

Bluetooth low energy for internet of things: review, challenges, and open issues

Mahmood A. Al-Shareeda¹, Murtaja Ali Saare², Selvakumar Manickam¹, Shankar Karuppayah¹

¹National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia

²Department of Computer Technology Engineering, Shatt Al-Arab University College, Basrah, Iraq

Article Info

Article history:

Received Dec 18, 2022

Revised Mar 27, 2023

Accepted Apr 2, 2023

Keywords:

BLE challenges

BLE-IoT review

Bluetooth low energy

Bluetooth low energy for internet of things

Internet of things

ABSTRACT

As a result of its ultra-low power consumption, simple development, sufficient network coverage, and rapid data transfer speed, Bluetooth low energy (BLE) has emerged as the standard communication standard for internet of things (IoT) nodes. Therefore, in this review paper introduces the concept of Bluetooth low energy for the internet of things (BLE-IoT) in terms of Bluetooth classic, Bluetooth version, applications for BLE-IoT, and new features of BLE-IoT. We then provide a taxonomy of literature reviews based on the parameter adjustment approach (e.g., advertiser side schemes, scanner side schemes, hybrid schemes) and collision avoidance approach (e.g., advertiser side schemes and scanner side schemes). Finally, we discuss research challenges and future opportunities for BLE-IoT.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Selvakumar Manickam

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia

11800 USM, Penang, Malaysia

Email: selva@usm.my

1. INTRODUCTION

Commonly referred to as "Bluetooth smart," Bluetooth low energy (BLE) [1], [2] is the most popular wireless standard for IoT gadgets. The Bluetooth Special Interest Group (SIG) created and continues to support this wireless personal area network (WPAN) technology. BLE was created by Nokia under the name Wibree [3]-[5] and has now been adopted by Bluetooth SIG [6], [7], which has over 20,000 active members. In June of 2010, BLE was initially presented in Bluetooth core specification 4.0 [8], and it has a few unique capabilities compared to traditional Bluetooth [9], [10]. The BLE protocol was developed for use in low-power, short-range communications between internet of things (IoT) sensors and other devices. Compared to competing low-power wireless systems like ZigBee [11], [12], Z-wave, and Wavenis, BLE has seen the most adoption. Compared to rival protocols like ZigBee and ANT, BLE is significantly more energy efficient. BLE is unique among wireless technologies (including Bluetooth and WiFi) in that it uses essentially no energy. Many of its security and privacy issues stemming from its streamlined protocol stack [13].

Researching BLE's security flaws is essential as it is now used by billions of devices. Every new piece of technology we add to our homes or workplaces makes our lives easier and boosts our output, but it also increases the number of potential points of attack. The security and privacy problems associated with BLE's widespread deployment in healthcare applications are potentially catastrophic [14]-[16]. The rest of this paper is organized as follows. Section 2 introduces the concept of Bluetooth low energy for the internet of things (BLE-IoT). Section 3 provides a taxonomy of literature reviews. Section 4 discuss research challenges and future opportunities for BLE-IoT. Finally, this review is provided conclusion in section 5.

2. BLUETOOTH LOW ENERGY FOR THE INTERNET OF THINGS

2.1. Internet of things

Over the past decade, the IoT has seen widespread implementation in a variety of settings, including industrial systems, healthcare systems, military applications, beacons, and smart home goods. Presently, there are 14.2 billion IoT devices connected to the internet, and this number is expected to climb to 25 billion by 2021. BLE is used by the vast majority of IoT devices to transfer data and connect to the web. Since BLE and classic Bluetooth [17] share an identical implementation, the former's popularity helped pave the way for the latter's adoption. Windows 10, Linux, Android, and even Mac OS X all support classic Bluetooth, and BLE is becoming increasingly popular.

2.2. Introduction to Bluetooth classic

With Bluetooth [18] innovation, the cable is no longer necessary for short-range wireless data exchange between mobile devices like a cell phone, laptop, or headphones and other peripherals. Bluetooth was originally standardised as IEEE 802.15.1 [19], but its requirement and trademark are now managed by the Bluetooth SIG. Bluetooth uses the unlicensed but still regulated ISM band, which is between 2.40 GHz and 2.48 GHz. In a Bluetooth network, a "master" device can link to a maximum of seven "slaves," each of which can then transmit data in packet form. Piconet is the term for this particular network architecture.

