Exploiting Bluetooth Vulnerabilities in e-Health IoT Devices

Mohammed Zubair
Qatar University
Doha, Qatar
mz1808904@qu.edu.qa

Devrim Unal
Qatar University
Doha, Qatar
dunal@qu.edu.qa

Abdulla Al-Ali
Qatar University
Doha, Qatar
abdulla.alali@qu.edu.qa

Abdullatif Shikfa
Qatar University
Doha, Qatar
ashikfa@qu.edu.qa

ABSTRACT

Internet of Things (IoT) is an interconnected network of heterogeneous things through the Internet. The current and next generation of e-health systems are dependent on IoT devices such as wireless medical sensors. One of the most important applications of IoT devices in the medical field is the usage of these smart devices for emergency healthcare. In the current interconnected world, Bluetooth Technology plays a vital role in communication due to its less resource consumption which suits the IoT architecture and design. However Bluetooth technology does not come without security flaws. In this article, we explore various security threats in Bluetooth communication for e-Health systems and present some examples of the attacks that have been performed on e-Health systems by exploiting the identified vulnerabilities

CCS CONCEPTS

• **Wireless Communication** → **Bluetooth**; • **Cybersecurity** → *Exploiting Vulnerabilities*; • **IoT** → e-Health.

KEYWORDS

Bluetooth, Wireless Communication, E-health system, Internet of Things (IoT), Cybersecurity

ACM Reference Format:
Mohammed Zubair, Devrim Unal, Abdulla Al-Ali, and Abdullatif Shikfa. 2019. Exploiting Bluetooth Vulnerabilities in e-Health IoT Devices. In *3rd International Conference on Future Networks and Distributed Systems (ICFNDS '19), July 1–2, 2019, Paris, France.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3341325.3342000

ICFNDS '19, July 1–2, 2019, Paris, France

ACM ISBN 978-1-4503-7163-6/19/07…$15.00
https://doi.org/10.1145/3341325.3342000

1 INTRODUCTION

Internet of Things (IoT) is a self-configuring, adaptive, complex network that interconnects things to the Internet [19]. Researchers predict that the number of connected IoT devices will reach 75 billion by 2025 with major portion in healthcare sector [1]. IoT devices in medical field have various applications such as health monitoring, curing chronic diseases, fitness programs, etc. IoT healthcare devices deliver efficient management of limited resources by ensuring appropriate service and usage for various patients, making them a good choice for the e-Health domain. Health records are generated and delivered on demand services to the authorized personnel by the use of gateways, medical servers and health databases. With the help of IoT devices, data is exchanged between the devices and other networks with a low power consumption and low computational resources. The data exchange is possible by various communication technologies, such as WiFi, Bluetooth, Zigbee, Z-wave, RFID, Near Field Communication (NFC) and ultra-wide bandwidth (UWB). Bluetooth technology is generally preferred in the e-Health market, since it is economical, suitable for use in compact devices and permits ad-hoc connectivity which suits the resource constraints of IoT devices [25]. Bluetooth is a open standard technology, using the unlicensed 2.4GHz signal range for industrial, scientific and medical (ISM) band, for interchanging the information through radio transmission, identifying and connecting the devices. Bluetooth Special Interest Group (SIG) is an elemental instigator of the specification and its services [8]. The introduction of Bluetooth technology in wireless medical sector was in the year 2003. The Bluetooth enabled medical devices has given a innovative direction to the e-Health domain [21]. Some examples of such devices are shown in Figure 1. In the Figure, (a) is a remote sensing Pulse Oximeter which is used for monitoring

oxygen saturation level in patient's body. It consists of wireless sensors which is placed on the patient's body, usually on fingertip or earlobe. This sensor device sends wavelengths in to the patient's body to sense oxygen absorbance. (b) is a wireless Blood Pressure monitoring device which keeps track of blood pressure readings. (c) shows an Electrocardiogram which is used for heart-rate monitoring. This device consists of a sensor, which when placed on patient's body records heartbeat and gives a graph of those readings .

