EMIT: Reflection-Based Charging Jamming Attack

Tang Liu, *Member, IEEE*, Jing Gao, Yuan Yin, Die Wu, *Member, IEEE*, Jian Peng, *Member, IEEE*, Wenzheng Xu, *Member, IEEE*, Baijun Wu, and Yazhou Tu, *Member, IEEE*

***Abstract*—Recently, Wireless Rechargeable Sensor Networks (WRSNs) based platforms have become promising for broad applications. However, if an adversary disrupts the wireless charging process in WRSNs, sensors may die due to lack of timely energy supply, compromising the reliability and availability of systems relying on sensing tasks. In this paper, we develop a zero-cost power jamming attack in WRSNs, termed rEflection-based jaMmIng aTtack (EMIT), which introduces an off-the-shelf and inconspicuous reflector such as a Coca-Cola can that intentionally reflects the wave from the charger to destructively interfere with the charging wave at the target sensor. Our approach lifts the limitations of traditional charging attacks, including high cost, complex implementation and ease of detection. We conduct extensive field experiments to evaluate EMIT attack in different types of WRSNs. The results show that on average, the success rate of EMIT attack is 90% in WRSNs with fixed charging locations, and 75% in WRSNs with dynamic charging locations. Finally, we build a real-world WRSN on university campus to study the effectiveness of EMIT attack in complex scenarios. In total, EMIT attack causes 134 sensor deaths over 66 days.**

***Index Terms*—Wave reflection, power jamming, network destructiveness, wireless charging.**

I. Introduction

WIRELESS Power Transfer (WPT) technology [1] enables wireless chargers to deliver power to rechargeable devices via radio waves across the air gap. Given its distinctive advantages like no-wiring, no-contact, and low-cost, WPT has gained substantial commercial viability. It attracts significant attention from both industry and academia, and is undergoing rapid development. For instance, with the integration of WPT into healthcare, several wireless charging systems that can wirelessly charge biomedical devices (e.g., pacemakers, insulin pumps, and defibrillators) implanted in or carried by the human body have been successfully developed [2], [3], [4]. These systems eliminate the necessity for traditional battery replacement surgeries, significantly improving patients' quality of life and ensuring safety. Moreover, WPT has been beneficial for smart cities and smart homes [5], [6], [7], where the wireless charging of sensors performing various sensing tasks contributes to the convenience and intelligence of urban life, offering considerable economic benefits. According to Fortune Business Insights, the global wireless charging market reached $19.9 billion as of 2024 and is projected to grow to $52.4 billion by 2033 [8].

Recently Wireless Rechargeable Sensor Networks (WRSNs) [9], [10], [11], [12] is proposed as an effective way to realize WPT in various real-world applications [13], [14], [15]. In WRSNs, a mobile charger (MC), e.g., a mobile vehicle equipped with radio transmitters and batteries, is scheduled based on the network's charging demands to perform charging tasks [16], [17], [18], [19], [20], [21]. Specifically, the MC moves along a pre-designed path constructed by a series of charging locations, and it stays at each charging location until the surrounding sensors are fully charged. The goal of the MC charging schedule is to timely charge every sensor before its energy is exhausted, which extends the infrastructure's operational lifespan and, in turn, ensures the uninterrupted functionalities of the associated application.

A. Jamming Attack in WRSNs

Although WRSNs have created a new dimension of alleviating the energy limitation problem for real applications, its charging process is vulnerable to attacks, which could lead to application failures due to sensor energy depletion. For example, in the scenario of human healthcare with biomedical implants such as leadless pacemakers and cochlear implants [4], the energy exhaustion of these devices hinders their ability to perform crucial tasks like physiological sensing and patient health monitoring, posing a significant threat to human health.

To ensure the security and robustness of WRSNs, a key strategy is to design charging attacks that expose potential vulnerabilities in the wireless charging process, thereby facilitating the development of effective defense mechanisms. However, only few work [22], [23], [24] have focused on the security issues in WRSNs and developed power jamming attacks to hinder sensors from receiving adequate energy during the charging process.

Fig. 1 illustrates the basic idea of power jamming attack, which is motivated by *wave interference* [25], in WRSNs. When the legitimate MC is charging a target sensor, the adversary places a malicious device to the vicinity of the target sensor,

Received 20 April 2025; revised 26 July 2025; accepted 13 August 2025. Date of publication 19 August 2025; date of current version 3 December 2025. This work was supported in part by the National Natural Science Foundation of China under Grant 62072320 and Grant 62272328, and in part by the Natural Science Foundation of Sichuan Province under Grant 2022NSFSC0569, Grant 2024NSFJQ0026, and Grant 2025ZNSFSC0501. Recommended for acceptance by Y. Zeng. *(Corresponding author: Wenzheng Xu.)*

Tang Liu, Jing Gao, Yuan Yin, and Die Wu are with the College of Computer Science, Sichuan Normal University, Chengdu 610101, China (e-mail: liutang@sicnu.edu.cn; jinggao@stu.sicnu.edu.cn; yuanyin@stu.sicnu.edu.cn; wd@sicnu.edu.cn).

Jian Peng and Wenzheng Xu are with the College of Computer Science, Sichuan University, Chengdu 610065, China (e-mail: jianpeng@scu.edu.cn; wenzheng.xu@scu.edu.cn).

Baijun Wu is with the University of Louisiana at Lafayette, Lafayette, LA 70503 USA (e-mail: scu.bjwu@gmail.com).

Yazhou Tu is with the Department of Computer Science & Software Engineering, Auburn University, Auburn, AL 36849 USA (e-mail: yzt0065@auburn.edu).

Digital Object Identifier 10.1109/TMC.2025.3600093

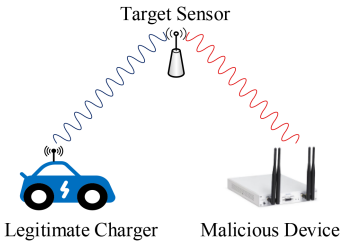


Fig. 1. A power jamming example of a target sensor being attacked by a malicious device.

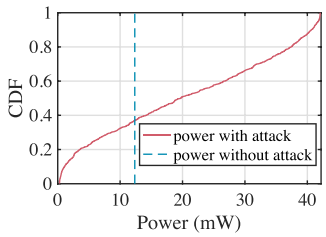


Fig. 2. The CDF of the received power when randomly changing the initial phase of the legitimate wave.

and disrupts the charging process by radiating wave to interfere destructively with the legitimate wave. To guarantee the effectiveness of such a jamming attack, it requires (1) the frequency of the malicious wave should be the same as the legitimate wave, namely **frequency alignment**; and (2) the phase difference of the two waves at the target sensor must be an odd multiple of π [26], [27], [28], namely **phase synchronization**.

Achieving frequency alignment is easy. The frequency of legitimate wave can be measured by using a spectrum analyzer, and then the malicious wave could be adjusted accordingly.

On the other hand, it is challenging or even impossible to synchronize the phase between legitimate charger and malicious device. This is because as long as the legitimate charger keeps randomly changing the initial phase of the wave, the attack will fail. Fig. 2 shows the cumulative distribution function (CDF) of the power received by the target sensor based on 3000 charging iterations. In the experiment, the initial phase of the legitimate wave randomly changes at each iteration, while the malicious device uses the initial phase of the legitimate wave at the first iteration to interference the charging process in all iterations. The results show that the malicious device not only fails to consistently attack the target sensor, but often unintentionally enhances the received power. For example, the power received by target sensor exceeds that without attack in about 63% of 3000 iterations.

B. Our Zero-Cost Attack Approach

Inspired by the fact that the wave reflected by a metal object naturally has the same frequency as the incident wave, and its initial phase always synchronizes with the incident wave no matter how it changes dynamically, we in this paper propose a novel power jamming attack by adopting a reflector as the malicious device, referred to as rEflection-based jaMmIng aTtack (EMIT). The advantages of EMIT are threefold as follows.

First, owing to the high reflection coefficient of metals, a small-sized metal reflector is sufficient to launch an attack, such as a Coca-Cola can, which is readily available and negligible in cost.

Second, no extra devices are required to help the reflector perform the attack, and no future maintenance such as recharging the reflector is needed. Thus, our attack is easy-to-deploy and low-maintenance.

Last, since the radio waves can penetrate paper, the adversary could print the environmental background on paper and affix it to the reflector. By doing so, identifying the reflector as malicious becomes difficult, and hence makes our jamming attack stealthier.

The question now is how to select the reflector's location to effectively attack the charging process. As described aforementioned, MC charges sensors by visiting a set of locations. If we properly place the reflector around a charging location to cause destructive interference, MC has to stay at this location for a longer time in order to fully charge all the surrounding sensors, which delays charging the other sensors from later locations and hence could cause their energy depletion. Apparently, the selection of reflector location is related to the charging locations. In general, WRSNs can be categorized into two types based on how charging locations are determined: (1) fixed charging locations [29], [30]; and (2) dynamic charging locations [19], [31]. In the next, we will discuss how our EMIT can perform destructive and concealable attacks in both scenarios of WRSNs.

WRSNs with fixed charging locations are designed for scenarios where sensors consume energy at a fixed rate, for example, in environment surveillance or health monitoring. This means the total amount of energy transmitted to sensors per charging cycle is pre-known and fixed. Thus, the conventional charging schemes select a set of fixed charging locations to maximize the overall wattage (i.e., charging utility described in Section II-C). Such charging schemes actually enable application developers to detect potential power jamming attacks if the monitored wattage is decreased per charging cycle. To address this issue, our EMIT attack selects the optimal reflector location that can minimize the power received by the target sensor and simultaneously maintains the overall charging utility of the charging location.

WRSNs with dynamic charging locations are proposed to charge sensors with nondeterministic sensing tasks, such as in smart cities or smart homes. Due to the dynamic energy consumption rate of sensors, most charging schemes use online algorithms to dynamically determine the charging locations to satisfy on-demand charging requests in each charging cycle. This raises the challenge of how to place the reflector that can robustly disrupt the charging process of the target sensor regardless of its charging location. To tackle the challenge, we first identify a potential charging area where MC could perform charging tasks to the surrounding sensors, and then we determine the reflector position by maximizing the possibility of reducing the received power of the target sensor.

The main contributions of this work are summarized below.

- To the best of our knowledge, this is the first work that utilizes the wave reflection by adopting a zero-cost Coca-Cola can to launch a jamming attack in WRSNs.

TABLE I
SYMBOLS AND DEFINITIONS

Symbols	Definitions
S	Set of rechargeable sensors
s_i	ith sensor, or its location
N	Number of sensors
b	Energy capacity of each sensor
ec_i	energy consumption rate of sensor s_i
re_i	residual energy of sensor s_i
rl_i	residual lifetime of sensor s_i
B	Battery capacity of MC
l_j	jth charging location
t_{l_j}	charging duration at l_j
S_{l_j}	sensor set belonging to l_j
d_{MC,s_i}	charging distance to s_i
R	Reflector, or its position
d_{R,s_i}	distance between R and s_i
$d_{MC,R}$	distance between MC and R
λ	wavelength
P_{MC,s_i}	The average power arrived at s_i from MC
P_{s_i}	The combined power at s_i
P_{th}	Power threshold for charging utility function
$u(P_{s_i})$	charging utility received by s_i
U_{l_j}	overall charging utility of by S_{l_j} before attack
U'_{l_j}	overall charging utility of by S_{l_j} after attack

- We propose an attack scheme called EMIT to extend the charging duration. The key differences between EMIT and existing jamming attack methods include: (*i*) EMIT does not require any extra charging devices; (*ii*) Once deployed, the reflector requires no maintenance; (*iii*) EMIT can adapt to both WRSNs with fixed and dynamic charging locations.
- We provide theoretical analysis to prove the effectiveness of our EMIT attack. We also demonstrate the EMIT attack in an extensive evaluation, including a real-world WRSN on campus. Through 66 days of experiments, the results show that the number of sensor deaths caused by our EMIT attack is 67 times higher than that without any attacks.
- We provide discussions on several potential defense mechanisms, including using metal detector, implementing manual inspections, and dynamically changing the charging environment.

