

Article

Not peer-reviewed version

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

[Renato Lo Cigno](#)^{*}, [Francesco Gringoli](#), Stefania Bartoletti, [Marco Cominelli](#), [Lorenzo Ghiro](#), [Samuele Zanini](#)

Posted Date: 29 August 2024

doi: 10.20944/preprints202408.2131.v1

Keywords: Integrated Communications and Sensing; PHY Layer Security; Pervasive Communications and Sensing; Privacy Protection; Analog Signals Manipulation





Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Article

Communication and Sensing: 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 Ghio ¹ and Samuele Zanini ^{2,4}

¹ University of Brescia and Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT), Italy

² University of Rome Tor Vergata and CNIT, Italy

³ Politecnico di Milano, Italy

⁴ IMT School for Advanced Studies Lucca, Italy

* Correspondence: renato.locigno@unibs.it

Abstract: Recent advances in signal processing and AI-based inference enable the exploitation of 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 opens new and exciting opportunities for IoT systems, but at the same time poses unprecedented threats to security and privacy of data, devices, and systems. In fact, ISAC operates at the PHY and Medium Access Control (MAC) layers, where it is impossible to protect the information with standard encryption techniques, or with any other purely digital methodologies. The work we present analyzes, within the framework of IoT and distributed, pervasive communication systems, the threats to security and privacy posed by ISAC and how they do intertwine at the PHY layer. Next, possible countermeasures are presented and discussed, with proper architectural choices and tradeoffs to implement them, as well as solutions and protocols to preserve the potential benefits of ISAC while ensuring data protection and users' privacy.

Keywords: integrated communications and sensing; PHY layer security; pervasive communications and sensing; privacy protection; analog signals manipulation

1. Introduction

There is no doubt that the IoT (Internet of Things) is a multifaceted reality, growing to cover scenarios not included in its scope when the term was introduced in the late '90s of the past century. Today, IoT scenarios are extended to cover almost anything from industrial plants to smart mobility, and access technologies supporting it range from cellular network (4G/5G and beyond), to WiFi, to LoRa and LoRAWAN, and many other standard and proprietary communication technologies.

It is thus no wonder that privacy and security are for the IoT fundamental features, not differently from other highly sensitive communication services, as, for instance the banking system or the medical sector. Actually, the medical sector is also becoming part of the IoT, as wearable medical devices empowers e-health systems, and smart living spaces allow elderly people to stay active and independent for longer years. Privacy and security is so badly needed in the IoT, that surveys, special issues, and tutorial publications on the subject can be counted by the hundreds, while specific contributions in scholarly venues are approaching one million, making a selection of relevant publication 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 still require novel approaches and pose specific challenges that pertain to the unique mixture of devices and elements that make up the IoT environment. As a telltale of this difficulty, we can mention the recent survey [1], citing more than 130 references and highlighting the fragmentation of research and solutions for IoT S&P. The authors do a thorough classification work and focus on intrusion attacks and

intrusion detection systems, starting at the networking level up to the data integration and application level. Within the networking level, the physical (PHY) and Medium Access Control (MAC) layers are collectively called *perception layer*, and the only threat considered is jamming.

Albeit this perspective is probably the most common in the community, recent results contrast it and show that there are many more, and more sophisticated threats at the PHY and MAC layer than jamming. This work addresses this novel and emerging topic in S&P that affects all wireless networks, including the IoT: Integrated Sensing And Communication (ISAC) and PHY layer security attacks.

Traditionally, S&P focused on the protection of data by way of encrypting the information during transmission, processing and storage, and protecting it from illegitimate use. Any protection means is based on the digital processing of the information and disregards information embedded in the analog signals for transmission, whose access, in the case of wireless networks, is freely available to anybody and it is extremely difficult to protect due to its analog nature; indeed, at the state of the art not even quantum cryptography can be applied to analog transmissions, hence alternative solutions must be searched for.

PHY layer attacks relate to different aspects, starting from device fingerprinting [2] to localization spoofing and deception [3,4]. Here, differently from, e.g., the authors of [5], we do not include in PHY layer security the attacks targeted to break cryptographic channels. Indeed, even if these are often called *PHY layer*, the secure channels of wireless communications, from cellular networks, to 802.11 and 802.15 standards, and all other technologies are built, from a protocol architecture perspective, above the MAC protocols where the headers and control information need to be in clear for channel control and management. We deal instead with the emerging techniques that exploit analog properties of the signals to hamper some functionality. One simple example is tampering with anchor positions in active device localization: The attack does not require to break any cryptographic protocol, but can be carried out moving one or more devices from their intended positions.

ISAC refers instead to the capability of exploiting the same signals used for the transmission of digital information to perform some measures (or sensing) on the environment [6–12] and covers many aspects of sensing and measurements, with a keen bias, however, on human beings activities, thus clearly hampering privacy.

ISAC itself can be split into many different technologies and applications 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 device itself, from its location to its identity, which can be used e.g., to reinforce authentication ... or to track people jeopardizing their privacy. In the second case the signals are used to capture some properties of the propagation environment, in general unrelated to the device themselves, from the state of an ambient (e.g., presence of people or even change in temperature), to the activities of people operating into a room or laboratory.

The two topics sometimes overlap, as for instance in device fingerprinting, while in other cases are (almost) unrelated, but they always share the fact that S&P threats are rooted in the analog domain and traditional protection techniques are not suitable. The goal of this paper is thus to outline the state of the art on S&P threats due to the intrinsic analog nature of transmissions and delineate possible countermeasures that are just starting to be explored by the community. The contribution is not a survey on the topic: On the one hand the topic is too vast, and on the other hand there are already valid surveys on its many facets. Rather, we delineate the contours of the problem, and analyze which solutions are viable and which are not (and why they are not).

2. State of the Art

The goal of this section is to provide a systematic view of PHY layer S&P, highlighting what is today the edge of research and the main known attacks, sometimes disguised as potential services, that can be carried out with the analysis of the transmission signals. Only foundational papers and recent achievements are reported trying to give a concise, yet clear view on the achievements reached by knowledge and research.