Figure 1: Bluetooth enabled medical devices

At the same time, Bluetooth has become an attack surface to launch various attacks. These attacks can cause serious implications on the health of patients and sometimes, can also threaten life. Most of the research work has been done in identifying vulnerabilities in e-health communication using WiFi and other wireless communication technologies. However, very less research has been done in identifying Bluetooth communication vulnerabilities. The objective of our research is to fill this gap by identifying weakest links in Bluetooth communication. This paper explores Bluetooth communication threats that can be exploited by an adversary. We have performed some Bluetooth attacks on medical IoT devices by exploiting the identified vulnerabilities. To protect the interest of the stakeholders, we will not disclose the make and model of these devices. The organization of the paper is as described below: Section 2 provides an overview and background on the IoT based e-health system architecture and the Bluetooth protocol stack, Section 3 discusses the vulnerabilities of the Bluetooth technology, cyber threats and the Bluetooth attacks performed in our testbed. Finally, the paper is concluded in Section 4 with further research directions.

2 BACKGROUND

The Bluetooth technology is adopted in many application domains such as laptops, cell phones, speakers, medical devices etc. Bluetooth enables medical devices to connect more easily with each other and with the information access points provided by LANs. Bluetooth is widely used in the e-health systems for the Wireless Personal Area Network(WPAN). Devices communicating in a WPAN are prone to less error rates [29]. It facilitates the treatment of patients without consulting to the clinic and also maintains all the critical data of the patient, even when the individual is consulted to more than one clinic [26]. With the aim to identify Bluetooth vulnerabilities in IoT medical devices, we provide information on the e-health system architecture. Figure 2, describes the IoT based health architecture. The architecture comprises of three domains: IoT domain, Multi-cloud storage and User/action domain. In this article, we have focused on Bluetooth communication and its vulnerabilities, which is part of the IoT domain. The IoT domain consists of wireless wearable or implanted medical device which is used for data acquisition of patient and convey the treatment accordingly. In an emergency case of an ambulance, biosensors attached to the patient's body, provide real time vital biofeedback such as body temperature of the patient in the form of alert and recommendations to the staff inside the ambulance [4]. The communication between the patient and the caregiver is carried out by wireless communication technologies such as Bluetooth, WiFi and Near Field Communication (NFC). This results in a heterogeneous scenario which composes of different protocols and modulation schemes, This kind of scenario presents a potentially vulnerable target for an adversary to exploit the system and escalate the privileges [30].

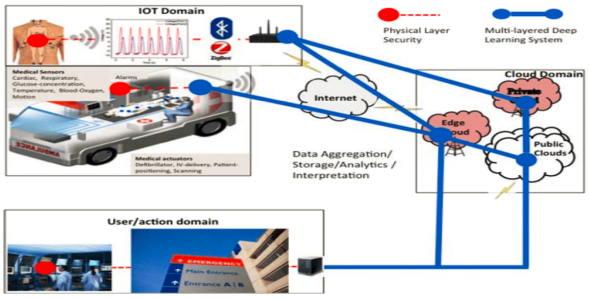

Figure 2: IoT based E-health network architecture

L.M. Ericsson invented Bluetooth technology in the year 1994 [27]. After further developments it was approved by IEEE as the 802.15.1 standard in 2002 as the first version of Bluetooth supporting 768 Kbps. Progressively, now Bluetooth is an important player in the market, with respect to its specifications and data transfer rate that has exceeded upto 50 Mbps in its version 5 [31]. Bluetooth has 3 different classes for various connectivity ranges: Class 1 connectivity range is 100 meters and the permitted power is about 100 mW, Class 2 connectivity range is 10 meters and the permitted power is about 25 mW and Class 3 connectivity range is 1 meter and the permitted power is about 1 mW. The strength of this technology is that it supports both data and audio (i.e, asynchronous and synchronous links) where re-transmission of packets can be done through asynchronous link for error

handling. The network is ad-hoc in nature and is known as a *piconet*, where two or more Bluetooth devices are physically nearest to communicate on the same channel with same frequency hopping sequence. It operates on the unlicensed ISM band at 2.4GHz using advance spectrum frequency hopping technique, the hopping rate is about 1600 hop/sec for full duplex signal. Bluetooth induces wavelengths that are limited to some operating frequencies in a specified range (short range of communication).