II. PRELIMINARIES

In this section, we first present the network model and charging model with reflection. Then, we formulate our EMIT problem. For a quick reference, the major notations used in this paper are listed in Table I.

A. Network Model

We consider a 2D plane Ω with a base station (BS), a mobile charger (MC) with battery capacity B, and N stationary sensors. Let S denote the set of sensors, and each sensor $s_i \in S$ is powered by a rechargeable battery with energy capacity b. The energy consumption rate and residual energy of s_i are denoted by ec_i and re_i, respectively. Without confusion, we still use s_i to represent the location of sensor s_i.

In one *charging cycle*, MC departs from the BS with full energy and travels along a pre-designed charging path H to visit a series of charging locations to fully charge surrounding sensors. Particularly, when the MC moves to a charging location, it will fully charge all sensors within its charging range. We denote by l_j the j_{th} charging location in charging path H. When the MC stays at l_j, we use t_{l_j} and d_{MC,s_i} to denote the charging duration and the charging distance to sensor s_i, respectively. Before MC exhausts its energy, it will return to the BS to get recharged for the next charging cycle.

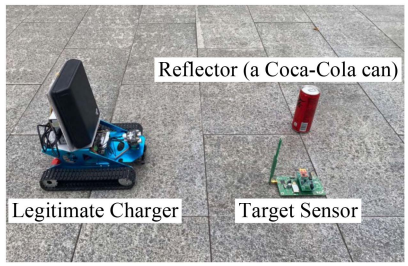


Fig. 3. An illustration of reflection-based jamming attack.

A cylindrical reflector (i.e., Coca-Cola can) R is provided to mount a jamming attack. We still use R to represent the position of the reflector, and denote by d_{R,s_i} and $d_{MC,R}$ the distances between R and s_i, MC and R, respectively. Fig. 3 depicts an instance of the reflection-based jamming attack. In Section VIII-B, we discuss that reflectors of other shapes, sizes, and materials also can be used to launch attacks.

B. Charging Model With Reflection

To explore the regularity of the power distribution with a placed reflector, a charging model with reflection needs to be built. First, we express the wave emitted from MC as:

$$A_{MC}(t) = A_0 \cos\left(\phi_0 + 2\pi f t\right), \tag{1}$$

where A_0, f, ϕ_0 are denoted as the amplitude, frequency and initial phase of the wave from MC, respectively. Since the amplitude of the wave attenuates with the increase of distance, the wave arrived at sensor s_i can be expressed as:

$$A_{MC,s_i}(t) = \frac{A_0}{\hat{d}_{MC,s_i}} \cos\left(\phi_0 + 2\pi f t - \frac{2\pi}{\lambda} d_{MC,s_i}\right). \tag{2}$$

In (2), $\hat{d}_{MC,s_i} = \frac{d_{MC,s_i}+\beta}{\sqrt{\alpha}}$ is the attenuation factor in the propagation of the wave from MC to sensor s_i, where β is a parameter to adjust the Friis' free space equation for short distance transmission. $\alpha = \frac{G_s G_r \eta}{L_P}(\frac{\lambda}{4\pi})^2$, where G_s and G_r are the antenna gains of MC and sensor, respectively, η is the rectifier efficiency, L_p is the polarization loss, and λ is the wavelength. Assume that the period of the radio wave is T, the average power at s_i can be written as:

$$P_{MC,s_i} = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} \left[A_{MC,s_i}(t)\right]^2 \mathrm{d}t = \frac{A_0^2}{2\hat{d}_{MC,s_i}^2}. \tag{3}$$

In the charging scenario with reflector, the wave reflection has the two following characteristics:

(*i*) After reflection, the wave amplitude experiences varying degrees of attenuation depending on the material of the reflector. For instance, when radio waves encounter a metal surface, the high conductivity enables the free electrons to generate a counter propagating electric field, leading to very low attenuation [32]. On the other hand, the attenuation caused by non-conductive materials is much greater. We use Γ to represent the reflection coefficient of the reflector, which is the amplitude ratio of the reflected wave to the incident wave;

(*ii*) When the incident wave is reflected by a more dense medium, the crests get reflected as troughs and troughs as crests, i.e., the reflected wave undergoes a 180° phase change on reflection. Such a phenomenon is called *half-wave loss* [25].

Considering these two characteristics, we can obtain the reflected wave:

$$A_R(t) = \frac{\Gamma A_0}{\hat{d}_{MC,R}} \cos\left(\phi_0 + 2\pi f t - \frac{2\pi}{\lambda} d_{MC,R} - \pi\right). \quad (4)$$

When the reflected wave arrives at s_i, it can be expressed as:

$$A_{R,s_i}(t) = \frac{\Gamma A_0}{\hat{d}_{MC,R}\hat{d}_{R,s_i}} \cos\left(\phi_0 - \pi + 2\pi f t - \frac{2\pi}{\lambda}\left(d_{MC,R} + d_{R,s_i}\right)\right). \quad (5)$$

Since the combined wave at s_i is $A_{s_i}(t) = A_{MC,s_i}(t) + A_{R,s_i}(t)$, similarly to (3), the average power of the combined wave at s_i can be calculated as:

$$\begin{aligned} P_{s_i} &= \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} [A_{s_i}(t)]^2 \mathrm{d}t = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} [A_{MC,s_i}(t) + A_{R,s_i}(t)]^2 \,\mathrm{d}t \\ &= \frac{-\Gamma A_0^2}{\hat{d}_{MC,s_i}\hat{d}_{MC,R}\hat{d}_{R,s_i}} \cos\frac{2\pi}{\lambda}\left(d_{MC,R} + d_{R,s_i} - d_{MC,s_i}\right) \\ &\quad + \frac{A_0^2}{2\hat{d}_{MC,s_i}^2} + \frac{\Gamma^2 A_0^2}{2\hat{d}_{MC,R}^2\hat{d}_{R,s_i}^2}. \end{aligned} \quad (6)$$

From (6), we can see that once a reflector is placed, the power distribution will be very complicate, which is related to the position relationships between MC, sensor, and reflector. Specifically, when $d_{MC,R} + d_{R,s_i} - d_{MC,s_i}$ equals $k\lambda$, $(k \in N)$, the combined power at sensor s_i will be weakened, and when $d_{MC,R} + d_{R,s_i} - d_{MC,s_i}$ equals $(k + \frac{1}{2})\lambda$, $(k \in N)$, the combined power will be enhanced.

To verify our charging model, we conduct a field experiment. The testbed consists of a commodity off-the-shelf wireless charger TX91501 produced by Powercast [34], a rechargeable sensor equipped with an omnidirectional antenna, and a metallic cylindrical reflector (i.e., a Coca-Cola can). The coordinates of the charger and the sensor are (0 cm, 0 cm) and (0 cm, 80 cm), respectively. We place the reflector at different positions around the sensor and record the power received by it. We adopt (6) to fit the experimental data. The fitting results are shown in Fig. 4. It can be seen that the field experimental data is consistent with the simulation results, which proves that our proposed charging model with reflection is feasible and practical in our experimental environment.

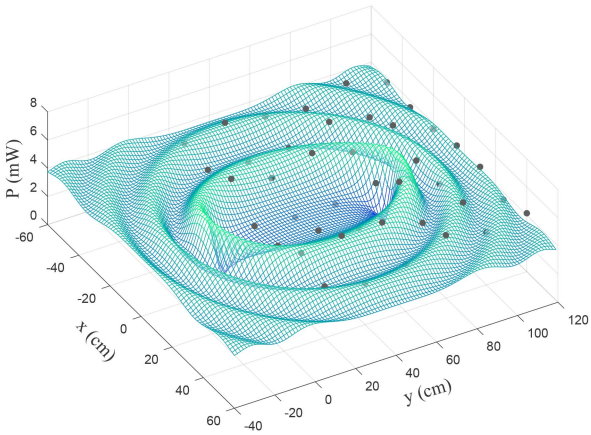


Fig. 4. Comparing experimental data (black dots) and fitted data (mesh). Fitted results are based on $\alpha = 9.5$, $\beta = 6.0$, $\Gamma = 0.98$ [33].

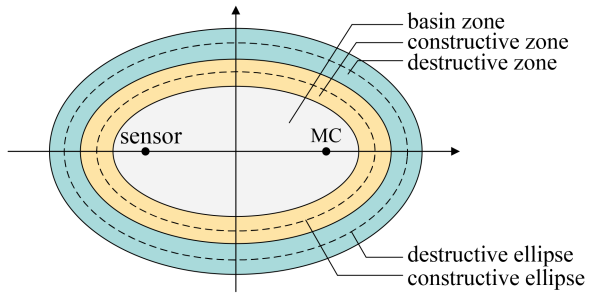


Fig. 5. An illustration of ellipses and regions around MC and sensor.

Furthermore, Fig. 4 shows a trend of the elliptical ripple expanding outward, and the ellipses with high and low power appear alternatively. We refer to the high-power ellipses as *constructive ellipses* and the low-power ellipses as *destructive ellipses*, because once the reflector is placed anywhere on these ellipses, the waves from the charger and the reflector will constructively or destructively interfere at the sensor. Fig. 4 also illustrates that the innermost constructive and destructive ellipses exhibit the most significant enhancement or weakening effects, attributed to the shorter propagation distances of the reflected wave. The experimental data show a substantial difference in the enhancement effect between the innermost and the second constructive ellipses, amounting to 271.01%. Similarly, there is a 198.39% disparity in the weakening effect between the innermost and the second destructive ellipses. We name the high-power zone containing the constructive ellipse as the *constructive zone*, and the low-power zone containing the destructive ellipse as *destructive zone*.

Note that when the reflector is placed between the sensor and the MC (we call the region *basin zone*), it will block the line-of-sight transmitting power and raise the suspicion of the network maintainers. Therefore, in order to guarantee the destructiveness and concealment of our jamming attack, we stipulate that the reflector can only be placed on the innermost destructive ellipse of the target sensor. For better comprehension, we use Fig. 5 to illustrate the specific locations of constructive and destructive ellipses and zones.

C. Charging Utility Model

In practice, limited to the sensor's hardware, the power in watt received by each sensor cannot exceed a threshold P_{th}. For sensor s_i, we can calculate its *charging utility* according to the power it received:

$$u(P_{s_i}) = \begin{cases} \frac{1}{P_{th}} \cdot P_{s_i}, & P_{s_i} < P_{th}, \\ 1, & P_{s_i} \geq P_{th}. \end{cases} \tag{7}$$

From (7), we can see that the normalized charging utility of sensor s_i is first proportional to the received power and then reaches a constant when the received power exceeds P_{th}.

