Received 27 December 2020; accepted 14 January 2021. Date of publication 26 January 2021; date of current version 22 February 2021.

Digital Object Identifier 10.1109/OJCOMS.2021.3054066

Wireless Communication, Sensing, and REM: A Security Perspective

HAJI M. FURQAN [1], MUHAMMAD SOHAIB J. SOLAIJA [1] (Student Member, IEEE), HALISE TÜRKMEN [1], AND HÜSEYIN ARSLAN [2] (Fellow, IEEE)

[1] Department of Electrical and Electronics Engineering, Istanbul Medipol University, 34810 Istanbul, Turkey

[2] Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA

CORRESPONDING AUTHOR: H. M. FURQAN (e-mail: furqan_ahmed89@hotmail.com)

The work of Haji M. Furqan was supported by the HISAR Lab at TUBİTAK BILGEM, Gebze, Turkey.

ABSTRACT The diverse requirements of next-generation communication systems necessitate awareness, flexibility, and intelligence as essential building blocks of future wireless networks. The awareness can be obtained from the radio signals in the environment using wireless sensing and radio environment mapping (REM) methods. This is, however, accompanied by threats such as eavesdropping, manipulation, and disruption posed by malicious attackers. To this end, this work analyzes the wireless sensing and radio environment awareness mechanisms, highlighting their vulnerabilities and provides solutions for mitigating them. As an example, the different threats to REM and its consequences in a vehicular communication scenario are described. Furthermore, the use of REM for securing communications is discussed and future directions regarding sensing/REM security are highlighted.

INDEX TERMS 5G, 6G, cryptography, joint radar and communication (JRC), physical layer security, radio environment mapping (REM), REM security, sensing security, vehicle-to-everything (V2X) communication, wireless sensing, WLAN sensing.

I. INTRODUCTION

A. MOTIVATION AND BACKGROUND

FIFTH generation (5G) of mobile communication signaled a paradigm shift in wireless networks by introducing diverse services with varying requirements rather than focusing merely on increasing the achievable data rates. Though this was catered to under the enhanced mobile broadband (eMBB) service, fifth generation (5G) also introduced massive machine-type connectivity (mMTC), and ultra-reliable low-latency communication (uRLLC) services to support massive number of devices and mission-critical applications [1]. Sixth generation (6G) is envisaged to extend this diversity of applications and use cases even further, laying down the foundation of a human-centric digital society [2]–[4]. This vision of the digital society encompasses work, healthcare, education, industry, entertainment, banking, and transportation - of which communication is just one (albeit critical) part. Figure 1 provides a glimpse of its different aspects, i.e., enabling technologies, application areas, and deployment environments.

The myriad of use cases characterized by diverse user requirements and varying capabilities of devices presents a challenge from the perspective of network design and management. The future networks, therefore, need to be capable of dynamically adapting to varying user/application requirements. This requires three things, namely awareness, intelligence, and flexibility; where awareness embodies the knowledge of the radio environment and everything that affects wireless signals, intelligence is the capability to determine the best possible option at any given time or scenario, while flexibility refers to the availability of different options (in terms of signal design, resource allocation, optimization and so on) [5], [6].

As a radio signal traverses the air, its properties are altered due to its interaction with the environment. This modification of the signal is effectively the fingerprint of the propagation environment (and devices) that the signal passes through. As such, this signal is a rich source of information for everything related to the radio environment. Here, the radio environment can consist of network infrastructure, propagation environment, attributes of the physical signal (multiple accessing scheme, waveform, modulation, etc.), and characteristics of the user equipment and users, among other things. The extraction

FIGURE 1. Illustration of different aspects of the digital society of the future from a communication perspective, including (some of) its enabling technologies, application areas, infrastructure, and deployment scenarios.

of information from the radio signals has been used in domains such as radio environment map/mapping (REM) and wireless sensing. REM is a multidimensional database containing information regarding the radio environment [7], which has been used to enhance the user experience by improving network deployment, resource allocation, and user-cell association [8]–[10]. Wireless sensing also has a rich history and has been used in a plethora of applications such as environmental monitoring, logistics, and robotics [11], [12]. Over the recent years, however, wireless sensing has also become more human-centric with the focus shifting towards smart healthcare, smart appliance interaction, and health monitoring [13]. This increasing interest is also reflected in the formation of a Task Group (TGbf) for standardization of sensing by 802.11 Working Group of the Institute of Electrical and Electronics Engineers (IEEE) [14].

Radio environment awareness and its applications highlighted above are generally aimed at improving human life. However, the very fact that radio signals can be used to get environmental awareness renders them prone to be eavesdropped, manipulated, and generally exploited by malicious nodes/entities. While REM/sensing security has been considered from the perspective of device authentication [15], the security of physical link and physical signal is often overlooked. This forms the motivation for our work, where we look at REM and wireless sensing from the security point of view.

B. CONTRIBUTIONS OF THIS WORK

The contributions of this work to the literature are itemized below:

- To the best of authors' knowledge, this is the first work that provides a comprehensive analysis of different components, processes, and methods of wireless sensing and REM from a security point of view. Furthermore, a distinction is made between the security perspectives of communication and sensing.
- Taking inspiration from wireless communication security literature, the attacks on wireless sensing/REM are defined, and their consequences are highlighted.
- Solutions for the highlighted (security) weaknesses are then provided from diverse domains such as wireless communications, military radars, machine learning, and crowdsourcing.
- To enable easier understanding of the threats to sensing/REM and their consequences, vehicle-to-everything (V2X) communication is presented as a case study. This use case is chosen since it relies on both communication and sensing for its proper operation.
- The concept of REM-assisted cognitive wireless security is proposed and presented, supported by yet another case study illustrating its applicability in V2X scenario.
- The various challenges and roadblocks in realizing secure wireless sensing and REM are pointed out. Moreover, the guidelines for addressing these challenges are provided.

C. STRUCTURE OF THIS ARTICLE

As illustrated in Fig. 2, the structure of this article is as follows. Preliminary concepts related to wireless security are covered in Section II. Section III describes the different aspects of radio environment awareness including architecture, standardization activities, sensing methods and processes. Sections IV, V, and VI discuss the exploratory, manipulation, disruption attacks with solutions, respectively. A case study to highlight the need for a secure REM in the context of V2X communication is described in Section VII. Section VIII presents the concept of sensing/REM-assisted cognitive security for wireless networks, while Section IX highlights the challenges in realizing a secure communication, sensing, and REM framework. Section X provides our concluding remarks.

II. SECURITY PRELIMINARIES

Here, preliminary information related to communication and sensing security is presented. This includes possible

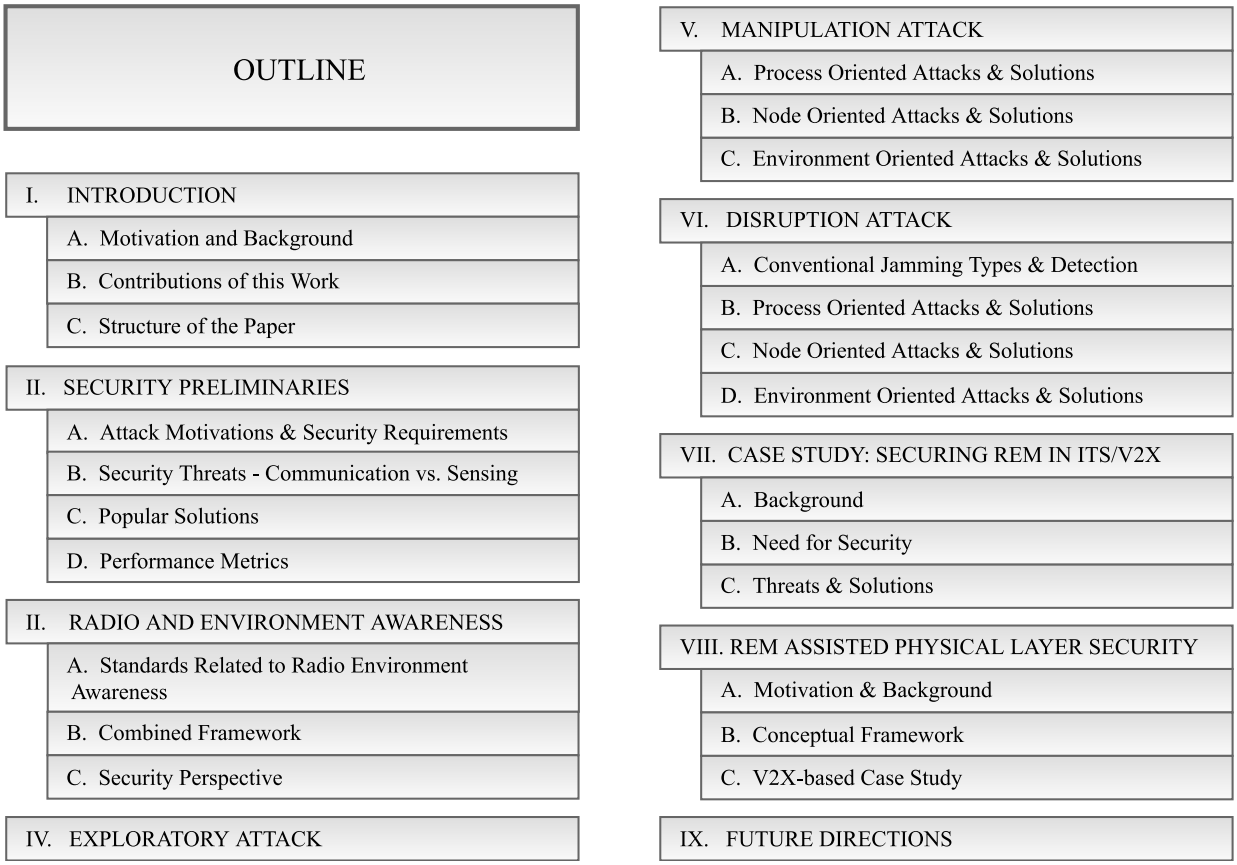


FIGURE 2. Structure/outline of this article.

motivations of the different attacks, the requirements of communication and/or sensing from a security perspective, definitions of different security threats, overview of possible solutions, and the corresponding performance metrics.

A. ATTACK MOTIVATIONS AND SECURITY REQUIREMENTS

As explained earlier, our surroundings contain a myriad of radio signals. These signals can be leveraged to extract information about the environment itself and the users/devices within. As such, a malicious node might have the following motivations when attacking a (communication and/or sensing) wireless network:

- *Confidentiality Violation:* The malicious node tries to intercept either the communication or characteristics of the legitimate nodes. In the context of sensing, this information may include a user's location, mobility pattern, social trends, etc.
- *Degradation:* The malicious node attempts to impair the communication link and/or sensing capabilities of the legitimate parties.
- *Exploitation:* The malicious node tries to exploit the communication and/or sensing for its own benefit. This may include learning and then manipulating the legitimate communication (or sensing) to acquire resources for itself.

Corresponding to the aforementioned intentions of the malicious attackers, the network strives to guarantee that its nodes and users are protected. This includes ensuring no illegitimate access to the information/transmission is allowed, the data shared between legitimate nodes is accurate, and there is no disruption of the services offered by the network [16].

B. SECURITY THREATS - COMMUNICATION VS SENSING

The broadcast nature of wireless communication (or signals in general) renders it susceptible to various security threats. Given below is an overview of how these threats compare for communication and sensing aspects.

- *Eavesdropping vs. Exploratory Attacks:* In eavesdropping, an unauthorized user attempts to intercept and interpret the data being shared between legitimate nodes [16]. In the case of exploratory attack, however, the malicious node tries to get radio and environment awareness using others' signals. In essence, this attack is geared towards violating the privacy of both users and the network. This attack is discussed in more detail in Section IV.
- *Spoofing vs. Manipulation:* A spoofer aims to hide its own identity or impersonate a legitimate node of the network to carry out malicious activities. These

attackers may lead to wastage or exploitation of communication resources [16]. The manipulation attack, on the other hand, does not only interfere with the communication but also leads to incorrect sensing and faulty REM construction. For instance, incorrect sensing in healthcare-related applications may cause issues such as wrong administration of drugs, while a faulty REM can lead to the illegitimate use of radio resources. Section V discusses this category of attacks in more detail.

- *Jamming vs. Disruption:* The intention of a jammer is to impair the wireless channel such that the legitimate node cannot utilize the radio resources to carry out its communication. This can be achieved by the generation of intentional interference by the malicious node on the same radio frequency (RF) resources as the ones being used by legitimate communication [17]. Disruption can be considered a more generalized approach to interrupting a wireless network, where apart from sending a jamming signal, other approaches such as flooding the sensing or processing nodes with information, are also used by the attacker. The different variants of this attack are discussed in Section VI.

Note that in the remainder of this article, Alice, Bob, and attacker terms are used for the legitimate transmitter, legitimate receiver, and malicious/illegitimate node, respectively. It should be noted that both Alice and Bob can have sensing capabilities, i.e., they can have initiating, responding, and communicating functionalities.

C. POPULAR SOLUTIONS

There are two well-established approaches to securing wireless networks; *cryptogrpahy* and *physical layer security (PLS)*. The former tries to secure the message or content of communication while the latter attempts to protect the wireless link (and the physical signal traversing it) between legitimate nodes. An overview of both these approaches is given below:

1) CRYPTOGRAPHY

Cryptography aims to provide privacy to the communication between legitimate nodes such that the attacker is unaware of what is being communicated. This is achieved by converting a message or *plaintext* to *ciphertext* using some encryption mechanism [18]. There are three techniques/approaches that are commonly used under the cryptography umbrella, namely, *hashing*, *symmetric* and *asymmetric* encryption.

Hashing is primarily used to check the integrity of the shared message/data. It utilizes a one-way function (easy to calculate in one direction but very difficult to reverse) to ensure that the transmitted information has not been tampered with. This involves the legitimate transmitter sharing the output of the hash function with the data, following which the receiver runs the received data through the same hash function. If the obtained output of the hash function matches the original one, the message is considered to be authentic. One of the constraints or challenges of hashing is to ensure the secure sharing of the hash function and its output between the nodes.

Symmetric cryptography, also referred to as private-key cryptography, uses the private key for both encryption and decryption of the message. Like hashing, this method depends on the secure exchange of keys between the legitimate nodes. Asymmetric cryptography, also referred to as public-key cryptography, effectively splits the key into two parts. A public key is made readily available by the receiver, and any node intending to send a message uses this key to encrypt the data. The decryption is carried out by the private key of the receiver. The most significant advantage of this method is the lack of need for any secure key exchange mechanism [19]. The public-key cryptography methods use one-way functions making it difficult to break the encryption. One of the foremost realizations of asymmetric cryptography is the RSA algorithm which leverages the difficulty of prime factorization to secure the shared messages [20].

To summarize, hashing only provides a mechanism to ensure or verify the authenticity of the data without actually providing a mechanism to secure it. Symmetric cryptography provides a lightweight solution to data protection but requires a secure mechanism for key sharing. While asymmetric cryptography solves this problem, it requires the devices to be capable of carrying out considerable computations (such as modular exponentiation in the case of RSA). This might not be feasible for power-constrained and computation-limited Internet of Things (IoT) and mMTC devices. Furthermore, the key-sharing (whether private or public) requires trusted third parties which becomes increasingly challenging in the presence of heterogeneous networks, devices, and applications in the upcoming generations. This necessitates an alternative solution, which is relatively lightweight in terms of complexity and scalable with the heterogeneity of future networks.

2) PHYSICAL LAYER SECURITY

As mentioned earlier, PLS secures the wireless link/signal by exploiting the characteristics of the environment or anything within that interacts with the physical signal. This includes the randomness of the wireless channel, interference, noise, fading, dispersion, reciprocity, and analog front-end (AFE) imperfections of the transceivers [21]. These mechanisms are used not only to provide confidentiality to the communication [22] but also to ensure reliability in the presence of jamming [17] and protection against non-authorized access [23]. Since PLS mechanisms depend on the channel and/or device characteristics to provide the security, they require inherent randomness of these entities to differentiate between the legitimate and malicious nodes. Situations that fail to fulfill this requirement, such as a static or poor scattering environment and devices with the indecipherable difference in AFE characteristics, pose a challenge to PLS phenomena.

The brief overview of both cryptography and PLS is provided to illustrate the fact that neither approach is capable of addressing all the security requirements in wireless systems. Rather, a complementary approach is needed for future networks. That being said, since the focus of cryptographic approaches is securing the content of wireless transmissions, they might not be readily suited to sensing and/or REM security. Therefore, for the rest of this work, we will primarily focus on PLS mechanisms for different communication, sensing, and REM security challenges.

D. PERFORMANCE METRICS

The security metrics vary depending on the type of attack as well the approach used for mitigating it. For instance, in the case of eavesdropping, there are generally two approaches, namely, signal-to-interference-plus-noise ratio (SINR)-based and key-based. In the former, the intention is to increase the gap between SINR experienced by Bob and the attacker. The degradation in SINR leads to increased bit error rate (BER). The term *security gap* is used for this difference in achievable error rate performance of the two nodes [22]. While not present in the literature, a similar approach can be used to quantify sensing security, where the goal is to maximize the estimation error in the information learned by the exploratory attacker. As far as the key-based methods are concerned, they leverage reciprocity and randomness of the channel to extract keys, which are then used to encrypt data. Since these methods focus on data security rather than the link itself, their metrics are not discussed here, but the authors would refer the readers to [24] for more discussion regarding this approach.

As mentioned earlier, spoofing (or its sensing/REM counterpart, manipulation) involves the malicious node either hiding its own identity or assuming that of a legitimate one. Therefore, the performance metrics related to spoofing focus on the correct classification of nodes (as authentic or otherwise). As such the conventional classification metrics such as *false alarm* and *missed detection* rates can be utilized [25]. An interesting thing to note here is that these metrics can be conflicting in nature, which makes it challenging to reduce them simultaneously. To address this issue, the (area under) *receiver operating characteristic (ROC)* curve metric can be used [26]. The same problem of node/user authentication persists in the case of sensing, therefore these metrics are applicable to the manipulation attacks as well. The performance metrics related to jamming (or disruption) attacks also focus on the detection of an attacker or jamming signal in the environment. As such, this also translates to a classification problem, and the same performance metrics as the ones described for spoofing can be used.

III. RADIO AND ENVIRONMENT AWARENESS

As mentioned before, REM is a flexibility enabler, comprising a multi-dimensional database containing information, learning algorithms, and models relevant to wireless devices, networks, and the environment [9]. Early works on the actualization of REM are limited to network controllers, base stations (BSs) and access points (APs). The main motivation of REM in these devices was generating signal strength maps, or radio frequency REMs (RF-REMs) [27], for opportunistic access of licensed spectrum in cognitive radios (CRs) [8]. Later, environment fingerprinting for localization and positioning services [28] also became an area of interest for applications such as autonomous robots. With the development of powerful processors and memory units, the previously limited REM actualization is now possible to some degree in common wireless devices, such as cellular phones, and can have features other than RF-REM. As such, REM can provide awareness to otherwise dumb wireless devices. For example, user-specific mobility patterns [29] can be used by network users to predict the trajectory of users for supporting handover [30] and content caching for device-to-device applications [31].

A. STANDARDS RELATED TO RADIO ENVIRONMENT AWARENESS

Several projects and standardization entities have undertaken the task of studying and incorporating REM and wireless sensing into wireless standards. The FARAMIR project has developed the fundamental architecture of REM for cognitive radio systems [32]. The European Telecommunications Standards Institute (ETSI) reconfigurable radio systems (RRS) project utilizes this architecture for use-cases where REM could be used in the context of RRS and the accompanying technological challenges.

The concept of obtaining information on the physical environment through wireless signal measurements has increased studies in this direction, resulting in numerous applications and use-cases. Because of their ready availability and license-exempt operation, off-the-shelf wireless devices and wireless fidelity (Wi-Fi) signals have been used extensively in these studies - with promising results. This has resulted in the development of commercial wireless sensing devices utilizing Wi-Fi or millimeter-wave (mmWave) frequency bands. As a result, the IEEE Standards Association for wireless local area Networks (WLANs) has approved the 802.11bf WLAN Sensing task group, specifically to incorporate wireless sensing support for the upcoming Wi-Fi 7 release. This is in addition to the 802.11az Next Generation Positioning (NGP) task group, which is winding up.