2.3. Bluetooth version

The Bluetooth SIG has released five major Bluetooth versions. Every release is compatible with previous ones. The following are some of the key differences between the two versions:

- Bluetooth 1.x: in May of 1998, the original Bluetooth protocol debuted. It is rarely used these days. It has a low maximum speed (just 1 Mbit/s) and a plethora of pairing security flaws.
- Bluetooth 2.x: in 2005, the public saw the debut of this iteration. The ease with which it could pair with other phones made it a hit among those that were showcased. It allows for data transfer rates of up to 3 Mbit/s.
- Bluetooth 3.x: the Bluetooth SIG approved version 3 of the Bluetooth specification in April 2009. It can transfer data faster than its predecessors (up to 24 Mbit/s). However, increased velocity is accompanied by increased energy requirements.
- Bluetooth 4.x: the most intriguing low energy (LE) feature is included in this version, which was released in June of 2010. Because of this feature, BLE can support IoT devices that have limited battery life. A range of 50–100 metres is supported, and it is capable of higher speeds. With Bluetooth 4.1, you can connect devices in the Internet of Things indirectly. In the past, BLE IoT devices required a smartphone's Internet connection in order to function. To counter this, Bluetooth 4.2 included an internet protocol version 6 (IPv6) layer in the BLE protocol stack. Therefore, the BLE protocol can be used by IoT devices as a foundation for IPv6 networking.
- Bluetooth 5.x: compared to its predecessors, this 2016 release is noticeably speedier than the rest.

2.4. Applications for BLE-IoT

This subsection describes the applications for BLE-IoT. These applications are the technology of beacon, bleach and mobile payment. The description of these applications are as follows.

- Technology of beacon: a beacon is a radio transmitter that uses BLE to broadcast messages to nearby smartphones through geolocation services [20]. Shoppers who are in the immediate vicinity of a beacon can be alerted to the presence of that beacon's vendor by the device.
- Bleach: not being able to modify the underlying BLE radio driver or link layer is a significant limitation for BLE developers. It's essentially a black box that carries out data transfer instructions.
- Mobile payment: when combined with a payment app, BLE can enable mobile commerce. Every retail store makes use of BLE beacons to promote a variety of goods.

2.5. New features of BLE-IoT

This subsection describes the new features for BLE-IoT. These features are higher speed, support for IoT devices, cover larger range, long-lasting battery, LE advertising extensions, increase payload size, LE channel selection algorithm, LE audio, GATT caching, Slot availability mask, and security manager. The description of these features are as follows.

- Higher speed: in comparison to BLE v5, which can achieve up to 2 Mbps, BLE v4 can only achieve speeds of up to 1 Mbps. This means that the data transfer rate between the wearable device and mobile app can be increased and that live streaming is possible with BLE v5. The devices can be reprogrammed to improve speed or extend the range of their covert operations.
- Support for IoT devices: for optimal performance, many IoT devices call for low power consumption alongside high speed and throughput. Since BLE 5.0, it has been possible to use it with any kind of IoT device thanks to the variety of ways in which these issues can be addressed.
- Cover larger range: the range of BLE v5.0 is roughly 4 times that of its predecessors. There is a range of 50-100 metres outdoors with BLE v4, and 10-20 metres indoors. Whereas the range of BLE v5 is 200 metres outside and 40-50 metres inside. Because of this, it can serve as an alternative to wireless internet over WiFi.
- Long-lasting battery: energy consumption in BLE v5 is nearly half that of previous versions thanks to improvements in signal modulation design and spectrum utilisation.
- LE advertising extensions: thanks to advancements in advertising packet transmission, devices can now communicate by exchanging packets without needing to synchronise their clocks. Thanks to this improvement, beacons can be used extensively in any setting.
- Increase payload size: with BLE v4, there isn't much you can say in a message. The average size of a message is 31 bytes with a payload size of 17-20 bytes. The maximum message size for BLE v5.x is 255 bytes.
- LE channel selection algorithm: with the release of BLE v5.0, this functionality is now available. As a result of its ability to mitigate detrimental effects of interference and multi-path fading, this algorithm allows for a significant increase in data transmission throughput.
- LE audio: with the dual audio mode enabled, a mobile device can connect to two audio devices at once using the multiple audio connectivity features introduced in BLE v5.2.
- Generic attribute profile (GATT) caching: since BLE version 5.1, this capability has been available. In this way, GATT caching reduces the time needed to learn about the GATT database after re-connecting the previously connected devices.
- Slot availability mask: it is because of this function that BLE can exist in close proximity to long-term evolution (LTE) transmission. This means that it avoids packet loss by staying on its own channel and not interfering with other nearby LTE transmissions.
- Security manager: the newest BLE releases feature an improved SM, making it more challenging for an attacker to break.