D. Problem Formulation

In WRSNs, the MC travels along a charging path to visit a series of charging locations. At each location, the MC charges nearby sensors before proceeding to the next. If the MC arrives at a charging location too late, some sensors will deplete their energy before receiving charging services, leading to their deaths. To this end, in this paper, we study how to realize the rEflection-based jaMmIng aTtack (EMIT) by placing a reflector to maximize the charging duration.

For WRSNs with fixed charging locations, most charging schemes focus on maximizing the overall charging utility obtained by all sensors. Any placement of the reflector that reduces the charging utility of the sensors within the charging range makes the attack easily detectable. Therefore, to maximize the destructiveness and prevent our attack from being detected, our objective is: given a charging location l_j and a sensor set S_{l_j} belonging to l_j, how to choose a placement position for a reflector R to maximize the charging duration t_{l_j}, subject to that the overall charging utility of all sensors in S_{l_j} does not decrease. Formally, we state our goal as:

$$\begin{aligned} &\text{(P1)} \qquad \text{maximize} \quad t_{l_j}, \\ &\text{s.t.} \quad U_{l_j} \geq U'_{l_j}, \quad U_{l_j} = \sum_{s_i \in S_{l_j}} u(P_{s_i}), \end{aligned} \tag{8}$$

where the U'_{l_j} and U_{l_j} are the overall charging utility of S_{l_j} before and after the attack, respectively.

For WRSNs with dynamic charging locations, to launch a stably-working attack, our objective is: given a sensor set S_{l_j}, how to choose a placement position for a reflector R to maximize the charging duration t_{l_j} regardless of where the MC stays. Formally, we state our goal as:

$$\begin{aligned} &\text{(P2)} \qquad \text{maximize} \quad t_{l_j}, \\ &\text{s.t.} \quad \forall l_j \in \Omega. \end{aligned} \tag{9}$$

III. Threat Model

In this work, the adversary's goal is to maximize the charging duration, ultimately resulting in the deaths of sensors in WRSNs. To launch the attack, the basic knowledge required for adversary is the locations of to-be-charged sensors, which can be obtained by eavesdropping on network data flow [35] or acquiring knowledge of the network protocol [36]. For example, when a sensor has a charging request, it will send a charging request containing its location information to the MC. We can intercept this information to obtain the sensor's exact location. Moreover, methods to obtain the sensor location also include installing covert cameras at Points of Interests (PoIs) to capture the distribution of sensors [37].

In general, based on the types of the WRSNs, the possible intentions can be grouped into two categories:

WRSNs with fixed charging locations: in this type of WRSNs, the MC is scheduled to visit a series of fixed charging locations to charge sensors with deterministic sensing tasks. Besides eavesdropping on the network data flow and acquiring the network protocol, these fixed charging locations can also be obtained by deploying cameras near the charging sites. To ensure the concealment of the attack, the adversary needs to guarantee that the overall charging utility of all sensors within the charging range is not affected. This is to prevent the network maintainers from detecting the attack by monitoring changes in the overall performance of the network.

WRSNs with dynamic charging locations: in this type of WRSNs, the charging locations for each charging cycle change with the energy status of the sensors, making it suitable for charging sensors with dynamic sensing tasks. Therefore, the adversary has to launch the attack relying solely on the locations of the sensors and the wave frequency. In such dynamic environment, the adversary must ensure that the attack remains robust to the dynamic changes in charging locations, meaning that the attack should be effective regardless of where the MC stops.

In general, we consider that the adversary should seek to achieve a stably-working, easily-concealable, and low-cost attack. The simplest way to disrupt wireless charging is to damage the MC and sensors, or sabotage the roads that the MC travels. However, such physically destructive approaches require the adversary to be present at the attack site, posing a significant risk of being detected and facing severe legal consequences. In contrast, a zero-cost and inconspicuous Coca-Cola can provides a feasible way to disrupt the charging process by utilizing the wave reflection, which not only allows the adversary to avoid being present at the attack site, but also truly achieves a low-cost attack while substantially improving the concealment. Finally, to effectively launch the attack in real physical world, this attack scheme should be adaptive, easily extending to various complex application environments.

IV. Attack With Fixed Charging Locations

In this section, we develop the attack method for the WRSNs with fixed charging locations. Particularly, our attack method is consists of two algorithms: a target sensor selection algorithm and a reflector placement algorithm. The target sensor selection algorithm is specifically designed to identify the potential target sensor that could yield the maximum charging duration, and the reflector placement algorithm is used to determine the optimal position R for placing the reflector.

A. Target Sensor Selection Algorithm

When the MC reaches charging location l_j, it will fully charge all the sensors in sensor set S_{l_j}. As a result, the charging duration

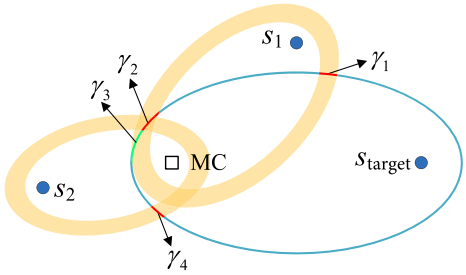


Fig. 6. An example of how to obtain candidate placing segments.

of the MC is decided by the sensor with the longest charging duration in S_{l_j}. In order to select an appropriate target sensor for maximizing the MC's charging duration, in this subsection, we jointly consider the position, residual energy, and energy consumption rate of each sensor in S_{l_j} to calculate the potential attack effects, and subsequently construct a target sensor queue. The sensor at the head of the queue will be selected as the first target sensor.

Although we have stipulated that the reflector must be placed on the innermost destructive ellipse of the target sensor, it is crucial to note that placing the reflector at different positions on this ellipse still has different impacts on the combined power received by the target sensor.

This is because when two waves interfere destructively, the power gap between them will determine the combined power, i.e., the smaller the gap, the weaker the combined power, and vice versa. Theoretically, we have the following theorem:

Theorem 1: When the reflector is placed at the innermost destructive ellipse of sensor s_i, selecting any vertex as the reflector's placement position will result in the maximum attack effect, while choosing any co-vertex as the placement position will yield the minimum attack effect.

Proof: Note that the amplitude of the wave will be inevitably attenuated during reflection, and the reflected wave experiences greater propagation attenuation compared to the wave from the MC. Thus, the power of the reflected wave arriving at the sensor must be lower than that of the wave from the MC. To achieve the maximum attack effect, we need to maximize the power of the reflected wave reaching the sensor. According to (5), we can calculate the power of the wave from reflector *R* reaching sensor s_i as:

$$P_{R,s_i} = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} [A_{R,s_i}(t)]^2 \mathrm{d}t = \frac{\Gamma^2 A_0^2}{2\hat{d}_{MC,R}^2 \hat{d}_{R,s_i}^2}. \tag{10}$$

Thus, we can see that P_{R,s_i} is determined by $\hat{d}_{MC,R}^2 \hat{d}_{R,s_i}^2$. Based on the geometric properties of ellipse, no matter where the reflector is deployed at the innermost destructive ellipse, the value of $d_{MC,R} + d_{R,s_i}$ remains constant, equivalent to $\hat{d}_{MC,R} + \hat{d}_{R,s_i}$ being constant. Consequently, by maximizing the difference between $\hat{d}_{MC,R}$ and $\hat{d}_{R,s_i}$, we can minimize $\hat{d}_{MC,R}^2 \hat{d}_{R,s_i}^2$, thereby maximizing the reflected power reaching the sensor. Thus, to maximize the attack effect, we should place the reflector at any vertex of the innermost destructive ellipse. Conversely, placing the reflector at any co-vertex results in the difference between $\hat{d}_{MC,R}$ and $\hat{d}_{R,s_i}$ being zero, thus minimizing the reflected power reaching the sensor. Hence, the theorem is proven. □

Since we need to guarantee the overall charging utility of the sensor set S_{l_j} does not decrease, the reflector may not be exactly placed at one of the vertexes at the innermost ellipse. So, we consider the lower bound of the attack effect, i.e., the placement position of the reflector is co-vertex, to calculate the potential charging duration of each sensor under EMIT attack.

For any sensor s_i in S_{l_j}, according to (6), when the reflector is placed at one of the co-vertexes, the received power by s_i is:

$$\begin{aligned} P_{s_i} &= \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} [A_{s_i}(t)]^2 \mathrm{d}t = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} [A_{MC,s_i}(t) + A_{R,s_i}(t)]^2 \mathrm{d}t \\ &= \frac{A_0^2}{2\hat{d}_{MC,s_i}^2} - \frac{\Gamma A_0^2}{\hat{d}_{MC,s_i}\hat{d}_{MC,R}\hat{d}_{R,s_i}} + \frac{\Gamma^2 A_0^2}{2\hat{d}_{MC,R}^2 \hat{d}_{R,s_i}^2}. \end{aligned} \tag{11}$$

Then, we can express the potential charging time for s_i under attack as:

$$t_{s_i} = \frac{b - re_i}{P_{s_i} - ec_i}. \tag{12}$$

If the potential charging time t_{s_i} of s_i exceeds the MC's charging duration without attack, it indicates that attacking s_i can prolong the charging duration, so s_i will be added to the candidate target sensor set S_{cand}.

When all potential sensors are picked out, we gradually select the sensor with the longest charging time from S_{cand} to add it to the target sensor queue Q_s, until all the candidate sensors are included. The sensor at the head of the queue then becomes the first target for our attack.

B. Reflector Placement Algorithm

Next, we design a reflector placement algorithm to place the reflector. For the target sensor, its charging utility will decline due to the attack. Thus, to escape being detected by maintaining the overall charging utility, the reflector must enhance the received power for at least one sensor in S_{l_j}.

From the analyses in Section II-B, we can find that if the reflector is placed within the constructive zone of a sensor, its received power will be enhanced due to constructive interference. Therefore, by calculating the overlaps of the target sensor's innermost destructive ellipse and the other sensors' constructive zones, we can find out several segments where placing the reflector can weaken the received power of the target sensor while simultaneously enhancing the power the other sensors receive. Further, by removing the segments located within the basin zone, we can obtain all the candidate segments for placing the reflector. Fig. 6 shows that 4 segments (i.e., γ_1, γ_2, γ_3 and γ_4) are located within the constructive zones of sensor s_1 and s_2. After removing γ_3, which is located within the basin zone of s_2, γ_1, γ_2, and γ_4 are the candidate segments for placing the reflector.

Now, although we have reduced the candidate placement range for the reflector from an ellipse to several short-length

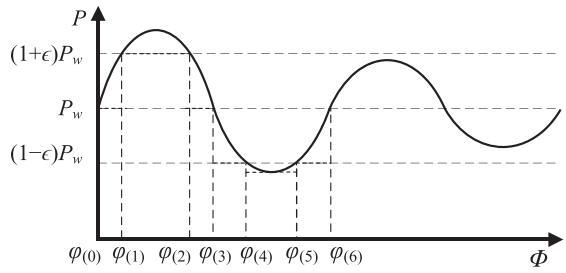


Fig. 7. Combined power approximation.

