Survey of Side-Channel Vulnerabilities for Short-Range Wireless Communication Technologies

Shannon Beck+, Manohar Raavi*, Caleb Dale+, Kaija Weishalla+, and Brennan Worrell+

+United States Air Force Academy *Kennesaw State University
shannon.beck@afacademy.af.edu, mraavi3@kennesaw.edu,
{C24Caleb.Dale, C24Kaija.Weishalla, C24Brennan.Worrell}@afacademy.af.edu

***Abstract*—Short-range wireless communications have become a part of everyday human life and protecting the security and privacy of user data is the primary goal in this digital era. Multiple short-range wireless communication technologies including RFID, Bluetooth, ZigBee, Qi, and Li-Fi are susceptible to side-channel vulnerabilities. We review the major side-channel vulnerabilities associated with each short-range wireless communication technology, categorize them to identify the type of associated threat and provide mitigation techniques. We use passive and active threats for categorization and to understand the level of impact. We discuss the implications of the identified vulnerabilities and present potential directions further to strengthen the protection of users' privacy and security.**

***Index Terms*—Qi, Li-Fi, ZigBee, Bluetooth, RFID, Side-channel vulnerabilities.**

I. Introduction

Billions of Internet of Things (IoT) devices such as light bulbs, sensors, and small appliances are online, with thousands of new IoT devices added to the internet every day, maintaining user security and privacy is challenging. Multiple short-range wireless communication technologies are standardized to protect user security and privacy. However, due to the open nature of wireless communications, short-range wireless communication technologies still face side-channel vulnerabilities, threatening users' information and security.

This survey paper reviews the side-channel vulnerabilities of short-range wireless communications including Radio-Frequency Identification (RFID), Bluetooth, ZigBee, Qi wireless charging, and Light-Fidelity (Li-Fi). We exclude Wi-Fi protocols in our survey for the following two reasons. First, Wi-Fi protocols are widely used and well-studied [1], [2], [3], [4]. Multiple studies have extensive works focusing on Wi-Fi side-channel vulnerabilities. Second, we want to focus on technologies other than Wi-Fi and specifically new technologies including Qi and Li-Fi. Our work excludes proprietary communication protocols including Apple Air Tags, AirDrop, Bonjour, and LoRaWAN.

Methodology: Many research resources were used for this survey paper. We utilized Engineering Village, Google Scholar, and the ACM Portal to find reputable sources. Different search terms were used for each topic when the team searched Engineering Village for articles to optimize the amount and quality of research material. The titles and partial summary of the articles were reviewed to assess their relevance to the topic. We include pertinent articles after an abstract review with a final inclusion check after reading the article or paper. Table I lists the wireless technologies we surveyed and the terminology we used to identify the relevant papers. For example, for RFID side-channel vulnerabilities literature we used the search terms RFID or NFC (Near Field Communications protocol) for the first search term while we used side-channel or vulnerability for the second search term.

TABLE I: The protocols and terminology used to search papers through ACM and Engineering Village.

Wireless Technology	Terminology
RFID	RFID/NFC & side-channel/vulnerability
Bluetooth	Bluetooth/BLE & side-channel/vulnerability
ZigBee	ZigBee & side-channel/vulnerablity
Qi	Qi charging/Qi wireless power & side-channel/vulnerablity
Li-Fi	light fidelity/Li-Fi & side-channel/vulnerablity

This paper surveys the state-of-the-art side-channel vulnerabilities for short-range wireless communication technologies listed in Table I and presents the implications of those vulnerabilities concerning the users' privacy and security. For each technology, we describe the technology, its applications and then provide the vulnerabilities, mitigations, and implications in each of the following protocol sections.

The rest of the paper is organized as follows. Section II categorizes the threats while Sections III-VII discuss each short-range wireless technology, following the order listed in Table I.

II. Threat Categorization

All short-range wireless technologies have side-channel vulnerabilities due to the open nature of the wireless channels. Exploiting these vulnerabilities to perform a passive or active attack threatens the security and privacy of the users. A passive attacker listens to the communication channels to learn as much information as possible. For example, an eavesdropping attack is a passive attack. An active attacker tries to modify

TABLE II: Side-channel Vulnerabilities and Associated Threats

	Passive Threats	**Active Threats**
RFID	[5], [6]	[5], [7], [8], [9], [10], [11], [12]
Bluetooth	[13], [14]	[13], [15], [16], [17], [18], [19], [20]
ZigBee	[21], [22], [23]	[21], [24], [25], [26], [27], [28]
Qi	[29], [30], [31], [32], [33], [34]	[29], [35], [36], [37], [38], [39]
Li-Fi	[40], [41], [42], [43], [44]	[42], [45], [46]

or gain control of the channel/information. For example, spoofing, jamming, or tampering attacks. We look at each of the technologies listed in Table I to identify the vulnerabilities associated and further categorize them into passive or active threats, as shown in Table I.

III. RFID

Radio Frequency Identification (RFID) technology uses microchip tags and scanners to enable device identification. An RFID scanner uses radio waves to scan for the tags and microchips reflect the radio waves uniquely [47]. The range depends on whether the technology is active (powered) or passive, and its operating frequency, from low frequency at 10cm to ultra-high frequency readable up to 12m.

