Integrating CSI Sensing in Wireless Networks: Challenges to Privacy and Countermeasures

Renato Lo Cigno, Francesco Gringoli, Marco Cominelli, Lorenzo Ghiro

***Abstract*—The path toward 6G is still long and blurred, but a few key points seems to be already decided: Integration of many different access networks; Adoption of massive MIMO technologies; Use of frequencies above current radio spectrum up to THz and beyond; Inclusion of Artificial Intelligence and Machine Learning in standard management and operations. One additional point that is less discussed, but seems key for success, is the advanced use of Channel State Information (CSI) both for equalization and decoding purposes and for sensing ones. CSI-based sensing promises a plethora of new applications and a quantum leap in service personalization and customer-centric network management. At the same time CSI analysis, being based on the physical characteristics of the propagated signal, poses novel threats to people's privacy and security: No software-based solution or cryptographic method above the physical layer can prevent the analysis of the CSI. The CSI analysis can reveal people's position or activity, allow tracking them, discover details on the environment that today can be seen only with cameras or radars. In this paper we discuss the current status of CSI-based sensing and present some technologies that can protect people's privacy and at the same time allow legitimate use of the information carried by the CSI to offer better services.**

I. Introduction

Operators are deploying 5G networks, and start experimenting with the novel technologies and architecture devised for it. Meanwhile, researchers and visionaries started foreseeing potential applications, requirements, and technologies beyond it: The 6th Generation (6G). The characteristics and scope of 6G are still under discussion, but several authors envision that this generation will not only be an access network for the Internet, but will finally substitute the Internet architecture promoting an entirely new communication model supporting holographic virtual presence, haptic and tactile services, and a globally interconnected system based mainly on integrated edge networking and computing to guarantee extremely low latency and reliability [1], [2]. The same authors, as many others, recognize the paramount importance of advanced Channel State Information (CSI) analysis to maintain the high throughput promises in wireless networks while the communication frequency skyrockets toward hundreds of GHz and beyond.

CSI is the information that, either explicitly with closed-loop feedback or implicitly analyzing preambles and pilot carriers, allows advanced channel equalization as well as Multiple Input Multiple Output (MIMO) operations. What is perhaps less known is that CSI information can be used to sense, or sound, the Electro-Magnetic (EM) environment to extract valuable information out of it, like people location and movements [3], [4]. The experimental work on CSI sensing has been done essentially on Wi-Fi system and indoor, thus one may think that this is a feature of Wi-Fi indoor communications. Indeed, the reason is only that experimenting with Wi-Fi is much easier than with Log Term Evolution (LTE) or 5th Generation (5G) technologies and indoor operation is also more amenable to repeatable setups for scientific research, but 5G-based experiments are under way [5], as there is no technical reason to believe that sensing the environment based on CSI information should not work outdoors or with technologies different from Wi-Fi.

The importance of sensing to deploy personal and context-aware services is pivot to most 6G designs and visions, where it is recognized that many, if not most of the services that go beyond infotainment, require automatic recognition of devices, device placement, and mutual positioning. CSI sensing is one of the few possibilities, together with Global Navigation Satellite System (GNSS) and active (meaning that the device cooperate with the infrastructure) Time-of-Flight (ToF) or Angle-of-Arrival (AoA) systems. CSI-based systems differentiate from the others because they are entirely passive, meaning that the device does not need to be cooperative, and can even work to sense, track, or measure people and objects that do not carry any communication device,