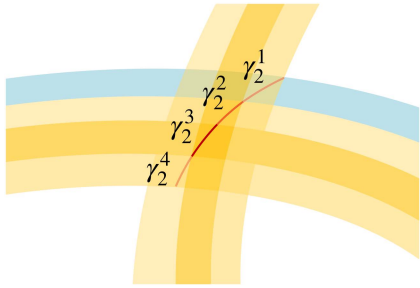


Fig. 8. An example of discretization to segment γ_2.

candidate segments, these segments are still continuous, which makes infinite candidate positions. Considering that when the reflector is placed at different positions on a short-length segment, the different phase differences between the waves from MC and reflector will play a dominant role in the combined power, we aim to design a discretization method by adopting a piecewise constant function to approximate the nonlinear relationship between the combined power and the phase difference. Let $P_{s_i}(\phi)$ denote the combined power in terms of the phase difference ϕ between the waves from MC and reflector. We present a piecewise constant function to approximate the combined power as follows:

$$\widetilde{P}_{s_i}(\phi) = \begin{cases} P_{s_i}(\varphi_{(0)}), & \phi = \varphi_{(0)}, \\ P_{s_i}(\varphi_{(m-1)}), & \varphi_{(m-1)} < \phi \le \varphi_{(m)} \\ & (m = 1, \ldots, M), \\ P_w, & \phi > \varphi_{(M)}, \end{cases} \tag{13}$$

where P_w represents the power received by s_i without any reflection. Since no segment is located within the basin zone, we just need to consider the situation that the phase difference greater than $\frac{\pi}{2}$, i.e., $\varphi_{(0)} = \frac{\pi}{2}$, in designing the piecewise function. Fig. 7 shows an instance of such a combined power approximation, the ϵ is a given approximation error and the endpoints of the piecewise constant function are $\varphi_{(1)}$,..., $\varphi_{(6)}$. When the phase difference exceeds $\varphi_{(6)}$, the combined power will fall within the range of $((1-\epsilon)P_w, (1+\epsilon)P_w)$, so under the given approximation error, the approximation power equals P_w. The reason behind this is that a larger phase difference means that the two waves have a larger distance difference when they reach the target sensor (i.e., the reflector is placed far away from the MC and the target sensor), resulting in a weak interference effect.

As shown in Fig. 7, we can see that the phase difference is divided into seven parts, each of which has a constant approximation power. For this discretization, we have the following Lemma:

Lemma 1: Let $\widetilde{P}_{s_i}(\phi)$ denote the approximated combined power received by s_i, the approximation error is subject to

$$\frac{\left|\widetilde{P}_{s_i}(\phi) - P_{s_i}(\phi)\right|}{\widetilde{P}_{s_i}(\phi)} \le \epsilon, \left(\frac{\pi}{2} \le \phi, 0 < \epsilon < 1\right). \tag{14}$$

By using our discretization method, each candidate segment γ_j can be divided into several subsegments, γ_j^1,..., γ_j^n. We use Fig. 8 to depict an example of such a discretization to candidate segment γ_2. It can be seen that segment γ_2 is divided into four distinct subsegments, γ_2^1, γ_2^2, γ_2^3, and γ_2^4. If a reflector is placed at any point on the one subsegment, the combined power the target sensor receives is approximately the same. Therefore, this discretization enables us to transform the continuous candidate placement segments with varying combined powers of sensors into several fine-grained subsegments with approximated constant combined power. Based on the discretization method and (7), we can use the following equation to calculate the approximated overall charging utility when a reflector is placed at a subsegment γ_j^q:

$$\widetilde{U}_{l_j}^{\gamma_j^q} = u\left(P_{s_{target}}\right) + \sum_{s_i \in S_{l_j/s_{target}}} u\left(\widetilde{P}_{s_i}(\phi)\right), \tag{15}$$

where $S_{l_j/s_{target}}$ denotes the set of sensors in S_{l_j} exclude the target sensor s_{target}. For (15), we have the following Theorem:

Theorem 2: Let $\widetilde{U}_{l_j}^R$ denote the approximated overall charging utility of set S_{l_j} as (15) expresses, and $U_{l_j}^R$ denote the overall charging utility of S_{l_j}. The approximation error is

$$\frac{|\widetilde{U}_{l_j}^R - U_{l_j}^R|}{\widetilde{U}_{l_j}^R} \le \epsilon, (0 < \epsilon < 1). \tag{16}$$

Proof: According to Lemma 1, $\frac{|\widetilde{P}_{s_i}(\phi) - P_{s_i}(\phi)|}{\widetilde{P}_{s_i}(\phi)} \le \epsilon$, for a single sensor s_i, there are three cases to be considered:

- Case 1: $\widetilde{P}_{s_i}(\phi) \le P_{s_i}(\phi) \le P_{th}, P_{s_i}(\phi) \le \widetilde{P}_{s_i}(\phi) \le P_{th}$;
- Case 2: $\widetilde{P}_{s_i}(\phi) \le P_{th} \le P_{s_i}(\phi), P_{s_i}(\phi) \le P_{th} \le \widetilde{P}_{s_i}(\phi)$;
- Case 3: $P_{th} \le \widetilde{P}_{s_i}(\phi) \le P_{s_i}(\phi), P_{th} \le P_{s_i}(\phi) \le \widetilde{P}_{s_i}(\phi)$.

For Case 1, $u(P_{s_i}(\phi)) = \frac{P_{s_i}(\phi)}{P_{th}}$, $u(\widetilde{P}_{s_i}(\phi)) = \frac{\widetilde{P}_{s_i}(\phi)}{P_{th}}$, according to Lemma 1, the conclusion obviously stands.

For Case 2, if $\widetilde{P}_{s_i}(\phi) \le P_{th} \le P_{s_i}(\phi)$, then $u_{(P_{s_i})} = 1$, $\frac{|u(\widetilde{P}_{s_i}(\phi))-1|}{u(\widetilde{P}_{s_i}(\phi))} \le \frac{|u(\widetilde{P}_{s_i}(\phi)) - \frac{P_{s_i}(\phi)}{P_{th}}|}{u(\widetilde{P}_{s_i}(\phi))}$; if $P_{s_i}(\phi) \le P_{th} \le \widetilde{P}_{s_i}(\phi)$, then $u(\widetilde{P}_{s_i}(\phi)) = 1$, $\frac{|1-u(P_{s_i}(\phi))|}{u(\widetilde{P}_{s_i}(\phi))} \le \frac{|\frac{\widetilde{P}_{s_i}(\phi)}{P_{th}} - u(P_{s_i}(\phi))|}{u(\widetilde{P}_{s_i}(\phi))}$, so, Case 2 stands too.

For Case 3, $u(P_{s_i}(\phi)) = 1$, $u(\widetilde{P}_{s_i}(\phi)) = 1$, $\frac{|u(\widetilde{P}_{s_i}(\phi)) - u(P_{s_i}(\phi))|}{u(\widetilde{P}_{s_i}(\phi))} = 0 < \epsilon$, the conclusion stands.

In all, for a single sensor, the conclusion stands, so for the all sensors in set S_{l_j}, the conclusion still stands. □

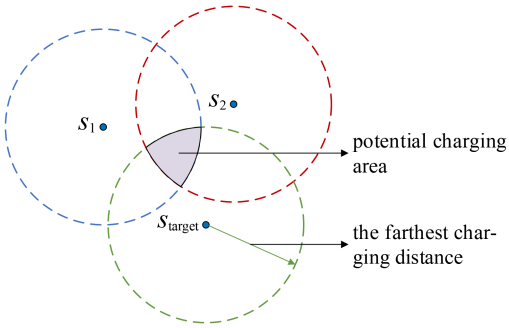


Fig. 9. An example of MC's potential charging area.

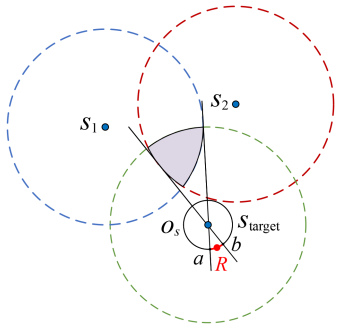


Fig. 10. An illustration of placing the reflector.

After applying the piecewise constant function to divide all the candidate segments into several fine-grained subsegments, we figure out all the candidate subsegments by identifying the subsegments where placing the reflector could potentially maintain the overall charging utility. For all candidate subsegments, we select the subsegment closest to any vertex to place the reflector, and the special placement position is the closest point to any vertex within the selected subsegment. For the target sensor s_{target}, i.e., the head node in the target sensor queue Q_s, if placing the reflector on all the subsegments failed in maintaining the overall charging utility, we choose the next sensor in Q_s as the new target sensor to launch EMIT attack. Further, if attacking any sensor in Q_s can not maintain the overall charging utility, we call that the EMIT fails in attacking the corresponding charging location, then we can choose another charging location to mount EMIT attack. In Section VI-C, we tried different sensor distributions, and the result suggests that the lowest attack success rate can reach 68%, even if there are only 2 sensors within the charging range.

V. Attack With Dynamic Charging Locations

In the scenarios like smart cities and smart homes, the energy consumption rate of sensors vary with the tasks over the time. As a result, the charging locations are dynamic in such WRSNs. In this section, we propose a robust charging attack that can consistently disrupt the charging process, regardless of the MC's specific charging location.

Note that, although the charging location is dynamic, as long as the MC performs its charging task, it still has a potential charging area limited by the farthest charging distance. Hence, our basic idea for launching a robust attack is to first identify a placeable range for reflector based on the MC's potential charging area and the target sensor's location. Then, we pinpoint the optimal location for the reflector from its placeable range that has the greatest chance to reduce the received power of the target sensor.

To find the potential charging area of the MC, we draw circles with multiple adjacent to-be-charged sensors as centers and the farthest charging distance as radius. To transfer energy to each sensor, the MC must stay within the overlap formed by these circles. We refer to this overlap the potential charging area of the MC. Fig. 9 depicts a potential charging area formed by three sensors.

Recall that in designing the previous attack with fixed charging location, we stipulated that the reflector should be placed on the innermost destructive ellipse with the MC and the target sensor as the foci to maximize the charging duration. However, when the charging location varies, the position of the innermost destructive ellipse formed by the MC and the target sensor also varies. Obviously, this presents a significant challenge in determining the placement position of the reflector.

Fortunately, we observed an interesting phenomenon: regardless of the position where the MC stops within the potential charging area, the distance between the target sensor and a vertex of the innermost destructive ellipse formed by the MC and target sensor remains constant.

Lemma 2: No matter where the MC stays within the potential charging area, one vertex of its innermost destructive ellipse formed by the target sensor and the MC always lies on a circle with a radius $\frac{\lambda}{2}$ and the target sensor as the center.

