A Survey on the Bluetooth 5.0 & 5.1 Standard for the IoT

Hendrik Pfaff
Frankfurt University of Applied Sciences
Faculty of Computer Science and Engineering

***Abstract*—Bluetooth (BT) is a commonly used wireless communication protocol for many interesting Internet of Things (IoT) projects and real world scenarios. In this survey paper we summarise the current state of research and proceedings on the two latest BT versions 5.0 and 5.1. Including newly added functionality such as improved low-power functions, mesh networking, device localisation and found security vulnerabilities. We also work out the four main research topics, BLE functionality, BT mesh networks, device localisation and security. After that we recognises the used research approaches as prototyping in different environments, measuring and evaluating wireless protocols and security analysis. Based on these insights, we classify the research publications into categories and present some of the representative papers.**
In conclusion of this paper we gain an overview of the current research in BT technology and its future developments.

***Index Terms*—Bluetooth, Internet of Things, BLE, Mesh Network, Localisation.**

I. Introduction

In the IoT, the BT wireless communication standard is widely used as a communication protocol between different devices. From headphones over cars to industrial sensors. New BT standards are managed and released by the Bluetooth Special Interest Group (SIG). Early specifications from 1.0 up to 4.2 focused on point-to-point connections between two units. On June 16, 2016 BT version 5.0 was released, implementing new features for its Bluetooth Low Energy (BLE) technology (formerly BT Smart) which was introduced in BT 4.0 [1] and, from July 13, 2017, adopting mesh network capability. [2] The most current version, BT 5.1, got released on January 21, 2019. With it, devices are now locatable via the Angle of Arrival (AoA) and Angle of Departure (AoD) method. The introduction of these features, sparks new applications, possibilities and research fields for the IoT.

In this Survey Paper we analyse the current state of the art in the application and research with BT standard 5.0 and 5.1 for the IoT, by summarising and categorising the most recent papers and publications by their topics and the approach they take.

This survey is structured as follows. In Section II the current Research topics and challenges are introduced. Section III provides an overview on the tools used to approach said challenges while section IV classifies and clusters those approaches into categories. Representative papers and proceedings are introduced in section V. At last, section VI concludes this article and provides a prospect in the future.

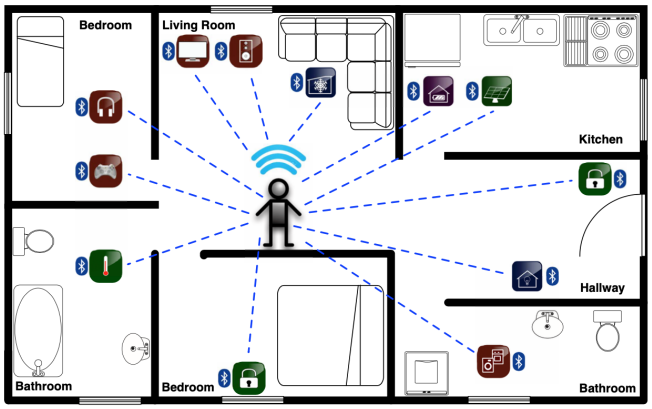

Fig. 1. Possible home automation scenario with BLE. BT connected devices could be implemented in almost every kind of home appliance due to low-energy consumption. Taken from [3].

II. Research topics

With the recently released BT features, as explained in section I, new research topics emerge in IoT. In this section we will present which four topics are the most frequently researched. These topics are BLE, BT mesh networks, device localisation and security. These topics are not purely distinct, as different BT applications and research challenges often use overlapping functionality of the BT protocol and BLE.

The research in BLE technology focuses on the fundamental low-power functions of BT. The goal is often to implement new prototypes and techniques to decrease the power consumption while, at the same time, keeping or increasing the range, speed or throughput for a given application. Reduced power consumption enables devices with internal power supply to last longer, which is a big objective in IoT. The applications reach from wearable technology, eHealth monitoring and wireless sensor networks (WSN) to usage in smart home or smart factory settings. In Fig. 1 we can see a possible smart home scenario with BLE devices.