3. LITERATURE REVIEWS

There are several researchers who have applied BLE-IoT to address concerns in wireless technology. As shown in Figure 1, this review taxonomies these studies according to both approaches, namely the parameter adjustment approach and collision avoidance approach. The parameter adjustment approach is advertiser side schemes, scanner side schemes, and hybrid schemes. These schemes describes are as follows.

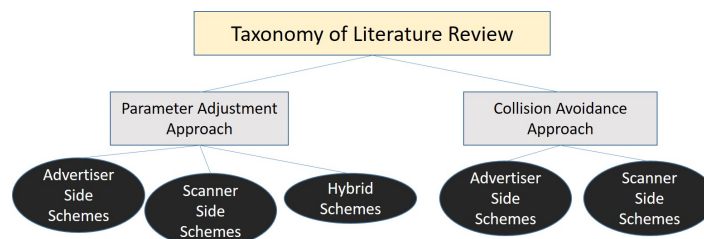


Figure 1. Taxonomy of literature reviews for BLE-IoT

3.1. Parameter adjustment approach

An approach of this type involves the modification of one or more parameters. According to the device that makes the necessary adjustments, the schemes can be broken down into one of three categories.

These names are advertiser-side schemes, scanner-side schemes, and hybrid schemes. These categories have been provided as follows.

3.1.1. Advertiser side schemes

Liu *et al.* [21], present a simple shrink discovery scheme for rapid discovery. The authors begin by examining the theoretical mode and simulation results to see how changing a parameter affects the time it takes to make a discovery. Seo *et al.* [22], explained a system of variable commercial breaks is proposed. The authors use a straight forward carrier sensing (CS) mechanism to gather up-to-date contention data on the network. In order to reduce the time it takes for complete advertisers to be discovered, Shan and Roh [23] and Mohammed *et al.* [24] propose an optimal advertisement interval scheme. The authors develop an analytical model to determine the time required to find all nearby marketers in the system. Renzler *et al.* [25] and Al-Mekhlafi *et al.* [26], propose an adaptive method for finding BLE devices. The goal of this scheme is to reduce power consumption and reduce the time it takes for objects to be discovered in smart lock systems.

3.1.2. Scanner side schemes

Liu *et al.* [27] find a proposal for an adaptive device discovery scheme. In this scheme, two crucial scanner parameters are dynamically adjusted in response to the current contention situation. The parameters are suggested by Kandhalu *et al.* in [28]. This method's primary goal is to ensure a finite discovery latency for vehicular networks.

3.1.3. Hybrid schemes

The discovery performance can be enhanced by using the proposed adaptive parameter setting algorithm in [29]. In particular, the process of establishing parameters involves both gadgets. These schemes are based on a parameter adjustment approach. Hybrid is combined with multiple scheme types.

3.1.4. Discussion

There are a variety of criteria that can be used to set the parameter. Each gadget's discovery efficiency is evaluated on its own merits, taking into account the characteristics of the corresponding schemes. In particular, the scalability is hampered by the two schemes in [25], [28] that are designed for a specific application to be implemented using BLE technology. Table 1 summarises the varying parameters for each scheme.

Table 1. Summarises of schemes based parameter adjustment approach

Paper	scan window	scan interval	adv interval
[21]	No	No	Yes
[22]	No	No	Yes
[23]	No	No	Yes
[25]	No	No	Yes
[27]	Yes	Yes	No
[28]	Yes	No	No
[29]	Yes	No	Yes

3.2. Collision avoidance approach

These approaches are motivated by the fact that the collision avoidance mechanisms provided by the BLE standard are insufficient for a busy BLE network. We distinguish between two groups of collision avoidance strategies. The widespread presence of advertisers and scanners on the BLE network is taken for granted.

