Comparison of Bluetooth Low Energy and IEEE 802.15.4 and known attacks

Semjon Kerner

***Abstract*—This paper provides a comparison between the communication protocols Bluetooth Low Energy and IEEE 802.15.4, commonly used in IoT networks. The architectures, especially the security mechanisms of both protocols are compared in order to present possible attack scenarios on these platforms. For this purpose, various studies are used which have analyzed both systems in order to summarize and differentiate attacks. Based on this research, possibilities of how to fight attacks are presented and compared. Bluetooth Low Energy is the more sophisticated alternative, while IEEE 802.15.4 depends on additional infrastructures for the same variety of possibilities and security mechanisms.**

I. Introduction

Both Bluetooth Low Energy (BLE) and IEEE 802.15.4 are widely used for communication between IoT devices. These two protocols offer similar services for mobile and smart devices as well as similar broadband, but rarely work in adjacent systems. Bluetooth is easily accessible for many people as it is installed on most smartphones, laptops and other mobile devices. In contrast, applications based on IEEE 802.15.4, mostly assisted by Zigbee or 6lowPAN, are also common in the private sector, but are rarely deployed or managed by consumers, e.g. in Smarthome applications. Users tend to be unaware of the risks associated with these systems in their mobile devices, home automation, transportation or payment. Many attacks on current systems are based on fundamental design decisions of these systems and are often related to the poor implementations of security relevant features made by vendors. While BLE offers a complex architecture of communication between two devices, IEEE 802.15.4 is based on a simple structure and comparatively small overhead. Many systemic differences between these two protocols are identified in this paper highlighting mainly security aspects. The purpose of this paper is therefore to derive and reason attacks on communication in low power networks and to demonstrate their characteristics using suitable examples. For this purpose a hierarchical structure was chosen which organizes attacks according to effort and effect and also illustrates how more complicated attacks can be supported and improved with less complex attacks. In this paper, an overview of the communication protocols BLE and IEEE 802.15.4 is given at the beginning of this chapter. The second chapter takes a more detailed look into the security features of both systems, whereas it is clearly pointed out that only proposals are made in connection with encryption in IEEE 802.15.4. The corresponding comparison of both systems is supplemented with an outlook on further security concepts in IEEE 802.15.4. A hierarchical overview is finally given in Chapter 3 providing insight into possible attack scenarios against both protocols.

A. *Bluetooth Low Energy Description*

The Bluetooth architecture provides short-range wireless communication for portable and fixed devices in a modular and robust manner with low power consumption and low cost. Since Bluetooth 4.0 specification the standard extended the Basic Rate mode with the Low Energy mode BLE [3]. Both systems include device discovery, connection establishment and connection mechanisms. BLE is designed for devices with very low power consumption and low complexity operating with lower data rates and lower duty cycles. [2]

1) Architecture: The Bluetooth core is divided into a Host and a Primary Controller sharing a common Host Controller Interface. A Controller contains the layers below the Host Controller Interface, whereas the Host defines the layers and components above the Host Controller Interface and below the non-core profiles. The hierarchy of the Primary Controller includes both physical channel with physical link an logical transport with logical link. The Primary Controller may be one of the following configurations [2]:

- A Basic Rate Controller including radio, baseband, Link Manager and optionally Host Controller Interface.
- A BLE Controller including the BLE Physical Layer (PHY), Link Layer (MAC) and optionally Host Controller Interface.
- A combination of the former Controller portion into a single Controller.

2) Physical Layer: BLE operates in the unlicensed 2.4 GHz ISM band, splitting it into 40 channels of 2 MHz each consisting of three Advertising Channels and 37 dedicated channels. To achieve robustness in the ISM band BLE utilizes frequency hopping spread spectrum. The standard employs Frequency Division Multiple Access such that multiple connections can be active on different channels. Besides, BLE uses a Time Division Multiple Access scheme for communication in time slots. BLE uses Gaussian Frequency Shift Keying (GFSK) to minimize transceiver complexity and increase robustness. With this a carrier frequency is modulated by halving its oscillation when a signal is low and otherwise the oscillation remains unchanged. The bitrates of the PHY are 1 Mb/s but can be extended with error correction where 1 bit is represented by 2 symbols with a rate of 500 kb/s or by 8 symbols with a rate of 125 kb/s. All devices in a connection execute channel hopping at the start of each time slot. Devices in a piconet use a specific frequency hopping pattern, which is algorithmically determined at the start of the connection. The hopping pattern is pseudo-random and can be adapted to exclude frequencies that are used by interfering devices improving BLE co-existence with channel static ISM systems such as IEEE 802.15.4 [2]. Each frame with a Maximum Transmission Unit of 27 bytes begins with a preamble that is followed by an address. The footer of the frame is a 3-byte field that contains the 24 bit CRC value [6], [13].

