IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

Review on Security in Bluetooth Low Energy Mesh Network in Correlation with Wireless Mesh Network Security

Anusha G and Ravikiran R
Department of ECE
S J C Institute of Technology, Chickballapur, Karnataka, India

Abstract: *In current high-tech era, Wireless Mesh Networks (WMN) are a necessity since they offer inexpensive access to broadband services. The technologists are also conducting research to improve the security and dependability of WMN. Due to its widespread availability in devices and low power consumption, Bluetooth Low Energy (BLE) is thus gaining significant importance among academics in the field of wireless ad hoc networking. BLE began with version 4.0 and recently released version 5 with mesh support capabilities. BLE, a low power, mesh enabled technology, is currently one of the hottest study issues for academics. Many scientists are developing BLE mesh technology to make it smarter and more effective. In addition to other efficiency factors, mesh network security is a major problem, as it is for all communication networks. In light of the aforementioned, this study offers a thorough analysis of a number of works pertaining to the security in WMN and BLE mesh networks as well as the research on the BLE security protocols. Additionally, this study has covered the advantages and disadvantages of the already proposed mesh security techniques after conducting extensive research on relevant studies. Additionally, this investigation has evolved some remedies as to how to minimize the BLE mesh network security flaws after extracting the pertinent information from the current research on WMN and BLE mesh security.*

Keywords: Bluetooth Low Energy, Security, Wireless.

I. INTRODUCTION

The development of wireless technology is quick. Most researchers in this field are aiming to increase its effectiveness, dependability, and security. Apart from efficiency, users these days are more concerned about communication's dependability, security, and privacy. Speaking about dependability, mesh topology support for any wireless technology is getting more and more popular because it is a reliable network structure. Additionally, Figure 1 depicts the whole mesh network architecture. Due to their lack of infrastructure requirements and minimal power requirements for connectivity, Additionally, Wireless Ad-Hoc Networks (WAHN) growing in popularity. These networks can be supported by a variety of technologies, including Bluetooth, Thread, ZigBee/XBee, etc. Among all other technologies, the BLE is currently capturing the market because to its simplicity.[1]

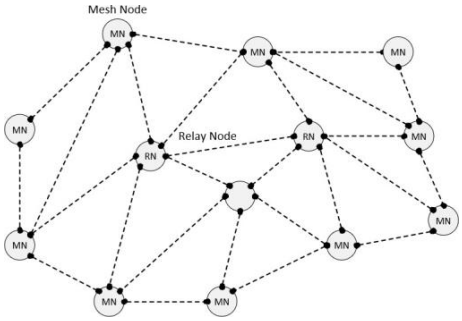

Figure 1: General Mesh Network Architecture

Availability in different products and low power consumption feature. The BLE technology also got greater notoriety after the release of version 5 because of its mesh support feature, which has increased the coverage area. Mesh topology is advantageous from a security perspective as well because there won't be a single point of failure. Mesh networks can also be attacked by internal or external attackers (hackers), in addition to the aforementioned. By deleting or altering the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

equipment's chip, physical (physical layer) attacks on the hardware are possible but extremely rare. Attacks may target any network layer, including MAC, Network, Transport, or Application. The classification of security attacks on wireless and BLE mesh networks. In the past, several researchers have worked to reduce security attacks. However, the mesh networks continue to struggle with security. In light of the foregoing, the purpose of this study is to outline the steps to improve security in the BLE mesh network following a thorough literature assessment of the most recent BLE and wireless mesh network research.

The remainder of the study is organized so that Section 2 discusses security in WMN and Section 3 reviews security in BLE mesh networks, including an analysis of security protocols created by researchers. Section 4 will then wrap up the paper after that.

Wireless Mesh Network (WMN) Security

For WMNs encounter the same security issues as wired networks. The message can be changed, added, replayed, interrupted, etc. during communication. Due to its multi-hop structure, WMN is susceptible to threats just like any other networks. Furthermore, security is needed for WMNs not only between clients, but also among mesh routers and between clients and mesh routers. Therefore, as WMNs use a variety of wireless technologies, internetwork security is also necessary. Additionally, WMNs encounter a number of restrictions when utilizing mobile nodes like PDAs, mobile phones, etc. In addition to these limitations, WMNs also raise a number of security-related issues, such as availability, authenticity, integrity, confidentiality, access control, authorization, fairness, etc. In light of the foregoing, the next sections will go over the main security risks to WMNs and the work being done to mitigate those risks.[2]

