information

MDPI

Article

Communication and Sensing: Wireless PHY-Layer Threats to Security and Privacy for IoT Systems and Possible Countermeasures

Renato Lo Cigno [1,*,†], Francesco Gringoli [1,†], Stefania Bartoletti [2,†], Marco Cominelli [3,†], Lorenzo Ghiro [1,†] and Samuele Zanini [2,4,†]

[1] Dipartimento di Ingegneria dell'Informazione (DII), University of Brescia and Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT), 25124 Brescia, Italy; francesco.gringoli@unibs.it (F.G.); lorenzo.ghiro@unibs.it (L.G.)
[2] Dipartimento di Ingegneria Elettronica (DIE), University of Rome Tor Vergata and CNIT, 00133 Roma, Italy; stefania.bartoletti@uniroma2.it (S.B.); samuele.zanini@imtlucca.it (S.Z.)
[3] Dipartimento di Elettronica, Informazione e Bioingegnaria (DEIB), Politecnico di Milano, 20133 Milano, Italy; marco.cominelli@polimi.it
[4] IMT School for Advanced Studies Lucca, 55100 Lucca, Italy
* Correspondence: renato.locigno@unibs.it
† These authors contributed equally to this work.

Abstract: Recent advances in signal processing and AI-based inference enable the exploitation of wireless communication signals to collect information on devices, people, actions, and the environment in general, i.e., to perform Integrated Sensing And Communication (ISAC). This possibility offers exciting opportunities for Internet of Things (IoT) systems, but it also introduces unprecedented threats to the security and privacy of data, devices, and systems. In fact, ISAC operates in the wireless PHY and Medium Access Control (MAC) layers, where it is impossible to protect information with standard encryption techniques or with any other purely digital methodologies. The goals of this paper are threefold. First, it analyzes the threats to security and privacy posed by ISAC and how they intertwine in the wireless PHY layer within the framework of IoT and distributed pervasive communication systems in general. Secondly, it presents and discusses possible countermeasures to protect users' security and privacy. Thirdly, it introduces an architectural proposal, discussing the available choices and tradeoffs to implement such countermeasures, as well as solutions and protocols to preserve the potential benefits of ISAC while ensuring data protection and users' privacy. The outcome and contribution of the paper is a systematic argumentation on wireless PHY-layer privacy and security threats and their relation with ISAC, framing the boundaries that research and innovation in this area should respect to avoid jeopardizing people's rights.

Keywords: wireless communications; wireless PHY-layer security; integrated sensing and communication; privacy protection; channel state information

Academic Editors: Xu Zheng, Zhuojun Duan and Yingjie Wang

Received: 4 December 2024
Revised: 23 December 2024
Accepted: 2 January 2025
Published: 7 January 2025

Citation: Lo Cigno, R.; Gringoli, F.; Bartoletti, S.; Cominelli, M.; Ghiro, L.; Zanini, S. Communication and Sensing: Wireless PHY-Layer Threats to Security and Privacy for IoT Systems and Possible Countermeasures. *Information* **2025**, *16*, 31. https://doi.org/10.3390/info16010031

Correction Statement: This article has been republished with a minor change. The change does not affect the scientific content of the article and further details are available within the backmatter of the website version of this article.

1. Introduction

The Internet of Things (IoT) is a multifaceted reality that has grown to cover scenarios not included in its scope when the term was introduced in the late 1990s. Today, IoT scenarios span from industrial plants to smart mobility, while access technologies supporting the IoT range from cellular networks (4G/5G and beyond) to Wi-Fi, including also LoRa, LoRAWAN, and many other standard and proprietary communication technologies.

Privacy and security are fundamental for the IoT, just like for other highly sensitive communication services such as the banking system or the medical sector. Actually, the

medical sector overlaps the IoT, as wearable medical devices empower e-health systems, while smart living spaces allow elderly people to stay active and independent for more years. Privacy and security are so much needed in the IoT that surveys, special issues, and tutorials on these subjects can be counted by the hundreds, while specific contributions in academic venues are approaching one million, making the selection of relevant publications an impossible task.

The IoT, however, differs in many aspects from other, more focused computing and communication contexts, and its holistic security and privacy (S&P from now on) guarantees require novel approaches and pose specific challenges that pertain to the unique mixture of devices and elements that compose the IoT environment. As a telltale sign of this difficulty, we can mention a recent survey [1] citing more than 130 references and highlighting the fragmentation of research and solutions for IoT S&P. The authors provided a thorough classification, focusing on intrusion attacks and detection systems from the network level up to the data-integration/application level. Below the networking level, the physical (PHY) and Medium Access Control (MAC) layers are collectively called the *perception layer*, and the only threat considered is jamming. From a telecommunications and distributed systems point of view, this is very reductive. In fact, jamming cannot be considered an attack on S&P because it is manifest, and the most destructive effect is the denial of service, with nothing more subtle or dangerous like data leakage or information dilution occurring.

Although the perspective reported above is possibly the most common in the community, recent results contrast it and show that there are many more sophisticated threats than jamming in the wireless PHY and MAC layers. In particular, this work addresses one novel, emerging topic in S&P that affects all wireless networks, including the IoT: wireless PHY-layer security attacks derived from Integrated Sensing And Communication (ISAC).

Traditionally, S&P focuses on protecting data by encrypting information during transmission, processing, and storage, shielding it from illegitimate access. This kind of protection can be applied successfully to data in the digital domain but cannot be applied to information otherwise embedded in the analog signals modulated to carry the data during transmission. In wireless transmissions, these signals are freely accessible to anybody, and it is challenging to protect them from attackers overhearing the transmission. Indeed, in the state of the art, not even quantum cryptography can be applied to analog transmissions; hence, alternative solutions must be sought.

Attacks in the wireless PHY layer can have different targets, from device fingerprinting [2] to localization spoofing and deception [3,4]. In this work, in contrast to other works such as [5], we do not consider attacks whose target is to break cryptographic channels in the wireless PHY layer. Indeed, the cryptographic security of channels of most wireless communication technologies—from cellular networks to 802.11 and 802.15 standards—are implemented, from an architectural perspective, within or above the MAC protocols because the PHY and MAC headers and control information need to be in clear mode for channel control and management, so we do not consider these attacks as *PHY-layer* threats. Instead, we deal with emerging techniques that exploit analog properties of the signals to hamper some functionality or illegitimately collect information on people. One simple example is tampering with anchor positions in active device localization. The attack does not require the breaking of any cryptographic protocol, but its success means that the estimated position of one or more devices is wrong, jeopardizing the services that rely on position and, in extreme, cases the users' safety, too—for, instance when the position of a person is estimated to be safe when it is actually not.

As wireless PHY-layer security attacks, ISAC harnesses analog physical properties of electromagnetic signals. ISAC exploits the same signals used for the transmission of

digital information to perform some measurements(or sensing) on the environment [6–12]. It can address many different measures; however, its intended use has a keen bias toward humans, clearly hampering privacy if performed without authorization. ISAC can be split into many different technologies and application domains. The first dichotomy in this field is the separation between *device* sensing and *environment* sensing. In the former, the signals are used to derive some properties of the sensed devices, for example, the identity and location of a device. The sensed information can then legitimately be used to reinforce authentication or to illegitimately track the device holder, jeopardizing her/his privacy. In the latter case, the electromagnetic signals are used to capture some properties of the propagation environment; for example, the ambient state can be captured in terms of the presence of people in a room, also revealing what the people in the room are doing. Sometimes, device and environment sensing overlap, as in the case of device fingerprinting, while in other cases, they do not. The common tract is that S&P threats are rooted in the analog domain, so traditional protection techniques based on cryptography cannot be used.

