On the Security of the Wireless Electric Vehicle Charging Communication

Sebastian Köhler, Simon Birnbach, Richard Baker, and Ivan Martinovic
Department of Computer Science
University of Oxford

***Abstract*—The adoption of fully Electric Vehicles (EVs) is happening at a rapid pace. To make the charging as fast and convenient as possible, new charging approaches are developed constantly. One such approach is wireless charging, also known as Wireless Power Transfer (WPT). Instead of charging an EV via a charging cable, the battery is charged wirelessly. For safety and efficiency reasons, the vehicle and the charging station continuously exchange critical information about the charging process. This includes, *e.g.*, the maximum voltage and current, battery temperature, and State of Charge (SoC). Since there is no physical connection between the vehicle and the charging station, this necessary control communication has to be implemented as a wireless connection. However, if the communication is interrupted, the charging process is aborted for safety reasons.**

In this paper, we analyze the attack surface of EV charging standards that use such a wireless control communication. More specifically, we discuss potential wireless attacks that can violate the availability and analyze the implemented security features of a real-world wireless charging station that has already been deployed. We found that the tested charging station does not implement even simple security measures, such as IEEE 802.11w, that can protect the communication from denial-of-service attacks. Finally, we discuss potential countermeasures, and give recommendations to improve the security and increase the resilience of wireless charging.

I. Introduction

Nowadays, Electric Vehicles (EVs) are mainly charged using conductive charging, *i.e.*, a charging cable is directly plugged into the vehicle inlet of the car for power delivery. However, there is a need to reduce charging times and to increase the convenience for the driver while still trying to reduce the battery costs and size [33]. To this end, new technologies have been developed to facilitate charging. One such approach is wireless charging, also known as Wireless Power Transfer (WPT). As the name indicates, the vehicle is charged without a physical connection to the charging station. Once the vehicle is located above the WPT pad, the battery is charged wirelessly. Figure 1 illustrates such a wireless charging station.

Since no user interaction is required, wireless charging increases the convenience for the driver. This can be particularly beneficial for car sharing companies that do not need to rely on the customer to connect the vehicle to a charging station after the rental, or for autonomous vehicles in the future. Once the vehicle is parked in the designated wireless charging bay, it is automatically charged. Moreover, taxis and buses can particularly benefit from interaction-less charging. So-called opportunity charging enables them to charge while they wait for passengers [15], [4]. However, vehicles can also be charged wirelessly while driving [7], [29]. Finally, wireless charging is thought to improve the Vehicle-2-Grid (V2G) communication and facilitate bidirectional charging [1], [19].

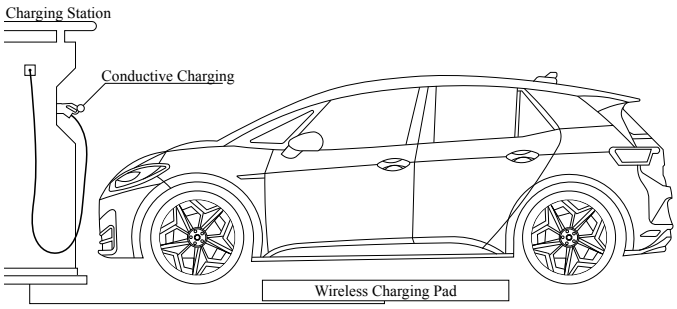

Fig. 1: Typical setup of a charging station providing the opportunity to charge wired or wireless.

