International Journal of Scientific Research in Multidisciplinary Studies **Research Paper**
Vol.7, Issue.7, pp.58-63, July (2021) **E-ISSN:** 2454-9312 **P-ISSN:** 2454-6143

Bluetooth: Enabling Technology for IoT, Security issues and solutions

Zahoor Ahmad Najar[1*], Roohe Naaz Mir[2]

[1]Department of Information Technology, Central University of Kashmir, Srinagar, India
[2]Department of Computer Science and Engineering, National Institute of Technology, Srinagar, India

[*]*Corresponding Author: zahoornajar@cukashmir.ac.in Tel.: +91700656362*

Available online at: www.isroset.org

Received: 02/Feb/2021, Accepted: 11/Feb/2021, Online: 31/Jul/2021

***Abstract*—** Internet of things(IoT) a ubiquitous network, an interconnecting large number of devices roughly to stretch 1.1 trillion by 2026. The number of devices or things is increasing per person, and an average of 5 devices per user will be in use and actively connected to the Internet. However, an exponential increase in the number of devices nearly automates everything around us because of the technology available. The communication technology involved has a significant role in realizing IoT networks. In particular, wireless communication technology has helped to accomplish the IoT concept because of no overhead of wires. In wireless communication technology, several standards are available, e.g., Wi-Fi, Zigbee, Bluetooth, RFID, etc. All the standards used have their utility and use, as per their specification, capability, and energy consumption. In this paper, we discuss the use and importance of Bluetooth Technology in IoT and address security loopholes associated with it to prevent such vulnerability. References to the literature and mathematical symbols/equations should not be included.

Keywords— Bluetooth, Wi-Fi, IoT, Security

I. INTRODUCTION

Internet of things, a pervasive network of devices of varying standards and description, is the only way forward in the present world to approximately reach 1.1 trillion by 2026. As per data available, 80% of the surveyed organization have adopted IoT and are achieving better results. It is estimated that by 2025, 152200 devices will be connected to the Internet every minute. IoT healthcare is anticipated to reach $14 billion by 2024. According to Ericsson, cellular Growth in IoT would contribute to 3.5 billion connections by 2023, with an anticipated annual growth of 30%.

According to a survey conducted across 11 countries, Executives 94% of the organization has digital transformation as their top strategic initiative.
The digital transformation is the outcome of the other supportive technologies like smart devices and communication technologies available. The IoT ranges from industry, Government, Health care, Home/ office, and personnel use. In IoT, communication technology is critical to address privacy, reliability, and usability. IoT demands free movement of the devices, so everything cannot be connected through wires.

For the Internet of Things, wireless communication technologies are a suitable option, and significant wireless communication technologies are Bluetooth, RFID, Zigbee, and Wi-Fi. To realize IoT networks, we need to implement different communication technologies for energy-efficient and reliable systems. This paper will briefly discuss all the mentioned technology; however, we will explore Bluetooth technology because it enables technology to be used in such networks.

Wi-Fi:
Wireless Fidelity, commonly known as Wi-Fi, is the most reliable way to connect the number of devices in the home or office. As per the IEEE 802.11x standard, a convenient choice for IoT home networks. Wi-Fi technology delivers a certain level of security to connect smart devices. However, this technology is more power-hungry [1],[2] than Bluetooth, RFID, and Zigbee. Wi-Fi suits better for the smart devices which can directly be connected to IoT with their IP addresses with longer battery life, with a coverage area ranging from 35meters(indoor) to 90 meters(outdoor) in 2.4 GHz

Zigbee
ZigBee is the IEEE 802.15.4 standard developed by ZigBee Alliance for controlling and monitoring limited range networks. It is used in Home Automation, controlling appliances due to low data rate and limited range. It supports a wide range of network topologies. In ZigBee, the communication is Master/Slave architecture wherein a slave is active during communication and sleeps the rest of the time, so battery life is longer [1],[2]. ZigBee technology comes with features like security, scalability, and better performance. The only drawback of this technology is low data rates.
RF (Radio Frequency)

An IEEE C95.1-2005 standard with Radio Frequency ranges from 100m to 1Km depends on the transmission power and antenna used as the enabling technologies for IoT networks. It only suits some applications of IoT. RFID devices can be both active and passive, depending upon the application of the RFID device; being Energy-efficient and low cost, it is preferably used for object identification. But due to passive components, which are part of the technology, it is vulnerable to several security threats. Data rates up to 1 Mbps are too low and need an Internet-enabled gateway to be part of the IoT network. NO TCP/IP-related protocol is implemented in RF communication modules. And RFID devices used for IoT have a limited range of 3 meters[3].