Starting from the state of the art with respect to S&P threats arising from the analog nature of wireless transmissions, the goal of this paper is to propose possible countermeasures. The community has just started to explore some of them, but a systematic analysis such as the one proposed in this paper is still missing. We discuss the literature extensively in Section 2, but we do not claim to offer the community a complete survey on the topic. On the one hand, the topic is too vast, and on the other hand, there are already valid surveys on some specific facets, such as [13–15]. In [13], the authors examined physical-layer security in smart mobile IoT networks, emphasizing the difficulty of applying universal solutions due to diverse device types and configurations. They noted that traditional cryptographic methods can introduce vulnerabilities while increasing the computational load, shortening battery life. In [14], IoT security was reviewed within a three-layer architecture, covering key concepts, current security demands, and recent developments, in addition to identifying open issues and suggesting directions for future research. Here, wireless PHY-layer security is acknowledged, but it is not the primary focus. The authors of [15] discussed how 6G systems can bring both greater context-awareness and further security challenges thanks to enhanced sensing and embedded intelligence at the wireless edge.

The contribution of this paper lies in the holistic perspective on the subject, highlighting the peculiar, novel characteristics of S&P threats at the wireless PHY layer—both intrinsic and those derived from ISAC. Compared with traditional S&P threats in the digital domain, these threats require different protection approaches. This paper further explores how to balance ISAC with privacy and security aspects, focusing on passive and active sensing attacks. Solutions for both categories are discussed, mainly considering *signal obfuscation techniques* and the use of *Reflective Intelligent Surfaces (RISs)*. These solutions are described and discussed, highlighting their potential and the limitations of their practical implementation. The key problems to be solved are discussed, as well as the properties that anti-tampering methods must deploy to be effective; furthermore, the contours of the research area are delineated, and the relationships of security with privacy (for instance, in localization and tracking) are disclosed. Before the final discussion, Section 3 analyzes which countermeasures are viable and which are not suitable for the problem, outlining future research directions.

2. State of the Art

This section analyzes the most recent research works dealing with S&P in the wireless PHY layer. The discussion focuses on known attacks carried out by manipulating electromagnetic signals. We report only foundational papers and recent achievements, trying to give a concise yet precise view of such achievements.

2.1. Security Threats in the Wireless PHY Layer

Jamming and eavesdropping [5,16,17] are the most studied threats in the PHY layer in wireless networks, but they are not the only ones and, above all, not the most treacherous. Jamming is a plain, open attack, while appropriate cryptographic techniques can generally defuse eavesdropping. Indeed, several other attacks must be considered in the context of wireless communication, including IoT and sensing applications [4,18–22]. Traditional attacks and threats also include wormhole attacks, Man-In-The-Middle (MITM) attacks, and spoofing. For instance, in mission-critical applications such as autonomous driving, if an attacker can tamper with positioning measurements through physical manipulations, then the outcome can pose severe safety hazards.

Figure 1 depicts some known attacks in the PHY layer in wireless communications, whose goals are described below.

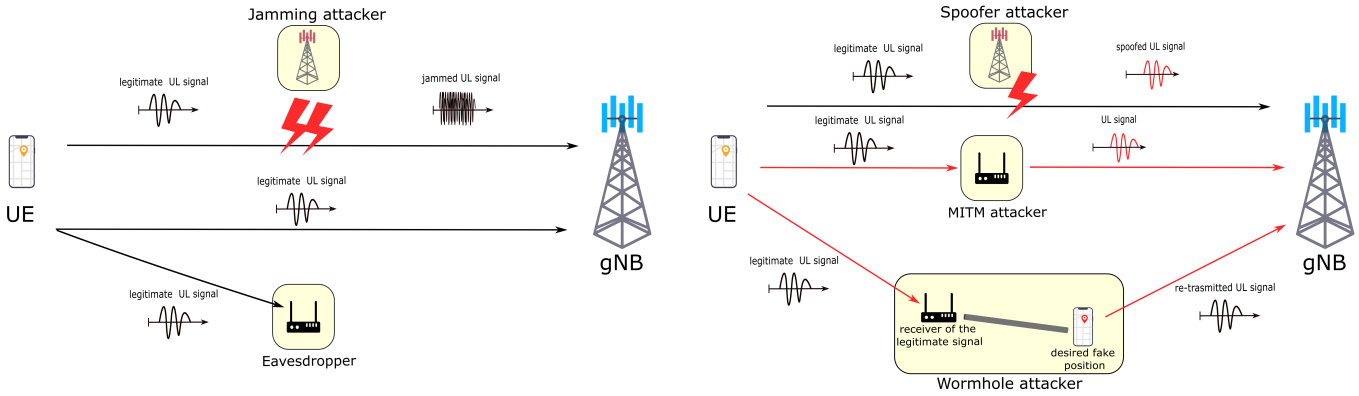

Figure 1. Visual illustration of some threats at the PHY layer in the context of 5G networks. (**a**) Jamming and eavesdropping attacks; (**b**) Spoofing, MITM, and wormhole attacks.

- **Eavesdropping:** The malicious entity aims to intercept confidential information transmitted over the air between the transmitter and receiver, resulting in privacy breaches.
- **Jamming:** The goal is to disrupt over-the-air communication, i.e., reducing the SNR of legitimate transmissions by transmitting noise/signal that prevents the receiver from decoding the data, thereby causing a denial of service. Jamming and eavesdropping can be combined to achieve additional goals. For instance, Jamming can force devices to change their transmitter power to maintain a given Signal-to-Interference plus Noise Ratio (SINR), allowing properly placed eavesdroppers to collect information on the transmitter position without the need to decrypt the signal.
- **Man-in-the-middle attacks**: A MITM attack in the PHY layer is based on the interception of wireless signals and the interposition of a device that mimics the other end of the communication for both parties. These attacks require access to higher communication layers and modify the transmitted information to operate on the victim's data. The attacker needs to operate in both directions of the communication, establishing a double fake connection: one for the victim device and the other one with the base station in a cellular context (an AP in a Wi-Fi context or in general with the "other" device).
- **Wormhole attacks:** A wormhole attack is based on the manipulation of signals to create a rogue tunnel, i.e., a communication path that is not the natural one between the two devices, instead forcing the electromagnetic signal to be routed through a different physical path but without the requirement to fully demodulate and re-modulate the digital content of the signals. The attacker does not manipulate the transmitted data but only routes it through another path, possibly providing some specifically deceptive

information, such as the propagation time, or tampering with the analog signal or, at most, the MAC layer headers to reach their goals.

- **Spoofing:** The attacker manipulates some properties of the signals or of the propagation environment to deceive the victim in some way. A classic example is GPS spoofing, in which the attacker tampers with the GPS signal to change the target's estimated location. Another example is MAC address de-anonymization, which is achieved by smartly using the information contained in standard Wi-Fi probes, whose outcome is the violation of users' privacy and security by allowing tracking and more.

In the context of the IoT, the authors of [18] provided an in-depth analysis of PHY threats in 5G networks, considering the different capabilities of attackers, such as various types of jamming based on prior knowledge of legitimate communication by the malicious node. They also suggested countermeasures against passive eavesdropping based on the characteristics of 5G IoT networks, such as massive Multiple Input Multiple Output (MIMO). Jamming and eavesdropping can lead to potential denial-of-service and privacy breaches, while other threats may cause additional problems related to applications and specific use cases. Other studies [4,22–24] have examined the impacts of attacks and the corresponding mitigation strategies for localization services specifically within 5G systems. These findings can also be applied to sensing scenarios in IoT and ISAC contexts. In these attacks, the vulnerabilities of the wireless PHY layer are exploited to tamper with the measurements, leading to erroneous position estimation outcomes.

Regarding attacks specific to the wireless PHY layer and typical of the IoT environment, let us consider de-anonymization and wormhole attacks on sensitive devices in more detail. As clearly described in [25,26], the key component of such attacks is a Wi-Fi probe, which is broadcast by devices looking for a network to connect. The authors of [25] explicitly explained how to achieve de-anonymization using anonymous Wi-Fi probes of devices that actively search for network connectivity. The goal of [26] was (apparently) legitimate, but it is not difficult to imagine how the same technique can be used for attacks. The key idea is that collecting large amounts of broadcast packets makes it possible to recover the position of and additional information on a specific device and, obviously, on the person who carries it.