Independent of the type of power transfer, wired or wireless, most charging standards, such as the Combined Charging System (CCS), CHAdeMO, Tesla's supercharger, and GB/T 20234, rely on a communication between the electric vehicle and the charging station to exchange vital information that is required to ensure a safe and efficient charging process. With conductive charging, this communication is realized via the charging cable, but with WPT, there is no physical connection, so control communication must be wireless. In any case, the availability of the communication is crucial, and if it fails or a timeout occurs, the charging session will be aborted for safety reasons [23], [26]. The researchers in [26] showed that the power-line communication (PLC) used by CCS, and thus the charging process can be interrupted by electromagnetic interference. Apart from depleted batteries and inconveniences for the driver, the interruption of charging sessions can have severe consequences, such as power instabilities. Due to the integration of electric vehicles into the power grid as a buffer to meet demand peaks, they contribute to its stability and can be considered part of the critical infrastructure [31]. Based on these observations, we hypothesize that the loss of WiFi communication between the vehicle and the wireless charging station causes the same effects as observed by the researchers in [26].

In this paper, we focus on the security of WPT that implements the High-Level Communication (HLC) between the vehicle and the charging station following the ISO 15118-8 and IEEE 802.11 standard. We focus in particular on the availability of communication, as it is crucial for the charging process, and as without a stable communication link, charging is not possible. In contrast to previous work, our work targets the WiFi-based communication, which does not require special

equipment, such as a software-defined radio, and can be executed with cheap off-the-shelf hardware, making it easier for an adversary to conduct. To the best of our knowledge, we are the first to analyze the attack surface of the wireless control communication used by wireless EV charging stations and to conduct a passive security evaluation of a real-world deployment.

In summary, we make the following contributions:

- We conduct a passive security evaluation of the WiFi network used by a wireless charging station in a real-world deployment.
- We find that the WiFi-based control communication of the analyzed charger is potentially vulnerable to denial-of-service attacks.
- We give recommendations to increase the security and resilience of wireless charging communication.

II. Electric Vehicle Charging

In contrast to vehicles with combustion engines, the main drawbacks of EVs are the reduced range and the longer recharging time. To counteract these limitations, new charging technologies have been developed over the years. In this section, we give a brief overview of the different EV charging standards and their underlying technical concepts and terminologies.

A. Wired

At present, wired charging is the most widely used charging approach for electric vehicles. A charging cable establishes a physical, conductive connection between the vehicle and the charging station, which is used for power delivery. Depending on the charging standard, the electric current can either be Alternating Current (AC) or Direct Current (DC). The main difference between AC and DC charging is the maximum charging capacity. Since AC charging requires the vehicle to be equipped with a rectifier, which converts the alternating current to direct current, the charging capacity for AC is often limited by the maximum possible size and weight of the rectifier. In DC charging, on the other hand, the rectifier is located in the charging station, which increases the power output and allows high-power charging with up to 350 kW. The higher charging capacity significantly shortens the charging time and makes it the first choice for charging electric vehicles. Four major DC rapid-charging standards exist — the Combined Charging System (CCS), CHAdeMO, Tesla's supercharger, and GB/T 20234. While CCS is the most widely used standard in the European and North American markets, CHAdeMO and GB/T 20234 are common in Asia [11]. In contrast, Tesla's supercharger technology is proprietary and can be found worldwide.

B. Wireless

The limitations of conductive charging have led to the development of wireless charging, also known as Wireless Power Transfer (WPT), as an alternative [30]. Instead of connecting the charging station via the charging cable to the vehicle's charging inlet, the battery is charged as soon as the vehicle is positioned above a so-called wireless power transfer pad [15]. The advantages of this concept are self-evident. The most important one is that a vehicle can be charged without a physical connection. As a result, no user interaction is required. This enables so-called opportunity charging, *i.e.*, charging as soon as the vehicle is located above a WPT pad. Typical examples are a bus stopping to let passengers board at the bus stop and a taxi waiting for customers at a taxi stand [15], [4]. Researchers have shown that opportunity charging enables the reduction of battery size and consequently the reduction of cost for the vehicle [28]. In addition to opportunity charging, wireless charging can also be used to charge a vehicle while it is in motion [29], [7]. While induction is currently the most widely adopted approach, power delivery can be via magnetic-resonant, capacitive, magnetic gear, laser, or microwave charging [1].