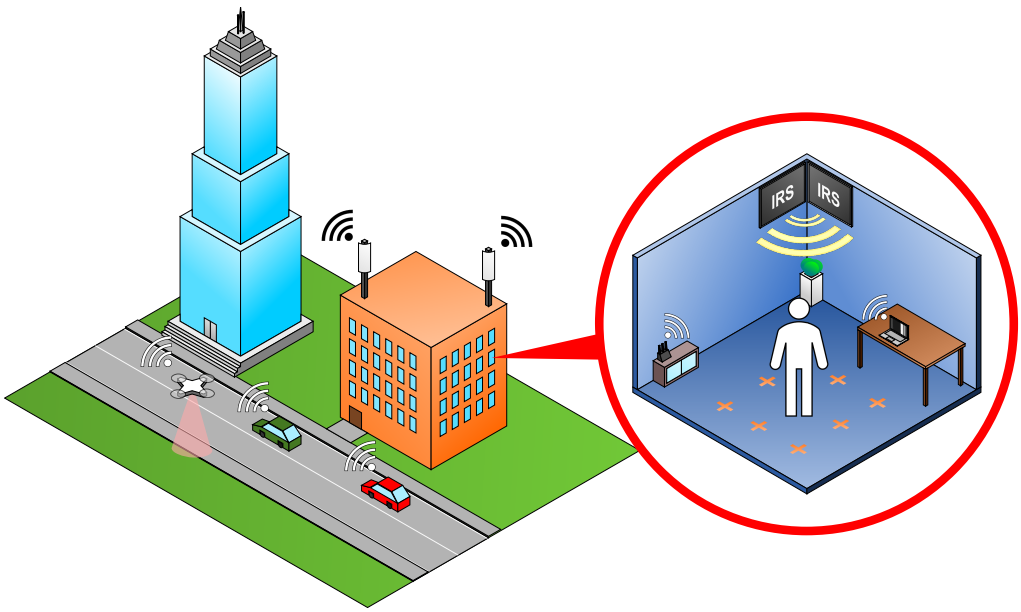

Figure 1: Possible sensing attacks can happen either outdoor or indoor using different wireless technologies.

making a perfect match with Artificial Intelligence (AI) based communications and Edge intelligence, as CSI analysis is normally based on advanced Machine Learning (ML) techniques.

This last property makes CSI sensing, and localization in particular, a significant threat to users' privacy and one that can be very difficult to counter with traditional means, because it is based on information leaks at the physical layer, and not data leaks from applications or software. The review [6] highlights how recent years have seen an explosion of *human sensing* works based on radio signal analysis and CSI in particular, witnessing the interest on the subject, but also the threats to privacy.

CSI-based sensing is founded on the use of ML techniques and AI that fingerprints the environment extracting characteristics that are otherwise difficult to identify, thus also recognizing the presence of an attack can be difficult. Fig. 1 depicts a typical situation, where the whereabouts of people are constantly tracked by a non-authorized system. Similarly, CSI can be used to fingerprint devices, tracking them even in presence of anonymization techniques, once more jeopardizing users' privacy and security, e.g., in vehicular and cooperative driving applications.

A. Contribution and Related Works

Very few works so far have tackled the problem of obfuscating the CSI while preserving communication capabilities. On the one hand, this is probably due to the excitement for the new possibilities that CSI sensing opens, leading researchers and industry to work on improving sensing performance; on the other hand, there is generally little awareness of physical layer privacy threats. Some works deal with the information leakage through hardware imperfections for device identification, but the idea of leaking personal information through the environment has been hardly considered so far. However, the interest on this subject is rising.

We split the discussion between techniques that can counter only passive attacks and those that can also counter active ones (see Sect. II for the definition of passive and active attacks). In general, defense from passive attacks requires some sort of signal manipulation to conceal personal information. CSI obfuscation in this sense can be achieved by training adversarial neural networks [7] that use a database of real CSI data to generate "fake" signals. This approach is very interesting but cannot work on-line (since the CSI is computed per-packet in realtime), and the problem of preserving communication performance is not explicitly addressed in the paper. A different approach to CSI obfuscation—but with a focus also on standard-compatibility and communication performance—is described in [8]–[10], in which different flavors of random CSI distortions are proposed and analyzed. The standard-compliance is proven by a working implementation of the proposed system in [10].

Protection also against active attacks requires the use of an additional device, as foreseen in [11], [12]. The approach in these works is similar, though not identical, and in both cases the idea is to mimic the presence of an Intelligent Reflective Surface (IRS) that adds a significant "variable" reflection that changes the CSI over time, thus preventing classification-based sensing. In both cases the presence of a dominant reflection improves communication performance because the reflecting device is active, thus adding energy to the transmitted signal. The implementation of the obfuscator in [11] is based on piece-wise linear delays, thus the obfuscation can be easily inverted by an attacker observing the system, while [12] uses a pseudo-random Markov process that is much harder to invert.

The contribution of this paper is the discussion of how anti-sensing techniques are possible, presenting a few countermeasures we are experimenting with that we consider feasible and standard-compliant, including the use of IRSs, which can modify the environment to improve communications, sensing, and privacy.

II. CSI Sensing

CSI sensing is based on the analysis of the EM field of a received signal, based on the a-priori knowledge of some parts of the transmitted signal itself, either preambles, pilots, or known symbols. These are described in the standard of protocols, thus they are well known to anyone. After the initial analysis, the sensing can be supported during the transmission also on the signal carrying user data, even if encrypted. The operation of CSI sensing is indeed similar to channel equalization: A-priori knowledge of some symbols allows estimating the distortion of the signal operated by the propagation environment and to compensate it; when the compensation is good enough, reception can start, and successfully decoded data can be be used to improve channel equalization exploiting also standard transmission and not only preambles and pilots. It is the use of this information that changes between equalization and sensing: Compensate the signal distortion in the former, measuring some ambient characteristics in the latter.

