Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey

Hossein Pirayesh and Huacheng Zeng, *Senior Member, IEEE*

***Abstract*—Wireless networks are a key component of the telecommunications infrastructure in our society, and wireless services become increasingly important as the applications of wireless devices have penetrated every aspect of our lives. Although wireless technologies have significantly advanced in the past decades, most wireless networks are still vulnerable to radio jamming attacks due to the openness nature of wireless channels, and the progress in the design of jamming-resistant wireless networking systems remains limited. This stagnation can be attributed to the lack of practical physical-layer wireless technologies that can efficiently decode data packets in the presence of jamming attacks. This article surveys existing jamming attacks and anti-jamming strategies in wireless local area networks (WLANs), cellular networks, cognitive radio networks (CRNs), ZigBee networks, Bluetooth networks, vehicular networks, LoRa networks, RFID networks, GPS system, millimeter-wave (mmWave) and learning-assisted wireless systems, with the objective of offering a comprehensive knowledge landscape of existing jamming and anti-jamming strategies and therefore stimulating more research efforts to secure wireless networks against jamming attacks. Different from prior survey papers, this article conducts a comprehensive, in-depth review on jamming and anti-jamming strategies, casting insights on the design of jamming-resilient wireless networking systems. An outlook on promising anti-jamming techniques is offered at the end of this article to delineate important research directions.**

***Index Terms*—Wireless security, physical-layer security, jamming attacks, denial-of-services attacks, anti-jamming strategy, cellular, 5G, 6G, Wi-Fi, vehicular networks, LoRa, ZigBee, Bluetooth, RFID, GPS, millimeter (mmWave), machine learning**

I. Introduction

With the rapid proliferation of wireless devices and the explosion of Internet-based mobile applications under the driving forces of 5G and artificial intelligence, wireless services have penetrated every aspect of our lives and become increasingly important as an essential component of the telecommunications infrastructure in our society. In the past two decades, we have witnessed the significant advancement of wireless communication and networking technologies such as polar code [1], [2], massive multiple-input multiple-output (MIMO) [3]–[5], millimeter-wave (mmwave) [6], [7], non-orthogonal multiple access (NOMA) [8]–[11], carrier aggregation [12], novel interference management [8], [13], learning-based resource allocation [14]–[16], software-defined radio [17], and software-defined wireless networking [18]. These innovative wireless technologies have dramatically boosted the capacity of wireless networks and the quality of wireless services, leading to a steady evolution of cellular networks towards 5th generation (5G) and Wi-Fi networks towards 802.11ax. With the joint efforts from academia, federal governments, and private sectors, it is expected that high-speed wireless services will become ubiquitously available for massive devices to realize the vision of Internet of Everything (IoE) in the near future [19].

As we are increasingly reliant on wireless services, security threats have become a big concern about the confidentiality, integrity, and availability of wireless communications. Compared to other security threats such as eavesdropping and data fabrication, wireless networks are particularly vulnerable to radio jamming attacks for the following reasons. First, jamming attacks are easy to launch. With the advances in software-defined radio, one can easily program a small $20 USB dongle device to a jammer that covers 20 MHz bandwidth below 6 GHz and up to 100 mW transmission power [31]. Such a USB dongle suffices to disrupt the Wi-Fi services in a home or office scenario. Other off-the-shelf SDR devices such as USRP [32] and WARP [33] are even more powerful and more flexible when using as a jamming emitter. The ease of launching jamming attacks makes it urgent to secure wireless networks against intentional and unintentional jamming threats. Second, jamming threats can only be thwarted at the physical (PHY) layer but not at the MAC or network layer. When a wireless network suffers from jamming attacks, its legitimate wireless signals are typically overwhelmed by irregular or sophisticated radio jamming signals, making it hard for legitimate wireless devices to decode data packets. Therefore, any strategies at the MAC layer or above are incapable of thwarting jamming threats, and innovative anti-jamming strategies are needed at the physical layer. Third, the effective anti-jamming strategies for real-world wireless networks remain limited. Despite the significant advancement of wireless technologies, most of current wireless networks (e.g., cellular and Wi-Fi networks) can be easily paralyzed by jamming attacks due to the lack of protection mechanism. The vulnerability of existing wireless networks can be attributed to the lack of effective anti-jamming mechanisms in practice. The jamming vulnerability of existing wireless networks also underscores the critical need and fundamental challenges in designing practical anti-jamming schemes.

This article provides a comprehensive survey on jamming attacks and anti-jamming strategies in various wireless networks, with the objectives of providing readers with a holistic knowledge landscape of existing jamming/anti-jamming techniques and stimulating more research endeavors in the design of jamming-resistant wireless networking sys-

The authors are with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824 (Corresponding author: H. Zeng). This work was supported in part by NSF Grant CNS-2100112.

TABLE I: This survey article versus prior survey papers.

Ref.	Studied networks	Studied layers	Attacks techniques	Anti-attack strategies	Attack detection
[20]	WSNs	PHY	✓	✓	✓
[21]	WSNs	PHY/Network/Session	✓	✓	✓
[22]	ZigBee networks	PHY/MAC	✓	✗	✗
[23]	WSNs	PHY/MAC/Network/Transport/Application	✓	✓	✓
[24]	WSNs/WLANs	PHY	✓	✓	✓
[25]	WSNs	PHY/MAC	✓	✓	✓
[26]	CRNs	PHY/MAC	✗	✓	✓
[27]	Cellular networks	PHY/Link/Network	✓	✗	✗
[28]	Ad-hoc networks	PHY/MAC	✓	✓	✓
[29]	OFDM networks	PHY	✓	✗	✗
[30]	Ad-hoc networks	PHY/MAC	✓	✓	✓
This article	**WLANs/Cellular/CRNs/ ZigBee/Bluetooth/LoRa Vehicular/GPS/RFID networks**	**PHY/MAC/Implementation**	✓	✓	✓

tems. Specifically, our survey covers wireless local area networks (WLANs), cellular networks, cognitive radio networks (CRNs), vehicular networks, Bluetooth and ZigBee networks, RFID communications, GPS systems, millimeter (mmWave) systems, learning-assisted wireless systems, etc. For each type of wireless network, we first offer an overview on the system design and then provide a primer on its PHY/MAC layers, followed by an in-depth review of the existing PHY-/MAC-layer jamming and defense strategies in the literature. Finally, we offer discussions on open issues and promising research directions.

Prior to this work, there are several survey papers on jamming and/or anti-jamming attacks in wireless networks [20]–[30], [34]–[37]. In [20], the authors surveyed the jamming attacks and defense mechanisms in WSNs. In [21], Zhou et al. surveyed the security challenges on WSNs' network protocols, including key establishment, authentication, integrity protection, and routing. In [22], Amin et al. surveyed PHY and MAC layer attacks on IEEE 802.15.4 (ZigBee networks). In [23], Raymond et al. focused on denial-of-service attacks and the countermeasures in higher WSNs' network protocols (e.g., transport and application layers). [24] classified the attacks and countermeasure techniques from both the attacker and the defender's perspective, the game-theoretical models, and the solutions used in WSNs and WLANs. In [25], Xu et al. surveyed jamming attacks, jamming detection strategies, and defense techniques in WSNs. [26] summarized the jamming attacks and anti-jamming solutions in CRNs. [27] surveyed the denial of service attacks in LTE cellular networks. [28], [30] reviewed the generic PHY-layer jamming attacks, detection, and countermeasures in wireless ad hoc networks. In [29], Shahriar et al. offered a tutorial on PHY layer security challenges in OFDM networks. Table I summarizes the existing survey works on jamming and/or anti-jamming attacks in wireless networks.

Unlike prior survey papers, this article conducts a comprehensive review on up-to-date jamming attacks and anti-jamming strategies, and provides the necessary PHY/MAC-layer knowledge for general readers to understand the jamming/anti-jamming strategies in a wide spectrum of wireless networks. The contributions of this paper are summarized

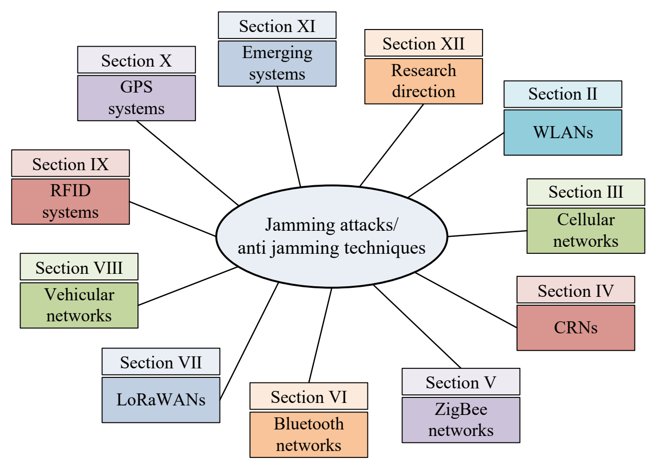


Fig. 1: The structure of this article.

as follows.

- We conduct a comprehensive, in-depth review on existing jamming attacks in various wireless networks, including WLANs, cellular networks, CRNs, Bluetooth and ZigBee networks, LoRaWANs, VANETs, UAVs, RFID systems, and GPS systems. We offer the necessary PHY/MAC-layer knowledge for general readers to understand the destructiveness of jamming attacks in those networks.
- We conduct an in-depth survey on existing anti-jamming strategies in wireless networks, including power control, spectrum spreading, frequency hopping, MIMO-based jamming mitigation, and jamming-aware protocols. We quantify their jamming mitigation capability and discuss their applications.
- We conduct a literature review on jamming attacks and anti-jamming strategies on emerging wireless technologies, including mmWave communications and learning-based wireless systems. In addition to the review of jamming and anti-jamming strategies, we discuss the lesson learned from this survey and open issues of jamming threats in wireless networks. We also point out promising research directions towards securing wireless networks.

The remainder of this article is organized following the

TABLE II: List of abbreviations.

Abbreviation	Explanation
ARF	Automatic Rate Fallback
ARQ	Automatic Repeat Request
BLE	Bluetooth Low Energy
CRC	Cyclic Redundancy Check
CRN	Cognitive Radio Network
CSMA/CA	Carrier-Sense Multiple Access/Collision Avoidance
CSS	Cooperative Spectrum Sensing
DCI/UCI	Downlink/Uplink Control Information
DoS	Denial of Service
DSSS	Direct-Sequence Spread Spectrum
FC	Fusion Center
FHSS	Frequency Hopping Spread Spectrum
GMSK	Gaussian Minimum Shift Keying
GPS	Global Positioning System
ICI	Inter Channel Interference
LoRaWAN	LoRa Wide Area Network
LTF	Long Training Field
MAC	Medium Access Control
MCS	Modulation and Coding Scheme
MIB/SIB	Master/System Information Block
MMSE	Minimum Mean Square Error
NAV	Net Allocation Vector
NDP	Null Data Packet
NOMA	Non-Orthogonal Multiple Access
PBCH	Physical Broadcast Channel
PDCCH/PUCCH	Physical Downlink/Uplink Control Channel
PDSCH/PUSCH	Physical Downlink/Uplink Shared Channel
PHICH	Physical Hybrid ARQ Indicator Channel
PRACH	Physical Random Access Channel
PRB	Physical Resource Block
PSS/SSS	Primary/Secondary Synchronization Signal
RAA	Rate Adaptation Algorithm
RAT	Radio Access Technology
RFID	Radio-Frequency Identification
RSI	Road Side Infrastructure
RSSI	Received Signal Strength Indicator
RTS/CTS	Request To Send/Clear To Send
SC-FDMA	Single Carrier Frequency Division Multiple Access
SDR	Software Defined Radio
STF	Short Training Field
UAV	Unmanned Aerial Vehicle
USRP	Universal Software Radio Peripheral
VHT	Very High Throughput
WCDMA	Wideband Code Division Multiple Access

structure as shown in Fig. 1. In Section II, we survey jamming and anti-jamming attacks in WLANs. In Section III, we survey jamming and anti-jamming attacks in cellular networks. In Section IV, we survey jamming and anti-jamming attacks in cognitive radio networks. Sections V and VI offer an in-depth review on jamming attacks and anti-jamming techniques for ZigBee and Bluetooth networks, respectively. Section VII presents an overview of jamming attacks and anti-jamming techniques in LoRa communications. Section VIII studies existing jamming and anti-jamming techniques for vehicular networks, including on-ground vehicular transportation networks (VANETs) and in-air unmanned aerial vehicular (UAV) networks. Section IX reviews jamming and anti-jamming techniques for RFID systems, and Section X reviews those techniques for GPS systems. Section XI reviews jamming and anti-jamming techniques in emerging wireless systems. Section XII discusses open problems and points out some promising research directions. Section XIII concludes this article.

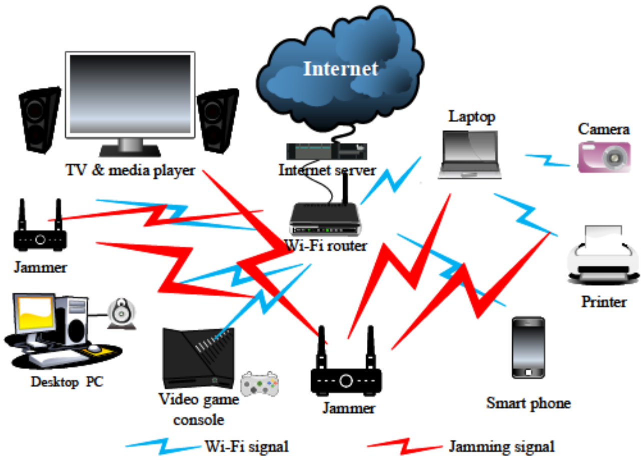


Fig. 2: Illustration of jamming attacks in a Wi-Fi network.

Table II lists the abbreviations used in this article.

II. Jamming and Anti-Jamming Attacks in WLANs

WLANs become increasingly important as they carry even more data traffic than cellular networks. With the proliferation of wireless applications in smart homes, smart buildings, and smart hospital environments, securing WLANs against jamming attacks is of paramount importance. In this section, we study existing jamming attacks and anti-jamming techniques for a WLAN as shown in Fig. 2, where one or more malicious jamming devices attempt to disrupt wireless connections of Wi-Fi devices. Prior to that, we first review the MAC and PHY layers of WLANs, which will lay the knowledge foundation for our review on existing jamming/anti-jamming strategies.

A. A Primer of WLANs

As shown in Fig. 2, WLANs are the most dominant wireless connectivity infrastructure for short-range and high-throughput Internet services and have been widely deployed in population-dense scenarios such as homes, offices, campuses, shopping malls, and airports. Wi-Fi networks have been designed based on the IEEE 802.11 standards, and 802.11a/g/n/ac standards are widely used in various commercial Wi-Fi devices such as smartphones, laptops, printers, cameras, and smart televisions. Most of Wi-Fi networks operate in unlicensed industrial, scientific, and medical (ISM) frequency bands, which have 14 overlapping 20 MHz channels on 2.4 GHz and 28 non-overlapping 20 MHz channels bandwidth in 5 GHz [38]. Most Wi-Fi devices are limited to a maximum transmit power of 100 mW, with a typical indoor coverage range of 35 m. A Wi-Fi network can cover up to 1 km range in outdoor environments in an extended coverage setting.

1) MAC-Layer Protocols: Wi-Fi devices use CSMA/CA as their MAC protocols for channel access. A Wi-Fi user requires to sense the channel before it sends its packets. If the channel sensed busy, the user waits for a DIFS time window and backs off its transmissions for a random amount of time. If the user cannot access the channel in one cycle, it cancels the random back-off counting and stands by for the channel to be idle

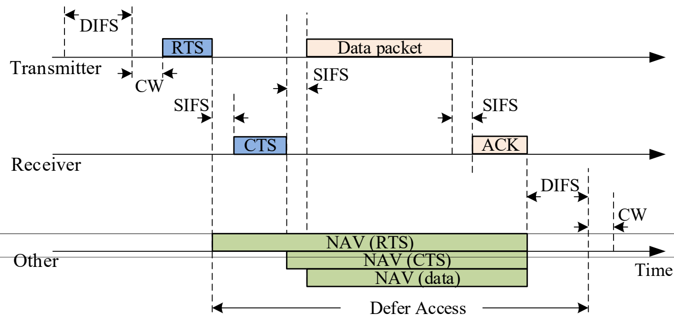
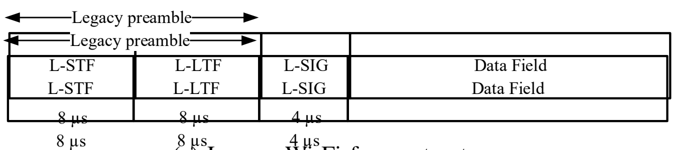
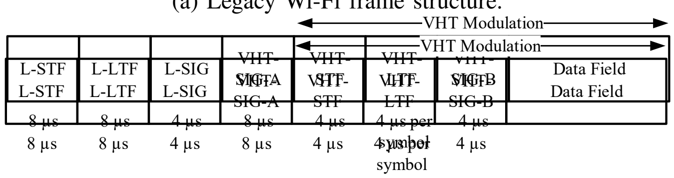


Fig. 3: The RTS/CTS protocol in 802.11 Wi-Fi networks [39].