Any device with an RFID tag can be identified with a unique ID, encrypted or not. However, RFID has gone from a simple identification method to enabling ambient or ubiquitous computing for IoT devices [7]. RFID enables features including product identification, inventory management, and tracking. These features have exposed RFID tags to side-channel attacks [7].

A. Applications:

RFID has uses in medical equipment [48], inventory [49] and supply chain management [50], and credit cards [51]. Applications transmitting sensitive information, such as passports and credit cards, use encryption to protect from bad actors.

B. Vulnerabilities:

Eavesdropping consists of an attacker getting close enough to the RFID tag, usually within 10 cm, [5] and simply listening or scanning the device's information. However, far-field attacks allow the attacker to adopt the readers' antenna design and perform eavesdropping from farther distances [6]. Depending on the level of encryption used, the attacker can gain as little information as a simple serial number, or as much data as serial number, device ID, or even user information threatening the security and privacy of the users.

Another common vulnerability in RFID-enabled systems is when the manufacturer fails to use encryption. Without encryption, RFID signals can be skimmed and replayed to imitate an authorized user, for example, gaining access to university buildings [8] or used for a tracking attack [9]. RFIDs can also be cloned with specialized equipment to imitate the identity of the tags [5], [11]. RFID cards that use 3DES encryption are vulnerable because multiple rounds of encryption can be exploited to recover the user encryption key [10].

Near Field Communications (NFC) is a related form of shorter-range RFID commonly used for payment transactions. Vulnerable to side-channel analyses and signal injection [12], NFC signal injection enables an attacker to adjust the amplitude of the carrier signal and manipulate, flipping payload bits. Another common vulnerability is a physical "tear-off" attack, when the RFID tag on a product is simply ripped off of it, for example on library books with tracking tags [52].

C. Mitigations:

Several mitigation techniques for RFID follow. Correct use of encryption and cryptography algorithms, such as the 128-bit AES cipher with randomization enabled is a commonly-used practice to counteract side-channel attacks [7], [9]. Detection of duplicate (cloned) or counterfeit RFID tags [11]. Cyber best practices apply here: implement secure key management practices to protect the cryptographic keys, conduct regular security audits, and install firmware and software updates to address known vulnerabilities.

D. Implications:

RFID technology is vulnerable to side-channel analyses and encryption is necessary to protect the security and privacy of the users. Care must be taken in the cryptographic algorithm selection and implementation to protect the confidentiality and integrity of users' data. The vulnerabilities from RFID cards can also occur when companies want to push out their products as fast as possible and take shortcuts with encryption schemes.

IV. Bluetooth

Bluetooth is widely used, next to Wi-Fi [53], by the majority of IoT devices. In 1998, Ericsson, IBM, Intel, Nokia, and Toshiba formed the Bluetooth Special Industry Group (SIG) to establish the Bluetooth protocol. The goal during development was to replace interconnect cables between devices, becoming the universal interface for a variety of devices [10], [4]. More than 20 years after Bluetooth was first developed, devices benefit from a newer ultra-low power communication standard, or Bluetooth Low Energy (BLE) [54]. Devices can have a longer battery duration between charging using BLE, as it consumes even less power per unit of energy when compared to ZigBee, as discussed in Section V, another protocol for the modern IoT device communication method [4], [55].

A. Applications:

Bluetooth-enabled equipment, such as speakers, mobile phones, keyboards, and computer mice, operates with a range up to roughly 100m [56]. The BLE protocol is used to send short-range communications up to roughly 50m [55]. While BLE has a shorter range, it conserves more energy than standard Bluetooth [57].

B. Vulnerabilities:

Bluetooth has multiple side-channel vulnerabilities [13] and one of the latest vulnerabilities lets the discovery of a mobile device that is set in non-discoverable mode [14]. One of the earliest vulnerabilities of Bluetooth is known as Bluejacking.

Bluejacking occurs when an attacker sends an unsolicited message to a recipient. This attack is relatively harmless, annoying the recipient of the request. These attacks also greatly depend on the location where attackers would send out mass messages in crowded areas like a subway or airport [15]. Another Bluetooth vulnerability is Bluesnarfing [20]. The vulnerability occurs when an attacker pushes a "get" request for files with a known filename. This attack was thought to only work on devices in "discoverable" or "visible" mode, but it can be carried out on devices that are in "non-discoverable" mode. This vulnerability requires the 48-bit Bluetooth device name, which requires brute force attacks and applications such as RedFang to acquire, which can be very time-consuming. Bluesnarfing takes advantage of the OBject EXchange protocol (OBEX), a built-in Bluetooth functionality used to exchange electronic business cards [16].

Bluebugging is a powerful Bluetooth attack that takes advantage of *all* phone features through the command parser [17]. An attacker executes a specific command in the parser that allows full access to a victim's phone to make phone calls, a phone acting as a bug, hence the name. Bluebugging can also send short message service (SMS) texts, read SMS messages stored on the phone, read and write contact list entries, alter phone service parameters, connect to the Internet, forward calls, and more.