In contrast, device-specific wormhole attacks seem to be a real IoT doom, as they target the typical small, cheap devices that are the backbone of the IoT. The work reported in [27] addressed the archetype of security threats: stealing money. The authors showed that in wireless-based money exchange, an attacker who properly places a device acting as a wormhole may deceive a merchant, ultimately performing illicit transactions using the victim's plastic or virtual (i.e., a smartphone app) money. The authors of [28,29], instead, used a similar technique to demonstrate wormhole attacks on another staple of our perceived security: cars. In [28], the authors used relays (a form of the wormhole) to show that passive remote entry and start systems can be compromised directly in the wireless PHY layer, without the need for sophisticated processing capabilities. Cars can be opened, started, and even partially operated remotely, posing threats not only of theft but also threats to the safety of the passengers. The authors of [29] presented a wide review of possible attacks on connected vehicles in the most widespread architectures. The goal of the work was broader, but wireless PHY-layer threats and attacks were also considered.

Finally, Anliker et al. [30] presented an attack on Ultra Wide Band (UWB) ranging systems, which are, in general, considered secure, in addition to discussing possible countermeasures against various attacks, including wormholes. An attack can be performed by someone controlling the wireless channel, i.e., with the ability to intercept signals and inject manipulated signals in the channel, but without any need to know the secret keys of the attacked victims; thus, such an attack cannot be countered with standard cryptography.

2.2. Integrated Sensing and Communication

More than ten years ago, pioneering work reported in [6,7,31] suggested that communication signals can also be used to detect physical objects not connected to the network. Indeed, any wireless signal can potentially become a "passive radar" signal that can be used to opportunistically *sense* the surrounding environment by analyzing the characteristics of the electromagnetic signal. This is particularly true for wide-band communication signals, where the Channel State Information (CSI) provides a detailed picture of the multipath in the environment enabling, for instance, the localization of nodes and objects or the recognition of particular human motions and gestures. Moreover, these works revealed that sub-6 GHz frequencies might provide a good tradeoff between sensing accuracy and the ability to operate through walls and in other complex scenarios without a line of sight.

Over the last decade, researchers have proposed several different ISAC systems to improve existing sensing applications or to address completely new problems. For example, in the case of localization of target devices, the CSI can be exploited to refine other types of measurements, such as Direction of Arrival (DoA) or Time of Arrival (ToA) [32]. Alternatively, deep learning methods have been shown to enhance localization based on round-trip time and RSSI measurements [33]. Otherwise, if other localization methods are unfeasible, deep learning can be used to localize the target devices following a fingerprinting approach [8,10].

However, some of the most interesting applications of ISAC systems involve estimating the position and motion of *passive* objects, i.e., objects that are *not connected devices*. This can be achieved by analyzing the variations in the physical channel captured by the CSI, as shown in Figure 2. Using this approach, many different applications have been proposed in the literature, from fall detection [34] to localization [35] and fine-grained gesture [36] and activity [37] recognition, notably all regarding *humans*. Figure 2 highlights a critical issue of all these approaches: the information about propagation resides at the wireless PHY level and is not secured. This implies that *any* device can collect raw CSI data, so an eavesdropper can opportunistically use the frames transmitted by other (legitimate) devices to perform the analysis described in all the cited research works.

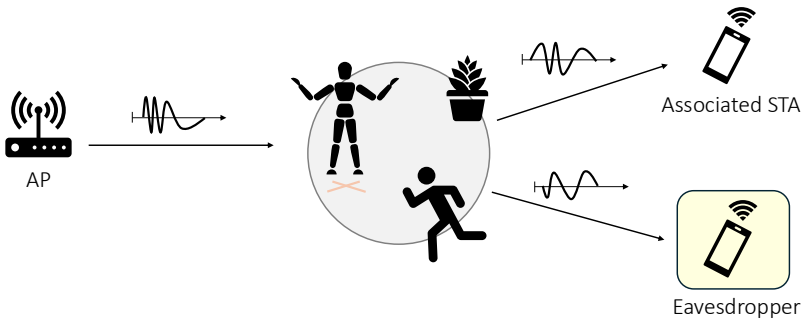

Figure 2. People and objects directly affect the propagation of wireless signals. Encryption of the data payload cannot prevent an eavesdropper from monitoring the environment using the electromagnetic properties of the transmitted signals.

Today, ISAC has become one of the key technologies driving the development of the next generation of wireless systems. Wi-Fi seems to have an edge in integrating sensing and communication functionalities, and most ongoing investigations focus on this technology. In fact, work on the standardization of ISAC procedures for Wi-Fi has already started through the IEEE 802.11bf task force [38]. Furthermore, the European Telecommunication Standards Institute (ETSI) revealed that ISAC will be one of the key scenarios for upcoming 6G cellular networks [39]. However, despite efforts to standardize sensing and communication operations, it is still unclear whether privacy-aware sensing will be available in future

wireless technologies [11]. To this end, the ISAC paradigm could also be combined with other novel technologies, such as reconfigurable meta-surfaces [9], to provide ubiquitous localization services in smart radio environments with increased accuracy, reliability, and privacy. Despite all the research done so far, the research community has yet to explore the combined effects of these technologies in depth.

3. Countermeasures

Section 2 gives an overview of the threats in the wireless PHY and MAC layer that, also utilizing analog signals and information, prevent the use of standard techniques to ensure S&P. Here, we discuss possible countermeasures against these attacks to achieve robustness and secure communication for IoT and ISAC applications.

3.1. Security Threats in the PHY Layer

Some possible solutions addressing eavesdropping and jamming involve techniques based on the spread spectrum, such as Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS) [16,40]. In the first technique, the signal is multiplied by a pseudo-noise digital signal known only to the transmitter and receiver. This way, the legitimate user can retrieve the original data by knowing the noise sequence. The latter technique involves rapidly changing the carrier frequency channel using a common algorithm known to both legitimate communicators. Both techniques have been studied and used for military communications and are, in general, best suited for sporadic, low-bit-rate communications, making it difficult to adapt them to modern, multi-Gbit/s communications. In addition to these two well-known techniques, ref. [18] suggests leveraging massive MIMO technologies to mitigate the threat of passive eavesdropping. This approach makes the attack task more difficult, since the malicious entity needs to be very close to the victim, with a similar channel condition, to gather useful information. However, these countermeasures have yet to be proven, especially because massive MIMO technologies are still in their infancy. We stress, again, that jamming is a very invasive attack and, as such, inherently less dangerous than others, as it is very simple to detect it and eventually take countermeasures, as the attacker can be easily localized.

Simple countermeasures against MITM attacks are available. They include mutual authentication between the entities involved in the communication using certificate authorities and cryptography to ensure the integrity of the communication [20]. These are important techniques, but they address attacks in the digital domain, while those in the analog domain, such as wormhole attacks, remain unscathed.

One way to counter wormhole attacks on wireless networks is by leveraging the statistical variations of the channel behavior, which are symptoms of an ongoing wormhole attack. For instance, one can exploit the additional time the malicious node's rogue path adds to the communication. Detection can rely on Time-of-Flight (ToF) computation, either in a single direction or a round trip, compared against a pre-computed threshold. The maximum acceptable value depends on the specific scenario, similar to the evaluation of the Round-Trip Time (RTT) in [19], but considering only the wireless hops of the communication; otherwise, the tiny increase due to the wormhole is lost in the length of the end-to-end transmission. A more sophisticated approach can be based on continuous runtime monitoring and estimation of the ToF. This estimation can use traditional stochastic analysis techniques, computing the probability of the ToF being subject to sudden changes (when the attacker intercepts the signal), or simply to statistics that cannot be met with direct communications. Alternative and more advanced techniques based on AI/ML can achieve the same result. The work reported in [41] explicitly introduced the concept of Physical-layer Message Integrity (PMI), which ensures that the physical-layer characteristics of a wireless

message, such as the time of arrival, signal strength, and angle of arrival, remain unaltered. The authors specifically focused on Message Temporal Integrity (MTI), addressing attacks that delay or advance message transmission. These attacks can disrupt time-sensitive applications like time synchronization and distance measurements. To counter such threats, they proposed a protocol leveraging specialized encoding, modulation, and techniques to detect and mitigate MTI attacks.