Bluetooth

Bluetooth is a low-cost and short-range communication standard defined by IEEE 802.15.1 standard with mobility support. Operating distance for Bluetooth devices ranges from 10m to 100m[4]. It operates in the ISM band (2.4GHz), which is a license-free band. It supports an aggregate data rate of up to 1 Mbps, also known as Basic Rate (BR). Bluetooth version 3, a traditional Bluetooth standard, consumes more power than its new versions 4 and 5, supporting data rates up to 3 Mbps, also known as Enhanced Data Rate (EDR) a throughput of approximately 2.1Mbps. Bluetooth version 4 was introduced as Bluetooth Low Energy (BLE), with a low data rate limited to 1 Mbps. And version 5 of the BLEs was introduced with data rates 2 Mbps, 1Mbps, 500kbps, and 125 kbps for varied ranges. Low data rate transmission is to accommodate the sensors that have to send a small amount of data but 240 m.

The scope of our paper is limited to Bluetooth communication technology. In the subsequent sections, we only explore the Bluetooth protocol stack and vulnerability and the solution.

Bluetooth Protocol Stack

Bluetooth protocol stack, like other protocol stacks, describes the communication of devices using Bluetooth technology. Fig 1 shows the Bluetooth architecture [5]. Bluetooth technology allows devices to establish an Adhoc network. Bluetooth specification provides separation functioning of host and Controller. The host is meant for higher layer protocols such as Logical Link Control, Adaptation Protocol (L2CAP), and Service Discovery Protocol(SDP). The controller functions are embedded in microchips either as integrated or external(USB) Bluetooth Adapter. The host and Controller communicate using standard communication over a Host Controller Interface (HCI). In some instances, Host and Controller functions are available on a single device. Bluetooth piconet allows up to 7 devices connected to Master/Slave Configuration, and inBLE, an unlimited number of slaves, can be connected to the network. Although in a piconet, only one device can act as a Master and others as a slave. However, Time-division Multiplexing allows one slave device to act as Mater for the

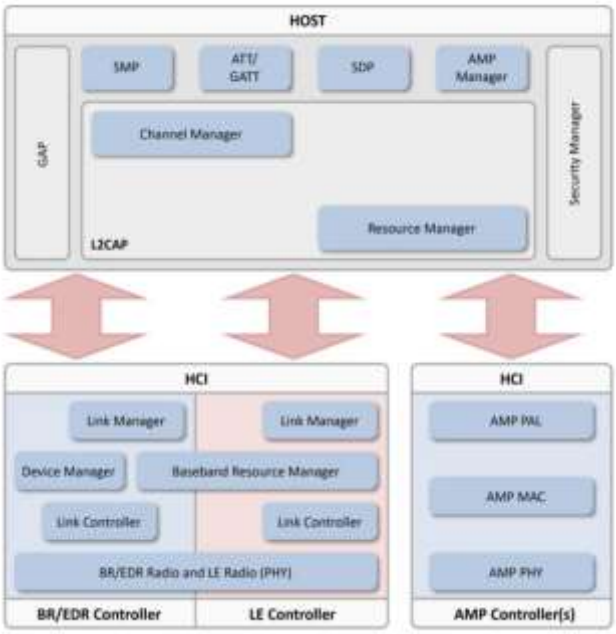

Figure 1:Bluetooth Architecture v 4

other piconets simultaneously, thus creating a chain of piconets called scatternet. This feature adds vulnerability to the devices, which are security issues in IoT.

1. BLUETOOTH SECURITY

Security services specified in Bluetooth standard are as follows;

1 **Authentication**: this includes verifying a device based on Bluetooth device address or link keys.

2 **Authorization:** granting or denying device access to use a particular resource.

3. **Confidentiality:** prevents information eavesdropping and compromised by using encryption schemes so that only authorized devices can access the data.

Bluetooth standard supports four security modes of connection to other devices as follows:

Security mode 1 (Non-Secure Mode):

In this mode, no security features in place, and devices do not employ any secure mechanism for other Bluetooth devices to connect to the device.