1) REM ARCHITECTURE

The results of the FARAMIR project built the backbone for future studies on REM-based network/communication optimization [8]. FARAMIR developed a functional REM architecture [32], illustrated in Fig. 3, consisting of the three elements briefly explained below:

- *Measurement-capable devices (MCDs)*: These devices are capable of measuring the various features of the wireless signal and the spectrum, such as power profile and channel state information (CSI). These can be

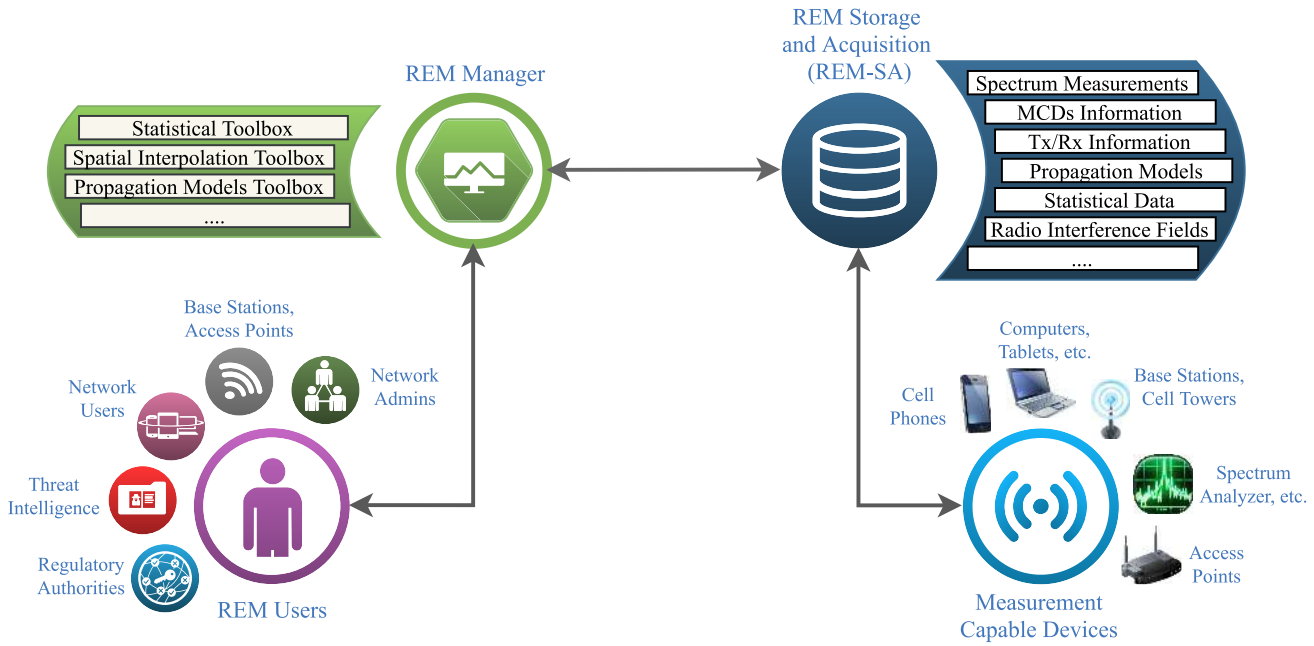


FIGURE 3. REM architecture developed by Flexible and spectrum-Aware Radio Access through Measurements and modelling In cognitive Radio systems (FARAMIR).

specialized spectrum measurement and analysis devices, network control devices, and other network infrastructure. Additionally, wireless communication devices, such as cell phones and laptops, can also be used as MCDs, along with other devices that have wireless capabilities, such as some IoT devices and smart home appliances.

- *REM storage and acquisition (REM-SA)*: This unit is responsible for storing and managing raw and processed data, as well as information about the measurement-capable devices (MCDs), such as their location and capabilities.
- *REM Manager*: The REM manager contains a number of processing modules, shown in Fig. 3, as well as interfaces for communication between the REM-SA and REM users. As such, the REM manager is responsible for managing data acquisition, processing data and relaying the queried information to the REM users.

A REM user can be any device which requires information from the REM, such as a user in the network, regulatory authorities, network controllers, BSs and APs. The REM can be divided into local and global, with local REM containing fast-changing data and fewer information layers, while the global REM contains static or quasi-static information.

2) WLAN STANDARDS

In 2015, the 802.11az task group began its efforts to support fine resolution relative positioning of stations (STAs) in WLAN networks to assist applications such as multiple-input multiple-output (MIMO) and beamforming, location based power control, spectrum management, indoor navigation, and smart audio systems [33]. The 802.11az standard proposes methods to enhance time-of-arrival (ToA), round trip time (RTT), and time-of-flight (ToF) based ranging techniques. Their scenario is comprised of up-to 200 STAs in a multiple AP network. The AP regularly transmits control signals, which the STAs synchronize to and utilize for calculating their relative position [34].

The 802.11bf task group was recently formed in order to provide standardization support for sensing applications in frequencies $1 - 7.125$ GHz and above 45 GHz through modifications to the medium access control (MAC) layer, Directional Multi-Gigabit (DMG) and enahnced-DMG (EDMG) physical layer designs. This amendment will allow devices to do the following tasks:

- communicate their sensing capabilities,
- define sensing transmissions and communicate which transmissions can be used for sensing,
- exchange sensed information and feedback,
- coordinate sensing transmissions and measurements,
- communicate measurements and measurement requests with the upper layer through a MAC service interface.

The difference between 802.11bf and the other standardization efforts is that its purpose is oriented more towards sensing for non-communication related applications, such as wireless health monitoring, user recognition, gesture recognition, and sleep monitoring. However, it also supports beam management and beamforming for multi-antenna communications.

B. COMBINED FRAMEWORK

Sensing for wireless communication optimization and sensing for other applications, while primarily revolving around measuring or extracting some information from the received

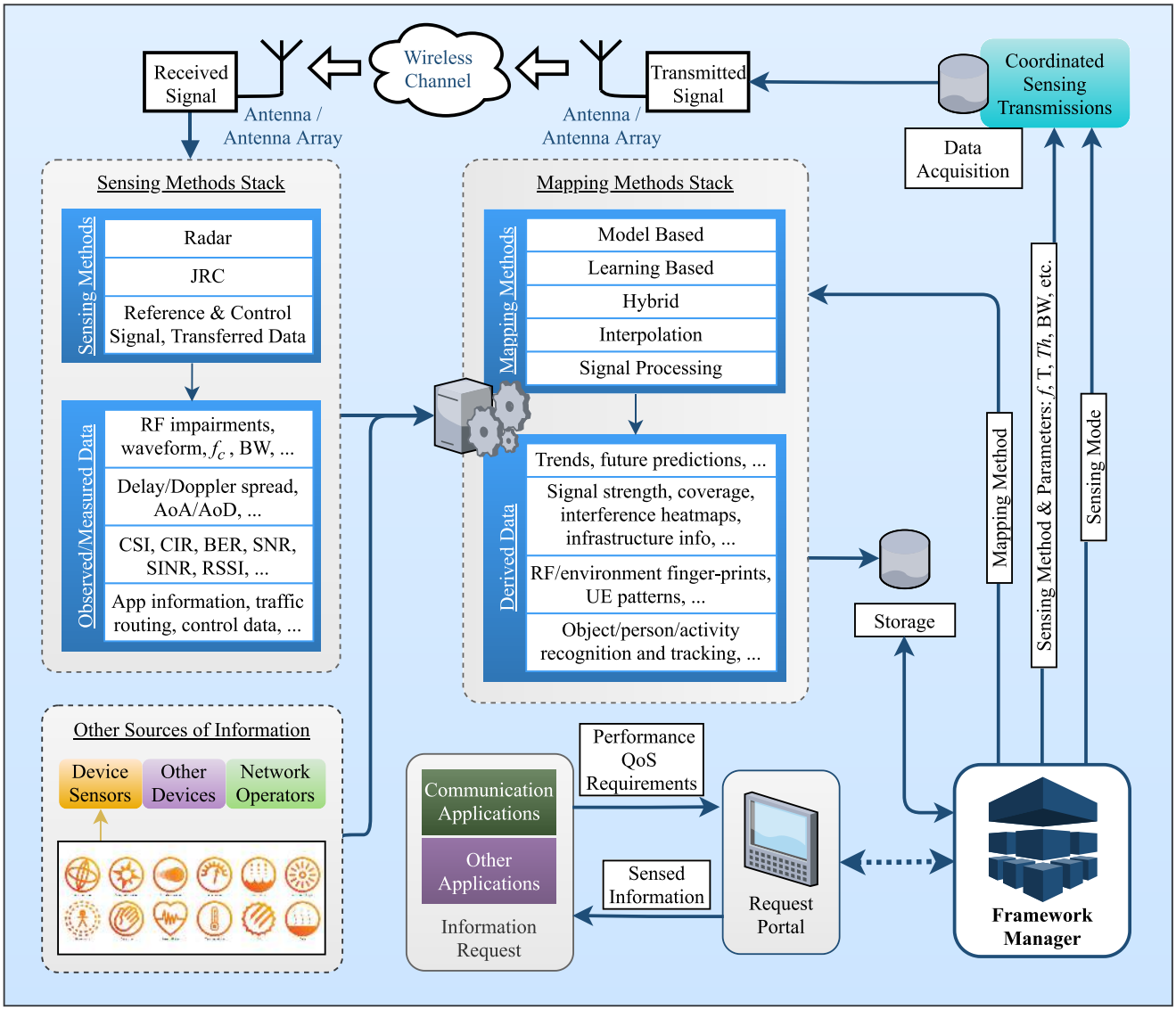


FIGURE 4. Generic radio environment awareness and map generation process.

signal, may have different requirements. Wireless sensing for wireless communication optimization is mainly done for channel or spectrum awareness. This is done through on-demand or periodic spectrum sensing, depending on the communication requirements. Information regarding the surroundings or mobility of the user-equipment (UE) is mostly obtained from the other layers of the REM. Exceptions to this are the positioning and localization techniques based on wireless fingerprinting. Wireless sensing for other applications, on the other hand, is solely performed to gain information or awareness on the environment or an object in it. However, developing wireless trends are leading to the convergence of sensing and communication functionalities. This makes them vulnerable to both communication and sensing related security threats. It will be beneficial, therefore, to provide a generic radio environment awareness process and components, depicted in Fig. 4, before highlighting its security vulnerabilities.

1) MEASURED DATA AND DERIVABLE INFORMATION

Measured data is the low level or raw data that can be directly measured from the signal, obtained through simple operations or as a by-product of communication processes. Examples can be delay, frequency offset, CSI and received signal strength indicator (RSSI). Derivable data, on the other hand, is obtained through applying one or more of signal processing techniques, interpolation algorithms, mapping methods, machine learning (ML)/deep learning (DL) algorithms, filters and models on the measured data, and information from other sources - device sensors and online databases. Examples of derivable data include trajectory patterns, spectrum power maps, and detection/recognition of various actions.

2) PARTICIPATING NODES

The nodes taking part in the monitoring process, whether knowingly or not, are wireless devices and are labeled

based on their role in the sensing session. Initiating nodes (INs) launch and/or coordinate the sensing session. They are assumed to be capable of generating and managing a REM. Responding nodes (RNs) send their measurements or sensing transmissions to the initiating node (IN) [35], while communicating nodes (CNs) do not actively take part in the sensing session, but their transmissions may be used for sensing. Either responding node (RN) or IN must be MCDs, while CN may not necessarily have measurement capabilities. For example, within a multi-device Wi-Fi network, an AP may be the IN, RN may be wireless capable electronic devices, cell phones, laptops, and other devices mentioned in Section III-A1.

3) SENSING MODES

The sensing modes define the nature of the transmissions (waveform, training/sensing sequences), spectrum, and other resources' utilization for sensing. Sensing can take place with dedicated sensing signals or by exploiting the available communication signals. There are five sensing modes that can be chosen based on the information and application requirements.

- *Instantaneous/On-Demand* mode makes an on-demand, singular, or a short burst of measurements.
- *Opportunistic* mode exploits the received and/or transmitted communication signals of the IN for sensing [36].
- *Passive* mode exploits sensing and/or communication signals transmitted by other devices (to each other) for sensing.
- *Periodic* mode takes measurements with a certain frequency/rate, whether from the available communications signals or dedicated sensing transmissions.
- *Threshold-based* mode only initiates a complete sensing process or forwards the observed data if the initial measurement passes a certain value [37].

Here, the threshold-based mode is optionally used alongside another sensing mode as a regulator for forwarding sensed data or frequency of sensing. Additionally, periodic and instantaneous sensing modes may require feedback [36], depending on which node is transmitting the sensing transmission. Certain parameters can be associated with each sensing mode, depending on the application scenario. These parameters could be sensing rate f, sensing period T, update threshold Th, sensing waveform, and its parameters, such as bandwidth BW and power. The parameters are chosen by the REM manager or sensing application based on the application performance metrics, such as accuracy.

4) SENSING METHODS

The sensing methods are used to extract measurements from the received signal. These methods include radar, joint radar and communication (JRC), and communication signal demodulation.

- *Radar*: Radar uses reflections or echoes of the transmitted signal to get measurements such as delay, Doppler shift, angle of arrival (AoA)/angle of departure (AoD), and reflected power, which can then be mapped to knowledge of the environment or objects. The reflections or received signal will be displaced in time and frequency to reflect the time delay and Doppler shift, respectively, and will have less power than the transmitted signal. The time offset and Doppler shift can be found as:

$$\Delta t = \frac{2(R + vt)}{c} \tag{1}$$

and

$$f_d = \frac{2vt\cos(\theta)}{\lambda}, \tag{2}$$

respectively, where R is the distance of the object from the receiver, v is the velocity of the object, t is the time instance, c is the propagation speed of light, θ is the angle of arrival, and λ is the wavelength. The received power will be less than the transmitted due to path loss, multipath fading, object material properties, and incidence cross-section area. In order to extract the difference between the transmitted and received signals, the transmitted and received signals are mixed, giving the beat signal. The distance of the object from the receiver can be found by taking the fast Fourier transform (FFT) of the beat signal. The peaks of the FFT output indicate the object range. The object velocity can be found by taking the range-Doppler FFT, which gives the Range-Doppler map. The maxima of this map correspond to object range and velocities. Estimating the direction of the object can only be performed if the radar is either rotatory or the receiver is an antenna array. In the former case, the angle of the object relative to the receiver is found as the angle of the receiver for which the received power is highest. In the latter case, beamforming methods, such as multiple signal classification (MUSIC) can be used [38], [39]. A more detailed explanation of radar concepts and derivation of the relationships can be found in [40].
- *Joint Radar and Communication*: JRC allows the coexistence of radar and communication functionalities in some domains to increase efficiency, at the cost of some communication and/or radar performance [41]. Coexistence in the time and frequency domain is studied under radar and communication coexistence (RCC). In these systems, the time and frequency resources are allocated such that the radar and communication signals are separable in at least one domain. Coexistence in the waveform domain is accomplished in dual function radar communication (DFRC) systems, where one waveform or signal is utilized for both radar and communication. These waveforms can be primarily radar waveforms enhanced with communication capabilities or primarily communication waveforms utilized as radar waveforms. Examples of the former include phase-modulated chirp signals [42], utilizing radar waveform

dictionaries to take advantage of waveform diversity for communication information embedding [43] or codebook-based communication information embedding for spatial index modulation in MIMO radar systems [44]. The bit modulation in these signals is limited and therefore, they cannot reach the high throughput provided by communication waveforms. The most common example of the latter is utilizing the orthogonal frequency division multiplexing (OFDM) waveform [45]. Here, the data throughput is higher, but due to poor auto-correlation properties, detecting the maxima (and therefore, the objects) can be difficult. There is a peak in interest in utilizing conventional communication OFDM-based data packets for JRC sensing due to compatibility with existing wireless devices. The frame design parameters for these packets, such as bandwidth, limit the range and velocity resolutions, however, research in this direction is promising. Since JRC sensing follows the same concepts as radar sensing, similar relations as given for radar are used to find the range, Doppler, and direction.

- *Communication Signal Processing/Demodulation*: Communication signal demodulation gives REM data as a by-product. For example, equalization removes the channel effects from the received signal by calculating CSI using the reference signals or pilots. In this scenario, the CSI is the by-product of equalization. Some measurements, like received signal strength (RSS), can directly be measured from the received signal. Others require more sophisticated methods, such as Blind signal analysis (BSA), which performs signal detection and analysis with limited to no prior information [46]. The transmitted information can also enable awareness. Control signals, for example, can contain information on network infrastructure, device locations, and beamforming parameters, to name a few. Similarly, Global Positioning System (GPS) signals contain navigation messages used to calculate a device's position.

5) MAPPING METHODS

Mapping methods are used to derive or extract information from the measured data or to map the data onto other domains. These include noise reduction, thresholding algorithms, signal processing, filtering algorithms, models, ML, and interpolation algorithms. These algorithms are used to extract and clean the relevant data, map it to other domains/actions, and/or estimate missing values. For example, a time-series of CSI and/or RSS can be used to train ML/DL networks to detect certain actions in the environment [47], [48].

6) WIRELESS SENSING PROCESS

A generic schematic of the realization of radio environment sensing is given in Fig. 4. When an application, communication or otherwise, makes an information request, the framework manager queries the storage unit. If the information is present, it is relayed to the application. If not, an IN initiates a sensing session. During a sensing session, depending on the application and information requirements, the nodes available to participate in the session and their capabilities, and the spectrum availability, a suitable sensing method and mode are chosen. Based on this, the IN performs feedback or no-feedback based sensing. The observed information is sent to the mapping methods stack, where a suitable technique is used to extract the requested information. Then, the information is relayed to the application through the request portal. This process is coordinated by the framework manager [8], [49].

C. SECURITY PERSPECTIVE

An important issue is the security and authenticity of REM and sensing information, which is easily susceptible to eavesdropping, spoofing, and jamming attacks. Similarly, the security and legitimacy of the characteristics of the sensing signal, along with the overall radio environment awareness and mapping process, are also susceptible to exploratory, manipulation, and disruption attacks. With the significance of wireless sensing evident for future wireless communication and other applications, large scale wireless sensing will not be feasible unless methods are developed to prevent, detect, and negate these attacks. The first step in this direction would be to form a categorization of attacks on the radio environment awareness and mapping process. In this regard, and considering the discussion provided in this section, the malicious attacks may be categorized as follows depending on their intended goal:

- *Process Oriented:* These attacks are on the modes and methods used in radio environment awareness and mapping process. Examples include attacks on the parameters used for different sensing methods, sensing modes, and mapping methods.
- *Node Oriented:* These attacks target the different nodes that are part of the radio environment awareness and mapping process. These nodes may support communication, sensing, or both. The attacker might be interested in information such as node's identity, data, velocity, size, angle, location, AFE characteristics (antenna type and numbers), AFE impairments, patterns, power, bandwidth, quality of service (QoS) requirements, application, carrier frequency, CSI, and waveform used.
- *Environment Oriented:* These attacks are on the physical/radio environment. This includes the line-of-sight (LoS)/non-line-of-sight (NLoS) characteristics, channel richness and sparsity, urban/rural categorization, mobility, physical objects, communication infrastructure, radio capable devices, interference, and so on.

These attack orientations, a summary of which along with their related parameters is given in Table 1, are used to group different attacks in the following sections.

TABLE 1. Summary of the attack orientations on the radio environment awareness and map generation process, related components, and the associated parameters.

Attack Orientations	REM Components	Parameters
Process	Sensing methods	Sensing frequency (f), sensing period (T), threshold (Th),
	Sensing modes	details about modes and methods, operating frequency, bandwidth (BW),
	Mapping methods	multiple accessing, waveform, pilots, radio access technology, etc.
Nodes	Initiating Nodes	Identity, velocity, size, angle, location, RF front-end characteristics,
	Responding nodes	RF impairments, patterns, power, etc.
	Communication nodes	
Environment	Propagation	Wireless channel characteristics, environmental features (urban/rural),
	Conditions	mobility, physical objects features, communication infrastructure,
	Hardware/objects	radio capable devices, etc.

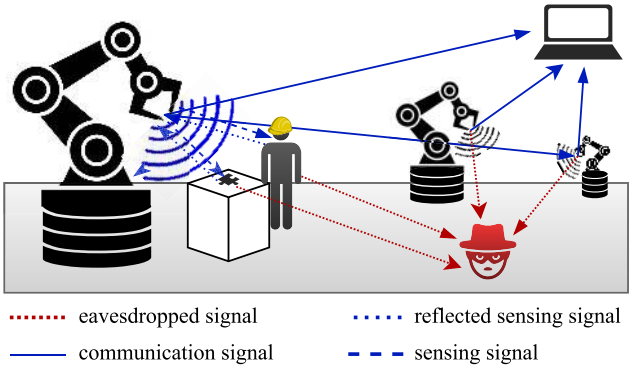


FIGURE 5. Exploratory attacks from communication and sensing perspective.

IV. EXPLORATORY ATTACK

As explained earlier, the term *eavesdropping* is used in the literature for attacks where an attacker tries to spy on or intercept the content (data and control information) of the communication. Exploratory attacks can be considered a generalized version of eavesdropping, where the attacker is not only interested in the content of the communication but its characteristics as well. Figure 5 shows the exploratory attack, where the attacker is not only listening to the ongoing communication but also sensing information related to pedestrians and environments.

In the context of radio environment awareness/sensing and REM generation, exploratory attacks can target the monitoring process, nodes, and the environment. Here, the aim may be to either simply extract the information related to sensing modes and methods, mapping algorithms, node location, control information, AFE characteristics, physical layer properties of the radio signals, and environment fingerprints or exploit this information for further manipulation or disruption attacks. Some realizations of this attack include learning user/node behavior, control information, node data, traffic analysis, and preferences. Even if not used to manipulate or disrupt the communication, this information is useful as real-world data and holds considerable value. Additionally, monitoring or learning the operating parameters of any node can enable smarter and more efficient attacks, reducing the effectiveness of classical security techniques.