3.2.1. Advertiser side schemes

A CS-based discovery scheme is proposed in [22], [30]. Prior to sending an connectable scannable undirected advertising (ADV_IND) protocol data unit (PDU), the advertiser uses the CS period, as in [22], to verify the state of all available advertising channels. This first type of collision avoidance approach is described.

3.2.2. Scanner side schemes

Kim and Han [31] propose a backoff scheme for the scanner. After sending an ADV_IND PDU, an advertiser will remain on that channel for the following WA. Yang and Tseng [32] propose a new time-slot waiting system. The authors first suggest a two-way handshake to replace the three-way handshake required by the BLE standard, in which the advertiser does not respond to a scan response packets sent (SCAN_RSP) PDU

even after receiving it successfully. Hernandez-Solana *et al.* [33] proposes an anti-collision adaptation scheme for dense IoT tracking applications. One intended outcome of this scheme is to reduce the load on the BLE standard's backoff mechanism. This scheme's foundation is the extension mode in the scanner's side known as opportunistic listening (OL) described in [34]. OL allows the scanner to listen in on messages intended for other devices.

3.2.3. Discussion

When it comes to the discovery process, the collision avoidance schemes deviate from the BLE standard operation and necessitate some adjustments. For this reason, it is questionable whether the proposed schemes can be realised in practical BLE devices. The feasibility of the scheme described in [33] is specifically examined.

4. RESEARCH CHALLENGES AND FUTURE OPPORTUNITIES

Here, we'll go over seven broad areas where researchers are facing problems right now and where they can find answers in the future. This raises questions for the future that can help security researchers design a better guideline for IoT device manufacturers by investigating potential security and privacy issues of these new features of BLE-IoT, as shown in Figure 2.

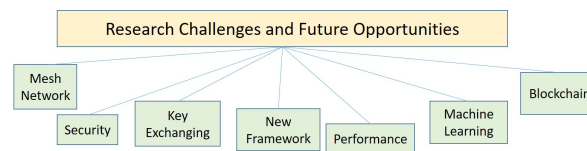


Figure 2. Research challenges and future opportunities for BLE-IoT

- Mesh network aspect: although BLE was developed with a star topology in mind, multi-hop mesh networks are required for use in industrial settings. Therefore, there are numerous areas for investigation into the development of a protected mesh network employing short-range BLE technology. There are many physical, link, network, and application layer security and privacy concerns that need to be investigated due to the large number of devices that are part of this network. Real-time communication [35], effective multicast [36], effective authentication, efficient auto-configuration, and inter-operability are some of the challenges still to be solved in the BLE mesh network.
- Security aspect: the enhanced capabilities of BLE 5.x make it a desirable option for IoT gadgets. This, however, broadens the potential target of an assault. Having a wider area of coverage makes it easier for attackers to gain access to devices and eavesdrop from a greater distance. When it comes to protecting the privacy, authenticity, and integrity of BLE 5.x communications, there has not been enough research done on the newest features and security mechanisms [37].
- Key exchanging aspect: custom key exchange mechanisms used in legacy connections are a major security hole in the BLE protocol. The pairing methodologies and link-layer encryption used to ensure privacy and strong encryption for better security are the subject of constant improvement research. In later versions, BLE's encryption was refined [37]. This encryption, however, can be broken at any time if manufacturers of said devices fail to properly uphold standardised guidelines [38].
- Performance aspect: academic and professional researchers are collaborating on some unanswered research questions to boost BLE's functionality. In BLE v5.x, the physical layer, or radio or physical layer (PHY) mode, was introduced to boost collision avoidance throughput, range, speed, and energy efficiency, opening up a wealth of new opportunities for research [30]. Most of the time, using adaptive frequency hopping to avoid interference works, which could pave the way for coexistence with other wireless technology. Integrating Bluetooth low energy (5G) and virtual autonomous networks (VANET) is a challenging area of study [39].
- New framework aspect: when designing a new security system [40], it's important to have a few things in mind. The goal of developing a framework for secure communication between two BLE devices is a worthwhile one [41]. A mechanism to protect against various BLE threats and guarantee stable communication is required in such a framework.

