireh S., A Secure Data Communication System Using Cryptography and Steganography, International Journal of Computer Networks & Communications, 3 (vol.5), 2013.

8. J.Rahul, G.Lokesh and P.Salony , "Image Steganography With LSB", International Journal of Advanced Research in Computer Engineering & Technology ,Volume 2, Issue 1, January 2013.

9. S. S Mohammad., "Improving Mobile Banking Security Using Steganography", ITNG 07, Fourth International Conference on 2-4 April 2007.

10. P.Shiladitya, M.Sripati, "An Image based Steganography Scheme Implying Pseudo-Random Mapping of Text Segments to Logical Region of Cover Image. using a New Block Mapping Function and Randomization Technique" , International Journal of Computer Applications , Volume 50 – No.2, July 2012.

11. H.Ge, Huang , "Steganography and Steganalysis Based on Digital Image", International Conference & Signal Processing, IEEE, 2011.

12. Marwan Ali Albahar, Olayemi, Pekka Toivanen ,"A Novel method for Bluetooth pairing using Steganography" International Journal on Information Technologies & Security, № 1 (vol. 9), 2017