WMN Security Threats

The OSI Model divides data transport and communication processes into various sections, referred to as layers, to follow the proper order of execution. As an illustration, the data link layer handles switching whereas the physical layer deals with physical issues like wiring, connectors, etc. There are seven OSI in total. layers, each of which is in charge of carrying out a specific task. Whether a communication is wireless or cable, these layers are crucial. Whether a communication is wireless or cable, these layers are crucial. Additionally, layers play a large part in WMN communication. Furthermore, when discussing security, several dangers are present at each tier.[3]

1. Attacks on the Physical Layer: There are many attacks that can harm WMNs' physical layer. The equipment utilized may be mounted outside, outside of the facilities, etc. to facilitate long-distance and effective communication. In that situation, the attacker may physically harm the hardware, tamper with it, or steal some crucial data. Additionally, the intruder can interfere with network transmission by using radio jammers. The most frequent jamming attacks include trivial, periodic, and reactive ones.
2. Data connection Layer Attacks: The data connection layer is one of the most crucial levels from a security perspective. Media access control (MAC) and logical link control (LLC) are the two sublayers that make up this layer. The MAC layer of WMNs is also vulnerable to many attacks, including passive listening, jamming, flooding, and MAC spoofing.
3. Attacks at the Network Layer: WMN's network layer is also susceptible to various attacks on the data flow and routing, including respectively, the control plane (CP) and the data plane (DP). The following CP attacks may reduce routing capacity: rushing, routing table overflow, sybil, byzantine, wormhole, sinkhole, greyhole, sleep deprivation, local disclosure, and route error injection attacks. The network may contain a selfish or malevolent node that uses DP assaults to enhance its own performance at the expense of others.
4. Attacks on the transport layer: The transport layer is a crucial component of any communication network. Its primary job is to receive data packets from higher layers, break them up into smaller units, and transmit them on to the network layer.

   Among the most common attacks on the transport layer are flooding and desynchronization. Flooding occurs when an attacker makes connection requests over and over until all resources have been used. In order to stop successful data exchange, the rogue node will send fake messages to the end host continuously during desynchronization attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

5. Attacks on the application layer: The application layer, the top OSI layer, is in charge of facilitating effective communication between different application programmers. Application-level security is a requirement in communication to protect applications. Attacks on this layer may take the shape of worms, viruses, and other threats. In the event of an unencrypted data transfer, data sniffing is also possible during message transmission.[4]

The Future of BLE Mesh Protocols Research

The open research questions about BLE Mesh protocol enhancement and scalability were brought to light by the coverage of contemporary BLE Mesh protocols. The robustness of BLE Mesh networks against node failure and mobility is constrained because the majority of BLE Mesh topologies are created for scatternet topologies employing connection-oriented communications. Given that most suggested approaches only use a small number of inter-cluster links also hinders the scalability of scatternets.

Multipath BLE with no connections to overcome the restrictions, pure mesh topologies require mesh protocols. However, most of the connectionless protocols now under consideration for packet forwarding use broadcast-based flooding. The significant packet forwarding overheads present in flooding-based solutions must be overcome by more effective connectionless protocols that make use of directional forwarding. Support for real-time communication in BLE Mesh networks is a fundamental problem. Although the focus of this survey is on connection-oriented scatternets, scalable real-time communications in large BLE Mesh networks are unlikely to be possible without the use of connectionless packet forwarding protocols due to the difficulty in achieving bounded end-to-end delays.

As the BLE specifications only cover broadcast and unicast transmissions, multi-hop and multicast packet forwarding are not supported by BLE Mesh protocols. An efficient method for delivering data to a group of cooperating nodes is multicasting. IoT apps that manage a set of lights or gather sensor data for a smart home frequently use similar scenarios.[5]

Security Issues with BLE Mesh

To understand the situation as of the security challenges for BLE Mesh networks, it is necessary to first present an overview of Wireless Personal Area Network (WPAN) Networks attacks, in order to provide the context for categorizing BLE specific attacks and current BLE vulnerabilities. A summary of security features for BLE can be found in the Appendix B. Figure 6 provides an overview of the attacks affecting WPANs, as well as security threats that are specific to BLE.[6]

Improved Bluetooth Security

The efforts to strengthen Bluetooth low energy security were focused on boosting authentication and improving the integrity of the scatternet formation process considering the numerous Bluetooth security threats. To secure scatternet generation, Yu and Wang suggested a security upgrade for the Bluetooth Topology Construction Protocol (BTCP). By assuring correct authentication during the scatternet construction phase, the protocol can defeat MITM attacks. Like this, Sadghzadh et al.'s proposal for a security protocol for Bluetooth networks combined encrypted key exchange techniques with a focus on authentication. An improved Bluetooth pairing mechanism created by Xu and Yu can counter MITM attacks.