(a) Legacy Wi-Fi frame structure.



(b) VHT Wi-Fi frame structure.

Fig. 4: Two frame structures used in 802.11 Wi-Fi networks.

for the DIFS duration. In this case, the user can immediately access the channel as the longer waiting users have priority over the users recently joined the network.

The CSMA/CA MAC protocol, however, suffers from the hidden node problem. The hidden node problem refers to the case where one access point (AP) can receive from two nodes, but those two nodes cannot receive from each other. If both nodes sense the channel idle and send their data to the AP, then packet collision occurs at the AP. The RTS/CTS (Request-to-Send and Clear-to-Send) protocol was invented to mitigate the hidden node problem, and Fig. 3 shows the RTS/CTS protocol mechanism. The transmitter who intends to access the channel waits for the DIFS duration. If the channel is sensed idle, the transmitter sends an RTS packet to identify the receiver and the required duration for data transmission. Every node receiving the RTS sets its Net Allocation Vector (NAV) to defer its try for accessing the channel to the subsequent frame exchange.

While previous and current Wi-Fi networks (e.g., 802.11g, 802.11n and 802.11ac) use the distributed CSMA/CA protocol for medium access control, the next-generation 802.11ax Wi-Fi networks (marketed as Wi-Fi 6) come with a centralized architecture with features such as OFDMA, both uplink and downlink MU-MIMO, trigger-based random access, spatial frequency reuse, and target wake time (TWT) [40], [41]. Despite these new features, 802.11ax devices will be backward compatible with the predecessor Wi-Fi devices. Therefore, the jamming and anti-jamming attacks designed for 802.11n/ac Wi-Fi networks also apply to the upcoming 802.11ax Wi-Fi networks.

2) Frame Structures: Most Wi-Fi networks use OFDM modulation at the PHY layer for both uplink and downlink transmissions. Fig. 4(a) shows the legacy Wi-Fi (802.11a/g) frame, which consists of preamble, signal field, and data field. The preamble comprises two STFs and two LTFs, mainly used for frame synchronizations and channel estimation purposes. In particular, STF consists of ten identical symbols and is used for start-of-packet detection, coarse time and frequency synchronizations. LTF consists of two identical OFDM symbols and is used for fine packet and frequency synchronizations. LTF is also used for channel estimation and equalization. Following the preamble, the signal (SIG) field carries the necessary packet information such as the adopted modulation and coding scheme (MCS) and the data part's length. SIG field is always transmitted using BPSK modulation for minimizing the error probability at the receiver side. Data field carries user payloads and user-specific information. Wi-Fi may use different MCS (e.g., OQPSK, 16-QAM, and 64-QAM) for data bits modulation, depending on the link quality. Four pilot signals are also embedded into four different tones (subcarriers) for further residual carrier and phase offset compensation in the data field.

Fig. 4(b) shows the VHT format structure used by 802.11ac. As shown in the figure, it consists of L-STF, L-LTF, L-SIG, VHT-SIG-A, VHT-STF, VHT-LTF, VHT-SIG-B, and Data Field. To maintain its backward compatibility with 802.11a/g, the L-STF, L-LTF, and L-SIG in the VHT frame are the same as those in Fig. 4(a). VHT-SIG-A and VHT-SIG-B are for similar purpose as the header field (HT-SIG) of 11n and SIG field of 11a. In 802.11ac, signal fields are SIG-A and SIG-B. They describe channel bandwidth, modulation-coding and indicate whether the frame is for a single user or multiple users. These fields are only deployed by the 11ac devices and are ignored by 11a and 11n devices. VHT-STF has the same function as that of the non-HT STF field. It assists the 11ac receiver to detect the repeating pattern. VHT-LTF consists of a sequence of symbols and is used for demodulating the rest of the frame. Its length depends on the number of transmitted streams. It could be 1, 2, 4, 6, or 8 symbols. It is mainly used for channel estimation purposes. Data field carries payload data from the upper layers. When there are no data from upper layers, the field is referred to as the null data packet (NDP) and is used for measurement and beamforming sounding purposes by the physical layer.

3) PHY-Layer Signal Processing Modules: Fig. 5 shows the PHY-layer signal processing framework of a legacy Wi-Fi transceiver. On the transmitter side, the data bitstream is first scrambled and then encoded using a convolutional or LDPC encoder. The coded bits are modulated according to the pre-selected MCS index. Then, the modulated data and pilot signals are mapped onto the scheduled subcarriers and converted to the time domain using OFDM modulation (IFFT operation). Following the OFDM modulation, the cyclic prefix (CP) is appended to each OFDM symbol in the time domain. After that, a preamble is attached to the time-domain signal. Finally, the output signal samples are up-converted to the desired carrier frequency and transmitted over the air using a radio frequency (RF) front-end module.

Referring to Fig. 5 again, on the receiver side, the received radio signal is down-converted to baseband I/Q signals, which

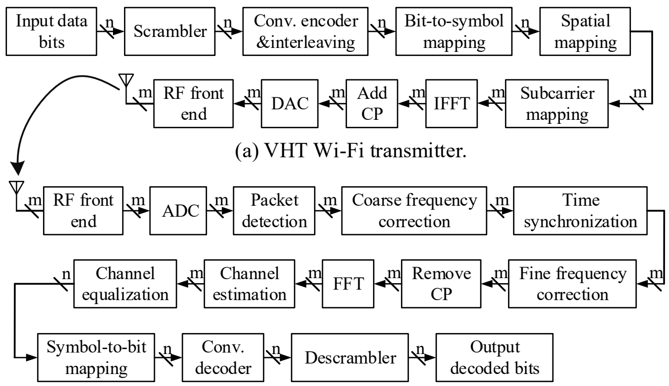


Fig. 5: A schematic diagram of baseband signal processing for an 802.11 Wi-Fi transceiver [39] ($n \leq 4$ and $m \leq 8$).

are further converted to digital streams by ADC modules. The start of a packet can be detected by auto-correlating the received signal stream with itself in a distance of one OFDM symbol to identify the two transmitted STF signals within the frame. The received STF signals can be used to coarsely estimate the carrier frequency offset, which can then be utilized to correct the offset and improve the timing synchronization accuracy. Timing synchronization can be done by cross-correlating the received signal and a local copy of the LTF signal at the receiver. LTF is also used for fine frequency offset correction. Once the signal is synchronized, it is converted into the frequency domain using the OFDM demodulation, which comprises CP removal and FFT operation.

The received LTF symbols are used to estimate the wireless channel between the Wi-Fi transmitter and receiver for each subcarrier. Channel smoothing, which refers to interpolating the estimated channel for each subcarrier using its adjacent estimated subcarriers' channels, is usually used to suppress the impact of noise in the channel estimation process. The estimated channels are then used to equalize the channel distortion of the received frame in the frequency domain. The received four pilots are used for residual carrier frequency, and phase offsets correction. After phase compensation, the received symbols are mapped into their corresponding bits. This process is called symbol-to-bit mapping. Following the symbol-to-bit mapping, convolutional or LDPC decoder and descrambler are applied to recover the transmitted bits. The recovered bits are fed to the MAC layer for protocol-level interpretation.

B. Jamming Attacks

With the primer knowledge provided above, we now dive into the review of existing jamming attacks in WLANs. In what follows, we first survey the generic jamming attacks proposed for Wi-Fi networks but can also be applied to other types of wireless networks and then review the jamming attacks that delicately target the PHY transmission and MAC protocols of Wi-Fi communications.

1) Generic Jamming Attacks: While there are many jamming attacks that were originally proposed for Wi-Fi networks, they can also be applied to other types of wireless systems. We survey these generic jamming attacks in this part.

Constant Jamming Attacks: Constant jamming attacks refer to the scenario where the malicious device broadcasts a powerful signal all the time. Constant jamming attacks not only destroy legitimate users' packet reception by introducing high-power interference to their data transmissions, but they also prevent them from accessing the channel by continuously occupying it. In constant jamming attacks, the jammer may target the entire or a fraction of channel bandwidth occupied by legitimate users [28], [30]. In [42], Karishma et al. analyzed the performance of legacy Wi-Fi communications under broadband and partial-band constant jamming attacks through theoretical exploration and experimental measurement. The authors conducted experiments to study the impact of jamming power on Wi-Fi communication performance when the data rate is set to 18 Mbps. Their experimental results show that a Wi-Fi receiver fails to decode its received packets under broadband jamming attack (i.e., 100% packet error rate) when the received desired signal power is 4 dB less than the received jamming signal power (i.e., signal-to-jamming power ratio, abbreviated as SJR, less than 4 dB). The theoretical analysis in [42], [43] showed that Wi-Fi communication is more resilient to partial-band jamming than broadband jamming attacks. The experimental results in [42] showed that, for the jamming signal with bandwidth being one subcarrier spacing (i.e., 312.5 KHz), Wi-Fi communication fails when SJR < -19 dB. In [31], Vanhoef et al. used a commercial Wi-Fi dongle and modified its firmware to implement a constant jamming attack. To do so, they disabled the CSMA protocol, backoff mechanism, and ACK waiting time. To enhance the jamming effect, they also removed all interframe spaces and injected many packets for transmissions.

Reactive Jamming Attacks: Reactive jamming attack is also known as channel-aware jamming attack, in which a malicious jammer sends an interfering radio signal when it detects legitimate packets transmitted over the air [44]. Reactive jamming attacks are widely regarded as an energy-efficient attack strategy since the jammer is active only when there are data transmissions in the network. Reactive jamming attack, however, requires tight timing constraints (e.g., < 1 OFDM symbols, 4 μs) for real-world system implementation because it needs to switch from listening mode to transmitting mode quickly. In practice, a jammer may be triggered by either channel energy-sensing or part of a legitimate packet's detection (e.g., preamble detection). In [45], Prasad et al. implemented a reactive jamming attack in legacy Wi-Fi networks using the energy detection capability of cognitive radio devices. In [46], [47], Yan et al. studied a reactive jamming attack where a jammer sends a jamming signal after detecting the preamble of the transmitted Wi-Fi packets. By doing so, the jammer is capable of effectively attacking Wi-Fi packet payloads. In [48], Schulz et al. used commercial off-the-shelf (COTS) smartphones to implement an energy-efficient reactive jammer in Wi-Fi networks. Their proposed scheme is capable of replying ACK packets to the legitimate transmitter to hijack its retransmission protocol, thereby resulting in a complete Wi-Fi packet loss whenever packet error occurs. In [49], Bayraktaroglu et al. evaluated the performance of Wi-Fi networks under reactive jamming attacks. Their experimental results showed that reactive jamming could result in a near-zero throughput in real-world Wi-Fi networks. In [31], Vanhoef et al. implemented a reactive jamming attack using a commercial off-the-shelf Wi-Fi dongle. The device decodes the header of an on-the-air packet to carry out the attack implementation, stops receiving the frame, and launches the jamming signal.

Deceptive Jamming Attacks: In deceptive jamming attacks, the malicious jamming device sends meaningful radio signals to a Wi-Fi AP or legitimate Wi-Fi client devices, with the aim of wasting a Wi-Fi network's time, frequency, and/or energy resources and preventing legitimate users from channel access. In [50], Broustis et al. implemented a deceptive jamming attack using a commercial Wi-Fi card. The results in [50] showed that a low-power deceptive jammer could easily force a Wi-Fi AP to allocate all the network's resources for processing and replying fake signals issued by a jammer, leaving no resource for the AP to serve the legitimate users in the network. In [51], Gvozdenovic et al. proposed a deceptive jamming attack on Wi-Fi networks called truncate after preamble (TaP) jamming and evaluated its performance on USRP-based testbed. TaP attacker lures legitimate users to wait for a large number of packet transmissions by sending them the packets' preamble and the corresponding signal field header only.

Random and Periodic Jamming Attacks: Random jamming attack (a.k.a. memoryless jamming attack) refers to the type of jamming attack where a jammer sends jamming signals for random periods and turns to sleep for the rest of the time. This type of jamming attack allows the jammer to save more energy compared to a constant jamming attack. However, it is less effective in its destructiveness compared to constant jamming attack. Periodic jamming attacks are a variant of random jamming attacks, where the jammer sends periodic pulses of jamming signals. In [49], the authors investigated the impact of random and periodic jamming attacks on Wi-Fi networks. Their experimental results showed that the random and periodic jamming attacks' impact became more significant as the duty-cycle of jamming signal increases. The experimental results in [49] also showed that, for a given network throughput degradation and jamming pulse width, the periodic jamming attack consumes less energy than the random jamming attack. It is noteworthy that, compared to the random jamming attack, periodic jamming attack bears a higher probability of being detected as it follows a predictable transmission pattern.

Frequency Sweeping Jamming Attacks: As discussed earlier, there are multiple channels available for Wi-Fi communications on ISM bands. For a low-cost jammer, it is constrained by its hardware circuit (e.g., very high ADC sampling rate and broadband power amplifier) in order to attack a large number of channels simultaneously. Frequency-sweeping jamming attacks were proposed to get around of this constraint, such that a jammer can quickly switch (e.g., in the range of 10 μs) to different channels. In [52], Bandaru analyzed Wi-Fi networks' performance under frequency-sweeping jamming attacks on 2.4 GHz, where there are only 3 non-overlapping 20 MHz channels. The preliminary results in [52] showed that the sweeping-jammer could decrease the total Wi-Fi network throughput by more than 65%.

2) WiFi-Specific Jamming Attacks: While the above jamming attacks are generic and can apply to any type of wireless network, the following jamming attacks are dedicated to the PHY signal processing and MAC protocols of Wi-Fi networks.

Jamming Attacks on Timing Synchronization: As shown in Fig. 5, timing synchronization is a critical component of the Wi-Fi receiver to decode the data packet. Various jamming attacks have been proposed to thwart the signal timing acquisition and disrupt the start-of-packet detection procedure, such as false preamble attack, preamble nulling attack, and preamble warping attack [29], [53], [54]. These attacks were sophisticatedly designed to thwart the timing synchronization process at a Wi-Fi receiver. Preamble nulling attack [53], [54] is another form of timing synchronization attacks. In this attack, the jammer attempts to nullify the received preamble energy at the Wi-Fi receiver by sending an inverse version of the preamble sequence in the time domain. Preamble nulling attack, however, requires perfect knowledge of the network timing, so it is hard to be realized in real Wi-Fi networks. Moreover, preamble nulling attack may have considerable error since the channels are random and unknown at the jammer. Preamble warping attack [53], [54] designed to disable the STF-based auto-correlation synchronization at a Wi-Fi receiver by transmitting the jamming signal on the subcarriers where STF should have zero data.

Jamming Attacks on Frequency Synchronization: For a Wi-Fi receiver, carrier frequency offset may cause subcarriers to deviate from mutual orthogonality, resulting in inter-channel interference (ICI) and SNR degradation. Moreover, carrier frequency offset may introduce an undesired phase deviation for modulated symbols, thereby degrading symbol demodulation performance. In [55], Shahriar et al. argued that, under off-tone jamming attacks, the orthogonality of subcarriers in an OFDM system would be destroyed. This idea has been used in [56], where the jammer takes down 802.11ax communications by using 20–25% of the entire bandwidth to send an unaligned jamming signal. In Wi-Fi communications, frequency offset in Wi-Fi communications is estimated by correlating the received preamble signal in the time domain. Then, the preamble attacks proposed for thwarting timing synchronization can also be used to destroy the frequency offset correction functionalities. In [57], two attacks have been proposed to malfunction the frequency synchronization correction: *preamble phase warping attack* and *differential scrambling attack*. In the preamble phase warping attack, the jammer sends a frequency shifted version of the preamble, causing an error in frequency offset estimation at the Wi-Fi receiver. Differential scrambling attack targets the coarse frequency correction in Fig. 5, where STF is used to estimate the carrier frequency. The jammer transmits interfering signals across the subcarriers used in STF, aiming to distort the periodicity pattern of the received preamble required for frequency offset estimation.