3) Physical Layer: BLE supports transmissions in connected and unconnected mode. In the unconnected mode devices in advertisement state propose transmission of data, while devices in the scanning state listen for data advertisements and may answer with transmission requests, the transmission will then happen on a different channel. In the connected mode devices in advertisement state propose connections and devices in initiating state initiate the connection and become the master, while the advertising device becomes the slave. Thus a network, called piconet, is composed of one master and one or more slaves, and is based on a star topology [8]. A physical link within a physical channel provides halfduplex packet transport in a polling scheme, such that the master polls the slaves for data. The resource manager multiplexes logical links onto the physical link between devices [3]. All communication happens in timeslots called events. After its discovery by the master, the slave wakes up at the beginning of each event and waits for a polling frame before sending its data. BLE communication between device and mobile application follows usually a scheme [8]:

1) Device A broadcasts an advertisement.
2) Device B scans for advertisements.
3) Once the specific advertisement packet is received, the device B stops scanning, and initiates a connection to device A. Device B becomes the master while device A becomes the slave.
4) The master browses the slave for available services.
5) The master exchanges information with slaves using polling.

In connected mode several transmissions are performed, as driven by the ‘More Data’ bit. Reliable, in-order delivery is ensured by sequence numbers and Acknowledgement (ACK) packets. The devices achieve time synchronization through polling packets sent all 8.0 s by the master. Slave devices can save further energy by polling packets, but must wake up at least all 32.0 s [13], [11].

4) Above Physical and Link Layer: The Host employs the Logical Link Control and Adaptation Protocol (L2CAP), the Attribute Protocol (ATT), the Generic Attribute Profile (GATT), the Security Manager Protocol (SMP) and the Generic Access Profile (GAP). On top of them there are standardized profiles for various use cases utilized by the application layer [13]. The Link Layer Protocol (LL) is a control protocol carried over logical links in addition to user data. The L2CAP layer provides an abstraction to applications and services. It performs fragmentation and de-fragmentation of application data and multiplexing and de-multiplexing of multiple channels over a shared logical link. The main goal is to multiplex the data of the three higher layers protocols: ATT, SMP and LL signaling, on top of a PHY connection. [8]. The SMP uses a fixed L2CAP channel to implement the security functions between devices. The ATT provides a method to communicate small amounts of data over a fixed L2CAP channel. The ATT is also responsible to determine the services and capabilities of other devices [2].

B. IEEE 802.15.4 Description

The IEEE 802.15.4 standard specifies the wireless medium access control and PHY for low-rate wireless sensor networks [12]. The standard focuses on simplicity, flexibility and low-cost in a low-power environment, relaxing on throughput requirements. Devices in an IEEE 802.15.4 network can either be Full Function Device (FFD) or Reduced Function Device (RFD). Only an FFD may take over the role as coordinator or Wireless Personal Area Network (WPAN) coordinator. RFDs are supposed to solely be suitable for extremely simple tasks, but can be implemented with minimal resources, memory and long battery life. A device has a single radio interface that implements an IEEE Std 802.15.4 MAC and PHY. Two or more devices communicating on the same physical channel constitute a WPAN. A WPAN includes at least one FFD, operating as the PAN coordinator. An IEEE 802.15.4 WPAN operates in either of two topologies: the star topology or the peer-to-peer topology, depending on the application requirements, with the PAN coordinator acting as primary controller. All devices have a unique address, this is by default an extended address, but a device may be assigned with a short address. A peer-to-peer network allows the implementation of mesh networks with multiple hops between devices. The standard does not define a solution for routing in mesh networks, but there are routing protocols such as RPL allowing routing of IPv6 nodes. Upper layers typically employ UDP and CoAP [19], [13].

1) Physical Layer: In IEEE 802.15.4 the features of PHY are activation and deactivation of the radio transceiver, energy detection and link quality indication for medium access, channel selection as well as transmitting and receiving packets across the physical medium. [19] Medium Access is organized either in slotted or unslotted mode. Slotted mode is administered by a controller device structuring medium access into superframe with beacon frames. After the beacon, bounding the superframe, devices send requests in the Contention Access Period to allocate a Guaranteed Time Slot (GTS) in the following Contention Free Period. The contention free period consists of seven GTS for collision free transmission, each assigned by the controller to at most one sender [18]. Unslotted mode is not administered by the controller and is organized by all devices perfoming Carrier Sense Mutliple Access / Collision Avoidance (CSMA/CA) [19]. With CSMA/CA whenever a device has a packet to send the PHY listens to the medium to assess availability. In case the medium is busy transmission is deferred for a preestablished amount of time. With CSMA/CA, nodes keep their radio always on for multihop routing, operate on a single channel, and access the medium through contention [18], [3]. IEEE 802.15.4 is based on Offset Quadrature Phase Shift Keying (QPSK) modulation, shifting a carrier signal by symbols of 2 bits. For robust transmissions the standard implements Direct Sequence Spread Spectrum

(DSSS), spreading a signal onto the whole spectrum of the channel [11]. The standard offers a nominal data rate of 250 kb/s with a maximum transmission unit of 127 bytes. IEEE 802.15.4 splits the 2,4 GHz ISM into 16 channels with a width of 2 MHz and 5 MHz space inbetween [13]. Each frame begins with a preamble and a start frame delimiter, followed by a length field. The payload can be up to 125 bytes protected with a 2-byte CRC value. [3].