2.1. Security Threats at the PHY Layer

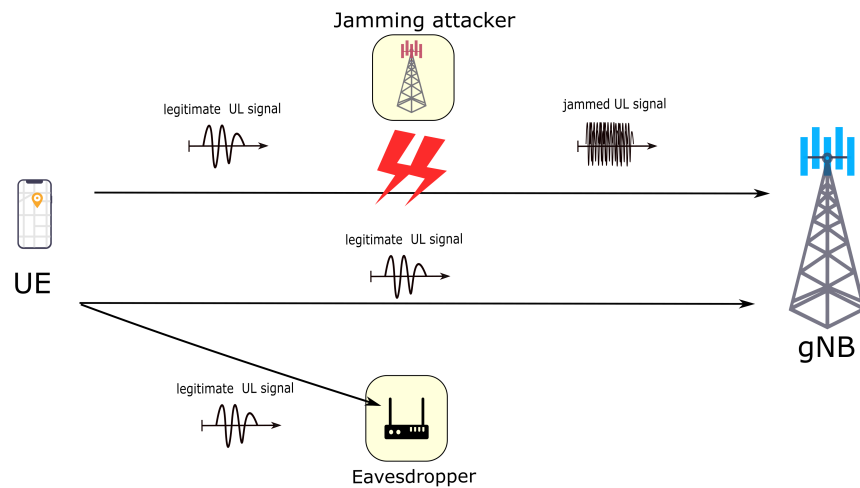
Jamming and eavesdropping [5,13,14] are the most studied threats at the PHY layer, but they are not the only ones and most of all not the most treacherous. Jamming is a plain, open attack, and eavesdropping can be countered in general with appropriate cryptographic techniques. Indeed, several other attacks must be considered, especially in the context of wireless communication and more specifically for IoT and sensing applications [4,15–19]. Traditional attacks and threats include also wormhole attacks, Man-In-The-Middle (MITM) attacks, and spoofing. For instance, in mission-critical applications, e.g., autonomous driving, if the positioning measurements are tampered with by an attacker through physical threats, the outcome could potentially cause harm and pose safety hazards.

Figure 1 depicts some of the known attacks at the PHY layer, whose goals are described below.

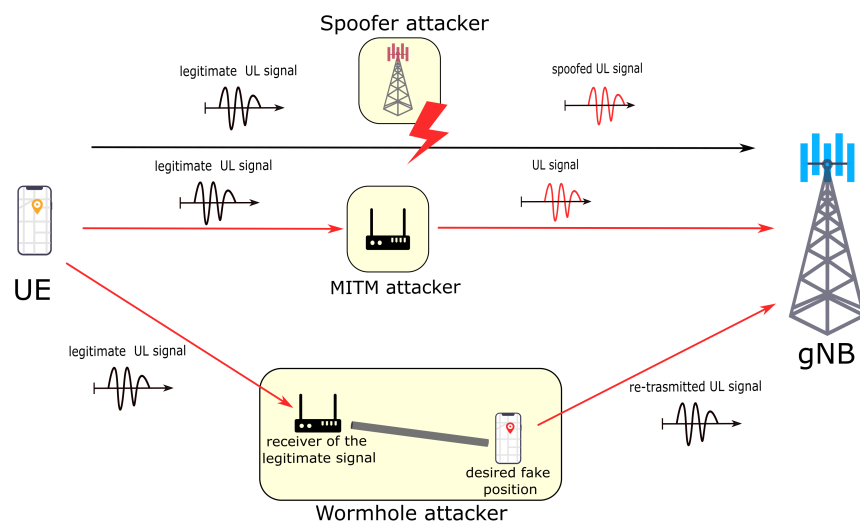
- **Eavesdropping:** The malicious entity aims to intercept confidential information transmitted over the air between the transmitter and receiver resulting in privacy breaches, but also in safety challenge when the information captured can be used for further, maybe off-network, attacks.
- **Jamming:** The goal is to disrupt over-the-air communication, i.e., reducing the SNR of legitimate transmission 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. This way a proper combination of techniques can build attacks that cannot be protected with available digital techniques.
- **Man-in-the-middle** A MITM attack at the PHY layer is based on the interception of the signals and the interposition of a device that mimics the other end of the communication for both parties. In general these attacks require to access also higher layers of the communication and to be able to operate on the victim's data by modifying the transmitted information. The attacker needs to operate both directions of the communications, by establishing a double fake connection, one for the victim device and the other one with the base station in a cellular context, and AP in a Wi-Fi one or in general the "other" device.
- **Wormhole:** The wormhole attack, instead is based on the manipulation of signals in order to create a rogue tunnel, i.e., a communication path which is not the natural one between the two devices, but instead forces the actual information to be routed through a different physical path, but without the requirement to decode and re-encode all the layers of the communication. Specifically, the attacker does not manipulate the data transmitted but it only routes it through another path, possibly deceiving some specific information, e.g., the propagation time, or tampering with the analog signal or at most with the MAC layer headers to reach his/her goals.
- **Spoofing:** In this scenario the attacker manipulates some properties of the signals or of the electromagnetic properties of the environment to deceive the victim in some way. A classical example is GPS spoofing, where the attacker tampers the GPS signal to change the location estimated by the target as desired. Another example is MAC address de-anonymization, obtained by smartly using the information contained in standard Wi-Fi probes, whose final outcome is the violation of users' privacy and security by allowing tracking and more.

In the context of IoT, the authors of [15] provide 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 suggest countermeasures, both general and specifically based on the characteristics of 5G IoT networks, such as massive Multiple Input Multiple Output (MIMO), against passive eavesdropping. Jamming and eavesdropping can lead to potential denial-of-service and privacy breaches, while other threats may cause additional problems related to applications and use cases. Various other studies [4,19–21],

examine the impact of potential attacks and corresponding mitigation strategies on 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 PHY layer are exploited to tamper the measurements, leading to erroneous outcomes of position estimation.



(a) Jamming and eavesdropping attacks



(b) Spoofing, MITM, and wormhole attacks

Figure 1. Visual illustration of some threats at PHY layer in the context of 5G networks.

Coming to attacks specific of the PHY layer and typical of the IoT environment, let's consider in more detail de-anonymization and wormhole attacks on sensitive devices.

As clearly described in [22,23], the key component for the attack is the Wi-Fi probe, which is broadcast by devices looking for a network to connect. The authors in [22] explicitly explain how to achieve de-anonymization using anonymous Wi-Fi probes of devices that actively search for network connectivity, while in [23] the goal is (apparently) legitimate, but indeed it is not difficult to imagine how the same technique can be used for attacks. The key idea is that collecting large amounts of these broadcast packets, that otherwise do not contain sensitive information, it is possible to retrieve the position, the whereabouts and many other information on the devices themselves, but also, and obviously, on the people that carry them.