Since exploratory attacks are passive, they depend on the ongoing wireless transmissions between different nodes of the network. As such, the sensing methods described earlier can be considered as the primary objective of these attacks, since they are responsible for obtaining and sharing information related to the monitoring process, nodes, and environment with the participating entities. The security solutions presented below cover radar, JRC, communication, and pilot signals from both communication and sensing perspectives. A summary of the exploratory attacks and possible solutions is provided in Table 2.

1) LPI-BASED APPROACH

In order to diminish the attacker's capability to eavesdrop on the content and characteristics of the wireless signal, low probability of intercept (LPI) based transmission has gained increased attention. The reason is that LPI/covert transmission prevents the transmission of legitimate nodes from being detected by the attacker. For example, as illustrated in Fig. 6, LPI based methods can avoid detection by hiding the information below the noise floor. This is achieved by spreading the energy in time, frequency, and spatial domains using a secret sequence. This is realized in the three domains through high duty cycle waveforms, wide bandwidths, and broad transmitted beams, respectively. Examples of these approaches include frequency agility, where operating frequency is changed swiftly, spread spectrum techniques, and irregular scan patterns, which can help evade interception [50]. Additionally, in combination with

TABLE 2. Exploratory attacks and solutions with selected references.

Attack Types	Attack Orientations	REM Components	Threat Details/Types	Possible Solutions
Exploratory Attack	*Process*	Sensing methods	Spying the information related to sensing modes, sensing methods, waveforms, bandwidth, pilots, operating frequency, access technologies.	LPI-based approach [50], [51] Adaptation-based techniques [52]–[54], [56], [64] Interfering signal assisted techniques [60]–[62] Cooperative jamming [62], [65] Security for the reference signals [68]–[70] RIS-based solutions [22], [71], [72] Physical layer key extraction [75]–[77], [79] ML and DL based solutions [83]
		Sensing modes		
		Mapping methods		
	Nodes	Initiating nodes	Spying the information related to nodes including identity, velocity, size, angle, location, hardware features, power.	
		Responding nodes		
		Communication nodes		
	Environment	Propagation	Spying information related to environment and objects, channel characteristics, communication infrastructure.	
		Conditions		
		Hardware/objects		

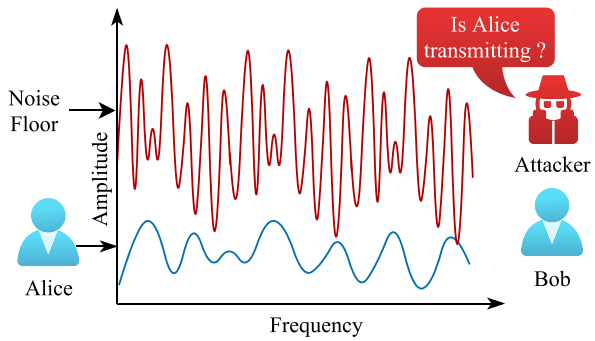


FIGURE 6. LPI-based design, where the energy of the information signal is spread in the frequency domain to hide it below the noise floor.

waveform design, the design and optimization of the antenna arrays can also be utilized to avoid interception [51].

2) ADAPTATION-BASED TECHNIQUES

The basic idea in these techniques is to adapt the transmission parameters based on the requirements, location, or channel conditions of the legitimate nodes [52]. These approaches enhance the reliability of both contents and/or characteristics of the wireless signal at the legitimate node, improving their security in the process.

A beamforming-based solution [53], [54] is shown in Fig. 7(a) as an example for spatial anti-exploratory techniques. These techniques enhance the signal power in the direction of Bob while suppressing it in other directions. As shown in the figure, the attacker does not have access to the transmitted signal or its reflection. This provides reliable and secure communication and/or sensing by avoiding signal leakage. Similarly, Fig. 7(b) presents a directional modulation-based security concept [55], where the constellation points maintain their standard format in the direction of Bob, while being scrambled and irrecoverable at the other directions. Hence, the side-lobes can be used for radar-based sensing, even when the targets are potential eavesdroppers. Other examples of adaptation-based techniques include adaptive resource allocation (e.g., sub-carriers), precoding, transmit antenna selection, signal constellations rotation,

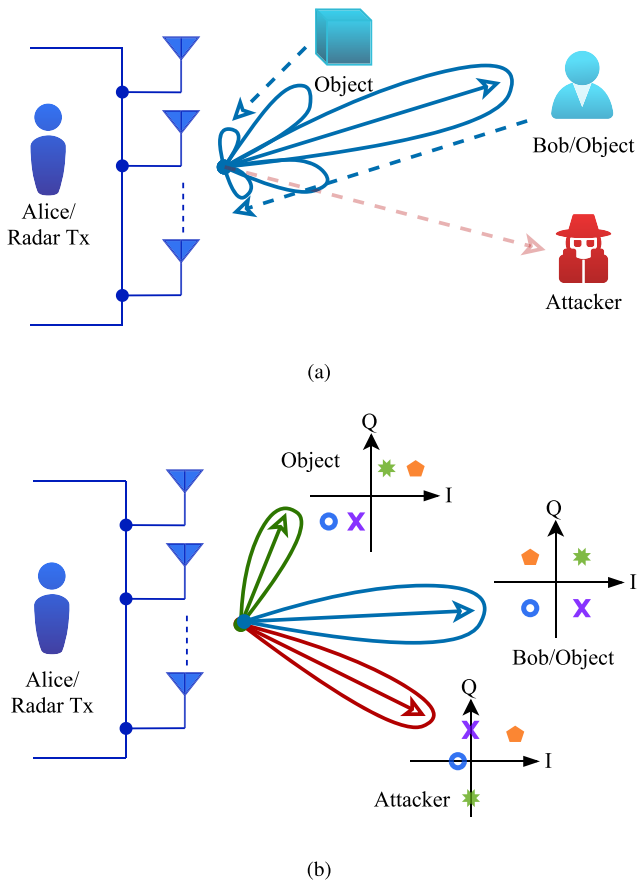


FIGURE 7. Adaptation based techniques for enhancing security against exploratory attacks (a) multi-antenna beamforming, (b) directional modulation.

interference alignment, relay selection, and adaptive power control [56]–[59].

Apart from improving security and reliability, adaptation-based techniques also enhance resource efficiency. These techniques do not need extra processing at the receiver for implementation. Therefore, they are suitable for devices with limited processing capabilities, such as the IoT systems. Additionally, these techniques are applicable to both time-division duplexing (TDD) and frequency-division duplexing

(FDD) systems. However, despite their considerable benefits, adaptation-based techniques may not be effective in the presence of multiple collaborative attackers. One possible solution to provide security in such cases is to amalgamate these techniques with other security techniques, such as interfering signal-based explained below.

3) INTERFERING SIGNAL-BASED TECHNIQUES

In this approach, an interfering (jamming or artificial noise) signal is added by a trusted node (such as a transmitter, receiver, or relay) to the transmission using the null space of the legitimate receiver's channel in order to degrade the attacker's performance while ensuring that it does not affect the reception at the legitimate receiver [60]–[63]. These solutions are capable of protecting both the data and the characteristics of the transmission, thus, useful for the security of both communication and sensing. For example, Fig. 8(a) illustrates an artificial noise-based technique with multi-antenna beamforming [64]. Here, the interfering signal is transmitted simultaneously with the communication or sensing signal in the null space of the legitimate channel to degrade the performance of the attacker. Another interesting example is cooperative jamming [62], [65], where external nodes (relays) are used to generate interference signal, as shown in Fig. 8(b).

A significant advantage of this approach is the provision of secure communication, even if the attacker has a better channel compared to the legitimate node. Additionally, these techniques are applicable to both TDD and FDD systems. However, the deployment of artificial noise in the interfering signals is power consuming and requires CSI or location knowledge of the object/receiver [66]. It can also cause some degradation in performance if the artificial noise is not designed properly. Hence, power allocation and noise design need to be kept in mind. To address the power consumption concerns, energy harvesting and wireless power transfer can be exploited [67].

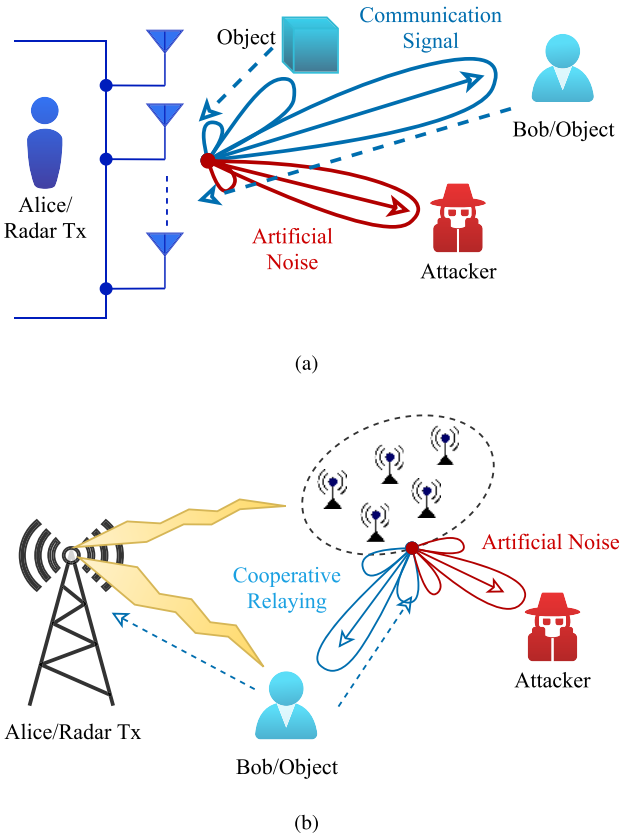


FIGURE 8. Interfering signal based techniques for enhancing security against exploratory attacks (a) multi-antenna beamforming with artificial noise, (b) Cooperative jamming.

4) SECURITY FOR REFERENCE SIGNAL

In order to learn about the features of the environment, known reference signals are transmitted from the source. If the security of the reference signal is ensured, the attacker can not learn about the environment. Several techniques have been proposed in the literature to ensure the security of reference signal including pilot tone manipulation [68], artificial noise embedding [69], and anti-eavesdropping pilot design [70].

In [68], the phases of pilots are rotated based on preceding instantaneous channel information of subcarriers at the transmitter. This deteriorates the eavesdropping capability during the channel estimation phase, where only the intended receiver can estimate the channel correctly. In [69], artificial noise is embedded in the pilot signal based on the uplink CSI to degrade the channel estimation performance at the attacker during downlink pilot transmission. Finally, [70] is based on the design of special anti-eavesdropping pilots for legitimate nodes with full-duplex capabilities. Particularly, the pilots from the legitimate nodes are designed in such a way that the composite pilot matrix has a full rank for legitimate nodes while having rank deficiency with respect to the attacker. This ensures that the attacker cannot observe the subspace of its CSI using the legitimate pilots.

5) RIS ASSISTED SOLUTIONS

A reconfigurable intelligent surface (RIS) is made up of low-cost passive elements organized in the form of a uniform planar array, where each element in the RIS can be controlled to reflect the incident signal with adjustable phase and/or amplitude. The ability of RISs to manipulate the propagation environment [71] renders them capable of protecting the wireless signals from being intercepted by unintended receivers, as shown in Fig. 9. This can be done by creating constructive and destructive interference at Bob and the attacker, respectively. This results in an enhanced signal at the former and a weakened signal at the latter. This, however, requires knowledge of the CSI of both Bob and Attacker. However, when CSI of the attacker is not available then the security design will be based on location, channel, and requirements of Bob only [22], [72].

The protected zone concept provides a way to ensure data confidentiality in the presence of exploratory attacks,

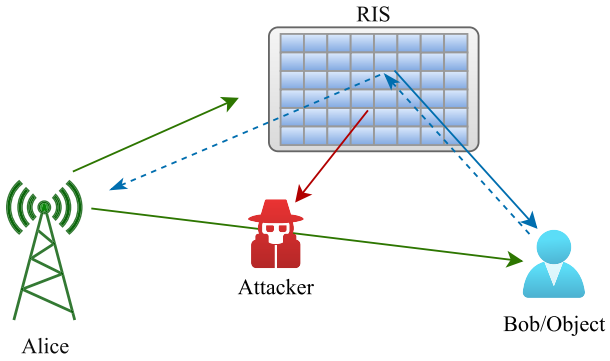


FIGURE 9. RIS assisted security solutions for communication and sensing security.

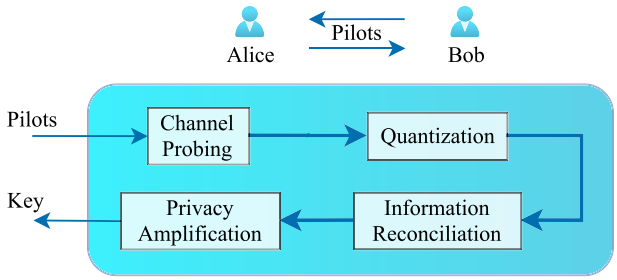


FIGURE 10. Basic steps for key generation algorithms.

where the location or existence of the attacker is unknown. Here, a region is formed around the legitimate nodes by masking leaking signals with artificial noise emitted by cooperating entities [73]. The transmission of artificial noise or interfering signals in different directions and beamwidths is based on the location of legitimate nodes, the geometry of the nodes, AoA, AoD, and the level of required protection.

RISs can also ensure secure communication even when some conventional PLS techniques may be ineffective. For example, when Bob and attacker are in the same direction, PLS techniques such as beamforming and directional modulation, cannot ensure secure communication because the attacker will be in the path of the transmitted signal. In such situations, RIS can be utilized to provide alternate and independent paths to the receiver [74], as shown in Fig. 9. Alternatively, RIS can be used in conjunction with interfering signal-based techniques to reflect or redirect these signals towards the attacker, enhancing the security of the transmission.

6) PHYSICAL LAYER KEY EXTRACTION

These techniques generate a secret key based on dynamic random wireless channel by exploiting CSI, RSSI, AoA, subcarrier indices, and feedback mechanisms [75]–[77]. The generated key can be used as the spreading sequence in LPI based solutions, securing contents and some of the features of the wireless transmission. The key-based solutions are based on three assumptions: channel reciprocity, channel decorrelation, and channel randomness. Channel reciprocity ensures similar observations at a pair of communicating nodes in a TDD system. Channel de-correlation implies that if the attacker is at least half a wavelength apart from the legitimate node in a rich scattering environment, it will experience an independent channel [78]. The channel randomness in spatial, temporal, and spectral domains helps in the generation of random key bits.

The basic steps of generating a secret key from a wireless channel include channel probing, channel quantization, information reconciliation, and privacy amplification [24], as illustrated in Fig. 10. First, channel probing is done at the communicating nodes using sounding techniques. Afterward, the secret key bits are generated from selected channel features by channel quantization. The information reconciliation step is then employed to minimize the mismatch between the generated key bits at legitimate nodes. Finally, privacy amplification is applied to enhance and optimize the randomness of the generated key bits.

One benefit of channel-based key techniques is their ability to resolve key sharing and management issues present in conventional security techniques. This approach is also applicable if the attacker experiences better channel conditions as compared to the legitimate receiver. On the other hand, key-based approaches require additional signaling and processing at the legitimate nodes. They are also sensitive to channel mismatch errors between legitimate nodes and are not effective in poor scattering environments. The latter problem, however, can be tackled by exploiting multi-beam resolution with variable steering angle [77], using virtual AoA and AoD to generate key bits in mmWave massive multiple-input multiple-output (mMIMO) channel [79], producing artificial interference [80], and implementing virtual channels [81].

7) MACHINE-LEARNING AND DEEP LEARNING ASSISTED SOLUTIONS

Utilizing artificial intelligence (AI) techniques to learn and adapt to the wireless environment has become increasingly popular in recent years. PLS methods, such as beamforming and precoding, interfering signal, and subcarrier allocation based approaches, are complex optimization problems. The complexity is compounded with the increasing heterogeneity of future wireless networks, multi-user/object scenarios, RIS assisted environmental manipulation, and mmWave mMIMO systems. Rather than modelling and solving optimization functions for these scenarios, ML and DL algorithms can be employed, resulting in efficient PLS approaches [82] and better quality of CSI [83], which is an integral part of all PLS techniques.

V. MANIPULATION ATTACK

Manipulation attack on wireless communication, sensing, and related components is a generalization of conventional spoofing. In spoofing attacks, the spoofer can intercept and modify the contents of the message between the legitimate parties. Manipulation, on the other hand, violates the

TABLE 3. Manipulation attacks and solutions with selected references.

Threats type	G-REM orientations	G-REM components	Threat details/type	Solutions
Manipulation attack	*Process*	Sensing methods	Radar/JRC related spoofing	Filtering-based [89], Challenge response-based [90], Spatio-temporal reflections-based [91], Randomized frequency hopping [92].
			Communication signal related spoofing	Active PLA [129], [130], Passive PLA [23], [78].
			Reference signal related spoofing	Channel coefficients comparison-based [96], Pilot superposition with random signal [98], Energy ratio test [99], Two-way training method [100].
		Sensing modes	Sensing session duration attack	Random duration-based solutions [101]
			Threshold-based manipulation attack	Hysteresis margin-assisted solutions [102], [103]
			Attacks on opportunistic/passive modes	Blind signal analysis [104], Active and passive PLA schemes.
		Mapping methods	Spatial interpolation attack	Crowdsourcing solutions [105] [117]
			Adversarial attack	Distillation [109], Region-based classification [110].
	Nodes	G-REM nodes	Authentication violation	Active PLA [133]–[135]
		Responding nodes	Integrity violation	Channel-based PLA [122]–[125]
		Communication nodes	Emulation attack	AFE-based PLA [23], [127]
	Environment	Propagation	Saptio-temporal environmental features manipulation	Crowdsourcing-based solutions [117]
		Conditions	Environmental conditions manipulation	
		Hardware/objects	Physical hardware manipulation	

integrity of the characteristics of the wireless transmissions as well. These attacks can be aided by information observed regarding the sensing process, contributing nodes, and radio environment during exploratory attacks. In this section, manipulation attacks on different aspects of the wireless sensing process and components, and their outcomes, are detailed, along with possible solutions. A summary of these attacks and their solutions is provided in Table 3.

A. PROCESS ORIENTED ATTACKS

Here, the goal of the attacker is to manipulate the wireless sensing process, including sensing modes, methods, and mapping approaches, to either degrade or tamper with the wireless sensing process and the resulting REM. The attacker can then exploit the radio environment resources undetected or deteriorate the performance of other nodes or applications.

1) ATTACKS AND SOLUTIONS RELATED TO SENSING METHODS

The knowledge of the specific sensing method allows the manipulator to tailor its attacks accordingly.

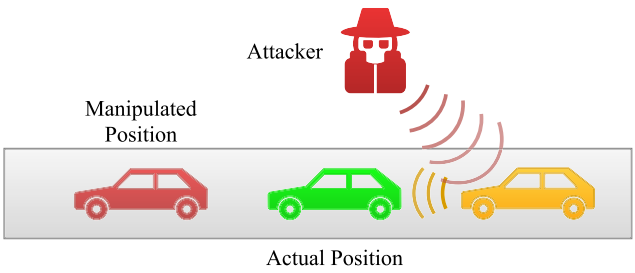


FIGURE 11. Radar/JRC manipulation in vehicular systems. The attacker manipulates the radar/JRC signal such that the next car seems farther than it actually is.

1) *Radar/JRC manipulation*: The goal of radar spoofing can be to add, remove, and/or change the location of existing objects [84]. Figure 11 illustrates a radar spoofing attack where the position of the green car is manipulated such that it seems further than it actually is, leading to a collision between the orange and green car. To add a fake obstacle, the spoofed radar signal should be a sum of multiple spoofed signals with the delays and phase offsets corresponding to the desired ranges and velocities of the fake objects. This

can be accomplished by either *replaying* previously recorded legitimate signals or transmitting new signals with the same characteristics as the legitimate one. The former can be accomplished with digital radio frequency memory (DRFM) systems, which are able to record signals and transmit them with adjusted parameters, such as delay, frequency, phase, and polarization offsets [85]–[87]. For example, a DRFM system is utilized in [88] to spoof passive radars, which do not actively transmit signals, but rather opportunistically use signals transmitted by other devices, including cellular and TV transmissions.