Proof: Note that, for any one vertex of the innermost destructive ellipse, it always satisfies $d_{MC,vertex} + d_{vertex,s_{target}} - d_{MC,s_{target}} = \lambda$. For the vertex closer to s_{target}, since $d_{MC,vertex} = d_{MC,s_{target}} + d_{vertex,s_{target}}$, the distance between the sensor and the vertex is $\frac{\lambda}{2}$. Thus, we can conclude that no matter the location the MC is, the distance between the target sensor and the vertex is always equal to $\frac{\lambda}{2}$. The lemma is proven. □

Let O_s denote the circle with the target sensor as the center and $\frac{\lambda}{2}$ as the radius. Since the MC can only perform its charging tasks when it is within the potential charging area, we identify an arc on O_s as the placeable range of the reflector based on the potential charging area. The specific method is to draw two straight lines through the target sensor from the edges of the potential charging area on different sides. After passing through the target sensor, these two straight lines will intersect the O_s at two points, and the arc between these two points is the placeable range of the reflector. To enable the placed reflector to adapt to as many potential charging positions of MC as possible, we set the reflector's placement position *R* at the center of the placeable range. Fig. 10 illustrates an example of determining the placement position of the reflector. It can be seen that the two lines from the different edges of the potential charging area to the target sensor intersect with the circle O_s at points a and b, and the midpoint of the arc $\overset{\frown}{ab}$ is the reflector's placement position *R*.

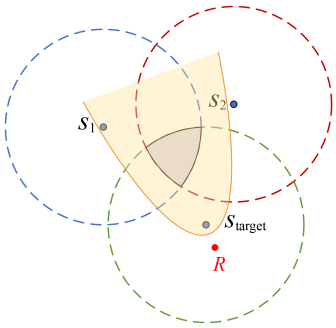


Fig. 11. An illustration of successful attack area.

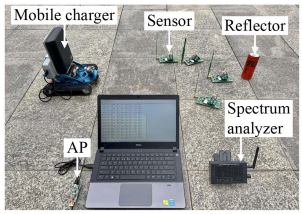


Fig. 12. Testbed.

Subsequently, we analyze the adaptability of our attack with dynamic charging location. Theorem 3 provides the conditions under which the reflector can successfully launch an attack. Here, we define a successful attack as follows: after placing the reflector, the power received by the target sensor is less than the received power without the reflector.

Theorem 3: The condition under which the placed reflector can successfully launch an attack on the target sensor is

$$\frac{3\lambda}{4} < d_{MC,R} + d_{R,s_{target}} - d_{MC,s_{target}} < \lambda. \quad (17)$$

Proof: According to principle of wave interference, destructive interference occurs when the phase difference between the direct wave and the reflected wave meets:

$$\frac{3\pi}{2} < \frac{2\pi}{\lambda}\left(d_{MC,R} + d_{R,s_{target}} - d_{MC,s_{target}}\right) < 2\pi. \quad (18)$$

Thus, when the path difference between the two waves satisfies $\frac{3\lambda}{4} < d_{MC,R} + d_{R,s_{target}} - d_{MC,s_{target}} < \lambda$, destructive interference will occur. Hence, the theorem is proven. □

Fig. 11 illustrates the condition required for the strategically placed reflector to launch an successful attack. Specifically, when the MC stays within the yellow-shaded area, the reflector can effectively reduce the power received by the target sensor.

VI. Attack Performance Evaluation

The eventual goal of our EMIT attack is to cause energy depletion of sensors in WRSNs. To achieve the goal, the two keys are:

- Maximize the charging duration of MC at the attacked charging location. The longer charging duration, the higher possibility the sensors at the later charging locations can not be timely charged before energy exhaustion.
- Minimize the power (in watt) received by the target sensor. MC needs to spend more time at the attacked charging location to fully charge the target sensor with smaller received power.

Apparently, the better attack performance achieved at the attacked charging location, the larger chance of the success of EMIT attack. In this section, we focus on evaluating the destructiveness and concealment of EMIT attack at the charging location under various conditions.

A. Experimental Setting

As shown in Fig. 12, our testbed consists of (1) an MC with the TX91501 wireless charger produced by Powercast [34]; (2) 6 rechargeable sensors equipped with P2110 power receivers with a battery capacity of 50J [34]; (3) a spectrum analyzer that measures the frequency of radio waves emitted by the MC; (4) a Coca-Cola can as the reflector, and its reflection coefficient Γ is 0.98 [33]; (5) an AP connected to a laptop to report the received power from the sensors. We used the data returned to the AP to observe the charging efficiency loss caused by EMIT on the laptop, with a precision of 10^{-2} mW.

The energy consumption rate of each sensor ranges between 0.1mJ/s-0.3mJ/s, and the initial residual energy of each sensor ranges between $0.5b$-$1b$. Due to the directional nature of the TX91501 charger, we rotate it to face the target sensor whenever we need to record experimental data, which is the same as the method used in the related studies [24], [27], [38], [39]. We calculate the placement position of the reflector with the measured wave frequency and the values of the parameters α, β, and ϵ in (6) set to 9.5, 6.0, and 0.05, respectively.

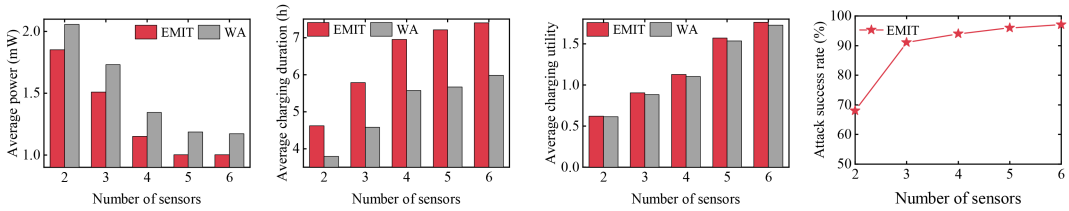
Considering that practical applications of WRSNs are usually deployed in real-world environments, we did not conduct the experiments under the ideal conditions of a microwave anechoic chamber. To closely simulate real wireless charging application scenarios, in Section 6.5, we evaluate our EMIT attack in both indoor and outdoor settings, as well as in urban and rural environments.

It is worth noting that during the experiments, there were no other wave sources operating at the same 915 MHz frequency as the MC in the vicinity. Since the sensor's receiving antenna is only capable of receiving waves within the 850–950 MHz range [34], other signals present in the environment (such as 5G signals, Wi-Fi signals, and broadcast waves) did not affect our experimental results.

B. Attack Performance Metrics

To evaluate the destructiveness and concealment of our EMIT, four metrics are introduced in our experiments:

- *Received Power*: The power in watt received by the target sensor, which represents the destructiveness caused by the attack on the target sensor.
- *Charging Duration*: The time duration that MC takes to fully charge all sensors within the charging range, which indicates the destructiveness of the attack on the charging location.
- *Overall Charging Utility*: The total utility obtained by all sensors within the attacked charging range, and is used to measure the concealment of our attack.



(a) Received power. (b) Charging duration. (c) Charging utility. (d) Success rate.

Fig. 13. Attack results with fixed charging locations.

- *Attack Success Rate*: In WRSNs with fixed charging locations, a successful attack means that the power received by the target is reduced while the overall charging utility does not decrease. In WRSNs with dynamic charging locations, a successful attack means the charging duration is larger than that without attack. We repeat our field experiment under different situations, and the attack success rate measures the effectiveness of the attack.

C. Attack Results With Fixed Charging Locations

In this subsection, we evaluate our EMIT attack performance with fixed charging locations under different situations. The charging scheme in [40] is used to determine the charging location. We vary the number of the sensors at the charging location from 2 to 6. In addition, we repeat the experiment 100 times for each sensor set, and at each iteration we randomly change the sensor locations. All experimental results are the average values.

Received power: As shown in Fig. 13(a), the average power received by the target sensor under EMIT attack is consistently lower than that Without Attack (**WA**), no matter how many sensors are located within the charging range. For example, the received power by the target sensor under attack is reduced by 0.20 mW when there are 2 sensors, while it is reduced by 0.17 mW when 6 sensors present. The results suggest that our EMIT attack can effectively disrupt the charging process of the target sensor.

Charging duration: Fig. 13(b) illustrates on average EMIT attack increases the charging duration by 24.77% under different sensor distributions. The results provide confidence that our attack can cause the charging delay at the later charging location, which could lead to sensor energy depletion.

Overall Charging Utility: From Fig. 13(c), we observed that the charging utility under EMIT attack does not decrease by comparing to WA in all cases. As a matter of fact, the charging utility under EMIT attack is even slightly better than WA. To explain this, we measure the power distribution of one experiment with 4 sensors. Fig. 14 depicts the power heatmap, which reveals how the reflector influences the received power of each sensor. Specifically, the area around the reflector appears to be alternating bright and dark regions due to the interference between the waves from the MC and from the reflector. Therefore, it is possible that the target sensor is situated within the low-power interference weakened region, while the other three sensors are within the interference enhanced regions. The results confirm the concealment of our EMIT attack in WRSNs with fixed charging locations, effectively avoiding an overall decrease in charging performance.

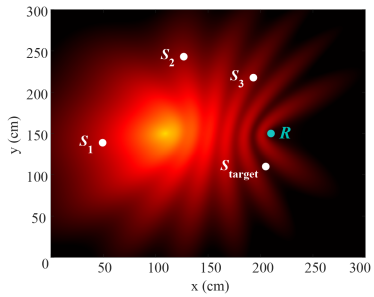


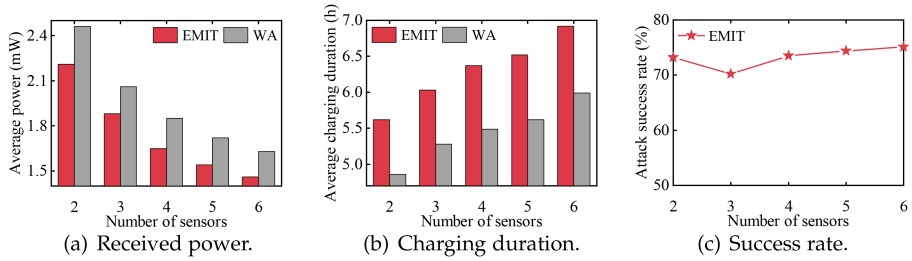
Fig. 14. Power heatmap.

Attack success rate: In Fig. 13(d), when the number of sensors located within the charging range is 2, the attack success rate is 68%. This is because when the number of sensors is too few, it poses a strong constraint to maintain the overall charging utility under attack. In other words, we must find the place for the reflector that the reduced power at the target sensor is equal to or small than the enhanced power at the other sensors. This constraint should be mitigated as the number of sensors increases. Fig. 13(d) shows that the attack success rate rapidly exceeds 90% when the number of sensors is larger than 2, showing that EMIT is highly flexible in different sensor distributions.

D. Attack Results With Dynamic Charging Locations

In this subsection, the dynamic charging locations vary with the energy consumption rates of all sensors. Specifically, we assign a weight to each sensor based on its energy demand, giving higher weights to sensors that require more energy. We randomly set the distribution of the sensor energy consumption rate 100 times, resulting in 100 different charging locations by adapting the charging scheme in [41]. We repeat EMIT attack under 100 scenarios with different charging locations, without given the exact charging location nor the energy consumption rate of each sensor. For each experiment iteration, we record the attack performance brought by the placed Coca-Cola can, and all experimental results are the average values of 100 attack instances.

Received power: Fig. 15(a) illustrates that the power received by the target sensor under attack is affected under different sensor sets. For example, when there are 2 sensors, the received power under attack is reduced by 0.25 mW. Similarly, the



(a) Received power. (b) Charging duration. (c) Success rate.

Fig. 15. Attack results with dynamic charging locations.