Encryption key attacks for both Bluetooth and BLE include BIAS [18] and Key Negotiation of Bluetooth (KNOB) [19]. KNOB is a standard-compliant entropy downgrade attack, enabling key negotiation protocols used to generate long-term keys for pairing and session keys for secure connection establishment to be shortened where the low-entropy keys can be brute-force attacked. Once compromised, the attacker can eavesdrop, decrypt ciphertext, and inject valid ciphertext in any Bluetooth/BLE network. Denial of service (DoS) attacks include Bluesmack [20] that transmits crafted oversized packets to crash the device or create a DoS attack.

C. Mitigations:

To overcome many of the vulnerabilities, recommended mitigations include using encryption, being cautious of connecting to unknown devices, turning off Bluetooth when not in use, setting visibility to hidden or non-discoverable, using secure pairing with a PIN or passphrase to prevent unauthorized devices from connecting to your device, and most importantly, keep the device software up-to-date. Updates have patched many of the vulnerabilities and attacks listed above.

D. Implications:

User-downloaded apps given generous device permissions, including Bluetooth access, can be exploited to identify and track devices. Location information could be used to advertise products or perform contact tracing. Users should be aware of which apps share information and how, as it can threaten user privacy. Many of these described exploits take advantage of very specific Bluetooth vulnerabilities that can be quickly patched. Consumers with Bluetooth-enabled devices can avoid many vulnerabilities by regularly installing security patches, and companies should ensure they implement best practices.

V. Zigbee

Zigbee targets low-cost wireless controls and is used to monitor and manage devices such as LED bulbs, switches, and key fobs. Zigbee, introduced as IEEE 802.15.4 in 2003, is a low-rate wireless personal area network (WPAN). The standard allows secure communications over radio frequencies [4], [24], [58], [59]. The Zigbee protocol operates using a coordinator, routers, and end devices. The coordinator manages the distribution of keys within the network. A Zigbee router controls information flow and connects the coordinator to the end devices [25]. Zigbee's three possible topologies include star, tree, and mesh, with mesh being the most flexible, allowing direct router-to-router communication. Zigbee's operating range is limited between 10-100m.

A. Applications:

Zigbee is used in industrial automation and healthcare because of its low power and design for battery conservation [24], [58], [59]. In industrial automation, Zigbee can be used to connect factory manufacturing devices to their control systems [4], [60]. In healthcare, Zigbee is used to monitor devices such as pacemakers and insulin pumps [61]. Zigbee's automated sensor applications can include home protection devices such as alarms, motion sensors, and light dimmers.

B. Vulnerabilities:

Zigbee is susceptible to both active and passive attacks due to various side-channel vulnerabilities [21], [22], [23], [25]. Five types of attacks are discussed in [28]: communication interruption, disconnection, key leakage, improper integrity check, and truncated packets.

One of the main security vulnerabilities regarding Zigbee is the ability for attackers to sniff the symmetric encryption network key that is stored in plaintext [24], [25]. Another specific attack Zigbee is vulnerable to is an End-Device Sabotage Attack that uses predictable polling rates and results in a DoS of Zigbee. A sleeping device uses polling rates so that it knows when to wake up and check if it is needed. This attack exploits those predictable polling rates to drain energy and cause power failures in devices [25], [26]. A Replay Attack [26], [27] occurs when a malicious actor captures Zigbee traffic, possibly using the KillerBee framework, to replay intercepted traffic to affect the physical devices.

Zigbee's use of carrier sense multiple access with collision avoidance (CSMA/CA) is also a liability concerning MAC-layer misbehavior [23]. A target device can be spammed by a bot and cause channels to flood. Due to the nature of the CSMA/CA protocol, the traffic with one device could cause certain channels to be busy causing a DoS attack.

C. Mitigations:

To overcome key sniffing, a recommended countermeasure is to use the High-Security level in safety-critical ZigBee-enabled systems, never transporting the network key unencrypted over-the-air [26]. Rotating the keys and secure key management can help to avoid a DoS attack. Another approach is to implement rate limiting, establishing limits on the frequency and volume of polling requests within the Zigbee network, or possibly adaptive polling based on network traffic.

Recommended mitigation approaches in [28] include address checking and verification, redefining the fixed authentication code lengths with more flexible lengths for the improper integrity check attack, protecting key leakage, adding a separate encryption key and putting the key management on the more computationally capable controller-side.

Using cyber best practices can reduce the likelihood or duration of Zigbee attacks including firmware updates, traffic monitoring, intrusion detection, and following vendor security guidelines, in addition to physically securing or tamper-proofing the devices.

D. Implications:

One of the biggest assets of Zigbee is its simplicity and straightforward security approach. This simplicity enables easy and affordable production of Zigbee devices as well as easy installation within smart homes. However, side channel and eavesdropping vulnerabilities suggest the possibility of information loss or system compromise. Using a strong key-establishment protocol and refreshing the keys can help protect the users' security and privacy, as well as following cybersecurity best practices for Zigbee devices.

VI. Qi

Qi is the first Wireless Power Transfer (WPT) standard and is currently the primary WPT standard. Qi was developed by the Wireless Power Consortium (WPC) and launched in 2008. Designed for small handheld devices of up to 5W, a current Qi protocol extension supports up to 15W devices [62]. Qi uses a primary coil and magnetic induction to transfer power to a secondary coil. The approach used is an inductive wireless charging approach [63]. Horizontal-Flux Approach or Vertical-Flux Approach [64] can be used for magnetic induction. The most commonly used approach is the Vertical-Flux Approach due to the user-friendly design allowing the charging device to be placed anywhere on the charging pad and receive power, rather than being in one specific spot [65]. A Qi charging pad can be effective for distances up to 4 cm.