2) Physical Layer: The MAC describes control mechanisms for the WPAN featuring beacon management in slotted mode, GTS management, channel access, frame validation, ACKs, retransmission and dis-/association with short addresses. Additionally provided are hooks for security mechanisms, low energy mechanisms like, Coordinated Sampled Listening (CSL) and receiver initiated transmission. CSL is a power saving mode where devices listen on specific wake up messages and otherwise remain in sleep mode [19]. Senders may inform receivers with the 'frame pending' bit that more packets are in their send queue, to perform efficient transmission of large portions of data. There are optional upper layers for IEEE 802.15.4 such as ZigBee and 6LoWPAN providing additional, extensive abstraction in the network stack [13].

C. Comparison

BLE and IEEE 802.15.4 are very different standards for wireless transmission in low power, low cost environments. Both provide a layered architecture for PHY and MAC layer but as BLE provides a complex network stack IEEE 802.15.4 is overly simplified and must be complemented by upper layers to achieve the same capabilities as BLE [6], [13].

1) Usability: One advantage of BLE is its usability with a vast deployment in modern smart and mobile devices, whereas support for IEEE 802.15.4 is practically nonexistent. Evaluations of [3] suggest that BLE offers a higher nominal data rate, while IEEE 802.15.4 supports larger frames. The robustness of BLE and IEEE 802.15.4 is achieved with different spread spectrum techniques, BLE using frequency hopping to minimize interferences while IEEE 802.15.4 implements direct sequence spread spectrum. Both using the same frequencies in the 2,4 GHz ISM band and also both introducing 8 bytes of overhead at the PHY [2], [19].

2) Power Consumption: For medium and high intensity traffic, BLE obtains the longest although 802.15.4 is traditionally expected to be better [11]. Measurements presented in [3] show that BLE consumes significantly less energy in all considered scenarios. This difference arises since IEEE 802.15.4 needs more time to transmit frames and holds the radio active for collision avoidance. They showed that IEEE 802.15.4 consumes up to three times more energy at high transmission powers and small payload sizes. However, IEEE 802.15.4 performed better in respect to the Received Signal Strength Indicator (RSSI) and thus to the maximum distance between communicating devices.

II. Security Mechanisms and Analysis

This section first introduces security mechanisms for BLE and IEEE 802.15.4. The focus is first on protocol-specific methods, after which a comparison is made between the two protocols. Subsequently, mechanisms for IEEE 802.15.4 will be outlined which are intended to increase security against specific attacks.

From a security perspective, wireless ad hoc networks are no different from any other wireless network. They are vulnerable to passive eavesdropping attacks and active tampering because physical access to the wire is not required to participate in communications. The very nature of ad hoc networks and their cost objectives impose additional security constraints, which perhaps make these networks the most difficult environments to secure [19].

A. Bluetooth Low Energy

1) Security modes: Bluetooth devices may support four hierarchical security modes called security modes 1 through 4. In security mode 1 the communication is not secured. Security mode 2 supports unpaired, encrypted security and mode 3 additionaly requires pairing. Security mode 3 is designed for link level enforced security, whereas Security Modes 2 and 4 are initiated after physical and logical link setup. Modes 1 to 3 are legacy security for devices that do not support security mode 4, which uses paired elliptic curve encryption. The Bluetooth security model includes five distinct security features [2]:

- **Pairing**: The process for creating one or more shared secret keys.
- **Bonding**: The act of storing the keys created during pairing for use in subsequent connections in order to form a trusted device pair.
- **Device authentication**: Verification that the two devices have the same keys.
- **Encryption**: Message confidentiality.
- **Message integrity**: Protects against message forgeries.

2) Pairing: Secure Simple Pairing (SSP) is the foundation of key establishment between two Bluetooth devices. The BLE legacy pairing is similar to SSP except it does not provide effective protection against passive eavesdropping. This is because SSP uses Elliptic Curve Diffie-Hellman and BLE legacy pairing does not. The link key is later used for other security procedures which are required to achieve security. BLE uses multiple keys, each for a specific purpose. Keys used for authentication and encryption, in BLE deployed with AES-CCM cryptography, are generated by combining contributions from each device during pairing. Pairing may be subject to Man in the Middle (MITM) attacks, since Bluetooth networks lack public key infrastructure. To address this issue following four models are offered to tackle MITM attacks [20]:

1) **Numeric Comparison** is a case where a user is shown a six-digit number on the displays of both devices and confirms if the numbers match. The devices calculate these numbers independently, which is why an attacker cannot guess them.
2) **Passkey entry** is the case where a user enters a six-digit number into both devices.
3) **Out of band** is designed for devices that require an additional wireless, e.g. near-field communication or

wired communication. This model assumes that the attacker is unable to compromise two technologies.

4) **Just works** is designed for cases where at least one participating device does not allow input or output of numbers. This model does not provide MITM protection.

These four association models are functionally equivalent in Bluetooth Basic rate and Bluetooth Low Energy. In BLE key generation is performed by the Host independently on each device [6].

3) Eavesdropping: Eavesdropping, another attack aimed to intercept and decrypt communication, is complicated by technical hurdles of the protocol. There are four values unique to a connection, which must be known by the attacker to be successful. First of all BLE devices hop across channels only staying for short time slots on each channel, with slot length and hopping sequence varying between connections. Additionally BLE uses access addresses to determine when a packet has been transmitted. The access address is supposed to prevent collision, where a receiver could listen for a packet, and actually receive a packet from someone else than the expected sender, since channels may be shared amongst different piconets. Finally packets are protected with a CRC value with an initial seed unique to the connection [17].