To fix ideas consider Fig. 2 that reports the amplitude and phase (i.e., the CSI) of the signal of ten 802.11ac frames collected changing the "environment": Environment 1 is a room with a person moving inside, and Environment 2 is the same room empty. What is immediately clear is that the two traces are very different, while all the CSI collected in the same environment are remarkably similar. The amplitude of each subcarrier changes, and the phase changes too, with characteristic jumps that modify the linear variation with the subcarrier number, i.e., with frequency. The jumps are always in the same places, independently from the linear change of a specific frame, thus, just like the amplitude, they carry information on the environment and can be fingerprinted.

The signal at any receiving device in the frequency domain, $S_R(f,t)$, is the product of the transmitted signal spectrum $S_T(f,t)$ with the so-called channel response $H(f,t)$, which includes frequency-dependent attenuation and phase rotations, as described by Eq. (1).

$$S_R(f,t) = S_T(f,t) \times H(f,t) \tag{1}$$

Notice that, contrary to standard theory taught in communication classes, we have explicitly left in the description the dependency on time of all spectra. Dropping the dependency on time can be done only if the system is stationary, an approximation legitimate in communication theory; however, this dependency is exactly what makes CSI-based sensing feasible. The information on the environment is embedded in $H(f,t)$, and a sensing device extracts it.

How the environment information is embedded into the signals by propagation is well known in its general principles, but still unknown in its details, meaning that the community still lacks a model that, given a transmitter position and antenna and the description of the environment itself, yields the expected CSI at a receiver.

The general principles lie in Maxwell equations that describe the evolution of the EM field and lead to the plethora of advances in the theory of propagation and communication, these latter enabling all the astounding results we observe today: from telecommunications to astronomy, from medical imaging (CT scan, fRMI, ...) to satellite earth observation and so forth.

The specific and detailed influence of the environment on the propagated signal is instead still too complex to be effectively modeled. Ray tracing techniques require too many components in a complex environment; other techniques as percolation theory and others are also too complex or not fully

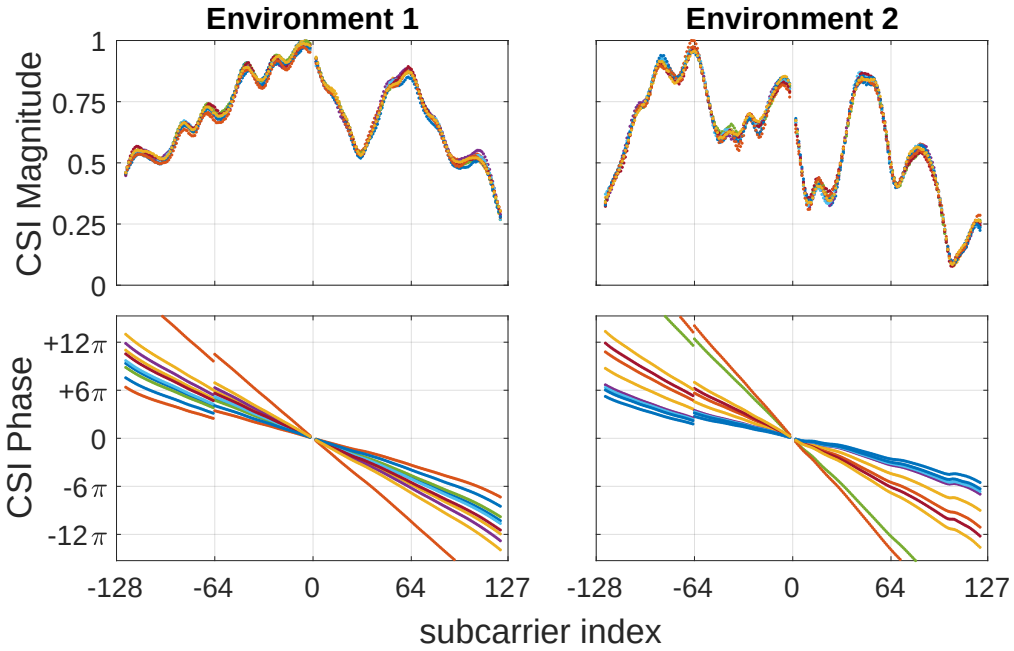

Figure 2: Plots of the CSI amplitude (upper row, in normalized units) and unwrapped phase (lower row, in radians) versus the subcarrier number for ten 802.11ac 80-MHz frames (256 subcarriers) collected in two different environments.