(a) Indoor. (b) Outdoor. (c) Urban. (d) Rural. (e) Attack success rate.

Fig. 16. Attack in different environments.

received power under attack is reduced by 0.15 mW when there are 6 sensors. The results verify that our EMIT attack can adapt to different sensor distributions, with dynamic charging locations.

Charging duration: From Fig. 15(b), the charging duration under attack is increased by an average of 15.49%, regardless of sensor distributions and charging locations. This shows our EMIT attack is destructive to the charging process in WRSNs with dynamic charging locations.

Attack success rate: Although the randomness in sensor distribution and the energy consumption rate brings slight fluctuations in success rate, as shown in Fig. 15(c), it remains consistently above 70%, validating that EMIT is robust to the dynamic charging locations. Moreover, to evaluate the adaptability of the EMIT attack across various environmental conditions, we conduct experiments in indoor, outdoor, urban, and rural environments. We fix the number of sensors at 2, randomly vary the charging location 100 times, and record the success rate of our EMIT attack. Fig. 16(a) to (d) show the experimental scenarios, and Fig. 16(e) presents the results. It can be seen that the attack success rate exceeds 70% in all tested environments.

VII. Attacks on a Real-World WRSN

To evaluate the effectiveness of our EMIT attack in real-world applications, we build a WRSN on the campus of a university. In this WRSN, 10 sensors with a battery capacity of 50 J are deployed at various Points of Interest (PoIs), including teaching buildings, roadsides, gardens, and sports fields. Each sensor is responsible to monitor various environmental information such as temperature, humidity, and light intensity.

Our real WRSN experiment lasts for 66 days. Excluding 6 days of rain, there are a total of 30 days of experiments without any attack, while the other 30 days are subject to the EMIT attack. In one charging cycle, an MC departs from our laboratory with full energy, then it moves along a charging path to replenish surrounding sensors at each PoI. According to the received power of each sensor, we can calculate the charging utility obtained at each PoI. After completing charging tasks at all PoIs, the MC returns to the laboratory and gets a 12-hour recharge for the next charging cycle. The total length of the charging path is 2.224 km, and the moving speed of the MC is 0.5 m/s. Fig. 17 shows the overview of the deployment of our WRSN and the charging path of the MC.

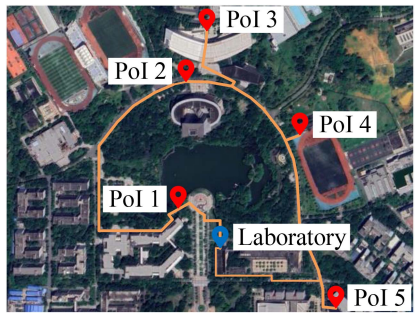
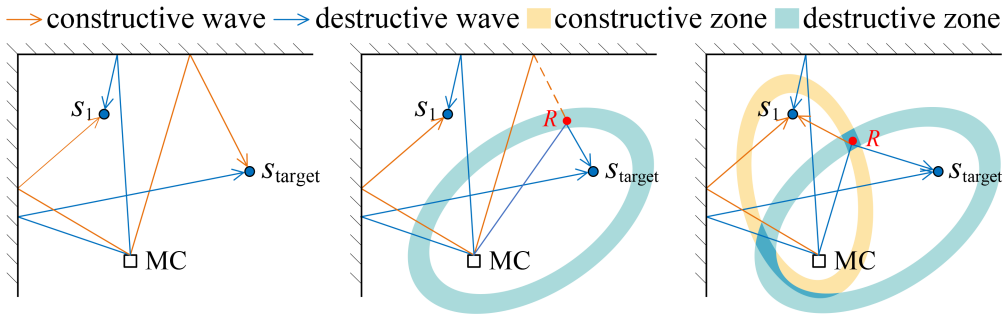


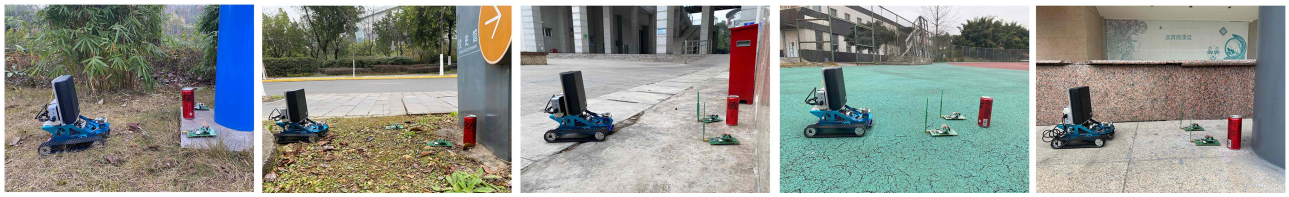
Fig. 17. Overview of WRSN on the university campus.

It is worth noting that our experiments were conducted outdoors, where the occasional passing of people, vehicles, and other objects near the PoIs will cause wave reflections. However, since the MC performs its charging tasks at each PoI for at least several hours, regardless of whether an EMIT attack is launched, the brief passing of these objects does not significantly affect the experimental results. Moreover, to prevent our sensors and reflectors from being unintentionally moved by people passing nearby, we assign personnel to inspect each PoI daily and check the positions of all experimental devices. To minimize the influence of environmental randomness on the results, all experimental results in this section are the average values over the entire experimental period.



(a) Charging scenario with multiple environmental objects. (b) Placing a reflector R. (c) Placing a reflector R to maintain the overall charging utility.

Fig. 18. An example of extending EMIT to real physical environments.



(a) PoI-1 with a metal pole near sensors. (b) PoI-2 with a metal road sign near sensors. (c) PoI-3 with a wall and a fire extinguisher box near sensors. (d) PoI-4 without any environment objects. (e) PoI-5 with an metal pillar and a wall near sensors.

Fig. 19. Attack sites of 5 PoIs.

A. Extending EMIT to Real Physical Environments

In practical applications of WRSNs, there may be different kinds of environmental objects near each PoI, including walls, poles, furniture, etc. These objects will reflect the radio wave emitted by the MC, leading to an extremely complex power distribution around the MC due to the interference among multiple waves. Intuitively, in such complex environments, mounting the EMIT attack may seem very challenging. However, is this indeed the case?

In Fig. 18(a), we give an example of a charging scenario with multiple environmental objects (i.e., walls). We can see multiple reflected waves reach the target sensor. Some of these waves constructively interfere with the wave emitted from the MC (we call this kind of wave *constructive wave*). Conversely, destructive interference occurs when other waves meet the wave from MC (we call this kind of wave *destructive wave*). Therefore, if we can block the propagation of the strongest constructive wave and generate a reflected wave that interferes destructively with the wave from MC by placing a reflector, our EMIT attack can be easily extended to complex environments.

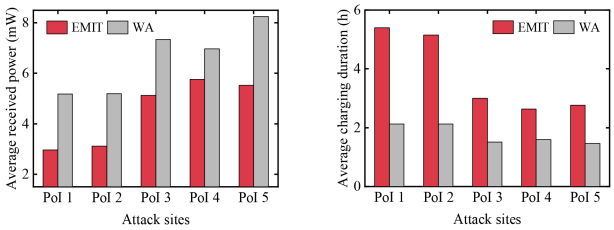
Specifically, our approach is to identify several propagation path segments from the strongest constructive wave within the innermost destructive zone formed by the MC and the target sensor. We then place the reflector on one of these segments closest to the vertex (see Fig. 18(b)). When aiming to maintain the overall charging utility to avoid detection, we find out the innermost constructive zones of other sensors, then prioritize the placement of reflector within the overlaps of these zones and the innermost destructive zone of the target sensor (see Fig. 18(c)).

B. Attack Results on Each PoI

According to the approach proposed in the above subsection, we place a Coca-Cola can at each PoI on campus to mount EMIT attack. Fig. 19 illustrates the attack sites of all 5 PoIs, demonstrating the diverse environments of these locations. Particularly, PoI-1 is situated in a garden by a lake, with a pole near the sensors; PoI-2 is located by the roadside, and the environmental object is a metal road sign; PoI-3 is a teaching building scenario consisting of a wall and a fire extinguisher box that stores hand-held extinguishers; PoI-4 represents an open sports field scenario; PoI-5 is also by a teaching building, with an iron pillar and a wall near the sensors. To verify the attack effectiveness of EMIT in these complex scenarios, we compare the average power received by each target sensor and the charging duration of each PoI before and after the EMIT attack. From the anonymous video we provided, the changes in the power received by the sensors before and after the attack are clearly observable.[1]

Received power: Fig. 20(a) shows the received power of target sensors at different PoIs. We can see that the received power of every target sensor decreases due to our EMIT attack. Notably, except for the sports field scenario without any environmental objects, the power received by the target sensors located at the other four PoIs all dropped by more than 30%, while the target sensor located in the sports field only experienced a 17.41% drop. This suggests our EMIT is more suitable for complex environments with various environmental objects. The reason behind this is our EMIT attack significantly prolongs the

[1]Anonymous demos of the proof-of-concept attacks are available at https://youtu.be/eJBWQmaRzxg



(a) Received power. (b) Charging duration.

Fig. 20. Attack results on each PoI.

TABLE II
COMPARISONS ON THE NUMBER OF SENSOR DEATHS, TOTAL CHARGING DURATION, OVERALL ENERGY CONSUMPTION AT POIS, AND THE NUMBER OF CHARGING CYCLES

	EMIT	WA
# of sensor deaths	134	2
total charging duration (hour)	430.44	291.34
overall energy consumption at PoIs (KJ)	4548.76	3146.47
# of charging cycles	23	33

charging duration required to fully charge the target sensor at each PoI, thus extending the time the MC spends completing each charging cycle.

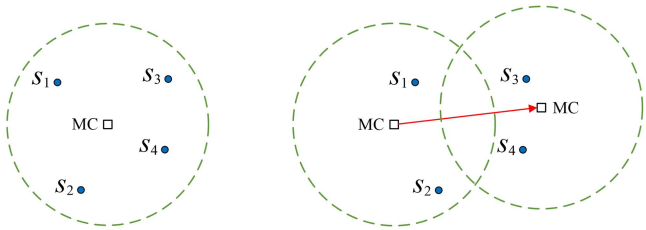
Charging duration: Fig. 20(b) depicts the impact of launching the EMIT attack on the charging duration for each PoI. It can been seen that there is a considerable increase in the charging duration of each PoI after placing the reflector, with most PoIs exceeding twice that of the scenario without the attack. Two factors contribute to this result: *(i)* the power received by the target sensor decreases due to the attack; *(ii)* the arrival time of the MC at each PoI is delayed, resulting in an increasing energy requirement for each sensor.

C. Attack Results on a Real-World WRSN

We investigate the impact of launching the EMIT attack on the performance of a real-world WRSN. Specifically, we compare the total number of sensor deaths over a 30-day period and Table II details the results. We can see that when the WRSN is not under any attack, there are only two sensor deaths, indicating that the charging scheme of the network can generally meet the energy requirement of each sensor for performing environmental monitoring tasks. However, under the EMIT attack, the number of sensor deaths reaches 134, verifying the destructiveness of our EMIT.