Security Mode 2 (service level enforced security mode):

In this mode, security procedures are initiated after link establishment but before logical channel establishment. In this mode, a centralized security manager keeps policies for access control with devices and other protocols. In this mode, partial access is granted to services while restricting other services for a device. The Controller executes the Authentication and encryption mechanism.

Security Mode 3 (Link Level enforced security mode) :

In this mode, before establishing the Physical Link, security procedures are initiated. This mode must provide Authentication and encryption to and fro from the devices. In this mode, authorization at the service level is taking place once the device is authenticated.

Security Mode 4 (Service level enforced security mode): this mode is similar to security mode 2 w after physical and logical link setup security procedure is initiated. This mode uses Secure Simple Pairing(SSP), in which the elliptical curve Diffie Hellman (ECDH) key agreement replaces the legacy key agreement of link key generation. SSP offers four association models, which are as follows:

Numeric Comparison:
In this association model, Bluetooth nodes are associated by displaying a six-digit number with the option of pair or not pair. The Pairing code is displayed on the display screen, thereby allowing users to pair or not to pair with other Bluetooth devices. The advantage of this association is the matching Key needs not to enter, and hence eavesdropper cannot use the Key even if captured.

Passkey Entry:
This association model is used for the devices where one device can enter the Pin, and another device is only capable of displays the Pin. This Pin gets associated with link key generation and hence is of no use to eavesdroppers.

Just Works:
This association model is intended for the scenario wherein one pairing device has no keyboard or a display for entering the Passcode Digits (Bluetooth mouse dongle). It completes Authentication similar to that of numeric Comparison. However, it is vulnerable to different attacks.

Out of Band:
This mode is designed for devices that support additional universal wireless or wired technology. Communication is allowed by simply tapping the devices against each other

The authentication process, initiated with a challenge-response mechanism in which one device acts as a claimant, and others as a verifier, validates the claimant. The Authentication gets completed in the following steps:
The verifier transmits a random challenge of 128 bits to the claimant.

The claimant uses his/her 48-bit device Address, link key, and Random Challenge an input to compute the authentication response using Safer and Secure Encryption Routine. Verifier performs the similar calculation, and only 32 most significant bits of authentication response is used for authentication purpose. The remaining 96 bit of the 128-bit output is used to create a Bluetooth encryption key, termed Authenticated Cipher offset(ACO).
The claimant returns the 32 most significant bits of the authentication response as the computed response called the signed response(SRES) to the verifier.
The verifier compares the SRES from the claimant with the value that it computes.
If the 32-bit values are equal, the Authentication is successful; otherwise, Authentication fails.

The above steps perform one-way Authentication, and if the same process gets reiterated with verifier and claimant switching their roles, mutual Authentication is attained.
In addition to security modes for Authentication and pairing, Bluetooth also provides confidentiality services.

II. RELATED WORK

In all the related works that other researchers have done, link keys based on unit keys are static and reused for every pairing, which is a significant critical vulnerability. Security mode 1 discussed above is the most insecure. Short PINs, used for pairing the devices, are also a vulnerability. Since the encryption key depends on the link key, random number, and clock, and if a connection continues for more than 24 hours, the clock value will start to repeat. Hence can generate a duplicate keystream. One way the authentication process is susceptible to Man in The Middle Attack(MITM)[6].

Bluetooth technology is susceptible to many threats, which are as follows
Denial of Service(DoS) Attack: Bluetooth is subject to the DoS attack in many ways. Especially in IoT, the long connectivity sessions of Bluetooth devices need to be power efficient and with limited security features associated with adversary devices. Hence, the battery can be drained and can be prevalent in the IoT Home scenario wherein devices of One Home are in the range of another home. DoS attacks can be carried in several ways. When pairing, an adversary may try to connect to the device even if he does not have the pairing code, thereby draining the battery resource [7].

Bluebugging: Blue bugging is an attack wherein using commands, the device gets controlled without the knowledge of its owner, thereby can access the mobile devices of the user for phone calls, emails, and other private communications. Since this vulnerability exists in old Bluetooth devices, upgrading the equipment can fix the issue.

Bluejacking: Bluejacking is an attack carried by the attacker on cell phones with enabled Bluetooth by sending some messages that require the user's response, based on the reaction, thereby permitting the malicious code to execute malicious activity on the user's mobile.