Device specific wormhole attacks seems instead a real IoT doom, as the target the typical small, cheap devices that are the backbone of the IoT. The work in [24] address the archetypal of security threats: stealing money. The authors show that, in wireless-based money exchange, an attacker that properly place a device that may act as a wormhole may deceive the merchant, thus making illicit transactions using the victim's plastic or virtual (i.e., a smartphone app) money, while he/she's doing another transaction or no transaction at all. The authors of [25,26], instead, use similar technique to demonstrate wormhole attacks to another staple or our perceived security: Cars. In [25] the authors use relays (a form of wormhole) to show that passive remote entry and start systems can be tampered with directly at the PHY layer, without the need of sophisticated processing capabilities: Cars can be opened, started, even partially operated remotely, posing threats not only for theft, but also for safety of passengers themselves. The authors of [26], instead, present a wide review of possible attacks to connected vehicles in the most widespread architectures. The goal of the work is broader, but PHY layer threats and attacks are considered too.

Finally, [27] presents an attack on Ultra Wide Band (UWB) ranging systems, which are in general considered secure, thus a possible countermeasure against other attacks, including wormhole. The 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 it cannot be countered with standard cryptography.

2.2. Integrated Sensing and Communication

More than 10 years ago, the pioneering works in [6,7,28] suggested that it is possible to use communication signals also to detect physical objects that are 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 through the analysis of the PHY layer information. 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, those works revealed that sub-6-GHz frequencies might provide a good tradeoff between sensing accuracy and the capability to operate through walls and in other complex non-line-of-sight scenarios.

Over the last decade, researchers proposed several different ISAC systems to either improve existing sensing applications or address completely new problems. For instance, 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) [29]. Alternatively, deep learning methods have been shown to help in improving localization based on round-trip-time and RSSI measurements [30]. Otherwise, if other localization methods are unfeasible, deep learning can be used to localize the target devices following a fingerprinting approach [8,10].

Still, some of the most interesting applications of ISAC systems lie in the estimation of the position and the 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 [31] to localization [32], to fine-grained gesture [33] and activity [34] recognition, notably all regarding *humans*!. Figure 2 highlights a critical issue of all these approaches, namely that the information about propagation resides at the PHY level and is not secured. This implies that *any* device can collect raw CSI data, so that an eavesdropper can opportunistically utilize the frames transmitted by other (legitimate) devices to perform the analysis described in all the cited research works.

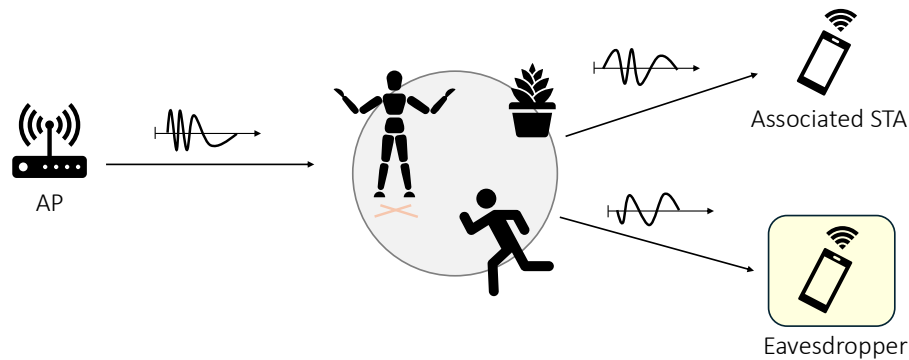


Figure 2. People and objects directly affect the propagation of wireless signals. Encryption of the data payload cannot prevent an eavesdropper from monitoring the environment using the signals' properties at the PHY layer.

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 the integration of sensing and communication functionalities, with most of the ongoing investigations focusing on this technology. Indeed, Wi-Fi already started working on standardizing ISAC procedures through the IEEE 802.11bf task force [35]. On the other hand, ETSI revealed that ISAC will be one of the key scenarios for the upcoming 6G cellular networks [36]. However, despite the efforts in standardizing 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. For all the research done so far, indeed the synergistic aspects between these technologies have yet to be explored in depth by the research community.

3. Countermeasures

Section 2 gives a clear overview of the several threats at the PHY and MAC layer that, exploiting also analog signals and information prevent the use of standard means to protect S&P. Here, we discuss possible countermeasures against these attacks to ensure robustness and secure communication for IoT and ISAC applications.

3.1. Security Threats at the PHY Layer

Some possible solutions to eavesdropping and jamming involve techniques based on spread spectrum, such as Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) [13]. 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 were studied and used for military communications, and are in general best suited for sporadic, low-bit-rate communications, and it is difficult to adapt them to modern, multi-Gbit/s communications. In addition to these two well-known techniques, [15] 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, thus having a similar channel condition, to gather useful information. These countermeasures, however have yet to be proven, if not for else, because massive MIMO technologies are 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 is very easily localized.

Simple countermeasures against MITM are available and include mutual authentication between the entities involved in the communication, the use of certificate authorities, and cryptography to ensure the integrity and encryption of the communication [17]. These are all important techniques, but they clearly address attacks that are carried out in the digital domain, while those in the analog domain remain unscathed, for instance the wormhole attack.

One possibility to counter wormhole attacks on wireless networks is leveraging the different statistic of the channel behavior when a wormhole attack is running. For instance one can leverage the additional time added by the malicious node's rogue path in the overall communication, hence increasing latency. The detection can be based on computing the Time-of-Flight (ToF), either in a single direction or round trip, and checking it against a pre-computed threshold, with the maximum acceptable value depending on the specific case scenario, similar to the evaluation of the Round-Trip-Time (RTT) in [16], but clearly considering only the wireless hop of the communication, otherwise the tiny increase due to the wormhole is lost in the length of the end-to-end transmission. Indeed, this seems a very naïve approach, and applying run-time estimation techniques seems a more sound approach. This estimation can be based on traditional stochastic analysis techniques, estimating the probability that the ToF is subject to sudden changes (when the attacker intercepts the signal), or simply to statistics that cannot be met with a direct communications. In alternative more advanced, AI/ML techniques can be applied to achieve the same result.

