Journal of The Gujarat Research Society

ISSN: 0374-8588
Volume 21 Issue 8, August 2019

A REVIEW OF BLUETOOTH NETWORK

Asha K S
Faculty of Engineering and Technology,
Jain (Deemed-to-be University), Ramnagar District, Karnataka – 562112
Email Id: ks.asha@jainuniversity.ac.in

Abstract

By offering short-distance wireless connectivity between two or more users with less power consumption and low cost, the Bluetooth network is an important aspect of communication. In Bluetooth technology, the mainstream Bluetooth 2.4 GHz is used. Because of certain vulnerability problems in Bluetooth networks, a malicious group receives unauthorized access and carries out internal attacks. Without any detection, the data is collected. Virus corrupts the files and modifies them. The security attacks create issues in privacy of a customer. Personal data can be hacked. Network protection is incorporated in Bluetooth to solve this challenge. Good security architecture is important for network security to be effective. This paper focuses on various security attacks and how to deal with them on a Bluetooth network. To solve these serious problems, various solutions as well as safety tips are given. Because of the vulnerability problem on the Bluetooth network, users would be aware of the attacks. As sensitive information should be protected, consumer privacy will be maintained.

Keywords: *Bluetooth, Man-In-The-Middle attacks, Denial of Services, Industrial scientific and medical.*

I. INTRODUCTION

A medium of contact embraced by the dominant and prominent communications and computer producers of the world. It allows devices to connect to each other, from phones and PCs to camcorders. In early 1994, in a high-spirited college town named Lund, Sweden, a team of researchers headed by Sven Mattisson and Jaap Haartsen explored the feasibility of establishing a wireless link between an ear-piece and a smartphone [1]. It came with the expectation that the promise of such a device was much greater than the cordless headset as science evolves further. Ericsson wanted to explore this technology further, and so the Bluetooth idea was born.

Basically, Bluetooth operates by detecting other nearby Bluetooth devices and then, if necessary, linking to them. It achieves this by building a piconet, where communications with up to seven others are managed by one computer. There are several piconets attached to create a scatternet. The technology resides in the unlicensed commercial, science and medical (ISM) band at 2.4 to 2.485 GHz, using an integrated spectrum, frequency hopping, full-duplex signal at a basic rate of 1600 hops/sec, as stated by the Bluetooth website [2]. The headset knows how to select a phone call. Bluetooth chips create wavelengths that for this form of short-range communication are limited to frequencies working within a range clearly set aside. Cordless telephones and displays have some gadgets that use this frequency. However, there is an issue of only keeping the same frequency. Other instruments running at or closest to the same frequency will induce signal interruptions [3]. The signal is spread over a broader spectrum of frequencies to prevent this from being a concern. The pulse bounces around the spectrum to accommodate this, and in the case of Bluetooth, it drops in at 1600 times a second [4]. The periodic variation in wavelength ensures that for more than 1/1600th of a second, even a clear signal will not disrupt and will not be interrupted. In two different types, using a full or part duplex link, Bluetooth headsets may be described.

A. **Suggestions for Well-organized Bluetooth usage: -**

1. Bluetooth users must be aware of the problems involved with encryption.
2. Threat evaluation must be conducted at a periodic time interval.
3. Manuals on the precautionary steps to be taken when using the Bluetooth network should be given to consumers.
4. The PIN must be long, and static PINs such as all or all zeroes must also be stopped at random.
5. The antivirus must be mounted on the Bluetooth-enabled host computer, since the ransom ware is also targeted.
6. If any Bluetooth activated computer is stolen, the device's link is automatically cut off as data could be stolen.

II. LITERATURE SURVEY

Study paper 'Assessing Bluetooth Low Energy in Practical Wireless Settings' by Mohamad Omar Al Kalaa et.al. presents Bluetooth Low Energy Applications (BLE). This paper identifies the wireless contact risk that has emerged and adversely affects the functionality of BLE systems. To figure out the risk of transmitting loss, it includes the technique for using spectrum. The paper's findings illustrate how data transmission channels in a BLE system are chosen when interference is present [5]. This paper also shows that when operated in a high interference environment, the likelihood of failed transmission is much smaller. Research paper 'Bluetooth Technology Threats and Solutions: A Review' by Nateq Be-Nazir Ibn Minar et.al. The security threats in the Bluetooth technology are presented along with numerous security

threats from the past. It also gives countermeasures to the security protocol's vulnerabilities [6]. When using the Bluetooth network, it provides the user with instructions so that they are aware of the security risks and be more vigilant of their details [7]. This paper also supplies the Bluetooth network with potential security enhancements.

