# Securing EV Charging System against Physical-layer Signal Injection Attack

Soyeon Son
Korea University
mil05122@korea.ac.kr

Kyungho Joo
Korea University
khjoo0512@gmail.com

Wonsuk Choi
Korea University
beb0396@korea.ac.kr

Dong Hoon Lee
Korea University
donghlee@korea.ac.kr

***Abstract*—The proliferation of electric vehicles (EVs) and the simultaneous expansion of EV charging infrastructure have underscored the growing importance of securing EV charging systems. Power line communication is one of the most widely implemented communication technologies that is standardized by combined charging system (CCS) and the North American charging standard (NACS). Recently, it has been revealed that an unshielded charging cable can function as a susceptible antenna. As a result, attackers can eavesdrop on communication packets between charging stations and EVs or maliciously suspend charging sessions.**

**To secure EV charging systems against signal injection attack, we propose a signal cancellation system that restores benign charging sessions by annihilating the attack signal. An essential step in the proposed method is accurately estimating the carrier phase offset (CPO) and channel state values of the attack signal. Due to the inaccurate estimation of CPO and channel state values, continuous updates using linear interpolation are necessary. To evaluate the effectiveness of the proposed technique, we show that normal communication is achieved with the success of the signal level attenuation characterization (SLAC) protocol within 1.5 seconds. Experiments are conducted to determine the appropriate update parameters for attaining a 100% success rate in normal communication. We also analyze the error between the predicted CPO and channel state values and the actual CPO and channel state values of the attack signals. Furthermore, the effectiveness of the proposed method is evaluated based on the power of the injected attack signal. We have confirmed that when the power of the received attack signal is less than $-31.8\mathrm{dBm}$, applying the proposed technique with the suitable update parameters leads to 100% success in normal communication.**

## I. Introduction

In recent years, there has been a notable increase in the adoption of EVs, accompanied by the rapid development of electric vehicle charging infrastructure, commonly referred to as electric vehicle supply equipment (EVSE). Modern charging systems offer diverse functionalities, catering to users with services like payment processing, fee management, and real-time charging updates. For seamless provision of these services, high-level data communication is required. The adoption of charging standards varies by region and manufacturer. For example, prominent standards include Tesla's NACS, CCS developed by a consortium of European and American vehicle manufacturers, and CHAdeMO, which was developed by Nissan. NACS, recognized as a North American standard by the society of automotive engineers (SAE), utilizes the controller area network (CAN) communication protocol at the physical layer [3], [22]. Power line communication (PLC) is another pivotal technology utilized in EV charging systems. It enables the transmission of data through power lines, facilitating both power supply and data transfer simultaneously without necessitating additional communication infrastructure. The specifications for PLC technology are outlined by HomePlug GreenPHY (HPGP). Among the various communication protocol, PLC is employed in CCS and NACS is standardized in ISO-15118. Designed to be resilient against noise interference and to minimize residual electromagnetic fields, PLC is, however, not immune to certain vulnerabilities.

However, unshielded charging cables can leak electromagnetic signals, effectively functioning as antennas [15], [23]. This vulnerability makes PLC technology prone to signal emissions and susceptible to malicious signal injection. Exploiting this weakness, researchers carried out eavesdropping and signal injection attacks on the EV charging system without requiring direct physical access [5], [13]. The signals emitted from the unshielded charging cable enabled attackers to recover the transmission of network secret keys, such as the network membership key (NMK) and network encryption key (NEK) [5]. Furthermore, the attacker executed a signal injection attack on the unshielded cable continuously, exploiting PLC's vulnerability to intentional electromagnetic interference (IEMI) and the channel access method in the physical layer [13]. By doing so, the attacker disrupted charging sessions between EVs and EVSEs within a short timeout. This attack demonstrated its capability to disrupt charging sessions at a distance of 47 meters using less than 1W of power in real-world scenarios. Therefore, it presents a more practical and critical threat compared to previous wired attacks.

To cope with signal injection attack, hardware-based or software-based solution can be applicable [13]. As an alternative to replacing hardware, upgrading to a charging cable that is more resistant to electromagnetic interference (EMI) can also be a possible solution. However, it does not guarantee complete protection but increase the cost and weight of charging cable which hinders the usability of EV charging

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.23079
www.ndss-symposium.org

system. For the software-based solution, increasing the signal-to-noise ratio (SNR) thresholds for the preamble detection in the PLC modem can effectively complicate attacker efforts. Implementing re-authentication protocols can allow systems to automatically re-establish security credentials following a disruption. Additionally, monitoring for an increased frequency of invalid packets detects anomalous activities. Although these strategies may reduce the impact of one-time attacks and aid in their detection, they cannot guarantee the complete restore of normal communication.

In this paper, we present a novel signal cancellation system designed to counteract practical denial of service (DoS) attack on EV charging systems. Notably, DoS attacks emerge as a particularly pressing threat given that, to our current understanding, they are the only form of attack demonstrated to be executable wirelessly. Our method effectively generates a cancellation signal by analyzing the changing channel state values and carrier phase offset (CPO) of the attack signal. Consequently, this allows for the restoration of normal communication between EV and EVSE. The concept of annihilating RF signal was originally developed for malicious attacker. Especially, signal cancellation attacks on orthogonal frequency division multiplexing (OFDM) signals, known in WiFi and LTE systems, degrade the accuracy of channel estimation by invalidating the legitimate signal within the OFDM framework [8], [14], [16]. We propose a paradigm shift in signal cancellation attack techniques, viewing them from a defensive purpose. Through the evaluations, we evaluate the effectiveness of the proposed method employing commercial-off-the-shelf (COTS) device implemented with a Qualcomm QCA 7000 chipset, the most widely implemented modem chipset for PLC communication. The detailed contributions are as follows:

- To the best of our knowledge, we are the first to propose an attack cancellation technique against practical DoS attacks on PLC. Our method, which synchronizes to the attack signals, continuously updates the channel state and CPO estimate values. This effectively annihilates the attack signal, enabling normal communication between EV and EVSE.
- Compared to hardware-based solutions that alleviate electromagnetic interference, our method can be effectively implemented without hindering the usability of EV charging systems. Our software solution enhances EV charging systems by allowing for swift updates and improvements without hardware changes, providing a rapid response to evolving cyber threats. This approach, crucial in the dynamic cyber threat landscape, can be deployed remotely, greatly reducing the effort and time needed for system upgrades or adding new security measures, thereby boosting the efficiency and robustness of EV charging infrastructures.
- We evaluate our method on COTS devices. We employ evaluation boards with a Qualcomm QCA 7000 chipset, the most widely implemented chipset for PLC communication. Within the on-board environment, when the attack signals are annihilated, the SLAC protocol operates normally without interference.