Removing or changing the location of existing obstacles is more difficult. For example, in [84], three spoofing attacks are proposed - random signal attack, synchronous attack, and asynchronous attack. The attacks vary on how the direction of the object (with respect to the radar) is spoofed. In a random signal attack, assuming that the radar receiver uses an optimal estimator to estimate the AoA, the attacker transmits a Gaussian waveform with controlled power. This causes correlation with the radar's own signal, leading to the incorrect estimation of AoA. For synchronous and asynchronous attacks, the attacker must eliminate the signal reflected off of the object before transmitting the spoofed radar signal. Here, the attacker can use a jamming signal can be used to eliminate legitimate reflection. Then, for synchronous attack, spoofed radar signals are transmitted to the radar receiver using coordinated multipoint (CoMP) such that they add constructively at the radar receiver to mimic an object between the attackers. For this technique to work, the attackers must be perfectly synchronized, otherwise the transmitted signals can be separated by the radar receiver. For asynchronous attacks, there are two attackers. One attacker transmits the spoofed signal with correlated noise while the other transmits only correlated noise. This causes the spoofed signals to be correlated at the receiver such that the received signal appears to come from a different direction (AoA), thus changing the detected location of the object. Here, the second attacker also acts as a jammer eliminate the legitimate reflection.

The first line of defence for spoofing attacks on radar systems is detecting and filtering the spoofed radar signals. Proposed solutions are required to detect the illegitimate signals in a timely and consistent manner, while not interfering with other functionalities or devices [89]. The LPI-based solutions mentioned earlier in the context of exploratory attacks are also applicable here since they make it difficult for an attacker to intercept and target the radar transmissions. Furthermore, a randomized probing in time can be used to detect manipulation attacks where the radar randomly stops transmitting and listens to any other incoming signals [90]. An attacker might need some time to detect the discontinued transmission before it can turn off its own signals. This latency exposes the manipulation attempt at the cost of a gap in sensing and sensed information. An extension to this approach in the spatio-temporal domain is also possible, in which multiple narrow beams are sent in random directions and their reflections are observed. Any received signal from an unprobed direction indicates the presence of a possible manipulating node [91]. Similarly, randomized frequency hopping during a single frame transmission is also proposed to detect attackers [92]. Here, the radar/legitimate knows the frequency hop time and sequence, while the attacker does not. Therefore, when the reflected signal is received and reconstructed, the peaks of the beat frequency of the attack signal are spread out and are lower, while the legitimate signal's are precise and higher. Network-level solutions are also possible, where radar traffic can be analyzed and machine learning techniques can be used to detect spoofing signals [93]. JRC can be more robust to spoofing due to the required authentication techniques used in communication [94].

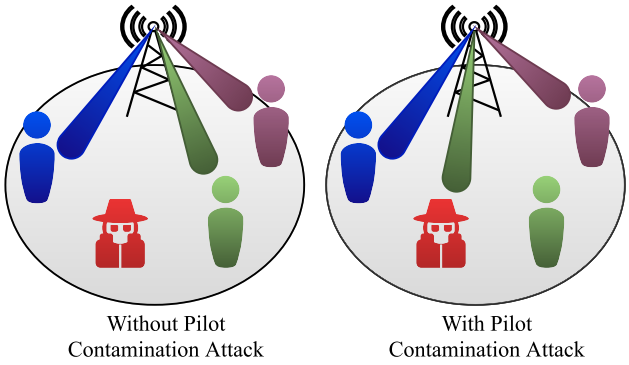


FIGURE 12. Pilot contamination attack on reference signal.

2) Communication & reference signal manipulation: An attacker with precise knowledge about the control signals, reference signals, and pilots can launch replay, pilot contamination, and conventional spoofing attacks. Replay attacks are similar to that in radar manipulation and are often seen in GPS spoofing [95]. In pilot contamination attacks, pilots similar to that of the legitimate node are transmitted by the attacker, causing an incorrect estimation of the channel. This will impair CSI-based mapping methods and sensing, along with other CSI-based communication designs, such as precoding and beamforming. Pilot contamination attacks can also be used to enhance an attacker's eavesdropping ability [96], as shown in Fig. 12. Similarly, the transmitted signals containing REM information can be spoofed to report incorrect measurements.

A possible solution for these attacks is to allow the legitimate nodes to compare either their channel estimates or the generated secret key at the physical layer [96]. Other solutions for the detection of such attacks include employment of random pilots that are selected from a set of known constellation symbols [97], pilot superposition with random signal [98], energy ratio test [99], and two-way training method [100]. The solutions explained in Section V-B (Node Oriented Attacks) are also applicable for communication/reference signal spoofing.

2) ATTACKS RELATED TO SENSING MODES

As explained erlier, the sensing modes are based on different application-specific parameters such as sensing rate f, sensing period T, update threshold Th, and so on, which can be attacked to affect the overall performance. These attacks include sensing session duration attack, threshold-based manipulation, and attack(s) on opportunistic/passive modes.

1) Sensing session duration attack: This attack is based on the exploitation of the sensing period parameter T of sensing modes. More specifically, if the attacker knows the duration of the sensing session, it can hide its presence by exploiting resources outside of that period, resulting in measurements that are useless, as they do not reflect the actual status of the radio environment. Alternatively, it can intelligently attack only during that period to reduce the sensing quality. This would also allow more efficient use of the attacker's resources.

Since these attacks exploit knowledge of the sensing duration, an effective solution can be the random initiation and duration of a sensing session [101]. An attacker can not detect this strategy immediately and thus can be detected. Another solution can be continuous sensing or sensing for a very long time period, and thus not giving a chance for the attacker to utilize the resources. These solutions, however, are subject to the requirements of the sensing performance. Other solutions may include analysis of the efficiency of different resources used by the overall network to detect the exploitation of resources by an attacker. This area, however, requires further study for the development of better solutions.

2) Threshold-based manipulation: The threshold parameter plays an important role in deciding when, and if, sensing transmissions need to be carried out and the corresponding extracted information shared with the other nodes in the network. Keeping this in mind, if the threshold value is transmitted by the application device and intercepted by the attacker, it may launch two kinds of attacks. It may change the environmental information just enough to create frequent threshold crossing, triggering renewed sensing and increased overhead of the measurement transmissions and processing. Alternatively, it can ensure that the change in the environment (and REM parameters) is less than the said threshold so that an update of sensing is not triggered. Meanwhile, it can go on and use the resources without being found out.

In the former case, an approach similar to the hysteresis margin for alleviating ping-pong handovers in cellular networks [102] can be utilized to avoid unnecessary or redundant sensing updates. Rather than triggering the update immediately after the threshold is crossed, the system can wait for a predefined (or adaptive) margin [103] to ensure the change in environment is indeed stable and not just the result of a malicious attack. In fact, the adaptive hysteresis approach along with randomized sensing can also help identify the threshold attacks of the second type. However, at present, there is a scarcity of literature surrounding such attacks and their solutions.

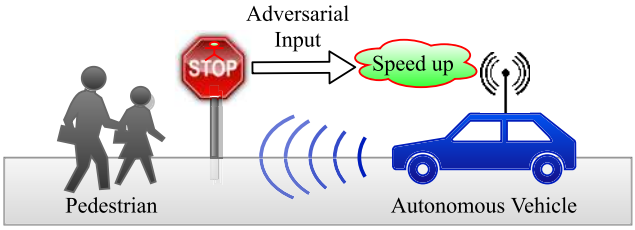


FIGURE 13. Example of an adversarial (evasion) attack in vehicular communication with a manipulated road sign.

3) Attacks on opportunistic/passive modes: Unlike periodic sensing, where the legitimate node is aware of the sensing signals and their parameters, opportunistic sensing only knows certain parameters of the signals, while passive sensing is unaware of the majority of these parameters. The dependency of these sensing modes on external signals, and the inability to send sensing signals of their own renders them more vulnerable to manipulation attacks. Common manipulation attacks such as replay, falsification, and impersonation can have a more profound effect on the sensing quality in the opportunistic/passive modes as compared to periodic sensing.

The solutions for ensuring authentication/message integrity presented in Section V-B (Node Oriented Attacks) are also applicable for both cases. Additionally, blind signal analysis (BSA) [104] and AFE-based authentication [21] can be performed. However, in the passive mode, if there is no apriori fingerprint information on the legitimate nodes in the network, reliable authentication may not be possible. In this case, fingerprint-based node differentiation and social reputation assignment [105] can be used to distinguish between legitimate and illegitimate nodes, thus filtering manipulation attempts.

3) ATTACKS RELATED TO MAPPING METHODS

The knowledge of the mapping method used to derive information from the observable data can be leveraged to launch effective attacks by the manipulator. Some of the attacks relevant to this are described below:

1) Adversarial attack: Machine learning has found increasing application in the domain of communication and sensing for various learning and decision making problems. As such, this renders these processes prone to the same threats faced by classical machine learning problems. These threats can be roughly categorized into *poisoning*, *evasion*, *model inversion* and *extraction* [106].

Poisoning refers to the malicious corruption of the training data such that the learned model is inaccurate and may provide wrong decisions. Evasion, on the other hand, involves the attacker adding certain features to its own information/data such that the classifier predicts a wrong label. Figure 13 illustrates an evasion attack where the attacker adds some features to the stop sign, making it appear as a command/suggestion to speed up the vehicles. This may cause collisions or harm the pedestrians crossing the road.

In model inversion, the attacker attempts to learn about the source of the (training) data from the model itself. This poses risks to the user's privacy. Model extraction, as the name suggests, refers to the learning of the model and its parameters by the attacker. Apart from compromising the intellectual property, this attack and the consequently learned parameters can then be used to launch more effective inversion and evasion attacks. Specifically, in the domain of wireless communication, a generative adversarial network (GAN)-based spoofing attack has shown to be effective enough to possibly mitigate authentication mechanisms such as AFE fingerprinting [107]. Similarly, other attacks realized through adversarial ML such as jamming, priority violation, and spectrum poisoning have been illustrated in [108].

Out of the aforementioned attacks, evasion is arguably the most well-studied. A popular solution against this attack is *distillation*, where the knowledge from a deep neural network (DNN) is used to increase its own robustness to adversarial data [109]. An improved *region-based classification* technique [110] is also proposed where samples around the test data are also passed through the learned/trained model and majority polling of the outputs of these samples is considered to be the output label of the desired sample. Another approach to mitigate these attacks has been provided in [108], where the defense mechanism tries to increase the uncertainty for the attacker in its inference stage, i.e., when it is learning about the ML algorithm deployed in the system. Apart from the specific solutions developed in the domain of ML to address these adversarial attacks, ensuring that only authentic data is fed to the mapping algorithm is imperative. Furthermore, any unauthorized access to the data or the learning needs to be eliminated.

2) Spatial interpolation attack: Interpolation methods are extensively used in REM construction. Inverse distance weighting [111] and Kriging algorithm [112], [113] are some of the more classical methods used for this purpose. These methods are sensitive to outliers which can be exploited by an attacker [114]. Some recent works have also explored the use of GANs for spatial interpolation [115], [116]. Intuitively speaking, an attack on spatial interpolation can be considered as a special case of the aforementioned adversarial attacks, where interpolation model/data is targeted. Alternatively, it can follow a model extraction attack. An example pertaining to the first case can be derived by switching the perspective of the solution provided in [108], where the learning can be adversely affected by increasing the uncertainty in the system. In the case of the latter approach, an attacker can exploit the knowledge of positions of the nodes and the interpolation method to communicate or launch attacks in locations between the nodes, ultimately rendering the sensed information useless. This may enable an attacker to go undetected while exploiting the resources of legitimate nodes, degrading their performance.

A crowdsourcing approach to address the interpolation attacks is proposed in [117], where REM is built in an iterative manner. The process starts by utilizing information from a small number of trusted nodes and updates the REM by incorporating measurements from other nodes after evaluating their trustworthiness, as presented in Fig. 14. This evaluation considers the alignment of information provided by trustworthy sources nearby and the user's long term behavior. A large number of measurements/observations means an increased spatial resolution of correct data for the interpolation. This limits or reduces the space or locations where the manipulators can attack, mitigating the outlier problem in the process. Furthermore, the attacks related to model learning and poisoning can borrow the solutions of adversarial attacks described above.

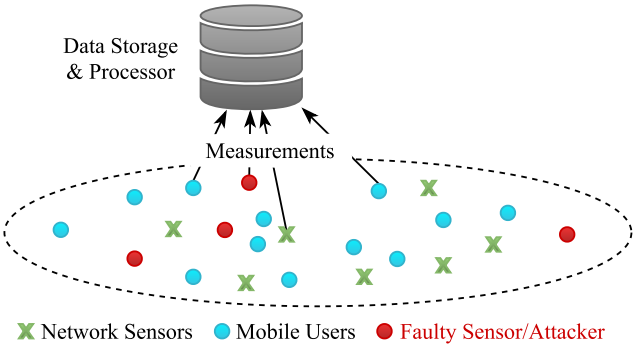


FIGURE 14. Crowdsourcing against manipulation attacks.

B. NODE ORIENTED ATTACKS

Node oriented manipulation attacks target different nodes by violating their authenticity or the integrity of the contents/characteristics of the wireless signal. They can manipulate identity, synchronization, data, position, patterns, etc. These attacks are categorized as follows:

1) Authentication violation: In this attack, the attacker poses as a trustworthy participating node (IN, CN or RN) in the REM system [118]. Examples of this are impersonation and man-in-the-middle attacks. Once the attacker establishes itself as part of the network, it can propagate faulty information regarding the content/characteristics of the wireless network.

2) Integrity violation: These attacks breach the data integrity of REM by launching malicious attacks [119] such as false reporting about location, falsified information injection, data modification, and Global Positioning System (GPS) spoofing attack. The aforementioned threats can be realized by a compromised node (IN, CN or RN), which has been taken over by the attacker.

3) Emulation attack: This attack is based on emulating the features of legitimate transmission to deceive the legitimate nodes about resource occupancy. A popular example of this is primary user emulation attack (PUEA) in CRs, where the attacker mimics the characteristics of the primary users (PUs) in order to raise false alarms regarding spectrum occupancy [120].

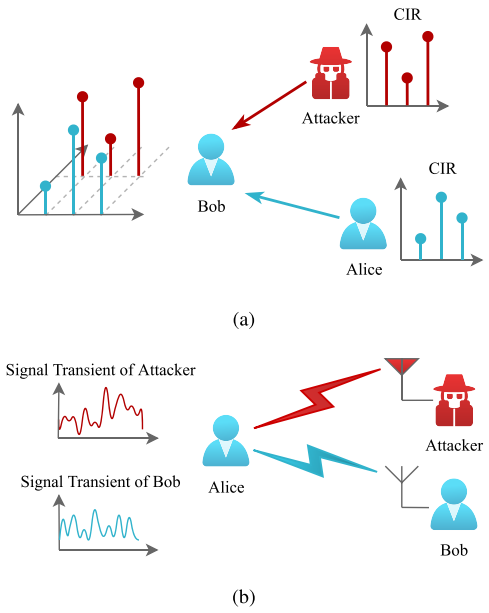


FIGURE 15. Passive PLA approaches (a) Channel-based, (b) AFE-based.

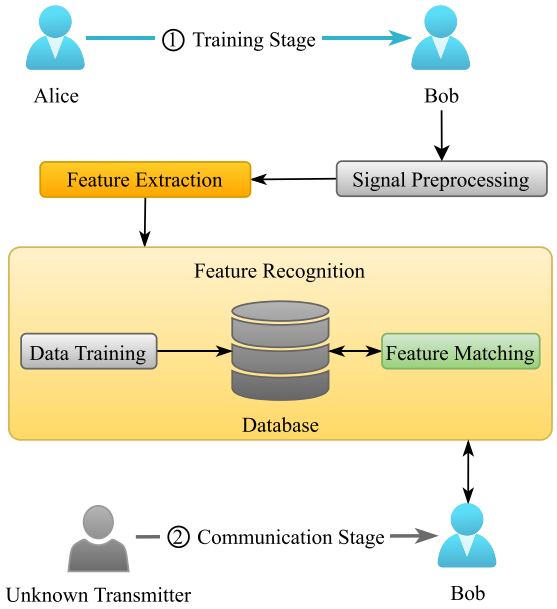


FIGURE 16. Basic steps for passive PLA algorithms.

Popular physical layer authentication (PLA) techniques against node orientation manipulation attacks are divided into the following categories:

1) PASSIVE SCHEMES

This group of solutions leverages the properties of the physical layer characteristics of the received signal, e.g., channel and/or AFE characteristics [23] for authentication as shown in Fig. 15(a) and Fig. 15(b), respectively.

Any passive PLA method comprises of two stages: training and message transmission [25]. In the training stage, features related to legitimate nodes are collected and selected in order to construct a reliable database of (channel/device) fingerprints. In the message transmission stage, the receiver receives a noisy version of the signal from an unknown transmitter. It extracts the useful features from the received signal. Afterward, it compares the extracted features with the database fingerprints to verify the identity of the transmitter. A flow diagram of passive techniques is illustrated in Fig. 16. The training and final verification steps can be done with and without ML and DL algorithms. However, ML and DL methods are very effective for enhancing the performance of PLA methods [121].

1) Channel-based PLA: Channel-based PLA techniques are based on exploitation of unique radiometric features of propagation environment between communicating nodes such as CSI, RSSI, AoA, AoD, and RTT [23]. These techniques are based on the assumption of the channel decorrelation. Hence, CSI of nodes located at different locations can be used as fingerprints for their identification in the network [78]. Moreover, it is also assumed that the channel observations are highly correlated in training and message transmission or channel coefficients vary slowly between training and transmission period.

Channel-based PLA methods work well in a slow varying environment. However, in the case of a time-variant or fast fading environment, the basic algorithms need to be modified. The modification approaches to overcome the channel dynamics include channel tracking methods based on time-varying multipath correlation models [122]–[124] or clustering the observations leveraging ML and DL approaches [125], [126].

2) AFE-based PLA: AFE based techniques are based on exploitation of AFE front-end imperfections caused by various manufacturing and environmental factors, such as phase noise, in-phase/quadrature imbalance (IQI), carrier frequency offset (CFO), imperfect power amplifier, power spectral density (PSD), clock offset, and imperfect antenna array design [23]. As explained earlier, in the training state the database is constructed based on different AFE features and then the resultant database is used for authentication during the message transmission stage. Compared to channel-based authentication, AFE based features are more stable with time [127].

It is possible to use the channel and AFE-based mechanisms together, with different weights depending on the scenario at hand. This enables more robust, reliable, and secure PLA. For instance, AFE-based approaches might be more reliable in the case of a mobile environment as compared to channel-based solutions. Finally, ML can be utilized to enhance the performance of passive PLA mechanisms by determining the most effective features for discrimination between devices [25], [128].

2) ACTIVE SCHEMES/WATERMARK EMBEDDING-BASED PLA

As the name suggests, active schemes intentionally incorporate some sort of identity information at the physical layer in

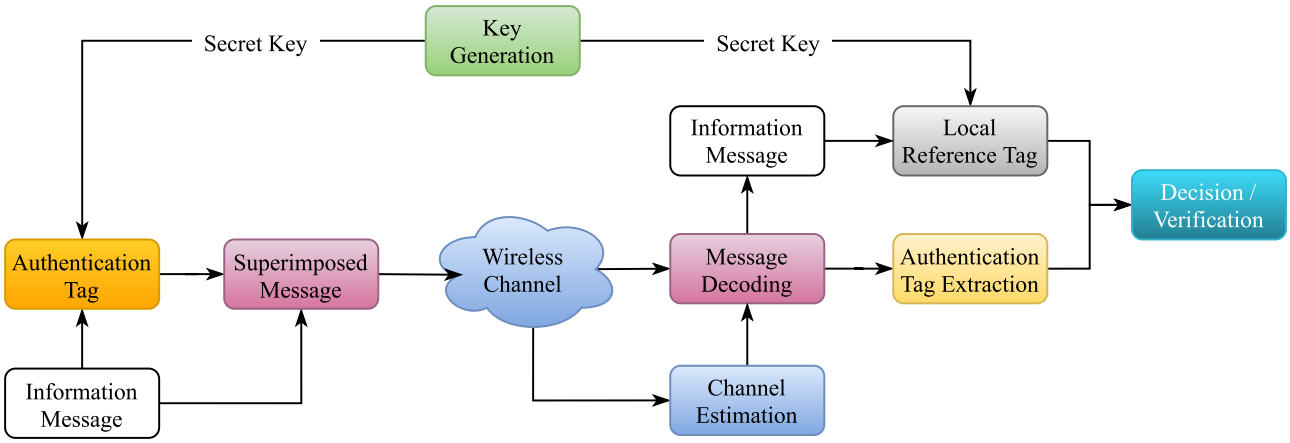


FIGURE 17. Basic framework of active PLA techniques.

the communication rather than relying on the device front-end or the channel to provide it. This information, referred to as a *tag*, is added based on a pre-shared (or channel-based) key and a complicated tag generating function [129]. This approach provides not only a way to authenticate the node but also ensures the integrity of the message since any manipulation of the message would alter the tag as well. Time-varying tags can also provide robustness against replay attacks, which might otherwise pass the conventional authenticity checks. The basic framework for active schemes is shown in Fig. 17. In the first step, the transmitter generates an authentication tag as a function of a secret key and information message using tag generating function [104], [130]. Note that the power should be allocated properly between the signal and tag while considering the robustness, security, and covertness requirements. Afterward, the resultant tag is superimposed with the information message and sent through the wireless channel. At the receiver (authenticator), the tag is extracted from the received signal first. Afterward, the extracted tag is compared with the locally generated tag to verify the source. The authentication tag can be added to the data frame [130] or to the training pilots [104]. Other types of the active schemes using pre-shared key include transmission parameters modification [131], [132], frame structure modification [133], and tag insertion by replacing source data bits [134].