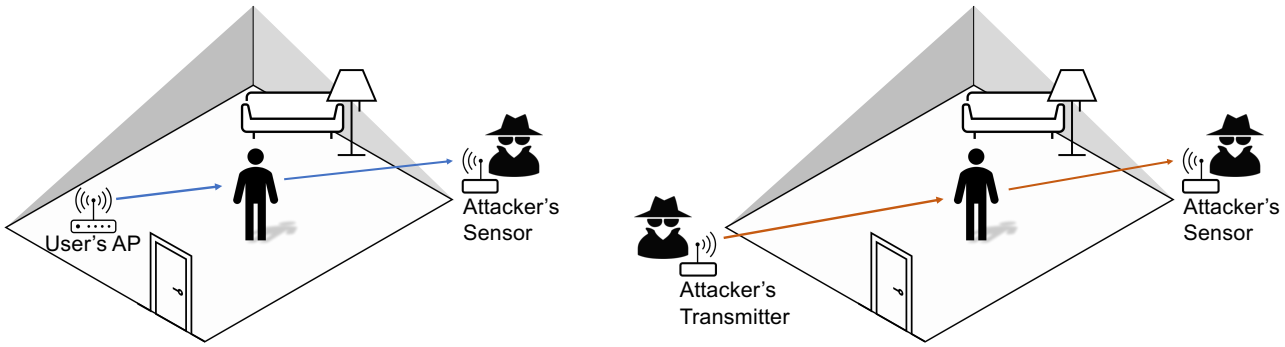

Figure 3: Sensing attacks can be either passive (on the left), meaning that the attacker controls only one or more sensing receivers, or active (on the right), meaning that the attacker is able to also inject ad-hoc traffic controlling also one or more transmitters.

developed to yield explicit results. The use of Neural Network (NN) and Convolutional Neural Network (CNN) in particular, but also Reinforcement Learning and several other AI techniques, have instead given very good results, especially for localization, gesture recognition (including identifying falls of elderly people), and many other applications.

A. *Threat Models and Privacy Issues*

All of the applications discussed above are useful, but they also pose a threat to people privacy and security if used with malicious intent and without authorization. In particular, the fact that the relevant information is embedded in $H(f,t)$ at the physical layer prevents any defense based on software, protocols, or cryptography, as the information is available to anyone who can intercept the signal $S_R(f,t)$. This is the key problem we address in this paper.

With reference to Fig. 1, we can distinguish different types of attacks, and specifically attacks whose target is a device (and the person carrying it) and those that do not require a device, but sense directly the person, even if she/he do not carry any device. We concentrate on these later, which can be classified as passive or active and are described in Fig. 3.

- **Passive attacks** are carried out using only the standard and legitimate traffic transmitted by base stations. The attacker controls only one or more sensing device placed near the attacked area. The only requirement is that the transmitter must be fixed (as Access Point (AP) and base stations normally are); its position does not need to be known, but if the transmitter or the sensing device change position then $H(f,t)$ changes as the transfer function depends on the transmitter and receiver position.
- **Active attacks** are implemented injecting additional, ad-hoc traffic or generic signals that resemble traffic even if they do not carry user information. In this case the attacker must control also one or more transmitters, also close to the attacked area.

We highlight that the sensing devices are not necessarily the information receivers, and they do not need to be in the same position. Furthermore, if more than one sensing device is available, the sensing is normally more accurate and reliable [9].

The training of the sensing devices can be done in many different ways, which also depend on the specific sensing attack. For instance, if the goal is only to know if someone is inside a room, then the device can be trained to recognize an empty room, fingerprinting the characteristics of $H(f,t)$ of the empty room, and during the attack any CSI that does not match the empty room fingerprint is taken as an indication that there is someone in the room. Training to identify the exact position of a person or even an estimate of the (x,y) coordinates can be more complex, but it is feasible as shown in the literature.

B. The Proposed Solution

Seeking to protect or remove information embedded by the environment in a physical EM signal seems a desperate task, as the signal can be analyzed by anyone receiving it and the information is in the analog domain. Thus, the solution we propose is blurring or diluting this information in such a way that any analysis an attacker can do would yield a response that is no better than a random guess on the information itself. For instance if the sensing is meant to recognize gestures and the system has been trained to distinguish *standing*, *walking*, *sitting*, and *lying* any attack should result in an accuracy of the estimate (the probability of correct answer) around 25%. We call this process of CSI blurring *obfuscation*, and we motivate and describe it in the next section.

III. CSI Obfuscation

As noted, completely removing the information embedded in $H(f,t)$ is not possible. However, we can blur $H(f,t)$ so that it is not usable by an attacker.

A. Motivation for Obfuscation and its Principles

The information that enables sensing is in some sense "collected" from the environment by the signal while it propagates from the transmitter to the receiver, thus removing the information means in some sense removing the environment itself, or at least the part of the environment that generates the information we want to hide. If the information, for instance, is related to a person, then removing the person from the environment is not an option, and even endowing him/her with the cloak of (EM) invisibility would not suffice. It is not enough that a person does not reflect or scatter the signal, because the absence of reflections of the signal absorbed by the person is an indication of her/his presence, and as far as we know it can be enough for a good algorithm to locate the person and identify his/her gestures.

