

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.

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.
- [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.