However, problems arise if same frequencies are used by many devices, which cause signal interruptions or collisions [28]. In order to avoid and manage this issue, the signals are expanded over wide range of frequencies. So far, various protocols have been adopted in the Bluetooth standards (i.e, TCP/IP stack running over PPP), Bluetooth network encapsulation protocol (BNEP), and object exchange protocol for exchanges (vCalendar and vCard) with IrDA interfaces. Similar to the Internet protocol stack, Bluetooth also have a list of protocols that promote its communication. We will provide a brief overview on the Bluetooth protocol stack in the next subsection.

Bluetooth Protocol Stack

The Bluetooth protocol stack is classified as core specification and profile specification as illustrated in Figure 3 [24]. Core specification, demonstrates the protocols from physical layer to the data link control with its management functions [6]. The profile specification deals with the different protocol and functions, and it delineates how to use Bluetooth technology [7].

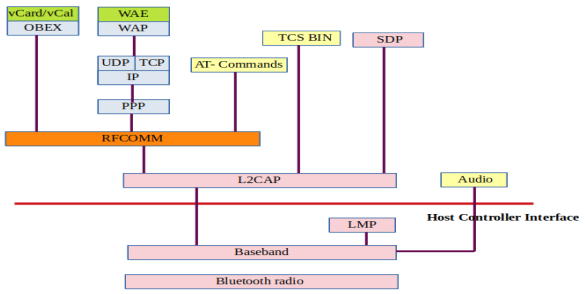

Figure 3: Protocol Stack of Bluetooth

RFCOMM is a serial port emulator/cable replacement protocol and emulates the serial interface RS-232 standard.This allows replacement of the serial cable and enables the operation of distinct applications and protocols. The signalling, establishing and controlling of voice calls and data calls between Bluetooth devices is done by the bit oriented protocol TCS-BIN (Telephony control protocol specification-binary) [18]. The host controllers interface (HCI) links the baseband and L2CAP, to access the hardware, control the register, render the command interface, and to link manager and baseband controller [15].

Now, the protocol stack of Bluetooth will be elaborated for further understanding.

(1) **Bluetooth Radio Layer:** Carrier frequencies and output power are defined in this layer. For transmission, frequency hopping, time-division duplex scheme and Gaussian Frequency Shift Keying (GFSK) form modulation is used at the hopping rate 1600 hops/sec [5]. Each slot is defined as the time difference between two hops.

(2) **Baseband layer:** This layer defines not only physical links and packet format but also perform frequency hopping and interference mitigation [14]. Time Division Duplex (TDD) is used for the transmission directions. Bluetooth packets at baseband layer consist of following three sections:
- Access code: The packet partition is used for time synchronization and piconet identification
- Packet header: It consists of packet type, packet flow control, error control, address and checksum. Packet header protection is done by a header checksum with Forward Error Correction(FEC)[13]. Since, it holds valuable link and survive bit error.
- Payload: The structure of the payload field is depend on the type of link that is being used and usually, its size is upto 343 bytes.

(3) **Physical Link:** Physical links are of two types of: Synchronous Connection-oriented Link (SCO) and Asynchronous Connectionless Link(ACL).

(a) Synchronous connection-oriented link (SCO): In this link the master device fixes two consecutive slots at fixed interval of times. Three SCO links are supported by master device for the same or different slave device. Two links are supported by a slave to enable connection to different masters and up to three links are allowed from the same master device. Various Forward Error Correction (FEC) schemes can be applied for increasing the data amount depending upon the channel error rate. Re-transmission of voice over data cannot be done in SCO link. A robust technique, continuous variable slope delta (CVSD) is applied for voice encoding to ensure the security of the data [12].

(b) Asynchronous connectionless link (ACL):In this link type, a polling scheme is adopted by the master device and slave devices are addressed in the priority slots. Only one link is generated between a master and slave. Data transmission is carried out by various slots packets. Usually, in noisy environment, packet

protection is accomplished by FEC schemes with high link error rate and overhead too. Hence, Bluetooth proposed a fast repeat request (ARQ) scheme for error free and efficient data transmission [12].