Standardization bodies are developing specifications to standardize countermeasures against wireless PHY threats, but these may worsen the problem instead of solving it due to the possibilities opened by modern AI/ML algorithms in analog signal analysis. In the 5G documentation, 3GPP defined the generation of reference signals (i.e., periodic transmissions of known data at both the receiver and transmitter) to be used by communication-enhancement technologies as channel estimation and timing/angle measurements. If such symbols are constant, then ISAC becomes possible for anyone, so pseudo-random techniques are under study. The transmitted symbols are based on pseudo-random sequences where the seed depends on high-level parameters of the application [42]. For example, the Reference Signals (RSs) for positioning purposes—Sounding RS (SRS) and Positioning RS (PRS)—can be derived from parameters of the trusted entities involved, and they are exchanged securely, similarly to the discussion in Section 4. This way, an external third party cannot forge these signals and cannot perform a spoofing attack to disrupt the positioning estimation of the user's location. In fact, the standardization bodies do not provide any evidence that these signals cannot be exploited to breach S&P in the analog domain. The focus seems to be more on ensuring that positioning on the network side remains robust enough for applications rather than for the protection of users S&P. Sometimes, these two goals overlap, but they may also be independent or even contrast one another, e.g., when the user does not fully trust the network.

Countermeasures against attacks in the wireless PHY layer are essential for secure and efficient communications and to build solid trust of users in the IoT. People must be guaranteed that their smart space can safeguard their S&P, independently of whether users carry IoT devices with them or not, as we discuss in the following subsection.

3.2. Integrated Sensing and Communication

Securing ISAC to prevent passive eavesdroppers from sensing what happens in the environment is not an easy task. Unlike traditional cryptography techniques used to encrypt data payloads, information about how communication signals propagate in an environment is readily available to *all* the devices in an area (see Figure 2).

Early works proposed using special devices that act as dynamic reflectors to *obfuscate* the real electromagnetic properties of the environment and disrupt eavesdroppers' attempts to perform sensing [43]. By dynamically changing the reflective properties of some objects, the electromagnetic characteristics of the environment are also modified, possibly defusing any sensing technique based on channel fingerprinting. However, the *obfuscators* proposed in such works require expensive hardware and have limited reconfigurability. Moreover, the privacy performance (i.e., the ability to disrupt illegitimate sensing) highly depends on the relative positions of transmitters, eavesdroppers, and obfuscators. The work reported in [43] fostered additional research in recent years, and the evolution of Reflective Intelligent Surfaces (RISs) might make such approaches more appealing.

It must be noted that, given the current state of the art, sensing-based fingerprinting requires ISAC signals to be transmitted by devices that are in a fixed position. The actual position is not important, as long as the transmitter remains fixed in a given location. In fact, signal analysis does not depend on the transmitter coordinates; still, any movement of the

transmitter would alter its radiation properties, preventing any form of pattern recognition, including fingerprinting. Thus, two lines of research have emerged:

1. Obfuscating signals directly at the transmitter;
2. RIS deployment to "protect" the entire environment, creating a smart living space that preserves S&P.

The goal of both approaches is to artificially distort the signal picked up by any receiver so that the information imprinted by the environment—because of its characteristic electromagnetic propagation properties—gets *obfuscated*. In other words, it should look like the signal was transmitted through a different propagation channel. It is important to note that information about the environment cannot be deleted, but it is possible to hamper sensing operations by arbitrarily changing such information.

Obfuscating wireless signals directly at the transmitter requires the modification of radios to arbitrarily manipulate the signals to be transmitted. For instance, a *sensing-proof* transmitter may artificially distort the signals sent over the wireless channel by applying pseudo-random amplitude modifications to some subcarriers. Such distortions can be chosen to be either uniformly random [44] or based on some more complex random process (e.g., a Markov process [45]) to make the obfuscated signals appear less artificial. Anyhow, if the distortion changes frequently enough, the receiver will witness an "ever-changing" obfuscated channel that does not correlate well with the real electromagnetic properties of the environment (thus, it is not possible to apply any fingerprinting technique to sense the environment). These approaches are quite easy to experiment with, since they require modification of only the transmitters' firmware and not the receiving devices, which follow their normal operation modes. However, these approaches only work against passive attacks, that is, illegitimate sensing operations that capitalize on signals transmitted by other (legitimate) stations.

Manipulating signals at the transmitter does not work if the attacker controls a transmitter that is fixed in one location, such as an additional AP. In this case, a possible solution is the introduction of one or more RIS in the environment to create controlled signal reflections. By dynamically configuring the RIS to modify the amplitude, the direction, and the delays of the reflections, it should be possible to obfuscate the electromagnetic properties of the environment. Furthermore, it is possible to mimic many different multipath propagation scenarios (especially if multiple RISs are strategically placed in the environment), practically preventing ambient fingerprinting [46]. Still, the present literature does not clarify how to configure and control every RIS to prevent sensing within a smart environment. The work reported in [46] shows a proof-of-concept implementation based on software-defined radios that emulate the behavior of smart surfaces, but such techniques are still in their infancy, mainly due to the technical limitations of RISs.

Although the two obfuscation approaches described above have already been implemented successfully, a couple of shortcomings still require attention. First, arbitrary manipulations of the signals can degrade the throughput of legitimate communications, resulting in a tradeoff between the achievable bit rate and the privacy protection level offered by the system. Secondly, the obfuscation scheme might not be completely reversible; thus, it may prevent both adversarial and legitimate sensing. In principle, it is possible to devise a signaling method that avoids the exchange of secret information about the applied *obfuscation* (or distortion) between legitimate users [47]. The following section discusses problems and possibilities that arise when trying to generalize the issue of legitimate sensing in practical scenarios, also discussing the possible application scenarios, as described in Figures 3–5.

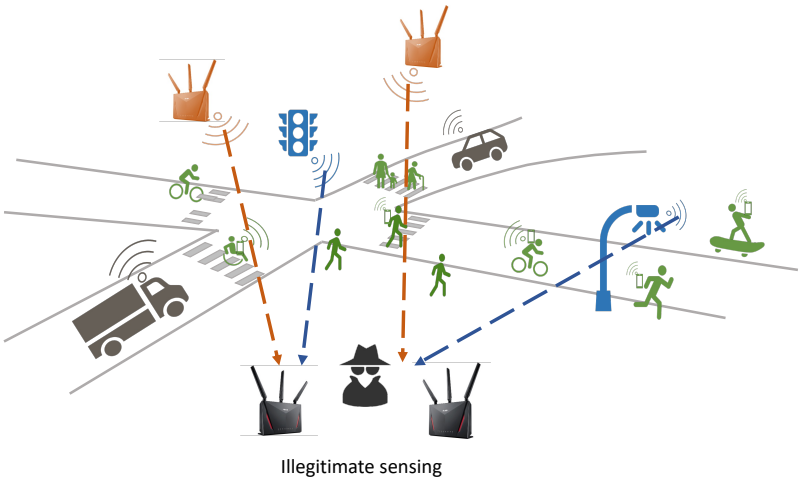

Figure 3. General scenario for smart mobility: Legitimate devices receive normal communication signals between users and the infrastructure. An attacker may overhear normal signals from fixed transmitters (blue devices) or inject additional signals (orange devices).

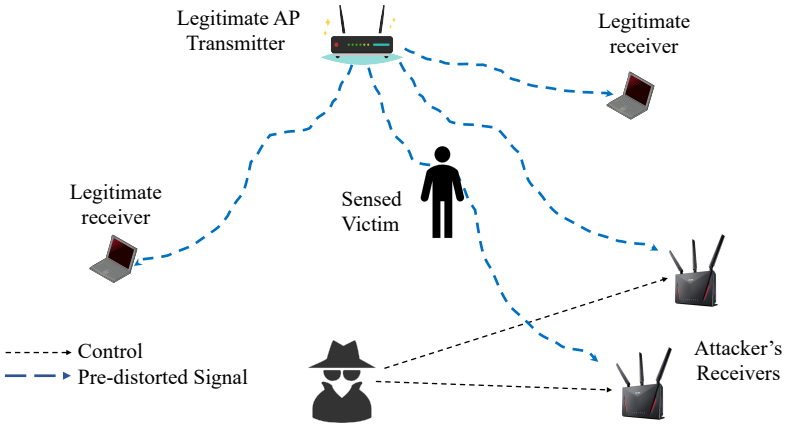

Figure 4. Obfuscation of an indoor passive attack. The legitimate AP transmitter randomly pre-distorts the signals to mimic ever-changing ambient propagation.