A. Applications:

Qi is primarily used for charging handheld devices and medium-sized electronics. Qi's popularity has caused many devices to adapt device hardware to enable Qi compatibility [62]. Some Qi-compatible devices include Apple, Samsung, and LG mobile phones. The WPC has been developing a new Qi version 2.0, which should include a wider variety of potential uses including kitchen appliances with the Ki protocol.

B. Vulnerabilities:

Recent studies have shown that Qi is vulnerable to side-channel analyses, including eavesdropping and hijacking attacks [29], [31]. The information leaked includes a Qi ID [32] of the charger and the device charging, as well as the charge level based on the current battery charge. For instance, the power levels requested by a charging phone can indicate which website is being accessed or other actions taken on the phone, such as taking a phone call. Intercepted Qi packets could be used to track user behavior.

With Hijacking, an adversary coil could mimic the charging device and possibly request too much power (over-charge), too little power (under-charge), or no power (denial of charge) [29], [39]. There is a method of mobile phone tracking based on slight imperfections and differences in some of the phones' internal systems. These differences occur during manufacturing and are virtually impossible to prevent, including differences in a phone's audio system [35], [36], [37], [38]. These differences cause relatively no hindrance to the usage of the phone but do allow for a form of tracking [32], [33], [34]. While this method of tracking is not Qi-specific, it can occur when charging due to the phone sending signals to the charging coil.

C. Mitigations:

Encrypting the sensitive information exchanged during the Qi communication protects user privacy from tracking-based attacks. This includes encrypting device ID, charging state, and control information [29], [66]. Masking signals by randomizer, duplication methods, and dynamical switching of amplitude/frequency can mitigate eavesdropping attacks while sliding window-based anomaly detection mechanisms are proposed to defend against Hijacking attacks [67], [68].

D. Implications:

The number of privacy and security concerns with Qi can be concerning to anyone thinking about using a wireless charger. Being able to track a phone can lead to potential human tracking. Human tracking is already used today with other methods, such as Bluetooth and Wi-Fi sensors in shopping malls to track location and timestamp information on individual devices. It can be used to optimize store locations in a shopping mall, offer customized location-based ads, and map a location based on where a phone is located [69]. The range and capabilities of human tracking vary depending on what method is used, but most do not have the range to track people outside the building they are located in. With the possibility of having private information such as app usage or web browser information being disclosed, denial of charge, and even over-charging, Qi can be a highly volatile WPT standard. Given these risks, Qi is still currently the most popular WPT standard for small devices and some home appliances. Qi's new v2.0 standard is expected to address these threats and protect the users' data security and privacy, which was not publicly available at the time this paper was written.

VII. Li-Fi

Light-Fidelity (Li-Fi) is a newer visible light communication faster than Wi-Fi wireless transmission technology [42], [45], [46]. However, Wi-Fi and Li-Fi's relationship is more about cooperation and less of a competition. Li-Fi can supplement Wi-Fi in areas where Wi-Fi is weak or cannot or should not be used, such as in classified computing areas [40]. Li-Fi uses light and a transceiver as a form of communication. Unlike other light-related communication mediums, Li-Fi is fully networked, bidirectional (full-duplex), and is a high-speed wireless communication standard, IEEE 802.11bb. Li-Fi has speeds upwards of 10 Gbps depending on the use of modulation [45]. Modulation refers to how binary data is transmitted through the LED when it flickers on and off.

A. Applications:

Li-Fi uses include low-infrastructure communications, ideal for disaster relief and radio broadcasting [46]. Future applications include real-time vehicular communications for road hazard information; underwater applications avoid acoustic waves that have the potential to disrupt marine life; and in airplanes to provide high-speed data transmission without interrupting aircraft instruments and signals [46]. The range is highly variable, depending on the type of technology used to implement the Li-Fi. Li-Fi requires line-of-sight and is therefore spatially limited with no way of transmitting around solid surfaces or through walls like Wi-Fi radio.

B. Vulnerabilities:

Li-Fi is considered more secure than other wireless technologies since it does not operate on radio frequencies [42], [46], [43], [44]. According to [42], there are multiple types of attacks: Processing and Transmission Level Attacks, Input Level Attacks, Back-End Attack (especially for DoS) and Enrollment Attack. Transmission-level attack include eavesdropping and interference [40], [41]. E.g. an adversary within range can gain access to the information being transmitted [40]. Li-Fi is not effective in outdoor spaces with natural sunlight as additional light can disrupt information transmission. Li-Fi is also vulnerable to DoS attacks as an adversary can target the devices with external light sources. A dongle is an authentication mechanism that the Li-Fi environment uses to store unique IDs for each user/device. Information exchanged between the Li-Fi tag and the user is susceptible to side-channel attacks and system fraud due to the poor protection and storage space of the tag [45], [46]. Another possible vulnerability not yet deeply explored due to limited forensics tools is the copying of dongle authorizations. This can create a similar privacy concern as Qi IDs being tracked through charging stations.