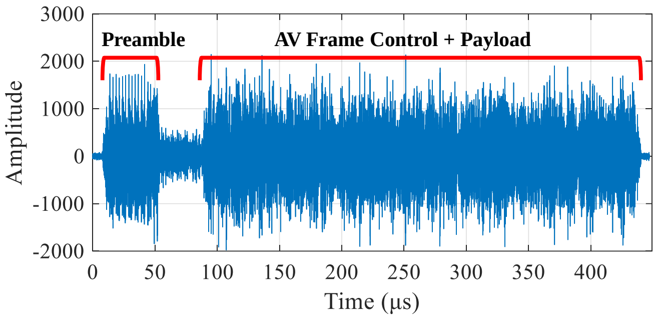


Fig. 1: An actual PPDU signal in the time domain

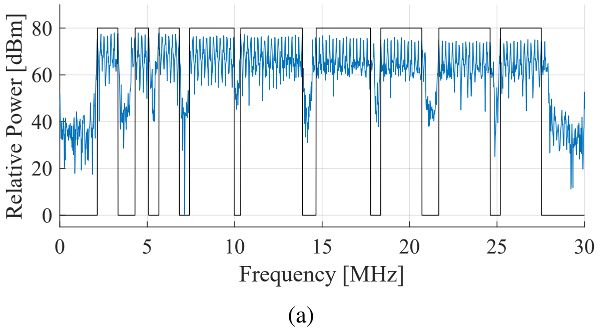
## II. Background

### A. HomePlug Green PHY (HPGP)

According to the international standard ISO/IEC 15118 [2], the communication stack between EV and EVSE defines the physical layer using HomePlug Green PHY (HPGP) capable of high-level communication. HomePlug GP is one of the PLC technologies used for smart grid and home networking applications. It is a cost and power-efficient version derived from the HomePlug AVLAN standard. Equipped with robust communication skills, it can adapt to channel variations caused by noise and interference in power line environments, ensuring the accuracy and stability of data, thereby increasing communication reliability.

HomePlug GP [24] employs quadrature phase shift keying (QPSK) as the data modulation scheme and utilizes turbo convolutional coding to add redundancy, enabling error recovery even in the presence of errors. The data stream is structured with OFDM modulation at the physical layer, dividing OFDM into multiple orthogonal subcarriers in the available bandwidth. Each subcarrier is modulated with its own set of data bits, allowing for simultaneous parallel transmission. The modulated data is then converted to time domain signals using an inverse fast Fourier transform (IFFT), and these time domain signals are communicated based on a 75 MHz sampling clock.

A physical protocol data unit (PPDU), as depicted in Figure 1, is a physical entity generated for transmission from the PHY interface to the power line, consisting of a preamble, AV frame control, and optionally, a payload. The preamble initiates a data frame, enabling the receiver to enter a prepared state to receive the data signal. Its structure includes SYNCP AV symbols and SYNCM AV symbols. SYNCP AV symbols use carriers spanning 384 samples (5.12us) in the 1.8-30MHz range. The SYNCM time domain waveform is defined as the SYNCP AV waveform multiplied by $-1$. Particularly, a hybrid preamble waveform consists of 7.5 SYNCP symbols and 1.5 SYNCM symbols.



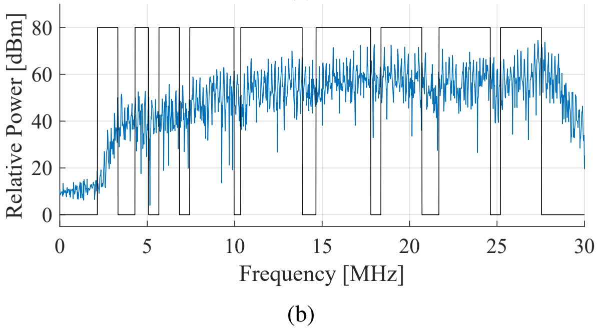


Fig. 2: (a) Spectral occupancy of reference preamble signal, (b) Spectral occupancy of captured preamble signal

### B. *Channel state value and Carrier phase offset*

When transmitting information within a communication system, a channel is formed, influenced by various factors. Channels exhibit diverse characteristics affected by elements such as path loss, multi-path fading, interference, frequency-selective fading, and time-selective fading. The reduction in signal strength over distance and the distortion of specific frequency components or time intervals present challenges in accurately recovering the transmitted signal. Therefore, to mitigate distorted signals, it's essential to measure channel information and adjust parameters like timing offset and frequency offset. This correction process is crucial for the effective operation of communication systems, enabling accurate signal restoration and thereby enhancing communication performance.

*1) Carrier Phase Offset (CPO):* Carrier Phase Offset (CPO) is a phenomenon in frequency-modulated communication systems, signifying a misalignment in carrier phase between the transmitter and receiver [6]. This arises due to channel effects and clock disparities between the transmitter and receiver. CPO can hinder precise signal demodulation at the receiver, necessitating offset correction. Typically, correcting CPO involves utilizing specific symbols or signal components contained in the transmitted signal.

*2) Channel Estimation:* Channel estimation, a fundamental technique in wireless communication systems [17], addresses fading effects, particularly in frequency-selective channels. In frequency-selective channels, various frequency components traverse distinct paths, causing fading effects. The Figure 2a represents the spectral mask of the unmasked carrier within the HPGP-compliant reference preamble signal, covering the frequency range of 1.8 to 30MHz. When receiving this reference preamble signal, the signal power varies across frequency components due to the channel's condition. As shown in Figure 2b, this variability introduces distortion and signal loss, underscoring the necessity for precise channel estimation. Typically, utilizing pilot signals or applying Fourier transform on received signals to analyze channel characteristics in the frequency domain enables accurate channel estimation.

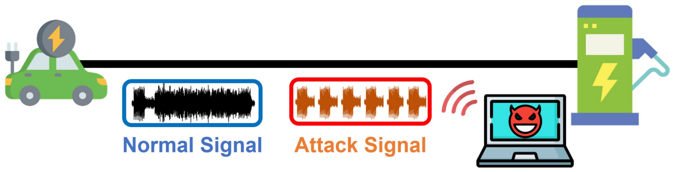


Fig. 3: Adversary model

## III. Threat Model

### A. *Adversary model*

An attacker's aim is to covertly disrupt one or more EV charging sessions simultaneously. To achieve this, the attacker is aware of a specific preamble signal defined in the ISO 15118 standard and uses it as an attack signal. Unshielded charging cables unintentionally act as antennas, enabling the attacker to remotely inject attack signals into the system without physical access. Per the HPGP specification, the receiver detects the preamble at a signal power of -35dBm or higher, even in the presence of Gaussian noise, provided the SNR exceeds 2dB. Consequently, the attacker must adjust the signal power to ensure the receiver detects the preamble above the -35dBm power threshold at the receiving terminal. The attacker exploits the HPGP-specified channel access method, CSMA/CA (Carrier-sense multiple access with collision avoidance), injecting preamble signals and effectively seizing control of the channel through this ongoing attack. According to [12], attackers can execute this attack with less than 1W of power from a distance of up to 47m.

## IV. Our method

### A. *Overview*

Detecting attack signals can be relatively straightforward, especially when the received packet format deviates from the expected norms or when utilizing preamble counters. However, to maintain normal communication, it's crucial not only to detect attacks but also to respond effectively. The proposed method involves generating a signal that counters the attack signal, nullifying the attack signal, and ensuring uninterrupted communication. This cancellation system can be deployed within an EV or EVSE equipped with a PLC modem chip.