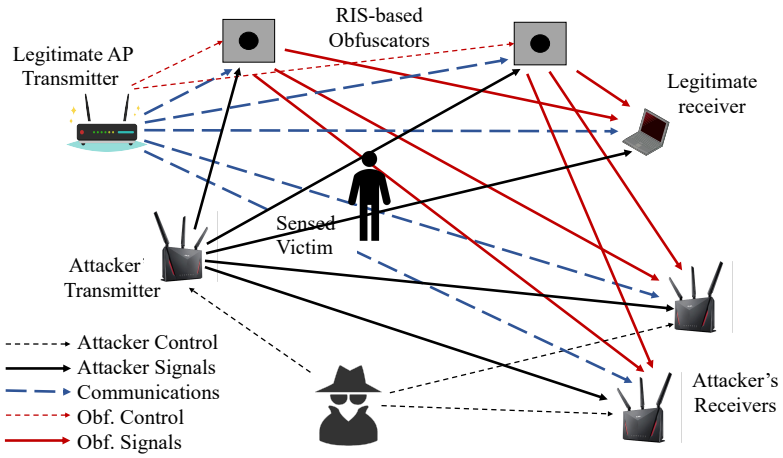

Figure 5. Obfuscation of an indoor active attack with the use of an RIS. The attacker controls one or more transmitters and one or more receivers; thus, the only possibility of protection is with intelligent surfaces that reflect the incoming signal with pseudo-random, sub-symbol delays.

4. Enabling Legitimate Sensing Use

The discussion on the threats to S&P posed by wireless PHY-layer signal manipulation and on the possible countermeasures raises a question: Is it possible to keep the advantages

of CSI sensing while protecting the S&P of users at the same time? In other words, is it possible to design a system where the signal obfuscation is reversible, maybe even with a continuum from full obfuscation to full sensing capabilities, but only for legitimate and enabled devices?

A first attempt in this direction was discussed in [48], where the authors, after implementing an obfuscation technique with an FPGA in openwifi [49,50] (The openwifi project is an open-source software and hardware implementation of 802.11n and is available at https://github.com/open-sdr/openwifi (accessed on 20 December 2024)) discussed one possible method based on the standard four-way-handshake Wi-Fi security to exchange information on the obfuscation technique between the transmitter, considered trusted, and legitimate sensing devices.

Building on that work, we analyze principles and techniques to achieve solutions that fully preserve communication capabilities and selectively enable sensing capabilities for specific devices. The implementation or formal analysis of the proposal is beyond the scope of this paper, which, instead, focuses on analyzing the current state of the art and possible directions for future research.

Recall that the focus is on wireless PHY-layer and CSI-based techniques; to frame them in the Wi-Fi context, refer to 802.11bf ubiquitous Wi-Fi sensing (The 802.11bf PAR was approved in September 2020 and has already released drafts and other documents; see https://standards.ieee.org/ieee/802.11bf (accessed on 20 December 2024). The current status of the Task Group work can be found in [38]). Active measurement techniques such as those based on time of flight (tof) and angle of arrival (AoA) tackled by the 802.11az Task Group (see https://standards.ieee.org/ieee/802.11az (accessed on 20 December 2024)) require the cooperation of the device; therefore, they are outside the scope of this wor, as they do not pose particular threats to S&P because they are based on authenticated collaboration.

To devise mechanisms that enable legitimate sensing, we have to recall the two possible types of sensing attacks: passive and active. In a passive attack, the attacker controls one or more receivers but observes only the signals generated by legitimate devices. Essentially, the attacker does not introduce any additional signal into the ambient environment, making it extremely difficult to identify such a silent attack. In an active attack, instead, the attacker also generates additional Wi-Fi signals, making it easier to identify the ongoing attack, since additional Wi-Fi frames beyond those generated by the legitimate traffic can be identified. However, an active attack complicates the obfuscation task because legitimate transmitters do not control the attacker's signals. Figures 3–5 illustrates three different scenarios, starting from a general one depicting a smart mobility space and detailing two simpler cases of indoor passive and active attacks.

Figure 3 describes one of the most ambitious scenarios for ISAC: smart mobility. In this general scenario, ISAC serves two purposes: coordination of the actors in the smart mobility area and identification through cooperative perception principles of Vulnerable Road Users (VRUs), which may or may not carry a communication device. ISAC and especially CSI-based technologies are, therefore, very promising for these tasks, but an attacker can easily overhear signals to hamper users' security or breach their privacy. Plain obfuscation simply prevents the application of CSI-based sensing to smart mobility spaces; thus, it is important to devise de-obfuscation techniques to allow for legitimate sensing. Recall that only signals from fixed receivers can be used for sensing (the blue and orange in Figure 3) because those emitted by mobile devices (gray and green) are influenced by mobility so that the training of any Artificial Intelligence (AI) method or algorithm is, based on current knowledge, impossible.

Even if the scenario in Figure 3 is enticing, we prefer to restrict the discussion to scenarios that are more readily set up, even if conceptual extension to the general case is

not difficult. Figure 4 shows how a passive attack can be countered with a proper pre-distortion of the transmitted signal, as shown in [44,45]. The key idea of pre-distortion is the multiplication of the transmitted signal by a random function that mimics an ever-changing condition of the propagation environment. Thus, the training of sensing devices becomes useless. Even if the environment is the same, the transmitted signal is multiplied by a different function, and recognizing the same situation is impossible. We talk about a random function and not a random value because the goal is not to attenuate the signal but to distort it, so attenuation must change with frequency.

The pre-distortion of transmitted signals cannot work for an active attack, where the attacker controls the injected traffic. Figure 5 depicts an indoor active attack countered with one or more Reflective Intelligent Surfaces (RISs) [46]. The role of the RIS is similar to the pre-distortion procedure: it introduces fake, random reflections of the transmitted signal, continuously changing the propagation pattern and multipath fading, effectively fouling any attempt to classify and fingerprint the scenario.

First of all, consider that all modern Wi-Fi systems use encryption as defined in the standard [51], which establishes a cryptographically secure communication channel between an AP and an STA—any device connected to the Basic Service Set (BSS)—and the encryption is different for any STA. This channel is normally used to transmit user data, but it can also be used to transfer signaling and management information.

4.1. Four-Way Handshake for Passive Attacks

Passive attacks exploit the normal Wi-Fi signals transmitted by legitimate APs; thus, obfuscation and de-obfuscation can be driven by the APs themselves. APs can exploit the standard secure channel negotiated through 802.11i Four-Way Handshake (4WS). Figure 6 sketches the process and the de-obfuscation signaling on the secure channel.

Obfuscation, as explained in Section 3.2, is based on the multiplication of the transmitted signal by a pseudo-random stochastic process, with the proper correlation in time and frequency. In principle, exchanging the parameters and initializing this process would suffice to enable any legitimate sensing device to apply the inverse of the distortion and recover the non-distorted signal. In reality, things are more complex: What happens if the sensing device and the AP lose synchronization? What happens after a long period of silence? Long can indicate either only a few seconds or tens of seconds.

As shown in Figure 6, after the secure channel is set up, the obfuscation function can, from time to time, send messages to keep the obfuscation and de-obfuscation functions aligned. There are several possibilities to achieve this, but all fall into two categories: extended headers or management frames. In the first case, an additional field must be inserted in the MAC header, which contains the proper information to align the functions at the transmitter and receiver. In the second case, instead of adding fields to standard traffic frames, special management frames can be used when necessary. This second option may be necessary in any case, for instance, when the sensing device gets completely misaligned and is not able to recover enough information from the other frames to work properly.

