Wi-Fi sensing: Risk and Potential on IT Security and Privacy

Osenstätter, Kilian
University of applied Science
Munich, Germany
osenstae@hm.edu

***Abstract*—As wireless networks increasingly supplant stationary network infrastructures, and with the burgeoning proliferation of devices capable of wireless communication, the significance of Wi-Fi sensing and its foundational technologies has become paramount. This study delves into the ramifications of Wi-Fi sensing on privacy and IT security within various environments, drawing on literature research to highlight both the impacts, potential and further mitigation strategies. Notably, Wi-Fi sensing is capable of detecting the presence of individuals and even discerning keyboard inputs, opening new avenues for future applications and technological advancements. This work aims to offer a comprehensive overview of the fundamental principles of Wi-Fi sensing, juxtaposed with detailed analytical methodologies, thereby contributing to a deeper understanding of its capabilities and implications.**

***Index Terms*—channel state information (CSI), Wi-Fi sensing, IT security, privacy, recognition**

I. Introduction

Nowadays, Wi-Fi is seen as a natural means of communication in public and private spheres. In this context, the Wi-Fi Alliance according as Du et al. [1] shows a steady growth in the use of Wi-Fi enabled devices. A rapid development and innovation cycles see new opportunities via Internet of Things (IoT) to Artificial intelligence of Things (AIoT) as Yang et al. in [2] describes. The advancements in Wi-Fi sensing technology, as evidenced by current research, suggest a diminishing demarcation between what was once considered science fiction and reality. Even if these boundaries seem to be disappearing, it is all the more important to analyze and ask for new technologies for both potentials and risks. This paper gives an overview of the current state of research in the field of Wi-Fi sensing and the resulting challenges, risks and potential for IT security and privacy.

II. Fundamentals

The following chapter is intended to explain the fundamental concepts of Wi-Fi sensing and put them into context. Different areas of application are shown and a general procedure is explained.

A. Usage of Wi-Fi Sensing

Everyone knows about Wi-Fi usage on Routers, mobile phones or Access Points (APs) in company's or in private areas. The bandwidth and high range of Wi-Fi in local area networks is predestined for buildings and not only restricted to rooms Du et al. [1]. So Wi-Fi sensing based on Channel state informations (CSIs) can be used for recognizing and tracking people or gathering data of there behavior Giro et al. [3]. Furthermore, applications such as fall detection as Du et al. [1] and Nakamur et al. [4] shows are also possible. CSIs allow a fine-grained measure of physical environmental changes in case of movement. This can be used in particular in the smart home sector or for monitoring systems Yang et al. [2, S. 3]. To understand how this works, there is a need to go back on models like Received Signal Strength Indicator (RSSI). In simplified terms, RSSI can be used to determine the distance between transmitter (Tx) and receiver (Rx) Du et al. [1]. In order to differentiate between the subjects, as in the related work by Yang et al. [2], it is necessary to distinguish whether the person is carrying a Wi-Fi device or not. For this purpose, neural networks (NN) and machine learning (ML) i.e were used by Cominelli et al. [5] and Liu et al. [6] to create a unique CSI fingerprint of persons, devices or environments. In addition, following the widespread use of artificial intelligence (AI), sensing methods based on this can play an important role in the future Ghiro et al. [3].

B. Functionality

On the first step to understand what CSIs do is to explain how Wi-Fi amplitudes are sent and received and via which paths the beams reach the receiver, as well as this can be used as state information. However, the reason is that wireless amplitudes how Yang et al. [2, p. 3] explained are reflected, scattered or refracted by objects in the environment on that way from Tx to Rx [2]. These properties change the behavior of Wi-Fi signals, i.e. the way they propagate in space, and thus also the phase and polarization of the amplitudes [2, p. 4]. For this reason, paths from the transmitter to the receiver change and a so-called multi-path construct occurs. However, this results in a certain delay, shift and loss of individual frequencies, also known as frequency-selective fading. This is then understood as CFR [2, p. 12]. For the characterization of individual paths, the channel is modulated by a linear-time filter, which can then be referred to as the channel impulse response (CIR) [2, p. 12]. However, the direct path, without multi path between Tx and Rx can be identified as Line-of-Sight (LoS) [2, p. 13]. The steps for performing various Wi-Fi

sensing methods can be generally divided into the following sections as Ma et al. shows in [7].