C. High-Level Communication

In order to ensure a safe and perfectly optimized charging process, all of the aforementioned DC rapid-charging standards rely on a communication between the vehicle and the charging station. The two entities constantly exchange messages with important information, such as maximum possible voltage, required current, battery temperature, and the State of Charge (SoC). Depending on the charging standard, the used communication technology varies. For example, CCS implements basic, low-level communication using a pulse-width modulation (PWM) protocol defined in the IEC 61851 standard [20], which is used to initialize the communication. Once successfully initialized, a high-bandwidth IP link via power-line communication (PLC) is established [23]. The other three DC rapid-charging standards CHAdeMO, Tesla's supercharger, and GB/T 20234, use CAN for the charging communication. Even though the charging standards differ in the underlying communication technology, they all have one thing in common — they use a wired communication.

Without a physical connection between the vehicle and the charging station, WPT requires the implementation of the control communication via a wireless link. However, even vehicles that use conductive charging, such as buses with pantographs, sometimes use a wireless communication [32]. In general, the implementation details for the wireless charging communication are governed by the ISO 15118-8 and 15118-20 standard [24], [22]. On the physical layer, IEEE 802.11n, often referred to as Wireless LAN (WLAN) or WiFi, is used [24]. According to the standard, the Supply Equipment Communication Controller (SECC) operates as the Access Point (AP) for the wireless network and can control the charging session of one or more power outlets [24]. This means the EV Charging Controller (EVCC) acts as the station (STA) or client and connects to the SECC once in close proximity. In order to ensure that the EV connects to the correct charging station even if another access point is already broadcasting the same SSID, the ISO 15118-8 standard recommends that the

SECC includes a so-called Vendor Specific Element (VSE) in the beacon frames to uniquely identify itself [24]. Once successfully connected, the vehicle and the charger are ready to start the charging process.

III. Threat Model

A. Goals

In this paper, we focus on an adversary who wants to disrupt the control communication and cause the charging session of one or more vehicles to abort. The incentives for such an attack can vary widely, with the simplest motivation being just for "fun and profit". However, a more sophisticated attacker might aim to cause more serious problems. In this category, we consider an attacker seeking widespread disruption of transportation and critical infrastructure, as well as potential instability in the power grid. This could either be by causing a denial-of-service of the charging communication in a larger scale or by gaining access to the wireless network and interfering with the V2G communication. At the same time, the attacker wants to conduct the attack in a stealthy, fast, and scalable manner.

B. Capabilities

Due to the low entry barrier for carrying out denial-of-service attacks against WiFi communication, we assume that the malicious actor needs none to little knowledge in the area of wireless communications and digital signal processing. Many detailed step-by-step tutorials and video resources on how to get started are available online for free. In addition, offensive security Linux distributions, such as Kali Linux, already provide a large selection of suitable tools (*e.g.*, aircrack-ng) to assess WiFi network security and conduct attacks. Moreover, unlike attacks against other communication technologies, most WiFi attacks do not require special equipment, such as a software-defined radio. Instead, they can be executed with cheap off-the-shelf hard- and software, for example, an external USB WiFi card and free, open-source software. Finally, due to the widespread use of WiFi, suitable amplifiers with high output power are cheap and widely available and can be used to further amplify the attack signal and increase the attack radius.

IV. Attack Surface

In this section, we give an overview of well-known attacks against WiFi networks and how they can impact wireless vehicle charging. While a plethora of attacks could be carried out, we will focus on attacks that violate the availability of the communication and cause the charging session to abort.

A. Gaining Access to the WiFi Network

One of the most significant risks for WiFi networks is the unauthorized access to the network by an adversary. The risk is exceptionally high for networks that use a pre-shared key (PSK). If the pre-shared key is leaked, anyone who knows the secret can join the network. In the following, we give a short overview of potential attacks an adversary can conduct once they have successfully infiltrated the network and how these attacks can affect the availability of the charging communication.