C. ENVIRONMENT ORIENTED ATTACKS

These attacks affect the propagation environment, alter the physical objects, and change the environmental conditions. The goal of these attacks could be to fool resource allocation and optimization algorithms, causing the selection of sub-optimal parameters for communication transmissions. Similarly, these attacks could aim to cause frequent updates of the REM, preventing network entities from using it, and wasting the computational and power resources of the REM device. For instance, RISs can be used by the attackers to generate a fake multipath channel or absorb signals to misrepresent the coverage area. Similarly, devices sensitive to heat, sound, electromagnetic waves, humidity, rain, wind, pressure, and other physical and environmental conditions can be manipulated by artificially changing these conditions.

The solution against artificial environment manipulation is an open issue from a wireless sensing point of view. However, it is possible to detect such attacks using external sensors, such as cameras, sensor fusion techniques, or sensor networks. For example, collaborative sensing or crowdsourcing can be used.

VI. DISRUPTION ATTACK

The purpose of a disruption attack is to introduce disorder in the communication and/or sensing processes. The most popular manifestation of this attack is the disruption of the contents and characteristics of wireless signals by directing intentional interference towards communication/sensing systems [17]. For example, in wireless communication, the power of the received signal must be more than the overall power of ambient noise and interference. However, the attacker intentionally increases the interference level in the transmission channel which leads to the disruption of legitimate transmissions. This degrades the overall performance of both communication and sensing and can affect network service availability. Moreover, it will also cause wastage of resources. Figure 18 represents a disruption attack at Alice and Bob, where at Alice it raises a false alarm about channel occupancy while at Bob it degrades the signal quality. A summary of the disruption attacks and possible solutions is provided in Table 4.

A. CONVENTIONAL JAMMING TYPES AND DETECTION

There are various approaches that can be utilized by a disruptive attacker (jammer) to interrupt wireless communication and/or sensing [16]. The crudest form of jamming attacks is the *constant* jamming, where the attacker transmits an interfering signal continuously over the same spectral resources as the legitimate nodes. This signal may be pseudorandom noise or a modulated waveform. Not only does such an attacker lead to degraded SINR, but it also makes

TABLE 4. Disruption attacks and solutions with selected references.

Threats type	Attack orientations	REM components	Threat details/type	Solutions
Disruption attack	*Process*	Sensing methods	Causing interference to affect the performance of pilot, radar, and JRC based sensing.	Cooperative relaying schemes [138]–[140] RIS assisted Solutions [141] Spread Spectrum Techniques [142] Channel Surfing & Protocol Hopping [143] Multi-Antenna-based Approaches [144] Machine Learning and AI-based Solutions [145] [146]
		Mapping methods	Flooding attack to degrade mapping procedures.	
	Nodes	Initiation nodes	Bombarding nodes with unnecessary messages to hamper resource availability and signal quality.	
		Responding nodes		
		Communication nodes		
	Environment	Propagation	Creating interference in different regions of the environment to affect sensing information related to the environment.	
		Conditions		
		Hardware/objects		

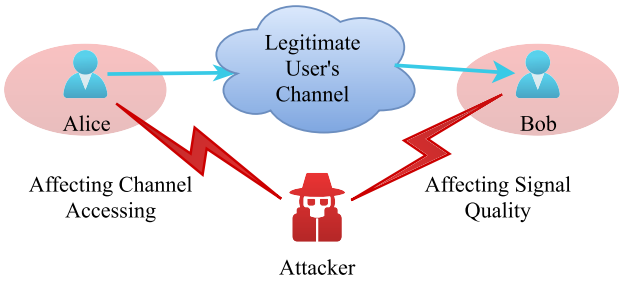


FIGURE 18. Disruption attack at transmitter or receiver.

the channel busy for legitimate node. This jamming approach can be detected by observing parameters such as RSS, packet error rate (PER), and carrier sensing time [135]. As compared to normal communication, the former two would be increased while the distribution of the latter would vary under a jamming attack. A slightly more efficient form of jamming is the *intermittent* attack where the attacker randomly alternates between transmitting the interfering signal and sleeping (no transmission during this period). This provides a trade-off between energy consumption and jamming effectiveness. This type of attacker can also be detected by the methods described for a constant attacker.

Reactive jamming provides a more sophisticated attacking model. Here, the attacker senses the channel and only attacks when it detects an ongoing legitimate transmission. This renders these attacks more energy efficient as compared to constant and intermittent ones. However, this also means that this attack does not have any effect on the channel access procedure of the legitimate nodes. This renders the carrier sensing time approach invalid for reactive jamming detection. The RSS and PER approaches are, however, still applicable. An *adaptive* attacker possesses the additional ability to modify its transmit power depending on the legitimate user's channel condition. Similar to the reactive attacker, it senses the legitimate transmission, and then depending on the RSS at the legitimate node modifies the power of the jamming signal to disrupt the legitimate transmissions. As such, this allows the adaptive attacker to be the most energy-efficient of the aforementioned jamming methods. However, achieving this jamming capability requires knowledge of the legitimate channel which renders this attack impractical in most real-life scenarios. Such attacks can be detected by jointly considering PER and RSS statistics [135]. Generally, increased RSS improves the PER of a communication system. But in the case of a jamming attack, the PER would decrease even though RSS increases.

While these attacks use little to no information about the communication protocol being used by the legitimate node, an *intelligent* attacker can leverage such knowledge to disrupt the communication. Rather than trying to interfere continuously with the legitimate nodes, this attacker only targets certain critical control signals such as Request To Send (RTS)/Clear To Send (CTS) or Acknowledgement (ACK) frames in Wi-Fi. As per the Wi-Fi protocol, after sensing the channel to be available for a certain duration, the transmitter sends an RTS frame and waits for the CTS response from the receiver. Once the receiver is ready to receive, it sends the CTS frame. If the attacker can ensure these packets are not correctly delivered, it can halt the legitimate communication. Similarly, jamming the ACK message can lead to unnecessary re-transmissions and resource wastage. The detection of these attackers is quite difficult but careful tracing of MAC control packets and identification of any abnormality can indicate the presence of an intelligent attacker [16].

B. PROCESS ORIENTED ATTACKS

1) ATTACKS RELATED TO SENSING METHODS

Disruption attacks can affect the reliability of the content and characteristics of the wireless signals by transmitting a jamming signal during the usage of different sensing methods.

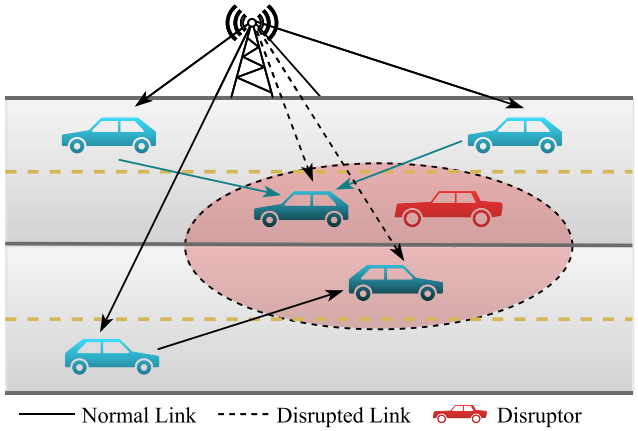


FIGURE 19. Cooperative relay-based anti-jamming solutions.

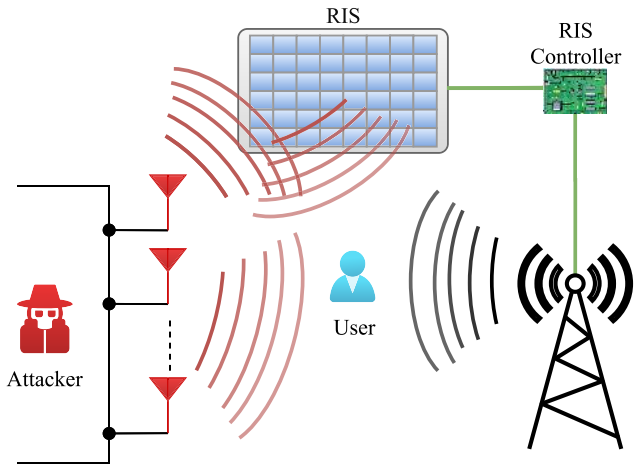


FIGURE 20. RIS-assisted anti-jamming solutions.

The general approach for mitigating disruption attacks involves either providing some sort of diversity or avoiding the interfering signals. The former approach includes techniques such as multi-antenna and cooperative relaying schemes, while spread-spectrum and protocol hopping techniques [136] fall under the latter category.

1) Cooperative relaying schemes: Cooperative communication with trusted relay(s) is one of the simplest anti-jamming solutions for both communication and sensing. Particularly, the use of relay selection and cooperative beamforming techniques [137], [138] provides alternate path(s) for signal propagation between the legitimate nodes, mitigating the effect of disruption caused by the attacker. This phenomenon is illustrated in Fig. 19, where attacker, relays, and intended receivers are shown in red, green, and black, respectively. The attacker disrupts the legitimate transmissions in its surroundings, however, the relays cooperate to serve the legitimate receiver. Recent literature has also proposed the use of unmanned aerial vehicles (UAVs) as relays due to their three-dimensional mobility and easy deployment [139].

2) RIS assisted anti-jamming solutions: The channel manipulation capability of RIS can be exploited to mitigate

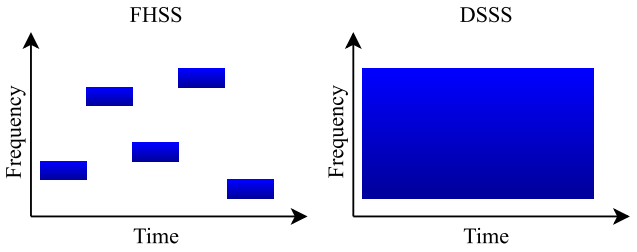


FIGURE 21. Spread spectrum (FHSS and DSSS) based anti-jamming solutions.

jamming by adjusting the phase and/or amplitude of the reflection of incident jamming signals to weaken their effect at the legitimate nodes [140]. For example, in Fig. 20, Bob will receive signals from Alice, attacker, and a reflected version of the jamming signal from the RIS. Here, the RIS adjusts the phases of its elements such that the original and reflected jamming signals are destructively added at Bob. The RIS can also be used to provide alternative paths for the legitimate signal.

3) Spread spectrum techniques: The solutions mentioned earlier in the context of exploratory attacks based on the spreading of energy in time and frequency are also applicable here from both communication and sensing perspectives. These techniques make signals robust to disruption attacks due to the spread of energy in different domains [141]. Examples of spread spectrum techniques are frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), chirp spread spectrum (CSS), parallel-sequence spread spectrum (PSSS), time-hopping spread spectrum (THSS), and their hybrid variants. However, the most popular of them are FHSS and DSSS.

In FHSS modulation technique, narrowband jamming is avoided by changing the carrier frequency repeatedly. The shifting in frequency over the whole spectrum is based on pre-shared secret sequence or PLS key generation. Similarly, DSSS is another effective technique against narrowband jamming attacks, where the transmitted signal is expanded into a wider frequency band by multiplying it with a secret key based pseudo-noise sequence. As a result, the narrowband jamming signal can only affect a negligible part of the transmitted signal's frequency spectrum. Figure 21 illustrates the concepts of FHSS and DSSS. Although FHSS and DSSS are effective anti-jamming techniques, they both require a wideband spectrum, which makes them spectrally inefficient.

4) Channel surfing & protocol hopping: Channel surfing is an adaptive form of FHSS in which the carrier frequency is not hopped continuously as in FHSS. Instead, the frequency is shifted to another frequency after the discovery that the current band is being jammed. The jamming can be detected based on the high PER and high RSS values. Similarly, protocol hopping is another interesting anti-jamming solution. In these solutions, legitimate nodes hop between different available protocol parameters (or even technologies) to ensure reliable communication even in the presence of an attacker [142].

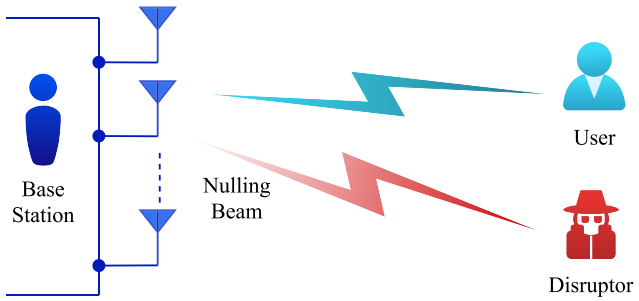


FIGURE 22. Multi-antenna based anti-jamming solutions.

5) Multi-antenna-based approaches: Multi-antenna systems enable the use of adaptive antenna arrays and digital beamforming for directional transmission to avoid interference from unwanted sources. Particularly, it allows the node to receive signals from a particular direction and also enables adaptive beam nulling in the direction of jamming sources as illustrated in Fig. 22 [143]. This provides an enhancement in communication and sensing performance as well as robustness against the disrupting attacks for both communication and radar systems.

6) Machine learning and AI-based solutions: Recently, some ML based approaches have been developed to combat jamming/disruption attacks. For instance, [144] considers the use of deep reinforcement learning to learn the attacker's strategy. Once the strategy is learned, the legitimate nodes find the optimum countermeasures. The authors consider adapting the transmission rate, harvesting energy from the received interfering signal, or using this interfering signal to transmit the legitimate one by leveraging ambient backscatter communication (ABC) techniques as possible mitigation options. This approach, however, is not applicable to reactive attacks since they are preceded by channel sensing done by the attacker. To address this, [145] proposes the use of "fake" transmission to stimulate the reactive attacks. The interfering signals sent as a result are then used either for energy harvesting or ABC. Not only does this approach deplete the energy of the attacker, but also allows the legitimate nodes to transmit with more power (using the harvested energy). This approach may be of particular interest for power-limited use cases such as IoT. Reinforcement learning has also been used for joint optimization of anti-jamming power allocation and reflecting beamforming in RIS-assisted [140] mitigation techniques.

2) ATTACKS RELATED TO MAPPING METHODS

Disruption in the mapping methods can occur when there are more readings than can be processed in the designated or required time interval, which is referred to as a flooding attack. This can happen during model learning, where the mapping model is being formed, or afterward. The aim of the attacker, in this case, is to flood the RN or IN with data to significantly degrade or disrupt the mapping method. For example, an illegitimate user can send more repeating measurements than the required amount within a packet. In the learning stage, this can significantly increase the learning period, thus disrupting the method. In the mapping stage, this can fill the buffer of the processor, making it take longer to get to the actual measurement, leading to out-dated decisions or outputs.

Here, the goal of the solution should be to detect and remove the incoming fake data or sensing transmissions in a simple and quick manner. In feedback based periodic sensing mode, the attacker or corrupted RN can send random data or multiple replications of the actual measurement along with the real measurement in the packet. In the former case, fake data can be detected by predicting the expected measurement and discarding the data which deviates from the prediction. Then the remaining measurements can be averaged to get one measurement. This is suitable for phenomena with temporal correlation. No doubt, this would reduce the accuracy of the mapping, but may still give usable results. The pattern of fake and real measurements in the transmitted packet, if there is one and it can be deduced, can be used to ignore those carriers which contain fake measurements. If the ratio between fake and real measurements is known, this could also be used to discard some measurements, at the cost of accuracy. In the latter case, dimensionality reduction methods can be used to reduce the complexity/number of measurements to be processed. More solid solutions would involve the physical and MAC layer designs. Here, protocols and standards could be developed to perform handshakes for every measurement and prevent the overloading of packets with measurements. However, this would be at the cost of incurred delays, additional complexity, and reduced spectral efficiency. Alternatively, detecting the attacker or corrupted node would allow ignoring measurements from these nodes.

C. NODE ORIENTED ATTACKS

Similar to the disruption attack covered in the context of mapping methods above, it is possible for a RN to be made to bombard the IN with unnecessary/repetitive messages, possibly disabling it from carrying out any communication or sensing with other nodes. This disruption approach, however, is preceded by manipulation of the said RN. Therefore, the solutions presented in both Section VI-B1 (Attacks Related to Sensing Methods) and Section V-B (Node Oriented Attacks) are applicable here.

D. ENVIRONMENT ORIENTED ATTACKS

The basic idea here is to generate interference in certain regions to disable communication or sensing. For example, smart environment technologies, such as RIS, can be used to reflect any incoming signals to locations of the RN or IN, rendering them unable to extract the sensing or communication signals and take measurements [146]. Alternatively, frequent and repeated artificial environment manipulations can be made, which may result in frequent and/or redundant triggering of the REM process. These attacks essentially cause the thresholding related attacks, therefore, the solutions

presented in Section V-A2.2 (Attacks Related to Sensing Modes - Threshold Based Manipulation) and Section VI-B2 (Attacks Related to Mapping Methods) are applicable here.

VII. CASE STUDY: SECURING REM IN ITS/V2X

A. BACKGROUND

This section highlights intelligent transportation systems (ITSs) and V2X communication to exemplify the need for a secure radio environment awareness and mapping process. Solely from a financial standpoint, V2X networks present a huge opportunity with a forecasted market of over $110 billion by 2026 [147]. The numerous sensors onboard autonomous vehicles and their need to communicate with each other, road-side units (RSUs), and other traffic infrastructure necessitate an intelligent and secure integrated sensing and communication system to ensure a safe, economical, and overall more efficient driving experience [148].

The importance of this use case is also illustrated by the various standardization efforts carried out to fulfill its requirements. At present, there are two main families of candidates for V2X communication, namely, IEEE 802.11p based dedicated short-range communications (DSRC) and ETSI's ITS-G5 standards, and the 3rd Generation Partnership Project (3GPP) backed cellular V2X (C-V2X) standard [149]. The emergence of these competing standards has led to various studies being conducted related to their performance comparison [150], inter-working [151], and coexistence [152]. While DSRC/ITS-G5 standards have the advantage of being more mature technologically and operating on license-exempt (free) bands, they might have congestion issues in case of dense deployments with collisions in channel access. Furthermore, the autonomous vehicles would require much higher bandwidths for image processing applications, which might not be supported by these standards. C-V2X, on the other hand, might be able to address these issues but would take a while in ensuring the provision of a communication infrastructure strong enough to support the requirements of V2X users. It is also possible that both standards would converge at some point; DSRC/ITS-G5, for instance, might be reserved for vehicle-to-vehicle (V2V) aspect of the communication in such networks.

Both families of the aforementioned standards, however, are vulnerable to security threats. Some of these are described below, considering the radio environment awareness process and associated attacks described in Sections III–VI.

B. NEED FOR SECURITY

In the upcoming years, ITSs are expected to bring about significant developments in vehicular networks [153], [154]. With the help of REM-based radio environment awareness, assisted by advanced computing, communicating, and sensing technologies, ITS can support various useful applications. These applications include vehicular and pedestrian safety, fully/semi-automated driving, remote driving, traffic flow optimization, and efficient routing.

In order to get environmental awareness, REM can be constructed via external infrastructure and V2X communication technologies. REM in such scenarios is based on vehicular users' equipment, RSUs, road signs, traffic lights, parking areas, smart roadblocks, and cellular infrastructure. Note that V2X is a generic term given to the vehicular system. It incorporates a vehicle's communication with other vehicles (V2V), infrastructure (V2I), the network (V2N), pedestrians (V2P), surroundings (V2S), ecosystem (V2E), and transportation networks (V2TN) [154]. The construction or update of REM in V2X is vulnerable to exploratory, manipulation, and disruption attacks. These attacks can compromise the confidentiality of sensitive information and affect the overall functionality of different entities of ITSs by attacking sensing, communication, and control capabilities. For example, these attacks can affect the environmental sensing, control (of speed, steering, and brakes of semi/full autonomous vehicle), and features related to in-vehicle and external environment [155], [156]. This can cause property damages, risk the lives of the pedestrians, drivers and passengers, and degrade the overall efficiency of ITS. Some attacks on REM and their consequences on the corresponding ITS are described below.

C. THREATS AND SOLUTIONS IN V2X

The *exploratory attack* on features and contents of wireless signals in ITS system will enable the attacker to learn specific details about vehicles and vehicular networks that affect the integrity and confidentiality of REM, as illustrated by ① in Fig. 23. This includes illegitimate access to information such as driving route, mobility patterns, size, speed, engine capacity, power, terrain, traffic information, REM process-related information, mileage, network topology, and state of the vehicle. The attacker can use this information to learn about the behavior and preferences of different vehicles, design efficient manipulation and jamming attacks, track legitimate nodes or get unauthorized access to certain places/services. Popular PLS solutions for ensuring the confidentiality of contents and features in V2X communication include adaptation based security techniques (based on location, channel, and requirements of legitimate nodes), interfering signal assisted and cooperative jamming solutions, multihop V2X relaying, LPI based approaches, RIS assisted solutions, and physical layer key extraction based techniques. The details of these methods have already been explained earlier.