Study paper "Security vulnerabilities in Bluetooth technology as used in IoT" by Angela M. Lonzetta et.al. introduces the fundamentals of IoT Bluetooth technology. It addresses security challenges, risks, weaknesses and offers options for risk reduction. In this article, real life examples are also given. Research paper by Boldizsar Bencsath et al. Security against DDoS Attacks Based on Traffic Level Measurements in Bluetooth networks, DoS attacks are present, in which the attacker destroys the system and interrupts it from receiving any data or files. Dennis Kugler's research paper "Man in the Middle Attacks on Bluetooth" discusses the MIM attacks present in the Bluetooth network [8]. It slows the interaction of data between the computers [9]. Ollie Whitehouse's research paper "War Nibbling: Bluetooth Insecurity" discusses the war nibbling attacks present in the Bluetooth network. This paper discusses Bluetooth system security evaluation approaches in regards to protocol architecture and implementation shortcomings. A Study on the Bluetooth Contact Protection Mechanism" research paper by Trishna Panse et.al." introduces the different security modes. The protection measures being used in the Bluetooth network are explained in this article [10]. A research paper by Jae-shin Lee et.al. "Bluetooth device and method for providing service determined according to Bluetooth PIN" In Bluetooth technology, the main generation is presented. The method for delivering a service decided according to Bluetooth PIN is given in this article.

B. **Various versions of the Bluetooth: -**

The following table illustrates the various versions and its specifications of the Bluetooth technology.

Bluetooth Versions	Specification
Bluetooth v1.0 to v1.08	Mandatory Bluetooth hardware device and address
Bluetooth v1.1	IEEE standard 802.15.1-2002
Bluetooth v1.2	Faster connection
Bluetooth v2.0+EDR	Enhanced data rate
Bluetooth v2.1	Secure simple pairing
Bluetooth v3.0	High-speed data transfer
Bluetooth v4.0	Low energy consumption recently used in apple I – phone 4s

III. DISCUSSION

There are different bugs on Bluetooth networks. Through following the precautionary principle when using the Bluetooth network, all threats and attacks are mitigated. During the pairing process, the system is switched off while the device remembers one another for the first time after pairing, until it is unpaired. The different Bluetooth attacks that exist in the Bluetooth network are reduced to the optimal amount. The possibility that personal data files may be destroyed is therefore reduced. Before forming a link between the two machines, the strong long and random PIN is created such that it hits the destination target elsewhere than anywhere else. Before submitting the data to the destination, the data is encrypted such that even though the data is intercepted, the thief does not recognize it and data is translated back to the original format at the receiving end.

IV. CONCLUSION

The numerous Bluetooth attacks that Bluetooth networks have experienced over the years are discussed in this article. In depth, the solution to these problems is clarified. Any precautionary principles are provided so that the user is conscious and more vigilant about their personal data and files when connecting with each other on Bluetooth networks. A majority of smartphones today use Bluetooth technology, but if the security threat is ignored, the danger will escalate to a larger degree. Security protocols should be subject to daily upgrades. Protection of consumer data must be prioritized. Because of the vulnerabilities, all the emerging devices have Bluetooth features, so the security threat increases. Technology is really critical, and to deal with these security challenges, it must develop.

V. REFERENCES

[1] I. J. Dilworth, “Bluetooth,” in *The Cable and Telecommunications Professionals’ Reference: PSTN, IP and Cellular Networks, and Mathematical Techniques*, 2012.

[2] N. Sriskanthan, F. Tan, and A. Karande, “Bluetooth based home automation system,” *Microprocess. Microsyst.*, 2002, doi: 10.1016/S0141-9331(02)00039-X.

[3] D. A. Diartono, “Teknologi Bluetooth untuk Layananan Internet padaWireless Local Area Network,” *Din. - J. Teknol. Inf.*, 2009.

[4] P. Singh, D. Sharma, and S. Agrawal RIT, “A Modern Study of Bluetooth Wireless Technology,” *Int. J. Comput. Sci. Eng. Inf. Technol.*, 2011, doi: 10.5121/ijcseit.2011.1306.

[5] C. Gehrmann, “Bluetooth Security,” in *Network Security: Current Status and Future Directions*, 2007.

[6] Y. Peng, Q. Du, L. Hua, and Y. Shao, “Cognitive FH Channel Selection for Bluetooth Network,” *TELKOMNIKA Indones. J. Electr. Eng.*, 2013, doi: 10.11591/telkomnika.v11i3.2317.

[7] R. Faragher and R. Harle, “Location fingerprinting with bluetooth low energy beacons,” *IEEE J. Sel. Areas Commun.*, 2015, doi: 10.1109/JSAC.2015.2430281.

[8] R. A. Rashid and R. Yusoff, "Bluetooth performance analysis in personal area network (PAN)," in *2006 International RF and Microwave Conference, (RFM) Proceedings*, 2006, doi: 10.1109/RFM.2006.331112.

[9] J. Nieminen *et al.*, "Networking solutions for connecting bluetooth low energy enabled machines to the internet of things," *IEEE Netw.*, 2014, doi: 10.1109/MNET.2014.6963809.

[10] E. Ferro and F. Potortì, "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," *IEEE Wireless Communications*. 2005, doi: 10.1109/MWC.2005.1404569.

ISSN: 0374-8588
Volume 21 Issue 8, August 2019