Thus, we are left with the second option: blur the information to the point that the *mutual information* carried by the signal from the environment to the sensing devices is either null or unusable. We talk now of mutual information in the sense of information theory, and not of information as a general term or the semantics associated with it. Removing the mutual information does not imply that the information does not exist, but that it cannot be retrieved by the receiver, in our case the sensing device. In other words the information is *obfuscated*. Ideally, this obfuscation should also be removable for legitimate use, but we discuss this later.

The key idea to obfuscate the sensing information can be formalized by Eq. (2), where the additional multiplicative term $O(f,t)$ is added to Eq. (1).

$$S_R(f,t) = S_T(f,t) \times O(f,t) \times H(f,t) \quad (2)$$

Observing Eq. (2) it is clear that, from the perspective of the receiver, the product $O(f,t) \times H(f,t)$ looks exactly like another channel response, and it cannot

in principle separate $O(f,t)$ from $H(f,t)$, at least if $O(f,t)$ is well crafted.

Thus the problem of anti-sensing becomes the design of an appropriate obfuscation function $O(f,t)$ with the following properties:

1) $O(f,t) \times H(f,t)$ should be indistinguishable from any physically realizable channel response, ideally it should be indistinguishable from the channel response of the environment where it is applied;
2) The obfuscated signal at the legitimate information receiver must not jeopardize the transmission performance, as communication is the principal service of the system;
3) $O(f,t)$ should be non-invertible, at least not within a reasonable time and with a reasonable amount of computing power; this means that an attacker should not be able to reconstruct $O(f,t)$, not even observing it for a very long period of time T, with multiple observation points, and huge computational capabilities.

At the state of the art it is not known if these three requirements can be fully achieved, and this mainly for lack of foundational results on the subject. The next two subsections describe two possible realizations of $O(f,t)$, the first one that can protect users from passive attacks only, and the second one that can instead protect users also from active attacks. Next, we present some initial experimental results obtained on 802.11ac systems.

B. Transmission side CSI Obfuscation

The first possibility to implement $O(f,t)$ is its integration into transmitters. The function should modify the transmitted signal in such a way that (at the receiver) it does not carry useful information on the environment itself, or at least on the part of the environment that we want to protect.

A relatively easy solution is the implementation of $O(f,t)$ as a frequency and time dependent multiplier that follows an appropriate random pattern. The pattern should be casual enough to confound the sensing algorithm, but not so random (as white noise for instance) to allow filtering it out with a long observation. Furthermore, the amplitude and phase pattern of the multiplier should not prevent the correct reception and equalization of the signal.

This solution is not difficult to implement, and we have realized a few prototypes, both using Matlab emulation plus a powerful Software Defined Radio (SDR) module and directly into the openwifi system[1]; however, it has the drawback that it works only against passive attacks, because if the transmitter is controlled by the attacker, then the obfuscation cannot be applied. Indeed, such a solution is technologically mature and it can easily be embedded into standards, possibly with a proper protocol that allows sensing by legitimate actors by inverting the $O(f,t)$ function. We presented a working prototype of the system and a discussion on a protocol to allow legitimate sensing in presence of obfuscation in [10]. The implementation only requires some little additional area on the original FPGA design and does not require transmitting any additional information.

C. IRS Based Environment Modification

The second possibility is the realization of $O(f,t)$ as an environment modifier. Modification of the environment with IRSs to enhance transmission performance is indeed being considered by researcher (see for instance [13]). The same principle can be used to modify the channel response with an appropriate obfuscating function. Fig. 1 depicts an IRS placed in the corner of the room; indeed, they can be multiple small patches distributed in the ambient, indoors or outdoors, coordinated to produce the desired response while remaining aesthetically in-conspicuous. This solution protects the ambient and the people in it both from passive and from active attacks. Actually, fusing in the same IRS the functions to improve performance and the privacy-protecting ones looks like the classical win-win solution, as results we present later show.

An intelligent reflector, controlled by appropriate preambles and pilots in the transmitted signal, can introduce signal reflections with random sub-symbol delays. These reflections blur the environment information, because they make the CSI time varying even if the environment does not change. At the same time, as we have shown in [12] and was also studied in [11]., they can improve the communication performance in two different ways: First, since these surfaces are active, they introduce dominant reflections that help the data receiver to properly equalize the channel –and this is an intrinsic, passive

[1]openwifi is an open project implementing 802.11 stack in Linux plus Field Programmable Gate Array (FPGA), the project is on GitHub: https://github.com/open-sdr/openwifi

property; second, if a proper protocol is implemented between the communications system and the legitimate receivers, these latter can fully de-obfuscate the signal, thus exploiting the additional energy that IRSs inject in the channel, further improving communication performance.