The wirelessly injected preamble signal undergoes distortion due to the wireless channel's condition. To counter this distortion, estimating the received signal's CPO and the channel state becomes necessary. To ensure prompt restoration of normal communication, estimation of CPO and channel state values for all symbols of the initial attack signal is conducted. Based on previous estimations, subsequent attack signals are predicted and nullified. For accurate predictions, these estimates require regular updates. Using the first symbol of the preamble employed for synchronization, calculations for CPO and channel estimation values are executed, followed by updates through linear interpolation. Achieving precise signal nullification necessitates time synchronization with the wireless reception of attack signals. Therefore, 1.5 symbols are used for effective synchronization with wireless attack signals.

### B. Synchronization

To accurately annihilate the injected attack signal, precise time synchronization is crucial. This involves aligning the annihilation signal precisely with the attack signal, achieved by correlating a portion of the attack signal for synchronization. Through this process, it is possible to identify the starting point of the attack preamble and to differentiate subsequent attack preambles. Algorithm 1 describes synchronization process between attack and reference signals.

During the cross-correlation of an attack preamble with reference symbols, similar patterns between the two signals result in peaks appearing in the cross-correlation. A threshold is set based on the maximum peak value, and the peak count is calculated when this threshold is exceeded. Upon reaching a peak count of 7, the attack preamble is segmented, enabling the collection of synchronized attack data. This specific peak count is determined based on the preamble structure used in the charging communication system, which varies in the number of SYNCP and SYNCM symbols. In our experimental setup, the preamble consists of 7.5 SYNCP and 1.5 SYNCM symbols. When cross-correlating 1.5 SYNCP with the received preamble, 7 peaks are observed. Therefore, the peak count value needs to be adjusted according to the number of symbols within the received preamble to accurately collect attack data.

### C. Estimation of CPO and Channel state value

In this procedure, the proposed system conducts estimation of the CPO and channel state from the collected data. In wireless communication, the transmitted signal is distorted and attenuated due to channel characteristics such as path loss, fading, and noise. Especially, signals traverse with different path due to the physical obstacles creates multi-path effect. Hence, an estimation process for the channel state becomes essential to compensate for these diverse delays. Moreover, discrepancies in clock synchronization between the transmitter and receiver hardware can occur. Consequently, the receiver must estimate the CPO and correct carrier phase mismatches. This method, designed for the swift annihilation of the attack signal, initially estimates the CPO and channel state values for the entire set of symbols within the first detected attack preamble. Subsequently, it performs CPO and channel estimation only on a portion of the received preamble for subsequent updates.

```
Algorithm 1: Synchronization
  Data: S (a set of signals), $P_{ref}$
  Result: $P_{attack}$ (Signal synchronization)
  $lags,\ corr \leftarrow \mathrm{corr}(S, P_{ref})$;
  $\theta_{\text{peak}} \leftarrow \max(|\mathrm{corr}|) \cdot \lambda$;
  $index_{\text{peak}} \leftarrow \mathrm{corr} > \theta_{\text{peaks}}$;
  for $i$ = 1 to length($index_{peak}$) do
      if $index_{i+1} - index_i \leq 384$ then
          $count+ = 1$;
          $start = index_{i+1}$;
      else
          $count = 0$;
      end
      if $count = 7$ then
          $P_{attack} \leftarrow \mathrm{S}(start, start + L_{preamble})$;
      else
      end
  end
```

The CPO estimation process involves calculating the CPO values between each symbol within a set of seven SYNCP preamble symbols, subsequently averaging these values for precision [5], [6]. The specific formula used for CPO estimation is as follows:

$$\widehat{CPO} = \frac{1}{7}\left[\sum_{sym=1}^{7}\left(\frac{1}{384}p_{sym}\cdot\overline{p_{sym+1}}\right)\right] \tag{1}$$

where $p$ is received preamble samples and $sym$ is symbol number. The received preambles are complex samples within the time domain of OFDM. The preamble comprises 7 SYNCP symbols, each containing 384 samples. To assess the phase offset due to clock differences between the transmitter and receiver, the first symbol is multiplied by the conjugate of the subsequent 384 samples from the SYNCP symbol. This multiplication result yields data that aids in analyzing the correlation between symbols and obtains an estimation of the phase offset. The phase offset per sample is then calculated by dividing the total phase offset by 384, the number of samples in a symbol. This method is applied across all symbols to compute the CPO values and averaged them. As the estimated CPO may not precisely reflect the actual CPO, it is necessary to continuously update the CPO for each received preamble symbol. Further details on the CPO updates are provided in Section IV-E.

Based on the estimated CPO values, CPO correction is performed for all samples of the preamble. The correction equation for CPO, utilizing the frequency shift property of the Fourier transform, is as follows:

$$p_{corr}[i] = p[i]\cdot e^{-j\cdot\widehat{CPO}\cdot i} \tag{2}$$

In the next step, channel information is estimated in the frequency domain. As signals are often attenuated or distorted within specific frequency bands in the OFDM system. Analyzing the frequency response is crucial for understanding

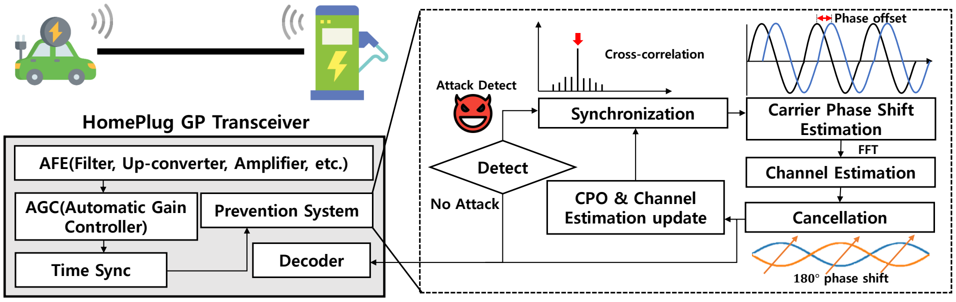


Fig. 4: System overview

the channel characteristics and improving communication reliability by compensating for distortions or errors that may occur during transmission. In a typical communication channel model, the received data samples, denoted as the received data $y_i$ are the result of original transmitted data $p_i$ propagated through the channel $h_i$ and added to an additive noise $n_i$. Leveraging the convolution theorem, the complex convolution operation that represents the channel model in the time domain simplifies into a multiplication in the frequency domain. This transformation allows for an intuitive interpretation of the channel's response and characteristics. Channel model in the frequency domain is represented in (3) where $Y_i$, $H_i$, $P_i$, $N_i$, are the frequency domain representations of $y_i$, $h_i$, $p_i$, $n_i$ respectively.

$$\begin{aligned} y_i &= h_i * p_i + n_i \\ Y_i &= H_i \cdot P_i + N_i. \end{aligned} \tag{3}$$