Standard organizations are developing specifications to standardize countermeasures against PHY threats, but these may worsen the problem instead of solving it, due to the possibilities opened in analog signal analysis by modern AI/ML algorithms. The 3GPP, in the 5G documentation, addresses 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 the channel estimation, and timing/angle measurements. If these symbols are constant, then ISAC becomes possible to anyone, so pseudo-random techniques are under study. The symbols transmitted are based on pseudo-random sequences where the seed depends on high-level parameters of the application [37]. For example, the Reference Signals (RS) for positioning purposes (Sounding RS (SRS) and Positioning RS (PRS)) depend on the parameters between 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 is unable to perform a spoofing attack to disrupt the positioning estimation of the end-user's location. Indeed, 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 more on ensuring that positioning on the network side remains robust enough for applications, rather than for protecting users S&P. Sometimes these two goals overlap, but they may also be independent or even contra-posed, e.g., when the network is not fully trusted or trustable by the user.

Countermeasures against attacks at the PHY layer are essential for secure and efficient communications and to build a solid trust of users in the system. IoT systems will become pervasive in the future, and are the backbone of smart living spaces; however, people must be guaranteed that a smart space is also a space that preserves S&P, independently of the fact that it carries IoT devices 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 propagated in an environment is readily available to *all* the devices in an area (see Figure 2). Only a few works have dealt with this issue, which will become more critical as ISAC technology is integrated into future wireless systems.

Early works proposed using special devices that act as dynamic reflectors in order to *obfuscate* the electromagnetic properties of the environment and disrupt the eavesdroppers' attempts to perform sensing [38]. However, the *obfuscators* proposed in this work require expensive hardware and have

limited reconfigurability. Moreover, the privacy performance (i.e., the ability to disrupt illegitimate sensing) is highly dependent on the relative position of transmitters, eavesdroppers, and obfuscators. This initial work spawned additional research as discussed below and the evolution of Reflective Intelligent Surfaces (RISes) in these last years is making these approaches more appealing.

First of all, it must be noted that signals useful for ISAC are, to the state of the art, only those transmitted by devices that are in a fixed position. Their actual position is not important, as the signal analysis does not require to know the transmitter position, but since the analysis is based on fingerprinting, the movement of the transmitter would change the pattern and prevent recognizing the same pattern. Thus, two lines of research emerged: *i)* Obfuscating signals directly at the transmitter, and *ii)* using one or more RIS to protect the entire propagation environment creating a smart living space that protects S&P. In both cases the key idea is distorting randomly the signal in such a way that the information embedded by the environment during propagation is obfuscated (it cannot be deleted) and the received signal looks like a normal propagation channel, thus the information can be decoded, but a different one, always changing, so that sensing operations fail.

Working at the transmitter protect only against passive attacks, i.e., illegitimate sensing that uses the transmissions by legitimate APs. The manipulation can either be completely random [39] or dictated by a more complex process—for instance, a Markov process in [40], that makes the signal more realistic, and also more difficult for a powerful, multi-point attack to filter out the distortion. These approaches require modifying only the transmitters' firmware and not the receiving devices, which follow their normal operation modes.

Manipulating signals at the transmitter does not work if the attacker controls a fixed transmitter, e.g., an additional AP. In this case, one or more RIS (or similar devices) can be added in the environment that introduce controlled reflections with random delays. In practice, these reflections mimic multipath propagation in varying environments practically preventing ambient fingerprinting [41]. This technique is still in its infancy, mainly due to technical limitations of RISes, thus the work above presented a proof-of-concept based on (delayed) signal replication.

Albeit the approaches above have been implemented, and so far there are no works that show that an attack can still be built against such obfuscation, there are still two shortcomings that require attention. First, arbitrary manipulations can degrade the throughput of legitimate communications, presenting a tradeoff between the achievable rate and the privacy protection offered by the system. Second, the obfuscation scheme might not be completely reversible and thus 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 [42]. The following section discusses problems and possibilities that arise when trying to generalize the problem of legitimate sensing in practical scenarios, also discussing in more detail the possible application scenarios as described in Figures 3–5.

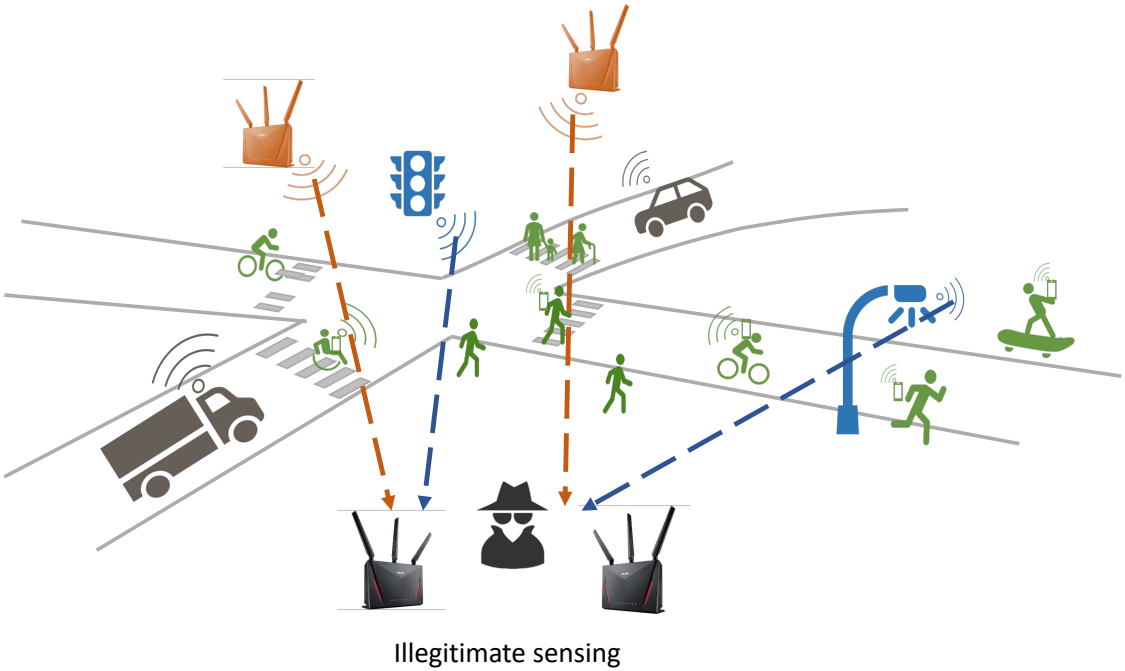


Figure 3. General Scenario for smart mobility: legitimate devices receive normal communications signals between users and the infrastructure. An attacker may overhear normal signals from fixed transmitter (blue devices) or inject additional signals (orange devices).