Jamming Attacks on Channel Estimation: As shown in Fig. 5, channel estimation and channel equalization are essential modules for a Wi-Fi receiver. Any malfunction in their operations is likely to result in a false frame decoding output.

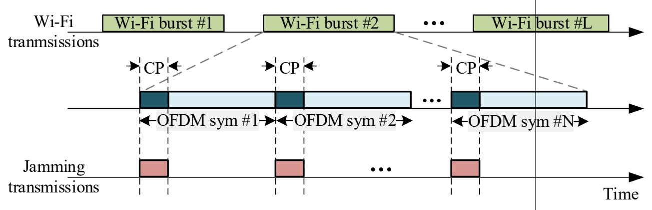


Fig. 6: Illustration of a jamming attack targeting on OFDM symbol's cyclic prefix (CP) [62].

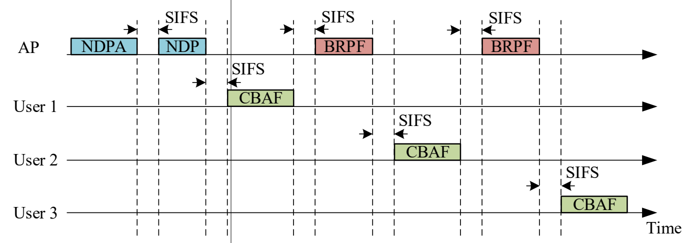


Fig. 7: The beamforming sounding protocol in 802.11 VHT Wi-Fi networks.

A Wi-Fi receiver uses the received frequency-domain preamble sequence to estimate the channel frequency response of each subcarrier. A natural method to attack channel estimation and channel equalization modules is to interfere with the preamble signal. Per [53], [58], the preamble nulling attack can also be used to reduce the channel estimation process's accuracy. The simulation results in [58] showed that, while preamble nulling attacks are highly efficient in terms of active jamming time and power, they are incredibly significant to degrade network performance. However, it would be hard to implement preamble nulling attacks in real-world scenarios due to the timing and frequency mismatches between the jammer and the legitimate target device. The impact of synchronization mismatches on preamble nulling attacks has been studied in [59]. In [60] and [61], Sodagari et al. proposed the singularity of jamming attacks in MIMO-OFDM communication networks such as 802.11n/ac, LTE, and WiMAX, intending to minimize the rank of estimated channel matrix on each subcarrier at the receiver. Nevertheless, the proposed attack strategies require the global channel state information (CSI) to be available at the jammer to design the jamming signal.

Jamming Attacks on Cyclic Prefix (CP): Since most wireless communication systems employ OFDM modulation at the physical layer and every OFDM symbol has a CP, jamming attacks on OFDM symbols' CP have attracted many research efforts. In [62], Scott et al. introduced a CP jamming attack, where a jammer targets the CP samples of each transmitted OFDM symbol, as shown in Fig. 6. The authors showed that the CP jamming attack is an effective and efficient approach to break down any OFDM communications such as Wi-Fi. The CP corruption can easily lead to a false output of linear channel equalizers (e.g., ZF and MMSE). Moreover, the authors also showed that the CP jamming attack saves more than 80% energy compared to constant jamming attacks to pull down Wi-Fi transmissions. However, jamming attack on CP is challenging to implement as it requires jammer to have a precise estimation of the network transmission timing [29].

Jamming Attacks on MU-MIMO Beamforming: Given the asymmetry of antenna configurations at an AP and its serving client devices in Wi-Fi networks, recent Wi-Fi technologies (e.g., IEEE 802.11ac and IEEE 802.11ax) support multi-user MIMO (MU-MIMO) transmissions in their downlink, where a multi-antenna AP can simultaneously serve multiple single-antenna (or multi-antenna) users using beamforming technique [38]. To design beamforming precoders (a.k.a. beamforming matrix), a Wi-Fi AP requires to obtain an estimation of the channels between its antennas and all serving users. Per IEEE 802.11ac standard, the channel estimation procedure in VHT Wi-Fi communications is specified by the following three steps: First, the AP broadcasts a sounding packet to the users. Second, each user estimates its channel using the received sounding packet. Third, each user reports its channel estimation results to the AP.

Fig. 7 shows the beamforming sounding protocol in VHT Wi-Fi networks. The AP issues a null data packet announcement (NDPA) in order to reserve the channel for channel sounding and beamforming processes. Following the NDPA signaling, the AP broadcasts a null data packet (NDP) as the sounding packet. The users use the preamble transmitted within the NDP to estimate the channel frequency response on each subcarrier. Then, the Givens Rotations technique is generally used to decrease the channel report overhead, where a series of angles are sent back to the AP as the compressed beamforming action frame (CBAF), rather than the original estimated channel matrices. The AP uses beamforming report poll frame (BRPF) to manage the report transmissions among users [69].

In [63], Patwardhan et al. studied the VHT Wi-Fi beamforming vulnerabilities. They have built a prototype of a radio jammer using a USRP-based testbed that jams the NDP transmissions such that the users will no longer be able to estimate their channels and then report false CBAFs. Their experimental results showed that, in the presence of the NDP jamming attack, less than 7% of packets could be successfully beamformed in MU-MIMO transmission.

Jamming Attacks on MAC packets: A series of jamming attacks on MAC packets, also called intelligent jamming attacks, have been proposed in [64] and [65], aiming to degrade Wi-Fi communications' performance. The main focus of intelligent jamming attacks is on corrupting the control packets such as CTS and ACK packets used by Wi-Fi MAC protocols. For CTS attack, the jammer listens to the RTS packet transmitted by an active node, waits a SIFS time slot from the end of RTS, and jams the CTS packet. Failing to decode the CTS packet can simply stop data communication. A similar idea was proposed to attack ACK packet transmissions. As the transmitter cannot receive the ACK packet, it retransmits the data packet. Retransmission continues until the TCP limit is reached or an abort is issued to the application. An intelligent jamming attack can also target the data packet where the jammer senses the RTS and CTS and sends the jamming signal following an SIFS time slot.

Jamming Attacks on Rate Adaptation Algorithms: In Wi-Fi

TABLE III: A summary of jamming attacks in Wi-Fi networks.

Attacks	Ref.	Mechanism	Strengths	Weaknesses
Generic jamming attacks	[28], [30] [31], [42], [43]	Constant jamming attack	Highly effective	Energy inefficient
	[44]–[47] [31], [48], [49]	Reactive jamming attack	Highly effective Energy efficient	Hardware constraints
	[50], [51]	Deceptive jamming attack	Energy efficient	Less effective
	[49]	Random and periodic jamming attack	Energy efficient	Less effective
	[52]	Frequency sweeping jamming attack	Highly effective	Energy inefficient
Timing synchronization attacks	[29], [53]	Preamble jamming attack Preamble nulling attack	High effective Energy-efficient High stealthy	Hard to implement Tight timing synchronization required
Frequency synchronization attacks	[55], [56]	Asynchronous off-tone jamming attack	Energy-efficient High stealthy	Less effective
	[57]	Phase warping attack Differential scrambling attack		
Channel estimation (pilot) attacks	[53], [59]	Pilot jamming attack	Energy-efficient High effective High stealthy	Hard to implement Tight timing synchronization required
	[58], [59]	Pilot nulling attack		
	[60], [61]	Singularity jamming attack		
Cyclic prefix attacks	[62]	Cyclic prefix (CP) jamming attack	Energy-efficient High effective High stealthy	Hard to implement Tight timing synchronization required
Beamforming attacks	[63]	NDP jamming attack	Energy-efficient	Applies to 802.11ac/ax and beyond
Jamming attacks on MAC packets	[64], [65]	CTS corruption jamming attack ACK corruption jamming attack Data corruption jamming attack	Energy-efficient High effective High stealthy	Tight timing synchronization required
Rate adaptation algorithm attacks	[66]–[68]	Keeping the network throughout below a threshold	Energy-efficient High stealthy	Less effective

networks, rate adaptation algorithms (RAAs) were mainly designed to make a proper modulation and coding scheme (MCS) selection for data modulation. RRAs can be considered as a defense mechanism to overcome lossy channels in the presence of low-power interference and jamming signals. However, the pattern designed for RRAs can be targeted by jammer to degrade the network throughput below a certain threshold. RAAs change the transmission MCS based on the statistical information of the successful and failed decoded packets. The Automatic Rate Fallback (ARF) [70], SampleRate [71], and ONOE [72] are the main RAAs using in commercial Wi-Fi devices.

In [66], Noubir et al. investigated the RAAs' vulnerabilities against periodic jamming attacks. In [67] and [68], Orakcal et al. evaluated the performance of ARF and SampleRate RAAs under reactive jamming attacks. The simulation results showed that, in order to keep the throughput below a certain threshold in Wi-Fi point-to-point communications, higher RoJ is required in ARF RAA compared to the SampleRate RAA, where the RoJ is defined as the ratio of the number of jammed packets to the total number of transmitted packets. This reveals that SampleRate RAA is more vulnerable to jamming attacks.

3) A Summary of Jamming Attacks: Table III summarizes existing jamming attacks in WLANs. As it can be seen from the table, jamming attacks become increasingly sophisticated to disrupt the communications in WLANs. Generally speaking, constant jamming is the most destructive jamming attack for wireless networks without jamming protection mechanism. However, it is neither the most energy-efficient jamming attack nor the hardest jamming attack to thwart. Attacks such as reactive jamming, pilot jamming, MAC packet jamming and rate adaptation jamming have better energy efficiency compared to constant jamming attacks. Attacks such as random jamming and deceptive jamming pose more serious threat to wireless networks, and these attacks are harder to mitigate compared to constant jamming. In addition, different jamming attacks bear different implementation complexity. For example, constant jamming attack is easy to implement; it can be launched with a $20 USB-based SDR dongle. In contrast, reactive and pilot jamming attacks are more difficult to launch as they require a fine-grained timing alignment with the legitimate transmission.

C. Anti-Jamming Techniques

In this subsection, we review existing anti-jamming countermeasures proposed to eliminate or alleviate the impacts of jamming threats in WLANs. In what follows, we categorize the existing anti-jamming techniques into the following classes: channel hopping, MIMO-based jamming mitigation, coding protection, rate adaptation, and power control. We note that, given the destructiveness of jamming attacks and the complex nature of WLANs, there are no generic solutions that can tackle all types of jamming attacks.

1) Channel Hopping Techniques: Channel hopping is a low-complexity technique to improve the reliability of wireless communications under intentional or unintentional interference. Channel hopping has already been implemented in Bluetooth communications to enhance its reliability against undesired interfering signals and jamming attacks. In [73], Navda et al. proposed to use channel hopping to protect Wi-Fi networks from jamming attacks. They implemented a channel hopping scheme for Wi-Fi networks in a real-world environment. The reactive jamming attack can decrease Wi-Fi network throughput by 80% based on their experimental results. It was also shown that, by using the channel hopping technique, 60% Wi-Fi network throughput could be achieved in the presence of reactive jamming attacks when compared to the case without jamming attack. In [74], Jeung et al. used two concepts of window dwelling and a deception mechanism to secure WLANs against reactive jamming attacks. The window dwelling refers to adjusting the Wi-Fi packets' transmission time based on the jammer's capability. Their proposed deception mechanism leverages an adaptive channel hopping mechanism in which the jammer is cheated to attack inactive channels.

2) Spectrum Spreading Technique: Spectrum spreading is a classical wireless technique that has been used in several real-world wireless systems such as 3G cellular, ZigBee, and 802.11b. It is well known that it is resilient to narrowband interference and narrowband jamming attack. 802.11b employs DSSS to enhance link reliability against undesired interference and jamming attacks. It uses an 11-bit Barker sequence for 1 Mbps and 2 Mbps data rates, and an 8-bit complementary code keying (CCK) for 5.5 Mbps and 11 Mbps data rates. In [42], Karishma et al. evaluated the resiliency of DSSS in 802.11b networks against broadband, constant jamming attacks through simulation and experiments. Their simulation results show that the packet error rate hits 100% when SJR < -3 dB for 1 Mbps data rate, when SJR < 0 dB for 2 Mbps data rate, when SJR < 2 dB for 5.5 Mbps data rate, and when SJR < 5 dB for 11 Mbps data rate. Their experimental results show that an 802.11b Wi-Fi receiver fails to decode its received packets when received SJR < -7 dB for 1 Mbps data rate, when SJR < -4 dB for 2 Mbps data rate, when SJR < -1 dB for 5.5 Mbps data rate, and when SJR < 2 dB for 11 Mbps data rate. In addition, [75] evaluated the performance of 11 Mbps 802.11b DSSS communications under periodic and frequency sweeping jamming attacks. The results show that 802.11b is more resilient against periodic and frequency sweeping jamming attacks compared to OFDM 802.11g.

3) MIMO-based Jamming Mitigation Techniques: Recently, MIMO-based jamming mitigation techniques emerge as a promising approach to salvage wireless communications in the face of jamming attacks. In [46], [47], Yan et al. proposed a jamming-resilient wireless communication scheme using MIMO technology to cope with the reactive jamming attacks in OFDM-based Wi-Fi networks. The proposed anti-jamming scheme employs a MIMO-based interference mitigation technique to decode the data packets in the face of jamming signal by projecting the mixed received signals into the subspace orthogonal to the subspace spanned by jamming signals. The projected signal can be decoded using existing channel equalizers such as zero-forcing technique. However, this anti-jamming technique requires the knowledge of channel state information of both the desired user and jammer. Conventionally, a user's channel can be estimated in this case because the reactive jammer starts transmitting jamming signals in the aftermath of detecting the preamble of a legitimate packet. Therefore, the user's received preamble signal is not jammed. Moreover, it is shown in [46] that the complete knowledge of the jamming channel is not necessary, and the jammer's channel ratio (i.e., jammer's signal direction) suffices. Based on this observation, the authors further proposed inserting known pilots in the frame and using the estimated user's channel to extract the jammer's channel ratio. In [76], a similar idea called multi-channel ratio (MCR) decoding was proposed for MIMO communications to defend against constant jamming attacks. In the proposed MCR scheme, the jammer's channel ratio is first estimated by the received signals at each antenna when the legitimate transmitter stays silent. The jammer's channel ratio and the preamble in the transmitted frame are then used to estimate the projected channel component, which are later deployed to decode the desired signal.

While it is not easy to estimate channel in the presence of an unknown jamming signal, research efforts have been invested in circumventing this challenge. In [77], Zeng et al. proposed a practical anti-jamming solution for wireless MIMO networks to enable legitimate communications in the presence of multiple high-power and broadband radio jamming attacks. They evaluated their proposed scheme using real-world implementations in a Wi-Fi network. Their scheme benefits from two fundamental techniques: A jamming-resilient synchronization module and a blind jamming mitigation equalizer. The proposed blind jamming mitigation module is a low-complex linear spatial filter capable of mitigating the jamming signals from unknown jammers and recovering the desired signals from legitimate users. Unlike the existing jamming mitigation algorithms that rely on the availability of accurate jamming channel ratio, the algorithm does not need any channel information for jamming mitigation and signal recovery. Besides, a jamming-resilient synchronization algorithm was also crafted to carry out packet time and frequency recovery in the presence of a strong jamming signal. The proposed synchronization algorithm consists of three steps. First, it alleviates the received time-domain signal using a spatial projection-based filter. Second, the conventional synchronization techniques were deployed to estimate the start of frame and carrier frequency offset. Third, the received frames by each antenna were synchronized using the estimated frequency offset. The proposed scheme was validated and evaluated in a real-world implementation using GNURadio-USRP2. It was shown that the receiver could successfully decode the desired Wi-Fi signal in the presence of 20 dB stronger than the signals of interest.

4) Coding Techniques: Channel coding techniques are originally designed to improve the communication reliability in unreliable channels. In [78] and [79], the performance of low-density parity codes (LDPC) and Reed-Solomon codes were analyzed for different packet sizes under noise (pulse) jamming attacks with low duty cycle. It was shown that, for long size packets (e.g., a few thousand bits), LDPC coding scheme is a suitable choice as it can achieve throughput close to its theoretical Shannon limit while bearing a low decoding complexity.