Unfortunately, while the implementation of the transmitter-based obfuscation is technologically feasible, programmable IRS as the one depicted are still not available. We implemented a prototype with Matlab emulation and the use of two SDR for 802.11ac systems: One playing the transmitter role and the other one the role of the IRS providing a Proof-of-Concept of the system [12], a similar proof of concept was presented in [11].

IV. Examples based on Wi-Fi

Experimenting these ideas with 6G technologies is obviously impossible since they are still not defined. Also 5G experimentation is very difficult, due to the complexity of extracting CSI information from 5G chips. Instead, thanks to the work in [14] it is possible to extract the CSI for manipulation different from the equalization for Wi-Fi systems. We consider 802.11ac with 80 MHz channel (256 subcarriers), and we have implemented both the transmitter side obfuscation technique and the IRS emulation, and we have experimented both the anti-sensing properties and the communication performance in many configurations, using as sensing technique a CNN-based localization fingerprinting derived from [15] that can localize people even if they do not wear or carry any communication device.

To grasp the intuition of why sensing, and in particular localization, is possible and how the proposed countermeasures work, let us analyze Fig. 4. The figure reports the heatmap (yellow means high power, blue low power) of the CSI measured at a generic device, the x axis is the number of transmitted frames, thus it represents time as framed are transmitted sequentially. The left column refers to one ambient, for instance a person in a given position, and the other one to another ambient, for instance an empty room or a different position of the person. It is clear that the CSI remains constant in time (first row) and clearly different in a different environment. Both obfuscation techniques (second and third row) randomize the CSI, changing it from one frame to another, making it impossible to fingerprint a situation, and hence to sense anything in the ambient. IRS-based obfuscation looks less random than transmission side one, but it is still effective in preventing localization (see Tab. I), furthermore it is based on a single emulated IRS: a very simple configuration.

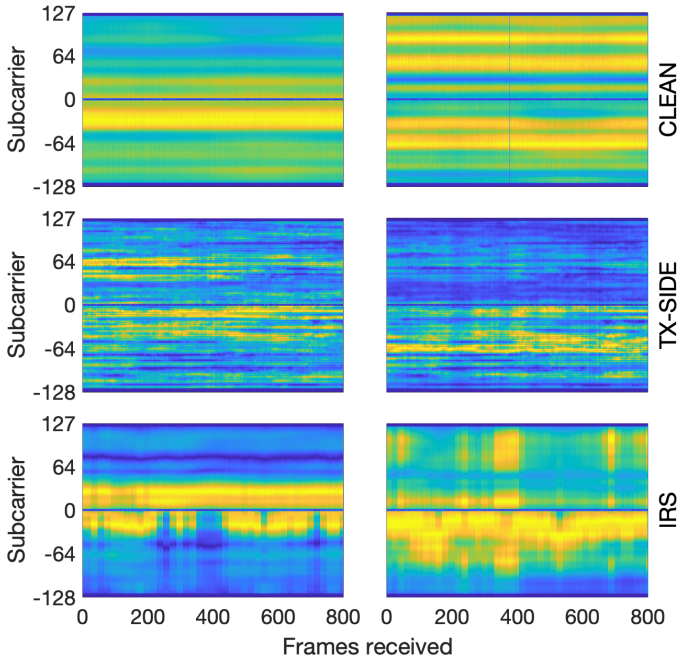

Figure 4: Heatmap of the CSI of 800 802.11ac frames with 256 subcarriers. The first row shows how the CSI characterizes two different ambient, the second and third row how transmission-side and IRS-based obfuscation randomize the CSI making it impossible to fingerprint the ambient.

Position	CLEAN	SC1	SC2
1	100%	42%	9%
2	100%	1%	0%
3	100%	0%	0%
4	94%	2%	0%
5	97%	62%	100%
6	80%	15%	3%
7	89%	36%	22%
8	100%	2%	0%
Average	**95%**	**20%**	**17%**

Table I: Accuracy of localization in one of 8 possible locations in the room; a random guess yields 12.5%.

Out of the many configurations and experiments we have run, we have selected two sets of results presented in Tab. I and Fig. 5, the interested reader can find details and further results in [8], [9], [12] where we also report results for complex

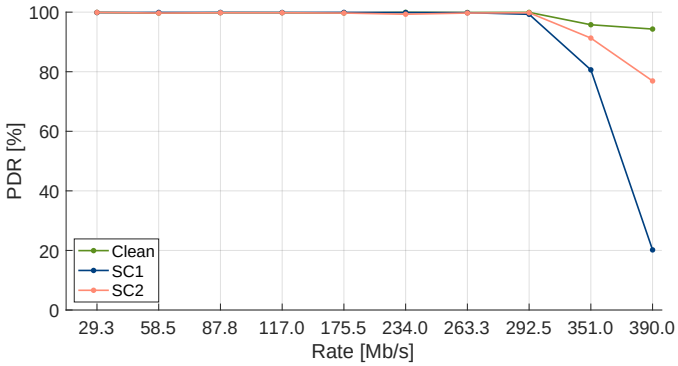

Figure 5: Packet Delivery Rate (PDR) without obfuscation (Clean) and with obfuscation on SC1 and SC2.

multi sensing-device attacks, and develop an initial theory of sensing obfuscation. The two scenarios we consider are one passive and one active, both indoor, with experiments run in our laboratory in Brescia, a 7m $\times$ 7m room with a fairly complex EM environment.