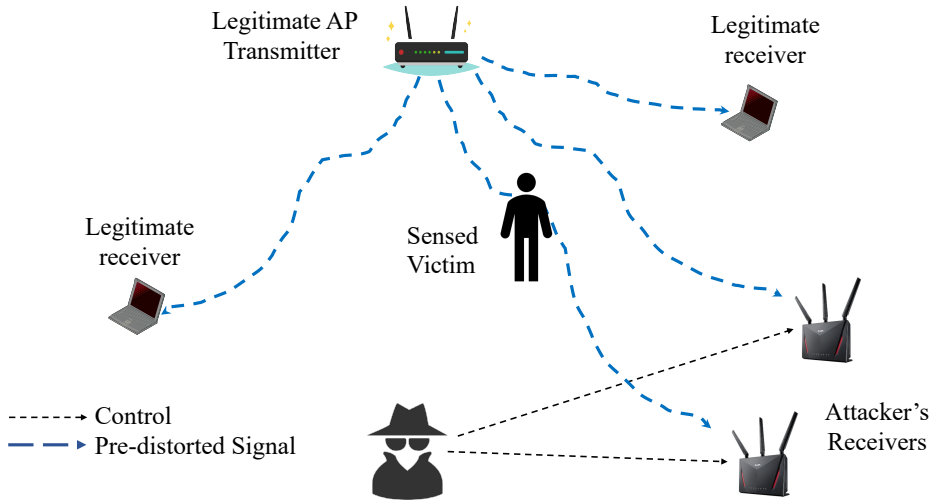


Figure 4. Obfuscation of and indoor passive attack. The legitimate AP transmitter randomly pre-distorts the signals to mimic an ever-changing different propagation ambient.

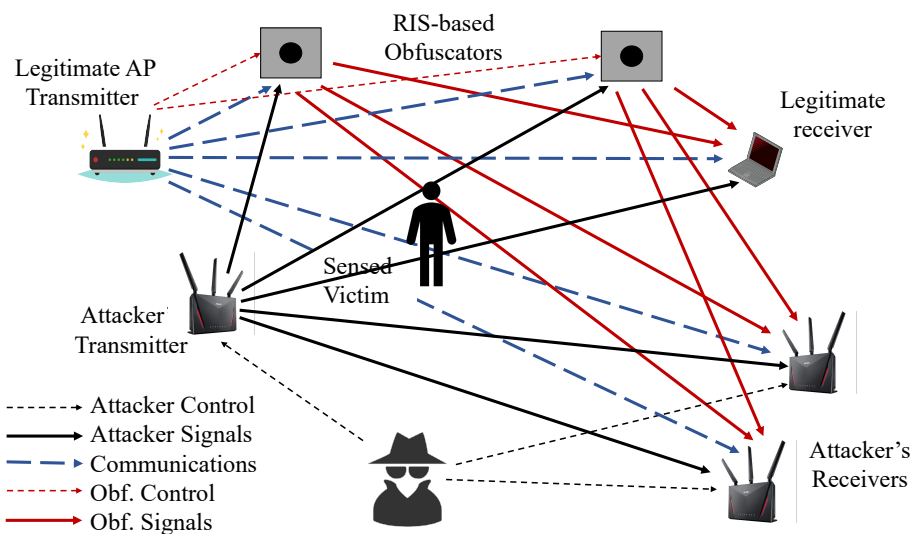


Figure 5. Obfuscation of an indoor active attack with the use of RIS. The attacker controls one or more transmitters and one or more receivers, thus the only possibility of protection is with intelligent surfaces that reflect the incoming signal with pseudo-random, sub-symbol delays.

4. Enabling Legitimate Sensing Use

After the discussion on the threats to privacy and security posed by PHY-layer signal analysis and the possible countermeasures available thanks to signal obfuscation a question arise: Is it possible to maintain the advantages of CSI sensing and protect the privacy and security of users? In other words, is it possible to design a system and protocol where 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 [43] where the authors, after implementing an obfuscation technique with an FPGA in openwifi [44,45]¹, discuss one possible method based on the standard Wi-Fi security four-way-handshake to exchange information on the obfuscation technique between the transmitter, considered trusted, and legitimate sensing devices.

Moving on in the direction of that work we analyze principles and techniques that can be used to achieve solutions that fully preserve communication capabilities and selectively enable sensing capabilities for specific devices. Recall that the focus is on PHY-layer and CSI-based techniques; to frame them into the Wi-Fi context, refer to 802.11bf ubiquitous Wi-Fi sensing.² Active measurement techniques such as those based on Time of Flight (ToF) and Angle of Arrival (AoA), tackled by the 802.11az Task Group³ that require the cooperation of the device, are outside the scope of this work.

To properly identify mechanisms to enable legitimate sensing we have recall the two possible types of sensing attack: Passive or Active. In a passive attack the attacker controls one or more receiver, but exploits only the signals generated by the normal devices to carry traffic, thus he/she does not introduce in the ambient any additional signal, which makes identifying the attack extremely difficult. In an active attack, instead, the attacker also inject additional Wi-Fi signals in the ambient, making it easier to identify the presence of an attack (additional Wi-Fi frames beyond those generated by the normal traffic), but also making it more difficult to obfuscate the signals to prevent sensing. Figures 3–5 depict the situations, starting from a very general scenario suitable also for smart mobility ans

¹ The openwifi project is an Open Source software and hardware implementation of 802.11n. It is available at: <https://github.com/open-sdr/openwifi>.

² The 802.11bf PAR was approved in Sept. 2020 and has already released drafts and other documents, see <https://standards.ieee.org/ieee/802.11bf>. The current status of the Task Group work can be found in [35].

³ See <https://standards.ieee.org/ieee/802.11az>.

smart living spaces, very promising scenarios, albeit in our opinion not yet feasible at the state of the art, to arrive to more manageable and realistic cases of indoor passive or active sensing attacks.