- Machine learning aspect: in industrial and home automation networks, there are many BLE-driven IoT devices. Security in BLE 5.x is predicated largely on protecting data exchanged among two devices [42]. Insufficient methods exist for protecting BLE mesh networks. There is a current window of opportunity for researchers to figure out how to use intrusion detection systems [37], [43] and intrusion prevention systems [watchdogs] to keep the BLE mesh network safe from zero-day vulnerabilities, denial-of-service attacks, and spoofing attacks [44]. Improving IoT security and privacy by developing novel machine learning algorithms is an exciting area of study. A number of methods, including neural networks (NN) [45], [46] and support vector machines (SVM) [47], [48], can be used to detect network intrusion. A deep neural network (DNN) [49] or a SVM [50] can be used to detect spoofing. Gaussian mixture models with infinite parameters can improve authentication's secrecy [51], [52].
- Blockchain aspect: IoT devices enabled by BLE have become ubiquitous. As a result, it is crucial to ensure that IoT devices have strong access controls and that sensitive data is managed securely. Connecting to an IoT device via a server, rather than each device individually, could improve both device management and user privacy [53], [54].

5. CONCLUSION

Because of its low energy requirements and high reliability in data transmission, BLE has quickly become one of the most popular technologies in the IoT industry worldwide. It's become crucial to our regular activities and IoT interactions. Despite BLE's low power consumption and speedy data transfer, some of its pairing methods are insecure, putting BLE communications at risk. Therefore, this review provides a comprehensive of BLE-IoT technology. Then we provide a taxonomy of literature reviews and discuss research challenges and future opportunities for BLE-IoT.

Since its initial release, BLE's architecture has undergone significant changes, making it difficult to identify serious vulnerabilities in its newest features. BLE will be more trustworthy after recent research on various pairing mechanisms, encryption improvements, structured mesh topology, and network protection via IDS and block-chain. BLE will be a desirable solution in the future IoT because of its low power consumption, high efficiency, and high security.

REFERENCES




- [1] Bluetooth SIG, "Bluetooth specification version 4.0." pp. 1–106, 2010, [Online]. Available: <https://www.bluetooth.com/specifications/specs/core-specification-4-0/>.
- [2] J. Haartsen, M. Naghshineh, J. Inouye, O. J. Joeressen, and W. Allen, "Bluetooth: vision, goals, and architecture," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 2, no. 4, pp. 38–45, Oct. 1998, doi: 10.1145/1321400.1321402.
- [3] M. A. Al-Shareeda, S. Manickam, S. A. Laghari, and A. Jaisan, "Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications," *Sustainability*, vol. 14, no. 23, p. 15900, Nov. 2022, doi: 10.3390/su142315900.
- [4] L. Huang *et al.*, "Ultra-low power sensor design for wireless body area networks: challenges, potential solutions, and applications," *International Journal of Digital Content Technology and its Applications*, vol. 3, no. 3, 2009, doi: 10.4156/jdcta.vol3.issue3.18.
- [5] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 29, no. 1, pp. 518–526, Jan. 2022, doi: 10.11591/ijeecs.v29.i1.pp518-526.
- [6] J. Decuir, "Introducing Bluetooth smart: part ii: applications and updates," *IEEE Consumer Electronics Magazine*, vol. 3, no. 2, pp. 25–29, Apr. 2014, doi: 10.1109/MCE.2013.2297617.
- [7] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: a review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 30, no. 2, pp. 778–786, May 2023, doi: 10.11591/ijeecs.v30.i2.pp778-786.
- [8] S. K. Pattnaik *et al.*, "Future wireless communication technology towards 6G IoT: an application-based analysis of IoT in real-time location monitoring of employees inside underground mines by using BLE," *Sensors*, vol. 22, no. 9, p. 3438, Apr. 2022, doi: 10.3390/s22093438.
- [9] M. A. Al-Shareeda *et al.*, "Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without road-side unit (RSU)," *Sustainability*, vol. 14, no. 16, p. 9961, Aug. 2022, doi: 10.3390/su14169961.
- [10] D. Chen *et al.*, "Coexistence and interference mitigation for WPANs and WLANs From traditional approaches to deep learning: a review," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25561–25589, Nov. 2021, doi: 10.1109/JSEN.2021.3117399.
- [11] M. A. Al-Shareeda and S. Manickam, "MSR-DoS: modular square root-based scheme to resist denial of service (DoS) attacks in 5G-enabled vehicular networks," *IEEE Access*, vol. 10, pp. 120606–120615, 2022, doi: 10.1109/ACCESS.2022.3222488.
- [12] P. Kinney, "ZigBee technology: wireless control that simply works," in *Communications Design Conference*, 2003, pp. 1–20.
- [13] M. A. Al-Shareeda and S. Manickam, "COVID-19 vehicle based on an efficient mutual authentication scheme for 5G-enabled vehicular fog computing," *International Journal of Environmental Research and Public Health*, vol. 19, no. 23, p. 15618, Nov. 2022, doi: 10.3390/ijerph192315618.