The first scenario, SC1, is a passive attack where the attacker has placed a single sensing device in the room (see Fig. 1 for reference), and exploits the transmissions of the local AP or base station to fingerprint the position of a victim, who moves standing in 8 possible locations. The countermeasure in this case is the one described in Sect. III-B. The second scenario, SC2, is an active and passive attack, where the attacker has placed the sensing device outside the room, assuming he does not have easy access to it, exploits the AP transmissions and additionally also ad-hoc transmissions from another device placed outside the room. The countermeasure in this case is IRS-based as described in Sect. III-C.

Tab. I reports the localization accuracy; we consider 8 possible positions, thus a random guess yields a 12.5% accuracy. It is clear that without protection, labeled CLEAN, the localization accuracy is very good, while the obfuscation systems we propose are both very efficient, bringing the average accuracy quite close to a random guess, and in any case low enough to be usable for any purpose. We observe a different behavior between transmission-side and IRS based obfuscation. In the first case, the accuracy is in general low for all positions (but position 5), while IRS obfuscation tends to concentrate the estimates always on position 5. This is a general trend we have observed, which is probably rooted in the different impact on the CSI and also on the fact that the localization device makes a classification, hence it takes a decision in any case: The fact that the accuracy in one position is high, is due to the fact that the localization system decides with preference for this location, but the result is indeed useless for an attack.

Fig. 5 reports instead the PDR as a function of the physical transmission speed without the obfuscation and with the two obfuscation methods we described, SC1 and SC2 respectively. The transmission side obfuscation (SC1) affect transmissions at the highest bit rates, while IRS-based obfuscation does almost not impact transmission performance as expected; in this case the reason is that the IRS emulation actually injects a second copy of the frame on the channel with a random delay, creating an environement that resembles a simple one with a 2-ray approximation. As discussed a true active IRS should even improve the performance.

Both the localization accuracy and the PDR reported are the average over many experiments, accounting for several thousands packets transmitted. Results may change from one experiment to another, but the insight remains substantially the same: Anti-sensing techniques to protect people's privacy are possible and effective, and they do not affect transmission performance significantly.

V. Challenges and The Work Ahead

The success of a novel technology requires that people trust it, and this is valid also for joint communication and sensing in the path toward 6G: if privacy concerns prevail trust may fail. The stakes are extremely high: Should the trust of the people fail, the evolution of advanced mobile telecommunications can be hampered.

The technical challenge is the inclusion of privacy provisioning within the technology itself, giving people the freedom to choose the amount of information they want the system to use to provide the service and, at the same time, prevent any information leakage to attackers or external entities.

The work toward this ambitious goal include several lines of research. First, we need better insight and understanding of the information that the environment embeds into signals. Traditionally, networking and telecommunication professionals have considered the fingerprint of the environment on signals just as an impairment to be removed to

improve transmission performance, but AI advances on the one hand and IRS studies on the other hand started to treat the environment more as a potential friend than a foe. Now the goal becomes understanding this friend to make it a trustable and dependable one.

Next, we should search for methodologies that allow either removing the information a signal carries on specific features of the EM environment, or, more likely, blurring them through obfuscation so that only legitimate use is possible.

Third, we have to learn how to use communication-based sensing to build services that help the advancement of society respecting people's privacy and rights. Examples range from safety in vehicular traffic, reducing accidents and injuries, to fine grained positioning for personal services, to anti-intrusion systems, elderly care, and much more. We are confident that privacy-preserving communication and sensing systems will be part of future mobile networks.

ACKNOWLEDGMENTS

Work partially funded by GÉANT Educational Activities and Services Agreement ref. SER-21-142, Project "Design and Implementation of an 802.11 Privacy Preserving Sub-Layer (DI-P^{2}SL)" and by the European Commission under the Horizon 2020 Orchestration and Reconfiguration Control Architecture – ORCA project (grant no. 732174) Open Call 3 "Experimental analysis of CSI based anti-sensing techniques – CSI-MURDER" experiment.

Additional information on this subject and the patrons sponsoring it can be found from our website https://ans.unibs.it.

REFERENCES

[1] H. Tataria et al., "6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities," *Proceedings of the IEEE*, vol. 109, no. 7, pp. 1166–1199, Mar. 2021.