C. Mitigations:

Dynamic ID updates can be used in Li-Fi dongles to protect against privacy-based attacks [70]. Li-Fi technologies should adopt and integrate multiple defense mechanisms that are already used in other short-range technologies to protect against spoofing and hijacking. Development of protocols including authentication and handover help in defending against denial of service attacks [71].

D. Implications:

Li-Fi is new and more studies are needed to understand the full extent of passive and active attack impacts. More analyses on the side-channel vulnerabilities are linked with the sophisticated Li-Fi implementations. New equipment and standards are under development and should go through extensive analyses by the community before the Li-Fi technology is deployed. As Li-Fi is vulnerable to side-channel analyses, it is important to understand the risk associated with the user data and implement mechanisms to protect the privacy of the user.

VIII. Conclusion

Short-range wireless communication technologies are susceptible to side-channel vulnerabilities due to their use of open channels. We review the vulnerabilities associated with such technologies including RFID, Bluetooth, ZigBee, Qi, and Li-Fi. Each of these technologies has different vulnerabilities. We review and categorize them into passive and active threats. Zigbee is arguably the least secure while Li-Fi is likely the safest. Zigbee and Bluetooth have been around long enough for many of these attacks to have been exploited, documented, and patched. Qi is susceptible to both hijacking and eavesdropping side-channel attacks and is also a potential source for phone tracking, which links to human tracking as well. As stated previously, despite having some vulnerabilities, Qi itself is overall safe for WPT, and Qi version 2 under development is expected to provide additional security mechanisms. LiFi is the most secure protocol discussed above. LiFi is a very short-range protocol because of the nature of its components. Though Li-Fi is very new and has not yet reached its limits, it is already widely considered much more secure than Wi-Fi. Li-Fi is ideal in windowless rooms or high-security areas. To protect user privacy and security, all short-range technologies need to address the vulnerabilities discussed, make use of the mitigation techniques listed, including industry-specific cybersecurity best practices, and explore additional security mechanisms.

References

[1] M. D. Aime, G. Calandriello, and A. Lioy, "Dependability in wireless networks: Can we rely on wifi?" *IEEE Security & Privacy*, vol. 5, no. 1, pp. 23–29, Jan 2007.

[2] A. Ismukhamedova, Y. Satimova, A. Nikiforov, and N. Miloslavskaya, "Practical studying of wi-fi network vulnerabilities," in *2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)*, July 2016, pp. 227–232.

[3] E. Al Neyadi, S. Al Shehhi, A. Al Shehhi, N. Al Hashimi, M. Qbea'H, and S. Alrabaee, "Discovering public wi-fi vulnerabilities using raspberry pi and kali linux," in *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, April 2020, pp. 1–4.

[4] J.-S. Lee, Y.-W. Su, and C.-C. Shen, "A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi," in *IECON 2007 - 33rd Annual Conference of the IEEE Industrial Electronics Society*, 2007, pp. 46–51.

[5] S. Gabsi, V. Beroulle, Y. Kieffer, H. M. Dao, Y. Kortli, and B. Hamdi, "Survey: Vulnerability Analysis of Low-Cost ECC-Based RFID Protocols against Wireless and Side-Channel Attacks," *Sensors*, vol. 21, no. 17, p. 5824, Aug. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/17/5824

[6] D. Dobrykh, D. Filonov, A. Slobozhanyuk, and P. Ginzburg, "Hardware rfid security for preventing far-field attacks," *IEEE Transactions on Antennas and Propagation*, vol. 70, no. 3, pp. 2199–2204, 2021.

[7] T. Plos, M. Hutter, and M. Feldhofer, "On Comparing Side-Channel Preprocessing Techniques for Attacking RFID Devices," in *Information Security Applications*, ser. Lecture Notes in Computer Science, H. Y. Youm and M. Yung, Eds. Berlin, Heidelberg: Springer, 2009, pp. 163–177.

[8] H. Pereira, R. Carreira, P. Pinto, and S. I. Lopes, "Hacking the RFID-based Authentication System of a University Campus on a Budget," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, Jun. 2020, pp. 1–5, iSSN: 2166-0727.

[9] M. Burmester and B. De Medeiros, "Rfid security: attacks, countermeasures and challenges," in *The 5th RFID academic convocation, the RFID journal conference*, 2007.

[10] R. Xu, L. Zhu, A. Wang, X. Du, K.-K. R. Choo, G. Zhang, and K. Gai, "Side-Channel Attack on a Protected RFID Card," *IEEE Access*, vol. 6, pp. 58 395–58 404, 2018.

[11] M. Lehtonen, D. Ostojic, A. Ilic, and F. Michahelles, "Securing rfid systems by detecting tag cloning," in *Pervasive Computing: 7th International Conference, Pervasive 2009, Nara, Japan, May 11-14, 2009. Proceedings 7*. Springer, 2009, pp. 291–308.

[12] J. Liu, H. Li, M. Sun, H. Wang, H. Wen, Z. Li, and L. Sun, "Nfceraser: A security threat of nfc message modification caused by quartz crystal oscillator," in *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2024, pp. 165–165.

[13] S. Al-Githami, Z. A. Solangi, and M. S. B. M. Rahim, "Investigation of bluetooth security issues," in *2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*. IEEE, 2023, pp. 1–4.