The research of the BT mesh network standard applies the new mesh network capability released in BT 5.0 as well as

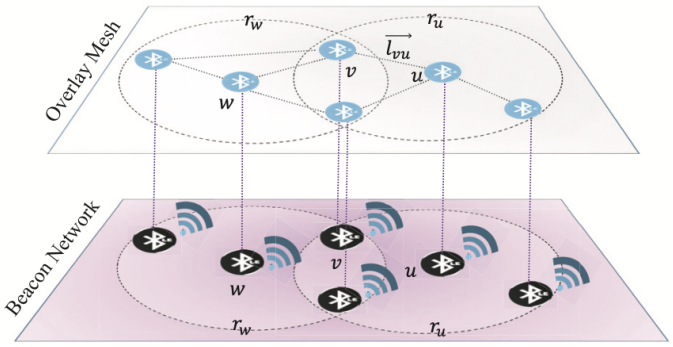

Fig. 2. A new approach of BT mesh networks is the BLE-based Overlay Mesh (BOM). It allows devices, running older BT versions, performing mesh functionality and compatibility with BT 5. Taken from [4]

with alternative approaches. Mesh networks are especially useful in settings where distributed sensors and devices are needed to be highly connected. In combination with BLE functions, WSN with a lot of different IoT devices and in many different contexts can be created.

Device localisation and direction finding with BT, indoors as well as outdoors, has already been researched before the release of BT 5.1. [5] To know the position and / or orientation of a device can offer a valuable context in IoT projects. The newest release provides, with the out of the box support of AoA and AoD, new ways of application and research, as it gets easier to implement and to save energy due to BLE functions.

The research in BT security focuses on hardening BT connections between devices against malicious attacks. Previous versions of the BT protocol have repeatedly been the focus of IT-Security specialists for its vulnerabilities. With the aforementioned newly released features, new potential security threats emerge, as previously impossible attack vectors are created.

III. Tools and Approaches

After we introduced the current main research challenges in section II, we now describe the approaches taken to accomplish their results. There are several ways of doing research in the IoT area. From developing working prototypes, applying new BT technology in testing-setups or real world scenarios, over evaluating and comparing BT functions with its older versions or different wireless protocols up to directly searching and finding security vulnerabilities.

Developing working prototypes with new BT technology focuses on the feasibility in real world applications. Shown in Figure 3 is that different scenario setups are possible. Either controlled testing environments or real world setting with potentially disturbing surroundings. The focus in this

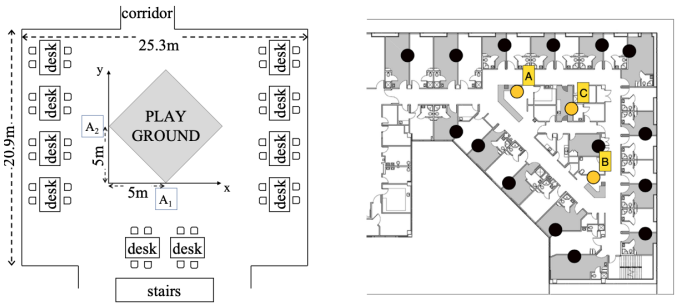

Fig. 3. Different testing-setups for prototyping. Left: Controlled testing environment, with senders on the inside and receivers on the outside. Taken from [6]. Right: Real world hospital (noisy) setting. Taken from [7].

approaches lies on the feasibility of a concept and a possible implementation with BT capable hardware, for the planned use case.

An evaluation approach, on the other hand, has the goal of measuring certain BT properties of already tested implementations to compare them with older BT versions or other protocols. A direct comparison helps to make informed decisions on choosing the right technology for future implementations.

The publications focusing on the security field, either demonstrate vulnerabilities in concrete use cases or techniques for specific attack vectors. Due to legal reasons, non-disclosure agreements with vendors often lead to a delayed publication, after finding a valid exploitation. The results of the research often leads to publicly available software, to enable future work or to test the own network security. The approaches taken in BT security research compare to those in other security related fields. They reach from packet manipulation [6] to comparable brute denial-of-service kind attacks. [8] Classic Man-in-the-middle approaches are, yet a less prominent, taken approach. [9].

IV. Classification

After describing the four main research challenges in section II and the different approaches to tackle them in section III, we can now classify the publications into three different categories of joint characteristics. We can differentiate between lab implementations, real world implementations and theoretical concepts. This helps us to understand how future contributions in this field can be made.

The first category, the lab implementation, is the most common among recent papers. In the lab implementation, first studies of feasibility or evaluation are performed. Future research can build upon its results and extend its context to real world implementations.

Real world implementations build up on prior research to create a minimum viable proof of work within a realistic scenario. In contrast to lab implementations, these settings need to take disturbance and interference, by human

TABLE I
OVERVIEW OF REPRESENTATIVE PAPERS

Title	Category	Research Topic
A fully integrated... [10]	Lab	BLE
Sensors and systems for ... [11]	Lab	BLE
Bluetooth based sensor.. [12]	Lab	BLE
A wearable, low-power,... [13]	Real World	BLE
Experimental performance... [14]	Lab	BLE
From bluetooth low-energy... [15]	Theoretical	BLE
Bluetooth mesh energy... [16]	Lab	Mesh
A novel overlay mesh... [4]	Lab	Mesh
Bluetooth mesh networking... [17]	Lab	Mesh
Mesh networking for iot... [18]	Lab	Mesh
Dead on Arrival: An emperical...[6]	Lab	Localisation
Direction finding capability... [19]	Lab	Localisation
Bluetooth based indoor... [7]	Real World	Localisation
Toxic Friends in your Network... [8]	Lab	Security

interaction or other devices, into account.