1) Processing: In a nutshell, in this section addition to noise reduction, signal transformations and extractions are carried out. Various techniques are used to enhance the signal quality and usability and eliminate discarded and interfering frequencies. [7]

2) Algorithm: In order to be able to interpret the interference-free CSI, algorithms must be used. As Ma et al. [7] described, models like Angle of Arrival (AoA) and Time of Flight (ToF) are often used. Various algorithms can be used for the representation and calculation, such as Cominelli et al. [5], Yang et al. [2] or Du et al. [1] and will be shown in the further course of the work.

3) Application: This is followed by the interpretation of the displayed values and parameters for a certain application. As already mentioned, the application could be for fall detection or tracking [1].

C. Historical view

After the number of devices with a Wi-Fi module increased significantly, the first Wireless LAN standard was engaged 1991, published in 1997 and implementations follows on 1999 how Banerji and Chowdhury [8] shows. Equivalently, the bandwidth and transmission rate of published standards is constantly increasing. The increased interest in Wi-Fi sensing became known with the dawn of this century as Ma et al. describes in [7]. If various wireless technics and their applications such as RFID or Bluetooth are compared as Du et al. [1] shows, Wi-Fi sensing is characterized by a wide range of applications and low costs. Also, no additional devices are required.

III. Methodology

The following chapter describes the semi-systematic scientific process described by Snyder [9] and the techniques used to collate the literature. It also provides an overview of the data sources used for this purpose.

A. Literature Research

First of all there was the goal to get an overview of the topic in order to gain a general understanding of Wi-Fi sensing and the potential issue at hand. After the search for basic literature [2] was completed, the search for deeper literature was expanded and keywords such as Wi-Fi-sensing, privacy, recognizing, IT security and channel state information were already included. Two different search strings were used from the keywords supplied. In order to limit the searches as much as possible, these were linked with AND operators.

1) Search String one: [Full Text: Wi-Fi sensing] AND [Full Text: recognizing] AND [Full Text: privacy] AND [All: channel state information] AND [E-Publication Date: (01/01/2010 TO 12/31/2023)]

2) Search String two: [Full Text: channel state information] AND [Full Text: attack] AND [All: it-security] AND [All: Wi-Fi] AND [E-Publication Date: (01/01/2010 TO 12/31/2023)].
As already shown, the strings were arranged according to the superordinate group, i.e. the superordinate theme, and then in descending order of influence on the research question Snyder [9]. What are the risks and potentials of Wi-Fi-based sensing technologies in terms of privacy and IT security?
This divides them into two meta-groups. In particular, a survey of Ma et al. [7] was used as related work for the assessment of current new technologies. Several databases such as IEEE Explore, Science Direct, MDPI and ACM were used. The ACM database returned the most results for all queries. In addition, Google Scholar was used to find papers that provided additions to already selected literature. The period was limited to 2010-2023 in order to include only the most recent papers. In order to check papers for their suitability for the research topic, the title was read. Following this, the abstract and conclusion were worked through in each case. The distinction between the potential for IT security of wireless-based networks and the risks for privacy was based on a differentiation between the two topics. Which is why there were different requirements for the search terms. Once key terms and findings had been identified, these were examined more closely and important passages were highlighted. Essential terms were then recorded in a mind map. The mind map was used to structure the paper. This was particularly helpful for graphically displaying links and references to related topics. In the final selection of papers, attention was paid to the historical development of different methods. When the preparation of the literature research was completed, it became clear that privacy topics in particular were being considered, which is why this perspective will be more emphasized.