Manipulation attacks on the V2X REM can lead to traffic congestion, inefficient transportation, damage to property, and even danger to human lives. An attacker can modify the geospatial features/information and can create fake obstacles in the environment. Moreover, it can manipulate radar/JRC signals (by rebroadcasting the radar signals with some modification) [86] and GPS information (by sending incorrect but realistic GPS signals) to manipulate speed, range, navigation, positioning ②, cause misdetection of objects and

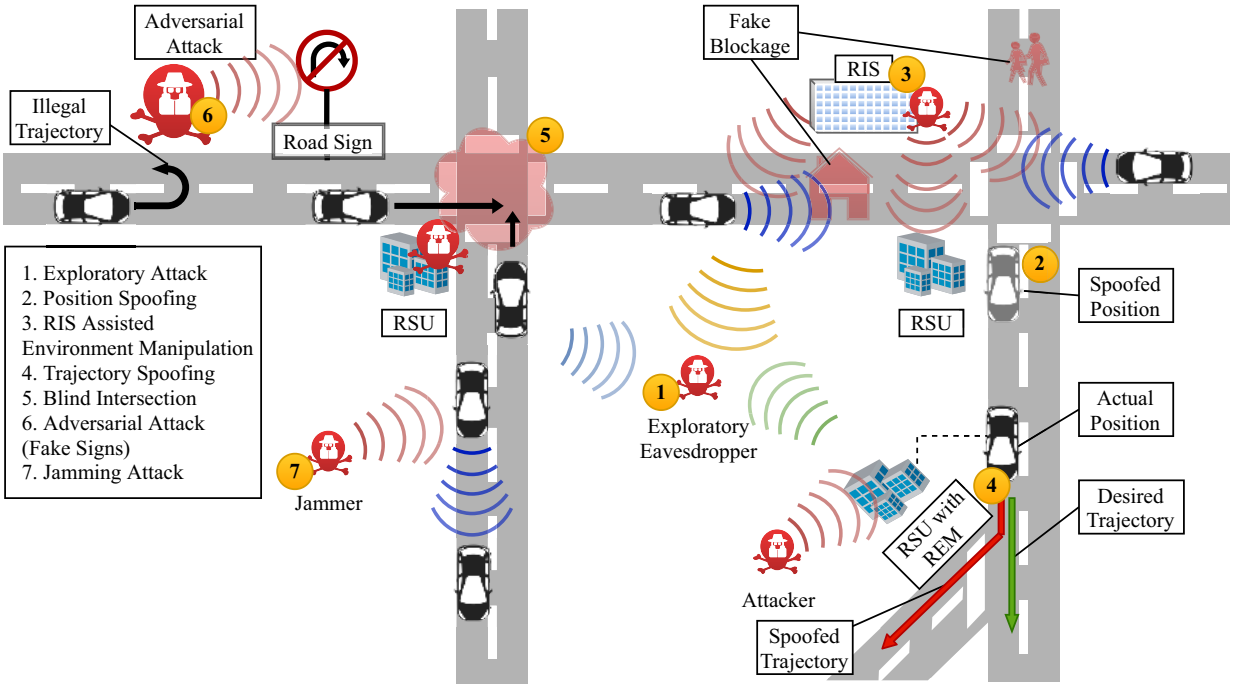


FIGURE 23. This figure depicts the security threats with related to REM and sensing.

surrounding information ③, manipulate the trajectory ④, and prevent sensing of approaching vehicles, leading to blind regions ⑤. This can have dire consequences for autonomous driving applications. Impersonation attacks can be used by the attacker, such as assuming the identity of an emergency vehicle, to acquire the right of the way in otherwise congested scenarios [157]. An injection attack can be used to inject fake/modified messages to control and manipulate the vehicular speed, brake, steering, motion pattern, and so on [158]. In the replay attack, the vehicle's real-time functionalities are impeded by re-sending authenticated frames continuously with and without modification. Illusion attacks can be used to create fake traffic by manipulating the vehicle sensors via environmental modifications. This triggers the vehicles to send false information about traffic to other vehicles. A sybil attack allows the attacker to take on multiple identities simultaneously, purporting fake traffic overflow, affecting navigation systems, and generated trajectories. Similarly, compromised RSUs can feed incorrect information to REM, leading to collisions. An attacker can also launch a timing attack to affect real-time applications, where it can manipulate the timing information by causing artificial delay to messages. Moreover, an attacker can launch an adversarial attack by modifying the road markings, traffic lights, delineations, or road signs, for example, as in ⑥, and causing incorrect and life-endangering decisions. Popular solutions to tackle these attacks include active and passive authentication schemes, distillation, crowdsourcing, and randomized probing in time/space-based techniques, as explained earlier.

The exceedingly autonomous nature of upcoming ITSs and their dependence on real-time sensing and communication assisted REM renders them vulnerable to any *disruption* [159]. For instance, disruption of the collision avoidance message between V2X entities or jamming the radar signals can lead to traffic accidents, shown as ⑦. The disruption itself can be caused by either transmitting noise-like signals or bombarding the IN or RN nodes with unnecessary messages, interfering with the ongoing transmissions. The solutions for jamming attacks include cooperative relaying schemes via different (terrestrial/flying) nodes in V2X communication, spread spectrum based techniques, multi-antenna-based adaptive beam nulling approaches, machine learning-based solutions, and RIS-assisted anti-jamming solutions, as explained earlier.

It is clear from the aforementioned discussion that, although REM assisted environmental awareness will open a new area of applications in V2X, it is vulnerable to exploratory, manipulation, and disruption attacks, which can cause catastrophic losses for ITS. Hence, efficient and effective solutions need to be applied for reaping the benefits of REM [160].

Simple simulations are presented for single-input single-output (SISO) and multiple-input single-output (MISO) case, where Alice contains two antennae while each of Bob and attacker has a single antenna, to show the effectiveness of different security techniques for V2X-REM. Figure 24(a) illustrates BER versus signal-to-noise ratio (SNR) performances at Bob and attacker node for beamforming and artificial noise-based security techniques. It is observed from

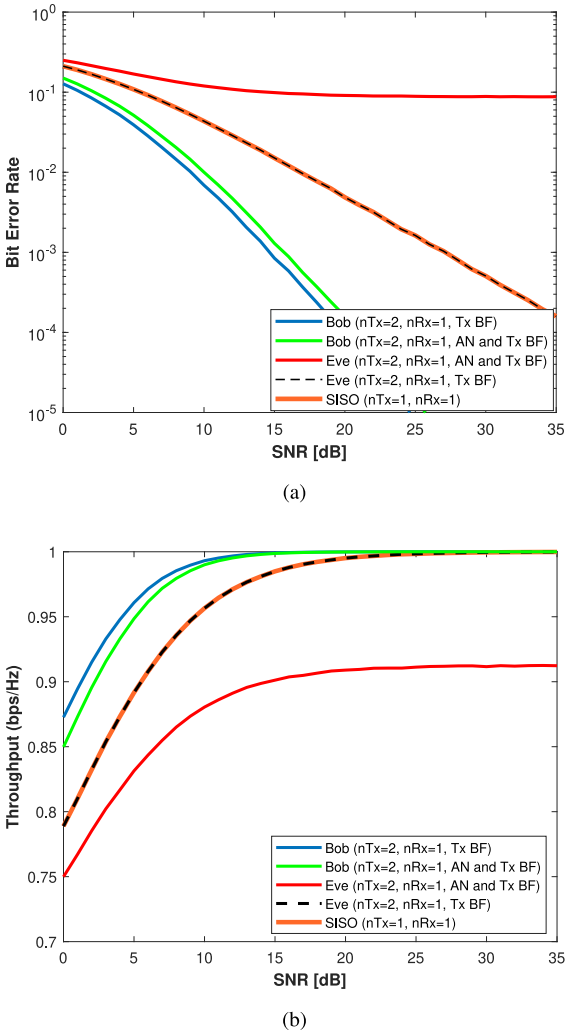


FIGURE 24. Performance comparison of transmit beamforming and artificial noise based solutions at legitimate (Bob) and illegitimate receivers (Eve). (a) BER vs SNR, (b) Throughput vs SNR.

the figure that transmit beamforming enhances the BER performance at Bob while there is no performance gain for the attacker and its performance is similar to the SISO case. Thus, the BER performance gap between Bob and attacker indicates the capability of beamforming to provide a measurable level of secrecy.

To further enhance the BER performance gap between Bob and Alice, the effect of artificial noise-based techniques is also shown in Fig. 24(a). It is clear from the figure that there is a considerable degradation in the BER performance of attacker due to artificial noise, where 20% of total transmit power is allocated for noise generation here. The power allocated can be adjusted based on the security requirements. Similarly, Fig. 24(b) presents the throughput at Bob and attacker for different schemes as explained earlier. Similar to the above observations, it is observed that beamforming based on Bob's channel enhances his throughput. Moreover, it also confirms that the injection of noise significantly enhances the throughput gap between Bob and the attacker, illustrating the effectiveness of this category of solutions.

VIII. REM-ASSISTED PHYSICAL LAYER SECURITY

A. MOTIVATION AND BACKGROUND

The increasing diversity of wireless networks and varying capabilities of devices necessitate future networks capable of intelligently adapting to user requirements on the fly, instead of being designed for a handful of scenarios [2], [4], [161], [162]. Keeping in line with the direction of this article, we look at a particular case (or requirement), namely, PLS and how REM or wireless sensing can be used to enable cognitive PLS.

The concept of adaptive or "cognitive" PLS was initially proposed in [163], which was driven by the scenario-specific PLS solutions. For instance, there are two basic approaches for securing wireless communication, i.e., increasing the SINR gap between legitimate and illegitimate nodes and using the channel reciprocity to generate keys for securing communication. The former approach fails if the attacker can improve its SINR by increasing the number of antennas or processing at its end, while the latter approach fails if the channel reciprocity assumption does not hold. This failure of reciprocity could either be due to AFE impairment mismatch at the transceivers or use of FDD mode of transmission. These issues illustrate that there is no "one-fits-all" PLS solution that can be used to secure communication (and sensing) in wireless networks. To this end, authors in [83] propose a multi-faceted coordinated defense architecture that takes into account the information about the user, application, and environment to develop secure methods corresponding to physical, network, and application layers (corresponding to the Open System Interconnection Reference Model), resulting in resource allocation for PLS methods in time, frequency, space dimensions.

B. CONCEPTUAL FRAMEWORK

Figure 25 illustrates the conceptual cognitive security framework. Information pertaining to the user, application, and environment is obtained from wireless sensing and REM. The user information includes device capabilities and AFE fingerprints, location, trajectory, and behavior while the requirements and constraints related to applications being used are also extracted. Environmental information is made up of knowledge regarding network infrastructure, propagation environment, and attributes of the physical signal, such as multiple accessing scheme, waveform, and modulation, in the surroundings. All this information is fed to a risk identification block, the goal of which is to determine the identify the potential threat types and their severity (level). For this purpose, AI/ML-based models are trained with behavioral characteristics of nodes and information of the historical social relationship between them as features [83]. Once the threat/risk identification is accomplished, the cognitive security framework decides upon the most suitable method of security provision. This block also depends on the cognition

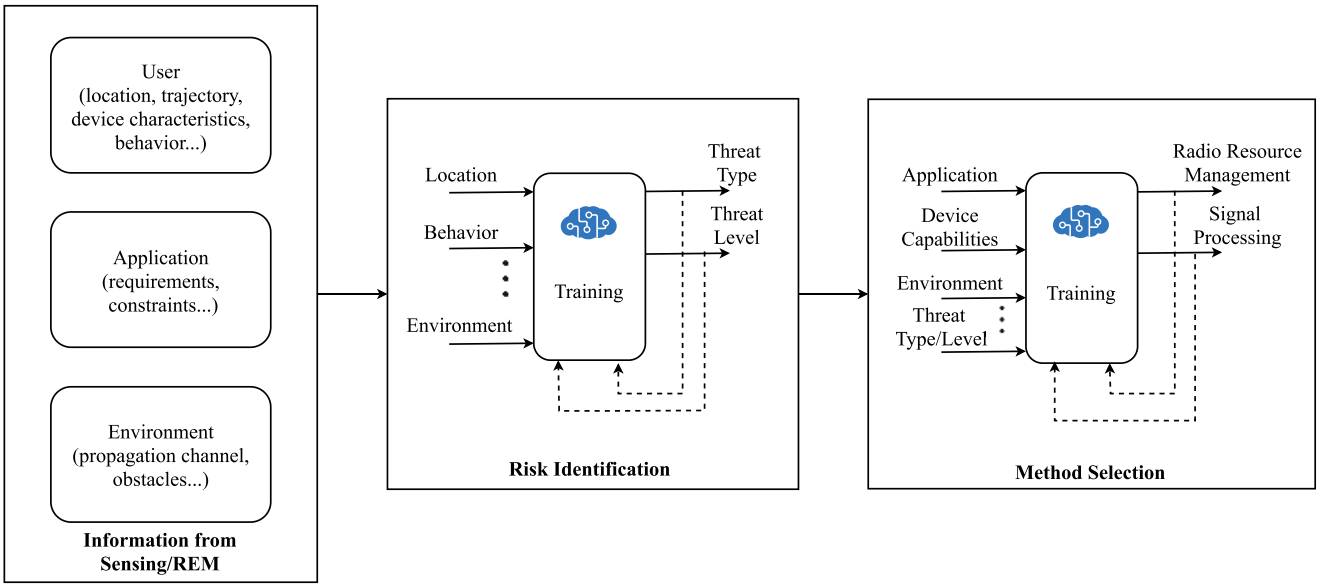


FIGURE 25. REM/Sensing-assisted cognitive physical layer security framework for future wireless communication systems.

of AI for this decision making, where the risk identification, capabilities of the legitimate (and malicious) nodes, environment, and application requirements serve as inputs to the training. The outputs include resource allocation and other signal processing methods aimed at improving the security of the legitimate nodes. For instance, the resource management can achieve this by selecting subcarriers (in multi-carrier systems) that provide better channel frequency response (CFR) to the legitimate users, while signal processing methods may achieve the same goal by techniques such as beamforming and precoding.

Here, it should be highlighted that the training mechanism may differ depending on the available resources. While in an ideal case, an intelligent device (or system) should have its own AI core [164] that can help make decisions regarding PLS mechanisms to secure its wireless transmission, it is not practically feasible. An alternative to this is to use cloud computing resources for training the models, which can be done offline. Once these models are trained, they are quite lightweight and may be utilized by normal wireless devices. However, in the case that the environment and/or user distribution is changing too frequently for the cloud-based solution to be feasible, a compromise in terms of edge/fog computing nodes is also possible.

To enable easier understanding of the proposed REM-supported cognitive PLS concept, its application to the V2X scenario discussed in Section VII is described below.

C. V2X-BASED CASE STUDY

One of the reasons V2X presents a particularly interesting use case is because it combines the flavors of all 5G services [165]. For instance, the collision avoidance messages between vehicles correspond to uRLLC due to their strict reliability and latency requirements, infotainment services fall under the eMBB umbrella due to high data rate requirements, while the large number of vehicles and RSUs reflect the high connectivity requirement of mMTC service. Considering the above-mentioned examples, collision-avoidance messages between vehicles are far more critical, and therefore have a higher need for security, as compared to infotainment or Internet access for the users. This variation in the criticality of tasks makes the case for a cognitive security framework like the one described earlier.

As illustrated in Fig. 25, the cognitive security framework utilizes information provided by REM/sensing for risk identification. Example information, along with their corresponding (potential) security risks, are described below [166]:

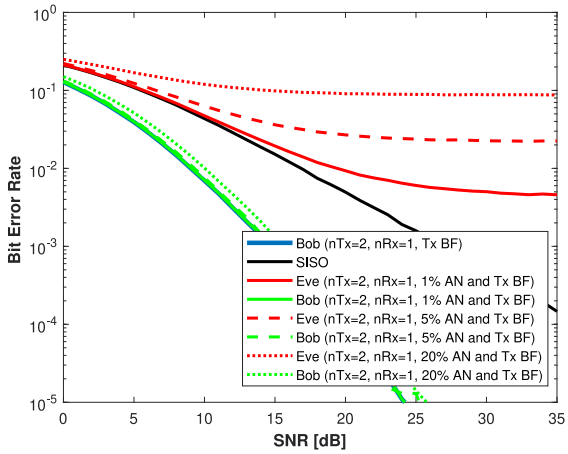
- *Environment Information:* REM provides awareness regarding the types of environment, such as rural, sub-urban, and urban, along with their traffic densities, population, communication, and road-side infrastructure. Furthermore, the information of physical characteristics of the propagation medium (e.g., LoS/NLoS and path loss information) can help identify the locations of potential attackers.
- *Location:* The awareness about the location of the (vehicular) user is a very important factor for security design because of its high correlation with the security risks. Apart from localizing the nodes that may pose a security threat, this information also identifies the level of risk posed to other nodes in the network. For example, security risks/threats to a vehicle at an intersection (or bridge or mountainous place) have more significant consequences compared to other locations, as any active attacks at these locations can cause major problems. Therefore, even if all other factors are similar, the

risk identified for a vehicle at an intersection would be higher than one on a side street.

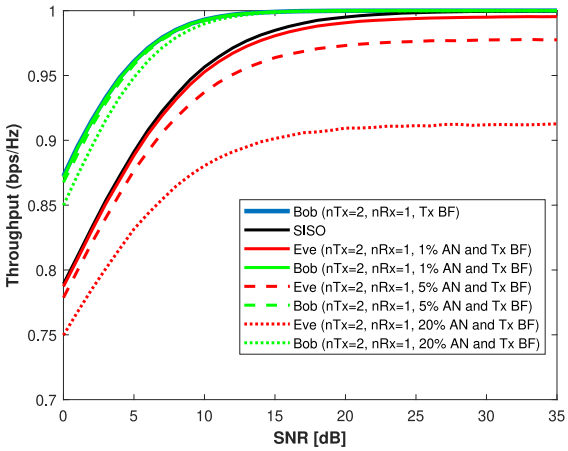
- *Application:* As mentioned earlier, V2X communication has various components and applications. For instance, a vehicle interacts with other vehicles for collision avoidance (V2V), with some infrastructural nodes for toll payments (V2I), or with a cellular network for Internet access for browsing (V2N). These applications have their own importance, and consequently, security requirements. For instance, if a vehicular node wants to do both collision avoidance and Internet access, the risk identifier will prioritize the former over the latter.
- *Vehicle Characteristics:* The information about vehicle characteristics, such as power, size, engine capacity, control (full/semi-autonomous), and utility (emergency, municipality, public transport, or private usage) allows the risk identification block to determine the inherent vulnerability of the vehicle to security threats, identify secure/legitimate vehicles, or assign social reputation values to surrounding vehicles. Additionally, the reliability of surrounding vehicles supports information sharing and other various wireless cooperation technologies such as relaying or forming ad hoc networks.

As explained earlier, appropriate resources and methods will be allocated and then provided based on the threat level and type for ensuring secure communication. Note that when allocating resources for secure communications, there is a trade-off between security and communication performance. In conventional designs, resource allocation is performed considering either average or maximum threat levels. The drawbacks here are insufficient security or wastage of resources, respectively. In this aspect, method selection and resource allocation provided by the REM based framework is more efficient compared to conventional design approaches because it is able to dynamically detect threat levels and adapt accordingly.

In order to further clarify the above-mentioned framework, the example of an adaptive artificial noise-based security technique is presented. This can enable secure communication for different applications and services based on threat type and level by adaptive adjustment of resources. Figures 26(a) and 26(b) show BER versus SNR and throughput versus SNR curves, respectively, for different percentages of total transmitted power allocated to artificial noise based on security requirements, where the simulation parameters are similar to those used in Section VII. It is observed that as the power allocated to noise increases from 1% to 20%, the BER as well as the throughput performance at the attacker degrades while causing little to no degradation on the performance of the legitimate receiver. From a practical point of view, different services have different QoS requirements and if it is ensured that the attacker is operating below those QoS requirements then practical secrecy can be ensured for that service [167]. Hence, by adding 1%, 5%, and 20% noise, it can be ensured that the BER at the attacker can be ensured to be above 10^{-3}, 10^{-2}, and 10^{-1}, respectively, which can be used for providing security suitable for varying QoS requirements.



(a)



(b)

FIGURE 26. Performance comparison of transmit beamforming and adaptive artificial noise based solutions at legitimate (Bob) and illegitimate receivers (Eve). (a) BER vs SNR, (b) Throughput vs SNR.

IX. FUTURE DIRECTIONS AND RECOMMENDATIONS

- The majority of the solutions discussed in the previous sections, as well as in the literature, are focused on a single attack at any time but ignore the fact that an attacker can also launch different attacks simultaneously. Furthermore, most works overlook the possibility of multiple attackers colluding together. These adversaries can help each other in interpreting the information exchanged between legitimate nodes. Another consideration that an overwhelming majority of the literature has failed to cater to is the cognitive capability of the attacker(s). An intelligent attacker can learn about its environment and wireless network to find its weaknesses and find the most suitable way to exploit them [56].

