Encyclopedia

Bluetooth Low Energy Mesh Networks

Created by: Muhammad Rizwan Ghori [1] , Tat-chee Wan [2]

1, Universiti Sains Malaysia; mrizwanghori@student.usm.my
2, Universiti Sains Malaysia; tcwan@usm.my

Version received: 20 July 2020

Bluetooth Low Energy (BLE) Mesh Networks enable flexible and reliable communications for low-power Internet of Things (IoT) devices. Most BLE-based mesh protocols are implemented as overlays on top of the standard Bluetooth star topologies while using piconets and scatternets. Nonetheless, mesh topology support has increased the vulnerability of BLE to security threats, since a larger number of devices can participate in a BLE Mesh network. To address these concerns, BLE version 5 enhanced existing BLE security features to deal with various authenticity, integrity, and confidentiality issues. Despite of the BLE version 5 security enhancements, viable IDS solutions for BLE Mesh networks remain a nascent research area.

1. Definition

Bluetooth Low Energy (BLE) is an increasingly prevalent Wireless Ad-Hoc Network (WAHN) technology for battery-powered Internet of Things (IoT) devices [1]. The BLE standard was introduced by the Bluetooth Special Interest Group (SIG) in Bluetooth version 4.0, and subsequently enhanced in versions 4.2 and 5. Initially, BLE 4.x adopted the legacy Bluetooth Personal Area Network (PAN) model for multi-hop communications and the interconnection of networks. BLE 5 intends to address these inadequacies via the implementation of pure mesh topology to provide enhanced network coverage, inter-network connectivity, and improved security [2].

2. Introduction or History

The vast majority of BLE-based applications still assume a star network topology while using BLE Beacons in broadcast mode [3][4][5][6][7][8][9]. To enhance the coverage of BLE 4 networks, hybrid mesh topologies extend the master-slave piconet concept into various interconnected scatternets via the fusion of star and mesh links [10]. Nonetheless, reliability and scalability remain an issue. In contrast, a pure mesh topology removes the master–slave limitation by making nodes peer with each other to form scalable networks.

The BLE specifications has adopted various useful security features. However, security exploits have highlighted the vulnerabilities in existing BLE security features [11]. Consequently, security features must be supplemented with strong Intrusion Detection Systems (IDS) to detect zero-day attacks. Because the BLE 5 Mesh protocol expands the reach of the network significantly, the potential for intrusion also increases proportionally. Moreover, it is necessary to reference existing IDS approaches adopted by other low-power wireless network technologies for comparison due to the lack of research into suitable IDS for BLE Mesh networks.

3. Data, Model, Applications and Influences

Ghori et al. [12] surveyed the most recent BLE-based communication protocols and related security issues in order to understand the current state of BLE Mesh protocol development and open research areas. The research has mostly addressed new protocols and issues discovered since the publication of the existing surveys. Additionally, the authors have analyzed both BLE based communication protocols and security-related concerns to address mesh network issues and BLE 5 specific security weaknesses, respectively.

3.1 BLE Mesh System Architecture

The BLE Mesh System Architecture is defined on top of the BLE core specifications[13], as shown in Figure 1. In the figure, the Bearer Layer leverages the BLE Network Stack Host protocols to support its operation.

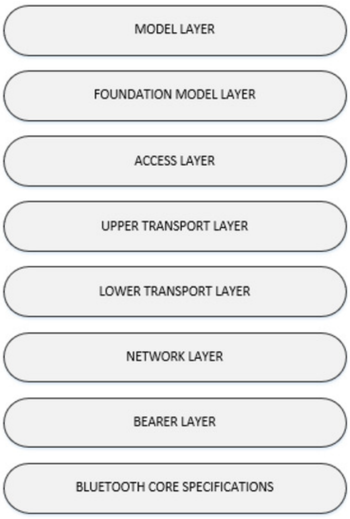

Figure 1. Bluetooth Low Energy (BLE) Mesh System Architecture[13].

3.2. BLE Mesh Communication Protocols

A recent survey of mesh based protocols[12] classifies the various protocols as shown in Figure 2.

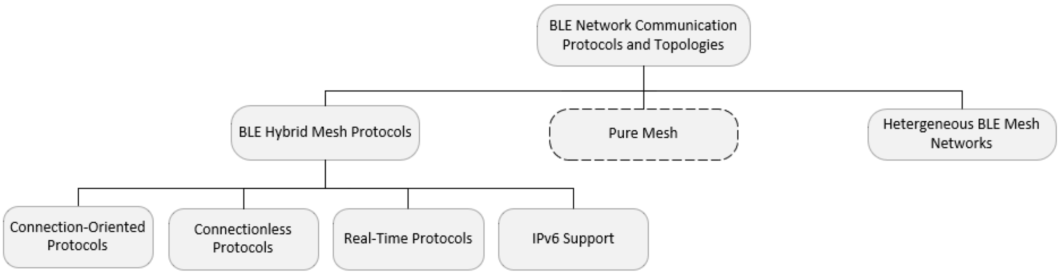
BLE Network Communication Protocols and Topologies
BLE Hybrid Mesh Protocols
Pure Mesh
Hetergeneous BLE Mesh Networks
Connection-Oriented Protocols
Connectionless Protocols
Real-Time Protocols
IPv6 Support

Figure 2. Classification of BLE Communication Protocols[12].