5) MAC Layer Strategies: Rate adaptation and power control mechanisms are proposed to combat jamming attacks, provided that wireless devices have sufficient power supply and the jamming signal's power is limited. In [66], a series of rate adaptation algorithms (RAAs) were proposed to provide reliable and efficient communication scheme for Wi-Fi networks. Based on channel conditions, RAAs set a data rate such that the network can achieve the highest possible throughput. Despite the differences among existing RAAs, all RAAs trace the rate of successful packet transmissions and may increase or decrease the data rate accordingly. A power control mechanism

TABLE IV: A summary of anti-jamming techniques for WLANs.

Anti-jamming technique	Ref.	Mechanism	Application Scenario
Channel/frequency hopping techniques	[73]	Channel hopping scheme for Wi-Fi networks	All jamming attacks on a channel
	[74]	Window dwelling and adaptive channel hopping	Reactive jamming attack on a channel
DSSS techniques	[42], [75]	802.11b performance evaluation	Constant, periodic, and frequency-sweeping jamming attacks
MIMO-based techniques	[46], [47]	Mixed received signals projection onto the subspace orthogonal to the jamming signal.	Reactive jamming attack
	[76]	Multi-channel ratio (MCR) decoding.	Constant jamming attack
	[77]	Blind jamming mitigation and jamming-resilient synchronization.	Constant jamming attack
Coding techniques	[78], [79]	LDPC and Reed-Solomon code schemes' analysis	Low-power random jamming attack
MAC layer strategies	[80], [81]	Rate adaptation and power control mechanism evaluation	Random and periodic jamming attacks
	[82]	Randomized rate adaptation	Reactive jamming attacks
	[50]	Packet fragmentation	Low-power random jamming attack
	[83]	Cell breathing and load balancing concepts	Low-power constant jamming attack
	[84]	Adapting transmission probability based on local observations	Random and periodic jamming attacks
Detection mechanisms	[85]	Multi-factor learning-based algorithm	Constant and reactive jamming attacks
Learning-based techniques	[86]	DeepWiFi; auto-encoding, feature extraction NN-based channel classification, RF fingerprinting	Probabilistic, sensing-based, and adaptive jamming attacks

is another technique that can be used to improve wireless communication performance over poor quality links caused by interference and jamming signals. However, the power control mechanisms are highly subjected to the limit of power budget available at the transmitter side. Clearly, rate adaptation and power control techniques will not work in the presence of high power constant jamming attacks.

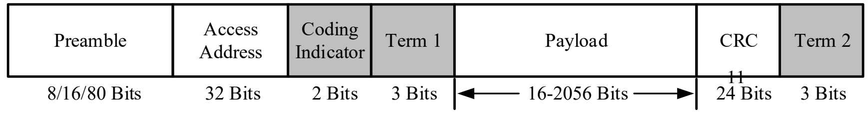
In [80], [81], Pelechrinis et al. studied the performance of these two techniques (rate adaptation and power control) in jamming mitigation for legacy Wi-Fi communications via real-world experiments. It was shown that the rate adaptation mechanism is generally effective in lossy channels where the desired signal is corrupted by low-power interference and jamming signals. When low transmission data rates are adopted, the jamming signal can be alleviated by increasing the transmit power. Nevertheless, power control is ineffective in jamming mitigation at high data rates. In [82], a randomized RAA was proposed to enhance rate adaptation capability against jamming attacks. The jammer attack was designed to keep the network throughput under a certain threshold, as explained earlier in RAA attacks. The main idea of this scheme lies in an unpredictable rate selection mechanism. When a packet is successfully transmitted, the algorithm randomly switches to another data rate with a uniform distribution. The proposed scheme shows higher reliability against this class of attacks. The results in [82] show that a jammer aiming to pull down network throughput below 1 Mbps will need to transmit a periodic jamming signal with $3\times$ more energy in order to achieve the same performance when legacy ARF algorithm applies.

In [50], an alternative approach was proposed for RAAs to cope with low-power jamming attacks using packet fragmentation. Although the smaller-sized packet transmissions induce more considerable overhead to the network, it can improve communications reliability under periodic and noise jamming attacks by reducing each packet's probability of being jammed. In [83], Garcia et al. borrowed the concept of cell breathing in cellular networks and deployed it in dense WLANs for jamming mitigation purposes. Here, cell breathing refers to the dynamic power control for adjusting an AP's transmission range. That is, an AP decreases its transmission range when bearing a high load and increases its transmission range when bearing a light load. Meanwhile, load balancing was proposed as a complementary technique to cell breathing. For a WLAN with cell breathing capability, the jamming attack can be treated as a case with a high load imposed on target APs [83].

In [84], Richa et al. designed a local MAC mechanism, called JADE, to secure multi-hop wireless networks against jamming attacks. The authors assumed that the jammer sends jamming signal to any node for a fraction of time and proposed an algorithm that allows the legitimate user to access the medium in the presence of jamming attack. In the proposed algorithm, each node adapts its transmission probability based on its local observations. In particular, every legitimate user updates its transmission probability according to its sensing results and the number of successfully received packets. The simulation results showed that JADE could achieve an optimal data rate in the presence of jamming attacks when the number of distributed nodes is large.

6) Jamming Detection Mechanisms: In [85], Puñal et al. proposed a learning-based jamming detection scheme for Wi-Fi communications. The authors used the parameters of noise power, the time ratio of channel being busy, the time interval between two frames, the peak-to-peak signal strength, and the packet delivery ratio as the training dataset, and used the random forest algorithm for classification. The performance of the proposed scheme was evaluated under constant and reactive jamming attacks. The simulation results show that the proposed scheme could detect the presence of jammer with 98.4% accuracy for constant jamming and with 94.3% accuracy for reactive jamming.

7) Learning-based Techniques: In [86], Davaslioglu et al. proposed DeepWiFi, a jamming-resilient receiver design that integrates deep learning into Wi-Fi 5 (i.e., IEEE 802.11ac) architecture to enhance the robustness of multi-hop communications against jamming attacks. The authors considered three different types of attacks, namely *probabilistic*, *sensing-*



based, and *adaptive* jamming attacks, in their model and leveraged machine learning to mitigate interference signal and increase network throughput. In particular, DeepWiFi adds the following four functions on top of the 802.11ac standard. First, it applies auto-encoding to I/Q signal to extract channel features. Second, it uses a convolutional neural network to classify the channel into three categories: idle, busy with other Wi-Fi signals, and jammed. Third, it uses RF fingerprint to authenticate legitimate Wi-Fi signal for channel access. The simulation results showed that the throughput loss of the proposed scheme is zero when the network has 40 channels and the jamming probability is 60%.

8) A Summary of Anti-Jamming Techniques: The increasing sophistication of jamming attacks leads to growing advancement of anti-jamming design. Table IV summarizes existing anti-jamming techniques designed for WLANs. Among these anti-jamming techniques, frequency hopping (FHSS) and spectrum spreading (DSSS) are easy to implement, but they are not efficient in spectrum utilization. Actually, their jamming resiliency comes at the cost of spectrum efficiency. MIMO-based techniques emerge as an effective anti-jamming approach, which can mitigate time-varying, frequency-varying jamming signals. As MIMO is a key technology for next-generation wireless networks, securing wireless systems by MIMO-based design is a promising research direction.

III. Jamming and Anti-Jamming Attacks in Cellular Networks

Although cellular networks have been evolving for more than four decades, existing cellular wireless communications are still vulnerable to jamming attacks. The vulnerability can be mainly attributed to the lack of practical yet efficient anti-jamming techniques at the wireless PHY/MAC layer that are capable of securing radio packet transmissions in the presence of jamming signals. The vulnerability also underscores the critical need for an in-depth understanding of jamming attacks and for more research efforts on the design of efficient anti-jamming techniques. In this section, we consider a cellular network under jamming attacks. We first provide a primer of cellular networks, focusing on long-term evolution (LTE) systems. Then, we conduct an in-depth review on existing jamming attacks and anti-jamming strategies at the PHY/MAC layers of cellular networks.

A. A Primer of Cellular Networks

Cellular networks have evolved from the first generation toward the fifth-generation (5G). While 5G is still under construction, we focus our overview on 4G LTE/LTE-advanced cellular networks. Generally speaking, the jamming attacks in 4G LTE networks can also apply to 5G networks as they share the same wireless technologies at the PHY/MAC layers. 4G LTE/LTE-advanced has been widely adopted by mobile network operators to provide wide-band, high throughput, and extended coverage services for mobile devices. Due to its success in mobile networking, the LTE framework is now known as the primary reference scheme for future cellular networks such as 5G. LTE supports channel bandwidth from

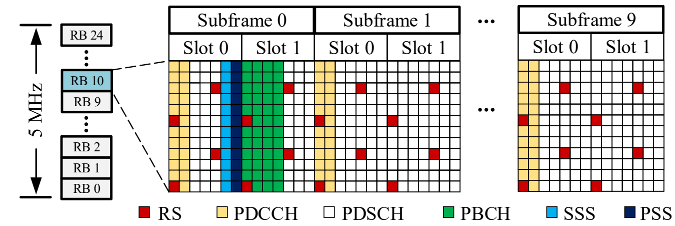
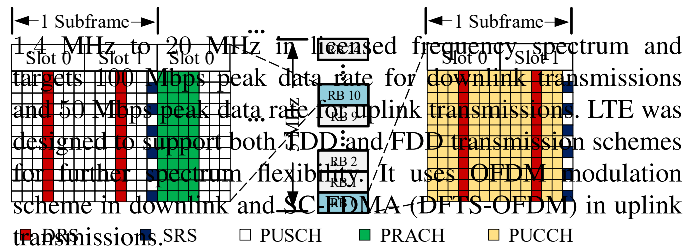


Fig. 8: LTE downlink resource grid [88].



1.4 MHz to 20 MHz in licensed frequency spectrum and targets 100 Mbps peak data rate for downlink transmissions and 50 Mbps peak data rate for uplink transmissions. LTE was designed to support both TDD and FDD transmission schemes for further spectrum flexibility. It uses OFDM modulation scheme in downlink and SC-FDMA (DFTS-OFDM) in uplink transmissions.

In what follows, we will overview the PHY and MAC layers of LTE, including its downlink/uplink time-frequency resource grid, the uplink/downlink transceiver structure, and the random access procedure.

LTE Downlink Resource Grid: Fig. 8 shows a portion of LTE downlink resource grid for 5 MHz channel bandwidth. The frame is of 10 ms time duration in the time domain and includes ten equally-sized 1 ms subframes. Each subframe consists of two time slots, each composed of seven (or six) OFDM symbols. In the frequency domain, a generic subcarrier spacing is set to 15 KHz. Every 12 consecutive subcarriers (180 KHz) in one time slot are grouped as one physical resource block (PRB). Depending on the channel bandwidth (i.e., FFT size), the frame may have $6 \leq \text{PRB} \leq 110$. The LTE downlink resource grid shown in Fig. 8 carries multiple physical channels and signals for different purposes [87], which we elaborate as follows.

- *Synchronization signals* consist of primary synchronization signal (PSS) and secondary synchronization signal (SSS), both of which are used for UE frame timing synchronization and cell ID detection.
- *Reference signals* (a.k.a. pilot signals) are used for channel estimation and channel equalization. There are 504 predefined reference signal sequences in LTE, each corresponding to a 504 physical-layer cell identity. Different reference signal sequences are used in neighbor cells.
- *Physical downlink shared channel (PDSCH)* is the primary physical downlink channel and is used to carry user data. The main part of the system information, known as system information blocks (SIBs), required for random access procedure is also transmitted using PDSCH.
- *Physical downlink control channel (PDCCH)* is used to transmit downlink control information (DCI), which carries downlink scheduling decisions and power control commands.
- *Physical broadcast channel (PBCH)* carries the system information called master information block (MIB), including downlink transmission's bandwidth, PHICH configuration, and the number of transmit antennas. PBCH is always transmitted within the first 4 OFDM symbols

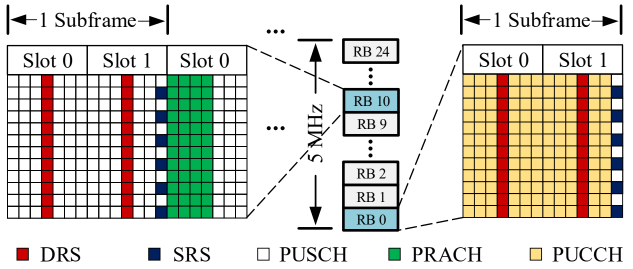


Fig. 9: LTE uplink resource grid.

of the second slot in subframe 0 and mapped to the six resource blocks (i.e., 72 subcarriers) centered around DC subcarrier.

LTE Uplink Resource Grid: To conserve mobile devices' energy consumption, LTE employs single carrier frequency division multiple access (SC-FDMA) for uplink data transmission. Compared to OFDM modulation, SC-FDMA modulation renders a better PAPR performance and provides a better battery lifetime for mobile devices. Fig. 9 shows the resource grid for uplink transmission. Most of the physical transport channels and the signal processing blocks in an LTE transceiver are common for uplink and downlink. In what follows, we focus only on their differences:

- *Demodulation reference signals (DRS)* are used for uplink channel estimation.
- *Sounding reference signals (SRS)* are transmitted for the core network to estimate channel quality for different frequencies in the uplink transmissions.
- *Physical uplink shared channel (PUSCH)* is the primary physical uplink channel used for data transmission and UE-specific higher layer information.
- *Physical uplink control channel (PUCCH)* is used to acknowledge the downlink transmission. It is also used to report the channel state information for downlink channel-dependent transmission and request time and frequency resources required for uplink transmission.
- *Physical random access channel (PRACH)* is used by the UE for the initial radio link access.

LTE Downlink Transceiver Structure: Fig. 10(a) shows the signal processing block diagram used for PDSCH transmission. PDSCH is the main downlink physical channel, which carries user data and system information. The transport block(s) to be transmitted are delivered from the MAC layer. Legacy LTE can support up to two transport blocks in parallel for downlink transmission. For each transport block, the signal processing chain consists of CRC attachment, code block segmentation, channel coding, rate matching, bit-level scrambling, data modulation, antenna mapping, resource block mapping, OFDM modulation, and carrier up-conversion. CRC is attached for error detection in received packets at the receiver side. Code block segmentation segments an over-lengthed code block into small-size fragments matched to the given block sizes defined for Turbo encoder. It is particularly applied when the transmitted code block exceeds 6,144 bits. Turbo coding is used for error correction. Rate matching is applied to select the exact number of bits required for each packet transmission. The scrambled codewords are mapped into corresponding complex symbol blocks. Legacy LTE can support QPSK, 16QAM, 64QAM, and 256QAM, corresponding to two, four, six, and eight bits per symbol, respectively. The modulated codeword(s) are mapped into different predefined antenna port(s) for downlink transmission. Antenna port configuration can be set such that it realizes different multi-antenna schemes, including spatial multiplexing, transmit diversity, or beamforming. Codeword(s) can be transmitted on up to eight antenna ports using spatial multiplexing. For transmit diversity, only one codeword is mapped into two or four antenna ports. The symbols are assigned to the corresponding PDSCH resource units, as illustrated in Fig. 8. The other physical channels and signals are then added to the resource grids. The resource grids on each antenna port are injected through the OFDM modulation and then up-converted to the carrier frequency and transmitted over the air.

Fig. 10(b) shows the signal processing block diagram of a receiver for downlink frame reception. It comprises synchronization, OFDM demodulation, channel estimation and equalization, and data extraction blocks. We elaborate on them as follows.

- *Synchronization:* PSS and SSS are used for detecting the start of a frame and searching for the cell ID. Particularly, the received signal is cross-correlated with PSS to find the PSS and SSS positions. A SSS cross-correlation is later performed to find the cell ID. LTE uses the CP, which is appended to the end of every OFDM symbol, to estimate carrier frequency offset in the time domain.
- *OFDM Demodulation:* OFDM demodulation is performed to transform the received signals from the time domain to the frequency domain, where the resource grid is constructed for further process.
- *Channel Estimation:* Channel estimation is performed by leveraging the reference signals embedded in the resource grid. Specifically, it is done by the following three steps: i) the received reference signals are extracted from the received resource grid; ii) least square or other method is used to estimate the channel frequency responses at the reference positions in the resource grid; and iii) the estimated channels are interpolated using an averaging window, which can apply to the time domain, the frequency domain, or both of the resource grid.
- *Channel equalization:* The estimated channel is used to equalize the received packet. Minimum mean square error (MMSE) or zero-forcing (ZF) are the most two equalizers used in cellular systems. For the MMSE equalizer, it is also required to take the noise power into account as well. The noise power is estimated by calculating the variance between original and interpolated channel coefficients on the pilot subcarriers. Compared to the MMSE equalizer, the ZF equalizer does not require the knowledge of noise power. It tends to offer the same performance as MMSE equalizer in the high SNR scenario.