B. Limitations

In Addition, this work only focuses on privacy and IT security and does not provide a comprehensive overview of other applications. One limitation of this study was the inability to access preliminary drafts from the IEEE Wi-Fi Task Group, precluding the direct incorporation of information on emerging 802.11bf Enhancements for Wi-Fi sensing. Additionally, the research scope was deliberately narrowed to papers that empirically tested methods in experimental setups, which facilitated a comprehensive understanding of the current developmental landscape. In the screening process, papers with disorganized structures or those offering minimal contributory value to the research were excluded. Furthermore, no distinctions were made between different Wi-Fi standards. Nevertheless, the findings from this work are important for future work on this topic. Furthermore, only techniques based on CSI are discussed in this paper.

IV. Impact on the protection of privacy

As already described in the previous chapters, CSIs offer great potential in combination with various algorithms and learning models. The following chapter deals with the effects

on privacy and presents models and suitable mitigation proposals.

However, passive detection of human bodies without a device is a key feature of CSIs. This discrimination has a particular influence on the protection of privacy, for example at home or in business premises. Equivalent to objects, human bodies change the physical properties of signals on the PHY layer between Tx and Rx Yang et al. [2, p. 28]. If people move in the area, CFR reacts particularly sensitively to the changes. If these changes are repeated in a closed room, the presence of people in rooms can be recognized without the need to install cameras or external motion sensors. [2, S. 30f]. Widar3.0 [2, S. 188ff] or GaitID [2, S. 215ff], which can characterize gestures or gaits, are more critical variants. Both are based on the logic of the body coordinates velocity profile (BVP). The values from the Doppler Frequency Spectrum (DFS) are categorized in a BVP matrix and a profile is created as [2] shows. In Fig. 1 serves as an illustration, which shows the DFS based on a changed compression with human contact. This technique

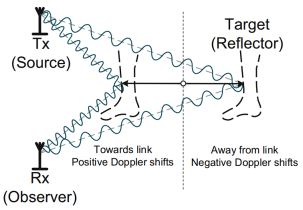
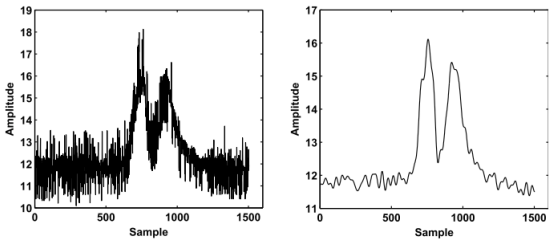


Fig. 1. Doppler shift differences, source: Yang et al. [2, p. 162]

makes it possible both to interpret gestures and to identify the human gait. However, the great strength of the model results from the additional transfer model as Yang et al. [2, p. 217] describes. Here, human characteristics that every person possesses are adopted for follow-up measurements and only variable characteristics are recorded. This allows significantly faster recording times. Both approaches offer the possibility of profiling based on NNs or DLs. With a performance of 93.2 %, GaitID can uniquely identify people based on their behavior, as Yang et al. [2, p. 225f] shows. The performance rate decreases when the number of people in the environment increases. However, this means that movement data within the room can be recorded and used for profiling. The gait can be identified as biometric data, which constitutes a special category of personal data according to Art. 9 GDPR. Another method discussed in relation to gesture recognition is the GWrite application by Regani et al. in [10]. This is an application that can detect gestures through walls. It uses the key feature of Wi-Fi signals, which is that they can detect changes through walls.

In the related work of Ali et al. [11] the application WiKey based on CSIs are used to model keystrokes based on the specific movement of the hand and fingers. As in the previous example, the change in the multi-path spectrum is measured using different indicators. The Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA) algorithms are used in this work. PCA was used to reduce the noise, thus reducing hand movements and other unnecessary movements from the CSIs for further analysis [11]. To correctly interpret the keystrokes, shape recognition was performed using the DWT algorithm. DWT provides both frequency and time domain information. In addition, DWT significantly shortens the repetitions for the learning process, which is why it is particularly suitable for finely granular recognition patterns. As an illustration, Fig. 2 shows the registered keystroke with the reduction of noise using PCA. As the work of Ali et al.