(4) **Link Manager Protocol (LMP):** This protocol enhances the baseband functionality and covers Authentication, Encryption and many other functions. During piconet establishment the device begins inquiring by broadcasting an inquiry access code(IAC) to 32 wake-up carriers. Standby devices sniff the IAC messages periodically on the wake-up carrier and enter the inquiry mode. By setting up a piconet, the master is able to communicate after identifying the device. The special hopping sequence is calculated by master based on address received by the devices and in return synchronizes with the master clock, finally the devices enters the fully-connected states [22].
The connection states are categorized as Active state and the Low power states. In the Active state, the slave listens, transmits and receives by participating in the piconet. ACL and SCO links can be used for this purpose. All devices in the active state must have a 3-bit active member address (AMA). Bluetooth devices gets into the low power state for less power or battery consumption. Low power state is further classified into three, namely: Sniff, Hold and Park states.

(5) **L2CAP:** The logical link control and adaption protocol(L2CAP) which creates logical channels between various Bluetooth devices with Quality of Service (QoS) properties. Three different types of logical channels can be established between master and slave: **Connectionless, Connection-oriented and signalling**. Each channel has its own identity (channel identifier) CID. CID 1 value used for signaling channel, CID value 2 is reserved for connectionless channel. Connection oriented channel has a unique CID value greater than 64 which is dynamically assigned for each channel to recognize the connections uniquely. The CID from 3 to 63 are reserved. Connectionless Protocol Data Units (PDUs) is a protocol/service that provides segmentation and reassembling function.

(6) **Service Discovery Protocol(SDP):** It defines the new services in the radio proximity of the Bluetooth. It only discovers services not their usages. SDP server has to be installed on the device for offering services to the rest of the devices as a SDP client. Service records are maintained about the services and service attributes are identified by 32- bit service record handle, consisting of attribute value and ID. The attribute value can be defined as integer UUID, a string, a URL.

3 BLUETOOTH ATTACKS

We will explore some of the existing attacks on Bluetooth that could be used to target medical IoT devices in this section. Compromising of Bluetooth enabled devices and accessing the sensitive data of the user without authorization could be achieved by attackers through exploiting the vulnerabilities in Bluetooth stack implementation. The vulnerabilities in Bluetooth architecture itself presents the weakest link which gives ways to compromise the security of communication between devices [16].

The Bluetooth security posture is different in each version of the standard and device driver software versions, some of the vulnerabilities are constantly fixed in the newer versions of the driver software.

In Bluetooth Version 4.0 there are numerous authentication challenge, which allows the attacker to get the detailed information and to get the access on secret link keys. Moreover, the cipher function is also weak in this version[17]. Whereas, Bluetooth poses vulnerabilities in all versions, but zero-day attacks are emerging everyday. In the section below, we investigate some of the most significant attacks against IoT devices using Bluetooth.

Possible Attacks

- Blue smacking: This attack is comes under the category of "Denial of Service (DoS)" attack and "Ping of Death attack" is also a "DoS attack". Which overflow and burden the devices with redundant and random packets approximately 600 bytes and multiple L2CAP echo requests causing the device to crash [11].
- Blue snarfing: With this attack, the information can be stolen from wireless device through a Bluetooth connection. An adversary makes a link by exploiting OBEX file transfer protocol [9] and collects all data from the device.
- Bluejacking: In this attack, the attacker send multiple illegitimate and irrelevant messages to Bluetooth-enabled devices to manoeuvre the user into using an access code allowing the attacker to access the target files without the users' knowledge [23].
- Blue bugging: Remotely accessible the Bluetooth enabled devices and using its features without the consent of authorized user [23]. The attacker gets the access and take over the RFCOMM protocol control through the AT commands to fully control the device.
- Blue Printing: This attack collects general information of the Bluetooth enabled device such as manufacturer details, device information and firmware [9].
- Mac spoofing attack: In this attack the attacker intercepts the data intended for other Bluetooth enabled

devices by using an attacker Bluetooth device in the medium of communication [23].