PDSCH is extracted from the received resource grid and demodulated into bits. The received bits are then fed into the

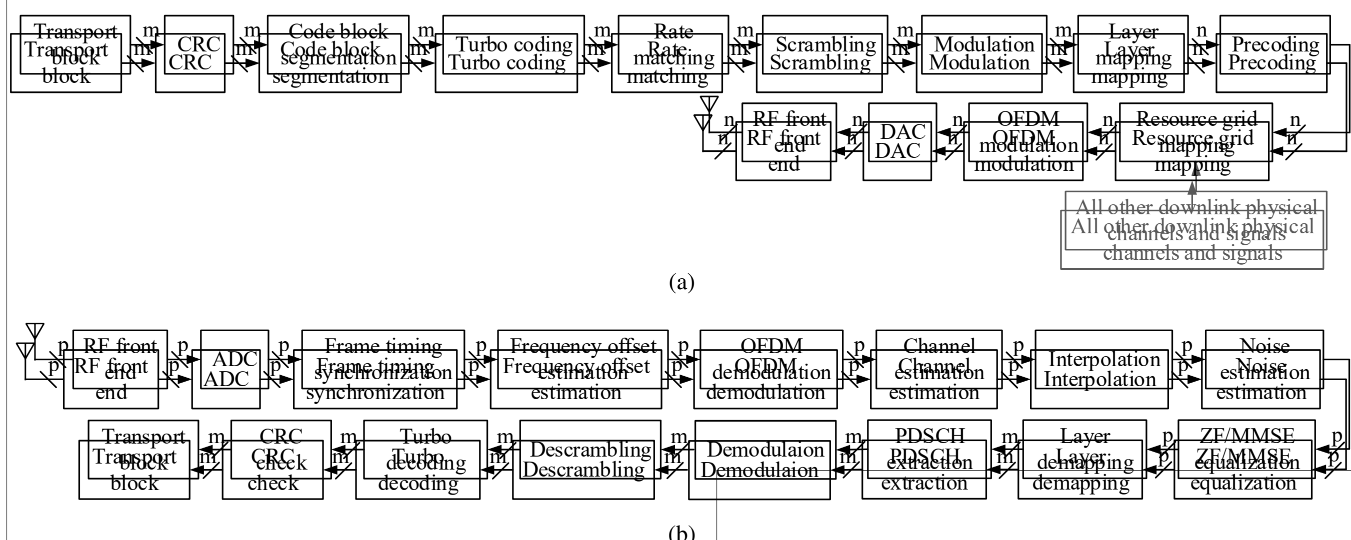


Fig. 10: (a) The schematic diagram of downlink LTE PDSCH signal processing. (b) The schematic diagram of a LTE receiver to decode PDSCH signal, where $n \leq 8$, $m \leq 2$, and $p \leq 4$.

reverse process of PDSCH in order to recover the transport data.

M=2, n= 8, p=4
M=2, n= 8, p=4

LTE Uplink Transceiver Structure: In the uplink, the scrambled codewords are mapped into QPSK, 16QAM, or 64QAM modulated blocks. The block symbols are divided into sets of M modulated symbols, where each set is fed into DFT operation with the length of M. Finally, physical channels and reference signals are mapped into resource blocks, as illustrated in Fig. 9, and fed into the OFDM modulator. The uplink receiver structure is similar to that of PDSCH decoding in the downlink except that the frequency and symbol synchronizations to the cell and frame timing of the cell are performed in the cell search procedure.

LTE Random Access Process: Before an LTE user can initiate the random access procedure with the network, it has to synchronize with a cell in the network and successfully receive and decode the cell system information. LTE users can acquire the cell's frame timing and determine the cell ID using PSS and SSS synchronization signals transmitted within the downlink resource grid, as illustrated in Fig. 8. PDSCH and PBCH carry system information in the downlink resource grid. Once the system information is successfully decoded, the user can communicate with the network throughout the random access procedure. The basic steps in the random access procedure have been illustrated in Fig. 11. In the first step, the LTE user transmits the random access preamble (i.e., PRACH in uplink resource grid as illustrated in Fig. 9) for uplink synchronization. It allows the eNodeB to estimate the transmission timing of the user. In the second step, the eNodeB responds to the preamble transmission by issuing an advanced timing command to adjust uplink timing transmission based on the delay estimated in the first step. Moreover, the uplink resources required for the user in the third step are provided in this step. In the third step, the user transmits the mobile-terminal identity to the network using the UL-SCH resources assigned in the second step. In the fourth and final step, the network transmits a contention-resolution message to the user using DL-SCH.

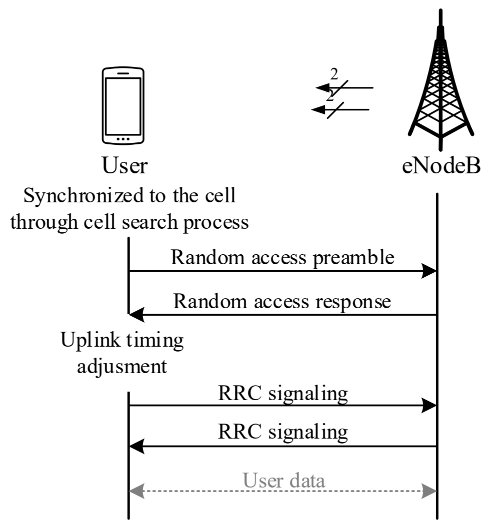


Fig. 11: Illustration of random access process in cellular networks.

B. Jamming Attacks

With the above knowledge of LTE networks, this section dives into the review of malicious jamming attacks in cellular networks. A jammer may attempt to disrupt cellular wireless communications either using generic jamming attacks (see Section II-B) or using cellular-specific jamming attack strategies.

In [89], Romero et al. studied the performance of LTE uplink transmission under a commercial frequency-sweeping jamming attack. The authors conducted experiments to evaluate the sensitivity of uplink reference signal when the jammer sweeps the 20 MHz channel within T microseconds, where

$T \in [1,\ 200]$. The EVM of uplink demodulation reference signal was measured at the receiver and used as the performance metric. The experimental results show that, for a given signal-to-jamming ratio (SJR), a jammer with $T \in [20,\ 40]$ is least destructive (yielding highest EVM), while a jammer with $T \in [160,\ 200]$ is most destructive (yielding lowest EVM).

In [90] and [91], Zorn et al. proposed an intelligent jamming attack for WCDMA cellular networks, with the aim of forcing a victim user to switch from WCDMA to GSM service. To do so, the jammer sends interfering signal to degrade the SNR of WCDMA cell primary common pilots. The authors argued that, if the SNR of WCDMA CPCPCH is below a certain threshold, the user will leave the WCDMA to use GSM service. Through experiments, the authors show that 37 dBm jamming power is sufficient to force a user leave WCDMA to join GSM service.

As we discussed earlier in section III-A, the PHY layer of LTE is made up of several physical signals and channels that carry specific information throughout the downlink and uplink resource grids to provide reliable and interference-free communications between eNodeB and users within a cell. In what follows, we focus on cellular-specific jamming attacks that target on PHY-layer downlink/uplink signaling and channels of cellular networks.

1) Jamming Attacks on Synchronization: In cellular networks, synchronization signals, PSS and SSS, are critical for the cell search process, through which a user can obtain the frequency synchronization to a cell, the frame timing of the cell, and the physical identity of the cell. An LTE user must perform a cell search before initializing the random access procedure, and the cell search is also performed for cell reselection and handover. In FDD LTE networks, synchronization signals are transmitted within the last two OFDM symbols of the first time slot of subframe 0 and subframe 5, as illustrated in Fig. 8. Once a user decodes PSS, it will find the cell's timing, the two positions of SSS, and partial information of cell identity. Then, SSS is used to acquire frame timing (start of packet) and determine cell identity. Once cell identity is obtained, the user becomes aware of the reference signals and their positions within the resource grid used in downlink transmission. This information allows the user to perform channel estimation and extract the system information by decoding PBCH and PDSCH.

Clearly, the synchronization process is critical in cellular networks. If a user fails to detect the synchronization signals, it cannot conduct the cell search process and cannot access it. The synchronization process is, however, vulnerable to jamming attacks. In [92], Krenz et al. studied jamming attack on synchronization signals and PBCH. The authors studied the LTE network under such jamming attacks where the jammer interferes with the bandwidth portions occupied by synchronization signals.

2) Jamming Attacks on PDCCH and PUCCH: PDCCH and PUCCH are critical control channels in cellular networks, and their vulnerability to jamming attacks have been investigated. In [93], Aziz et al. considered PDCCH and PUCCH as potential physical channels that a smart jammer may target to interrupt since they carry critical control information on downlink and uplink resource allocations. Before a jammer can attack the PDCCH, it requires to decode the physical control format indicator channel (PCFICH) that determines the position of the PDCCH resource elements within the downlink frame. In [94], Kakar et al. studied PCFICH jamming attacks. Control format indicator (CFI) is a two-digit binary data encoded into 32 bits codeword and modulated into 16 QPSK symbols and mapped into 16 sparse resource elements within the downlink resource grid. It was argued in [94] that the jamming attack on PCFICH is an efficient and effective jamming strategy in LTE networks because PCFICH occupies only a small fraction of the downlink resource grid and carries vital information on PDCCH resource allocations. That means the user will no longer be able to decode the PDCCH and suffer from a denial of service when jamming the PCFICH. In [95], Lichtman et al. analyzed the physical uplink control channel (PUCCH) vulnerabilities against jamming attacks. The authors argued that a jammer could simply attack PUCCH only by learning the LTE channel bandwidth since PUCCH is transmitted on the uplink resource grid's edge. That means the PUCCH highly susceptible to jamming attacks as their locations within the resource grid is fix and predictable for a malicious attacker.

3) Jamming Attacks on PDSCH and PUSCH: PDSCH and PUSCH carry user data and upper-layer network information and dominate the major available resources in downlink and uplink transmissions, respectively. In [96], Litchman et al. investigated the vulnerability of PDSCH and PUSCH under jamming attacks. However, the jamming attacks on PDSCH and PUSCH require the synchronization to the cell and a prior knowledge of control information and cell ID. In [97], Girke et al. implemented a PUSCH jamming attack using srsLTE testbed for a smart grid infrastructure and evaluated uplink throughput for different jamming gains. The results in [97] show that the total number of received packets reduces approximately by 90% under jamming signal 35 dB stronger than PUSCH signal.

4) Jamming Attacks on PBCH: PBCH is used to carry MIB information in downlink required for LTE users to initial random access process. MIB conveys the information on downlink cell bandwidth, PHICH configuration, and system frame number (SFN) required at the user side for packet reception and data extraction. PBCH is transmitted only within the first subframe and mapped to the central 72 subcarriers regardless of channel bandwidth. In [96] and [98], PBCH jamming attack was introduced as an effective and efficient adversary attack to the LTE PHY-layer communications. This is because the PBCH carries essential system information for the user and occupies a limited portion of the resource elements (i.e., $< 0.7\%$) in the downlink resource grid [99]. PBCH jamming attack prevents LTE users from performing their random access process. This may lead LTE users to switch to neighbor cells [99]. In [92], Krenz et al. evaluated the network's performance under the PBCH jamming attack using a real-world system implementation. Their experimental results show that the LTE communications can be blocked when the jamming signal is 3 dB stronger than the desired signal at LTE receivers.

5) Jamming Attacks on PHICH: Physical hybrid automatic repeat request (ARQ) indicator channel (PHICH) is used to carry hybrid-ARQ ACKs and NACKs in response to PUSCH transmissions. The hybrid-ARQ acknowledgment is a single bit of information (i.e.,'1' stands for ACK and '0' stands for NACK). The bit is further repeated three times, modulated by BPSK, and spread with an orthogonal sequence to minimize the error probability of the acknowledgment detection. PHICH occupies a small portion of the downlink resource grid (e.g., $\leq 0.3\%$ in 10 MHz channel bandwidth). In [96], Lichtman et al. introduced a jamming attack on PHICH, where a jammer attacks the logic of ACK/NACK bit in order to degrade the network performance by wasting the resources for false retransmission requests.

6) Jamming Attacks on Reference Signal: Reference signals are transmitted within the frame for channel estimation purposes. Downlink reference signals (pilots) are generated using a pseudo-random sequence in the frequency domain, followed by a quadrature phase shift keying (QPSK) modulation scheme. The reference signals in the LTE downlink resource grid are transmitted on a subset of predefined subcarriers. The estimated channel responses for the subcarriers carrying reference signals are later interpolated for the entire bandwidth.

In [93], [96], [98], the authors introduced potential jamming attack on cell-specific reference signals. The LTE user under reference signals jamming attack will fail to demodulate the physical downlink channels transmitted within the downlink resource grid. Moreover, it will lose its initial synchronization to the cell and fail to perform the handover process [93]. However, a jamming attack on reference signals requires prior knowledge of the cell identity to determine the resource grid's reference signals' position.

In [58], Clancy et al. proposed a reference signal nulling attack (a.k.a. pilot nulling attack). This attack attempts to force the received energy at the pilot OFDM samples (i.e., reference signal resource elements) to zero, thereby disabling channel estimation capability at cellular networks. In [60] and [61], Sodagari et al. studied pilot jamming attack in MIMO-OFDM communications, where their main goal is to design jamming signal so that the estimated channel matrix at a cellular receiver is rank-deficient and, as a result, the channel matrix will no longer be invertible. This prevents the cellular receiver from correctly equalizing the received resource grid.

7) Jamming Attacks on Random Access: An LTE user can establish a radio connection to a cellular base station by using a random access procedure, provided that it correctly performs cell search as explained in Section III-A. In [100]–[102], jamming attacks on PRACH were introduced as one of the critical PHY-layer vulnerabilities in LTE networks. The jamming attacks on random access channels will cause DoS by preventing LTE users from connecting to the network or reestablishing the link in a handover process. However, neither theoretical analysis nor experimental measurements were presented for PRACH jamming attacks.

8) Jamming Attacks on 5G New Radio: 5G is the latest 3GPP radio access technology designed to improve the cellular network performances in terms of data rate, latency, link reliability, availability, connectivity, and user experiences. Per [103], 5G targets $10\times$ to $100\times$ higher user throughput, $10\times$ to $100\times$ more connected devices, lower power consumption for machine type connections, and lower latency (e.g., < 5 ms) when comparing to LTE and LTE-advanced. In the PHY layer, 5G new radio (NR) and LTE share many similarities, such as downlink and uplink transmission schemes, DL-SCH processing, frame length, etc. They, however, differ in details. In the following, we first highlight the main differences between NR and LTE in their PHY and then survey the jamming attacks on 5G systems.

- **Operating Bandwidth:** NR can operate in frequency bands below 6 GHz and above 24 GHz (i.e., mmWave). In sub-6 GHz frequency bands, it supports channel bandwidth of up to 900 MHz (band n77), while in legacy LTE, the channel bandwidth is limited to 20 MHz. In mmWave frequency bands, it supports up to 3250 MHz channel bandwidth (band n258).
- **Downlink Subcarrier Spacing:** Both LTE and 5G NR use OFDM modulation for their downlink communications. However, the subcarrier spacing in LTE is fixed to 15 kHz, while 5G NR supports subcarrier spacing of 15 kHz, 30 kHz, 60 kHz, 120 kHz, and 240 kHz. It may use higher subcarrier spacing values (e.g., 120 kHz) for wider channel bandwidths (e.g., mmWave communications) in order to increase the link robustness.
- **Slot Format:** In 5G NR, uplink and downlink resources are assigned at an OFDM symbol level. On the contrary, in LTE, uplink and downlink transmissions occur at the subframe level in TDD mode. 256 slot formats have been defined for 5G NR that specify the transmission patterns for uplink and/or downlink communications within a single time slot (i.e., 14 OFDM symbols with normal CP). This delivers higher flexibility in resource allocation for 5G NR compared to LTE TDD configurations. It, however, requires highly tight timing requirements as it may switch between downlink and uplink transmissions in an OFDM symbol duration (i.e., < 100 μs).
- **Reference Signals:** Three types of reference signals have been defined for 5G NR in its downlink communications: Demodulation reference signal (DM-RS), channel state information reference signal (CSI-RS), and phase tracking reference signal (PT-RS). DM-RSs are used for coherent demodulation of PDSCH, PCCH, and PBCH data. A cellular UE uses CSI-RS to estimate the downlink channel and report the results to the gNodeB (5G BS). PT-RSs can be used to compensate the impact of phase noise in decoding the PDSCH.
- **Synchronization signal block (SSB):** Unlike LTE downlink frame format, where synchronization signals (PSS and SSS) and PBCH are always sent over fixed resource blocks within the resource grid, in 5G NR frame format, synchronization signals and PBCH are wrapped altogether as an SSB block and will be transmitted in diverse patterns depending on the subcarrier spacing, channel bandwidth, and some other system configuration settings.