Spoofing Messages: The ISO 15118-20 standard states that "all data sent over the WLAN is in plain text unless specific encryption protocols are implemented" [22]. Once the attacker has access to the wireless network, it is easy for them to inject malicious packets and impersonate the vehicle or charging station. This would allow the adversary to spoof various messages, for example, the SessionStopReq message, which ends the charging session [21]. However, with the introduction of Vehicle-2-Grid communication and bidirectional charging, the adversary could also manipulate messages that specify the grid demand to trick the vehicle into providing less power than actually required.

Spoofing Access Point: As described in Section II-C, the WiFi access point in the SECC advertises itself by broadcasting beacon frames with a unique VSE. If the attacker is in possession of the VSE and the pre-shared key, they can set up an evil twin AP with the same SSID and secret to trick the EV into connecting to them. Since the EV connects to the AP based on the Received Signal Strength Indicator (RSSI), the adversary only needs to ensure that their malicious access point has a higher output power to overshadow the legitimate signal. This would cause the EV to connect to the rogue access point instead. Normally, the vehicle does not automatically disconnect from the SECC even if the RSSI of the evil twin AP is higher. Nevertheless, this approach can be used to prevent establishing a connection in the first place.

B. Denial-of-Service (DoS)

As described earlier, the communication is crucial for the charging process. Without a stable connection, the charging process will be aborted for safety reasons. In this section, we discuss known attacks against WiFi that violate the availability and can cause the disruption of the charging session.

Deauthentication Attack: Most WiFi networks are known to be vulnerable to a simple, so-called deauthentication attack [5], [14]. This attack exploits the lack of encryption and authentication of the management frames. Before a WiFi client disconnects from a network, it sends a deauthentication frame to the AP it is connected to. However, the deauthentication frame is not authenticated, and can therefore be spoofed and sent by a malicious actor. Once deauthenticated, the AP does no longer accept data frames from the client. Continuously transmitting the spoofed deauthentication frame can prevent the client from communication with the AP indefinitely [5]. In the context of WPT, this could cause the charging session to abort. With the introduction of IEEE 802.11w, these deauthentication messages must be authenticated, limiting the broadcast to the legitimate station [38]. By default, IEEE 802.11 networks that use WPA3 need to follow the IEEE 802.11w standard [38], [43]. However, as recent research by [38] has shown, even networks that use WPA3 can be vulnerable to deauthentication attacks.

Exploiting Media Access Control: Before transmission, a

Fig. 2: Results of the WiFi network scan conducted with a WiFi Pineapple, showing the usage of WPA2 (PSK) and the lack of management frame protection (MFP).

WiFi client checks the transmission medium to ensure that no other node is communicating to avoid interference [8]. However, this medium access control mechanism, known as Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA), has been shown to be exploitable to prevent the WiFi clients from communicating and to cause a denial-of-service [44], [5], [8]. In general, the adversary tricks the client into thinking that the communication medium is busy in order to force them to wait for a substantial time before transmitting. One example of such an attack is the so-called Queensland attack, which exploits the Network Allocation Vector (NAV) that allows a client to set its transmission duration. All clients receiving this frame will only transmit once they waited for the specified time. An attacker can set the NAV to a high value to force clients to wait a long time before sending [8].

Physical-layer Jamming: In contrast to the previously introduced attacks, which exploit vulnerabilities in the protocol, another way to cause a denial-of-service is the disruption of the communication on the physical layer. Like any other wireless communication, WiFi is susceptible to electromagnetic interference. The most straightforward approach is broadband noise jamming [35]. As the name indicates, noise is emitted in the entire spectrum in which WiFi is operating. This increases the background noise at the receiver and decrease the Signal-to-Noise Ratio (SNR) of the communication. As a result, the receiver cannot decode the legitimate signal anymore, causing the communication to fail [35]. However, such jamming attacks are easily detectable and expensive in terms of energy and hardware requirements. As such, smarter approaches, for example, reactive jamming, have been proposed. Instead of continuously emitting noise, the adversary only transmits a burst of noise to destroy the pilot tone [35].