The coverage of recent BLE Mesh protocols highlighted the open research issues related to enhancement and scalability of BLE Mesh protocols [12]. Because most BLE Mesh topologies are designed for the scatternet topologies using connection oriented communications, the robustness of BLE Mesh networks against node failure and mobility is limited [10]. Furthermore, the scalability of scatternets is hampered by the fact that only a limited number of inter-cluster links are used by most proposed protocols [12].

3.3. BLE Mesh Security Issues

To understand the current state of the security challenges for BLE Mesh networks, it is necessary to 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. Figure 3 provides an overview of the attacks affecting WPANs, as well as security threats that are specific to BLE.

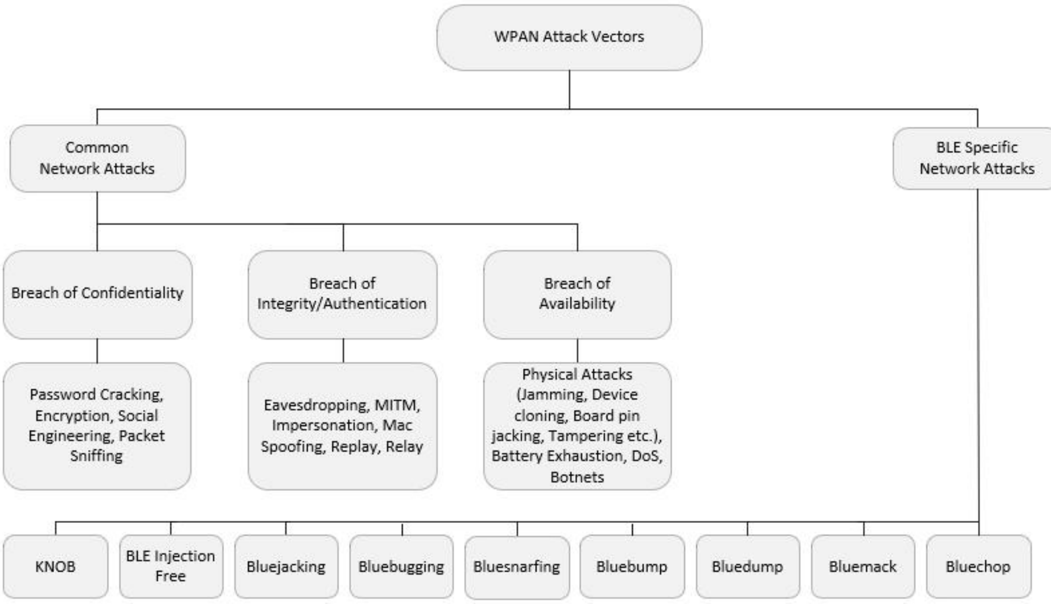
WPAN Attack Vectors
Common Network Attacks
BLE Specific Network Attacks
Breach of Confidentiality
Breach of Integrity/Authentication
Breach of Availability
Password Cracking, Encryption, Social Engineering, Packet Sniffing
Eavesdropping, MITM, Impersonation, Mac Spoofing, Replay, Relay
Physical Attacks (Jamming, Device cloning, Board pin jacking, Tampering etc.), Battery Exhaustion, DoS, Botnets
KNOB
BLE Injection Free
Bluejacking
Bluebugging
Bluesnarfing
Bluebump
Bluedump
Bluemack
Bluechop

Figure 3. Wireless Personal Area Network (WPAN) Attack Vectors[12].

3.4. Current BLE Vulnerabilities

Because new vulnerabilities are continually being discovered and existing implementation-related vulnerabilities (which are not due to flaws in the protocol design) are fixed by vendors, it is not possible to provide a definitive list of BLE vulnerabilities. A report identified various Bluetooth security susceptibilities, collectively known as the SweynTooth exploits, resulting in DoS attacks on affected devices [11]]. Figure 4 summarizes these exploits.

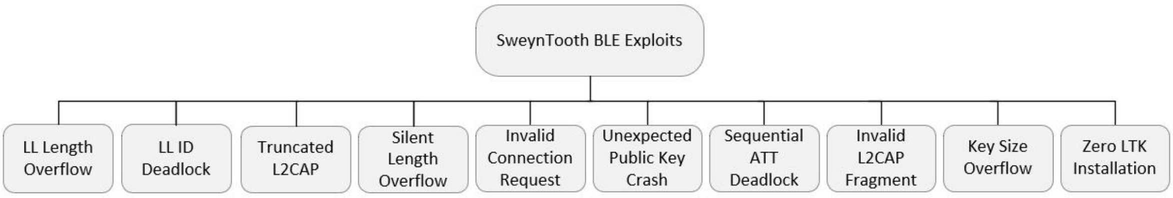

Figure 4. SweynTooth BLE Exploits [11].