In the proposed method, as EV charging systems operate in a wired environment, a high SNR is typical, enabling the assumption of additive noise as ideal for channel estimation.To measure the channel state, time-domain attack data samples corrected by the CPO are transformed into frequency-domain data via fast Fourier transform (FFT) [7]. The channel estimation is performed for 7.5 out of the 9 preamble symbols, excluding a portion of the attack signal dedicated to synchronization. Specifically, this estimation targets the unmasked carriers as defined in HPGP. The calculation of the channel estimation values by dividing the frequency domain received attack preamble samples by the reference preamble samples is presented in (4). SYNCM symbols are treated as signals with their phase shifted by 180 degrees from the SYNCP symbols, and the channel state for SYNCM symbols is estimated by dividing the reference preamble signals multiplied by negative.

$$Channel\, estimation = \widehat{H_i} = \frac{Y_i}{P_i} \tag{4}$$

Similar to CPO, the channel estimation values also require continual updating as they do not precisely match the actual channel state values. The details regarding channel updates are elaborated in Section IV-E.

```
Algorithm 2: Update of CPO
Data: s (1.5 SYNCP symbols of attack preamble)
Result: $\widehat{CPO}_{update}$
for $i$ = 1 to $length(SYNCP_{half})$ do
    $total+ = \overline{s[i]} \cdot s[i+384]$;
end
$\widehat{CPO}_{curr} = \frac{1}{384} \cdot \mathrm{angle}(total)$;
$\widehat{CPO}_{update} = \alpha \cdot \widehat{CPO}_{prev} + (1-\alpha) \cdot \widehat{CPO}_{curr}$;
```

```
Algorithm 3: Update of Channel
Data: $p_{attack}$, $p_{ref}$ (1 SYNCP symbol of preamble)
Result: $\widehat{H}_{update}$
$P_{attack} \leftarrow FFT(p_{attack})$;
$val \leftarrow FFT(p_{ref})$;
if PREAMBLE_TONE_MASK == 1 then
    $H_{curr}[i] = P_{attack}[i]/val[i]$;
else
    $\widehat{H}_{curr}[i] = 1$;
end
$\widehat{H}_{update} = \beta \cdot \widehat{H}_{prev} + (1-\beta) \cdot \widehat{H}_{curr}$;
```

### D. Phase shift

To cancel out two identical signals, one signal's phase is rotated by 180 degrees, and when the two signals are then added together, they can theoretically cancel each other out. However, merely relying on a 180 degree phase shift does not entirely eliminate a signal. For complete annihilation, the two signals must be precisely inverted in frequency, amplitude, and timing. Using the channel characteristic values estimated in Section IV-C, a signal similar to the attacking signal is generated, and the phase of this similar signal is rotated by 180 degrees. As OFDM signals are represented as complex signals, the phase shift of the complex signal can be accomplished through Euler's formula. The equation for adjusting the phase by 180 degrees on the complex plane is as follows:

$$X_i = X_i \cdot e^{-j \cdot \pi} \tag{5}$$

The signal rotated by 180 degrees is transmitted by aligning the timing, as explained in Section IV-B. This alignment enables the two signals to effectively cancel each other out.

### E. Update of CPO and Channel

In Section IV-C, the estimated of CPO and channel state values deviate from their actual values, necessitating continual adjustments based on the received attack signals. The CPO and channel state values are updated using a portion of received attack signal designated for synchronization. Firstly, to update the CPO, the first half of the SYNCP symbol, containing 192 samples from the received attack signal, is utilized to estimate the CPO between it and the subsequent 192 samples. Subsequently, using linear interpolation, the CPO of the upcoming attack is predicted [19]. The linear interpolation is used to blend the old and new estimates to create a smooth transition and maintain a balance between stability and adaptability in changing conditions. In the proposed method, an update parameter ($\alpha$) is used to blend the current CPO estimate with the previous one for updating. Following the correction of the attack signal based on the current CPO estimate, the time-domain signal is converted into the frequency domain for channel estimation. For one SYNCP symbol, channel estimation is performed only for the frequencies not subjected to tone masking, as defined in HPGP. Then, similar to CPO, the channel is updated using linear interpolation by an update parameter ($\beta$). The effectiveness of annihilating the attack signal relies on how accurately the updated CPO and channel state values predict the forthcoming attack signal's CPO and channel values. The appropriate update parameters for updates are determined experimentally in V-C.

### F. Cancellation

The method for annihilating the attack signal using previously estimated values and techniques is introduced in a step-by-step. As detailed in Section IV-C, the cancellation method computes estimation values for the entire first attack preamble after detecting the attack. Based on the estimated values, the CPO and channel state values of the second attacking preamble are inferred to create a similar attacking preamble signal. Subsequent attack preambles are predicted based on estimated values updated in Section IV-E. The previously estimated channel state values are multiplied with the reference preamble signal to generate a signal with similar amplitude and phase values to the attack signal. Since this is frequency domain data, it is converted into time-domain data through IFFT. Rectifying the frequency characteristics among subcarriers by adjusting the similar signal to the attack signal using previously estimated CPO values and the phase of this corrected signal is rotated by 180 degrees. The signal rotated by 180 degrees is transmitted by aligning the timing through time synchronization to portion of attack signals, as explained in Section IV-B. Finally, computing estimation for CPO and channel state values for the portion of the attack signal used for synchronization. And using linear interpolation technique to predict and update the CPO and channel state values for subsequent attack preambles.

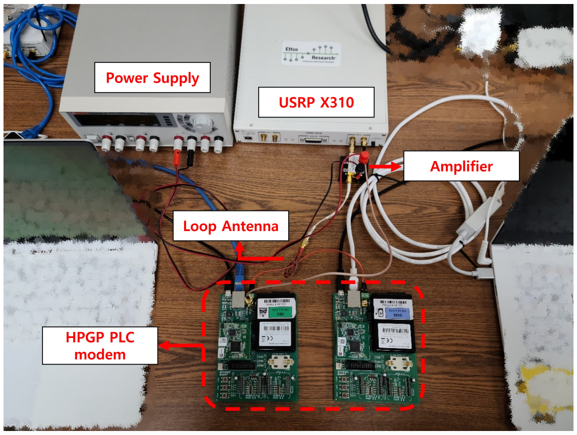


Fig. 5: Experiment setup

## V. EVALUATION

In this section, we present the results of our experiments on the effectiveness of annihilation against signal injection attacks in a controlled laboratory environment. We also analyze the discrepancy between the predicted CPO and channel state values and the actual CPO and channel state values of the attack signal. Furthermore, an experiment was conducted to evaluate the performance of the proposed method in relation to varying power levels of the attack signal.

### A. Experimental Setup

We evaluate our method, using a testbed consisting of two HomPlug Green PHY evaluation boards equipped with Qualcomm QCA 7000 chipsets from Devolvo. The boards were interconnected via a jumper cable for PLC communication. One board was configured to represent an EV, while the other acted as an EVSE. We verify the normal communication between the two boards through the operation of the SLAC protocol. This protocol ensures the correctness of the connection between the EV and the EVSE, addressing potential confusion often encountered in public networks. The process involves vehicles transmitting multiple sound messages received and measured for attenuation by the charging stations. The SLAC protocol implementation utilized tools from the Qualcomm Atheros Powerline Toolkit, available as open-source [1]. According to ISO 15118, to prevent charging session disruptions, an average timeout of 1.5 seconds is maintained. We consider the communication between EV and EVSE successful if the SLAC protocol operates within 1.5 seconds and unsuccessful if it exceeds this time. Therefore, we assess the recovery of normal communication by evaluating the operation success rate of the SLAC protocol, performing 50 iterations of the protocol execution.