An overview of jamming attacks on 5G communications

TABLE V: A summary of jamming attacks in cellular networks.

Attacks	Ref.	Mechanism	Strength	Weakness
Generic jamming attacks	[89]	Frequency-sweeping jamming attack	Easy to implement High effective	Energy-inefficient Less stealthy
WCDMA CPCPCH jamming attacks	[90], [91]	Forcing a user to leave WCDMA RAN and switch to GSM by interfering the CPCPCH signal	Energy-efficient High stealthy	Cell synchronization required Less effective
Synchronization signals jamming attacks	[92], [99]	PSS and SSS corruption jamming attack	Energy-efficient High effective High stealthy	Tight timing constraint
PDCCH/PUCCH jamming attacks	[93]	Downlink control information (DCI) jamming attack	Energy-efficient High effective High stealthy	Cell synchronization required
	[94]	Control format indicator (CFI) jamming attack		
	[95], [99]	Uplink control channel attack		
PDSCH/PUSCH jamming attacks	[96], [97], [99]	User data corruption jamming attack System information block (SIB) jamming attack	High effective	Energy-inefficient Cell synchronization required
PBCH jamming attacks	[92], [96], [98], [99]	Master information block (MIB) jamming attack	Energy-efficient High effective High stealthy	Cell synchronization required
PHICH jamming attacks	[96]	Hybrid-ARQ acknowledgement bit jamming attack	High energy-efficient High effective High stealthy	Cell synchronization required
Reference signal jamming attacks	[93], [96], [98], [99]	Reference signal jamming attack	Energy-efficient High Effective High stealthy	Cell synchronization required
	[58]	Reference signal nulling attack		
	[60], [61]	Singularity jamming attack in MIMO-OFDM communications		
Random access attacks	[100]–[102]	PRACH, handover and link re-establishing jamming attack	Energy-efficient High Effective High stealthy	Cell synchronization required
5G learning-based applications jamming attacks	[104]	Jamming attack on environmental sensing capability	Energy-efficient High stealthy	Hard to implement in practice Hardware constraints Training phase required
	[105]	Adversarial attack on mmWave beam pattern prediction		
	[106]	Jamming attack on network slicing capability		

was presented in [101] and [99]. The authors studied the vulnerability of the NR physical layer to jamming attacks. Similar to LTE, it was shown that the NR physical channels and signals could be targeted by network-specific jamming attacks. In particular, the authors studied jamming attacks on PSS, SSS, PBCH, PDCCH/PUCCH, PDSCH/PUSCH, PRACH, and reference signals. Per [99], jamming attacks on PSS/SSS can be conducted in a similar way as for LTE, as discussed in Section III-B1. To implement jamming attacks on NR synchronization signals, the jammer will, however, require more information regarding the system settings, such as the subcarrier spacing value and *offset-ref-low-scs-ref-PRB* parameter to identify the location of the PSS/SSS in the frame.

As discussed in Section III-B4, jamming attack on PBCH is regarded as a serious security threat to LTE/5G networks, because PBCH carries critical information of the cell, called MIB. A cellular UE under PBCH jamming attack cannot acquire MIB information and cannot complete the cell search process, thereby suffering from service denial. Unlike LTE, where the PBCH is always mapped to the 72 subcarriers centered around DC and sent within the first 4 OFDM symbols of the second slot in subframe 0, the PBCH in 5G NR occupies 240 subcarriers and is sent over 24 OFDM symbols for the frequency bands above 3 GHz and below 6 GHz. Per [99], a jammer can constantly interrupt the 5G PBCH channel subcarriers and prevent UEs to access the cell by only jamming $\frac{240}{1272} \times 100 = 19\%$ of the total downlink resources when the signal bandwidth and subcarrier spacing are set to 20 MHz and 15 kHz, respectively.

The authors in [99] also studied the possibilities of jamming attacks on PDCCH. Per [99], in order to disrupt the PDCCH in 5G NR communications, the jammer needs to have prior knowledge of the *CORESET-freq-dom* and *CORESET-time-dur* parameters, indicating the PDCCH subcarrier indices and its number of occupied OFDM symbols within the NR resource grid, respectively. The authors also investigated jamming attacks on 5G reference signals. They argued that the jamming attack on PBCH DM-RS is a highly effective and efficient jamming strategy as PBCH DM-RS occupies 25% of the PBCH resources and can be targeted to block any 5G UE communications. Similar to jamming attacks on LTE networks, the authors introduced the jamming attacks on 5G PDSCH/PUSCH as low-complex and ineffective jamming strategies since they occupy the major portion of the resource grids and require a high duty cycle for the jammer to block them.

In [107], Sheikhi et al. studied the impact of power-optimized jamming attacks on the spectral efficiency of both FDD and TDD massive MIMO systems. The jammer uses the reciprocity between uplink and downlink channels in TDD mode and turns the estimated channels in the uplink to optimize its jamming attack strategy in the downlink. While in the FDD mode, the jammer uses the second-order statistics of the channels to design the jamming signal. The numerical results showed that TDD mode is more vulnerable to smart jamming attacks compared to the FDD mode.

Recently, the PHY-layer vulnerability of 5G cellular networks has been studied for learning-based applications [104]–[106]. In [104], Sagduyu et al. introduced an adversarial attack to fool the deep learning model built for dynamic spectrum sharing in 5G networks. The proposed scheme attacks the environmental sensing capability (ESC) of 5G by sending well-designed jamming signals during the sensing or data transmission phases, aiming to manipulate the ESC classifier input. In [105], Kim et al. designed a malicious attack against learning-based beam pattern prediction for 5G mmWave networks. The beam pattern prediction scheme leverages the measured RSSIs and trains a deep neural network to enhance the robustness and latency of the beam selection process. In the proposed scheme, a jammer adds a perturbation to the neural network input so that the legitimate 5G user fails to classify beam patterns. The authors further developed the proposed scheme and designed a perturbation that forces the neural network to choose the worst beam pattern. In [106], Shi et al. investigated the vulnerability of learning-based network slicing in 5G networks. In the proposed scheme, a power-constrained jammer constructs a reinforcement learning-based model by monitoring the channels and attacks the PRBs to maximize the number of disrupted network slicing requests. The simulation results in [104]–[106] showed that, while machine learning holds great potential to improve the reliability and efficiency of 5G networks, it is highly susceptible to adversarial attacks. This vulnerability can be easily leveraged to degrade 5G performance.

9) A Summary of Jamming Attacks: Table V presents a summary of jamming attacks that were delicately designed for cellular networks. We note that those generic jamming attacks (e.g., constant jamming, reactive jamming, deceptive jamming, and random jamming) are not included in this table to avoid redundancy. Most of the jamming attacks in Table V target on the control signaling in cellular communications. These jamming attacks typically require fine-grained timing synchronization so that the specific control signaling can be interfered. Since the synchronization signal in cellular network is periodically broadcasting, it is easy for malicious attackers to acquire the timing information. Therefore, such signaling-specific jamming attacks pose a serious threat to cellular networks.

C. Anti-Jamming Techniques

In the presence of security threats from existing and potential jamming attacks, researchers have been studying anti-jamming strategies to thwart jamming threats and secure cellular wireless services. In what follows, we survey existing anti-jamming strategies and present a table to summarize the state-of-the-art jamming defense mechanisms.

1) MIMO-based Jamming Mitigation Techniques: The anti-jamming strategies, such as the ones originally designed for WLANs in [46], [47], [76], [77], can also be applied to secure wireless communications in cellular networks. The interference cancellation capability of MIMO communications can be enhanced when the number of antennas installed on the devices tends to be large (i.e., massive MIMO technology). However, massive MIMO is very likely deployed in cellular base stations (eNodeB) as it requires a high power budget and a large space to accommodate massive number of antennas. Therefore, massive MIMO techniques are exploited to mitigate jamming attacks in the cellular uplink transmissions.

In [108], a massive MIMO jamming-resilient receiver was designed to combat constant broadband jamming signal in the uplink transmission of cellular networks. The basic idea behind their design is to reserve a portion of pilots in a frame so that these unused pilots can be leveraged to estimate the jammer's channel. At the same time, a legitimate user can also estimate its desired channel in the presence of jamming signal. This can be done using the pilots in a frame based on the large number law originated from the massive number of antennas on BS. With the estimated channel information, a linear spatial filter can be designed at the BS to mitigate the jamming signal and recover the legitimate signal.

In [109], Vinogradova et al. proposed to use the received signal projection onto the estimated signal subspace to nullify the jamming signal. The main challenge in this technique is to find the correct user's signal subspace. The eigenvector corresponding to the legitimate user eigenvalue in eigenvalue decomposition of the received covariance matrix can be used for signal projection. It is known that the user's eigenvalues can be expressed as its transmitted power when the legitimate user's and jammer's power are distinct. In this case, the eigenvalues corresponding to the legitimate users can be selected by an exhaustive search over all the calculated eigenvalues.

In [110], Akhlaghpasand et al. proposed a method for detecting the presence of the jammer in massive MIMO systems. Their proposed scheme relies on the unused pilots in the training phase and assumes that the jammer does not have prior knowledge of the pilot patterns. The base station can detect the existence of a jammer by examining the received signal on these empty or unused pilots in the uplink transmissions. This is done through a generalized likelihood ratio test over some coherence blocks. The authors evaluated the accuracy of their method and studied the impact of the number of unused pilots and the number of antennas at the base station on its performance.

A similar idea was proposed in [111] for jamming detection and suppression in massive MIMO systems. In this scheme, the authors proposed to estimate the jammer's channel by exploiting the received signals within the unused pilots and designed a minimum mean-squared error-based jamming suppression (MMSE-JS) estimator to estimate the users' channels in the presence of the jamming signal. Then, the authors exploit the estimated users and jammer's channels and design a linear zero-forcing jamming suppression (ZFJS) filter to cancel the jamming signal and recover the desired signal. The simulation results demonstrated that their proposed scheme could secure the massive MIMO system against 30 dB stronger jamming attacks.

In [112], the authors studied jamming protection of massive MIMO systems in spatially correlated channels. The authors proposed a framework consisting of a linear estimator in the channel training phase and a bilinear equalizer in the data phase. The authors also considered the hardware impairments in their design and evaluated the performance of their scheme in terms of spectral efficiency. Their simulation results demonstrated that the performance degradation is less than 1 b/s/Hz when the received jammer's power sweeps from -20 dB to 20 dB.

2) Spectrum Spreading Techniques: Spectrum spreading is a classic anti-jamming technique, which has been used in 3G CDMA, WCDMA, TDS-CDMA cellular systems. It is particularly effective in coping with narrowband jamming signals. At the PHY layer of WCDMA communications, the bit-streams are spread using orthogonal channelization codes called orthogonal variable spreading factor (OVSF) codes. The length of OVSF codes are determined by a spreading factor (SF) that varies in the range from 4 to 512 for downlink and from 4 to 256 for uplink. The chip rate of WCDMA communications is 3.84 Mcps, and the bit rate can be adjusted by selecting different SF values.

In [113], Pinola et al. studied the performance of WCDMA PHY layer under broadband jamming attacks by conducting experimental measurements. The authors reported the results for different services provided by WCDMA. For the uplink services, the acceptable quality can be achieved when SJR ≥ -22 dB for voice service, SJR ≥ -13 dB for text message service, and SJR ≥ -16 dB for data service with SF $= 32$ (i.e., 64 kbps data rate). For the downlink services, the acceptable quality can be achieved when SJR ≥ -26 dB for voice service, SJR ≥ -14 dB for text message service, and SJR ≥ -18 dB for data service with SF $= 32$.

3) Multiple Base Stations Schemes: In addition to MIMO-based jamming mitigation, another approach for coping with jamming attacks in cellular networks is rerouteing the traffic using alternative eNodeB. When current serving eNodeB is under jamming attacks and out of service, a user can re-connect to another eNodeB if available [114]. This mechanism has already been used in LTE networks. When a user fails to decode the MIB of its current serving eNodeB, it will search for the strongest neighboring eNodeB for a new connection [87].

4) Coding and Scrambling Techniques: Coding and scrambling techniques have also been used to protect wireless communications against jamming attacks in cellular networks. In [115], Jover et al. focus on the security enhancement for the physical channels of LTE networks, including PBCH, PUCCH, and PDCCH. These physical channels carry crucial information and must be well protected against malicious jamming adversary. To protect the information in these physical channels, the authors proposed using spectrum spreading for PBCH modulation, scrambling the PRB allocation for PUCCH transmissions, and distributed encryption scheme for PDCCH coding.

5) Dynamic Resource Allocation Schemes: The static resource allocation for the physical channel such as PUCCH is regarded as the main vulnerability of the LTE framework that can be used by a malicious attacker to interrupt the legitimate transmissions, thereby causing DoS to the network. The PUCCH is transmitted on the edges of the system bandwidth, as illustrated in Fig. 9. It carries HARQ acknowledgments in response to PDSCH transmissions. When the acknowledgment signals cannot be correctly decoded, the eNodeB will need to retransmit the downlink data packets, thereby imposing traffic congestion on the network and wasting the resources. In [95], Lichtman et al. studied the vulnerability of PUCCH and proposed a dynamic resource allocation scheme for PUCCH transmission by incorporating a jamming detection mechanism. In the jamming detection process, the energy of the received PUCCH signal is continuously monitored and compared with the signal strength of other physical channels to identify any unexpected received energy behavior. Moreover, the number of consecutive errors on PUCCH decoding is tracked to detect the jamming attack on PUCCH. The key idea of the proposed dynamic resource allocation scheme is to assign pseudo-random resource elements or a diverse combination of resource blocks for PUCCH transmissions in the uplink frame.

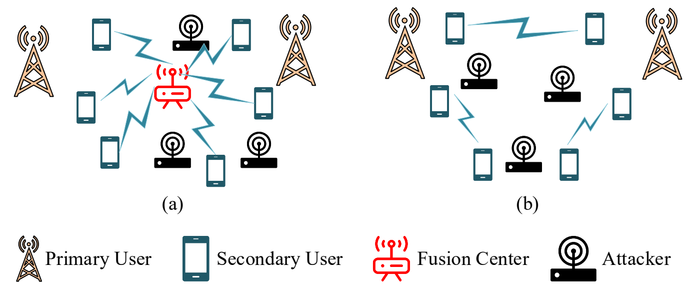


Fig. 12: (a) Security attack in a cooperative sensing cognitive radio network, (b) Security attack in a non-centralized cognitive radio network.

6) Jamming Detection Mechanisms: In [116], Arjoune et al. studied the performance of existing machine learning methods in jamming detection for 5G communications. Particularly, the authors evaluated the accuracy of neural networks, super vector machine (SVM), and random forest algorithms. They generated the database using packet error rate, packet delivery ratio, and the received signal strength features. The simulation results show that the random forest algorithms achieve higher accuracy (95.7%) in jamming detection compared to other algorithms.

7) A Summary of Anti-Jamming Techniques: To ease the reading, we summarize existing cellular-specific anti-jamming techniques as well as their mechanisms in Table VI. Since 4G/5G have a stringent requirement on spectrum efficiency and OFDM modulation has been used for their data transmissions, anti-jamming techniques such as spectrum spreading are not suited for cellular applications. MIMO-based anti-jamming techniques become increasing popular as a base station typically has many antennas. In addition, MIMO-based jamming mitigation techniques have the potential to cope with jamming attacks on signaling-specific jamming attacks and secure cellular communications by design. The introduction of massive MIMO in 4G/5G has also fueled the research and development of MIMO-based anti-jamming techniques in cellular networks.