Furthermore, we compare the total charging duration of the MC, the overall energy consumption of the MC at all PoIs, and the number of charging cycles completed by the MC over a 30-day period. The experimental results are also presented in Table II. As shown, after launching the EMIT attack, the total charging duration of all PoIs increased from 291.34 hours to 430.44 hours, and the total energy consumption rose from 3146.47 KJ to 4548.76 KJ. Meanwhile, the number of charging cycles completed by the MC within 30 days decreased by 10.

Fig. 21. Coca-Cola cans are concealed by stickers.



(a) The origin charging task. (b) The changed charging tasks.

Fig. 22. A defense method of changing charging tasks.

The rationale behind is our EMIT attack significantly prolonged the time required to fully charge the target sensor at each PoI.

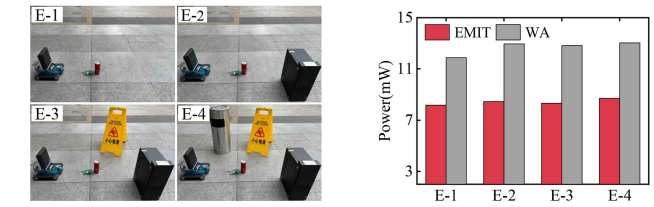
VIII. DISCUSSION

A. Potential Defense Strategies

Installing the metal detector on MC: Since the metal detector can detect the presence of metal nearby, the network maintainers can install it on the MC to detect the reflector within the charging range. However, this approach not only significantly increases the cost of the MC but also consumes its limited energy resources, reducing the number of sensors the MC can serve. Additionally, when the MC performs its charging tasks, the metal detector may generate false alarms for normal metal objects in the real-world environment, such as poles, signposts, hydrants, etc.

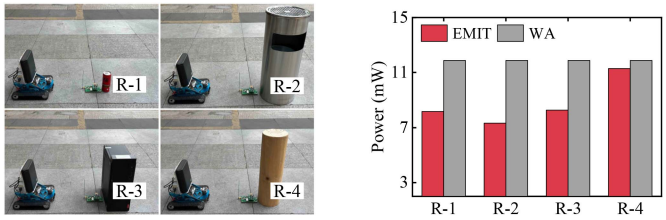
Manual inspection: The network maintainers can dispatch staff to inspect all the charging locations in the WRSNs regularly to identify suspicious objects. Nevertheless, for large-scale WRSNs with numerous sensors and broader geographical distribution, this method will bring extremely high labor costs and low inspection efficiency. The adversary can further complicate the manual identification by attaching stickers to the reflector to mimic the environment. Fig. 21 shows the Coca-Cola cans affixed with stickers in various real-world scenarios. It becomes more challenging to visually distinguish the reflector.

Changing the charging tasks: Our EMIT can robustly disrupt the charging process of the target sensor as long as MC performs the charging tasks within the charging area. Fig. 22 provides an example of a potential defense method, where MC charges sensors outside of the original charging area by changing the charging tasks. Specifically, the task of MC in Fig. 22(a) is to charge all the 4 sensors. On the other hand, the task of MC in Fig. 22(b) is to first charge sensors s_1 and s_2, and then moves to the next charging location to charge s_3 and s_4. By changing the charging task, MC may charge sensors at the location that EMIT can not destructively interfere the charging process. However,



(a) Different charging environments. (b) Received power.

Fig. 23. Attack results in dynamic charging environments.



(a) Different reflectors. (b) Received power.

Fig. 24. Attack results by using different reflectors.

the side effect of changing charging tasks for defense is that the number of charging locations and the traveling time of the MC both increase, which substantially increases the chance of sensor energy depletion in WRSNs.

Dynamically changing the charging environment: One seemingly feasible defense method is to dynamically change the charging environment, e.g., by adding or removing environmental objects at the charging site, to render the attack ineffective by leveraging the dynamic multipath effects. To verify the adaptability of our EMIT to dynamic environments, we randomly place objects such as trash can, plastic board, and computer case around the sensor. Fig. 23(a) shows four different charging environments, and Fig. 23(b) presents the power received by the sensor. As observed, although there are some variations in the attack effects under different environments, the reduction in received power from the attacks all falls within the range of 33.2% to 35.1%. The reason is that no matter how the environment changes, the reflector always generates a reflected wave to destructively interfere with the wave from the MC.

B. Can Reflectors With Different Shapes, Sizes, and Materials Be Used to Launch Attacks?

As shown in Fig. 24(a), we use various reflectors to amount EMIT attack: a Coca-Cola can (15 cm high), a trash can (60 cm high), a cuboid-shaped computer case (26.5 cm high), and a wooden stake (50 cm high). Fig. 24(b) compares the power received by the target sensor. It shows that all three metal reflectors produced significant attack effects, with delicate differences among them. This not only confirms that reflectors of various shapes can be used to launch attack but also demonstrates that smaller reflectors do not result in weaker attack effects. Additionally, we observe that the wooden stake, due to its low reflection coefficient, produced the weakest attack effect. In conclusion, we can choose different common metal objects in various environments as reflectors to launch concealed attacks.

C. How to Extend Our EMIT Attack to the Directional Charging Mode?

Directional charging is an important charging paradigm. Directional MC equipped with beamforming-capable antennas can concentrate radiated power in a specific direction, thereby achieving a longer charging range. Due to the higher power intensity of energy beam, launching a jamming attack under this mode can result in a more significant disruptive effect. However, it should be noted that the narrow beamwidth limits the available area for reflector placement. Therefore, when extending the EMIT attack to directional charging mode, we should select placement position for the reflector within the coverage area of the directional beam, based on the spatial relationship between sensors and MC. Additionally, if non-cylindrical reflectors are used, the reflector's angle should be adjusted to ensure that the reflected waves can propagate to the target sensor.

IX. Related Work

A. Reflection-Based Security Issues

Many prior arts concerning the security issues of physical reflection have been proposed in various fields, such as human identification [42], [43], object detection [44], [45], [46], and wireless communication [47]. As for human identification, the authors in [42] design a system that can distinguish different users based on the structure-borne echos reflected off the device and the user's hand. [43] leverages the information carried by the WiFi signals reflected off the human body and realize person visualization for better recognition. In the scope of object detection, [44] investigates the adversarial attacks on the DNN-based radar object detection models commonly used in autonomous driving through passive reflection. The authors in [45] deceive the camera-based perception system in autonomous driving using the reflected invisible light, while [46] focuses on mimicking a real object's reflection to launch an automotive radar spoofing attack. Regarding wireless communication, [47] is relevant to our work since it also focuses on reflecting the legitimate signals to disrupt wireless communication. They introduce an intelligent reflecting surface to manipulate the wireless channel in real-time and rapidly vary the electromagnetic propagation environment, leading to an attack on the physical layer of wireless communication systems.

Although many researchers have investigated reflection-based security issues, reflection attacks have yet to be introduced into the field of wireless charging. In this work, we focus on utilizing wave reflection to achieve a stably-working, easily-concealable, low-cost, and easy-to-deploy wireless charging attack. The goal is to reduce the power received by sensors, ultimately resulting in the death of numerous sensors.

B. Attacks on Wireless Charging

In recent years, with the breakthrough WPT technology, researchers have begun to pay attention to the security issues of wireless charging. For instance, the scheme demonstrated in [48] exploits the information leaked from the power side-channel of the wireless charging system, where the current draw of a

wireless charger is monitored when a smartphone charges and loads popular websites. The authors in [49] describe a wireless attack against the charging system for electric vehicles, which causes the charging sessions to abort by disrupting the control communication between the vehicle and the charger.

In terms of security in WRSNs, a few researchers have begun to study charging attack issues in WRSNs. In [22], the authors consider developing a Deny of Charging (DoC) attack in WRSNs for the first time, aimed to maximize the missing events by generating fake charging requests. Recently, they also extended the DoC attack scenario to Marine Wireless Rechargeable Sensor Networks [50]. [23] studies how to maximize the number of missed Point of Interests (PoIs) by manipulating a malicious MC. [24] also uses a malicious MC to send radio waves toward the charged sensor, causing destructive interference between the waves from the legitimate MC and the malicious MC, thereby preventing the sensor from obtaining adequate energy.

However, all of these attacks require extra devices (e.g., software-defined radio, malicious MCs, or sensors). As for the charging attacks towards the WRSNs, these devices are costly, and their concealment is also not satisfactory.

X. Conclusion

In this paper, we targeted the vulnerability of the wireless charging process in WRSNs. We developed a zero-cost power jamming attack, named EMIT, to disrupt the charging process. Our attack method utilized a Coca-Cola can to reflect wave from the charger to the target sensor, and ensured the reflected wave destructively interfere with the charging wave. We provided theoretical analysis to prove that EMIT attack is effective in different types of WRSNs. Extensive field experiments and real-world evaluations were conducted to verify the effectiveness of EMIT attack. The results showed that the attack success rate of EMIT in WRSNs with fixed charging locations and with dynamic charging locations are around 90% and 75%, respectively. In future work, we will focus on the security issues in 3D WRSNS. In such 3D networks, sensors are typically deployed on the poles, trees, or mounted on walls, with charging services provided by drones. Our goal is to develop a novel attack scheme aimed at preventing sensors from receiving sufficient power from the drones.

References

[1] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljacic, "Wireless power transfer via strongly coupled magnetic resonances," *Science*, vol. 317, no. 5834, pp. 83–86, 2007.

[2] Wireless chargers for medical devices: Resonant link [ol], 2023. [Online]. Available: https://www.resonant-link.com/solutions/implantable-medical-devices

[3] J. Zhang, G. Balakrishnan, S. Srinidhi, A. Bhat, S. Kumar, and C. Bettinger, "NFCapsule: An ingestible sensor pill for eosinophilic esophagitis detection based on near-field coupling," in *Proc. ACM Conf. Embedded Netw. Sensor Syst.*, 2022, pp. 75–90.

[4] X. Fan et al., "Towards flexible wireless charging for medical implants using distributed antenna system," in *Proc. ACM Annu. Int. Conf. Mobile Comput. Netw.*, 2020, pp. 1–15.

[5] T. Liu, B. Wu, W. Xu, X. Cao, J. Peng, and H. Wu, "RLC: A reinforcement learning-based charging algorithm for mobile devices," *ACM Trans. Sensor Netw.*, vol. 17, no. 4, pp. 1–23, 2021.

[6] IoT (Internet of Things) brings about smart city [ol], 2023. [Online]. Available: https://www.samsungsdi.com/column/all/detail/49.html

[7] W. Yang et al., "Precise wireless charging in complicated environments," *IEEE/ACM Trans. Netw.*, vol. 32, no. 6, pp. 4944–4959, Dec. 2024.

[8] Wireless charging market report by technology [ol], 2024. [Online]. Available: https://www.imarcgroup.com/wireless-charging-market

[9] M. Ren et al., "Understanding wireless charger networks: Concepts, current research, and future directions," *IEEE Commun. Surv. Tuts.*, vol. 27, no. 4, pp. 2247–2282, Aug. 2025.

[10] C. Lin et al., "Maximizing charging efficiency with fresnel zones," *IEEE Trans. Mobile Comput.*, vol. 23, no. 1, pp. 612–629, Jan. 2024.

[11] C. Lin et al., "Wireless charging for uncertain location nodes," *IEEE Trans. Mobile Comput.*, vol. 24, no. 8, pp. 7074–7091, Aug. 2025.