Elliptic-curve Diffie-Hellman (ECDH) key agreement-based existing solutions are effective against passive eavesdropping attacks but are unable to counteract MITM assaults. The suggested procedure employs a robust public key exchange system to fend off threats like MITM, passive eavesdropping, replay, and impersonation. To safeguard data communications, Diallo and Wajdi created a technique that uses double layered encryption. By doing away with cleartext public key and password exchanges and employing Hash-based Message Authentication Code (HMAC) to guard against message manipulation during the key exchange process, the proposed protocol avoids the flaws of Secure and Simple Pairing (SSP).

Bluetooth version 4 defines the Numeric Comparison (NC) pairing mechanism, which calls for input and output capabilities, in accordance with Fan et al. They looked at the drawbacks of a pin-based authentication strategy in the event that one of two devices lacks output functionality. In order to perform message authentication and integrity checks, guard against MITM attacks, and spot message modifications, Priyanka and Nagajayanthi created a link-layer

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

security mechanism for the Bluetooth stack. A lightweight Physical Unclonable Function (PUF)-based authentication protocol was created by Nai and Yohan for joint authentication and session key confidentiality maintenance.
The suggested protocol was utilized to put into place a micropayment system that allows users to safely conduct transactions using BLE-capable wearables. The authors then confirmed that the devised solution can thwart traditional attacks including passive eavesdropping, replay, MITM, and impersonation attacks in addition to fake payment and session hijacking threats.[7]

IDS for IoT Networks

IoT networks are networks that use fewer resources than WPAN-based networks, according to this article. IoT devices may also be mains-powered and often use Ethernet or Wi-Fi technologies for connectivity. As a result, they are not constrained by resource issues that battery-powered gadgets. The Online Sequential-Extreme Learning Machine (OS-ELM) algorithm was used by Prabavathy et al.to create an IDS based on fog computing that effectively detects assaults in a large size network of IoT-based devices. In contrast to centralized methods, the employment of distributed intelligence in local fog nodes produced a system that was more effective, versatile, and interoperable and had a 25% faster attack detection capability.
The Key-Match (KMA) and Cluster-Based (CBA) IDS and IPS algorithms were created by Choudhary and Kesswani and have strong true positive detection rates to safeguard against sinkhole and selective forwarding routing attacks. Tian et al.'s proposal for an anomaly-based intrusion detection system combined shallow learning with deep learning. The SLA in the proposed system consists of a Support Vector Machine (SVM) employing an Artificial Bee Colony (ABC) algorithm parameter optimization while using Five-fold Cross Validation (5FCV), whilst the DLM employs a deep auto-encoder for feature learning. Compared to the Principal Component Analysis (PCA)-based technique, the proposed framework outperformed it. One of the primary sources of assaults against IoT systems is DoS attacks. The presented IDS approaches, according to Jan et al., cannot completely prevent intrusions. The authors suggested a very simple Machine Learning (ML)-based method for identifying attacker-initiated unwanted data injection. To effectively detect intrusions in IoT networks, the received data properties were fed into the SVM classifier. Comparing SVM to rival Neural Network (NN), k-Nearest Neighbors (k-NN), and Device Tree (DT) techniques, it was discovered that SVM was more accurate.[8]