Figure 3 describes one of the most ambitious scenarios for ISAC: a smart mobility environment. In a general scenario like this one, ISAC serves several purposes: Coordination of the actors in the smart mobility area, but also identification, through cooperative perception principles, of Vulnerable Road Users (VRUs), which may or may not carry a communication device. Clearly, ISAC and specially CSI-based technologies are very promising for these tasks, but an attacker can easily overhear signals to hamper security of users or breach their privacy. We have discussed countermeasures to obfuscate the sensing information carried by the signals while preserving communication performance, but how can we retain the advantages of ISAC and protect users' at the same time? 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 the mobility itself so that training 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 the 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 [39,40]. The key idea of pre-distortion is the multiplication of the transmitted signal by a random function that mimics an always changing condition of the propagation environment, so that training sensing devices is useless: next time the environment is the same, the transmitted signal will be multiplied by a different function, thus recognizing the same situation is impossible. We talk about a random function and not a random value, because the goal is not attenuating the signal, but distorting it, so attenuation changes with frequency.

Pre-distorting 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 Surface (RIS) [41]. 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 use encryption as defined in the standard [46], which establishes a cryptographically secure communication channel between an AP and a 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 in the secure channel.

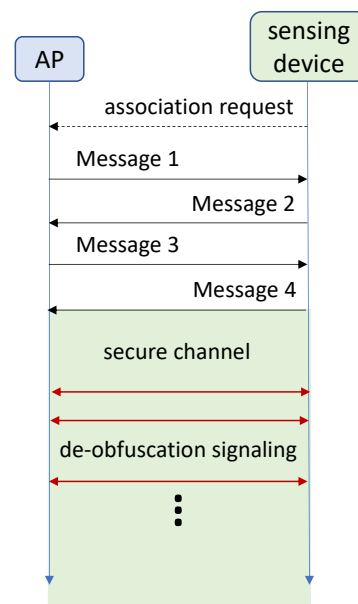


Figure 6. De-obfuscation signaling (red arrows) exploiting the secure channel after the 802.11i 4WHS.

Obfuscation, as explained in Section 3.2, is based on the multiplication of the transmitted signal by a pseudo-random Markovian process, with the proper correlation in time and frequency. In principle, it would suffice to exchange the parameters and initialization of the Markov process to enable any legitimate sensing device to apply the inverse of the distortion and recover the non-distorted signal. In reality, as usual, 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 indeed be only a few seconds or tens of seconds. As shown in Figure 6, after the secure channel is setup, the obfuscation function can, from time to time, send messages to maintain the obfuscation and de-obfuscation functions aligned.

There are several possibilities to achieve this, but all falls into two categories: Extended headers or management frames. In the first case, an additional fields must be inserted in the MAC header, which contain 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, indeed, may be necessary in any case, for instance in case the sensing device gets completely mis-aligned and is not able to recover enough information from the frames to work properly.

In both cases the system must be properly adapted to the pseudo-random Markovian process, which, as discussed, can be time-based or frame-based. The details of the protocol and the information exchanged may change slightly depending on the details, but the principle remains the same described here.

4.2. Control of the RSI for Active Attacks

The situation in presence of active attacks is different and has not been addressed in any way so far. For obfuscation purposes, the RIS(es) do not even need to be controlled by the AP(s), since reflections randomly delayed will make the CSI collected at any receiver look like the effect of a continuously changing channel, independently from the transmitter; however, for de-obfuscation, the sensing device must be aware of the actual delay introduced by the RIS, and also of its actual position, so as to be able to separate the RIS(es) reflected signal(s) from all the other multipath reflections that compose the true CSI. This process will allow legitimate sensing devices to use the AP(s) generated signals to perform sensing, while preventing any other device to retrieve information on the environment, even exploiting frames transmitted ad-hoc by an attacker, because these signals will be affected by the dominating randomly-delayed reflections of the RISes.

Figure 7 depicts a possible solution for a time-based obfuscation process. RIS(es) 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 it is not relevant, and depends on cost and architecture of the deployment. When a legitimate sensing device connects to the AP, another secure channel (the green-shaded in Figure 7) can be setup as already discussed in Section 4.1. Once the secure channel is setup, the AP can communicate to the RIS and the sensing device the parameters of the obfuscation and 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 RISes and all the sensing devices the parameters valid for the next epoch. In case a message gets lost, it means that the device (RIS or sensing) that missed the message will misbehave for an epoch, but the next message will re-align it. The effect of these lost messages are different if a sensing device misses it or if a RIS misses it: In the first case only the sensing device will be affected, while in the second all sensing devices will be, because the RIS missing the message will reflect with delays not coherent with those computed at the sensing devices.

Clearly, many details are missing and optimization can be applied. For instance, a multicast secure channel would enable to reduce the number of messages sent, but introduces the well known issues connected with reliable multicast.

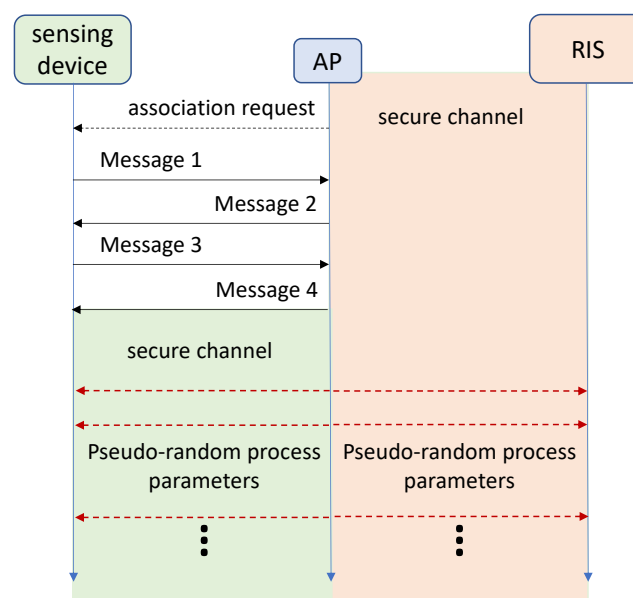


Figure 7. De-obfuscation signaling (red arrows) to drive the RIS and the de-obfuscation at a legitimate sensing device.

5. Discussion

The results and the ideas that we have presented in this work demonstrate that protecting the physical layer is possible. However, the solutions that have been adopted so far are still largely confined to the research phase. In particular, if we consider ICAS techniques, all demonstrations about restoring the privacy of the involved people have been discussed in principle and implementations have not been attempted even in well controlled lab environments [43]. Moreover, although the goal of these mechanisms is praiseworthy in principle, they may hinder the use of ICAS techniques. It is therefore necessary to study additional techniques that can restore sensing accuracy at least at legitimate receivers, i.e., by designing protocols capable of sharing information about the used signal obfuscation scheme between transmitters and receivers within the network.