Finding an approach that provides security to sensing and communication against such evolved adversaries is a huge challenge that needs significant research efforts to address it.

- A major limitation of the PLS approaches is the recurring assumption of independent channels being observed at the legitimate and illegitimate nodes. This does not necessarily hold true in poor scattering environments. In such cases, channel control mechanisms like RISs can be leveraged to enrich the environment such that independence of the observed channels is restored. Similarly, the use of techniques such as CoMP can help in providing multiple observations of the channel and/or device fingerprints, which can be utilized for authentication of nodes.
- While security metrics for wireless communications are well-defined, new metrics are required to quantify the performance of a secure radio environment awareness framework. These metrics should be capable of reflecting the level and accuracy of radio environment awareness in the presence of attacks, the complexity of the security technique, and level of security, among other things. Threats on REM construction only consider the presence of malicious or faulty sensing nodes [117], and therefore only consider accuracy as a quality metric. In light of the aforementioned threats, security metrics for REM construction in the presence of eavesdropping/exploratory and jamming/disruption attacks, and their respective prevention/mitigation techniques, need to be developed. Similar metrics are required for CSI/RSSI based environment awareness techniques. The figure of merit is a quality metric to evaluate the performance of radar systems in the presence of jamming attacks [168]. However, the security metrics for other attacks on radar/JRC and their solutions are also required.
- Because civilian and commercial use of wireless sensing is just being realized, not all the security aspects/threats have been considered by the community. As such, solid solutions are missing for some attacks mentioned previously. Manipulation attacks related to sensing modes, methods, and the environment are prime examples of security threats with subpar solutions. For the former two attacks, adaptive thresholding and authentication techniques are proposed. While adaptive thresholding can reduce redundant updates, it can also lead to missed detections. Similarly, while authentication techniques can filter malicious nodes, their capability to detect legitimate nodes with faulty sensors or manipulation of the channel of the legitimate nodes is limited. Therefore, other security techniques need to be developed. The feasibility of collaborative PLS techniques needs to be evaluated.
- Some of the most prominent wireless standardization bodies including - but not limited to - 3GPP, IEEE, ETSI, and International Telecommunication Union (ITU) have contributed security framework architectures, recommendations, specifications, and principles [169]. However, there are some limitations of these efforts. For instance, the interoperability between different standards becomes challenging with the exceeding heterogeneity of wireless networks. Furthermore, these activities are focused on higher network layers rather than physical layer. These approaches may secure the content of the wireless transmission, but fail to provide security to the characteristics of the environment and/or users. Therefore, standardized solutions that secure sensing need to be explored.
- Fully homomorphic encryption (FHE) allows performing different operations on data without the need for decrypting it. While the concept of homomorphic encryption dates to the late 70s [170], it was relatively dormant till IBM took up the mantle to develop practical schemes to implement it [171]. Over the last few years, industrial giants like Microsoft and IBM have put significant efforts towards it, with the former having demonstrated the possibility of applying neural networks on encrypted data [172], while the latter has recently developed a toolkit for FHE [173]. One of the most significant advantages of this technology is the ability to transmit the data securely through the networks. For instance, this could be leveraged in transferring the data to the cloud for learning/training risk identification and resource allocation models for cognitive PLS. However, there are still two hurdles before the use of fully homomorphic encryption (FHE) can become widespread; firstly, it consumes far more resources (computation and storage) as compared to conventional encryption and secondly, it can only provide security to the data/content. Therefore, even if an efficient realization of FHE is achieved, PLS mechanisms would still be needed to secure the sensing aspect of the wireless networks.
- This survey has gone over security threats and possible physical layer solutions for securing REM and utilizing REM for security. However, the field of communication security is ever evolving and this progress should be revisited from a REM and wireless sensing perspective. Examples of recent developments can be cross-layer and hybrid security designs. Cross-layer designs consider the functionalities, mechanisms, and principles of the upper layers, such as the MAC, network, and application layers, along with the physical layer. Hybrid security designs offer two layers of security, based on joint cryptography and PLS, increasing robustness against different attacks. Additionally, unresolved PLS issues, such as channel estimation error and reciprocity mismatch, should be further studied.
- Similar to the case of V2X studied in the preceding section, REM and sensing can be leveraged to secure other communication technologies/paradigms such as

visible light and terahertz communication, simultaneous wireless information and power transfer (SWIPT), and non-terrestrial networks. Visible light communication can serve as a particularly interesting use case since it is predominantly deployed in indoor scenarios and can leverage Wi-Fi sensing to provide knowledge of the environment to empower the cognitive PLS framework. SWIPT, on the other hand, would require an additional layer of REM comprising of information that helps in improving energy efficiency, such as optimized beamforming vectors for energy receivers. Furthermore, the identification of attackers trying to exploit these resources for harvesting energy for themselves can also be supported by REM.

- Recently, mMIMO has garnered increased attention due to its capability to enhance the overall performance from both communication and sensing perspectives. Due to the large antenna array, mMIMO can launch multiple narrow beams towards the intended receiver/object for sensing/communication. The narrower beam-width of beams provides some level of immunity against exploratory attacks. Similarly, a large number of antennas provide immunity against jamming attacks by providing better beam nulling capability. However, these systems are vulnerable to pilot contamination and manipulation attacks. There are some preliminary solutions to tackle manipulation attacks [174]. However, this is still an open area for further research from communication as well as sensing security perspectives.
- Generally, channel codes are designed for enhancing the reliability of the communication system. The popular channel coding candidates proposed for 5G include polar and low-density parity-check (LDPC) codes. Channel coding can provide secure communication if attacker's channel is poorer as compared to Bob's. However, if the quality of attacker's channel is similar to or better than Bob's channel, these methods may not work. In such a situation, artificial noise can be used to degrade the quality of the attacker's channel along with channel coding to improve the secrecy rate [175]. Moreover, the joint design of channel coding can also be employed along with cryptography for providing secure communication [169]. The practical design of channel coding for different scenarios and services need more research.

X. CONCLUSION

This work draws attention to the importance of security for wireless sensing and radio environment awareness. For this purpose, we have gone over generic radio environment awareness and map generation processes, highlighting their vulnerable aspects, namely, the sensing and mapping methods, participating nodes, and sensed environment. Conventional eavesdropping, spoofing, and jamming threats found in wireless communication literature were generalized to incorporate sensing aspects, leading to the discussions of the terms exploratory, manipulation, and disruption attacks. For each of these categories, possible threats to REM and wireless sensing and their solutions are provided from the domains of wireless communication, radar/sensing, and machine learning. The implications of these attacks are then highlighted in a V2X scenario, and methods to ensure secure operation are provided. Furthermore, we present the concept of radio-environment awareness empowered cognitive PLS. Recommendations regarding the development of sensing-centric security mechanisms for next-generation wireless networks are also provided.

LIST OF ACRONYMS

3GPP	3rd Generation Partnership Project
5G	fifth generation
6G	sixth generation
ABC	ambient backscatter communication
ACK	Acknowledgement
AFE	analog front-end
AI	artificial intelligence
AoA	angle of arrival
AoD	angle of departure
AP	access point
BER	bit error rate
BS	base station
BSA	blind signal analysis
CFO	carrier frequency offset
CFR	channel frequency response
CN	communicating node
CoMP	coordinated multipoint
CR	cognitive radio
CSI	channel state information
CSS	chirp spread spectrum
CTS	Clear To Send
C-V2X	cellular V2X
DFRC	dual function radar communication
DL	deep learning
DMG	Directional Multi-Gigabit
DNN	deep neural network
DRFM	digital radio frequency memory
DSRC	dedicated short-range communications
DSSS	direct-sequence spread spectrum
EDMG	enhanced-DMG
eMBB	enhanced mobile broadband
ETSI	European Telecommunications Standards Institute
FARAMIR	Flexible and spectrum-Aware Radio Access through Measurements and modelling In cognitive Radio systems
FDD	frequency-division duplexing
FFT	fast Fourier transform
FHE	fully homomorphic encryption
FHSS	frequency-hopping spread spectrum
GAN	generative adversarial network
GPS	Global Positioning System

IEEE	Institute of Electrical and Electronics Engineers
IN	initiating node
IoT	Internet of Things
IQI	in-phase/quadrature imbalance
ITS	intelligent transportation system
ITU	International Telecommunication Union
JRC	joint radar and communication
LDPC	low-density parity-check
LoS	line-of-sight
LPI	low probability of intercept
MAC	medium access control
MCD	measurement-capable device
MIMO	multiple-input multiple-output
MISO	multiple-input single-output
ML	machine learning
mMIMO	massive multiple-input multiple-output
mMTC	massive machine-type connectivity
mmWave	millimeter-wave
MUSIC	multiple signal classification
NGP	Next Generation Positioning
NLoS	non-line-of-sight
OFDM	orthogonal frequency division multiplexing
PER	packet error rate
PLA	physical layer authentication
PLS	physical layer security
PSD	power spectral density
PSSS	parallel-sequence spread spectrum
PU	primary user
PUEA	primary user emulation attack
QoS	quality of service
RCC	radar and communication coexistence
REM	radio environment map/mapping
REM-SA	REM storage and acquisition
RF	radio frequency
RF-REM	radio frequency REM
RIS	reconfigurable intelligent surface
RN	responding node
ROC	receiver operating characteristic
RRS	reconfigurable radio systems
RSS	received signal strength
RSSI	received signal strength indicator
RSU	road-side unit
RTS	Request To Send
RTT	round trip time
SINR	signal-to-interference-plus-noise ratio
SISO	single-input single-output
STA	station
SWIPT	simultaneous wireless information and power transfer
TDD	time-division duplexing
THSS	time-hopping spread spectrum
ToA	time-of-arrival
ToF	time-of-flight
UAV	unmanned aerial vehicle
UE	user equipment
uRLLC	ultra-reliable low-latency communication
V2I	vehicle-to-infrastructure
V2N	vehicle-to-network
V2V	vehicle-to-vehicle
V2X	vehicle-to-everything
Wi-Fi	wireless fidelity
WLAN	wireless local area network.

REFERENCES

[1] "5G vision—The 5G infrastructure public private partnership: The next generation of communication networks and services," 5G Infrastruct. PPP Assoc., Heidelberg, Germany, White Paper, Feb. 2015.

[2] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[3] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Netw.*, vol. 33, no. 4, pp. 70–75, Jul./Aug. 2019.

[4] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nat. Electron.*, vol. 3, no. 1, pp. 20–29, 2020.

[5] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6G: AI empowered wireless networks," *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84–90, Aug. 2019.

[6] A. Yazar, S. Dogan-Tusha, and H. Arslan, "6G vision: An ultra-flexible perspective," *ITU J. Future Evol. Technol.*, vol. 1, no. 1, pp. 1–20, 2020.

[7] P. Fouillot *et al.*, "D6.2 prototype description and field trial results," document D6.2, FARAMIR, Aachen, Germany, 2012.

[8] H. B. Yilmaz, T. Tugcu, F. Alagöz, and S. Bayhan, "Radio environment map as enabler for practical cognitive radio networks," *IEEE Commun. Mag.*, vol. 51, no. 12, pp. 162–169, Dec. 2013.

[9] Y. Zhao, B. Le, and J. H. Reed, "Network support: The radio environment map," in *Cognitive Radio Technology*. Boston, MA, USA: Elsevier, 2006, pp. 337–363.

[10] A. Umbert, J. Pérez-Romero, F. Casadevall, A. Kliks, and P. Kryszkiewicz, "On the use of indoor radio environment maps for Hetnets deployment," in *Proc. 9th Int. Conf. Cogn. Radio Orient. Wireless Netw. Commun. (CROWNCOM)*, Oulu, Finland, 2014, pp. 448–453.

[11] T. Arampatzis, J. Lygeros, and S. Manesis, "A survey of applications of wireless sensors and wireless sensor networks," in *Proc. IEEE Int. Symp. Mediterr. Conf. Control Autom. Intell. Control*, Limassol, Cyprus, 2005, pp. 719–724.

[12] F. J. Oppermann, C. A. Boano, and K. Römer, "A decade of wireless sensing applications: Survey and taxonomy," in *The Art of Wireless Sensor Networks*. Heidelberg, Germany: Springer, 2014, pp. 11–50.

[13] J. Liu, H. Liu, Y. Chen, Y. Wang, and C. Wang, "Wireless sensing for human activity: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1629–1645, 3rd Quart., 2020.

[14] C. da Silva, *SENS SG Proposed CSD Draft*, document IEEE 802.11-20/0042r6, IEEE, Piscataway, NJ, USA, 2020.

[15] S. Subramani, T. Farnham, and M. Sooriyabandara, "Deployment and interface design considerations for radio environment maps," in *Proc. IEEE 8th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)*, Barcelona, Spain, 2012, pp. 480–487.

[16] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[17] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 4th Quart., 2009.

[18] R. L. Rivest, "Cryptography," in *Handbook of Theoretical Computer Science, Volume A*, J. Van Leeuwen and J. Leeuwen, Eds. Amsterdam, The Netherlands: Elsevier, 1990, ch. 13, pp. 718–755.

[19] M. E. Hellman, B. W. Diffie, and R. C. Merkle, "Cryptographic apparatus and method," U.S. Patent 4 200 770, Apr. 1980,

[20] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[21] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Physical layer security designs for 5G and beyond," in *Flexible and Cognitive Radio Access Technologies for 5G and Beyond*, H. Arslan and E. Basar, Eds. London, U.K.: IET, 2020, ch. 18, pp. 545–587.

[22] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[23] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: Current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152–158, Jun. 2016.

[24] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[25] L. Bai, L. Zhu, J. Liu, J. Choi, and W. Zhang, "Physical layer authentication in wireless communication networks: A survey," *J. Commun. Inf. Netw.*, vol. 5, no. 3, pp. 237–264, Sep. 2020.

[26] T. Fawcett, "An introduction to ROC analysis," *Pattern Recognit. Lett.*, vol. 27, no. 8, pp. 861–874, 2006.

[27] M. Pesko, T. Javornik, A. Košir, M. Štular, and M. Mohorčič, "Radio environment maps: The survey of construction methods," *KSII Trans. Internet Inf. Syst.*, vol. 8, pp. 3789–3809, Dec. 2014.

[28] Y. Ye and B. Wang, "RMapCS: Radio map construction from crowdsourced samples for indoor localization," *IEEE Access*, vol. 6, pp. 24224–24238, 2018.

[29] H. Tabassum, M. Salehi, and E. Hossain, "Fundamentals of mobility-aware performance characterization of cellular networks: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2288–2308, 3rd Quart., 2019.

[30] C. Suarez-Rodriguez, Y. He, and E. Dutkiewicz, "Theoretical analysis of REM-based handover algorithm for heterogeneous networks," *IEEE Access*, vol. 7, pp. 96719–96731, 2019.

[31] L. T. Tan, R. Q. Hu, and L. Hanzo, "Heterogeneous networks relying on full-duplex relays and mobility-aware probabilistic caching," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 5037–5052, Jul. 2019.

[32] *REM Prototype Implementation, Ver 1.0f*, FARAMIR Standard TSD4.3, Feb. 2012.

[33] C. W. S. Pandy and B. Hart, *NGP Use-Case Document, Ver R4*, Standard TS D16/0137, Mar. 2016.

[34] *IEEE P802.11—Next Generation Positioning Study Group. IEEE 802.11*. Accessed: Dec. 21, 2020. [Online]. Available: https://www.ieee802.org/11/Reports/tgaz_update.htm

[35] I. Jang, J. Choi, J. Kim, S. Lim, and D. Kim, *Discussion on WLAN Sensing Roles*, document IEEE 802.11-20/1805r1, IEEE, Piscataway, NJ, USA, 2020.

[36] C. da Silva, C. Chen, B. Sadeghi, and C. Cordeiro, *A Channel Measurement Procedure for WLAN Sensing*, document IEEE 802.11-20/0842r0, IEEE, Piscataway, NJ, USA, 2020.

[37] C. Liu, M. Zhang, R. Du, and Y. Sun, *Follow-Ups on Channel Measurement Procedure for WLAN Sensing*, document IEEE 802.11-20/1120r1, IEEE, Piscataway, NJ, USA, 2020.

[38] X. Gao, X. Zhang, G. Feng, Z. Wang, and D. Xu, "On the MUSIC-derived approaches of angle estimation for bistatic MIMO radar," in *Proc. Int. Conf. Wireless Netw. Inf. Syst.*, Shanghai, China, 2009, pp. 343–346.

[39] X. Zhang, L. Xu, L. Xu, and D. Xu, "Direction of departure (DOD) and direction of arrival (DOA) estimation in MIMO radar with reduced-dimension MUSIC," *IEEE Commun. Lett.*, vol. 14, no. 12, pp. 1161–1163, Dec. 2010.

[40] B. R. Mahafza, *Radar Signal Analysis and Processing Using MATLAB*. Boca Raton, FL, USA: CRC Press, 2016.

[41] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, "Joint radar and communication design: Applications, state-of-the-art, and the road ahead," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3834–3862, Jun. 2020.

[42] F. Lampel, R. F. Tigrek, A. Alvarado, and F. M. J. Willems, "A performance enhancement technique for a joint FMCW radcom system," in *Proc. 16th Eur. Radar Conf. (EuRAD)*, Paris, France, 2019, pp. 169–172.

[43] A. Ahmed, Y. D. Zhang, and B. Himed, "Distributed dual-function radar-communication MIMO system with optimized resource allocation," in *Proc. IEEE Radar Conf. (RadarConf)*, Boston, MA, USA, 2019, pp. 1–5.

[44] T. Huang, N. Shlezinger, X. Xu, Y. Liu, and Y. C. Eldar, "MAJoRCom: A dual-function radar communication system using index modulation," *IEEE Trans. Signal Process.*, vol. 68, pp. 3423–3438, May 2020. [Online]. Available: http://dx.doi.org/10.1109/TSP.2020.2994394

[45] Y. L. Sit, C. Sturm, L. Reichardt, T. Zwick, and W. Wiesbeck, "The OFDM joint radar-communication system: An overview," in *Proc. Int. Conf. Adv. Satellite Space Commun. (SPACOMM)*, 2011, pp. 69–74.

[46] H. Arslan, *Design and Analysis of Wireless Communication Signals: A Laboratory-Based Approach*, 1st ed. Hoboken, NJ, USA: Wiley, May 2021.

[47] Y. Ma, G. Zhou, and S. Wang, "WiFi sensing with channel state information: A survey," *ACM Comput. Surveys*, vol. 52, no. 3, p. 46, Jun. 2019. [Online]. Available: https://doi.org/10.1145/3310194

[48] S. He and S.-H. G. Chan, "Wi-Fi fingerprint-based indoor positioning: Recent advances and comparisons," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 466–490, 1st Quart., 2016.

[49] ETS Institute, "Reconfigurable radio systems (RRS); use cases for building and exploitation of radio environment maps (REMs) for intra-operator scenarios," Dept. Informatics, Univ. Zurich, Zürich, Switzerland, Rep. ETSI TR 102 947, Jun. 2013.

[50] D. Lynch, *Introduction to RF Stealth*, Raleigh, NC, USA: Scitech Publ. Inc, 2004.

[51] D. E. Lawrence, "Low probability of intercept antenna array beamforming," *IEEE Trans. Antennas Propag.*, vol. 58, no. 9, pp. 2858–2865, Sep. 2010.

[52] H. Khodakarami and F. Lahouti, "Link adaptation for physical layer security over wireless fading channels," *IET Commun.*, vol. 6, no. 3, pp. 353–362, Feb. 2012.

[53] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[54] Z. Sheng, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Beamforming optimization for physical layer security in MISO wireless networks," *IEEE Trans. Signal Process.*, vol. 66, no. 14, pp. 3710–3723, Jul. 2018.

[55] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan, "Secure spatial multiple access using directional modulation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 563–573, Jan. 2018.

[56] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2nd Quart., 2019.

[57] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 693–702, 2011.

[58] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[59] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.

[60] K. Cumanan *et al.*, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, 2016.

[61] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, pp. 682–694, 2013.

[62] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[63] S. Naderi, D. B. da Costa, and H. Arslan, "Joint random subcarrier selection and channel-based artificial signal design aided PLS," *IEEE Wireless Commun. Lett.*, vol. 9, no. 7, pp. 976–980, Jul. 2020.

[64] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[65] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2734–2771, 3rd Quart., 2019.

[66] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[67] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, "Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks," in *Proc. IEEE Global Commun. Conf.*, Austin, TX, USA, 2014, pp. 3145–3150.

[68] M. Soltani, T. Baykas, and H. Arslan, "Achieving secure communication through pilot manipulation," in *Proc. IEEE 26th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Hong Kong, China, 2015, pp. 527–531.