(a) Original time series (b) Filtered time series

Fig. 2. PCA Keystroke noise reduction with and without filtering noise, source: Ali et al. [11]

[11] shows, it is possible to recognize keystrokes using CSIs and applied algorithms. Here, the success rate for keystroke recognition and letter interpretation reaches 96.4 % and the recognition of a sentence at 93.5 % [11]. However, it must be said that the input speed and a noise-reduced environment were taken into account for the experimental setup [11]. Mobile phone patterns such as those frequently used, as Zhanga et al. [12] described, also represent a potential attack. It is mentioned that the closer the person is to a recording device, the more accurate the measurements can be [12]. The main reason for this is the resulting background noise, which also leads to difficulties with the other applications discussed. As soon as the input parameters are recognized, this has a significant impact on securing data and ensuring security of devices and even infrastructures. Nevertheless, the following chapter looks at mitigation options to protect people from unwanted Wi-Fi sensing based attacks.

A. Mitigation of CSI Measurements

Firstly, the work of Zhanga et al. [12] shows how an application on devices can be used to actively warn of a possible analysis and the use of CSI-based attacks. The next solution, as Cominelli et al. described in [5], randomizes the CSI using DL to modify the data so that the output no longer corresponds to reality. Furthermore, an obfuscation option is presented by Cominelli et al. in [13] and Ghiro et al. [3] which is also intended to protect against unwanted Wi-Fi sensing and CSI measurements. The application is considered first, followed by the randomization and obfuscation. In particular, the signal to noise ratio (SNR) and the already defined RSSI's are used in Zhanga et al. [12]. SNR reflects the ratio between unwanted environmental noise and specific signals. This value is therefore described by Zhanga et al.in [12] as an indicator of the probability of a possible CSI based

attack. In combination with RSSI and SNR, a location can be sought at which the interference noise and signal strength is so low that the possibility of a successful attack based on CSIs is significantly reduced. As can be seen in Fig. 3, a high level of interference noise can already be identified at a distance of 2.5 metres, which is reflected in the graphic. Patterns 1-3 represent different inputs on a smartphone device. This refers to the distance to a device that is used for the

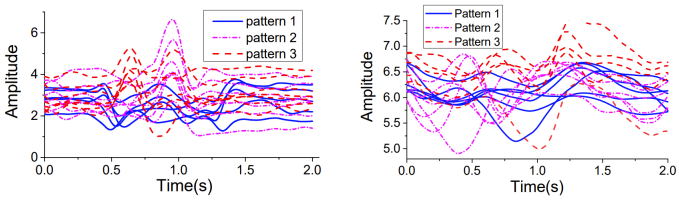


Fig. 3. Noise distance effect, different patterns with variantion in distance, source: Zhanga et al. [12]