V. Real-world Evaluation

To get an initial sense of the security measures implemented by wireless charging stations that have already been deployed in the real world, we evaluated the security of the wireless communication of an inductive charging station. The analyzed charging station was part of a public trial. We would like to emphasize that this evaluation was conducted solely passively and within legal boundaries. At all times, we ensured that our experiments did not interfere or tamper with wireless communications. Due to the responsible disclosure, we cannot reveal any details about the tested vehicle and charging station. However, the setup was similar to the one depicted in Figure 1.

A. Method

To collect information about the security features of the WiFi network used by the SECC and EVCC, we used a WiFi Pineapple Mark VII and a laptop running Kali Linux together with an external WiFi adapter, which supported 2.4 and 5GHz. We set both devices into monitoring mode to capture the probe requests from the EV and the beacon frames from the charging station in both frequency bands. Once we identified the BSSID of the SECC AP, we began collecting only frames destined for that AP. We then extracted the information about the network capabilities from the collected beacon frames.

B. Observations & Discussion of Countermeasures

During the passive evaluation of the WiFi communication, we detected multiple security flaws that could be exploited by a malicious actor.

Unprotected Management Frames: The most prominent security risk that we observed was the use of unprotected management frames that would allow an adversary to deauthenticate the vehicle and thus disrupt the charging session. Figure 2 shows the results of one of the WiFi network scans we performed and the absence of Management Frame Protection (MFP). As described earlier, it is recommended that WiFi networks follow the IEEE 802.11w standard and use MFP [37]. Because of this, it was surprising to see that the standard, which was introduced over ten years ago, has not been implemented. While we have not tried to spoof management frames and deauthenticate the vehicle from the charging station during the charging process, we are confident that a DoS attack would be successful due to the lack of MFP.

WPA2 (PSK): Another problem was the usage of the outdated Wi-Fi Protected Access 2 (WPA2) security protocol together with a pre-shared key. Since the PSK is static and needs to be known by the charging station and the vehicle, it can either be brute-forced offline or extracted from the firmware of the EVCC/SECC. Once the key has become public knowledge, anyone could connect to the charging station and eavesdrop on the traffic or interfere with the communication. Another disadvantage of PSKs is the high complexity of the key management. A compromised key would need to be replaced in all charging stations or EVs to guarantee a smooth operation and avoid incompatibilities. We have not tried to brute-force the key, however, given the cheap and easy access to high-performance cloud computing, we consider the risk to be high, especially if an easily guessed PSK is used.

In addition to the susceptibility of WPA2 (PSK) to brute-force attacks, WPA2 has been shown to be vulnerable to more sophisticated attacks. Recent research has shown that the KRACK vulnerability in WPA2 [41], which was disclosed in 2017, is still not patched in some devices and software implementations [37]. While we did not test the charging station for such vulnerabilities, it is possible that such a vulnerability is present. Given the known issues with WPA2

and the availability of the newer and more secure WPA3 protocol, we recommend, in line with the ISO 15118-20 standard, the usage of WPA3-Enterprise. Although attacks against WPA3 have also been demonstrated [13], [42], WPA3 reduces the attack surface for brute-force attacks and solves the problem of unprotected management frames since they are mandatory in the standard [43].

Only 2.4 GHz: Finally, we noticed that the access point only operated in the 2.4 GHz frequency band. This was somewhat unexpected since the ISO 15118-8 standard specifies the implementation of dual-band WiFi for WPT [24], which means the SECC and EVCC can communicate via 2.4 and 5 GHz. Using dual-band WiFi is a straightforward approach to harden the communication against interference. Since various other devices and technologies, such as microwaves, Bluetooth, and ZigBee, operate at around 2.4 GHz, the frequency band is usually more crowded and more likely to experience interference [39]. Moreover, the 5 GHz band provides more channels, making it more difficult for an adversary to jam the entire spectrum simultaneously.