To accelerate the development of mechanisms for the protection of the physical layer, it is important to encourage not only the efforts of researchers but also the development of coordinated standardization actions taking inspiration, for example, from the initiatives carried out by the IEEE

802.11bf task-force regarding the definition of ICAS-aware signals. It would be far more effective to act now and design privacy-aware signals, rather than trying to address the S&P issues after the first systems adopting such methods are deployed.

It should also be noted that the techniques and ideas discussed in this work, as still deeply rooted in laboratory settings, lack validation to determine how effectively they can protect the physical layer from attackers. For example, obfuscation techniques employed by a single transmitter could be probably exposed by a highly motivated attacker using multiple receivers, who can compare the signals received at various points and distinguish the effects of obfuscation from the actual changes introduced by the environment, such as someone moving through the space.

To counter this, it is necessary to make these techniques more sophisticated and physically modify the emission pattern of every single transmitter in addition to pre-filter the signals it emits. In addition to RIS, techniques similar to beamforming (BF) can be considered: a transmitter may hence leverage BF to change the shape of the electromagnetic signal in the environment on top of the configuration it would choose to just increase the signal-to-noise ratio at the intended receiver. In this way, reducing the SINR level a bit could be beneficial for deceiving sensing activities operated by an attacker. The problem could be further complicated by adopting a cooperative approach to security, where multiple transmitters send the same signal in order to confuse the attacker. If multiple signals are then transmitted with configurable phases and amplitudes, the effect would be similar to what can be obtained with beamforming but with a much larger spatial diversity. Regarding its feasibility, we can consider that in the context of Wi-Fi, such 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 [47], a feature that 802.11ax already guarantees. In cellular systems, this option would be even more viable thanks to the heavy signaling that the backhaul network makes possible.

By adopting such strategies, we can apply the classic approach of making the problem for attackers not “impossible” but “computationally unfeasible.” This means that the number of receivers required at the attacker side becomes so large that it would be difficult to conceive them in the environment. Also, heavy, coordinated signal processing requires time, so that by the time the attacker has managed to collect enough useful signals to defeat the obfuscation, the signal is no longer of any use.

6. Conclusions

ISAC and the use of analog signal manipulation to attack S&P of communications networks are emerging topics in research and applications. Most of the work on ISAC is focused on its benefits and its potential use for customized services that make use of ambient intelligence to optimize performance and personalize results. Some efforts have already been dedicated to PHY layer security, while privacy is still vastly under-considered, and very often perceived as a minor problem or even a nuisance on the base that “well-behaved” people have nothing to hide and should not bother about privacy, and only criminals and terrorists care to hide themselves and their personal information.

Privacy is instead an integral part of security, so that S&P should be tackled together, having in mind that breaching privacy always jeopardize also the security of people, which is the final concern and goal of preserving communications security. This work introduced the topic, discussing recent research on the subject and drafting open issues and research direction to achieve PHY layer S&P and to fully exploit the potential of ISAC without hampering people’s rights.

Funding: This research was partially supported at the University of Brescia by the project ISP5G+ (CUP D33C22001300002), part of the SERICS program (PE00000014) under the NRRP MUR program funded by the EU-NGEU and the project EMBRACE (CUP E63C22002070006) part of the RESTART program (PE000000001); at the University of Rome by the program SERICS (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 (Grant agreement No. 101078411).

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

References

1. Arisdakessian, S.; Wahab, O.A.; Mourad, A.; Otrók, H.; Guizani, M. A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology, and Explainable AI as Future Directions. *IEEE Internet of Things Journal* **2023**, *10*, 4059–4092.
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. *IEEE Symposium on Security and Privacy (SP)*, 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. *IEEE Conference on Computer Communications (INFOCOM)*, 2023, pp. 1–10.
4. Bartoletti, Stefania and Bianchi, Giuseppe and Orlando, Danilo and Palamà, Ivan and Blefari-Melazzi, Nicola. Location Security under Reference Signals' Spoofing Attacks: Threat Model and Bounds. *16th ACM International Conference on Availability, Reliability and Security (ARES)*, 2021.
5. Pecorella, T.; Brilli, L.; Mucchi, L. The Role of Physical Layer Security in IoT: A Novel Perspective. *MDPI Information* **2016**, *7*.
6. Chetty, K.; Smith, G.; Woodbridge, K. Through-the-Wall Sensing of Personnel Using Passive Bistatic WiFi Radar at Standoff Distances. *IEEE Trans. on Geoscience and Remote Sensing* **2012**, *50*, 1218–1226.
7. Adib, F.; Katabi, D. See through walls with WiFi! *ACM Int. Conf. of the Special Interest Group on Data Communication (SIGCOMM)*; , 2013; pp. 75–86.
8. Wang, X.; Gao, L.; Mao, S. CSI Phase Fingerprinting for Indoor Localization with a Deep Learning Approach. *Internet of Things Journal* **2016**, *3*, 1113–1123.
9. Di Renzo, M.; Debbah, M.; Phan-Huy, D.; et al.. Smart radio environments empowered by reconfigurable AI meta-surfaces: an idea whose time has come. *J Wireless Com Network* **2019**, 129.
10. Abbas, M.; Elhamshary, M.; Rizk, H.; Torki, M.; Youssef, M. WiDeep: WiFi-based Accurate and Robust Indoor Localization System using Deep Learning. *IEEE Int. Conf. on Pervasive Computing and Communications (PerCom)*; , 2019; pp. 1–10.
11. Lo Cigno, R.; Gringoli, F.; Cominelli, M.; Ghio, L. Integrating CSI Sensing in Wireless Networks: Challenges to Privacy and Countermeasures. *IEEE Network* **2022**, *36*, 174–180.
12. Schumann, R.; Li, F.; Grzegorzec, M. WiFi Sensing with Single-Antenna Devices for Ambient Assisted Living. *8th International Workshop on Sensor-Based Activity Recognition and Artificial Intelligence (iWOAR)*, 2023.
13. Mpitzopoulos, A.; Gavalas, D.; Konstantopoulos, C.; Pantziou, G. A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys & Tutorials* **2009**, *11*, 42–56.
14. Huo, Y.; Tian, Y.; Ma, L.; Cheng, X.; Jing, T. Jamming Strategies for Physical Layer Security. *IEEE Wireless Communications* **2018**, *25*, 148–153.
15. 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 of Things Journal* **2019**, *6*, 8169–8181.
16. Meghdadi, M.; Ozdemir, S.; Güler, I. A survey of wormhole-based attacks and their countermeasures in wireless sensor networks. *IETE technical review* **2014**, *28*, 89–102.
17. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. *IEEE communications surveys & tutorials* **2016**, *18*, 2027–2051.
18. Deshmukh-Bhosale, S.; Sonavane, S.S. A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things. *Procedia Manufacturing* **2019**, *32*, 840–847. *12th International Conference Interdisciplinarity in Engineering, INTER-ENG 2018, 4–5 October 2018, Targu Mures, Romania*.
19. Focarelli, G.; Zanini, S.; Bianchi, G.; Bartoletti, S. Physical Layer Threats to 5G Positioning: Impact on TOA-Based Methods. *2024 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2024, pp. 1–6.
20. Orlando, D.; Bartoletti, S.; Palamà, I.; Bianchi, G.; Blefari-Melazzi, N. Innovative Attack Detection Solutions for Wireless Networks With Application to Location Security. *IEEE Transactions on Wireless Communications* **2023**, *22*, 205–219.
21. 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, 2024; pp. 99–123.