[69] T.-Y. Liu, S.-C. Lin, and Y.-W. P. Hong, "On the role of artificial noise in training and data transmission for secret communications," *IEEE Trans. Inf. Forensics Security*, vol. 12, pp. 516–531, 2017.

[70] Q. Zhu, S. Wu, and Y. Hua, "Optimal pilots for anti-eavesdropping channel estimation," *IEEE Trans. Signal Process.*, vol. 68, pp. 2629–2644, Apr. 2020.

[71] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116753–116773, 2019.

[72] A. Almohamad *et al.*, "Smart and secure wireless communications via reflecting intelligent surfaces: A short survey," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1442–1456, 2020.

[73] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.

[74] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, Oct. 2019.

[75] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "New physical layer key generation dimensions: Subcarrier indices/positions-based key generation," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 59–63, Jan. 2021.

[76] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[77] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 48–54, Oct. 2019.

[78] R. H. Clarke, "A statistical theory of mobile-radio reception," *Bell Syst. Techn. J.*, vol. 47, no. 6, pp. 957–1000, Jul./Aug. 1968.

[79] L. Jiao, J. Tang, and K. Zeng, "Physical layer key generation using virtual AoA and AoD of mmWave massive MIMO channel," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Beijing, China, 2018, pp. 1–9.

[80] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "SmokeGrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1731–1745, 2013.

[81] P. Huang and X. Wang, "Fast secret key generation in static wireless networks: A virtual channel approach," in *Proc. IEEE INFOCOM*, Turin, Italy, 2013, pp. 2292–2300.

[82] Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2595–2621, 4th Quart., 2018.

[83] L. Zhao, X. Zhang, J. Chen, and L. Zhou, "Physical layer security in the age of artificial intelligence and edge computing," *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 174–180, Oct. 2020.

[84] Z. Sun, S. Balakrishnan, L. Su, A. Bhuyan, P. Wang, and C. Qiao, "Who is in control? Practical physical layer attack and defense for mmWave based sensing in autonomous vehicles," 2020. [Online]. Available: https://arxiv.org/abs/2011.10947.

[85] S. J. Roome, "Digital radio frequency memory," *Electron. Commun. Eng. J.*, vol. 2, no. 4, pp. 147–153, 1990.

[86] R. Chauhan, "A platform for false data injection in frequency modulated continuous wave radar," M.S. thesis, Dept. Digit. Commun. Utah State Univ., Logan, UT, USA, May 2014.

[87] E. Giusti, A. Capria, M. Martorella, C. Moscardini, and F. Berizzi, "Electronic countermeasure for OFDM-based imaging passive radars," *IET Radar Sonar Navig.*, vol. 13, no. 9, pp. 1458–1467, Sep. 2019.

[88] H. Kuschel, D. Cristallini, and K. E. Olsen, "Tutorial: Passive radar tutorial," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 34, no. 2, pp. 2–19, Feb. 2019.

[89] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," 2020. [Online]. Available: arXiv:2007.08041.

[90] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Security*, 2015, pp. 1004–1015. [Online]. Available: https://doi.org/10.1145/2810103.2813679

[91] P. Kapoor, A. Vora, and K.-D. Kang, "Detecting and mitigating spoofing attack against an automotive radar," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Chicago, IL, USA, 2018, pp. 1–6.

[92] T. Moon, J. Park, and S. Kim, "BlueFMCW: Random frequency hopping radar for mitigation of interference and spoofing," 2020. [Online]. Available: arXiv:2008.00624.

[93] T. de Riberolles, J. Song, Y. Zou, G. Silvestre, and N. Larrieu, "Characterizing radar network traffic: A first step towards spoofing attack detection," in *Proc. IEEE Aerosp. Conf.*, Big Sky, MT, USA, 2020, pp. 1–8.

[94] R. C. Daniels, E. R. Yeh, and R. W. Heath, "Forward collision vehicular radar with IEEE 802.11: Feasibility demonstration through measurements," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1404–1416, Feb. 2018.

[95] Z. Haider and S. Khalid, "Survey on effective GPS spoofing countermeasures," in *Proc. 6th Int. Conf. Innovat. Comput. Technol. (INTECH)*, Dublin, Ireland, 2016, pp. 573–577.

[96] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[97] D. Kapetanović, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. IEEE 24th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, London, U.K., 2013, pp. 13–18.

[98] J. K. Tugnait, "Self-contamination for detection of pilot contamination attack in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. 4, no. 5, pp. 525–528, Oct. 2015.

[99] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 932–940, 2015.

[100] Q. Xiong, Y.-C. Liang, K. H. Li, Y. Gong, and S. Han, "Secure transmission against pilot spoofing attack: A two-way training-based scheme," *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 1017–1026, 2016.

[101] R. G. Dutta *et al.*, "Estimation of safe sensor measurements of autonomous system under attack," in *Proc. 54th Annu. Design Autom. Conf.*, 2017, pp. 1–6.

[102] A. Murase, I. Symington, and E. Green, "Handover criterion for macro and microcellular systems," in *Proc. 41st IEEE Veh. Technol. Conf.*, St. Louis, MO, USA, 1991, pp. 524–530.

[103] Z. Becvar and P. Mach, "Adaptive hysteresis margin for handover in femtocell networks," in *Proc. 6th Int. Conf. Wireless Mobile Commun.*, Valencia, Spain, 2010, pp. 256–261.

[104] N. Xie and S. Zhang, "Blind authentication at the physical layer under time-varying fading channels," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1465–1479, Jul. 2018.

[105] Z. Wei, F. R. Yu, and A. Boukerche, "Cooperative spectrum sensing with trust assistance for cognitive radio vehicular ad hoc networks," in *Proc. 5th ACM Symp. Develop. Anal. Intell. Veh. Netw. Appl.*, 2015, pp. 27–33.

[106] B. Wang and N. Z. Gong, "Stealing hyperparameters in machine learning," in *Proc. IEEE Symp. Security Privacy (SP)*, San Francisco, CA, USA, 2018, pp. 36–52.

[107] Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, "Generative adversarial network for wireless signal spoofing," in *Proc. ACM Workshop Wireless Security Mach. Learn.*, 2019, pp. 55–60.

[108] Y. E. Sagduyu, Y. Shi, and T. Erpek, "IoT network security from the perspective of adversarial deep learning," in *Proc. 16th Annu. IEEE Int. Conf. Sens. Commun. Netw. (SECON)*, 2019, pp. 1–9.

[109] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, "Distillation as a defense to adversarial perturbations against deep neural networks," in *Proc. IEEE Symp. Security Privacy (SP)*, San Jose, CA, USA, 2016, pp. 582–597.

[110] X. Cao and N. Z. Gong, "Mitigating evasion attacks to deep neural networks via region-based classification," in *Proc. 33rd Annu. Comput. Security Appl. Conf.*, 2017, pp. 278–287.

[111] D. Denkovski, V. Atanasovski, L. Gavrilovska, J. Riihijärvi, and P. Mähönen, "Reliability of a radio environment map: Case of spatial interpolation techniques," in *Proc. 7th Int. ICST Conf. Cogn. Radio Orient. Wireless Netw. Commun. (CROWNCOM)*, Stockholm, Sweden, 2012, pp. 248–253.

[112] Z. Han, J. Liao, Q. Qi, H. Sun, and J. Wang, "Radio environment map construction by Kriging algorithm based on mobile crowd sensing," *Wireless Commun. Mobile Comput.*, vol. 2019, Feb. 2019, Art. no. 4064201.

[113] H. Xia, S. Zha, J. Huang, and J. Liu, "Radio environment map construction by adaptive ordinary Kriging algorithm based on affinity propagation clustering," *Int. J. Distrib. Sens. Netw.*, vol. 16, no. 5, 2020, Art. no. 1550147720922484.

[114] X. Liu, F. Chen, and C.-T. Lu, "Robust prediction and outlier detection for spatial datasets," in *Proc. IEEE 12th Int. Conf. Data Min.*, Brussels, Belgium, 2012, pp. 469–478.

[115] X. Han, L. Xue, F. Shao, and Y. Xu, "A power spectrum maps estimation algorithm based on generative adversarial networks for underlay cognitive radio networks," *Sensors*, vol. 20, no. 1, p. 311, 2020.

[116] D. Zhu, X. Cheng, F. Zhang, X. Yao, Y. Gao, and Y. Liu, "Spatial interpolation using conditional generative adversarial neural networks," *Int. J. Geograph. Inf. Sci.*, vol. 34, no. 4, pp. 735–758, 2020.

[117] Y. Hu and R. Zhang, "A spatiotemporal approach for secure crowdsourced radio environment map construction," *IEEE/ACM Trans. Netw.*, vol. 28, no. 4, pp. 1790–1803, Aug. 2020.

[118] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, 1st Quart., 2013.

[119] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surveys*, vol. 48, no. 4, p. 64, May 2016.

[120] D. Chaitanya and K. M. Chari, "Performance analysis of PUEA and SSDF attacks in cognitive radio networks," in *Computer Communication, Networking and Internet Security*. Singapore: Springer, 2017, pp. 219–225.

[121] F. Pan *et al.*, "Physical layer authentication based on channel information and machine learning," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Las Vegas, NV, USA, 2017, pp. 364–365.

[122] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. IEEE Int. Conf. Commun.*, Beijing, China, 2008, pp. 1520–1524.

[123] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[124] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171–4182, Jun. 2016.

[125] S. Van Vaerenbergh, O. González, J. Via, and I. Santamaría, "Physical layer authentication based on channel response tracking using Gaussian processes," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Florence, Italy, 2014, pp. 2410–2414.

[126] A. Weinand, M. Karrenbauer, J. Lianghai, and H. D. Schotten, "Physical layer authentication for mission critical machine type communication using Gaussian mixture model based clustering," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Sydney, NSW, Australia, 2017, pp. 1–5.

[127] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, 2008, pp. 116–127.

[128] J. Hall, M. Barbeau, and E. Kranakis, "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting," in *Proc. 3rd IASTED Int. Conf. Commun. Internet Inf. Technol. (CIIT)*, vol. 1, 2004, pp. 201–206.

[129] L. Y. Paul, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, pp. 38–51, 2008.

[130] P. L. Yu, G. Verma, and B. M. Sadler, "Wireless physical layer authentication via fingerprint embedding," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 48–53, Jun. 2015.

[131] X. Wang, F. J. Liu, D. Fan, H. Tang, and P. C. Mason, "Continuous physical layer authentication using a novel adaptive OFDM system," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, 2011, pp. 1–5.

[132] V. Kumar, J.-M. Park, and K. Bian, "Blind transmitter authentication for spectrum security and enforcement," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2014, pp. 787–798.

[133] S. H. Supangkat, T. Eric, and A. S. Pamuji, "A public key signature for authentication in telephone," in *Proc. Asia–Pac. Conf. Circuits Systems*, vol. 2. Denpasar, Indonesia, 2002, pp. 495–498.

[134] N. Xie, C. Chen, and Z. Ming, "Security model of authentication at the physical layer and performance analysis over fading channels," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 1, pp. 253–268, Jan./Feb. 2021.

[135] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2005, pp. 46–57.

[136] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[137] P. Gu, C. Hua, R. Khatoun, Y. Wu, and A. Serhrouchni, "Cooperative anti-jamming relaying for control channel jamming in vehicular networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Singapore, 2017, pp. 1–6.

[138] P. Gu, C. Hua, W. Xu, R. Khatoun, Y. Wu, and A. Serhrouchni, "Control channel anti-jamming in vehicular networks via cooperative relay beamforming," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5064–5077, Jun. 2020.

[139] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[140] H. Yang *et al.*, "Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach," 2020. [Online]. Available: arXiv:2004.12539.

[141] L. Freitag, M. Stojanovic, S. Singh, and M. Johnson, "Analysis of channel effects on direct-sequence and frequency-hopped spread-spectrum acoustic communication," *IEEE J. Ocean. Eng.*, vol. 26, no. 4, pp. 586–593, Oct. 2001.

[142] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "SPREAD: Foiling smart jammers using multi-layer agility," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Barcelona, Spain, May 2007, pp. 2536–2540.

[143] J. Wu, "Metricwave radar anti-jamming technology," in *Advanced Metric Wave Radar*. Singapore: Springer, 2020, pp. 101–129.

[144] N. Van Huynh, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, "'Jam me if you can': Defeating jammer with deep dueling neural network architecture and ambient backscattering augmented communication," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 11, pp. 2603–2620, Nov. 2019.

[145] D. T. Hoang *et al.*, "'Borrowing arrows with thatched boats': The art of defeating reactive jammers in IoT networks," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 79–87, Jun. 2020.

[146] B. Lyu, D. T. Hoang, S. Gong, D. Niyato, and D. I. Kim, "IRS-based wireless jamming attacks: When jammers can attack without power," 2020. [Online]. Available: arXiv:2001.01887.

[147] F. Liu and C. Masouros, "A tutorial on joint radar and communication transmission for vehicular networks—Part I: Background and fundamentals," *IEEE Commun. Lett.*, early access, Sep. 21, 2020, doi: 10.1109/LCOMM.2020.3025310.

[148] A. Gameiro, D. Castanheira, J. Sanson, and P. P. Monteiro, "Research challenges, trends and applications for future joint radar communications systems," *Wireless Pers. Commun.*, vol. 100, no. 1, pp. 81–96, 2018.

[149] K. Weevers and M. Lu. *V2X Communication for ITS—From IEEE 802.11p Towards 5G*. Accessed: Nov. 30, 2020. [Online]. Available: https://futurenetworks.ieee.org/tech-focus/march-2017/v2x-communication-for-its

[150] P. Roux, S. Sesia, V. Mannoni, and E. Perraud, "System level analysis for ITS-G5 and LTE-V2X performance comparison," in *Proc. IEEE 16th Int. Conf. Mobile Ad Hoc Sens. Syst. (MASS)*, Monterey, CA, USA, 2019, pp. 1–9.

[151] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9457–9470, Dec. 2016.

[152] P. Roux and V. Mannoni, "Performance evaluation for co-channel coexistence between ITS-G5 and LTE-V2X," in *Proc. IEEE 92nd Veh. Technol. Conf.*, 2020, pp. 1–5.

[153] S. Chen *et al.*, "Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G," *IEEE Commun. Stand. Mag.*, vol. 1, no. 2, pp. 70–76, Jul. 2017.

[154] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1858–1877, 3rd Quart., 2018.

[155] B. M. ElHalawany, A. A. A. El-Banna, and K. Wu, "Physical-layer security and privacy for vehicle-to-everything," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 84–90, Oct. 2019.

[156] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107093.

[157] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "Security and privacy issues for inter-vehicle communications in VANETs," in *Proc. 6th IEEE Annu. Commun. Soc. Conf. Sens. Mesh Ad Hoc Commun. Netw. Workshops*, Rome, Italy, 2009, pp. 1–3.

[158] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Netw.*, vol. 31, no. 5, pp. 50–58, Sep. 2017.

[159] A. Pathre, "Identification of malicious vehicle in VANET environment from DDoS attack," *J. Global Res. Comput. Sci.*, vol. 4, no. 6, pp. 30–34, 2013.

[160] P. Gu, C. Hua, R. Khatoun, Y. Wu, and A. Serhrouchni, "Cooperative antijamming relaying for control channel jamming in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7033–7046, Aug. 2018.

[161] B. Zong, C. Fan, X. Wang, X. Duan, B. Wang, and J. Wang, "6G technologies: Key drivers, core requirements, system architectures, and enabling technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 18–27, Sep. 2019.

[162] Z. Zhang *et al.*, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, Sep. 2019.

[163] M. H. Yılmaz, E. Güvenkaya, H. M. Furqan, S. Köse, and H. Arslan, "Cognitive security of wireless communication systems in the physical layer," *Wireless Commun. Mobile Comput.*, vol. 2017, Dec. 2017, Art. no. 3592792.

[164] Q.-Y. Yu, H.-C. Lin, and H.-H. Chen, "Intelligent radio for next generation wireless communications: An overview," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 94–101, Aug. 2019.

[165] L. Liang, H. Peng, G. Y. Li, and X. Shen, "Vehicular communications: A physical layer perspective," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10647–10659, Dec. 2017.

[166] H. M. Furqan, M. S. J. Solaija, J. M. Hamamreh, and H. Arslan, "Intelligent physical layer security approach for V2X communication," 2019. [Online]. Available: arXiv:1905.05075.

[167] M. Furqan, J. M. Hamamreh, and H. Arslan, "Adaptive OFDM-IM for enhancing physical layer security and spectral efficiency of future wireless networks," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–16, Aug. 2018.

[168] F. Qi, J. Wang, O. Kilic, and A. E. Fathy, "Effective figure of merit definition for MIMO UWB radar channels selection," in *Proc. IEEE Int. Symp. Antennas Propag. USNC-URSI Radio Sci. Meeting*, Atlanta, GA, USA, 2019, pp. 1571–1572.

[169] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.

[170] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–180, 1978.

[171] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA, USA, Sep. 2009.

[172] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, "CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy," in *Proc. 33rd Int. Conf. Mach. Learn.*, 2016, pp. 201–210.

[173] F. Bergamaschi. *IBM Releases Fully Homomorphic Encryption Toolkit for MacOS and iOS; Linux and Android Coming Soon*. Accessed: Dec. 19, 2020. [Online]. Available: https://www.ibm.com/blogs/research/2020/06/ibm-releases-fully-homomorphic-encryption-toolkit-for-macos-and-ios-linux-and-android-coming-soon/

[174] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin, "Securing massive MIMO at the physical layer," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Florence, Italy, Sep. 2015, pp. 272–280.

[175] H. Bai, L. Jin, and M. Yi, "Artificial noise aided polar codes for physical layer security," *China Commun.*, vol. 14, no. 12, pp. 15–24, Dec. 2017.

HAJI M. FURQAN received the B.E. and M.Sc. degrees in electrical engineering from the COMSATS Institute of Information Technology, Islamabad, Pakistan, in 2012 and 2014, respectively, and the Ph.D. degree from Istanbul Medipol University, Turkey, where he is currently a Postdoctoral Researcher. His research focuses on physical layer security, cooperative communication, adaptive index modulation, OFDM, V2X, cryptography, 5G systems, and wireless channel modeling and characterization.

MUHAMMAD SOHAIB J. SOLAIJA (Student Member, IEEE) received the B.E. and M.Sc. degrees in electrical engineering from the National University of Science and Technology, Islamabad, Pakistan, in 2014 and 2017, respectively. He is currently pursuing the Ph.D. degree with the Communications, Signal Processing, and Networking Center (CoSiNC), Istanbul Medipol University, Turkey, as a Member. His research focuses on interference modeling and coordinated multipoint implementation for 5G and beyond wireless systems.

HALISE TÜRKMEN received the B.S. degree in mechatronics engineering from Marmara University in 2016, and the M.Sc. degree in mechatronics engineering from Istanbul Technical University in 2019. She is currently pursuing the Ph.D. degree with Istanbul Medipol University, Turkey. Her research interests include radio environment monitoring and sensing for enabling 5G and 6G systems.

HÜSEYIN ARSLAN (Fellow, IEEE) received the B.S. degree from the Middle East Technical University, Ankara, Turkey, in 1992, and the M.S. and Ph.D. degrees from Southern Methodist University, Dallas, TX, USA, in 1994 and 1998, respectively.

From January 1998 to August 2002, he was with the Research Group, Ericsson, where he was involved with several projects related to 2G and 3G wireless communication systems. Since August 2002, he has been with the Electrical Engineering Department, University of South Florida, where he is a Professor. In December 2013, he joined Istanbul Medipol University to found the Engineering College, where he has worked as the Dean of the School of Engineering and Natural Sciences. In addition, he has worked as a part-time consultant for various companies and institutions, including Anritsu Company and the Scientific and Technological Research Council of Turkey. He conducts research in wireless systems, with emphasis on the physical and medium access layers of communications. He has been collaborating extensively with key national and international industrial partners and his research has generated significant interest in companies, such as InterDigital, Anritsu, NTT DoCoMo, Raytheon, Honeywell, and Keysight technologies. Collaborations and feedback from industry partners has significantly influenced his research. In addition to his research activities, he has also contributed to wireless communication education. He has integrated the outcomes of his research into education which led him to develop a number of courses with the University of South Florida. He has developed a unique "Wireless Systems Laboratory" course (funded by the National Science Foundation and Keysight technologies), where he was able to teach not only the theory but also the practical aspects of wireless communication system with the most contemporary test and measurement equipment. His current research interests are on 5G and beyond radio access technologies, physical layer security, interference management (avoidance, awareness, and cancelation), cognitive radio, multicarrier wireless technologies (beyond OFDM), dynamic spectrum access, co-existence issues, non-terrestial communications (high altitude platforms), joint radar (sensing) and communication designs.

Prof. Arslan has served as a general chair, a technical program committee chair, a session and symposium organizer, a workshop chair, and a technical program committee member in several ieee conferences. He is currently a member of the editorial board for the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS and the *Sensors Journal*. He has also served as a member of the editorial board for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, and several other scholarly journals by Elsevier, Hindawi, and Wiley Publishing.