[14] T. Tucker, H. Searle, K. Butler, and P. Traynor, "Blue's clues: Practical discovery of non-discoverable bluetooth devices," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 3098–3112.

[15] J. Thom-Santelli, A. Ainslie, and G. Gay, "Location, location, location: a study of bluejacking practices," in *CHI '07 Extended Abstracts on Human Factors in Computing Systems*. San Jose CA USA: ACM, Apr. 2007, pp. 2693–2698. [Online]. Available: https://dl.acm.org/doi/10.1145/1240866.1241064

[16] L. Owens, "First Bluejacking, Now Bluesnarfing," 2004.

[17] D. Browning and G. Kessler, "Bluetooth Hacking: A Case Study," *Journal of Digital Forensics, Security and Law*, 2009. [Online]. Available: https://commons.erau.edu/db-security-studies/26

[18] D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "Bias: Bluetooth impersonation attacks," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 549–562.

[19] ——, "Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy," *ACM Transactions on Privacy and Security*, vol. 23, no. 3, pp. 1–28, Aug. 2020. [Online]. Available: https://dl.acm.org/doi/10.1145/3394497

[20] N. Patel, H. Wimmer, and C. M. Rebman, "Investigating Bluetooth Vulnerabilities to Defend from Attacks," in *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, Oct. 2021, pp. 549–554.

[21] Y. Meng and H. Zhu, "Wireless traffic analysis based side-channel attacks and countermeasure in smart home," in *Proceedings of the ACM Turing Award Celebration Conference-China 2023*, 2023, pp. 150–151.

[22] W. Wang, F. Cicala, S. R. Hussain, E. Bertino, and N. Li, "Analyzing the attack landscape of zigbee-enabled iot systems and reinstating users' privacy," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 133–143.

[23] Y. Cheng, E. Graves, A. Swami, and A. Sabharwal, "Estimating traffic rates in csma/ca networks: A feasibility analysis for a class of eavesdroppers," *IEEE Transactions on Wireless Communications*, 2023.

[24] A. Zohourian, S. Dadkhah, E. C. P. Neto, H. Mahdikhani, P. K. Danso, H. Molyneaux, and A. A. Ghorbani, "IoT Zigbee device security: A comprehensive review," *Internet of Things*, vol. 22, p. 100791, Jul. 2023. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2542660523001142

[25] S. Khanji, F. Iqbal, and P. Hung, "Zigbee security vulnerabilities: Exploration and evaluating," in *2019 10th International Conference on Information and Communication Systems (ICICS)*, 2019, pp. 52–57.

[26] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen, "Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned," in *2013 46th Hawaii International Conference on System Sciences*. Wailea, HI, USA: IEEE, Jan. 2013, pp. 5132–5138. [Online]. Available: http://ieeexplore.ieee.org/document/6480466/

[27] M. S. Wara and Q. Yu, "New replay attacks on zigbee devices for internet-of-things (iot) applications," in *2020 IEEE International Conference on Embedded Software and Systems (ICESS)*, Dec 2020, pp. 1–6.

[28] X. Wang and S. Hao, "Don't Kick Over the Beehive: Attacks and Security Analysis on Zigbee," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. Los Angeles CA USA: ACM, Nov. 2022, pp. 2857–2870. [Online]. Available: https://dl.acm.org/doi/10.1145/3548606.3560703

[29] Y. Wu, Z. Li, N. Van Nostrand, and J. Liu, "Time to Rethink the Design of Qi Standard? Security and Privacy Vulnerability Analysis of Qi Wireless Charging," in *Annual Computer Security Applications Conference*. Virtual Event USA: ACM, Dec. 2021, pp. 916–929. [Online]. Available: https://dl.acm.org/doi/10.1145/3485832.3485839

[30] T. Ni, X. Zhang, C. Zuo, J. Li, Z. Yan, W. Wang, W. Xu, X. Luo, and Q. Zhao, "Uncovering user interactions on smartphones via contactless wireless charging side channels," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 3399–3415.

[31] A. S. La Cour, K. K. Afridi, and G. E. Suh, "Wireless Charging Power Side-Channel Attacks," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, Nov. 2021, pp. 651–665, arXiv:2105.12266 [cs]. [Online]. Available: http://arxiv.org/abs/2105.12266

[32] D. Yang, G. Xing, J. Huang, X. Chang, and X. Jiang, "QID: Robust Mobile Device Recognition via a Multi-Coil Qi-Wireless Charging System," *ACM Transactions on Internet of Things*, vol. 3, no. 2, pp. 1–27, May 2022. [Online]. Available: https://dl.acm.org/doi/10.1145/3498904

[33] H. Bojinov, Y. Michalevsky, G. Nakibly, and D. Boneh, "Mobile Device Identification via Sensor Fingerprinting," 2014, publisher: arXiv Version Number: 1. [Online]. Available: https://arxiv.org/abs/1408.1416

[34] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. San Francisco California USA: ACM, Sep. 2008, pp. 116–127. [Online]. Available: https://dl.acm.org/doi/10.1145/1409944.1409959