- [14] D. Kothandaraman, A. Balasundaram, E. Sudarshan, M. Sheshikala, and B. Vijaykumar, "BLE based secure text communication using IoT," in *AIP Conference Proceedings*, 2022, vol. 2418, p. 020064, doi: 10.1063/5.0081950.
- [15] B. A. Mohammed, M. A. Al-Shareeda, S. Manickam, Z. G. Al-Mekhlafi, A. M. Alayba, and A. A. Sallam, "ANAA-Fog: a novel anonymous authentication scheme for 5G-enabled vehicular fog computing," *Mathematics*, vol. 11, no. 6, p. 1446, Mar. 2023, doi: 10.3390/math11061446.
- [16] P. S. Farahsari, A. Farahzadi, J. Rezazadeh, and A. Bagheri, "A survey on indoor positioning systems for IoT-based applications," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7680–7699, May 2022, doi: 10.1109/JIOT.2022.3149048.
- [17] M. A. Al-Shareeda and S. Manickam, "Man-in-the-middle attacks in mobile ad hoc networks (MANETs): analysis and evaluation," *Symmetry*, vol. 14, no. 8, p. 1543, Jul. 2022, doi: 10.3390/sym14081543.
- [18] J. C. Haartsen, "The Bluetooth radio system," *IEEE Personal Communications*, vol. 7, no. 1, pp. 28–36, Feb. 2000, doi: 10.1109/98.824570.
- [19] "IEEE Standard for information technology - telecommunications and information exchange between systems - local and metropolitan networks - specific requirements - part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications: H," *IEEE Std 802.11b-1999*, pp. 1–96, 2000, doi: 10.1109/IEEESTD.2000.90914.
- [20] P. Kriz, F. Maly, and T. Kozel, "Improving indoor localization using Bluetooth low energy beacons," *Mobile Information Systems*, vol. 2016, pp. 1–11, 2016, doi: 10.1155/2016/2083094.
- [21] J. Liu, C. Chen, and Y. Ma, "Modeling and performance analysis of device discovery in Bluetooth low energy networks," in *2012 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2012, pp. 1538–1543, doi: 10.1109/GLOCOM.2012.6503332.
- [22] J. Seo, C. Jung, B. N. Silva, and K. Han, "A dynamic advertisement interval strategy in Bluetooth low energy networks," *International Journal of Sensor Networks*, vol. 27, no. 1, p. 52, 2018, doi: 10.1504/IJSNET.2018.092130.
- [23] G. Shan and B.-H. Roh, "Advertisement interval to minimize discovery time of whole BLE advertisers," *IEEE Access*, vol. 6, pp. 17817–17825, 2018, doi: 10.1109/ACCESS.2018.2817343.
- [24] B. A. Mohammed *et al.*, "FC-PA: fog computing-based pseudonym authentication scheme in 5G-enabled vehicular networks," *IEEE Access*, vol. 11, pp. 18571–18581, 2023, doi: 10.1109/ACCESS.2023.3247222.
- [25] T. Renzler, M. Spörk, C. A. Boano, and K. Römer, "Improving the efficiency and responsiveness of smart objects using adaptive BLE device discovery," in *Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects*, Jun. 2018, pp. 1–10, doi: 10.1145/3213299.3213306.
- [26] Z. G. Al-Mekhlafi *et al.*, "Chebyshev polynomial-based fog computing scheme supporting pseudonym revocation for 5G-enabled vehicular networks," *Electronics*, vol. 12, no. 4, p. 872, Feb. 2023, doi: 10.3390/electronics12040872.
- [27] J. Liu, C. Chen, Y. Ma, and Y. Xu, "Adaptive device discovery in Bluetooth low energy networks," in *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, Jun. 2013, pp. 1–5, doi: 10.1109/VTCspring.2013.6691855.
- [28] A. Kandhalu, A. E. Xhafa, and S. Hosur, "Towards bounded-latency Bluetooth low energy for in-vehicle network cable replacement," in *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, Dec. 2013, pp. 635–640, doi: 10.1109/IC-CVE.2013.6799869.
- [29] G. Park *et al.*, "An adaptive parameter setting algorithm to enhance performance in self-organizing Bluetooth low energy networks," *Wireless Personal Communications*, vol. 87, no. 3, pp. 953–969, Apr. 2016, doi: 10.1007/s11277-015-2619-4.
- [30] J. Seo, K. Cho, W. Cho, G. Park, and K. Han, "A discovery scheme based on carrier sensing in self-organizing Bluetooth low energy networks," *Journal of Network and Computer Applications*, vol. 65, pp. 72–83, Apr. 2016, doi: 10.1016/j.jnca.2015.09.015.
- [31] J. Kim and K. Han, "Backoff scheme for crowded Bluetooth low energy networks," *IET Communications*, vol. 11, no. 4, pp. 548–557, Mar. 2017, doi: 10.1049/iet-com.2016.0462.
- [32] T.-T. Yang and H.-W. Tseng, "Two-way communication with wait-slot scheme for neighbor discovery process in dense Bluetooth low energy networks," in *2017 13th International Conference on Network and Service Management (CNSM)*, Nov. 2017, pp. 1–7, doi: 10.23919/CNSM.2017.8255997.
- [33] A. Hernandez-Solana, D. Perez-Diaz-De-Cerio, A. Valdovinos, and J. L. Valenzuela, "Anti-collision adaptations of BLE active scanning for dense IoT tracking applications," *IEEE Access*, vol. 6, pp. 53620–53637, 2018, doi: 10.1109/ACCESS.2018.2870691.
- [34] A. F. Harris, V. Khanna, G. Tuncay, R. Want, and R. Kravets, "Bluetooth low energy in dense IoT environments," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 30–36, Dec. 2016, doi: 10.1109/MCOM.2016.1600546CM.
- [35] L. Leonardi, G. Patti, and L. Lo Bello, "Multi-hop real-time communications over Bluetooth low energy industrial wireless mesh networks," *IEEE Access*, vol. 6, pp. 26505–26519, 2018, doi: 10.1109/ACCESS.2018.2834479.
- [36] S. Darroudi and C. Gomez, "Bluetooth low energy mesh networks: a survey," *Sensors*, vol. 17, no. 7, p. 1467, Jun. 2017, doi: 10.3390/s17071467.
- [37] M. R. Ghori, T.-C. Wan, and G. C. Sodhy, "Bluetooth low energy mesh networks: survey of communication and security protocols," *Sensors*, vol. 20, no. 12, p. 3590, Jun. 2020, doi: 10.3390/s20123590.
- [38] K. Lotfy and M. L. Hale, "Assessing pairing and data exchange mechanism security in the wearable internet of things," in *2016 IEEE International Conference on Mobile Services (MS)*, Jun. 2016, pp. 25–32, doi: 10.1109/MobServ.2016.15.
- [39] J. Yang, C. Poellabauer, P. Mitra, and C. Neubecker, "Beyond beaconing: emerging applications and challenges of BLE," *Ad Hoc Networks*, vol. 97, p. 102015, Feb. 2020, doi: 10.1016/j.adhoc.2019.102015.
- [40] S.-C. Cha, M.-S. Chuang, K.-H. Yeh, Z.-J. Huang, and C. Su, "A user-friendly privacy framework for users to achieve consents with nearby BLE devices," *IEEE Access*, vol. 6, pp. 20779–20787, 2018, doi: 10.1109/ACCESS.2018.2820716.
- [41] Q. Zhang, Z. Liang, and Z. Cai, "Developing a new security framework for Bluetooth low energy devices," *Computers, Materials & Continua*, vol. 59, no. 2, pp. 457–471, 2019, doi: 10.32604/cmc.2019.03758.
- [42] A. Lacava, V. Zottola, A. Bonaldo, F. Cuomo, and S. Basagni, "Securing Bluetooth low energy networking: an overview of security procedures and threats," *Computer Networks*, vol. 211, p. 108953, Jul. 2022, doi: 10.1016/j.comnet.2022.108953.
- [43] B. Farzaneh, M. A. Montazeri, and S. Jamali, "An anomaly-based IDS for detecting attacks in RPL-based internet of things," in *2019 5th International Conference on Web Research (ICWR)*, Apr. 2019, pp. 61–66, doi: 10.1109/ICWR.2019.8765272.
- [44] W. Oliff, A. Filippopolitis, and G. Loukas, "Evaluating the impact of malicious spoofing attacks on Bluetooth low energy based occupancy detection systems," in *2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*, Jun. 2017, pp. 379–385, doi: 10.1109/SERA.2017.7965755.