purpose of recording CSIs, which can be the router, AP or a smart device in a room as Zhanga et al. [12] described. These values are divided into a 3-dimensional matrix with the parameters (X, Y, Z) as Zhanga et al [12] described. The information calculated from the signal strength and thus the distance can now be used to search for a point in the room where passwords and patterns can be entered. The system runs in a continuous loop and checks the surroundings for possible sources of danger. Another possibility described in Cominelli et al. [5] is an application that specifically manipulates the CSIs in order to also protect against an unintentional attack. It is assumed that a device for analyzing CSIs is installed and trained with the room data in a similar way. This would enable the attacker to recognize the positions of people, gestures and fine-grained movements. Various metrics to be used are described in [5] and an important aspect for the protection of privacy is already addressed. It is crucial that the phases and amplitudes are changed by the Tx in such a way that states and anomalies can no longer be tracked, but the shift is kept within limits so that an Rx can compensate for the shifts without affecting performance [5]. As Cominelli et al. in [5] described, three different cases were considered. Firstly, random spikes were added which change the overall CSI image. The next possibility is a phase shift and the insertion of notches [5]. The randomization only refers to the insertion of the interfering signals but not to the origin of the interfering signals. However, the Matlab Wi-Fi Toolbox [1] was used to inject the randomized values [5]. Implementation takes place on the Tx unit, which makes it possible to randomize the values. After [5], the use of random spikes proves to be an effective method to prevent localization. However, this method leads to a greater reduction in the packet delivery rate (PDR), i.e. the total number of packets that can still be delivered [5]. To illustrate how such randomization can affect localization, a localization parameter L was calculated using an NN and trained using fixed (x, y) coordinates. If L reaches the value 1, it can be assumed that it is the actual position of the person. In Cominelli et al. [5], a value $L = 0.05$ is achieved with the help of the randomization performed, which is why localization is not possible. In view of the localization probabilities from the previously presented sections of [2], the rate was reduced to 5% by applying randomization. As can be seen in Fig. 4, the measurements were carried out once without randomization algorithm and once with active randomization. As can be seen, the (x, y) differ strongly in front of each other, which is why the localization fails. Randomization on the part of Tx therefore

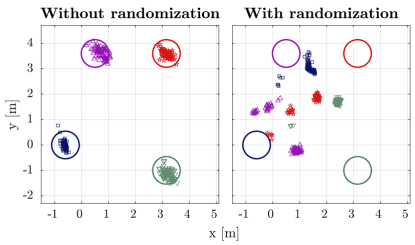


Fig. 4. Localization of a person in four different places with and without randomization, source: Cominelli et al. [5]

already provides good protection. However, the limits are reached here when it comes to the use case that a attacker has a Tx and Rx under his control. This problem is considered by Cominelli et al. [13]. No randomization algorithm is implemented on the transmitter unit instead, obfuscation takes place. As Cominelli et al. described [13], obfuscation is installed as an additional device, for example as an AP, and also has the task of concealing the position of an object. As obfuscation, signal reflections are included in the CSIs. In order to achieve a randomization of the occurrence here as well, the correlation is algorithmized for each obfuscation process according to the Markovian of the previous recording [13]. This method proves to be an alternative to the previously described implementation, as the transmission power or PDR is not influenced to the same extent as described in Cominelli et al. [5]. From the setup it can be deduced that the additional Tx, which acts as an obfuscator, does not reduce the PDR, more the obfuscator can even increase it, which is why the combination of high transmission power and privacy protection becomes possible Cominelli et al. [13]. However, when diverse applications are predicated on CSIs, the feasibility of de-obfuscation becomes essential. In this context, the study by Ghiro et al. [3] introduces another method for obfuscation where de-obfuscation specific to individual devices on an openwifi implementation is possible. In addition, the work of Abanto-Leon et al. [14] offers the possibility of incorporating the cryptographic properties of a random number generator into a randomization. However, this is not related to device-free scenarios as described, but to device-based fingerprinting.

B. Evaluation on the Mitigations

The first method from Zhanga et al. [12] proves to be a good application in unfamiliar buildings or confusing environments

[1]https://de.mathworks.com/products/wlan.html

with many devices. Since it is a loop that is executed, a simple application is conceivable as an application on the mobile device, so this is aimed more at the private sector. The method according to Cominelli et al. [5], on the other hand, describes a randomization of the values at Tx. This process can be of particular interest to distributors, manufacturers or system administrators. The described weakness is the reduction of the PDR, which is why too much randomization also leads to a reduction in performance. Finally, the method according to Cominelli et al. [13] was presented, which injects reflection signals due to an additional Tx unit. This method is also possible for the areas already mentioned, but it also has the strength of a fusion of obfuscation and transmission power so that it could conceivably be used for highly critical areas. Both methods work with non-cryptographic randomization procedures since the recording takes place on a physical level, a cryptographic implementation is difficult to realize Ghiro et al. [3].