BlueSnarfing: Bluesnarfing is an attack carried by exploiting the Bluetooth firmware wherein connection is forced to a Bluetooth device and allows the adversary to access the data stored in the mobile phone, including its International Mobile Equipment Identity(IMEI). An attacker can route all incoming calls from the user device to the attacker's device by using IMEI [8].

Pairing Eavesdropping:
Pairing in Bluetooth devices is susceptible to eavesdropping. The adversary can collect the pairing frame to determine the secret key (s), facilitating

impersonation and data encryption or decryption of the information on the go.

Secure Simple Pairing Attack :
A device can claim to have no input/ output capabilities. Therefore, it can force the device to connect using the Just works model and then exploits its lack of Man In The Middle Attack potential.

Fuzzy Attacks:
The fuzzy attack is executed by sending the non-standard data or distorted data to check the behavior of the Bluetooth connection, and if the link slows down or data rates changes, hence can be exploited to attack the Bluetooth connection.

Car Whisperer:
"Car Whisperer is a software tool developed by European security researchers that exploit a key implementation issue in hands-free Bluetooth car kits. Car whisperer software allows the attacker to send audio to car speakers and receive audio from the microphone". Since in IoT, voice commands are intended to drive the system, which, if compromised, can be harmful to such systems [9].

Health care Device Hacks: The Internet of things(IoT) is revolutionizing the health care system, especially the diseases which require timely attention from the medical practitioner and possible diagnosis of conditions like Heart Attack, Stroke, e.tc. But the devices wearable to gather information regarding the health-related data of a person use Bluetooth technology one or another way since the limited security feature can be misused to prove harmful for the patients.

Blueborne :
Blueborne is a vulnerability discovered in mobile, desktop, and IoT operating systems, including Andriod, iOS, Linux, and Windows operating systems. Blueborne attack is one of the dangerous attacks that can be carried out without the user's knowledge[10].

Btlejacking: Btlejacking is a new form of Bluetooth attack vector that allows an attacker to jam and take over Bluetooth Low Energy(BLE) devices.[10]

Bleeding bit: Bleeding bit is a defect in Bluetooth chips wherein malicious code can reside in chip memory and be remotely executed and send broadcast messages stored on the vulnerable chip. As long as the BLE is on, the malicious message can trigger an overflow of the critical memory and allows the adversary to create back doors for remote execution of the code.

Key Negotiation of Bluetooth(KNoB) attack: In KNoB attack, the firmware of the Bluetooth chip is targeted, wherein the encryption key negotiation protocol is vulnerable. Bluetooth devices use Encryption key negotiation protocol to approve the entropy of the link-layer encryption key, and all versions of Bluetooth standard uses entropy values from 1 to 16 bytes. Two devices negotiate using the negotiation key protocol by choosing the entropy value between 1 to 16. The other may lower the entropy value by asking the other device to accept it or reduce it further or abort the negotiation. Since the negotiation is carried over link Manager Protocol(LMP), it is neither authenticated nor encrypted. The lower entropy values can be easily compromised with the brute force technique and hence decrypt, eavesdrop the Bluetooth communication without being detected [11].

III. PROPOSED METHODOLOGY

Although in Bluetooth, four different security modes are available for authorization and authentication services. For Adhoc connections device-to-device communication, any of the security modes can be employed. However, for IoT Home scenarios, such security modes cannot be trusted as several vulnerabilities are listed above. We propose a framework for Bluetooth devices to be part of the IoT home network with centralized control. Where in Bluetooth devices to be used for IoT, Home or IoT office need to be registered with the controlling devices manually, thereby creating a signature of each device on that network. However, the full range of Bluetooth devices and their functionality sometimes limit the user to use the best security mode for Authentication and authorization. Using the central controlling device for such communication will surely enhance the security feature of Bluetooth communication among IoT devices. The registration of the devices wherein there is no provision for the pairing code to be entered or verified by the user, e.g., Bluetooth headphone. But due to the capability of such devices to get associated with any other device without any prior authentication. The following are the requirements that very Bluetooth devices must possess regardless of the capability and functionality.

1. All devices must come with a random pairing key of 256 bits or more as a key for initial registration with the system, as shown in fig 2.
2. That random key is required when pairing or associating the device with the Controller (SDN).
3. After registering it with the Controller, a Hash code of 512 bit is calculated from the pairing code and MAC id of the device. The hash thus calculated is to be mapped with the device Mac Id. which later can be associated with the key, to be used by the Controller for Authentication of the same device, for future communication.
4. The association of any such device to the network must send the packet for association with the MAC id. It must prompt the user for the pairing code, which must be equal to the Hash code generated at registration time after the hashing. If the hash is equal, then the only device can communicate from the network.