### B. Preliminary Analysis

For the signal injection attack, an attack signal could be generated using a reference preamble signal formula as defined in HPGP, or by intercepting packets during regular communication and extracting the preamble. These attack signals were

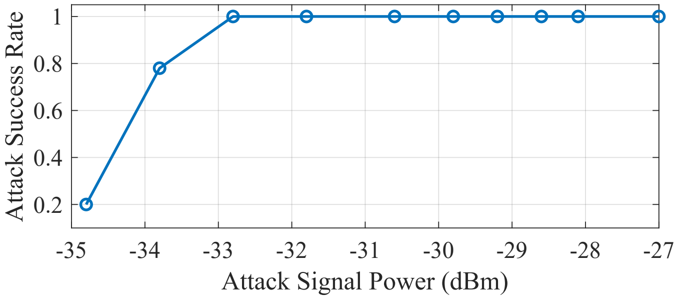


Fig. 6: Attack success rate based on attack power

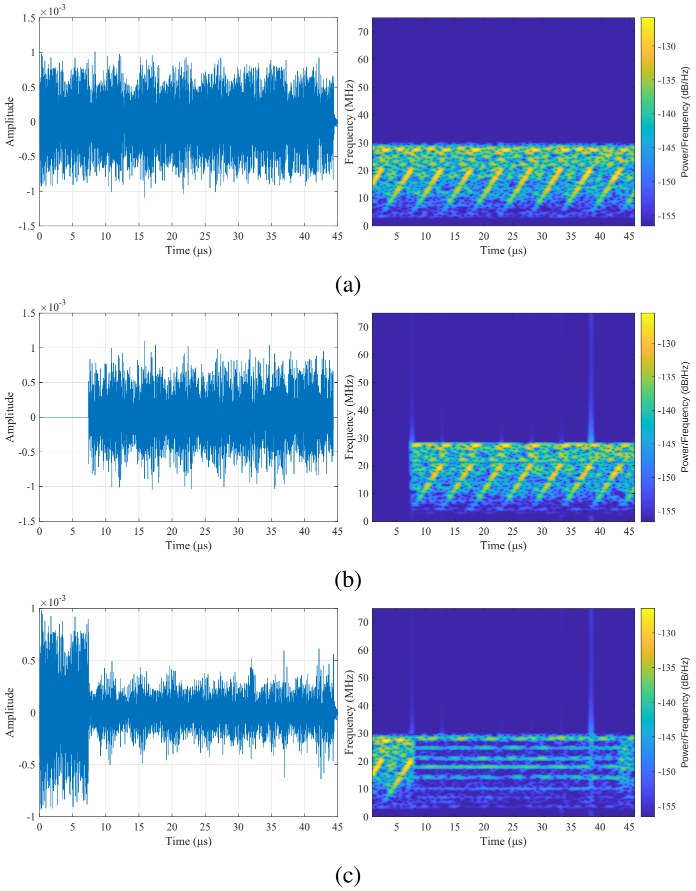
TABLE I: Operation efficiency of cancellation per symbol

| # of removed symbol | Success rate (%) |
|---|---|
| 1 | 0% |
| 2 | 0% |
| 3 | 86% |
| 4 | 92% |
| 5 | 98% |
| 6 | 100% |

then wirelessly injected into the evaluation board using SDR with GNU Radio, via a loop antenna connected to the USRP X310 tx component and a ZX60-100VH+ amplifier. In our experiment, the power of the attack signal is -1dBm with a duration of 46.08 microseconds. Upon wireless injection, the attack signal experiences amplitude attenuation and carrier phase shifts due to the characteristics of the wireless channel. In the testbed setup, when the attack signal was injected using a 1W amplifier, the received power of the attack signal, as collected by the USRP X310 rx component attached to the EVSE board, was measured to be -27dBm. In the context of 4G LTE reception in mobile networks, a signal strength above -50dBm indicates excellent signal sensitivity, enabling seamless wireless communication [4], [11]. Therefore, a power of -27dBm can be considered indicative of high signal sensitivity in wireless communications.

According to the HPGP standard, a receiver needs a minimum signal strength of -35dBm to detect the presence of preamble symbols. Figure 6 illustrates the success rate of signal injection attacks based on the received power of the attack signal. We measured the magnitude of the attack signal received by the USRP after wirelessly injecting the generated attack signal at decreasing power levels. As shown in Figure 6, while the received attack signal's power was -33.8dBm, the attack success rate dropped to 78%. This might be due to the reliance on USRP to measure the attack signal strength, which could render the value of -33.8dBm somewhat inaccurate. We evaluated the performance of our technique using an attack signal power of -31.8dBm, which ensures a 100% attack success rate.

We conducted to determine the minimum number of attack preamble symbols that need to be annihilated for normal communication. We injected signals with sequentially removed preamble symbols into the evaluation board wirelessly and assessed the operation efficiency of the SLAC protocol. The results, as shown in Table I, indicate that at least six symbols of the attack signal must be nullified to restore normal communication.



(a)

(b)

(c)

Fig. 7: Cancellation process: (a) Attack signal, (b) Annihilating signal, (c) Result

### C. Determine update parameter

Our method involves collecting the attack signal using the USRP X310 and GNU Radio flow graph. The application of our method to the collected signals is executed within MATLAB software, and the results are directly injected into the board to assess the effectiveness of our method. Initially, a segmentation process is conducted on the collected attack signals through synchronization. To demonstrate the time synchronization can be achieved with 1.5 SYNCP symbols of the attack signal, we perform cross-correlation between the 2 seconds of collected attack signals and 1.5 reference SYNCP symbols. The threshold is set to 70% of the maximum peak to segment the attack preambles, and the result is shown in Figure 7a. Following the process outlined in Section IV-F, an opposing signal to the attack signal is generated using the predicted CPO and channel state values. The result of adding the two signals, effectively annihilating the attack signal, is depicted in Figure 7c. The first 1.5 symbols were

TABLE II: Operation success rate for different update parameters

| $\alpha$ | $\beta$ | | | | | | | | | Average |
|---|---|---|---|---|---|---|---|---|---|---|
| | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | |
| 0.1 | 96% | **100%** | **100%** | 96% | **100%** | 78% | 98% | 98% | 78% | 93.78 |
| 0.2 | 54% | 54% | **100%** | 96% | 98% | 96% | 78% | **100%** | **100%** | 86.22 |
| 0.3 | 98% | 96% | **100%** | 78% | **100%** | 98% | 98% | 98% | **100%** | 96.22 |
| 0.4 | **100%** | **100%** | 76% | **100%** | **100%** | **100%** | **100%** | 98% | 98% | 96.89 |
| 0.5 | **100%** | **100%** | **100%** | 98% | **100%** | **100%** | 98% | 96% | **100%** | 99.11 |
| 0.6 | **100%** | **100%** | 98% | 96% | **100%** | **100%** | 98% | 96% | **100%** | 98.67 |
| 0.7 | 78% | **100%** | 94% | 81% | **100%** | 94% | 78% | 98% | **100%** | 91.44 |
| 0.8 | **100%** | **100%** | **100%** | 78% | **100%** | **100%** | **100%** | 78% | 90% | 94.00 |
| 0.9 | **100%** | **100%** | **100%** | 96% | **100%** | **100%** | **100%** | 98% | **100%** | 99.33 |
| Average | 91.78 | 94.44 | 96.44 | 91.00 | 99.78 | 96.22 | 94.22 | 95.56 | 96.22 | |