VI. Related Work

A. Security of WiFi Communication

The security of WiFi networks has been extensively discussed in the literature [36], [18], [9], [45]. In particular, attacks that violate the availability of the communication have been demonstrated. The most well-known one is the exploitation of unprotected management frames, which enables an unauthorized adversary to spoof deauthentication frames and deauthenticate and disconnect clients [5], [14]. In addition, attacks that exploit the medium access control to disrupt a communication have been shown in [40], [44], [27], [34], and the effects of physical-layer interference have been studied in [6], [16], [17].

Apart from attacks that target the availability, a large body of work has focused on the confidentiality and integrity of WiFi networks. More specifically, researchers have presented attacks that allow an attacker to join the network, decrypt the traffic or eavesdrop on the communication [41], [13], [42]. The authors in [41] showed that the 4-way handshake in WiFi networks that implement WPA2 is vulnerable to key reinstallation attacks. This enables an adversary to decrypt, replay and forge packets. With WPA3, the security of WiFi networks was further improved by replacing pre-shared key authentication with Simultaneous Authentication of Equals (SAE). Nevertheless, researchers in [42] and [13] have demonstrated successful attacks against the newly introduced protocol.

B. Security of EV Charging

While the security of wireless communications has been studied extensively, the implications and transferability to the field of electric vehicle charging have not yet been analyzed. In general, the security of EV charging is an active field of research [25]. For example, a theoretical analysis of the attack surface of the charging communication of the Combined Charging System was presented by [3]. The potential of a relay attack against the CCS charging communication was discussed in [10]. Recent research has also demonstrated real-world attacks against CCS. The researchers showed that the unshielded charging cable leaks signals of the PLC-based charging communication, which allow an adversary to eavesdrop wirelessly on the communication [2]. At the same time, it has been shown by researchers in [26] that the power-line communication is susceptible to electromagnetic interference, which can cause the charging process to abort. Intentional electromagnetic interference can also be used to manipulate the readings of the voltage and current sensors in a charging station, which could potentially lead to overcharging the battery [12]. Nevertheless, to the best of our knowledge, our paper is the first that evaluates the attack surface of wireless communication in the setting of wireless EV charging.

VII. Limitations & Future Work

We consider this paper to be work in progress, but believe that it is an essential and initial contribution that helps manufacturers and charge point operators to improve the security of wireless EV charging, and lays the basis for further analysis. The main limitation of our work is the lack of evaluation of active and more sophisticated attacks. However, interfering with the communication in a real-world deployment could cause issues for other parties in the proximity. Hence, we limited our evaluation to the passive observation of the wireless spectrum. We are working closely with industry and government agencies to extend our evaluation and to conduct the experiments in a controlled laboratory environment, but we consider this outside the scope of this paper. In the next step, we will expand our analysis and investigate attacks that are not only targeting the availability of the communication, *e.g.*, relay attacks, as recently presented by researchers in [10].

VIII. Conclusions

In this paper, we analyzed the attack surface of the WiFi-based control communication used by wireless charging stations in the context of denial-of-service attacks. We conducted a real-world evaluation of the security features implemented by a wireless charging station, which was part of a public trial. We found that the WiFi network did not even use simple measures (IEEE 802.11w) to protect against DoS attacks. Based on our insights, we gave recommendations on how to further increase the security of the communication. Our observations lay the basis for further and more in-depth analysis of the attack surface of the wireless control communication and help manufacturers and charging station operators to harden their products.

Acknowledgments

The authors gratefully acknowledge the kind support of Armasuisse S+T.

References

[1] A. Ahmad, M. S. Alam, and R. Chabaan, "A comprehensive review of wireless charging technologies for electric vehicles," IEEE transactions on transportation electrification, vol. 4, no. 1, pp. 38–63, 2017.

[2] R. Baker and I. Martinovic, "Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging," in 28th USENIX Security Symposium (USENIX Security 19). Santa Clara, CA: USENIX Association, 2019.