[35] Y. Zheng, T. He, X. Liang, Z. Kong, L. Lin, and J. Zhao, "Body-Channel Wireless Power Transfer Employing Transmitter-Side Received Power Monitoring and Maximum Point Tracking," in *2022 IEEE Biomedical Circuits and Systems Conference (BioCAS)*. Taipei, Taiwan: IEEE, Oct. 2022, pp. 495–499. [Online]. Available: https://ieeexplore.ieee.org/document/9948696/

[36] J. T. Hwang, D. S. Lee, J. H. Lee, S. M. Park, K. W. Jin, M. J. Ko, H. I. Shin, S. O. Jeon, D. H. Kim, and J. Rhee, "21.8 An all-in-one (Qi, PMA and A4WP) 2.5W fully integrated wireless battery charger IC for wearable applications," in *2016 IEEE International Solid-State Circuits Conference (ISSCC)*. San Francisco, CA, USA: IEEE, Jan. 2016, pp. 378–380. [Online]. Available: http://ieeexplore.ieee.org/document/7418065/

[37] Y. Qu, W. Shu, Y.-C. Kuan, S.-H. W. Chiang, Y. Li, Z. Zheng, and J. S. Chang, "A 12-W 96.1%-Efficiency eFuse-Based Ultrafast Battery Charger Supporting Wireless and USB Power Inputs," in *2021 IEEE Custom Integrated Circuits Conference (CICC)*. Austin, TX, USA: IEEE, Apr. 2021, pp. 1–2. [Online]. Available: https://ieeexplore.ieee.org/document/9431525/

[38] N. Wu, P. Wang, J. Xiao, X. Wu, Z. Wang, and Y. Sun, "Synchronous Transmission of Power and Data for Wireless Power Transfer System Using Double LCC," in *2022 IEEE 9th International Conference on Power Electronics Systems and Applications (PESA)*. Hong Kong, Hong Kong: IEEE, Sep. 2022, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/10038358/

[39] C. Wang, M. Ninan, S. Reilly, J. Ward, W. Hawkins, B. Wang, and J. M. Emmert, "Portability of Deep-Learning Side-Channel Attacks against Software Discrepancies," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*.

Guildford United Kingdom: ACM, May 2023, pp. 227–238. [Online]. Available: https://dl.acm.org/doi/10.1145/3558482.3590177

[40] E. Ramadhani and G. P. Mahardika, "The Technology of LiFi: A Brief Introduction," *IOP Conference Series: Materials Science and Engineering*, vol. 325, p. 012013, Mar. 2018. [Online]. Available: https://iopscience.iop.org/article/10.1088/1757-899X/325/1/012013

[41] D. Yucebas and H. Yuksel, "Power analysis based side-channel attack on visible light communication," *Physical Communication*, vol. 31, pp. 196–202, Dec. 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1874490717304913

[42] M. Arfaoui, M. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. Assi, and H. Haas, "Physical Layer Security for Visible Light Communication Systems: A Survey," *IEEE Communications Surveys & Tutorials, Communications Surveys & Tutorials, IEEE, IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1887–1908, Jan. 2020, publisher: IEEE.

[43] D. B. Kuttan, S. Kaur, B. Goyal, and A. Dogra, "Light Fidelity: A future of wireless communication," in *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*. Trichy, India: IEEE, Oct. 2021, pp. 308–312. [Online]. Available: https://ieeexplore.ieee.org/document/9591685/

[44] A. Thaljaoui, S. El Khediri, S. Zeadally, and A. Alourani, "Remote monitoring system using Light Fidelity and InfraRed technologies," *Computers and Electrical Engineering*, vol. 101, p. 108073, Jul. 2022. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0045790622003287

[45] L. Singh, M. Rout, J. Bishal, and J. Ratnam, "Data transfer using light fidelity (li-fi) technology—a methodological comparative study," in *Biologically Inspired Techniques in Many Criteria Decision Making: Proceedings of BITMDM 2021*. Springer, 2022, pp. 315–321.

[46] S. Gönen, H. H. Sayan, G. Karacayilmaz, E. SiNdiRen, F. Üstünsoy, H. Artuner, E. N. Yilmaz, and M. F. Işik, "A New Approach in Cyber Security of Industrial Control Systems: Li-Fi," *Politeknik Dergisi*, vol. 25, no. 2, pp. 895–902, Jun. 2022. [Online]. Available: http://dergipark.org.tr/en/doi/10.2339/politeknik.976886

[47] A. Juels, "Rfid security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, 2006.

[48] W. Yao, C.-H. Chu, and Z. Li, "The use of RFID in healthcare: Benefits and barriers," in *2010 IEEE International Conference on RFID-Technology and Applications*. Guangzhou, China: IEEE, Jun. 2010, pp. 128–134. [Online]. Available: http://ieeexplore.ieee.org/document/5529874/

[49] C. Saygin, "Adaptive inventory management using RFID data," *The International Journal of Advanced Manufacturing Technology*, vol. 32, no. 9-10, pp. 1045–1051, Mar. 2007. [Online]. Available: http://link.springer.com/10.1007/s00170-006-0405-x

[50] A. Sarac, N. Absi, and S. Dauzère-Pérès, "A literature review on the impact of RFID technologies on supply chain management," *International Journal of Production Economics*, vol. 128, no. 1, pp. 77–95, Nov. 2010. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0925527310002835

[51] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. O'hare, "Vulnerabilities in first-generation rfid-enabled credit cards," in *Financial Cryptography and Data Security: 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, February 12-16, 2007. Revised Selected Papers 11*. Springer, 2007, pp. 2–14.