Protocol Improvements for Bluetooth Network Security

The uses for wireless technology have grown significantly along with wireless communication technology. Additionally, Bluetooth technology is one of the wireless technologies that has grew in importance as a result of its accessibility. Therefore, Bluetooth network security is necessary, just like it is in all other networks. In light of the aforementioned, various researchers have worked on improving Bluetooth network security. A solution for Bluetooth intrusion detection was suggested by. For the purpose of identifying harmful behaviors, the detection system made use of pattern matching and a collection of plug-in modules. The proposed system can also react to attacks in addition to just detecting them. In order to assure reliable scatter net generation, added a security protocol to the original Bluetooth Topology Construction Protocol (BTCP).
The author claims that by requiring authentication during the scatter net formation, the created protocol can overcome MITM,created a security protocol that, when used with EKEP, can thwart various well-known attacks on Bluetooth, including denial of service attacks on authentication and relay attacks, among others. The paper's main objective was to address Bluetooth's authentication problems. The protocol has a few phases to it. Both the starting user A and the answering user B will first enter their respective PINs. Then, PINs and the Elliptic Curve Diffie Hellman (ECDH) key will combine to create TK(A) and TK(B). The authentication process will then begin after the original user sends an initiating message.
The responder will then send a random nonce (Nb) encrypted by TK(B) after receiving the message.Additionally, the initiating device will decrypt the message after receiving it and deliver an encrypted value made up of Na and Nb. Additionally, the responder will decode the message that was sent, confirm the accuracy of the Nb value, and then reply with the hash of Na (HNa). The communication will continue after the initiator hash-value-checked it. The connection will be broken if the HNa is unclear. A Bluetooth security protocol that can combat MITM was proposed by [9].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

Attacks on BLE Mesh Networks: Mitigation and Defenses

BLE mesh networks have the same security needs as other communication networks, whether they are wired or wireless, including availability, authentication, integrity, confidentiality, non-repudiation, and authorization. With a view to achieving. The network's security requirements, as well as the previously listed security concerns, must be addressed. Physical attacks are susceptible to mitigation at the implementation level. It is challenging to rule out the potential of any equipment physical mistreatment given the nature of these attacks. Additionally, the BLE defeats passive eavesdropping attacks by encrypting data using the AES-CCM cryptography.

The BLE's cryptography system is highly robust. However, key exchange procedures, often known as pairing methods, have significant security flaws. To defend against network attacks like MITM, the proper key exchange method must be chosen based on the network security requirements. Additionally, at the protocol level, the network and application keys should undergo key refreshment more frequently. To make the network the least susceptible to attacks, there must be a reliable method for refreshing the device key as well. The mechanism must be used to ensure the right approach for the device key renewal because each device key is unique and static. Speaking about side channel attacks, they can be prevented by the use of robust cryptography, either at the hardware or software level. Software-level cryptographic code can be applied to assure the least amount of vulnerability.

Additionally, a small cryptographic processor can be added to the hardware to ensure proper defense against vulnerabilities, such as those in the nRF52840 system-on-chip with the ARM Trust Zone Cryptocell-310, which can be secured during chip fabrication. Although these pieces of hardware include cryptographic processors, they are still susceptible to physical attacks, which makes it harder for the attacker.[10]

II. FUTURE SCOPE

Multiple nodes needed to be upgraded simultaneously.Personal sharing of Bluetooth stream with someone close by an unlimited number of audio devices simultaneously receive the same Bluetooth transmission. There is no security provided by this mechanism since device must accept connections without verification. A mesh topology provides redundant links across the network.

III. CONCLUSION

In this paper, we have discussed several research works related to the security in BLE and wireless mesh networks. Researchers have worked on security enhancements of mesh networks by proposing different techniques. After the detailed literature review, it is concluded that there are many security lapses in the area of BLE and wireless mesh network. Moreover, BLE being new in the arena of mesh networks, there are still many security gaps that are required to be filled.

ACKNOWLEDGEMENT

I want to sincerely thank our advisers at the Ravikiran R Department of ECE for their invaluable advice and assistance during the study process. I also want to express our gratitude to the SJC Institute of Technology for their assistance with this initiative.

REFERENCES

[1] S. Glass, M. Portmann, V. Muthukkumarasamy, “Securing Wireless Mesh Networking,” IEEE Internet Computing., vol. 12, issue. 4, pp. 30- 36, 2008.
[2] A. Sgora, D. D. Vergados, P. Chatzimisios, “A survey on security and privacy issues in Wireless Mesh Networks,” Security and Communication Networks., vol. 9, pp. 1877-1889, 2013.
[3] D. Bansal, S. Sofat, P. Pathak, S. Bhoot, “Detecting MAC misbehavior switching attacks in Wireless Mesh Networks,” International Journal of Computer Applications, vol. 26, issue. 5, pp. 55-62, 2011.
[4] J. Zhou, Z. Chen, W. Jiang, W, “Probability based IDS towards secure WMN,” 2nd International Workshop on Intelligent Systems and Applications, pp. 1-5, 2010.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 6, May 2023