- [45] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.
- [46] R. V. Kulkarni and G. K. Venayagamoorthy, "Neural network based secure media access control protocol for wireless sensor networks," in *2009 International Joint Conference on Neural Networks*, Jun. 2009, pp. 1680–1687, doi: 10.1109/IJCNN.2009.5179075.
- [47] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: algorithms, strategies, and applications," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1996–2018, 2014, doi: 10.1109/COMST.2014.2320099.
- [48] R. Kumar and T. Amgoth, "Reinforcement learning based connectivity restoration in wireless sensor networks," *Applied Intelligence*, vol. 52, no. 11, pp. 13214–13231, Sep. 2022, doi: 10.1007/s10489-021-03084-w.
- [49] C. Shi, J. Liu, H. Liu, and Y. Chen, "Smart user authentication through actuation of daily activities leveraging WiFi-enabled IoT," in *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Jul. 2017, pp. 1–10, doi: 10.1145/3084041.3084061.
- [50] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016, doi: 10.1109/TNNLS.2015.2404803.
- [51] L. Xiao, Q. Yan, W. Lou, G. Chen, and Y. T. Hou, "Proximity-based security techniques for mobile users in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 2089–2100, Dec. 2013, doi: 10.1109/TIFS.2013.2286269.
- [52] A. Švigelj, A. Hrovat, and T. Javornik, "User-centric proximity estimation using smartphone radio fingerprinting," *Sensors*, vol. 22, no. 15, p. 5609, Jul. 2022, doi: 10.3390/s22155609.
- [53] R. Qamar and B. A. Zardari, "A study of blockchain-based internet of things," *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 1, pp. 15–23, Oct. 2022, doi: 10.52866/ijcsm.2023.01.01.003.
- [54] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for BLE-based devices in the internet of things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018, doi: 10.1109/ACCESS.2018.2799942.