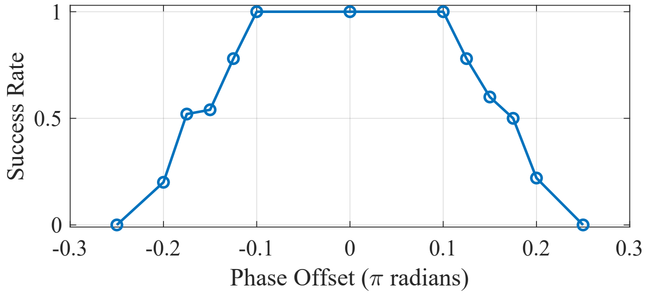


Fig. 8: Operation success rate for phase offset difference

not annihilated due to synchronization requirements, while the rest of the symbols were entirely annihilated.

According to Section IV-E, the technique of linear interpolation causes predicted CPO and channel state values to vary depending on specific update parameters. This parameter determines the balance between past and present estimations. When the parameter is close to 1, the interpolation relies more heavily on the previous values, providing stability but potentially less responsiveness to new changes. Conversely, when parameter is near 0, the interpolation is more influenced by the current values, making it more responsive to recent changes but possibly less stable. We conducted experiments to identify the appropriate parameters for accurately predicting the CPO and channel state values of the attack signal. Table II presents the results of evaluating the effectiveness of cancellation for each parameter by directly injecting the outcomes into the evaluation board and assessing whether the SLAC protocol operation was successfully performed within 1.5 seconds. When averaging the success rates of the SLAC protocol, the highest rate of normal communication was achieved when $\alpha$ was 0.9 and $\beta$ was 0.5. Even with successful cancellation, the residual 1.5 symbols dedicated to synchronization remained, leading to an overlap with the normal SLAC protocol signals. Despite this, the reason for achieving 100% successful communication in these cases is likely due to effective error correction defined in HPGP, which we hypothesize compensated for any residual interference from the attack signal.

### *D. Analyze error of CPO and channel estimation*

We evaluate how varying degrees of phase offset affect the ability to annihilate the attack signal. We deliberately altered the phase of the attack signal across a spectrum from $-\pi$ to $\pi$. For each phase offset, we generated a counteracting signal by inverting and then added this counteracting signal to the original attack signal to attempt signal cancellation. As shown in Figure 8, we find that when the phase offset difference falls within a range of -0.1$\pi$ to 0.1$\pi$, SLAC protocol proceeds with 100% success rate. This narrow phase offset range, our method effectively annihilate the attack signal, thereby allowing the SLAC protocol to operate undisturbed. However, as the phase offset deviates beyond this range, the success rate of SLAC protocol begins to decrease symmetrically about 0.

And we analyze the discrepancy between the phase offsets predicted by our method and the actual phase offsets in the attack signal. In the proposed method, correcting the attack signal with the estimated CPO before estimating the channel state values. Thereby, the accurate estimation of the CPO influences estimation of the channel state values. Consequently, the CPO update parameter ($\alpha$), which affects CPO estimation, also influences the update process of channel estimation. In contrast, the channel update parameter ($\beta$), affecting the estimation of the channel, does not impact CPO measurement.

Hence, the predicted CPO is solely influenced by the CPO update parameter. Varying the $\alpha$ from 0.1 to 0.9 to observe the changes in the predicted CPO values and calculated the differences (minimum, average, maximum) between these predicted values and the actual CPO values of the attack signals. As shown in the Table III, assigning 90% weight to the previous channel state values and 10% weight to the currently estimated channel state values resulted in the smallest error. This suggests that placing more weight on the current estimation significantly enhances the accuracy of CPO prediction.

We proceed to calculate the discrepancies in channel state values. Given that channel state values are vectors, we employ error vector magnitude (EVM) as a metric for gauging the deviation of the actual received signal from its actual version. We anchored $\alpha$ at 0.9 based on its proven efficacy in minimizing CPO discrepancies and explored the influence of $\beta$. Our findings indicate that while the minimum EVM values

TABLE III: CPO error with CPO update parameter

| $\alpha$ | CPO Error (rad) | | | |
|---|---|---|---|---|
| | Min | Average | Max | Standard Deviation |
| 0.1 | 1.20e-04 | 1.79e-04 | 2.21e-04 | 1.51e-05 |
| 0.2 | 1.06e-04 | 1.59e-04 | 1.93e-04 | 1.25e-05 |
| 0.3 | 9.35e-05 | 1.39e-04 | 1.66e-04 | 1.01e-05 |
| 0.4 | 8.01e-05 | 1.19e-04 | 1.40e-04 | 8.11e-06 |
| 0.5 | 6.67e-05 | 9.97e-05 | 1.15e-04 | 6.30e-06 |
| 0.6 | 5.34e-05 | 7.97e-05 | 9.10e-05 | 4.73e-06 |
| 0.7 | 4.01e-05 | 5.97e-05 | 6.72e-05 | 3.37e-06 |
| 0.8 | 2.67e-05 | 3.97e-05 | 4.40e-05 | 2.20e-06 |
| 0.9 | 1.33e-05 | 1.98e-05 | 2.15e-05 | 1.19e-06 |

TABLE IV: Channel estimation error with CPO update parameter

| $\alpha$ | Channel Estimation Error (%) | | | |
|---|---|---|---|---|
| | Min | Average | Max | Standard Deviation |
| 0.1 | 0.0962 | 0.1591 | 0.5890 | 0.0391 |
| 0.2 | 0.0973 | 0.1584 | 0.5814 | 0.0367 |
| 0.3 | 0.1008 | 0.1578 | 0.5739 | 0.0348 |
| 0.4 | 0.1078 | 0.1573 | 0.5464 | 0.0334 |
| 0.5 | 0.1046 | 0.1569 | 0.5590 | 0.0325 |
| 0.6 | 0.1000 | 0.1565 | 0.5518 | 0.0318 |
| 0.7 | 0.0883 | 0.1561 | 0.5455 | 0.0314 |
| 0.8 | 0.0729 | 0.1557 | 0.5408 | 0.0312 |
| 0.9 | 0.0659 | 0.1548 | 0.5395 | 0.0311 |

TABLE V: Channel estimation error with channel update parameter

| $\beta$ | Channel Estimation Error (%) | | | |
|---|---|---|---|---|
| | Min | Average | Max | Standard Deviation |
| 0.1 | 0.0659 | 0.1572 | 0.5404 | 0.0313 |
| 0.2 | 0.0659 | 0.1563 | 0.5403 | 0.0311 |
| 0.3 | 0.0659 | 0.1556 | 0.5402 | 0.0308 |
| 0.4 | 0.0659 | 0.1551 | 0.5401 | 0.0308 |
| 0.5 | 0.0659 | 0.1548 | 0.5395 | 0.0311 |
| 0.6 | 0.0659 | 0.1548 | 0.5376 | 0.0319 |
| 0.7 | 0.0659 | 0.1550 | 0.5313 | 0.0335 |
| 0.8 | 0.0659 | 0.1555 | 0.5129 | 0.0361 |
| 0.9 | 0.0659 | 0.1564 | 0.4731 | 0.0403 |

remained consistent across different $\beta$ settings, the average EVM was optimized at $\beta$ values of 0.5 and 0.6. Further tests, with $\beta$ fixed at 0.5, revealed that a $\alpha$ of 0.9 consistently yielded the lowest error rates, underscoring its significant role in enhancing estimation accuracy. These observations suggest that $\alpha$ plays a more dominant role in minimizing estimation errors compared to $\beta$, possibly attributed to the consistent power of the received attack signals and the resultant uniformity in channel conditions.