[5] Y. Yang, P. Zeng, X. Yang, Y. Huang, "Efficient intrusion detection system model in Wireless Mesh Networks; Network Security Wireless," 2nd International Conference on Communications and Trusted Computing, pp. 393-395, 2010.
[6] Hugelshofer, S. Fabian, H. Paul, R. David, J.P. Nicholas, "OpenLIDS: a lightweight intrusion detection system for wireless mesh networks," 15th Annual International Conference on Mobile Computing and Networking, pp. 309-320, 2009.
[7] O. Rodas, M.A. To, J. Alvarez, S. Maag, "Protecting Wireless Mesh Networks through a distributed intrusion prevention framework," 7th IEEE Latin-American Conference on Communications, pp. 1-6, 2015.
[8] A. Boudguiga, M. Laurent, "An authentication scheme for IEEE 802.11s mesh networks relying on Sakai-Kasahara ID-Based Cryptographic algorithms," 3rd International Conference on Communications and Networking, pp. 1-8, 2012.
[9] D. Yi, G. Xu, Z. Minqing, Z, "The research on certificateless hierarchical key management in Wireless Mesh Network," 3rd International Conference on Communication Software and Networks, pp. 504-507, 2011.
[10] H. Jiacheng, L. Ning, Y. Ping, Z. Futai, Z. Qiang, "Securing Wireless Mesh Network with Mobile Firewall,"International Conference on Wireless Communications and Signal Processing, pp. 1-6, 2010.
[11] A. Adomnicai, J.J.A. Fournier, A.Masson, "Hardware Security Threats Against Bluetooth Mesh Networks," IEEE International Workshop on Attacks and Defenses for Internet of Things, pp. 1-9, 2018.
[12] A.A. Pammi, "Threats, Countermeasures, and Research Trends for BLEbased IoT Devices," Master Thesis, Arizona State University, 2017.
[13] T. OConnor, D. Reeves, "Bluetooth Network Based Misuse Detection," Annual Computer Security Applications Conference, pp. 377-391, 2008.
[14] X. Yu, Y. Wang, "Secure Constructing Bluetooth Scatter Net Based on BTCP," 5th International Conference on Information Assurance and Security, pp. 200-203, 2009.
[15] S.H. Sadeghzadeh, S.J.R. Shirazani, M. Mosleh, "A new secure scheme purposed for recognition and authentication protocol in Bluetooth environment," 12th ICACT, pp. 1326-1331, 2010.
[16] G. Xu, B. Yu, "Security Enhanced Design of the BluetoothSimple Pairing Protocol," International Conference on Computer Science and Network Technology, pp. 292-296, 2011.
[17] C. Fan, S. Shieh, B. Li, "On the security of password based pairing protocol in Bluetooth," 13th Asia-Pacific Bluetooth Operations and Management Symposium, pp. 1-4, Taipei, 2011.
[18] S.S. Priyanka, B. Nagajayanthi, "Enhancing Security in Bluetooth Networks," International Conference on Science Engineering and Management Research, pp. 1-3, Chennai, 2014. [19] A.S. Diallo, A. Wajdi, R.F. Olanrewaju, F. Sado, "A Secure Authentication Scheme for Bluetooth Connection," 5th International Conference on Computer and Communication Engineering, pp. 60-63, Kuala Lumpur, Malaysia, 2014.
[19] A.M. Lonzetta, P. Cope, J. Campbell, B.J. Mohd, "Security Vulnerabilities in Bluetooth Technology as Used in IoT," Journal of Sensor and Actuator Networks, vol. 7, issue. 28, pp. 1-26, 2018.
[20] V.O. Adeniji, K. Sibanda, "Analysis of the effect of Malicious Packet drop attack on Packet transmission in Wireless Mesh Networks," 2018 Conference on Information Communications Technology and Society, pp. 1-6, Durban, 2018.
[21] S.M. Darroudi, C. Gomez, "Bluetooth Low Energy Mesh Networks: A Survey," Sensors, vol. 17, issue. 7, pp. 1-19, 2017. [23] M.R. Ghori, A. Ghani, "Review of Access Control Mechanisms in Cloud Computing," Journal of Physic.: Conf. Ser, vol. 1049, 2018.