V. Impact and Potential on the Protection of IT Security

As can be seen from the last chapter, even the disclosure of an access password using keystroke or patterns has a clear impact on IT security, as the confidentiality of data can be at risk. This chapter is therefore an attempt to examine the aspects of IT security in relation to Wi-Fi sensing and to present influencing factors. The focus of this chapter is no longer primarily on the analysis of movement information, but on different attack scenarios with which wireless networks are already confronted today. As described in the work of Liu et al. [6], spoofing attacks involve copying the physical address of a device and an attacker attempts to gain access to restricted information, thereby breaching its confidentiality. Additively, in Jianga et al. [15] attack scenarios where spoofing is extended via virtual network interface cards. The collisions caused by several addresses lead to the interruption of packet transmission, which is why a denial of service (DoS) can be achieved. Because the change only relates to the virtual address, the attacker is the only one in the network who still receives packets via the physical address [15]. In a Sybil attack, fake devices are placed in the wireless network to disrupt network traffic or intercept information, among other things. As described by Wang et al. in [16] a malicious device claims N identities, which is why the network is flooded with large requests. Once the number of Sybil nodes (N) is large enough, the network can be DoS and other devices can no longer connect to the network [16].

A. Mitigation on the Protection of IT Security

In the work of Liu et al. [6], a CSI profile of a user is defined on the basis of a permanently assigned device, which is therefore unique in its characteristics. A fingerprint of the device is created with the help of CSI samples [6]. Albanto-Leon et al. [14] point out that even if they are identical devices with the same chipset installed, they have different frequency characteristics. However, for this case the Orthogonal Frequency Division Multiplexing (OFDM) method is used. According to Liu et al. [6], this is a possibility whereby the modulation of the data streams is processed on different carrier frequencies. This measurement option has a higher authentication rate than is possible with RSSI, as already mentioned in the paper [6]. This prevents two identities with similar digital fingerprints from receiving the same authentication parameters. First, the samples are created at packet level to create a profile. As described by Liu et al. in [6], the profile creation also works if a spoofing attack is already taking place at this point. As soon as profiling is complete, the individual profile data is saved and used for subsequent matching mechanisms. A Machine Learning (ML) algorithm is also used here, which creates profile data that can already be used with 100 packets of investigation [6]. OFDM is also used in Jianga et al. [15] as well as a convolutional neural network (CNN). As in previous chapters, NNs are well suited for processing and interpreting large amounts of data. Similar to Liu et al. [6], in Jianga et al. [15] collects samples from existing devices as well. Its strength lies in the fact that both amplitude and phase properties are used [15]. In the work of Jianga et al. [15], CSIs are used to determine whether the packets originate or are claimed by one device or by two different ones. This makes it possible to determine if a physical address accepts several packets that are intended for other addresses. In this work, an accuracy of over 90% was achieved in the detection of both traditional and virtual spoofing attacks. [15] For mitigating Sybil attacks, the solution of Wang et al. in [16] that both static and dynamic devices (sybil nodes) can be identified based on their difference in the CSIs [16]. However, basic procedures such as noise reduction and motion detection are used as described in the Fundamentals. The difference lies in the behavior of the amplitudes and thus the CSIs, which is why for more accuracy an selfadaptiv Multiple Signal Classification (MUSIC) algorithm is used for the static devices [16] to detect the AoA and thus the angle of a device as well as the exact location from the amplitude information. The dynamic attack, on the other hand, is extracted after noise reduction and the detection of certain state features [16]. Consequently, a different algorithm is used which performs clustering based on density in spatial environments. This algorithm enables the detection of dynamic Sybil attacks and increases the overall accuracy. The result was a high average detection rate of both methods, at more than 98%. [16]