- MITM/Impersonation attack: Modifying data between Bluetooth devices while communicating in a piconet is categorized as Man In the Middle (MITM) or an Impersonating attack [**?**]. The attacker disconnects the connection between original communicators and establishes connection with both of them using his device.

The Attacking Testbed

We have performed some real-time attacks by using Bluetooth as a communication medium between IoT medical devices. When the data of the patient is extracted from the medical sensors through medical devices, this data is transmitted over Bluetooth Version 4.0 to the Electronic Patient Control record where the complete activity logs of a patient is diagnosed, monitored and recorded. The following steps provides details on tools and testing ways by which we analyzed the packets, explored Bluetooth communication to identify vulnerabilities and to perform real-time attacks.

- Patient health record is maintained on Windows environment with built-in Bluetooth adapter.
- Attacking node Linux with built-in Bluetooth adapter. Figure 4 shows the attacking Testbed.
- Attacking Tools : **Ubertooth One** This is an open source platform consisting of hardware and software packages, it is an eavesdropping tool and is used to monitor the Bluetooth traffic [2] [3]. This device suite includes several tools, one of those is spectrum analyzer to analyze the traffic in the 2.4 GHz frequency range and is also used for penetration testing [10].

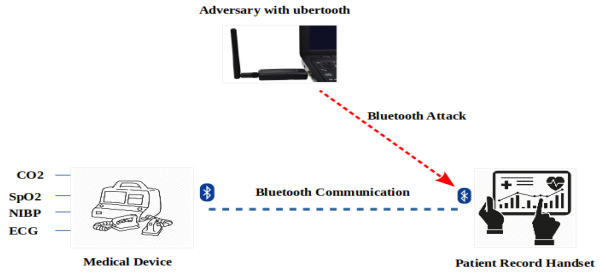

Figure 4: Attack Testbed

- We used various tools such as *Wireshark and hcidump* to analyze the Bluetooth packets, *hcitool* to scan the discoverable devices and to handle the configuration of Bluetooth connection and to provide special commands for the Bluetooth devices. In case of the non-discoverable device, it can be identified using *RedFang* tool. In non-discoverable mode a device must set to the exact hopping pattern to communicate with the BD-ADDR and response to direct name and services requested by inquiry request [32].
- Every Bluetooth entity have its own identity (i.e, BD-ADDR which is similar to MAC address) which can be spot out on the networks. By using command "hciconfig" in hcictool, it easy to identify the BD-ADDR of the devices. The "hciconfig" command reveals the information of the Bluetooth device, build-in adapter including name and class [20]. In addition to these operations, "hciconfig" perform various functions such as to "enable/disable" the encryption or authentication and "activate/deactivate" the Bluetooth devices.

Attacks Performed

We have performed sniffing of Bluetooth packets and BlueSmack attack on patient record collecting device with a Bluetooth V4. The attack performance and analysis is shown in the following graph below.

(1) Packet Sniffing:
In our approach, we used Ubertooth tool for spectrum analyzer and to monitor Bluetooth traffic between the devices. By running the command *hcitool scan* to find all the devices which are using Bluetooth. With the help of Ubertooth we captured the packets of all channels during random frequency hops among channels. Capturing encrypted packets in the process of pairing between Master and slave devices is difficult to be achieved due to the security and privacy settings of frequency hopping technique.
Additionally, using *Sdptool*, useful information such as open ports, various service versions, voice data and channel details are gathered. This is the easiest way of collecting information and services rendered for the target.

(2) Bluesmack:
This attack can be performed in two ways, by using Websploit framework tool and L2CAP echo request it is a particular case of DoS attack. DoS is a general category of attacks that aim at interrupting the service which is performed based on IP. To perform this attack, L2CAP echo ping command of high packet size is used. In our experiment we have used 600 bytes packet size. Usually, this is the maximum input buffer of fixed length in these devices. Due to which, the input buffer is overflowed leading to segmentation faults and finally the device gets down. We have shown the graph of the attack scenario and normal packet transmission in Figure 5.