3.5. IDS for Related WSN Technologies

To overcome the security threats mentioned in sections 3.3 and 3.4, it is necessary to adopt intrusion detection techniques to provide early warning against such threats. Due to the fact that research into Intrusion Detection Systems (IDS) for BLE Mesh Networks is still in its infancy, the survey conducted by [12] discussed the techniques used by IDS for other more established wireless technologies, as shown in Figure 5, which is expected to provide direction for further research in this area.

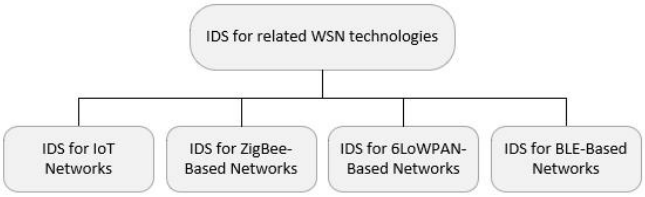
IDS for related WSN technologies
IDS for IoT Networks
IDS for ZigBee-Based Networks
IDS for 6LoWPAN-Based Networks
IDS for BLE-Based Networks

Figure 5. Intrusion Detection Systems (IDS) for related WSN technologies[12].

3.6. Conclusions

BLE Mesh is an emerging wireless mesh technology that is built upon the Bluetooth Low Energy standard. Nonetheless, most BLE Mesh topologies are overlay networks constructed using the connection-oriented scatternet links defined by the legacy Bluetooth architecture. Additionally, energy efficiency is an important design criteria for BLE

Mesh networks, especially due to their dependency on power-constrained devices. Also, despite the additional security measures that are introduced in Bluetooth 4.2 and Bluetooth 5, the focus of these security measures were mostly on securing the communications channel between a pair of nodes. Efficient techniques for performing authentication and ensuring the integrity of the mesh network are needed to support the widespread deployment of BLE Mesh networks. Furthermore, IDS is very important to augment the available security mechanisms and to protect the BLE Mesh network from zero-day attacks.

The article has been published on 10.3390/s20123590

References

1. Ghori, M.R.; Wan, T.C.; Sodhy, G.C. Bluetooth Low Energy 5 Mesh Based Hospital Communication Network (B5MBHCN). In Advances in Cyber Security; Springer: Singapore, 2020; Volume 1132, pp. 247–261.
2. Darroudi, S.M.; Gomez, C. Bluetooth Low Energy Mesh Networks: A Survey. Sensors 2017, 17, 1467.
3. Gohel, S. Bluetooth Attendance System with Android Application for ERP. In Proceedings of the International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, 28–29 Septtember 2018; pp. 481–484.
4. Sthapit, P.; Gang, H.; Pyun, J. Bluetooth Based Indoor Positioning Using Machine Learning Algorithms. In Proceedings of the IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), Jeju, Korea, 24–26 June 2018; pp. 206–212.
5. Yumantoro, G.; Kristalina, P.; Sudarsono, A. Performance Evaluation of Indoor Characteristic based on Bluetooth Low Energy Communication System through Statistical Approach. In Proceedings of the International Electronics Symposium on Engineering Technology and Applications (IES-ETA), Bali, Indonesia, 29–30 October 2018; pp. 189–195.
6. Handojo, A.; Lim, R.; Octavia, T.; Anggita, K. Museum Interactive Information Broadcasting Using Indoor Positioning System and Bluetooth Low Energy: A Pilot Project on Trowulan Museum Indonesia. In Proceedings of the 3rd Technology Innovation Management and Engineering Science International Conference (TIMES-iCON), Bangkok, Thailand, 12–14 December 2018; pp. 1–5.
7. Sunardy, A.; Surantha, N. Performance Evaluation of Indoor Positioning Algorithm using Bluetooth Low Energy. In Proceedings of the International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, 22–26 October 2018; pp. 503–507.
8. Mohsin, N.; Payandeh, S.; Ho, D.; Gelinas, J.P. Bluetooth Low Energy Based Activity Tracking of Patient. In Proceedings of the 15th International Conference on Control, Automation, Robotics and Vision (ICARCV), Singapore, 18–21 November 2018; pp. 1991–1996.
9. Giovanelli, D.; Farella, E.; Fontanelli, D.; Macii, D. Bluetooth-Based Indoor Positioning Through ToF and RSSI Data Fusion. In Proceedings of the International Conference on Indoor Positioning and Indoor Navigation (IPIN), Nantes, France, 24–27 September 2018; pp. 1–8.
10. Jung, C.; Kim, K.; Seo, J.; Silva, B.; Han, K. Topology Configuration and Multihop Routing Protocol for Bluetooth Low Energy Networks. IEEE Access 2017, 5, 9587–9598.
11. Bluetooth Vulnerabilities. Available online: https://thehackernews.com/2020/02/hacking-bluetooth-vulnerabilities.html (accessed on 20 February 2020).
12. Ghori, M.R.; Wan, T.-C.; Sodhy, G.C. Bluetooth Low Energy Mesh Networks: Survey of Communication and Security Protocols. Sensors 2020, 20, 3590.
13. Bluetooth. Available online: https://www.bluetooth.com (accessed on 19 February 2020).

Keywords

bluetooth low energy; BLE; wireless mesh networks; IoT security