[3] K. Bao, H. Valev, M. Wagner, and H. Schmeck, "A threat analysis of the vehicle-to-grid charging protocol ISO 15118," Computer Science-Research and Development, vol. 33, no. 1-2, pp. 3–12, 2018.

[4] BBC, "Wireless taxi charging to be trialled at Nottingham station," 2020, https://www.bbc.co.uk/news/uk-england-nottinghamshire-51140689.

[5] J. Bellardo and S. Savage, "802.11 Denial-of-Service attacks: Real vulnerabilities and practical solutions," in 12th USENIX Security Symposium (USENIX Security 03), 2003.

[6] A. Benslimane, M. Bouhorma et al., "Analysis of jamming effects on ieee 802.11 wireless networks," in 2011 IEEE International Conference on Communications (ICC). IEEE, 2011, pp. 1–5.

[7] J. Bolger, F. Kirsten, and L. Ng, "Inductive power coupling for an electric highway system," in 28th IEEE vehicular technology conference, vol. 28. IEEE, 1978, pp. 137–144.

[8] B. Chen, V. Muthukkumarasamy, N. Guimaraes, P. Isaias, and A. Goikoetxea, "Denial of service attacks against 802.11 dcf," in Proceedings of the IADIS International Conference: Applied Computing. Citeseer, 2006.

[9] J.-C. Chen, M.-C. Jiang, and Y.-w. Liu, "Wireless lan security and ieee 802.11 i," IEEE Wireless Communications, vol. 12, no. 1, pp. 27–36, 2005.

[10] M. Conti, D. Donadel, R. Poovendran, and F. Turrin, "Evexchange: A relay attack on electric vehicle charging system," arXiv preprint arXiv:2203.05266, 2022.

[11] H. Das, M. Rahman, S. Li, and C. Tan, "Electric vehicles standards, charging infrastructure, and impact on grid integration: A technological review," Renewable and Sustainable Energy Reviews, vol. 120, p. 109618, 2020.

[12] G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane, "Electromagnetic sensor and actuator attacks on power converters for electric vehicles," in 2020 IEEE Security and Privacy Workshops (SPW). IEEE, 2020, pp. 98–103.

[13] D. de Almeida Braga, P.-A. Fouque, and M. Sabt, "Dragonblood is still leaking: Practical cache-based side-channel in the wild," in Annual Computer Security Applications Conference, 2020, pp. 291–303.

[14] P. Ebbecke, "Protected Management Frames enhance Wi-Fi® network security," 2020, https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security.

[15] T. M. Fisher, K. B. Farley, Y. Gao, H. Bai, and Z. T. H. Tse, "Electric vehicle wireless charging technology: a state-of-the-art review of magnetic coupling systems," Wireless Power Transfer, vol. 1, no. 2, pp. 87–96, 2014.

[16] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of rf interference on 802.11 networks," ACM SIGCOMM Computer Communication Review, vol. 37, no. 4, pp. 385–396, 2007.

[17] I. Harjula, J. Pinola, and J. Prokkola, "Performance of ieee 802.11 based wlan devices under various jamming signals," in 2011-MILCOM 2011 Military Communications Conference. IEEE, 2011, pp. 2129–2135.

[18] K. J. Hole, E. Dyrnes, and P. Thorsheim, "Securing wi-fi networks," Computer, vol. 38, no. 7, pp. 28–34, 2005.

[19] X. Huang, H. Qiang, Z. Huang, Y. Sun, and J. Li, "The interaction research of smart grid and ev based wireless charging," in 2013 IEEE vehicle power and propulsion conference (VPPC). IEEE, 2013, pp. 1–5.

[20] IEC 61581, Electric vehicle conductive charging system. Genf, Schweiz: IEC, 2017.

[21] ISO 15118-2, Road vehicles – Vehicle to grid communication interface – Network and application protocol requirements. Genf, Schweiz: ISO, 2014.

[22] ISO 15118-20, Road vehicles – Vehicle to grid communication interface – Part 20: 2nd generation network layer and application layer requirements. Genf, Schweiz: ISO, 2022.