22. Di Luzio, A.; Mei, A.; Stefa, J. Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests. 35th IEEE International Conference on Computer Communications (INFOCOM), 2016, pp. 1–9.
23. Tsiamitros, N.; Mahapatra, T.; Passalidis, I.; Kailashnath, K.; Pipelidis, G. Pedestrian Flow Identification and Occupancy Prediction for Indoor Areas. *Sensors* **2023**, *23*.
24. Yang, M.H.; Luo, J.N.; Vijayalakshmi, M.; Shalinie, S.M. Contactless Credit Cards Payment Fraud Protection by Ambient Authentication. *Sensors* **2022**, *22*.
25. Francillon, A.; Danev, B.; Capkun, S. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. Network and Distributed System Security Symposium (NDSS), 2011, pp. 1–16.
26. 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*.
27. Anliker, C.; Camurati, G.; Capkun, S. Time for Change: How Clocks Break UWB Secure Ranging. 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 19–36.
28. 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.
29. Ricciato, Fabio and Sciancalepore, Savio and Gringoli, Francesco and Facchi, Nicolò and Boggia, Gennaro. Position and Velocity Estimation of a Non-Cooperative Source From Asynchronous Packet Arrival Time Measurement. *IEEE Trans. on Mobile Computing* **2018**, *17*, 2166–2179.
30. 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*.
31. Wang, Y.; Wu, K.; Ni, L.M. WiFall: Device-Free Fall Detection by Wireless Networks. *IEEE Trans. on Mobile Computing* **2017**, *16*, 581–594.
32. Cai, C.; Deng, L.; Zheng, M.; Li, S. PILC: Passive Indoor Localization Based on Convolutional Neural Networks. IEEE Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS); , 2018; pp. 1–6.
33. Zheng, Y.; Zhang, Y.; Qian, K.; Zhang, G.; Liu, Y.; Wu, C.; Yang, Z. Zero-Effort Cross-Domain Gesture Recognition with Wi-Fi. Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services. ACM, 2019, MobiSys '19, p. 313–325.
34. 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 Transactions on Mobile Computing* **2023**, *22*, 6160–6175.
35. Du, R.; Hua, H.; Xie, H.; Song, X.; Lyu, Z.; Hu, M.; Narengerile.; Xin, Y.; McCann, S.; Montemurro, M.; Han, T.X.; Xu, J. An Overview on IEEE 802.11bf: WLAN Sensing. *IEEE Communications Surveys & Tutorials* **2024**.
36. Kaushik, A.; Singh, R.; Dayarathna, S.; Senanayake, R.; Di Renzo, M.; Dajer, M.; Ji, H.; Kim, Y.; Sciancalepore, V.; Zappone, A.; Shin, W. Toward Integrated Sensing and Communications for 6G: Key Enabling Technologies, Standardization, and Challenges. *IEEE Communications Standards Magazine* **2024**, *8*, 52–59.
37. 3GPP. NR; Physical channels and modulation. Technical Specification (TS) 38.211, 3rd Generation Partnership Project (3GPP), 2023. 18.0.0.
38. Qiao, Y.; Zhang, O.; Zhou, W.; Srinivasan, K.; Arora, A. PhyCloak: Obfuscating Sensing from Communication Signals. 13th USENIX Conf. on Networked Systems Design and Implementation (NSDI'16); , 2016; p. 685–699.
39. 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 Computer Networks* **2021**, *191*, 107970.
40. Cominelli, M.; Gringoli, F.; Lo Cigno, R. On the properties of device-free multi-point CSI localization and its obfuscation. *Elsevier Computer Communications* **2022**, *189*, 67–78.
41. Cominelli, M.; Gringoli, F.; Lo Cigno, R. AntiSense: Standard-compliant CSI obfuscation against unauthorized Wi-Fi sensing. *Elsevier Computer Communications* **2022**, *185*, 92–103.
42. Wang, Y.; Sun, L.; Du, Q.; Elakashlan, M. PriSense: Privacy-Preserving Wireless Sensing for Vital Signs Monitoring. *IEEE Wireless Communications Letters* **2024**.
43. Ghiro, L.; Cominelli, M.; Gringoli, F.; Lo Cigno, R. Wi-Fi Localization Obfuscation: An implementation in openwifi. *Computer Communications* **2023**, *205*, 1–13.
44. Jiao, X.; Liu, W.; Mehari, M.; Aslam, M.; Moerman, I. openwifi: a free and open-source IEEE802.11 SDR implementation on SoC. 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 2020, pp. 1–2.

45. Jiao, X.; Liu, W.; Mehari, M.; Thijs, H.; Muhammad, A. open-source IEEE802.11/Wi-Fi baseband chip/FPGA design, 2023.
46. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2004. Amendment 6: Medium Access Control (MAC) Security Enhancements.
47. Gringoli, F.; Klose, R.; Hollick, M.; Nahla, A. Making Wi-Fi Fit for the Tactile Internet: Low-Latency Wi-Fi Flooding Using Concurrent Transmissions. 2018 IEEE International Conference on Communications Workshops (ICC Workshops), 2018.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.