4) Privacy: BLE provides a privacy procedure in order to prevent tracking, by allowing devices to frequently change MAC addresses, then called private addresses. Only paired devices will be able to resolve changed MAC addresses. Private addresses are either resolved and generated by the Host or by the Controller without involving the Host after the Host provides the Controller device identity information. It is also possible to whitelist MAC addresses of accepted devices. Privacy is achieved with two modes: device privacy mode and network privacy mode. A device is only concerned about its own privacy and accepts advertising packets from peer devices that contain either their identity address or their private address. In network privacy mode a device will only accept advertising packets containing private addresses [2].

5) Authentication: BLE supports authentication over an unencrypted ATT bearer between devices with a trusted relationship by signing the data with a Connection Signature Resolving Key after the Protocol Data Unit (PDU). The signature is composed of a Message Authentication Code generated from the signing algorithm and a counter. The counter is used to protect against replay attacks and is incremented on each signed PDU [2].

Some vendors do not implement abovementioned security features and thus a significant amount of devices is vulnerable to basic attacks. Many devices do not carry out a pairing procedure in a secure environment and in other cases such procedures lack various requirements such as usability or multiple devices in a piconet [8].

B. IEEE 802.15.4

In IEEE 802.15.4 implementation of security is optional. By the standard the MAC sublayer shall neither provide any mechanism to perform cryptographic transformation of frames nor set any security information in the packet header, if security is not implemented by the device. If the MAC security attribute is enabled, a device shall provide such cryptographic transformations. Moreover, establishment and maintenance of cryptographic keys is outside of the scope of the IEEE 802.15.4 standard.

1) Cryptographic frame protection: Keys are provided by higher layers with mechanisms based on symmetric key cryptography. The standard recommends secure implementation of cryptographic operations and secure and authentic storage of keying material, including mechanisms to prevent unauthorized access to locally stored keys. Cryptographic keys are either shared between two peer devices or among a group of devices, allowing for flexible tradeoffs between key maintenance and protection. Protection with group keys is only provided as long as no malicious devices take part in the key sharing group. The cryptographic operations can be adapted on a frame-by-frame basis allowing for combinations of following security services [19]:

- **Data confidentiality**: Assurance that transmitted information is only disclosed to parties for which it is intended.
- **Data authenticity**: Assurance of the source of transmitted information (information was not mannipulated).
- **Replay protection**: Assurance that duplicate information is detected.

2) security operations: The standard specifies two main security operations, the outgoing frame security procedure, performed on the sending side upon frame transmission, and the incoming frame security procedure, performed on the receiving side upon frame reception. Frame security consists of applying the cryptographic functions of each security level to the unsecured frame. Two main data structures are used for these procedures, the key table, storing the cryptographic keys as well as information about the usage of these keys, and the device table recording device addresses corresponding to the used keys related to devices which a given node can interact with in a secure and protected communication. The outgoing frame security procedure decrypts the unsecured frame with the input parameters security level, key identifier mode and the cryptographic key. The incoming frame security procedure gets the secured frame handed over from the PHY, parses it and determines security level, key identifier mode, and cryptographic key and proceeds with unsecuring the frame. The resulting unsecured frame is returned for reception. Also the incoming frame security procedure is responsible to check if a frame counter is valid, thus protecting against false retransmission and replay attacks [5], [18].

3) security levels: IEEE 802.15.4 defines eight security levels hierarchically describing encryption standard and authentication. A definite security level should be insured for every type of message, i.e. beacon frame, command frame, data packet, and ACK packets. The Counter (CTR) security mode requires a block cipher encryption operation for each block to encrypt with successive values of a counter, essentially making it a stream cipher encryption operation. The counter may be a simple increment counter as well as an algorithm giving complex, nondeterministic values which do not repeat frequently. The Cipher Block Chaining (CBC)-MAC security mode initially computes a 128-bit Message Integrity Code (MIC) by using the AES block cipher in the CBC mode. IEEE 802.15.4 employs 128-bits AES keys only. The CBC-MAC security level secures a frame by encrypting each block by the MIC as well as the preceding block. Finally, the combination of both CTR with CBC-MAC (CCM) security mode secures a frame by using the AES block cipher in the CTR with CBC-MAC mode. Also the MIC can be truncated at 4, 8 or 16 bytes producing additional variations of the CCM to achieve either simplification or increased security [5], [18], [19].

4) MAC Header: Security information are transmitted in the MAC header as an additional extension called Auxiliary Security Header which contains subfields for security level, key identification, frame counter and in case of authentication the MIC [5].

C. Comparison

BLE and IEEE 802.15.4 Security both rely on AES, yet BLE implements cryptographical functions in its MAC, whereas IEEE 802.15.4 only employs frame encryption in its MAC if provided by upper layers, which are not defined in the standard [23]. Both protocols are able to detect simple replay attacks with frame counters, additionally BLE is secure against basic eavesdropping, since channel hopping sequences are unique to each connection, although interception of unencrypted transmission in BLE does neither require sophisticated nor expensive hardware any more [8].