Theoretical concepts, as the third category, refrain from building a hardware prototype. Instead they lay the foundation to all future research, by providing new insights and concepts. They are not very common within the current publications.

V. REPRESENTATIVE PAPERS

With the research topics, approaches and classifications, we introduced in sections II, III and IV, we can list representative papers and assign them into the previously introduced categories in this section. A condensed overview of this assignment can be found in table I.

A performance evaluation between BT 4.0 and BT 5.0 on signal strength and throughput, concludes an increased performance of BLE functions in the newer version. A maximum range outdoors *800m* using *9dBm* transmit power with *1.1kbps - 26kbps* throughput, got reached. [14]

To increase the performance of BLE devices even more, new communication modules are constantly being developed. Such as this low-power transceiver to be used in IoT sensors. [10]

A theoretical paper focuses on energy generation in IoT devices. To achieve the objective of making IoT devices self sustainable, it is not enough only reduce the consumption of power. The device has also to make use of ambient energy, and maybe make use of more than one energy resource in the future. [15]

One real world implementation of BLE, is the embedding of a real time ECG within a wearable t-shirt. Due its use of BLE functions for data transfer it runs over 110 hours on a *240mAh* rechargeable battery, with an average power consumption of *5.2mW*. The potential use of webbed in solar panels is currently being researched. [13]

Other implementations of wearable IoT devices, focus on gathering location based, environmental data as well as the medical condition of its wearer. [11]

A study on the use of BT in industrial plants, simulated the feasibility and performance of local data gathering BT sensors connected to the internet via a gateway. It evaluates the BT to gateway access as robust up to a distance of *20m* with a mean latency of *34.96ms*.[12]

For BT mesh networks, one of the most important factors is, again, considered energy consumption. A hardware experiment on a 235 mAh battery-powered device results in a lifetime of *15.6mon*, instead of an asymptotic lifetime of *21.4mon*, while sending data packages every *10s*. [16]

To provide older BT devices with the same mesh functionality and compatibility, the BLE-based Overlay Mesh (BOM) got developed. Figure 2 gives an overview of the BOM. This new approach to mesh networking reduces packet collision rate (PCR) to *66.67%* by using best effort scheduling (BES), while improving packet delivery ratio (PDR) to *52%* by using received signal strength (RSS)-based bounded flooding (RBF). [4]

One possible application is within a smart factory scenario, which is currently being researched. A test setting shows feasibility and the benefits of BT mesh technology over other wireless mesh protocols due its interoperability. [17]

Yet a Master's Thesis on robotics compares the BT Mesh Standard against the Thread network protocol. Several drawbacks of BT (lower throughput, lower message payload, higher package loss) lead to the recommendation of the latter. [18]

The use the novel localisation feature of BT 5.1, is already being researched. With only slight changes in the BLE packet structure and the addition of the so called constant tone extension (CTE)-frame, location finding can be implemented. [19]

The AoA method for indoor device localisation with two receivers already got experimentally analysed. Within a test-setup, it shows an absolute positioning error of under *85cm* in *95%* of cases, while pushing the error under *10cm* in*15%* of cases. [6]

In addition of the built in methods, new algorithm alternatives are still being developed. One, using triplet embeddings through BT connectivity streams, is tested in a hospital scenario under realistic noisy conditions. This approach achieves a mean error of *4.10m*. [7]

The already mentioned localisation functionality in BT

5.1 does not contain any security mechanisms and thus can be targeted by a malicious device. By manipulating the package structure, the measured AoA can be distorted. A change in the usage of the receiving antennas, could prevent this attack, though. [6]

Another new possible vulnerability is the friendship feature, introduced in the BT mesh standard, to reduce the power consumption of a node. With a *denial-of-friendship* attack, outside devices can quickly drain the battery of a selected node. It is also possible to impersonate a befriended node by sniffing and manipulating the, usually unique, 24-Bit sequence number (SEQ). [8]

VI. Conclusion

Concluding from sections II, III, IV and V, the current research on the BT standard focuses on BLE, BT mesh networks, device localisation and protocol security. The overlapping nature of these topics are clear, as BLE functions are widely used in nearly every area. These topics are approached in several ways like, prototyping, evaluation or security analysis. We can classify the current research approaches into the categories lab implementation, real world implementation and theoretical concept.