B. Evaluation on the Mitigations

When considering the mitigation solution proposed by Liu et al. [6], it emerges as a viable strategy for implementation in environments where access solutions and restrictions are tightly linked to device IDs and fingerprints. This approach highlights the robustness of device profiling, even if there is an ongoing spoofing attack as noted by Liu et al. in [6]. However, this method does not address the issue of virtual MAC spoofing, as discussed by Jianga et al. [15]. Indicating that the latter's domain of application may be marked by greater complexity. Indeed, Jianga et al. [15] report a high

detection rate in such complex environments. In a unique approach, Wang et al. [16] also consider the treatment of dynamic attacks, achieving high accuracy in the detection of such incidents. Nevertheless, as Wang et al. [16] suggest, overly complex environments and a multitude of devices can diminish success rates, pointing to a more suitable application in laboratory settings or small office spaces. Therefore, this chapter elucidates that the application of CSI-based sensing methods in wireless networks significantly impacts the integrity of received packets, the confidentiality of information, and the availability of wireless-based infrastructures.

VI. Discussion

Wi-Fi sensing and the underlying CSIs as drivers of new capabilities in wireless networks are causing a disruptive change in the way such networks are managed. This means that issues of privacy and IT security need to be fundamentally addressed. All of the work presented has been tested and examined under experimental laboratory conditions, so the values and accuracies given may vary greatly due to interfering signals or strong environmental influences. The results show influences, risks and potentials of how Wi-Fi sensing with different algorithms will change the future of wireless networks. The studies also described the value of learning algorithms and AI, which could play an even greater role in the future Ghiro et al. [3] for the possible protection of privacy and IT security. Related works such as Ma et al. [7] compare a large number of different methods and give a good overview of Wi-Fi sensing applications, but this work aims to merge approaches specifically on the topics of IT security and privacy to fill this scientific gap. Further work includes topics such as the study of cryptography secure randomization procedures as Abanto-Leon et al. [14] shows or as well as the merging of applications from the mitigation of privacy and IT security and what effect they have on each other. However, this finding has revealed a research gap that needs to be filled for future work.

VII. Conclusion and open Challenges

This research seeks to elucidate the extent to which Wi-Fi sensing and its underlying technologies impact privacy and IT security, and to project their future trajectory. From an overall perspective, this is a research area that appears to be relatively young, with many investigations conducted in the last 10 years, and is evolving in line with new standards in the Wi-Fi space. As already described, CSIs are highly sensitive to changes in the environment, which is a clear challenge for all the topics described. However, the use of neural networks and artificial intelligence can provide even better results in the future, as they are already being used. In addition, the challenge also lies in interpreting cross-device signals to incorporate the influence of other signals into the measurement procedures for physical environmental changes Ma et al. [7]. Such observations suggest that Wi-Fi sensing is poised to play an increasingly central role in future technological landscapes. As such, new implementations in the future will need to explore the limits and, as this work shows, new mitigation options will need to be employed to address both IT security and privacy risks arising from the terminology of Wi-Fi sensing.

A. *Future Work*

The next step is to evaluate how the use of future approaches can be harmonized without the risks outweighing the benefits. For this to succeed, a large number of works need to be evaluated. This will result in a comprehensive assessment of the impact on the domains of IT security and privacy. Recommendations are needed on how to deal with this technology in the future and how to address this gap correctly at an early stage.

References

[1] R. Du, H, Xie, M. Hu, Y. Xin, S. McCann, M. Montemurro, T. Xiao Han, and J. Xu, "An overview on IEEE 802.11bf: WLAN Sensing, July. 2022, https://doi.org/10.48550/arXiv.2207.04859

[2] Z. Yang, K. Qian, C. Wu, Y. Zhang, "Smart Wireless Sensing-From IoT to AIoT,", in Springer Singapore, 2021, https://doi.org/10.1007/978-981-16-5658-3

[3] L. Ghiro, M. Cominelli, F. Gringoli, R. Lo Cigno "Wi-Fi Localization Obfuscation: An implementation in openwifi" in Computer Communications, VOL. 205, No. C, pp. 1-13, April. 2023, https://doi.org/10.1016/j.comcom.2023.03.026