BIOGRAPHIES OF AUTHORS






Mahmood A. Al-Shareeda    obtained his Ph.D. in advanced computer network from University Sains Malaysia (USM). He is currently a postdoctoral fellowship at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include network monitoring, internet of things (IoT), vehicular Ad hoc network (VANET) security, and IPv6 security. He can be contacted at email: alshareeda022@usm.my.






Murtaja Ali Saare    is an assistant professor at the Department of Computer Technology Engineering, Shatt Al-Arab University College, Iraq. He received his master's degree in information technology at Universiti Utara Malaysia (UUM), in 2017. He completed his Ph.D. at School of Computing, Sintok, UUM, Kedah, Malaysia, in 2021. His research interest includes aging and cognition, e-health, and human-centered computing. He has published his research work in reputable indexed journal. He can be contacted at email: mmurtaja88@gmail.com and murtaja.a.sari@sauc.edu.iq.



Selvakumar Manickam    is currently working as an associate professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include cybersecurity, internet of things, industry 4.0, and machine Learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 Ph.Ds. He has 10 years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@usm.my.



Shankar Karuppayah    is received the B.Sc. degree (Hons.) in computer science from Universiti Sains Malaysia, in 2009, the M.Sc. degree in software systems engineering from the King Mongkut's University of Technology North Bangkok (KMUTNB), in 2011, and the Ph.D. degree from TU Darmstadt with his dissertation titled advanced monitoring in P2P Botnets, in 2016. He has been a senior researcher/a postdoctoral researcher with the Telecooperation Group, TU Darmstadt, since July 2019. He has also been a senior lecturer at the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, since 2016. He is currently working actively on several cybersecurity projects and working groups, e.g., the National Research Center for Applied Cybersecurity (ATHENE), formerly known as the Center for Research in Security and Privacy (CRISP). He can be contacted at email: kshankar@usm.my.