[23] ISO 15118-3, Road vehicles - Vehicle to grid communication interface – Part 3: Physical and data link layer requirements. Genf, Schweiz: ISO, 2015.

[24] ISO 15118-8, Road vehicles – Vehicle to grid communication interface – Part 8: Physical layer and data link layer requirements for wireless communication. Genf, Schweiz: ISO, 2020.

[25] J. Johnson, T. Berg, B. Anderson, and B. Wright, "Review of electric vehicle charger cybersecurity vulnerabilities, potential impacts, and defenses," Energies, vol. 15, no. 11, p. 3931, 2022.

[26] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Brokenwire: Wireless disruption of ccs electric vehicle charging," arXiv preprint arXiv:2202.02104, 2022.

[27] P. Kyasanur and N. H. Vaidya, "Selfish mac layer misbehavior in wireless networks," IEEE transactions on mobile computing, vol. 4, no. 5, pp. 502–516, 2005.

[28] S. Lukic and Z. Pantic, "Cutting the cord: Static and dynamic inductive wireless charging of electric vehicles," IEEE Electrification Magazine, vol. 1, no. 1, pp. 57–64, 2013.

[29] S. D. Manshadi, M. E. Khodayar, K. Abdelghany, and H. Üster, "Wireless charging of electric vehicles in electricity and transportation networks," IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4503–4512, 2017.

[30] S. A. Q. Mohammed and J.-W. Jung, "A comprehensive state-of-the-art review of wired/wireless charging technologies for battery electric vehicles: Classification/common topologies/future research issues," IEEE Access, vol. 9, pp. 19 572–19 585, 2021.

[31] F. Mwasilu, J. J. Justo, E.-K. Kim, T. D. Do, and J.-W. Jung, "Electric vehicles and smart grid interaction: A review on vehicle to grid and renewable energy sources integration," Renewable and sustainable energy reviews, vol. 34, pp. 501–516, 2014.

[32] OppCharge, "OppCharge," 2020, https://www.oppcharge.org/.

[33] L. Patnaik, P. S. Huynh, D. Vincent, and S. S. Williamson, "Wireless opportunity charging as an enabling technology for ev battery size reduction and range extension: Analysis of an urban drive cycle scenario," in 2018 IEEE PELS Workshop on Emerging Technologies: Wireless Power Transfer (Wow). IEEE, 2018, pp. 1–5.

[34] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," IEEE Communications surveys & tutorials, vol. 13, no. 2, pp. 245–257, 2010.

[35] R. A. Poisel, Modern Communications Jamming Principles and Techniques, 2nd ed. Norwood, MA, USA: Artech House, Inc., 2011.

[36] B. Potter and B. Fleck, 802.11 Security. " O'Reilly Media, Inc.", 2002.

[37] D. Schepers, A. Ranganathan, and M. Vanhoef, "Let numbers tell the tale: measuring security trends in wi-fi networks and best practices," in Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2021, pp. 100–105.

[38] D. Schepers, A. Ranganathan, and M. Vanhoef, "On the robustness of wi-fi deauthentication countermeasures," in Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2022, pp. 245–256.

[39] G. Shi and K. Li, Signal interference in WiFi and ZigBee networks. Springer, 2017.

[40] A. L. Toledo and X. Wang, "Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks," IEEE Transactions on Information Forensics and Security, vol. 3, no. 3, pp. 347–358, 2008.

[41] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 1313–1328.

[42] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd," in 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020, pp. 517–533.

[43] Wi-Fi Alliance, "Wi-Fi Security," 2020, https://www.wi-fi.org/discover-wi-fi/security.

[44] Z. Zhang and M. Krunz, "Preamble injection and spoofing attacks in wi-fi networks," in 2021 IEEE Global Communications Conference (GLOBECOM). IEEE, 2021, pp. 1–6.

[45] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," Proceedings of the IEEE, vol. 104, no. 9, pp. 1727–1765, 2016.