With both solutions, the system must be properly adapted to the pseudo-random stochastic process, which can be very complex, as it is multivariate—one or two random variables for each subcarrier of the Orthogonal Frequency Division Multiplexing (OFDM)—and with a complex correlation structure to mimic a realistic channel. The details of the protocol and the exchanged information may change depending on the details, but the principle remains the same as described here.

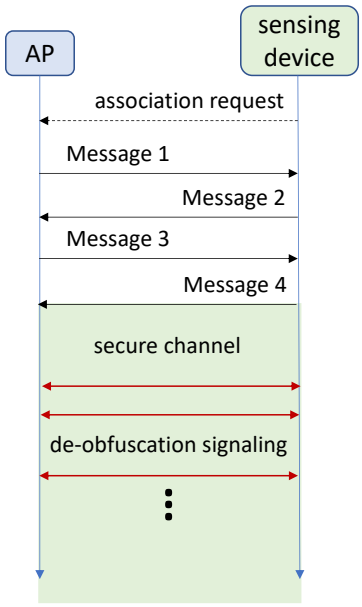

Figure 6. De-obfuscation signaling (red arrows) exploiting the secure channel after the 802.11i 4WHS.

4.2. Control of the RIS for Active Attacks

The situation in the presence of active attacks is different and has not been addressed in any way so far. For obfuscation purposes, the RIS(s) do not even need to be controlled by the AP(s). In fact, they reflect the incoming signal with a configurable, frequency-dependent delay. Consequently, each RIS adds reflection characterized by a time-dependent delay. This makes the CSI collected at any receiver look like the effect of a continuously changing channel, independently of the transmitter. However, for de-obfuscation, the sensing device must be aware of the actual delay introduced by the RIS and of its actual position so as to distinguish the signal(s) reflected by the RIS(s) from all the other multipath reflections that compose the true CSI. This process allows legitimate sensing devices to use the signals generated by the AP(s) to perform sensingwhile preventing any other device from retrieving information on the environment, even exploiting ad hoc frames transmitted by an attacker, because these signals are affected by the dominating randomly delayed reflections of the RIS(s). Using several RISs increases the obfuscation robustness, but it also increases the de-obfuscation complexity.

Figure 7 depicts a possible solution for a time-based obfuscation process. RISs are controlled by the AP(s), as sketched in Figure 5, through a secure, permanent channel (the orange-shaded channel highlighted in Figure 7). The communication can be wired or wireless; the choice depends only on costs and on the architecture of the deployment. When a legitimate sensing device connects to the AP, another secure channel (the green-shaded channel in Figure 7) can be set up, as already discussed in Section 4.1. Once the secure channel is set up, the AP can communicate to the RIS and to the sensing device the parameters for both the obfuscation and the de-obfuscation. In this case, a time-based approach seems simpler. The AP pseudo-periodically (e.g., every $0.5 \pm 20\%$ s) sends messages to all the RISs and all the sensing devices, conveying the valid parameters for the next epoch. If a message gets lost, then the (RIS or sensing) device that missed the message misbehaves for an epoch, but the next message re-aligns it. The effect of these lost messages is different if a sensing device misses them or if an RIS misses them. In the first case, only the sensing device is affected, while in the second, all sensing devices are affected because the RIS reflects the use of delays not coherent with those adopted by the sensing devices.

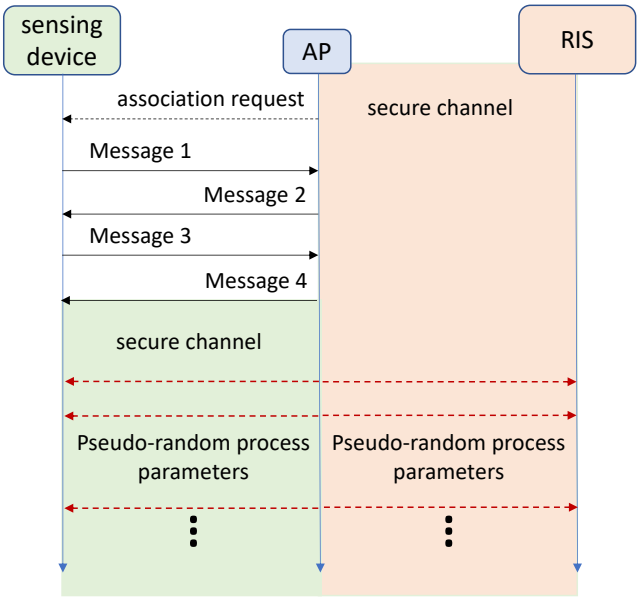

Figure 7. De-obfuscation signaling (red arrows) to drive the RIS and the de-obfuscation at a legitimate sensing device.

We stress that this is an entirely novel topic. Fast programmable RISs are not available; thus, details cannot be provided at this stage of the research. Several options are available, which depend on undisclosed technical details undisclosed of RISs, and many topics are open to optimization. For instance, a multicast secure channel could reduce the number of messages sent, limiting the obfuscation overhead, but it would introduce all the well-known issues related to reliable multicast channels. Another promising direction involves the exploration of optimal patterns for changing the delays and amplitudes of reflections, studying how different patterns affect obfuscation.

5. Discussion

The preliminary results and the ideas presented in this work demonstrate that protecting the wireless PHY layer from S&P attacks in the analog domain is possible. However, the solutions proposed so far are still largely confined to speculative reasoning. Concerning wireless PHY-layer privacy and ISAC techniques, controlled distortion (obfuscation) can prevent sensing. De-obfuscation is also feasible for legitimate devices, since the distortion parameters can be communicated through cryptographically secure channels, empowering the inversion of the distorting function. Pursuing S&P protection and legitimate sensing at the same time remains of the utmost importance to allow future IoT networks to fully exploit ISAC principles and technology, respecting people and society. Thus, to avoid hampering ISAC research, it is necessary to investigate fundamental principles and technologies and enable sensing capabilities only for legitimate receivers.

We identify two main challenges at the present stage. First, it has yet to be proven experimentally that it is possible to *reverse* the obfuscation techniques described in Section 3.2. To the best of our knowledge, even if invertible obfuscation schemes are possible in principle, there is not yet empirical evidence of prototypes that can restore the sensing capabilities of legitimate receivers. Secondly, it is important to define cryptographically secure procedures to share fundamental information about the specific obfuscation pattern (i.e., distortion) applied to the wireless signal. We recognize that this information should be coordinated and synchronized between the transmitters, the receivers, and all the active RIS devices that contribute to the obfuscation. This is a challenging task that could be resolved with multi-party key exchange protocols. Solving these two challenges is key to

demonstrating that privacy in the physical layer can be preserved, even when using new ISAC technologies.

To accelerate the development of mechanisms protecting the physical layer, it is important to encourage the development of coordinated standardization actions inspired, for example, by the initiatives carried out by the IEEE 802.11bf task force to define ISAC-aware signals.

It should also be noted that the techniques and ideas discussed in this work have only been tested in controlled laboratory settings and not in operational situations. To the best of our knowledge, no systematic studies have yet determined whether and to what extent obfuscation can protect users' privacy in generic scenarios. For example, the signal obfuscated by a single transmitter could be unmasked by a highly motivated and endowed attacker that uses many receivers. Comparing the signals received at various points may separate the effects of obfuscation from the actual changes introduced by the environment, but this remains a mere hypothesis until methodologies for realizing it are devised and experimented with. Also, developing a comprehensive, replicable framework to measure the privacy features offered by different obfuscation models is an important development.