[52] F. Michahelles, F. Thiesse, A. Schmidt, and J. R. Williams, "Pervasive RFID and Near Field Communication Technology," *IEEE Pervasive Computing*, vol. 6, no. 3, pp. 94–96, c3, Jul. 2007. [Online]. Available: http://ieeexplore.ieee.org/document/4287450/

[53] E. Ferro and F. Potorti, "Bluetooth and wi-fi wireless protocols: a survey and a comparison," *IEEE Wireless Communications*, vol. 12, no. 1, pp. 12–26, 2005.

[54] M. A. Al-Shareeda, M. A. Saare, S. Manickam, and S. Karuppayah, "Bluetooth low energy for internet of things: review, challenges, and open issues," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 2, p. 1182, Aug. 2023. [Online]. Available: https://ijeecs.iaescore.com/index.php/IJEECS/article/view/31257

[55] M. Siekkinen, M. Hiienkari, J. K. Nurminen, and J. Nieminen, "How low energy is bluetooth low energy? Comparative measurements with ZigBee/802.15.4," in *2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Apr. 2012, pp. 232–237.

[56] C. Bisdikian, "An overview of the Bluetooth wireless technology," *IEEE Communications Magazine*, vol. 39, no. 12, pp. 86–94, Dec. 2001.

[57] K. Mikhaylov, N. Plevritakis, and J. Tervonen, "Performance Analysis and Comparison of Bluetooth Low Energy with IEEE 802.15.4 and SimpliciTI," *Journal of Sensor and Actuator Networks*, vol. 2, no. 3, pp. 589–613, Aug. 2013. [Online]. Available: http://www.mdpi.com/2224-2708/2/3/589

[58] H. Li, Z. Jia, and X. Xue, "Application and Analysis of ZigBee Security Services Specification," in *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*. Wuhan, China: IEEE, 2010, pp. 494–497. [Online]. Available: http://ieeexplore.ieee.org/document/5480941/

[59] W. Wang, F. Cicala, S. R. Hussain, E. Bertino, and N. Li, "Analyzing the Attack Landscape of Zigbee-Enabled IoT Systems and Reinstating Users' Privacy," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 133–143, event-place: Linz, Austria. [Online]. Available: https://doi.org/10.1145/3395351.3399349

[60] Y. Yao, P. Sun, X. Liu, Y. Wang, and D. Xu, "Simultaneous Wireless Power and Data Transfer: A Comprehensive Review," *IEEE Transactions on Power Electronics*, vol. 37, no. 3, pp. 3650–3667, Mar. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9560041/

[61] Dayu He, "The ZigBee Wireless Sensor Network in medical care applications," in *2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering*. Changchun, China: IEEE, Aug. 2010, p. 5610435. [Online]. Available: http://ieeexplore.ieee.org/document/5610435/

[62] Y. Yang, S.-C. Tan, and S. Y. Ron Hui, "Communication-Free Control Scheme for Qi-Compliant Wireless Power Transfer Systems," in *2019 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2019, pp. 4955–4960.

[63] X. Mou and H. Sun, "Wireless power transfer: Survey and roadmap," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*. IEEE, 2015, pp. 1–5.

[64] S. Y. Hui, "Planar Wireless Charging Technology for Portable Electronic Products and Qi," *Proceedings of the IEEE*, vol. 101, no. 6, pp. 1290–1301, Jun. 2013. [Online]. Available: http://ieeexplore.ieee.org/document/6481427/

[65] X. Dang, P. Jayathurathnage, F. Liu, S. A. Al Mahmud, C. R. Simovski, and S. A. Tretyakov, "High-Efficiency Omnidirectional Wireless Power Transfer System," *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, vol. 3, no. 3, pp. 403–410, Jul. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9723531/

[66] J. Liu, X. Zou, L. Zhao, Y. Tao, S. Hu, J. Han, and K. Ren, "Privacy leakage in wireless charging," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[67] L. Benini, A. Macii, E. Macii, E. Omerbegovic, F. Pro, and M. Poncino, "Energy-aware design techniques for differential power analysis protection," in *Proceedings of the 40th Annual Design Automation Conference*, 2003, pp. 36–41.

[68] S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach," in *Design, Automation and Test in Europe*. IEEE, 2005, pp. 64–69.

[69] M. R. Ali Sarker, M. Hassanuzzaman, P. Biswas, S. H. Dadon, T. Imam, and T. Rahman, "An Efficient Surface Map Creation and Tracking Using Smartphone Sensors and Crowdsourcing," *Sensors*, vol. 21, no. 21, p. 6969, Oct. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/21/6969

[70] A. Sarker, S. Byun, M. Raavi, J. Kim, J. Kim, and S.-Y. Chang, "Dynamic id randomization for user privacy in mobile network," *ETRI Journal*, vol. 44, no. 6, pp. 903–914, 2022.

[71] I. I. A. Sulayman, R. He, M. Manka, A. Ning, and A. Ouda, "Lifi/wifi authentication and handover protocols: Survey, evaluation, and recommendation," in *2021 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2021, pp. 1–6.