1) Shortcomings of IEEE 802.15.4 Security: IEEE 802.15.4 describes the infrastructure of encryption and pairing, but lacks specification how to create and interchange keys in a secure manner. Also IEEE 802.15.4 does neither present a procedure to setup a fresh secured network with protection against MITM, nor give an explanation of network joining procedure for a fresh node which lacks security capabilities [18], [5]. In multihop networks IEEE 802.15.4 devices suffer energy starvation since intermediate nodes must be active all the time to be able to path on packets. Also IEEE 802.15.4 is vulnerable to basic Denial of Service (DoS) attacks e.g. utilizing energy draining or jamming [18]. Also security mechanisms increase frame length and memory overhead, able to impact overall network performance in terms of latency, throughput and memory usage. The authors in [5] have found that this overhead may even limit the scalability of a Wireless Sensor Network that is based on IEEE 802.15.4.

D. Scientific Security Approaches

IEEE 802.15.4 is vulnerable to different attacks such as jamming and eavesdropping. There are different approaches that conquer attacks by extending the protocol with additional functionality, for preventing these attacks.

1) DEEJAM: Jamming is a DoS attack aimed to interrupt communication between devices, by interfering packets in a whole or in parts. An anti-jamming technique presented in [22] is called DEEJAM (Defeating energy-efficient Jamming in IEEE 802.15.4). DEEJAM proposes methods to detect jamming and even avoid adaptive jamming, where attackers can react on countermeasures. If an attacker is able to permanently jam all available channels DEEJAM is not able to defeat jamming, so jamming is expected to be costly in terms of power consumption since it assumes that attackers use similar hardware as the defenders. Energy efficient jamming is accomplished by only jamming if a transmission is detected. Therefore an attacker will search for the preamble denoting the beginning of a frame. The preamble has a specific byte-pattern. In the frame masking defense proposed by DEEJAM, defenders agree on a secret preamble, so the attacker cannot detect a packet as long as the preamble is secret. However, if an attacker reacts on RSSI any pattern that looks like communication will be jammed. Since an attacker can only sample RSSI for one channel, in the channel hopping defense, the defenders change channels to evade the attacker. Attackers may now hop across all 16 channels sampling only a short period of time, to ensure that there is still enough time to detect and interfere packet transmission of large packets on each channel. In the packet fragmentation defense, a device breaks outgoing payload into fragments to be transmitted separately on different channels and with different preambles, to keep transmission on each channel as short as possible. The final defense against disrupting packets with pulse jamming is error correction by sending symbols redundantly. All defenses come with additional overhead in terms of throughput, power consumption and security measures, which must be communicated on secure channels. Also some of the mentioned defenses resemble techniques used in BLE, such as frequency hopping or redundant symbol transmission.

2) Secrect Codes Spread Spectrum: DSSS is a frequency multiplexing method employed by IEEE 802.15.4. Spreading is a method exploiting physical characteristics of the medium to broaden the frequency band of a signal by sending small bursts of a signal, so called chips, which spread in the spectrum, in correspondence to its chipping sequence. DSSS can be used to allow multiple logical channels on the same frequency channel if the hamming distance of the chipping sequences is high. IEEE 802.15.4 does not implement this feature, but instead recommends a default chipping sequence. In order to harden communication against interception and detection the authors in [12] present a protocol to utilize secret spreading codes in a dynamic, random fashion. Despite the randomness does not always provide a good hamming distance, random chip sequences are employed in the protocol, so that attackers will not be able to reduce the search space of possible chipping sequences. The authors define a Pairwise Code Synchronization Protocol on top of IEEE 802.15.4 minimizing code synchronization time. A pair of codes is then used to hop through pseudo-randomly generated, secret spreading codes in a synchronized fashion. Code hopping prevents an attacker from gathering enough information to compromise secrecy before the chipping sequence changes. Also the protocol provides randomly generated preambles, as explained in the last chapter, to prevent side channel attacks. The spreading code is shared on a secure connection over uncorrelated DSSS. The pair of codes consists of one code for sending and one code for receiving. Code pairs are unique to a connection and thus devices hold a table of codes corresponding to each device. Also spreading codes are given in sets, in order to detected code hopping if a codeword is recognized in a set which is not the active code of a connection. In that case or when the code lifetime is expired the devices hop to the next code by updating the active code and purging the last code from the set.

III. known Attacks

This section introduces known attacks on IEEE 802.15.4 and BLE, in some cases backed by real implementations. At the beginning, DoS attacks are presented, followed by eavesdropping, packet injection and finally MITM attacks. In this context, there will always be a reference to the communication protocols and to low-level IoT devices.

A. Denial of Service Attacks

Denial of Service (DoS) is a branch of attacks aimed to suppress communication between a sender and a receiver. There are different approaches to achieve DoS, such as energy starvation, cloning devices or jamming.