The research in the BT standard directly contributes to the fields of WSN, smart home / factory scenarios, eHealth and monitoring / wearable technology. In the future, new prototypes and implementations will produce further insights of the feasibility of large BT based wireless IoT networks and how to improve them in aspects like range, power consumption and localisation.
Future BT versions will certainly add new functionality to the protocol, improving the existing functions and address currently known security issues.

References

[1] S. Raza, P. Misra, Z. He, and T. Voigt, "Bluetooth smart: An enabling technology for the internet of things," in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2015, pp. 155–162.

[2] Bluetooth SIG. (2017) Bluetooth LE: mesh. [Online]. Available: https://web.archive.org/web/20170901202951/https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works/le-mesh

[3] M. Collotta, G. Pau, T. Talty, and O. K. Tonguz, "Bluetooth 5: A concrete step forward toward the iot," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 125–131, 2018.

[4] P. C. Ng and J. She, "A novel overlay mesh with bluetooth low energy network," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2019, pp. 1–6.

[5] B. Huang, J. Liu, W. Sun, and F. Yang, "A robust indoor positioning method based on bluetooth low energy with separate channel information," *Sensors*, vol. 19, no. 16, p. 3487, 2019.

[6] M. Cominelli, P. Patras, and F. Gringoli, "Dead on arrival: An empirical study of the bluetooth 5.1 positioning system," in *Proceedings of the 13th International Workshop on Wireless Network Testbeds, Experimental Evaluation & Characterization*. ACM, 2019, pp. 13–20.

[7] K. Mundnich, B. Girault, and S. Narayanan, "Bluetooth based indoor localization using triplet embeddings," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2019, pp. 7570–7574.

[8] F. Álvarez, L. Almon, A.-S. Hahn, and M. Hollick, "Toxic friends in your network: Breaking the bluetooth mesh friendship concept," in *Proceedings of the 5th ACM Workshop on Security Standardisation Research Workshop*. ACM, 2019, pp. 1–12.

[9] C. Robberts and J. Toft, "Finding vulnerabilities in iot devices: Ethical hacking of electronic locks," 2019.

[10] S. J. Kim, D. G. Kim, S. J. Oh, D. S. Lee, Y. G. Pu, K. C. Hwang, Y. Yang, and K. Y. Lee, "A fully integrated bluetooth low-energy transceiver with integrated single pole double throw and power management unit for iot sensors," *Sensors*, vol. 19, no. 10, p. 2420, 2019.

[11] M. A. Al Mamun and M. R. Yuce, "Sensors and systems for wearable environmental monitoring towards iot-enabled applications: A review," *IEEE Sensors Journal*, 2019.

[12] R. N. Gore, H. Kour, M. Gandhi, D. Tandur, and A. Varghese, "Bluetooth based sensor monitoring in industrial iot plants," in *2019 International Conference on Data Science and Communication (IconDSC)*. IEEE, 2019, pp. 1–6.

[13] T. Wu, J.-M. Redouté, and M. Yuce, "A wearable, low-power, real-time ecg monitor for smart t-shirt and iot healthcare applications," in *Advances in Body Area Networks I*. Springer, 2019, pp. 165–173.

[14] H. Karvonen, C. Pomalaza-Ráez, K. Mikhaylov, M. Hämäläinen, and J. Iinatti, "Experimental performance evaluation of ble 4 versus ble 5 in indoors and outdoors scenarios," in *Advances in Body Area Networks I*. Springer, 2019, pp. 235–251.

[15] W. Kruiskamp, "From bluetooth low-energy to bluetooth no-energy: System and circuit aspects of energy harvesting for iot applications," in *Low-Power Analog Techniques, Sensors for Mobile Devices, and Energy Efficient Amplifiers*. Springer, 2019, pp. 13–30.

[16] S. M. Darroudi, R. Caldera-Sànchez, and C. Gomez, "Bluetooth mesh energy consumption: a model," *Sensors*, vol. 19, no. 5, p. 1238, 2019.

[17] T. C. Y. Lam, S. S. L. Yew, and S. L. Keoh, "Bluetooth mesh networking: An enabler of smart factory connectivity and management," in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*. IEEE, 2019, pp. 1–6.

[18] K. F. Pedersen, "Mesh networking for iot-implemented on robots using bluetooth low energy mesh and thread," Master's thesis, NTNU, 2019.

[19] N. B. Suryavanshi, K. V. Reddy, and V. R. Chandrika, "Direction finding capability in bluetooth 5.1 standard," in *International Conference on Ubiquitous Communications and Network Computing*. Springer, 2019, pp. 53–65.