IV. Jamming and Anti-Jamming Attacks in Cognitive Radio Networks (CRNs)

In this section, we survey the jamming and anti-jamming strategies in cognitive radio networks. Following the previous section structure, we first provide an introduction of CRN and then review the jamming and anti-jamming attacks in literature. Fig. 12 describes a general scheme of security attacks on centralized and distributed CRNs.

A. Background

Cognitive radio network (CRN) is a technique proposed to alleviate the spectrum shortage problem by enabling unlicensed users to coexist with incumbent users in licensed

TABLE VI: A summary of anti-jamming techniques for cellular networks.

Anti-jamming technique	Ref.	Mechanism	Application scenario
Massive MIMO techniques	[108]	Jammer's channel estimation, Spatial linear filter design for jamming suppresion	Constant jamming attack
	[109]	Jamming signal nullification using signal projection techniques	Constant jamming attack
	[110]	Detecting jamming attacks using unused pilot	Constant jamming attack
	[111]	MMSE-JS estimator for jammer's channel estimation ZFJS filter design for jamming cancellation	Constant jamming attack
	[112]	Linear estimator for channel estimation in training phase Bi-linear equalizer in the data phase	Constant jamming attack
Spectrum spreading techniques	[113]	Evaluating of WCDMA-based cellular RAN against jamming attacks	Constant jamming attack
Alternative eNodeB	[114]	Rerouting the user's traffic via alternative eNodeBs	DoS jamming attacks
Coding techniques	[115]	Spread spectrum for PBCH modulation, scrambling of PRB allocation for PUCCH transmissions distributed encryption scheme for PDCCH coding	PBCH and PDCCH/PUCCH jamming attack
Dynamic resource allocation	[95]	Dynamic resource allocation for PUCCH transmissions	PUCCH jamming attack
Jamming detection mechanisms	[116]	Machine learning algorithms using PER, RSS, and PDR features	Constant jamming attack

spectrum bands without inducing interference to incumbent communications. Thus, a CRN has two types of users: primary users (PUs), which are also known as licensed users or incumbent users, and secondary users (SUs), which are also known as unlicensed users or cognitive users. In order to realize spectrum access for cognitive users, spectrum sensing plays a crucial role. Cooperative spectrum sensing (CSS) refers to combining the sensing results reported from multiple secondary users (SUs) and coming up with a near-optimal carrier sensing output to improve the spectrum utilization.

The main components in CSS are signal detection, hypothesis testing, and data fusion [117]. Signal detection in CSS is independently carried out by active SUs to sense the medium and record the raw information on possible PU activities. Signal detection can be implemented using matched filtering, energy detection, or feature detection techniques. While matched filtering and feature techniques use PU's signal shaping and packet format to detect the presence of its transmissions, the energy detection method does not need to have prior knowledge of the PU's protocols, making it easy to implement. However, the energy detection method will not be able to differentiate between the PU's transmitted signal and unknown noise and interference sources, resulting in a decrease of the sensing accuracy [118]. After signal detection, each user uses hypothesis analysis to reach to a binary decision whether the medium is busy or not. The hypothesis analysis can be performed using the Bayesian test, the Neyman-Pearson test, and the sequence probability ratio test [119]. Once individual SUs have made their decisions, data fusion is performed by leveraging the reports received from the SUs to turn them into a solid output. Data fusion can be done centralized or decentralized, corresponding to the network setting.

In centralized CCS, each SU's detection results are transmitted to a common control entity known as fusion center (FC). The FC performs the data fusion processing and broadcasts the final results to all the SUs collaborated in the sensing phase. Unlike centralized fusion, which relies on a fusion center to collect the data and make the fusion, for decentralized fusion in cognitive radio ad-hoc networks (CRAHN), no dedicated central entity exists to perform data fusion, and instead, each sensor exchanges its sensing output with its neighbors and iteratively fuses the sensing outputs from its neighbors [34].

B. Jamming Attacks

In what follows, we survey the jamming attacks uniquely designed for CRNs.

1) Jamming Attacks on Secondary Network and Common Control Channel: The common control channel is a medium through which the secondary nodes share their channel sensing reports. Common control channel attack refers to the overwhelming secondary network common control channel by fake MAC control frames. The attacker network launches the common control channel attack in order to cause denial of service to the secondary network. In [129], Bian et al. argued that the common control channel attack benefits from the following two features: First, it is hard to be detected as it injects the MAC control frames identical to the secondary networks' protocols. Second, it is an energy-efficient attack as it requires to send a small number of control packets to saturate the common control channel.

2) Learning-based Jamming Attacks: In [130], the authors proposed a deep learning-based jamming attack on cognitive radio networks. The proposed scheme takes advantage of users' ACK reports to train a deep learning classifier to predict whether an ACK transmission would occur through the medium. The performance of the proposed jamming attack was compared with a random jamming attack and a sensing-based reactive jamming attack. The simulation results show that the proposed deep-learning jamming attack could degrade the network's throughput to 0.05 packet/slot. As a comparison, the authors also show that the network's throughput is 0.38 packet/slot under the random jamming attack and 0.14 packet/slot under the sensing-based jamming attack.

C. Anti-Jamming Techniques

Generally speaking, the anti-jamming strategies presented in Section II-C (e.g., MIMO-based jamming mitigation) can also be applied to thwarting jamming attacks in CRNs. In what follows, we elaborate on the anti-jamming strategies uniquely designed for CRNs.

Per [121], [131], [132], game-theoretical modeling is a well-known technique used in CRNs to express the interaction among different parties contributing to the network. Particularly, the stochastic zero-sum game is widely adopted to model the interaction between secondary users and adversary jamming attackers since they have opposite objectives.

TABLE VII: A summary of anti-jamming techniques for CRNs.

	Ref.	Description	Application scenario
Anti-jamming techniques	[120]	Tri-CH; an anti-jamming channel hopping algorithm	Static, random, adaptive jamming attacks
	[121]	Zero-sum game modeling, channel hopping using Markov decision process	Smart reactive jamming attack
	[122]	JRCC game modeling; Cooperation for control channel allocation and adaptive rate learning for primary users.	Multi-band reactive jamming attack
	[123]	stochastic game modeling and minimax Q learning method for primary user strategy selection	Multi-band reactive jamming attack
	[124]	JENNA; Random channel hopping and network coding for control packets sharing	Reactive jamming attack
	[125]	Non-cooperative zero-sum game modeling and optimal pwoer allocation	Smart jamming attack
	[126]	Bayesian game modeling under packet traffic uncertainties	Reactive jamming attack
	[127]	Non-cooperative game framework under dynamic data traffic constraints	Energy-constrained reactive jamming attack
	[128]	Prospect theory analysis under players' future actions and channel gains uncertainties	Smart jamming attack

In [131], Li et al. proposed that secondary users randomly hop over the multiple channels to countermeasure PUE jamming attacks. For the secondary network, each user needs to search the optimal tradeoff between choosing good channels and avoiding jamming signals. In [120], Chang et al. introduced Tri-CH, an anti-jamming channel hopping algorithm for cognitive radio networks. In [121], the interaction between the secondary network and attackers is formulated as a zero-sum game, and a channel-hopping defense strategy is proposed using the Markov decision process.

In [122], Lo et al. proposed JRCC, a jamming resilient control channel game that models the strategies chosen by cognitive users and an attacker under the impact of primary user activity. JRCC uses user cooperation for control channel allocation and adaptive rate learning for primary user using the Win-or-Learn-Fast scheme. The optimal control channel allocation strategy for secondary users is derived using multiagent reinforcement learning (MARL).

In [123], a game-theoretical approach is picked up to model the cognitive radio users' interactions in the presence of a jamming attack. Secondary users at each stage update their strategies by observing the channel quality and availability and the attackers' strategy from the status of jammed channels. The strategies defined for cognitive users consider the number of channels they can reserve to transmit control and data messages and how they can switch between the different channels. A minimax-Q learning method is used to find the optimal anti-jamming channel selection strategy for cognitive users.

In [124], Asterjadhi et al. proposed a Jamming Evasive Network-coding Neighbor-discovery Algorithm (JENNA) to secure cognitive radio networks against reactive jamming attacks. JENNA combines random channel hopping and network coding to share the control packets with neighbor users. The proposed neighbor-discovery algorithm is fully distributed and scalable. The simulation results showed that JENNA could significantly reduce the discovery delay in the presence of reactive jamming attacks.

In [125], Altman et al. proposed a non-zero-sum game framework to model jamming attacks in CRNs. In the proposed framework, a legitimate transmitter aims at maximizing its throughput while minimizing its transmission cost. On the other hand, a non-cooperative jammer attempts to minimize its transmission cost and reduce the transmitter's data rate. The authors proved the existence and uniqueness of the Nash Equilibrium for the studied game, and proposed an algorithm to find the optimal strategies. It was shown that the solution to this game problem can be found by a generalization of the water-pouring algorithm.

In [126], the authors studied a game-based model for jamming attacks in distributed access networks, where the users have no prior knowledge of the other network's user types (e.g., jammer or legitimate transmitter), packet traffic, and network parameters. The authors argued that the Bayesian games are well-suited for tackling such uncertainties, in which the users are aware of their own parameters and use the distribution of the opposites' random behavior to adapt their strategies.

In [127], Sagduyu et al. studied a dynamic data traffic model and its performance in a wireless network under jamming attacks. Dynamic data traffic refers to the scenario where the transmitters in the network have randomly backlogged information in their buffers to send. The authors considered the uncertainty caused by this dynamic data flow in a jamming game, and used a non-cooperative game framework to formulate the problem. In the studied problem, the transmitters attempt to minimize their energy cost functions under the constraints of target achievable rate, and the jammers aim to maximize the transmitters' energy cost while keeping their energy lower than a certain level. The authors derived the Nash Equilibrium for the formulated problem and evaluated its uniqueness.

In [128], Xiao et al. used the prospect theory to analyze jamming games in CRNs. The subjective players, a legitimate secondary user and a jammer, aim to maximize their SINRs weighted by probability weighting functions that model the uncertainties on players' future actions and channel gains. the Nash Equilibrium was derived for the proposed game model and its uniqueness has been proved.

A Summary of Anti-Jamming Techniques: Table VII summarizes existing anti-jamming strategies designed for CRNs. Game-theoretical approaches have been widely used to model jamming attacks in CRNs. Particularly, zero-sum games, Bayesian game models, and non-cooperative games are intensively studied in the literature. In such theoretical models, game players update their strategies based on defined cost functions under given constraints. Our literature review shows that channel/subchannel selection and power control are

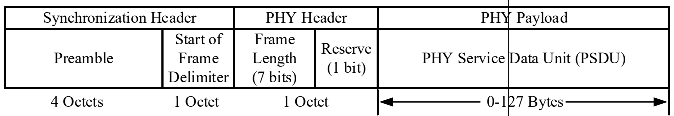


Fig. 13: ZigBee frame structure.

mostly adopted as the strategies in the studied game models.

V. Jamming and Anti-Jamming Attacks in ZigBee Networks

In this section, we survey existing jamming attacks and anti-jamming techniques in ZigBee networks. Following the same structure of previous sections, we first offer a primer of ZigBee communication and then explore existing jamming and anti-jamming strategies that were uniquely designed for ZigBee networks.

A. A Primer of ZigBee Communication

ZigBee is a key technology for low-power, low-data-rate, and short-range wireless communication services such as home automation, medical data collection, and industrial equipment control [133]. With the proliferation of low-power IoT devices, ZigBee becomes increasingly important and emerges as a crucial component of wireless networking infrastructure in smart home and smart city environments. ZigBee was developed based on the IEEE 802.15.4 standard. It operates in the unlicensed spectrum band from 2.4 to 2.4835 GHz worldwide, 902 to 928 MHz in North America and Australia, and 868 to 868.6 MHz in Europe. On these unlicensed bands, sixteen 5 MHz spaced channels are available for ZigBee communications. At the PHY layer, ZigBee uses offset quadrature phase-shift keying (OQPSK) modulation scheme and direct-sequence spread spectrum (DSSS) coding for data transmission. A typical data rate of ZigBee transmission is 250 kbit/s, corresponding to 2 Mchip/s.

Fig. 13 shows the frame structure of ZigBee communication. The frame consists of a synchronization header, PHY header, and data payload. Synchronization header comprises a preamble and a start of frame delimiter (SFD). The preamble field is typically used for chip and symbol timing, frame synchronization, and carrier frequency and phase synchronizations. The preamble length is four predefined Octets (32 bits) that all are binary zeros. The SFD field is a predefined Octet, which is used to indicate the end of SHR. Following the SFD is the PHY header, which carries frame length information. PHY payload carries user payload and user-specific information from the upper layers.

Fig. 14 shows the block diagram of the baseband signal processing in a ZigBee transceiver. Referring to Fig. 14(a), at a ZigBee transmitter, every 4 bits of the data for transmission are mapped to a predefined 32-chip pseudo-random noise (PN) sequence, followed by a half-sine pulse shaping process. The chips of the PN sequence are modulated onto carrier frequency by using the OQPSK modulation scheme. Referring to Fig. 14(b), at a ZigBee receiver, the main signal processing block chain comprises coarse and fine frequency correction, timing recovery (chip synchronization), preamble detection, phase ambiguity resolution, and despreading. The RF front-end module first demodulates the received signal from carrier radio frequency to baseband. The received chip sequences are passed through a matched filter to boost the received SNR. Then, an FFT-based algorithm is typically used for coarse frequency offset estimation. What follows is a closed-loop PLL-based algorithm for fine carrier frequency, and phase offsets correction. Timing recovery (chip synchronization) can be performed using classic methods such as zero-crossing or Mueller-Muller error detection. Following the timing recovery is the preamble detection, which can compensate for the phase ambiguity generated by the fine frequency compensation module. Finally, the decoded chips are despreaded to recover the original transmitted bits.

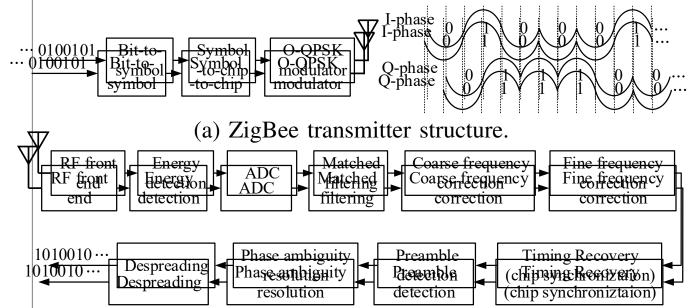


Fig. 14: The signal processing block diagram of a ZigBee transceiver.

B. Jamming Attacks

Since ZigBee is a wireless communication system, the generic jamming attack strategies (e.g., constant jamming, reactive jamming, deceptive jamming, random jamming, and frequency-sweeping jamming) presented in Section II-B can also be applied to ZigBee networks. Here, we focus on the jamming attack strategies that were delicatedly designed for ZigBee networks. Table VIII presents the existing ZigBee-specific jamming attacks in the literature. In what follows, we elaborate on these jamming attacks.

In [134], the authors studied the impact of constant radio jamming attack on connectivity of an IEEE 802.15.4 (ZigBee) network. They evaluated the destructiveness of jamming attack in an indoor ZigBee environment via experiments. In their experiments, the ZigBee network was configured in a tree topology, and a commercial ZigBee module with modified firmware was used as the radio jammer. The authors reported the number of nodes affected by a jamming attack when the jammer was located at different locations.

In [135], the authors studied reactive radio jamming attacks in ZigBee networks, focusing on improving the effectiveness and practicality of reactive jamming attacks. The reactive jammer first detects ZigBee packets in the air by searching for the PHY header in ZigBee frames shown in Fig. 13, and then sends a short jamming signal to corrupt the detected ZigBee packets. The results show that the jamming signal of more than

TABLE VIII: A summary of jamming attacks and anti-jamming strategies for ZigBee networks.