In addition to pre-distortion and RIS usage, techniques similar to beamforming (BF) can be considered. BF allows the electromagnetic signal to be shaped to increase the signal-to-interference plus noise ratio (SINR) only at the intended receiver(s) while reducing the SINR level for all others, hampering attackers' malicious sensing activities. This method is currently used to improve communications, and its impact on sensing has yet to be explored. A cooperative approach to security where multiple transmitters send the same signal in order to confuse the attacker is also an interesting idea. If multiple signals are transmitted with different and appropriate phases and amplitudes, the effect is similar to BF but with a much larger spatial diversity. Regarding its feasibility, we can consider that in the context of Wi-Fi, such a technique would not require coherence, as maintaining a CFO (Carrier Frequency Offset) of less than 1 kHz is sufficient for the concurrent transmission of the short frames used in Wi-Fi networks [52], a feature that 802.11ax already guarantees. In cellular systems, this option would be even more viable, thanks to the large capacity of the inter-BS backhaul network that makes substantial signaling possible and cheap.

All such strategies seem to suggest that the path to follow is to render the problem not "impossible" for the attacker but, rather, "computationally unfeasible" (or simply too costly for the benefit). This means that the number of receivers required by the attacker becomes so large that it would be difficult to conceal them in the environment. Also, heavy, coordinated signal processing requires time, so by the time the attacker has collected enough information to defeat the obfuscation, the information is stale and no longer useful.

6. Conclusions and Future Directions

ISAC and the manipulation of wireless analog signals jeopardize S&P of communications and people, but specific studies on this topic are still scarce. Most of work on ISAC is focused on its benefits and its use to customize services, optimize performance, and personalize results and not on its consequences for S&P. Some efforts have been dedicated to wireless PHY-layer security, while privacy is still vastly under-considered and very often perceived as a minor problem or even a nuisance on the basis that "well-behaved" people have nothing to hide and should not bother about privacy.

Privacy is, instead, an integral part of security, so S&P should be tackled together, keeping in mind that privacy breaches always also compromise the security of people, which is the final concern and goal of preserving communications security.

The following list summarizes the main takeaways of this paper and the research directions we deem important in this area.

- Wireless PHY-layer security and integrated sensing and communications (ISAC) are intertwined topics, as emerging sensing and signal manipulation techniques can be applied easily by attackers to imperil S&P.
- The information embedded by the environment in the propagating signals cannot be protected with standard cryptographic techniques; thus, different methods need to be devised for its protection. Obfuscation, i.e., controlled and variable distortion of the signals, is the only proposal that seems viable today.
- A better theoretical understanding of the analog domain is needed to foster research and innovation in the field of S&P protection, looking for innovative services that properly protect both users and infrastructure.
- Besides theoretical work, experiments producing open datasets are needed to enable better understanding of different situations and use cases.
- To improve the situation and avoid problems, both the academic and industrial communities have to act and cooperate now to produce sound standards that also guarantee the proper level of S&P in the analog domain.

Author Contributions: All authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by the University of Brescia through project ISP5G+ (CUP D33C22001300002), part of the SERICS program (PE00000014) under the NRRP MUR program funded by the EU-NGEU and project EMBRACE (CUP E63C22002070006) part of the RESTART program (PE00000001); and by the University of Rome through the SERICS program (PE00000014) under the NRRP MUR program funded by the EU-NGEU and by the European Research Council (ERC) under the European Union's Horizon Europe project (Grant agreement No. 101078411).

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Arisdakessian, S.; Wahab, O.A.; Mourad, A.; Otrok, H.; Guizani, M. A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology, and Explainable AI as Future Directions. *IEEE Internet Things J.* **2023**, *10*, 4059–4092. [CrossRef]
2. Givehchian, H.; Bhaskar, N.; Herrera, E.R.; Soto, H.R.L.; Dameff, C.; Bharadia, D.; Schulman, A. Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 23–25 May 2022; pp. 1690–1704.
3. Gao, K.; Wang, H.; Lv, H.; Gao, P. Your Locations May Be Lies: Selective-PRS-Spoofing Attacks and Defence on 5G NR Positioning Systems. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), New York, NY, USA, 17–20 May 2023; pp. 1–10.
4. Stefania, B.; Giuseppe, B.; Danilo, O.; Ivan, P.; Nicola, B.-M. Location Security under Reference Signals' Spoofing Attacks: Threat Model and Bounds. In Proceedings of the 16th ACM International Conference on Availability, Reliability and Security (ARES), Vienna, Austria, 17–20 August 2021; pp. 1–5.
5. Pecorella, T.; Brilli, L.; Mucchi, L. The Role of Physical Layer Security in IoT: A Novel Perspective. *Information* **2016**, *7*, 49. [CrossRef]
6. Chetty, K.; Smith, G.; Woodbridge, K. Through-the-Wall Sensing of Personnel Using Passive Bistatic WiFi Radar at Standoff Distances. *IEEE Trans. Geosci. Remote Sens.* **2012**, *50*, 1218–1226. [CrossRef]
7. Adib, F.; Katabi, D. See through walls with WiFi! In Proceedings of the ACM International Conference of the Special Interest Group on Data Communication (SIGCOMM), Hong Kong, China, 12–16 August 2013; pp. 75–86.
8. Wang, X.; Gao, L.; Mao, S. CSI Phase Fingerprinting for Indoor Localization with a Deep Learning Approach. *Internet Things J.* **2016**, *3*, 1113–1123. [CrossRef]
9. Di Renzo, M.; Debbah, M.; Phan-Huy, D.; Zappone, A.; Alouini, M.S.; Yuen, C.; Sciancalepore, V.; Alexandropoulos, G.C.; Hoydis, J.; Gacanin, H.; et al. Smart radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come. *J. Wirel. Com. Netw.* **2019**, *2019*, 129. [CrossRef]