[2] W. Saad et al., "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, 2020.

[3] F. Adib and D. Katabi, "See through walls with WiFi!" In *Conf. of the Special Interest Group on Data Communication (SIGCOMM)*, Hong Kong, Aug. 2013: ACM, Aug. 2013, pp. 75–86.

[4] J. Ding and Y. Wang, "WiFi CSI-Based Human Activity Recognition Using Deep Recurrent Neural Network," *IEEE Access*, vol. 7, pp. 174 257–174 269, Dec. 2019.

[5] A. Ashleibta et al., "5G-enabled contactless multi-user presence and activity detection for independent assisted living," *Nature Scientific Reports*, vol. 11, no. 17590, Sep. 2021.

[6] I. Nirmal et al., "Deep Learning for Radio-Based Human Sensing: Recent Advances and Future Directions," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 995–1019, 2021.

[7] W. Zhang et al., "Understanding and Modeling of WiFi Signal-Based Indoor Privacy Protection," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2000–2010, 2021.

[8] M. Cominelli et al., "IEEE 802.11 CSI randomization to preserve location privacy: An empirical evaluation in different scenarios," *Elsevier Computer Networks*, vol. 191, no. 22, p. 107 970, May 2021.

[9] M. Cominelli et al., "On the properties of device-free multi-point CSI localization and its obfuscation," *Elsevier Computer Communications*, vol. 189, pp. 67–78, May 2022.

[10] L. Ghiro et al., "On the Implementation of Location Obfuscation in openwifi and Its Performance," in *20th IEEE Mediterranean Communication and Computer Networking Conference (MedComNet)*, Paphos, Cyprus, Jun. 2022, pp. 1–8.

[11] Y. Qiao et al., "PhyCloak: Obfuscating Sensing from Communication Signals," in *13th USENIX Conf. on Networked Systems Design and Implementation (NSDI'16)*, Santa Clara, CA, USA, Mar. 2016, pp. 685–699.

[12] M. Cominelli et al., "AntiSense: Standard-compliant CSI obfuscation against unauthorized Wi-Fi sensing," *Elsevier Computer Communications*, vol. 185, pp. 92–103, Mar. 2022.

[13] M. Di Renzo et al., "Smart radio environments empowered by reconfigurable AI meta-surfaces: an idea whose time has come," *J Wireless Com Network*, vol. 129, 2019.

[14] F. Gringoli et al., "Free your CSI: A channel state information extraction platform for modern Wi-Fi chipsets," in *13th Int. Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH '19)*, Los Cabos, Mexico, Oct. 2019: ACM, 2019, pp. 21–28.

[15] C. Cai et al., "PILC: Passive Indoor Localization Based on Convolutional Neural Networks," in *Ubiquitous Positioning, Indoor Navigation and Location-Based Services (UPINLBS)*, Wuhan, China, Mar. 2018, pp. 1–6.

Renato Lo Cigno is Full Professor at the University of Brescia, Italy. He received a degree in Electronic Engineering with a specialization in Telecommunications from Politecnico di Torino. In 1998/9, he was Visiting Scholar at UCLA; from 2002 to 2019 he was with the University of Trento, Italy. Renato Lo Cigno has been General Chair of IEEE P2P, ACM WMASH and IEEE WONS, TPC Chair of IEEE VNC, ACM WMASH, IEEE MedComNEt, and IEEE WONS. He is Associate Editor for IEEE/ACM TNET. His current research interests are in performance evaluation of wired and wireless networks, modeling and simulation techniques, and networked systems in general. Renato Lo Cigno is senior member of IEEE and ACM.

Francesco Gringoli is Full Professor of Telecommunications at the Dept. of Information Engineering at the University of Brescia. He received the Laurea degree in telecommunications engineering from the University of Padua, Italy, in 1998 and the Ph.D. degree in information engineering from the University of Brescia, Italy, in 2002. His research interests include security assessment, performance evaluation and medium access control in Wireless LANs.

Marco Cominelli is a Ph.D. student in the Dept. of Information Engineering at the University of Brescia, Italy. He received a Laurea degree (BSc) in Electronics Engineering in 2016 and a Laurea Magistrale degree (MSc) in Communication Technologies and Multimedia in 2019, both from the University of Brescia. He has also been a visiting research student at The University of Edinburgh and at Northeastern University. His research activity is currently focused on performance and security evaluation of different environment sensing techniques using wireless technologies.

Lorenzo Ghiro is a post-doc researcher at the Dept. of Information Engineering at the University of Brescia, Italy. He received a PhD degree in Information and Communication Technology from the University of Trento, Italy and has been a visiting Scholar at the Northeastern University of Boston, MA, USA. His research interests include Distributed Systems & Algorithms, Blockchain technologies, Wireless and Vehicular Networks.