### *E. Effect of attack signal power*

The effectiveness of the proposed method varied with the power of the incoming attack signal. When the attacker injected the signal from an extremely close distance of 1cm to the charging cable, the power of the attack signal measured at the EVSE's board was -27dBm We evaluated our method across a range of attack signal powers, from -33dBm to -27dBm with the appropriate update parameters of $\alpha$: 0.9 and $\beta$: 0.5. The results showed that as the power of the attack signal decreased, our proposed method's ability to annihilate the attack effectively increased. When the power of the received attack signal was at -28.6dBm, we observed a notable decrease in the success rate of the SLAC protocol's operation to 0.6 after employing the cancellation technique as shown in Figure 9. This outcome suggests that while our method is generally effective, the accuracy of the predicted CPO and channel state values, derived from a relatively simplistic linear interpolation approach, might not be sufficient against stronger attack signals. Therefore, enhancing the accuracy of these predictions is crucial, potentially requiring a more sophisticated approach to updating the estimation of CPO and channel state values.

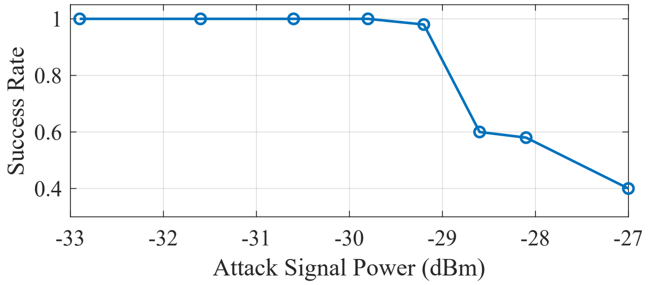


Fig. 9: Success rate of SLAC protocol as a function of attack power

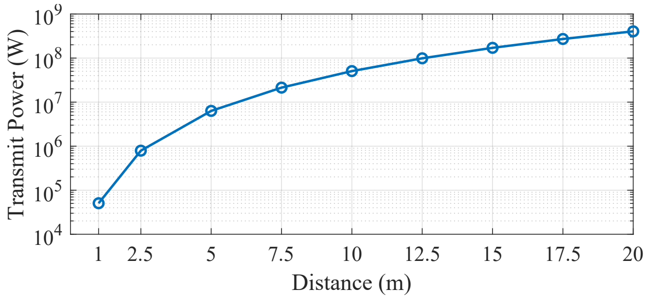


Fig. 10: Required transmit power to maintain -27dBm receive power

To bypass our method, an attacker would need to ensure a minimum received power of -27dBm. However, the transmit power required to maintain this received power level increases significantly with distance. Considering the previously measured reference values, where a transmit power of 1W results in a received power of -27dBm at a distance of 1cm, we estimated the minimum transmit power required to sustain a received power of -27dBm across various distances by applying the Log-distance path loss model with ideal parameters [20]. Using this model, we have predicted the minimum transmit power needed from a 1m to a 20m distance, and the results, presented on a logarithmic scale, are illustrated in Figure 10. As shown, at a 1m distance, the transmit power needs to be elevated to 50,000W to preserve the same -27dBm received power. This significant increase in required transmit power with even minor distance extensions presents a considerable challenge for attackers aiming to conduct DoS attacks from a distance stealthily. However, this analysis might not fully account for real world, as it does not consider the specific gains of the EV charging cable antenna and the antennas utilized by attackers.

## VI. Related Works

### A. Attacks on EV charging system

*1) Wired Attacks:* Malicious devices planted at charging stations perform a relay attack, controlling the communication between vehicles and stations [9]. These devices intercepted and forwarded unaltered messages, enabling control over power supply. When both the target and malicious vehicles connected, the attacker manipulated their charging requests. However, this attack has limitations as it requires manipulation of the charging system, making it challenging to execute in a real-world environment. By exploiting the SLAC protocol flaw through another device connected to the same power line network, it was possible to steal sensitive network keys to manipulate messages between vehicles and stations [10]. Furthermore, the V2G Injector was devised to tamper with messages exchanged in the ISO 15118 standard, enabling redirection to a fake charging server upon vehicle request.

*2) Wireless Attacks:* PLC-based charging systems emit electromagnetic waves through the charging cable, featuring antenna-like capabilities. Eavesdropping attacks were conducted using SDR to capture emitted electromagnetic signals between the EV and EVSE during the initialization phase of charging sessions [5]. Using their developed HPGP wireless eavesdropping tool, the attackers were able to extract network secret key at an average rate of 87%.

The signal injection attacks were executed by exploiting the vulnerability of PLC sensitive to IEMI on unshielded charging cables and the channel access method, CSMA/CA, at the physical layer [12] [13]. The attacker continuously injected a preamble signal defined in the HPGP spec, a component crucial for synchronization between transceivers, into the channel. As a result, the channel remained occupied, preventing the transmission of normal messages. Following the ISO 15118 standard, exceeding a short message timeout of 1.5 seconds terminates the communication session between the EV and EVSE. This study demonstrates that attacks are feasible not only for a single vehicle but also for numerous vehicles in real-world scenarios.

### B. Cancellation attacks

Research on attacks in wireless communication systems such as WiFi and LTE has introduced a method that precisely removes legitimate signals. This involves compromising or completely blocking the system's signals, posing a threat to the network's availability and reliability. In pilot denial attacks, a strategy is proposed to annihilate the reference signal [8]. In OFDM systems, pilot tones assist in estimating channel characteristics in each frequency band, aiding in the compensation for distortions in the channel that affect data signals [16]. The pilot denial attacks force the energy of the received pilot samples to zero, thereby reducing the accuracy of channel estimation functionality in cellular networks. Effectiveness of this attack was demonstrated through simulations. Subsequently, an analysis was conducted on the impact of timing and frequency mismatch on this attack [21]. Achieving timing and frequency alignment between the attacker and the target device is crucial, making practical implementation challenging. A preamble cancellation attacks transmit the inverse version of the preamble sequence in the time domain [14]. The attacker must know perfect network timing, to disrupt the timing synchronization process. However, in wireless systems, the channels are random, and the attack requires precise timing accuracy, making practical attack implementation in real Wi-Fi networks challenging.