1) Jamming: Jamming is a very common approach in low power systems since defenders have limited resources for jam detection and avoidance strategies. It is assumed that attackers have similar restrictions on power consumption. Therefore attackers wish to avoid continuous jamming. This assumption arises from the fact that better equipped attackers have the ability to continuously jam all available channels. However, malicious jamming is prohibited in most countries and jammers are easy to locate [14]. Therefore attackers wish to avoid detection and keep energy consumption at a minimum [22]. To achieve both, different levels of attacks were developed, some already outlaid in II-D1. There are two relevant categories of jamming attacks based on the attackers knowledge of the network architecture. The first category includes continuous, random and deceptive jamming, utilized when the network configuration is unknown to the jammer. Continuous jamming is the easiest method of jamming, blocking the entire frequency band, resulting in total loss of transmitted packets. But as stated above this attack is not efficient for IoT-devices and it is easy to detect. A more efficient continuous jamming can also be achieved by pulse jamming a frequency with short bursts in shorter intervals than intercepted packets would take. Pulse jamming can be extended by channel hopping to achieve wide-band jamming. Random pulse jamming consumes less energy and is harder to detect, but does not reach the maximum rate of disrupted packets [14]. The second category covers jammers that are aware of the network architecture and thus can employ custom strategies. A basic procedure called reactive or interruptive jamming works by listening to the medium and starting to send interruptive signals when a valid transmission is sensed. This is a simple but energy efficient method since the attacking device can enter sleep mode until a new transmission is sensed [22]. Evaluations presented in [9] have shown that this attack is able to prohibit all communication on a channel. This attack is hard to detect with low energy IoT devices since the interruption is masked by the legitimate transmission and does not appear spontaneously. Jamming a specific signal like IEEE 802.15.4 on a single channel or BLE in a specific hopping sequence will also minimize interference to other wireless protocols in the 2.4 GHz ISM band. To jam an IEEE 802.15.4 packet it is only necessary to corrupt the Frame Check Sequence (FCS) so that the receiver will discard a data packet. This is achieved since the frame length is given in the first byte of the packet and thus the attacker can easily predict when the FCS will be submitted and disrupt it, further minimizing energy consumption of the attacker. Also an attacker might be able to receive the package and still corrupt the FCS, denying the information to a receiver [14]. With deeper knowledge about the system the attacker has additional possibilities to execute a jamming attack. By reading the MAC header the attacker can determine if a packet is worth jamming.

Another target of jamming are ACK packets. If retransmission is enabled a transmission is acknowledged by the receiver with an ACK. If the sender does not receive the ACK within a given interval or receives a corrupted ACK it will retransmit the packet. In some use cases only attacking ACKs may be desired, since the channel is held busy by the defenders and additionally defenders have an increased power consumption compared to the effort of the attack. Note that packets are only retransmitted for a small number of times and also the original packet must already be received correctly for an acknowledgment to be sent [9]. Another attack surface is the beacon mode in IEEE 802.15.4. As mentioned before, beacon mode is a moderated contention mode minimizing wasted time due to collisions. This is achieved by arranging a short contention access period in the beginning of each superframe where senders can request slots for sending. If an attacker jams all contention requests the coordinator will not be able to assign slots to senders suppressing communication at all [18].

2) ”Network Shaping” Jamming: Wide-band jamming can also be utilized to shape a network to force devices onto a desired channel. This is possible when devices use upper layers that provide channel selection by congestion detection. This approach could be employed as a countermeasure against defensive techniques, such as channel hopping [14].

3) Other Denial of Service Attacks: In most cases, other forms of DoS attacks than jamming are protocol specific. There is a description of a DoS attack against BLE in [8]. The DoS is performed by cloning a device and mimicking its advertisement messages. A scanner trying to connect to the clone will not be able to access the device services, thus the scanner will start scanning again after some time. The scanner will stay connected to the clone even longer, if the services are cloned too, although the requests are not forwarded to the real advertiser. This DoS is a pre-stage to a more advanced MITM attack [8]. During initial bootstrapping, a method of configuring two nodes is required to establish a secure connection. Very resource constrained networks may involve a system where an attacker must not be present during the initial configuration, which may be sufficient for simple applications. DoS attacks can be used to force a particular device off the network, requiring bootstrapping to be performed again. Except in this case, the attacker is present during this process and can either eavesdrop on the secure key or perform other attacks [14].

B. Eavesdropping

Eavesdropping is a branch of attacks focused on intercepting communication and possibly breach security. In the majority of cases eavesdropping in a standard IEEE 802.15.4 network is a simple task, since communication is neither masked with a connection specific technique nor based on pseudo-random mechanisms. Only correctly implemented and executed cryptography is preventing a transmission to be compromised. Although AES with a key of 128 bit is mentioned, an implementation is not covered in the standard. Common stacks of upper layers to IEEE 802.15.4 are Zigbee and 6lowPAN, both implementing AES. In addition to AES encryption, the BLE standard employs connection specific methods to harden the transmission against eavesdropping as stated in II-A3. Due to the lower input and computing power of BLE devices compared to the Bluetooth Basic Rate mode, compromises have been made in the design of BLE which, in the event of a key exchange, contribute to endangering the security of a network. Based on the Ubertooth [1] platform, an implementation of a sniffer was presented in [17], which enables continuous monitoring of BLE connections without interception when establishing a secure connection. Ubertooth is a USB device that continuously monitors a BLE channel. In contrast to a classic Bluetooth Basic Rate connection, Ubertooth is able to monitor a BLE connection independently without additional calculations on the computer. In this case, the implementation of Ubertooth allows a more agile operation and precise timings, which must be known for the calculation of the jump interval and jump increment.