[12] J. Xue, D. Wu, J. Peng, W. Xu, and T. Liu, "Charger placement with wave interference," *IEEE Trans. Mobile Comput.*, vol. 24, no. 1, pp. 261–275, Jan. 2025.

[13] S. He, K. Hu, S. Li, L. Fu, C. Gu, and J. Chen, "A robust RF-based wireless charging system for dockless bike-sharing," *IEEE Trans. Mobile Comput.*, vol. 23, no. 3, pp. 2395–2406, Mar. 2024.

[14] Y. Sun et al., "Through-wall mobile charging: Theory, methodology, and implementation," *IEEE Trans. Mobile Comput.*, vol. 24, no. 6, pp. 4971–4986, Jun. 2025.

[15] W. Yang, C. Lin, Y. Sun, H. Dai, J. Ren, and L. Wang, "Accurate 3D wireless charging," *IEEE Trans. Mobile Comput.*, vol. 24, no. 6, pp. 4733–4746, Jun. 2025.

[16] S. Wu, H. Dai, L. Liu, L. Xu, F. Xiao, and J. Xu, "Cooperative scheduling for directional wireless charging with spatial occupation," *IEEE Trans. Mobile Comput.*, vol. 23, no. 1, pp. 286–301, Jan. 2024.

[17] W. Xu et al., "Approximation algorithms for the generalized team orienteering problem and its applications," *IEEE/ACM Trans. Netw.*, vol. 29, no. 1, pp. 176–189, Feb. 2021.

[18] T. Liu, B. Wu, S. Zhang, J. Peng, and W. Xu, "An effective multi-node charging scheme for wireless rechargeable sensor networks," in *Proc. IEEE Conf. Comput. Commun.*, 2020, pp. 2026–2035.

[19] M. Ren, D. Wu, J. Xue, W. Xu, J. Peng, and T. Liu, "Utilizing the neglected back lobe for mobile charging," in *Proc. IEEE Conf. Comput. Commun.*, 2023, pp. 1–10.

[20] T. Liu et al., "Utilizing the neglected back lobe for directional charging scheduling," *IEEE Trans. Mobile Comput.*, vol. 23, no. 6, pp. 7408–7421, Jun. 2024.

[21] H. Huang, J. Zhang, B. Wang, W. Miao, and G. Min, "Joint mobile energy replenishment and data gathering in wireless sensor networks via federated deep reinforcement learning," *IEEE Trans. Mobile Comput.*, vol. 24, no. 7, pp. 6460–6473, Jul. 2025.

[22] C. Lin, Z. Shang, W. Du, J. Ren, L. Wang, and G. Wu, "CoDoC: A novel attack for wireless rechargeable sensor networks through denial of charge," in *Proc. IEEE Conf. Comput. Commun.*, 2019, pp. 856–864.

[23] C. Lin, P. Wang, Q. Zhang, H. Wang, L. Wang, and G. Wu, "MDoC: Compromising WRSNs through denial of charge by mobile charger," in *Proc. IEEE Conf. Comput. Commun.*, 2022, pp. 1149–1158.

[24] C. Lin et al., "Are you really charging me," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst.*, 2022, pp. 724–734.

[25] D. K. Cheng et al., *Field and Wave Electromagnetics*. Noida, Uttar Pradesh, India: Pearson Education India, 1989.

[26] T. Liu et al., "Concurrent charging with wave interference for multiple chargers," *IEEE/ACM Trans. Netw.*, vol. 32, no. 3, pp. 2525–2538, Jun. 2024.

[27] Y. Ma, D. Wu, J. Gao, W. Sun, J. Yang, and T. Liu, "Dynamic power distribution controlling for directional chargers," in *Proc. IEEE Conf. Comput. Commun.*, 2024, pp. 1–10.

[28] J. Gao, D. Wu, L. Zhang, J. Li, J. Peng, and T. Liu, "Utilizing multipath effects for mobile charging," *IEEE Trans. Mobile Comput.*, vol. 24, no. 9, pp. 8668–8682, Sep. 2025.

[29] W. Yang et al., "Robust wireless rechargeable sensor networks," *IEEE/ACM Trans. Netw.*, vol. 31, no. 3, pp. 949–964, Jun. 2023.

[30] T. Liu, B. Wu, H. Wu, and J. Peng, "Low-cost collaborative mobile charging for large-scale wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 8, pp. 2213–2227, Aug. 2017.

[31] P. Yang et al., "MORE: Multi-node mobile charging scheduling for deadline constraints," *ACM Trans. Sensor Netw.*, vol. 17, no. 1, pp. 1–21, 2020.

[32] T. Koppel, A. Shishkin, H. Haldre, N. Toropovs, I. Vilcane, and P. Tint, "Reflection and transmission properties of common construction materials at 2.4 GHz frequency," *Energy Procedia*, vol. 113, pp. 158–165, 2017.

[33] M. Kanda, "The effects of resistive loading of "TE," horns," *IEEE Trans. Electromagn. Compat.*, vol. EMC-24, no. 2, pp. 245–255, May 1982.

[34] Powercast, (n.d.), 2025. [Online]. Available: https://www.powercastco.com/
[35] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Secur. Privacy*, 2005, pp. 49–63.
[36] T. Bonaci, L. Bushnell, and R. Poovendran, "Node capture attacks in wireless sensor networks: A system theoretic approach," in *Proc. IEEE Conf. Decis. Control*, 2010, pp. 6765–6772.
[37] M. Karakaya and H. Qi, "Collaborative localization in visual sensor networks," *ACM Trans. Sensor Netw.*, vol. 10, no. 2, pp. 1–24, 2014.
[38] W. You et al., "Practical charger placement scheme for wireless rechargeable sensor networks with obstacles," *ACM Trans. Sensor Netw.*, vol. 20, no. 1, pp. 1–23, 2024.
[39] Y. Sun et al., "Trading off charging and sensing for stochastic events monitoring in WRSNs," *IEEE/ACM Trans. Netw.*, vol. 30, no. 2, pp. 557–571, Apr. 2022.
[40] T. Wu, P. Yang, H. Dai, W. Xu, and M. Xu, "Charging oriented sensor placement and flexible scheduling in rechargeable WSNs," in *Proc. IEEE Conf. Comput. Commun.*, 2019, pp. 73–81.
[41] T. Wu, P. Yang, H. Dai, W. Xu, and M. Xu, "Collaborated tasks-driven mobile charging and scheduling: A near optimal result," in *Proc. IEEE Conf. Comput. Commun.*, 2019, pp. 1810–1818.
[42] Y. Yang, Y. Wang, Y. Chen, and C. Wang, "EchoLock: Towards low-effort mobile user identification leveraging structure-borne echos," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, 2020, pp. 772–783.
[43] Y. Ren, Y. Wang, S. Tan, Y. Chen, and J. Yang, "Person re-identification in 3D space: A WiFi vision-based approach," in *Proc. USENIX Conf. Secur. Symp.*, 2023, pp. 5217–5234.
[44] Y. Zhu et al., "TileMask: A passive-reflection-based attack against mmWave radar object detection in autonomous driving," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2023, pp. 1317–1331.
[45] W. Wang, Y. Yao, X. Liu, X. Li, P. Hao, and T. Zhu, "I can see the light: Attacks on autonomous vehicles using invisible lights," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2021, pp. 1930–1944.
[46] R. R. Vennam et al., "mmSpoof: Resilient spoofing of automotive millimeter-wave radars using reflect array," in *Proc. IEEE Symp. Secur. Privacy*, 2023, pp. 1807–1821.
[47] P. Staat, H. Elders-Boll, M. Heinrichs, C. Zenger, and C. Paar, "Mirror, mirror on the wall: Wireless environment reconfiguration attacks based on fast software-controlled surfaces," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, 2022, pp. 208–221.
[48] A. S. La Cour, K. K. Afridi, and G. E. Suh, "Wireless charging power side-channel attacks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2021, pp. 651–665.
[49] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Brokenwire: Wireless disruption of CCS electric vehicle charging," 2022, *arXiv:2202.02104*.
[50] Q. Wang, C. Lin, H. Dai, M. S. Obaidat, K.-F. Hsiao, and X. Fan, "Compromising rechargeable sensor networks in marine environment," *IEEE Trans. Mobile Comput.*, vol. 24, no. 8, pp. 6961–6977, Aug. 2025.

Tang Liu (Member, IEEE) received the BS degree in computer science from the University of Electronic and Science of China, China, in 2003, and the MS and PhD degrees in computer science from Sichuan University, in 2009 and 2015, respectively. Since 2003, he has been with the College of Computer Science, Sichuan Normal University, where he is currently a professor. He has authored more than 60 scientific papers in several conferences and journals, including INFOCOM, ICDCS, IPDPS, *IEEE Transactions on Mobile Computing*, *IEEE/ACM Transactions on Networking*, *IEEE Transactions on Wireless Communications*, *ACM Transactions on Sensor Networks*, and *IEEE Transactions on Communications*. His research interests include wireless charging, Internet of Things, and wireless sensor networks.

Jing Gao received the BS degree in energy chemical engineering from the Beijing Institute of Technology, Beijing, China, in 2020. She is currently working toward the MS degree with the College of Computer Science, Sichuan Normal University. Her research interest is wireless charging.

Yuan Yin received the BS degree in computer science from Sichuan Normal University, Chengdu, China, in 2023. He is currently working toward the MS degree with the College of Computer Science, Sichuan Normal University. His research interests include wireless charging and wireless sensor networks.

Die Wu (Member, IEEE) received the BS degree in information security and the PhD degree in computer architecture from the Electronic Science and Technology of China, in 2011 and 2018, respectively. From 2016 to 2017, he was with Nanyang Technological University, Singapore, as a visiting PhD Student. He is currently an assistant professor with the College of Computer Science, Sichuan Normal University, Chengdu, China. His research interests include RFID systems, wireless networks, and pervasive computing.

Jian Peng (Member, IEEE) received the BA and PhD degrees from the University of Electronic Science and Technology of China (UESTC), in 1992 and 2004, respectively. He is a professor with the College of Computer Science, Sichuan University. His recent research interests include wireless sensor networks, Big Data, and cloud computing.

Wenzheng Xu (Member, IEEE) received the BSc, ME, and PhD degrees in computer science from Sun Yat-Sen University, Guangzhou, China, in 2008, 2010, and 2015, respectively. He is currently an associate professor with Sichuan University. He was a visitor with the Australian National University and Chinese University of Hong Kong. His research interests include Internet of Things, UAV networking, mobile computing, approximation algorithms, combinatorial optimization, online social networks, and graph theory.

Baijun Wu received the BS and MS degrees in computer science from Sichuan University, China, in 2008 and 2011, respectively, and the PhD degree in computer science from the University of Louisiana at Lafayette, in 2020. He was a software engineer with Ericsson from 2011 to 2012, and he worked for TPLINK from 2012 to 2013. His current research interests include wireless sensor networks, and mobile crowdsouring.

Yazhou Tu (Member, IEEE) received the PhD degree in computer science from the University of Louisiana at Lafayette. He is currently an assistant professor with the Computer Science and Software Engineering Department, Auburn University. His research interests include cyber-physical security, side channels, sensing security, and embedded systems. He received the Distinguished Paper Award from IEEE S&P 2024.