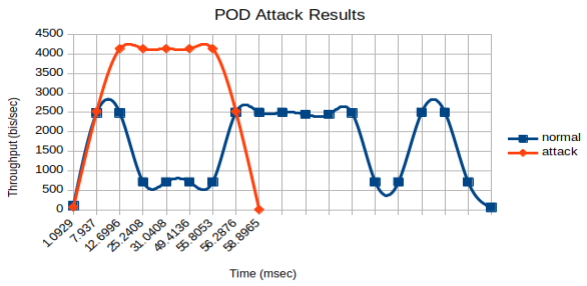

Figure 5: POD Attack Graph

The graph represents normal communication against the attack scenario. Here, the data packets of attack and normal scenarios are considered with respect to the random time interval. Thus, we infer from the graph, that sending a enormous number of packets at a time can disrupt the whole system.

4 CONCLUSION

This paper has explored various attack scenarios in the current Bluetooth architecture of medical IoT devices. Fixing the vulnerabilities in Bluetooth communication is predominantly important as implications of such attacks can be devastating in e-heath system. This paper confirms the need to re-investigate the Bluetooth architecture, its vulnerabilities and attacking scenarios in medical IoT devices. In future, we aim to identify further vulnerabilities, and to propose detection and mitigation techniques to implement a secure data and communication solution for the e-Health domain.

5 ACKNOWLEDGMENT

This publication was made possible by NPRP grant **NPRP10-0125-170250** from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] Antar Shaddad Abdul-Qawy, PJ Pramod, E Magesh, and T Srinivasulu. 2015. The Internet of Things (IoT): An Overview. *International Journal of engineering Research and Applications* 1, 5 (2015), 71–82.

[2] Wahhab Albazrqaoe. 2018. *Capturing Bluetooth Traffic in the Wild: Practical Systems and Privacy Implications.* Michigan State University. Computer Science.

[3] Wahhab Albazrqaoe, Jun Huang, and Guoliang Xing. 2019. A Practical Bluetooth Traffic Sniffing System: Design, Implementation, and Countermeasure. *IEEE/ACM Transactions on Networking* 27, 1 (2019), 71–84.

[4] Basem Almadani, Manaf Bin-Yahya, and Elhadi M Shakshuki. 2015. E-AMBULANCE: real-time integration platform for heterogeneous medical telemetry system. *Procedia Computer Science* 63 (2015), 400–407.

[5] Chatschik Bisdikian et al. 2001. An overview of the Bluetooth wireless technology. *IEEE Commun Mag* 39, 12 (2001), 86–94.

[6] SIG Bluetooth. 2001. Specification of the Bluetooth System, Volume 1, Core. Version 1.1.

[7] SIG Bluetooth. 2001. Specification of the Bluetooth System, Volume 2, Profiles. Version 1.1.

[8] Raffaele Bruno, Marco Conti, and Enrico Gregori. 2002. Traffic Integration in Personal, Local, and Geographical Wireless Networks. *Handbook of Wireless Networks and Mobile Computing* (2002), 145.

[9] Peter Cope, Joseph Campbell, and Thaier Hayajneh. 2017. An investigation of Bluetooth security vulnerabilities. In *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC).* IEEE, 1–7.

[10] Peter Cope, Joseph Campbell, and Thaier Hayajneh. 2017. An investigation of Bluetooth security vulnerabilities. In *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC).* IEEE, 1–7.

[11] Joshua Franklin, Christopher Brown, Spike Dog, Neil McNab, Sharon Voss-Northrop, Michael Peck, and Bart Stidham. 2016. *Assessing Threats to Mobile Devices & Infrastructure: the Mobile Threat Catalogue.* Technical Report. National Institute of Standards and Technology.

[12] Jaap Haartsen. 1998. Bluetooth-The universal radio interface for ad hoc, wireless connectivity. *Ericsson review* 3, 1 (1998), 110–117.

[13] Jaap Haartsen, Mahmoud Naghshineh, Jon Inouye, Olaf J Joeressen, and Warren Allen. 1998. Bluetooth: Vision, goals, and architecture. *ACM SIGMOBILE Mobile Computing and Communications Review* 2, 4 (1998), 38–45.