[4] T. Nakamura, M. Bouazizi, K. Yamamoto and T. Ohtsuki " Wi-Fi-Based Fall Detection Using Spectrogram Image of Channel State Information" in IEEE INTERNET OF THINGS JOURNAL, VOL. 9, No. 18, pp. 17220-17234, September. 2022, https://doi.org/10.1109/JIOT.2022.3152315

[5] M. Cominelli, F. Kosterhon, F. Gringoli, R. Lo Cigno, and A. Asadi, "IEEE 802.11 CSI randomization to Preserve Location Privacy: An Empirical Evaluation in Different Scenarios," March. 2021, https://doi.org/10.1016/j.comnet.2021.107970

[6] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen "Practical User Authentication Leveraging Channel State Information (CSI)" in ASIA CCS '14: Proceedings of the 9th ACM symposium on Information, VOL. 9, pp. 389-400, June. 2014, http://dx.doi.org/10.1145/2590296.2590321

[7] Y. Ma, G. Zhou, and S. Wang, "WiFi Sensing with Channel State Information: A Survey," in ACM Comput. Surv. 1, 1, Article 1, pp. 1-35, January. 2019, https://doi.org/10.1145/3310194

[8] S. Banerji, R. S. Chowdhury "On IEEE 802.11: Wireless LAN Technology," in International Journal of Mobile Network Communications & Telematics (IJMNCT) VOL. 3, Issue. 4, 2013, https://doi.org/10.5121/ijmnct.2013.3405

[9] H. Snyder " Literature review as a research methodology: An overview and guidelines ", in Journal of Business Research, VOL. 104, pp. 333-339, August. 2019, https://doi.org/10.1016/j.jbusres.2019.07.039

[10] S. D. Regani , B. Wang, Y. Hu and K. J. Ray Liu "GWrite: Enabling Through-the-Wall Gesture Writing Recognition Using WiFi" in IEEE INTERNET OF THINGS JOURNAL, VOL. 10, No. 7, pp. 5977-5991, April. 2023, https://doi.org/10.1109/JIOT.2022.3224313

[11] K. Ali, Alex X. Liu, W Wang, and M. Shahzad, " Recognizing Keystrokes Using WiFi Devices", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 35, No. 5, pp.1175-1190, 2017, https://doi.org/10.1109/JSAC.2017.2680998

[12] J. Zhanga, Z. Tanga, M.Lia, D.Fanga, X. Chena and Z. Wangb " Find Me A Safe Zone: A Countermeasure for Channel State Information Based Attacks " in Computers & Security VOL. 80, pp. 273-290, January. 2019, https://doi.org/10.1016/j.cose.2018.09.017

[13] M. Cominelli, F. Gringoli, R. Lo Cigno " Non Intrusive Wi-Fi CSI Obfuscation Against Active Localization Attacks" in Annual Conference on Wireless On-demand Network Systems and Services Conferece (WONS), VOL. 16, May. 2021, https://doi.org/10.23919/WONS51326.2021.9415586

[14] L. F. Abanto-Leon, A. B. G. Hong(Allyson) Sim, M. Hollick, A. Asadi " Stay Connected, Leave no Trace: Enhancing Security and Privacy in WiFi via Obfuscating Radiometric Fingerprints", in Proceedings of the ACM on Measurement and Analysis of Computing Systems, VOL 4, Issue 3, No: 44, pp. 1–31, June. 2021, https://doi.org/10.1145/3428329

[15] P. Jianga, H. Wua and C. Xin “A channel state information based virtual MAC spoofing detector” in High-Confidence Computing, VOL. 2 No. 3, September. 2022, https://doi.org/10.1016/j.hcc.2022.100067

[16] C. Wang, L. Zhu, L. Gong, Z. Zhao, L. Yang, Z. Liu and X. Cheng “Accurate Sybil Attack Detection Based on Fine-Grained Physical Channel Information ” in Sensors MDPI VOL. 18, No.3, March. 2018, https://doi.org/10.3390/s18030878