C. Packet Injection

Packet injection is a branch of attacks that aims to manipulate or forge packets in order to get malicious packets accepted by a receiver. These attacks usually lay the groundwork for further attacks, which is why they are an important area of research for identifying weaknesses in network security. One explanation for the success of packet injection is that most developers make de facto security assumptions about the origin and integrity of packets [7].

1) Overshadowing: By overshadowing a transmission with well-chosen interference signals an attack to modify packets is considered in [21] which is capable of manipulating any packet of the attackers choice by merging it with the original signal to form a new signal. This method allows modification of a part of a packet so that it is accepted and processed by the reciever, even though it contains dangerous or invalid data. To execute this method, an attacker must have specific knowledge of the system and, furthermore, an attack is made considerably more difficult and, at best, prevented by reasonable encryption. In addition to the tough timing requirements, this attack is made more difficult because an adjustment of amplitudes and phase must be controlled via the software. Therefore, this method has been further improved by the authors by taking advantage of the fact that in angle modulation schemes only the stronger of two colliding signals is received. Angle modulation schemes are used in IEEE 802.15.4 with QPSK and in BLE with GFSK. In this improvement, the timing requirements remain, but this attack is more robust and the acception of manipulated packets by the receiver is more reliable.

2) Packet-in-Packet Spoofing: Typically, to manipulate Layer 2 headers, an attacker must have access to the procedures in the kernel by inserting a device locally into the radio network or compromising one of the existing devices. To avoid this physical access, [7] explains a technique to achieve raw-fram-injection. This involves embedding a valid frame into the payload of a larger frame, which results in a gateway or firewall accepting the packet even though the inner packet contains potentially dangerous or unauthorized access, which is then transmitted without compromising the sender. When transmitting over the wireless network, noise or protocol differences are applied so that the receiver discards the outer packet and interprets the inner packet as a separate, valid packet instead. As symbol errors are assumed in the transmission of the packet, an attacker can repeat the transmission until only the inner packet is accepted by the receiver, e.g. due to symbol errors in the original preamble.

3) BLE Cloning: A spoofing attack on BLE networks is presented in two different ways in [15]. In the first case an advertiser was cloned to confuse the system and in the second case it was assumed that an attacker could compromise at least one node to manipulate its configuration. In the system used, beacons, in a non-connectable mode, send their Universally Unique Identifier (UUID) to determine the position of user devices using the RSSI. In the first case, it is assumed that the attacker has physical access to the beacon's area of use and has been able to determine their UUIDs. The attacker adds a beacon, called evil twin, that mimics one of the existing beacons by sending its UUID. It is shown that the classification results deteriorate overall, but most near the evil twin. When taking over a node, even stronger influences on the results can be observed, since additionally to the spoffing attack another node was no longer present.

D. Man in the Middle

Man in the Middle (MITM) attacks are a branch of attacks in which an attacker takes over a connection by forwarding all packets. The attacker can then eavesdrop, modify or infiltrate data. In the best case, the communicating devices do not detect that their packets are being forwarded via another device. The feasibility of MITM attacks is given when communication is not encrypted, keys are tapped or guessed during connection establishment, or devices condone other unsecured access. In the case of unencrypted IEEE 802.15.4 and BLE, such attacks are usually possible. There is a MITM attack on BLE presented in [8] wherein a sensor node clones an original device and its services. By sending advertising packets faster than the original advertiser, a scanner prefers to connect to the cloned device. A BLE radio can usually not connect to two devices, so for such attacks two radio components or two BLE devices are used, which are administered by an upper layer protocol. In the implementations of [8] and [10] WebSockets were used, providing bidirectional communication between the two hosts.

1) Attacking encrypted BLE: When connecting using the SSP Passkey method, the pairing key is the only secret that secures the connection. If the attacker knows the key before pairing or can guess it, he can perform a MITM attack. If a connection already exists that is secured by a pairing key, an attacker can try to force the pairing again by performing a DoS attack on the connection. One possibility for a DoS is described in [8], where again a device is cloned. In this case, an initiator cannot establish a connection because the attackers key does not match the one stored for the connection. The user will therefore presumably try to reconnect while the attacker turns off his advertisement and simultaneously eavedrops on the key transfer. A suggestion for determining the key is presented in [20], where an attacker can guess the key because the following assumptions are made about the key. On the one hand it is likely that devices reuse keys due to limited computational power, on the other hand people tend to reuse keys out of convenience. This is exploited with the algorithm given in [20]. Instead of guessing the key, it is suggested in [8] to decrypt the key using the tool Crackle [16].

2) Established Tools: In 2016 two tools were introduced which allow MITM attacks on BLE networks. Firstly, the tool GATTacker [8] developed by Slawomir Jasek (Securing) was presented at the Black Hat Conference in the USA, secondly Damien Cauquil (Digital Security) presented the tool BtleJuice [4] at the DefCon 24 Conference. GATTacker scans and copies advertisers, implements a WebSocket connection that allows packets to be read and manipulated, suppresses a connection, and, upon reconnection, performs a MITM attack. BtleJuice requires two BLE components, which also communicate via WebSocket. In addition to replay and spoofing attacks, MITM attacks are also supported by the software [10].