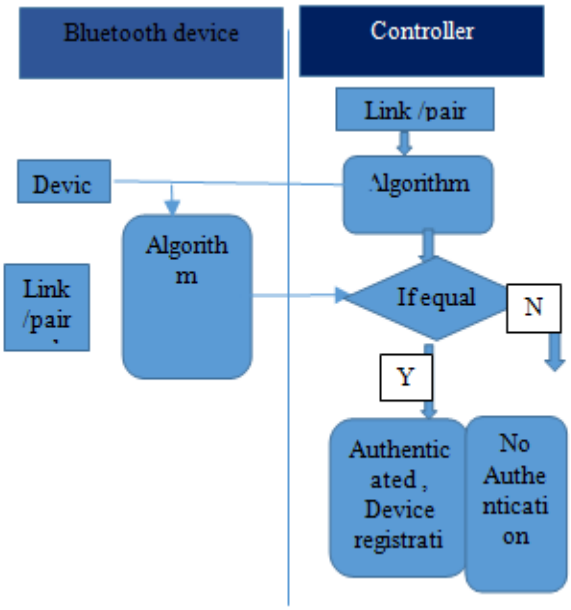

Figure 2:Registration of Bluetooth Device with Controller

5. For two Bluetooth devices to communicate with each other, the communicating device must get the key for the encryption process for ciphering the data from the Controller, as shown in figure 3.

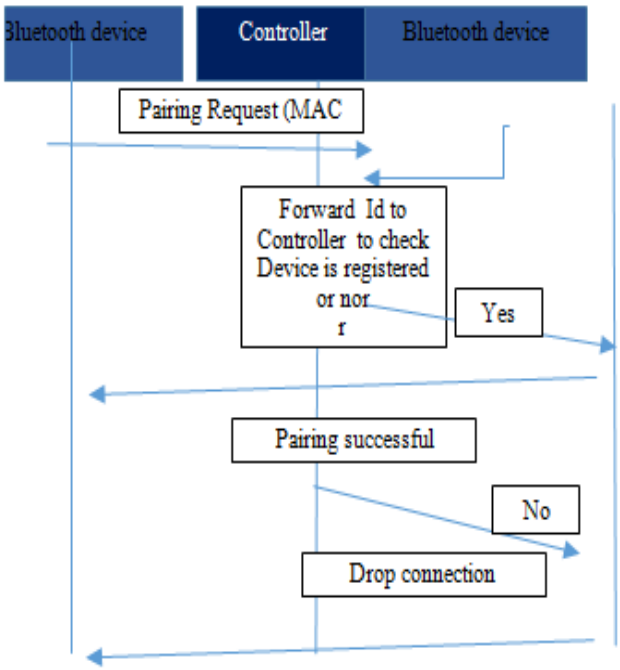

Figure 3 Pairing of Bluetooth device for D2D communication

The method discussed is robust than the security modes discussed in no case, even if one device does not have the interface to check or enter the pairing code./ link key. While registering with the Controller, the code or key associated with the device is required. Thereby the Controller will store a signature of the device along with its MAC Address. So In the IoT home scenario, it is needed that all Bluetooth devices need to be registered to make Home secure.

In normal security modes, wherein, e.g., Bluetooth earphones or car Bluetooth devices, if used in IoT networks, this is the simple vulnerability to breach in. Especially if the devices are wearables hence the in-home network, even if the similar device of another user may be guest cannot get connected to the network unless registered with the Controller. Hence there is no threat of misuse of the data of a user without his consent.

IV. RESULTS AND DISCUSSIONS

In the proposed system, the Controller will be like the Certification Authority with a stored database of Signatures of the Bluetooth devices registered in advance. By simply sharing the MAC id at the time re-association with the Controller. Hash Search will reveal the Legitimacy of the device and, based on that, will be linked or rejected. However, when two Bluetooth devices try to Communicate In device to device communication setup, the Job of the Controller Device to authenticate and optional session key can be generated for data encryption and transfer between the two devices in figure 4.