The previous research studies deemed signal cancellation attacks in the analog domain unrealistic due to synchronization challenges. However, [18] performs digital signal cancellation attacks using SDR. The attacker nullify the legitimate signal in GPS wireless systems. According to the evaluation, signal cancellation attacks, causing attenuation of up to 40dB at the receiver, are feasible in the air, but they possess limitations. The signals subject to cancellation must be predictable, as partial cancellation is not possible for random signals. Additionally, precise control over the attacker's transmitted phase is essential.

## VII. Discussion

**Concern for Adaptive attacker.** Our method for attack signal annihilation is tailored to synchronize with the attack signal, estimating both the CPO and channel state value. However, it's essential to consider the capabilities of attackers; our model assumes a fixed attack power, but in scenarios where attackers employ adaptive strategies by varying the power of the attack signal, our method might struggle to accurately predict and thereby neutralize the attack signal. Acknowledging these limitations, we recognize the need for a more robust annihilation mechanism as part of our future work, which will involve a deeper examination of the attack model to address adaptive attackers.

**Concern for Masquerade attacker.** Beyond our attack model, attackers could also record and replay normal signals to masquerade their attacks. While such attacks are theoretically possible, none have been proven to date. It's crucial to focus on the fundamental differences in channel characteristics between attack signals injected wirelessly and legitimate signals transmitted over wired channels to detect these attempts. Analyzing channel state values can help identify these discrepancies, potentially allowing for the neutralization of attack attempts by accurately predicting and erasing the preamble of the attack signal's channel state values. The practicality of defending against such masquerade attacks requires further study.

**Estimation Accuracy.** From the evaluation result, it can be seen that our method has a limitation to a high-power attack signal. Since our method is not properly able to estimate CPO and channel state if the attack signal has a high power (more than -27dBm). For this reason, we are planning to improve the estimation accuracy of our method for a high-power attack signal. On the other hand, however, it seems that it is difficult to conduct a stealthy attack with a high-power signal. Accordingly, the high-power signal would be easily detected even though our method is not able to estimate its CPO and channel state. Additionally, our experiments were conducted in controlled environments, which might not fully replicate real-world environments. As part of our ongoing research, we plan to develop strategies to apply our method in actual scenarios, acknowledging that results may vary outside of a controlled setting.

## VIII. Conclusion

In this work, we demonstrate a cancellation system capable of maintaining normal communication in the presence of wireless signal injection attacks, particularly targeting PLC-based infrastructures. By accurately estimating the attack signal's channel state and CPO, and through precise synchronization, our system effectively annihilates the intrusive signals, thereby safeguarding communication integrity. The system's adaptability across various power levels of attack signals showcases its practical applicability and resilience. While it shows some limitations against high-power, close-range attacks, it excels in mitigating more distant threats. Our findings and the proposed system not only enhance the security of EV charging stations but also have broader implications for the security of various applications reliant on PLC technology. This work paves the way for future research and development aimed at creating even more resilient and adaptive security mechanisms for critical communication infrastructures.

## Acknowledgment

This work was supported by the Institute for Information and Communications Technology Promotion (Development of Security Primitives for Unmanned Vehicles) under Grant 2020-0-00374.

## References

[1] "Qualcomm atheros powerline toolkit," https://github.com/qca/open-plc-utils/tree/master, 2013.

[2] *ISO 15118-3:2015 Road vehicles Vehicle to grid communication interface*, ISO, 2015.

[3] *SAE J3400: NACS Electric Vehicle Coupler*, SAE, 2023.

[4] F. Afroz, R. Subramanian, R. Heidary, K. Sandrasegaran, and S. Ahmed, "Sinr, rsrp, rssi and rsrq measurements in long term evolution networks," *International Journal of Wireless & Mobile Networks*, 2015.

[5] R. Baker and I. Martinovic, "Losing the car keys: Wireless {PHY-Layer} insecurity in {EV} charging," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 407–424.

[6] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "An ieee 802.11 a/g/p ofdm receiver for gnu radio," in *Proceedings of the second workshop on Software radio implementation forum*, 2013, pp. 9–16.

[7] E. O. Brigham, *The fast Fourier transform and its applications*. Prentice-Hall, Inc., 1988.

[8] T. C. Clancy, "Efficient ofdm denial: Pilot jamming and pilot nulling," in *2011 IEEE International Conference on Communications (ICC)*. IEEE, 2011, pp. 1–5.

[9] M. Conti, D. Donadel, R. Poovendran, and F. Turrin, "Evexchange: A relay attack on electric vehicle charging system," in *European Symposium on Research in Computer Security*. Springer, 2022, pp. 488–508.

[10] S. Dudek, J.-C. Delaunay, and V. Fargues, "V2g injector: Whispering to cars and charging units through the power-line," in *Proceedings of the SSTIC (Symposium sur la sécurité des technologies de l'information et des communications), Rennes, France*, 2019, pp. 5–7.

[11] H. K. Hoomod, I. Al-Mejibli, and A. I. Jabboory, "Analyzing study of path loss propagation models in wireless communications at 0.8 ghz," in *Journal of Physics: Conference Series*, vol. 1003, no. 1. IOP Publishing, 2018, p. 012028.

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

[13] ——, "End-to-end wireless disruption of ccs ev charging," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 3515–3517.

[14] M. J. La Pan, T. C. Clancy, and R. W. McGwier, "Jamming attacks against ofdm timing synchronization and signal acquisition," in *MILCOM 2012-2012 IEEE Military Communications Conference*. IEEE, 2012, pp. 1–7.

[15] L. Lampe, A. M. Tonello, and T. G. Swart, *Power Line Communications: Principles, Standards and Applications from multimedia to smart grid*. John Wiley & Sons, 2016.

[16] B. Li, S. Zhou, M. Stojanovic, and L. Freitag, *Pilot-tone based ZP-OFDM demodulation for an underwater acoustic channel*. IEEE, 2006.

[17] Y. Liu, Z. Tan, H. Hu, L. J. Cimini, and G. Y. Li, "Channel estimation for ofdm," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1891–1908, 2014.

[18] D. Moser, V. Lenders, and S. Capkun, "Digital radio signal cancellation attacks: An experimental evaluation," in *Proceedings of the 12th conference on security and privacy in wireless and mobile networks*, 2019, pp. 23–33.

[19] M. J. Powell, *A direct search optimization method that models the objective and constraint functions by linear interpolation*. Springer, 1994.

[20] T. S. Rappaport, *Wireless Communications - Principles and Practice*. Prentice-Hall, Inc., 1991.

[21] C. Shahriar, S. Sodagari, and T. C. Clancy, "Performance of pilot jamming on mimo channels with imperfect synchronization," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 898–902.

[22] B. VISNIC, "Sae to standardize tesla nacs charging connector," *SAE-intertnational*, 2023.

[23] B. Zarikoff and D. Malone, "Experiments with radiated interference from in-home power line communication networks," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 3414–3418.

[24] B. J. Zyren, "The homeplug green phy specification & the in-home smart grid," in *2011 IEEE International Conference on Consumer Electronics (ICCE)*, 2011, pp. 241–242.