IV. Summary

This paper provides an overview of the functionality of Bluetooth Low Energy (BLE) and IEE 802.15.4. These are integral parts of the current communication in the growing market of IoT devices. In particular, the focus of this work is therefore on security aspects and potential attacks. We frequently reflect upon possible ways to prevent attacks or make them more difficult in order to identify options to protect the system from dangerous attacks. For this purpose, a selection of attacks was presented, which should represent a broad spectrum of actual threats. In contrast to IEEE 802.15.4, BLE is a fairly complex network protocol that already minimizes the attack surface through its communication structure. Suggestions for the extension of the IEEE 802.15.4 protocol were also presented, revealing the advantages of connections in a Bluetooth network. Compared to Bluetooth Basic Rate, BLE is a reduced protocol format in which attacks are easier to accomplish. In particular, these communication mechanisms do not protect against smart attackers who have detailed knowledge regarding the infrastructure. In addition, it turns out that there are many weaknesses in Bluetooth technology, which particularly affect devices from manufacturers who do refrain from publishing their implementations. Therefore, BLE also offers AES encryption, which can only be cracked with constraints on the network security and considerable processing power unavailable to smaller sensor nodes. In contrast, IEEE 802.15.4 is a comparably simple protocol that does not by default offer security mechanisms against basic attacks. Furthermore, there is no component for creating or securely exchanging AES keys specified, although encryption is recommended by the standard. As a result of this investigation, it is concluded that BLE is superior to IEEE 802.15.4 both in terms of security and energy efficiency. In addition, Bluetooth is recommended with regard to robustness, also scoring well in the area of authenticated connections. The Bluetooth protocol is correspondingly complex in implementation and has a greater memory impact than IEEE 802.15.4. For an IEEE 802.15.4 network, however, there are stacks that significantly enhance functionality and security. For instance, 6lowPAN, which enables multi-hopping and routing in networks as well as direct translation into widely used Internet protocols through protocols such as IPv6 and COAP.

References

[1] Project ubertooth.

[2] Bluetooth core specification v 5.0. 2016.

[3] J. A. Afonso, A. F. Maio, and R. Simoes. Performance evaluation of bluetooth low energy for high data rate body area networks. 2018.

[4] D. Cauquil. Btlejuice framework.

[5] R. Daidone, G. Dini, and G. Anastasi. On evaluating the performance impact of the ieee 802.15.4 security sub-layer. 2014.

[6] X. Fafoutis, E. Tsimbalo, W. Zhao, H. Chen, E. Mellios, W. Harwin, R. Piechocki, and I. Craddock. Ble or ieee 802.15.4: Which home iot communication solution is more energy-efficient? 2016.

[7] T. Goodspeed, S. Bratus, R. Melgares, R. Shapiro, and R. Speers. Packets in packets: Orsonwelles' in-band signaling attacks for modern radios. 2018.

[8] S. Jasek. Gattacking bluetooth smart devices. 2016.

[9] G. Liu, J. Luo, Q. Xiao, and B. Xiao. Edjam: Effective dynamic jamming against ieee 802.15.4-compliant wireless personal area networks. 2011.

[10] T. Melamed. An active man-in-the-middle attack on bluetooth smart devices. 2018.

[11] E. Morin, M. Maman, R. Guizzetti, and A. Duda. Comparison of the device lifetime in wireless networks for the internet of things. 2018.

[12] B. Muntwyler, V. Lenders, F. Legendre, and B. Plattner. Obfuscating ieee 802.15.4 communication using secret spreading codes. 2018.

[13] P. Narendra, S. Duquennoy, and T. Voigt. Ble and ieee 802.15.4 in the iot: Evaluation and interoperability considerations. 2018.

[14] C. P. O'Flynn. Message denial and alteration on ieee 802.15.4 low-power radio networks. 2011.

[15] W. Oliff, A. Filippoupolitis, and G. Loukas. Evaluating the impact of malicious spoofing attacks on bluetooth low energy based occupancy detection systems. 2018.

[16] M. Ryan. crackle, crack bluetooth smart (ble) encryption.

[17] M. Ryan. Bluetooth: With low energy comes low security. 2018.

[18] S. M. Sajjad and M. Yousafy. Security analysis of ieee 802.15.4 mac in the context of internet of things (iot). 2014.

[19] I. C. Society. Ieee standard for low-rate wireless networks. 2016.

[20] D.-Z. Sun, Y. Mu, and W. Susilo. Man-in-the-middle attacks on secure simple pairing in bluetooth standard v5.0 and its countermeasure. 2017.

[21] M. Wilhelm, J. B. Schmitt, , and V. Lenders. Practical message manipulation attacks in ieee 802.15.4 wireless networks. 2018.

[22] A. D. Wood, J. A. Stankovic, and G. Zhou. Deejam: Defeating energy-efficient jamming in ieee 802.15.4-based wireless networks. 2018.

[23] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall. Securing wireless communications of the internet of things from the physical layer, an overview. 2017.