10. Abbas, M.; Elhamshary, M.; Rizk, H.; Torki, M.; Youssef, M. WiDeep: WiFi-based Accurate and Robust Indoor Localization System using Deep Learning. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom), Kyoto, Japan, 11–15 March 2019; pp. 1–10.
11. Lo Cigno, R.; Gringoli, F.; Cominelli, M.; Ghiro, L. Integrating CSI Sensing in Wireless Networks: Challenges to Privacy and Countermeasures. *IEEE Netw.* **2022**, *36*, 174–180. [CrossRef]
12. Schumann, R.; Li, F.; Grzegorzek, M. WiFi Sensing with Single-Antenna Devices for Ambient Assisted Living. In Proceedings of the 8th International Workshop on Sensor-Based Activity Recognition and Artificial Intelligence (iWOAR), Lübeck, Germanu, 21–22 September 2023.
13. Sharma, V.; You, I.; Andersson, K.; Palmieri, F.; Rehmani, M.H.; Lim, J. Security, Privacy and Trust for Smart Mobile- Internet of Things (M-IoT): A Survey. *IEEE Access* **2020**, *8*, 167123–167163. [CrossRef]
14. Adam, M.; Hammoudeh, M.; Alrawashdeh, R.; Alsulaimy, B. A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems. *IEEE Access* **2024**, *12*, 57128–57149. [CrossRef]
15. Chorti, A.; Barreto, A.N.; Köpsell, S.; Zoli, M.; Chafii, M.; Sehier, P.; Fettweis, G.; Poor, H.V. Context-Aware Security for 6G Wireless: The Role of Physical Layer Security. *IEEE Commun. Stand. Mag.* **2022**, *6*, 102–108. [CrossRef]
16. Mpitziopoulos, A.; Gavalas, D.; Konstantopoulos, C.; Pantziou, G. A survey on jamming attacks and countermeasures in WSNs. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 42–56. [CrossRef]
17. Huo, Y.; Tian, Y.; Ma, L.; Cheng, X.; Jing, T. Jamming Strategies for Physical Layer Security. *IEEE Wirel. Commun.* **2018**, *25*, 148–153. [CrossRef]
18. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet Things J.* **2019**, *6*, 8169–8181. [CrossRef]
19. Meghdadi, M.; Ozdemir, S.; Güler, I. A survey of wormhole-based attacks and their countermeasures in wireless sensor networks. *IETE Tech. Rev.* **2014**, *28*, 89–102. [CrossRef]
20. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. [CrossRef]
21. Deshmukh-Bhosale, S.; Sonavane, S.S. A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things. *Procedia Manuf.* **2019**, *32*, 840–847. [CrossRef]
22. Focarelli, G.; Zanini, S.; Bianchi, G.; Bartoletti, S. Physical Layer Threats to 5G Positioning: Impact on TOA-Based Methods. In Proceedings of the 2024 IEEE International Conference on Communications Workshops (ICC Workshops), Denver, CO, USA, 9–13 June 2024; pp. 1–6.
23. Orlando, D.; Bartoletti, S.; Palamà, I.; Bianchi, G.; Blefari-Melazzi, N. Innovative Attack Detection Solutions for Wireless Networks With Application to Location Security. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 205–219. [CrossRef]
24. Bartoletti, S.; Bianchi, G.; Blefari-Melazzi, N.; Garlisi, D.; Orlando, D.; Palamà, I.; Modarres Razavi, S. Chapter 5: Security, Integrity, and Privacy Aspects. In *Positioning and Location-Based Analytics in 5G and Beyond*; Wiley: Hoboken, NJ, USA, 2024; pp. 99–123.
25. Di Luzio, A.; Mei, A.; Stefa, J. Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests. In Proceedings of the 35th IEEE International Conference on Computer Communications (INFOCOM), San Francisco, CA, USA, 10–15 April 2016; pp. 1–9.
26. Tsiamitros, N.; Mahapatra, T.; Passalidis, I.; Kailashnath, K.; Pipelidis, G. Pedestrian Flow Identification and Occupancy Prediction for Indoor Areas. *Sensors* **2023**, *23*, 4301. [CrossRef] [PubMed]
27. Yang, M.H.; Luo, J.N.; Vijayalakshmi, M.; Shalinie, S.M. Contactless Credit Cards Payment Fraud Protection by Ambient Authentication. *Sensors* **2022**, *22*, 1989. [CrossRef] [PubMed]
28. Francillon, A.; Danev, B.; Capkun, S. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. In Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 27 February–3 March 2011; pp. 1–16.
29. Sheik, A.T.; Maple, C.; Epiphaniou, G.; Dianati, M. Securing Cloud-Assisted Connected and Autonomous Vehicles: An In-Depth Threat Analysis and Risk Assessment. *Sensors* **2024**, *24*, 241. [CrossRef]
30. Anliker, C.; Camurati, G.; Capkun, S. Time for Change: How Clocks Break UWB Secure Ranging. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USA, 9–11 August 2023; pp. 19–36.
31. Wu, K.; Xiao, J.; Yi, Y.; Chen, D.; Luo, X.; Ni, L. CSI-Based Indoor Localization. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 1300–1309. [CrossRef]
32. Ricciato, F.; Sciancalepore, S.; Gringoli, F.; Facchi, N.; Boggia, G. Position and Velocity Estimation of a Non-Cooperative Source From Asynchronous Packet Arrival Time Measurement. *IEEE Trans. Mob. Comput.* **2018**, *17*, 2166–2179. [CrossRef]
33. Rizk, H.; Elmogy, A.; Yamaguchi, H. A Robust and Accurate Indoor Localization Using Learning-Based Fusion of Wi-Fi RTT and RSSI. *Sensors* **2022**, *22*, 2700. [CrossRef] [PubMed]
34. Wang, Y.; Wu, K.; Ni, L.M. WiFall: Device-Free Fall Detection by Wireless Networks. *IEEE Trans. Mob. Comput.* **2017**, *16*, 581–594. [CrossRef]

35. Cai, C.; Deng, L.; Zheng, M.; Li, S. PILC: Passive Indoor Localization Based on Convolutional Neural Networks. In Proceedings of the IEEE Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS), Wuhan, China, 22–23 March 2018; pp. 1–6.
36. Zheng, Y.; Zhang, Y.; Qian, K.; Zhang, G.; Liu, Y.; Wu, C.; Yang, Z. Zero-Effort Cross-Domain Gesture Recognition with Wi-Fi. In Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services, Seoul, Republic of Korea, 17–21 June 2019; MobiSys '19; ACM: New York, NY, USA, 2019; pp. 313–325.
37. Meneghello, F.; Garlisi, D.; Fabbro, N.D.; Tinnirello, I.; Rossi, M. SHARP: Environment and Person Independent Activity Recognition with Commodity IEEE 802.11 Access Points. *IEEE Trans. Mob. Comput.* **2023**, *22*, 6160–6175. [CrossRef]
38. Du, R.; Hua, H.; Xie, H.; Song, X.; Lyu, Z.; Hu, M.; Narengerile; Xin, Y.; McCann, S.; Montemurro, M.; et al. An Overview on IEEE 802.11bf: WLAN Sensing. *IEEE Commun. Surv. Tutor.* 2024, *Early Access*.
39. Kaushik, A.; Singh, R.; Dayarathna, S.; Senanayake, R.; Di Renzo, M.; Dajer, M.; Ji, H.; Kim, Y.; Sciancalepore, V.; Zappone, A.; et al. Toward Integrated Sensing and Communications for 6G: Key Enabling Technologies, Standardization, and Challenges. *IEEE Commun. Stand. Mag.* **2024**, *8*, 52–59. [CrossRef]
40. Pirayesh, H.; Zeng, H. Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 767–809. [CrossRef]
41. Tippenhauer, N.O.; Rasmussen, K.B.; Capkun, S. Physical-layer integrity for wireless messages. *Elsevier Comput. Netw.* **2016**, *109*, 31–38. [CrossRef]
42. 3GPP. NR; Physical channels and modulation. Technical Specification (TS) 38.211, 3rd Generation Partnership Project (3GPP), 2023. 18.0.0. Available online: https://www.etsi.org/deliver/etsi_ts/138200_138299/138211/15.08.00_60/ts_138211v150800p.pdf (accessed on 20 December 2024).
43. Qiao, Y.; Zhang, O.; Zhou, W.; Srinivasan, K.; Arora, A. PhyCloak: Obfuscating Sensing from Communication Signals. In Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation (NSDI'16), Santa Clara, CA, USA, 16–18 March 2016; pp. 685–699.
44. Cominelli, M.; Kosterhon, F.; Gringoli, F.; Lo Cigno, R.; Asadi, A. IEEE 802.11 CSI randomization to preserve location privacy: An empirical evaluation in different scenarios. *Elsevier Comput. Netw.* **2021**, *191*, 107970. [CrossRef]
45. Cominelli, M.; Gringoli, F.; Lo Cigno, R. On the properties of device-free multi-point CSI localization and its obfuscation. *Elsevier Comput. Commun.* **2022**, *189*, 67–78. [CrossRef]
46. Cominelli, M.; Gringoli, F.; Lo Cigno, R. AntiSense: Standard-compliant CSI obfuscation against unauthorized Wi-Fi sensing. *Elsevier Comput. Commun.* **2022**, *185*, 92–103. [CrossRef]
47. Wang, Y.; Sun, L.; Du, Q.; Elkashlan, M. PriSense: Privacy-Preserving Wireless Sensing for Vital Signs Monitoring. *Proc. IEEE Wirel. Commun. Lett.* **2024**, *13*, 3000–3004. [CrossRef]
48. Ghiro, L.; Cominelli, M.; Gringoli, F.; Lo Cigno, R. Wi-Fi Localization Obfuscation: An implementation in openwifi. *Comput. Commun.* **2023**, *205*, 1–13. [CrossRef]
49. Jiao, X.; Liu, W.; Mehari, M.; Aslam, M.; Moerman, I. openwifi: A free and open-source IEEE802. 11 SDR implementation on SoC. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Virtual, 25 May–31 July 2020; pp. 1–2.
50. Jiao, X.; Liu, W.; Mehari, M.; Thijs, H.; Muhammad, A. open-source IEEE802.11/Wi-Fi baseband chip/FPGA design, 2023. Available online: https://github.com/open-sdr (accessed on 20 December 2024).
51. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2004. Amendment 6: Medium Access Control (MAC) Security Enhancements. Available online: https://ieeexplore.ieee.org/document/1318903 (accessed on 20 December 2024).
52. Gringoli, F.; Klose, R.; Hollick, M.; Nahla, A. Making Wi-Fi Fit for the Tactile Internet: Low-Latency Wi-Fi Flooding Using Concurrent Transmissions. In Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.