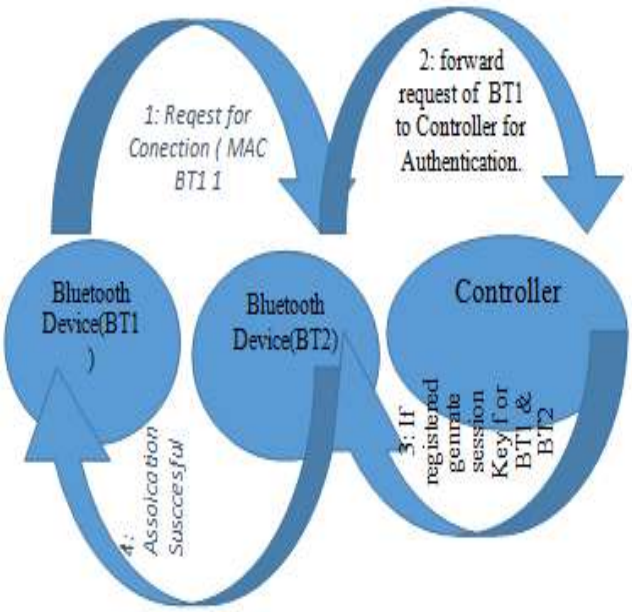

Figure 4:Centralied authentication Control Mechanism

V. CONCLUSION

Bluetooth connectivity is one of the IoT enabling technologies with low power consumption and energy-efficient technology for IoT types of networks. But the security of the system, especially for Home or Office, is the concern nowadays. Hence connectivity needs to be secured, and the solution in this paper is one of the ways wherein SDN technology can be used to implement the solution. Bluetooth technology is one of the existing technologies which can be leveraged for IoT Networks with efficient energy and Control measures. Moreover, we don't need to look for other protocols or switch to different communication technology.

REFERENCES

[1] Doukas, C." Building Internet of Things with the Arduino." CreateSpace Independent Publishing Platform, North Charleston, SC, USA **pp-347, 2012.**

[2] Lee, J.S., Su, Y.W., Shen, C.C." A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi." 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON 2007), **pp. 46–51, (November 2007.**

[3] D. Uckelmann, "Performance measurement and cost benefit analysis for RFID and Internet of Things implementations in logistics" in Quantifying the Value of RFID and the EPCglobal Architecture Framework in Logistics, New York, NY, USA:Springer-Verlag, **pp. 71-100, 2012.**

[4] P. C. Angela M. Lonzetta , Joseph Campbell, Bassam J. Mohd and Thaier Hayajneh, "Security Vulnerabilities in Bluetooth Technology as Used in IoT," Journal of Sensor and Actuator Networks **vol. 7, no. 28, 2018.**

[5] John Padgette ,John Bahr ,Mayank Batra, Marcel Holtmann, Rhonda Smithbey,Lily Chen, and Karen Scarfon "Guide to BluetoothSecurity" NIST Special Publication 800-121 Revision 2 , Natl. Inst. Stand. Technol. Spec. Publ. 800-121 Rev. 2, **pp 8, May 2017.**

[6] Melamed, T. "An Active Man-in-the-Middle Attack on Bluetooth Smart Devices". Int. J. Safety & Security. Eng. , **2018.**

[7] Nawir, M.; Amir, A.; Yaakob, N.; Lynn, O. "Internet of Things (IoT): Taxonomy of Security Attacks". In Proceedings of the 3rd International Conference on Electronic Design (ICED), Phuket, Thailand, **pp 11–12, 2016**

[8] Nateq Be-Nazir Ibn, M.; Tarique, M. "Bluetooth security threats and solutions: A survey".Int. J. Distrib.Parallel Syst. **Vol 3 pp 127 2012.**

[9] Herfurt, "Introducing the Car Whisperer at What the Hack."https://trifinite.org/trifinite_stuff_carwhisperer.html, 2005. Accessed:2020-01-19.

[10] A. Laurie, M. Holtmann, and M. Herfurt, "Hacking Bluetooth EnabledMobile Phones and Beyond." http://www.blackhat.com/html/bh-europe-05/bh-eu-05-speakers.html, 2007. Accessed: 2020-01-19.

[11] N. O. T. Daniele Antonioli, Kasper Rasmussen, "The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR," Proceedings of the 28th USENIX Security Symposium. Santa Clara, CA, **USAAugust 14–16, 2019**