[14] Jaap C Haartsen. 2003. Bluetooth radio system. *Wiley Encyclopedia of Telecommunications* (2003).

[15] Yanxia Liu, Shufen Li, and Liting Cao. 2009. Application of bluetooth communication in digital photo frame. In *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, Vol. 4. IEEE, 370–373.

[16] Angela Lonzetta, Peter Cope, Joseph Campbell, Bassam Mohd, and Thaier Hayajneh. 2018. Security vulnerabilities in Bluetooth technology as used in IoT. *Journal of Sensor and Actuator Networks* 7, 3 (2018), 28.

[17] Angela Lonzetta, Peter Cope, Joseph Campbell, Bassam Mohd, and Thaier Hayajneh. 2018. Security vulnerabilities in Bluetooth technology as used in IoT. *Journal of Sensor and Actuator Networks* 7, 3 (2018), 28.

[18] Brent A Miller and Chatschik Bisdikian. 2001. *Bluetooth revealed: the insider's guide to an open specification for global wireless communication.* Prentice Hall PTR.

[19] Roberto Minerva, Abyi Biru, and Domenico Rotondi. 2015. Towards a definition of the Internet of Things (IoT). *IEEE Internet Initiative* 1 (2015), 1–86.

[20] Robayet Nasim. 2012. Security threats analysis in Bluetooth-enabled mobile devices. *arXiv preprint arXiv:1206.1482* (2012).

[21] Len Ott. 2010. The Evolution of Bluetooth® in Wireless Medical Devices. *Socket Mobile, Inc. White Papers* (2010).

[22] Arto Palin, Juha Salokannel, and Jukka Reunamaki. 2008. Method and system for establishing a wireless communications link. US Patent 7,352,998.

[23] Trapti Pandey and Pratha Khare. 2017. Bluetooth hacking and its Prevention. *L & T Technology Services. Available online: http://www.larsentoubro. com/media/27618/bluetooth-hacking-and-its-prevention-2014. pdf (accessed on 1 April 2016)* (2017).

[24] Neungsoo Park, Bijoy Kumar Mandal, and Young-Ho Park. 2013. Sensor Protocol for Roaming Bluetooth Multiagent Systems. *International Journal of Distributed Sensor Networks* 9, 4 (2013), 963508.

[25] Heloise Pieterse and Martin S Olivier. 2014. Bluetooth command and control channel. *Computers & Security* 45 (2014), 75–83.

[26] Heloise Pieterse and Martin S Olivier. 2014. Bluetooth command and control channel. *Computers & Security* 45 (2014), 75–83.

[27] DB Popoviæ, D Bojaniæ, N Jorgovanoviæ, S Dosen, and R Petroviæ. 2003. TeleECG based on Bluetooth transceivers. In *Telecommunications Forum TELFOR*, Vol. 20.

[28] UL Muhammed Rijah, S Mosharani, S Amuthapriya, MMM Mufthas, Malikberdi Hezretov, and Dhishan Dhammearatchi. 2016. Bluetooth security analysis and solution. *International Journal of Scientific and Research Publications* 6, 4 (2016), 333–338.

[29] William E Saltzstein. 2002. BLUETOOTH: THE FUTURE OF WIRELESS TECHNOLOGY? *MEDICAL DEVICE AND DIAGNOSTIC INDUSTRY* 24, 2 (2002), 44–53.

[30] Aliya Tabasum, Zeineb Safi, Wadha AlKhater, and Abdullatif Shikfa. 2018. Cybersecurity Issues in Implanted Medical Devices. In *2018 International Conference on Computer and Applications (ICCA)*. IEEE, 1–9.

[31] NIDAL M Turab. 2018. IoT wireless home automation technologies and their relation to specific absorption rate. *Journal of Theoretical and Applied Information Technology* 96, 14 (2018), 4597–4609.

[32] Lih Wern Wong. 2005. Potential Bluetooth Vulnerabilities in Smartphones.. In *AISM*. Citeseer, 123–132.