	Ref.	Description	Strengths	Weaknesses
Jamming attacks	[134]	Constant jamming attack on ZigBee communications.	Highly effective	Energy inefficient
	[135]	Real-world implementation of reactive jamming attack	Highly effective Energy efficient	Hardware constraints
	[136]	Cross technology jamming using commodity WiFi dongle	Highly effective	Energy inefficient

	Ref.	Description	Application scenario
Anti-jamming techniques	[137]	MIMO-based receiver design using machine learning	High-power constant jamming attack
	[138]	Conventional DSSS performance evaluation against jamming signals	High-power noise-like signal
	[139]	Randomized differential DSSS	Constant jamming attack
	[140], [141]	Dodge-Jam; Channel hopping and frame segmentation	Reactive and ACK jamming attacks
	[142]	DEEJAM; frame masking, channel hopping, packet fragmentation, and fragment replication.	Reactive jamming attack
	[143]	Digital filter design for jamming frequency components rejection	periodically cycling jamming attack
	[144], [145]	Jammer's reaction time estimation and using the unjammed time slots for data transmissions.	Reactive jamming attack
	[146]	Jamming attack detection based on extracting statistics from jamming-free symbols of DSSS synchronizer.	Reactive jamming attack
	[136]	Multi-staged cross-technology jamming attack detection.	Constant jamming attack

26 μs time duration suffices to bring the packets reception rate of a ZigBee receiver down to zero. The authors also built a prototype of the proposed jamming attack on a USRP testbed and evaluated its performance in an indoor environment. Their experimental results show that the prototyped jammer blocks more 96% packets in all scenarios.

In [136], Chi et al. proposed a cross-technology jamming attack on ZigBee communications, where a Wi-Fi dongle was used as the malicious jammer to interrupt ZigBee communication using Wi-Fi signal. The firmware of Wi-Fi dongle was modified to disable its carrier sensing and set the SIFS and DIFS time windows to zero, such that the Wi-Fi dongle can continuously transmit packets. The reasons for using Wi-Fi cross-technology to attack ZigBee communications are three-fold: i) Wi-Fi dongle is cheap and easy to be driven as a constant jammer; ii) a WiFi-based jammer is easy to detect as its traffic tends to be considered legitimate; iii) Wi-Fi bandwidth (20 MHz) is larger than ZigBee bandwidth (5 MHz), making it possible to pollute several ZigBee channels at the same time.

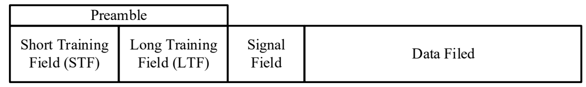
C. Anti-Jamming Techniques

Due to the use of chip spreading in its modulation, ZigBee is resilient to low-power jamming attacks by design. In addition, anti-jamming strategies such as MIMO-based jamming mitigation and spectrum spreading techniques can also be applied to ZigBee communications against jamming attacks. Particularly, ZigBee employs DSSS at its PHY layer, which can enhance the link reliability against jamming and interference signals. We elaborate on the existing anti-jamming techniques for ZigBee communications in the following.

As a performance baseline, Fang et al. [138] studied the bit error rate (BER) performance of DSSS in ZigBee communications. Their theoretical analysis and simulation show that, in the AWGN channel, a ZigBee receiver renders BER $= 10^{-1}$ when SNR $= 3$ dB, BER $= 10^{-2}$ when SNR $= 6$ dB, and BER $= 10^{-3}$ when SNR $= 8$ dB. These theoretical results provide a reference for the study of ZigBee communications in the presence of jamming attacks.

In [137], Pirayesh et al. proposed an MIMO-based jamming-resilient receiver to secure ZigBee communications against constant jamming attack. They employed an online learning approach for a multi-antenna ZigBee receiver to mitigate unknown jamming signal and recover ZigBee signal. Specifically, the proposed scheme uses the preamble field of a ZigBee frame, as shown in Fig. 13, to train a neural network, which then is used for jamming mitigation and signal recovery. A prototype of the proposed ZigBee receiver was built using on a USRP SDR testbed. Their experimental results show that the proposed ZigBee receiver achieves 100% packet reception rate in the presence of jamming signal that is 20 dB stronger than ZigBee signal. Moreover, it was shown that the proposed ZigBee receiver yields an average of 26.7 dB jamming mitigation gain compared to commercial off-the-shelf ZigBee receivers.

In [139], a randomized differential DSSS (RD-DSSS) scheme was proposed to salvage ZigBee communication in the face of a reactive jamming attack. RD-DSSS decreases the probability of being jammed using the correlation of unpredictable spreading codes. In [141] and [140], a scheme called Dodge-Jam was proposed to defend IEEE 802.15.4 ACK frame transmission against reactive jamming attacks. Dodge-Jam relies on two main techniques: channel hopping and frame segmentation. Particularly, frame segmentation is done by splitting the original frame into multiple small blocks. These small blocks are shifted in order when retransmission is required. In this scenario, the receiver can recover the transmitted frame after a couple of retransmission. In [142], a MAC-layer protocol called DEEJAM was proposed to reduce the impact of jamming attack in ZigBee communications. DEEJAM offers four different countermeasures, namely frame masking, channel hopping, packet fragmentation, and redundant encoding, to defend against different jamming attacks. Specifically, frame masking refers to using a confidential start of frame delimiter (SFD) symbols by the ZigBee transmitter and receiver when a jammer is designed to use the SFD detection for its transmission initialization. Channel hopping was proposed to defend against reactive jamming attacks. Packet fragmentation was proposed to defend against scan



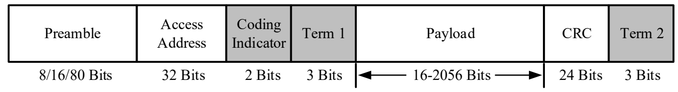


Fig. 15: Bluetooth low energy frame structure.

jamming. Redundant encoding (e.g., fragment replication) was designed to defend against noise jamming.

In [143], the impact of a periodically cycling jamming attack on ZigBee communication was studied, and a digital filter was designed to reject the frequency components of the jamming signal. In [144] and [145], an anti-jamming technique was proposed to defend against high-power broadband reactive jamming attacks for low data rate wireless networks such as ZigBee. The proposed technique undertakes reactive jammers' reaction time and uses the unjammed time slots to transmit data. In [146], Spuhler et al. studied a reactive jamming attack and its detection method in ZigBee networks. The key idea behind their design is to extract statistics from the jamming-free symbols of the DSSS synchronizer to discern jammed packets from those lost due to bad channel conditions. This detection method, however, focuses only on jamming attacks without considering jamming defense mechanism. In [136], Chi et al. proposed a detection mechanism to cope with cross-technology jamming attacks. Their proposed detection technique consists of several steps, including multi-stage channel sensing, sweeping channel, and tracking the number of consecutive failed packets. Once the number of failed packets exceeds a certain threshold, the ZigBee device transmits its packets even if the channel is still busy, letting the signal recovery be made at the receiver side.

A Summary of Anti-Jamming Techniques: Table VIII summarizes the existing anti-jamming strategies that were delicately designed for ZigBee networks. As it can be seen from the table, DSSS is the primary anti-jamming strategy studied for ZigBee communications. However, DSSS is notorious for its spectral inefficiency, and its capability in jamming mitigation is very limited. Recently, new approaches such as MIMO-based jamming mitigation and frequency hopping have been studied to enhance the resiliency of ZigBee communications against jamming attacks. However, it is not clear if these approaches (e.g., MIMO-based jamming mitigation) can be implemented on real-world ZigBee devices, as most of them are limited by their size, energy, and computational power.

VI. Jamming and Anti-Jamming Attacks in Bluetooth Networks

In this section, we survey existing jamming and anti-jamming attacks in a Bluetooth network. By the same token, we first offer a primer of the PHY and MAC layers of Bluetooth communication and then review the existing jamming/anti-jamming techniques that were dedicatedly designed for Bluetooth networks.

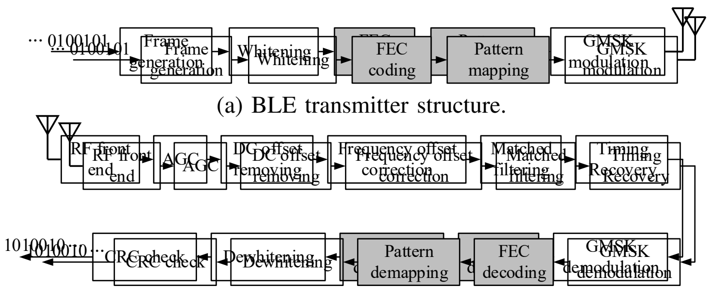
A. A Primer of Bluetooth Communication

Bluetooth is a wireless technology that has been deployed for real-world applications for many years. It was initially designed for short-range device to device (D2D) communication and then evolved toward many other communication purposes in the IoT applications. A Bluetooth network, also known as a piconet, is typically composed of one master device and up to seven slave devices. A Bluetooth device can serve as a master node in only one piconet, but it can be connected to multiple piconets as a slave. In response to the low power constraints in IoT networks, a new concept of Bluetooth Low Energy (BLE) was recently introduced to offer a more energy-efficient and flexible communication scheme compared to classic Bluetooth technology. BLE operates in unlicensed 2.4GHz–2.4835GHz ISM frequency bands, where there are 40 channels of 2 MHz bandwidth available for its communications. Unlike Wi-Fi channels, the BLE channels are not overlapping. In its latest version (e.g., BLE v5), BLE can support 1 Msym/s and 2 Msym/s symbol rates, where 1 Msym/s symbol rate is the mandatory modulation scheme while 2 Msym/s symbol rate is optional. BLE at 1 Msym/s modulation may use packet frames with coded or uncoded data. Fig. 15 shows a general packet structure for BLE at 1 Msym/s transmission. As can be seen, a BLE packet consists of a preamble, access address, payload, and CRC. The coding indicator and termination fields are further transmitted within the packet for the coded frame format, as shown in Fig. 15.

Fig. 16 shows the block diagram of baseband signal processing in a Bluetooth device. At the transmitter side, the generated frame is fed into a whitening (scrambling) operation to avoid transmitting long sequences consisting of consecutive zeros or ones. FEC and pattern mapping are used when the coded frame format is transmitted. The scrambled data is encoded using a $1/2$ rate binary convolutional FEC encoder. Pattern mapping might be used to map each encoded bit to 4-bits symbol to decrease the error decoding probability. The final bits to be sent are modulated on the carrier frequency using Gaussian minimum shift keying (GMSK). The data rate of uncoded packet format transmission is 1 Mbps. The data rate of coded packet format is 500 kbps. After applying pattern mapping to the encoded bits, the data rate is 125 kbps.

Referring Fig. 16(b), at the receiver side, the received signal power is adjusted using an AGC block. Following AGC, the DC offset of the received signal is removed. A coarse frequency offset correction algorithm is employed to estimate and compensate the carrier frequency mismatch between the transmitter and receiver clocks. The received signal is later passed through a Gaussian matched filter to reduce the noise. In the aftermath of matched filtering, the frame timing synchronization is performed based on preamble detection. Then, the received frame is demodulated using the GMSK demodulation block. FEC decoding and pattern de-mapping are used when the coded packet frames are transmitted. Finally, the decoded bits are de-whitened and the CRC check is performed to check the correctness of the decoded bits.

FHSS is a key technology of Bluetooth communications as it enhances the reliability of Bluetooth link in the presence of intentional or unintentional interference. With FHSS, Bluetooth packets are transmitted by rapidly hopping over a set of predefined channels, following a mutually-agreed hopping



(a) BLE transmitter structure.

(b) BLE receiver structure.

Fig. 16: Signal processing block diagram of Bluetooth communication.

pattern. Conventional Bluetooth has 79 distinct and separate channels, each of 1 MHz bandwidth. The new standard, Bluetooth Low Energy (BLE), has 40 distinct channels, each of 2 MHz bandwidth. The hopping pattern is determined by a pseudo-random spreading code, which is shared with the receiver to keep transmitter and receiver synchronized during the channel hopping. The spreading code must be shared after a pre-shared key establishment process to secure the data communication.

B. Jamming Attacks

In the original design of Bluetooth communication systems, frequency hopping spread spectrum (FHSS) technology was adopted to avoid interference so as to improve the communication reliability. The inherent FHSS technology provides Bluetooth systems with the capability of coping with jamming attacks to some extent. For this reason, the study of jamming attacks in Bluetooth networks is highly overlooked, and the investigation of Bluetooth-specific jamming attacks is very limited in the literature.

However, the FHSS technology is effective only for narrowband, low-power jamming attacks; and it becomes ineffective when the bandwidth of high-power jamming signal spans over all possible Bluetooth channels, i.e., $2.4-2.4835$ GHz ISM band. In fact, such a jamming attack can be easily launched in practice, thanks to the advancement of SDR technology. In light of powerful jamming attacks, Bluetooth networks are vulnerable to generic jamming attacks (e.g., constant, reactive, and deceptive jamming attacks, see Section II-B) as much as other wireless communication systems.

In the context of Bluetooth networks, although many works have been done to investigate the underlying security vulnerabilities of Bluetooth applications (see, e.g., [147]–[150]), the research effort on investigating jamming attacks for Bluetooth communications remains very limited. In [151], Köppel et al. built an intelligent jamming attack that synchronously tracks Bluetooth communications and sends the jamming signal. The proposed algorithm estimates the frequency hopping sequence of Bluetooth communications by i) decoding the master's upper address part (UAP) and the lower address part (LAP), and ii) determining the communication's clock. The jammer uses the estimated clock to synchronize itself with the Bluetooth devices. The experimental results demonstrate that a jammer is capable of completely blocking Bluetooth communications if the jammer can obtain a correct estimate of frequency hopping sequence and clock.

C. Anti-jamming Techniques

As mentioned before, FHSS is the key technology used at the physical layer of Bluetooth communication, which has a certain capability of taming interference and jamming signals. The pre-shared key establishment, however, is itself a challenging constraint in the presence of jamming attacks.

In Bluetooth communication, FHSS relies on a pre-shared key at a pair of devices to determine their frequency hopping pattern. The key establishment procedure (for reaching the consent on frequency hopping pattern at transmitter and receiver) exposes Bluetooth networks to adversarial jamming attackers. In [152]–[155], uncoordinated FHSS schemes were proposed to secure the key establishment procedure for Bluetooth communication in the presence of jamming attacks. These schemes employ a randomized FHSS technique, where a pair of Bluetooth devices randomly switch over multiple channels before being able to initiate the communication. Once the two Bluetooth devices come across on the same channel, they exchange the hopping and spreading keys. To fasten the convergence of the procedure, one approach is to let Bluetooth transmitter hop over the channels much faster than Bluetooth receiver (e.g., 20 times faster).

In [156], Xiao et al. proposed a collaborative broadcast scheme to eliminate the need for pre-shared key exchanging in an uncoordinated FHSS technique. The authors considered a star-topology network, where a master node intends to broadcast a message to its multiple slave nodes. The key idea behind this scheme is to broadcast messages in all possible channels and use the nodes having already acquired the message to serve as relays to forward the messages to other nodes. It is assumed that the jammer cannot block all available channels; otherwise, the proposed algorithm will not work. Multiple channel selection schemes, including random, sweeping-channel, and static, were considered for relaying broadcast messages. Packet reception rate and cooperation gain were investigated to evaluate the performance of the proposed scheme. Experimental results confirm a significant improvement of jamming resiliency. Moreover, it was shown that, for a certain jamming probability, when there is a small number of slave nodes in the network (e.g., less than 50), sweeping channel selection achieves a higher packet reception rate. But for a large number of nodes, static channel selection outperforms other channel selection methods.

A Summary of Anti-Jamming Techniques: As discussed above, Bluetooth adopted FHSS as medium access control; it thus has a certain jamming resiliency by nature. Nevertheless, FHSS always leads to an inefficient spectrum utilization and is vulnerable to the key exchanging procedure in the presence of jamming attacks. It is also susceptible to wideband jamming attacks. In the literature, very limited works have been done thus far to enhance the Bluetooth security against jamming attacks. One possible reason is that Bluetooth is typically used for short-range wireless communications, where jammers can be physically mitigated.

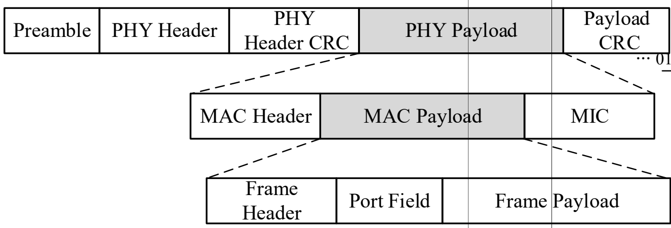
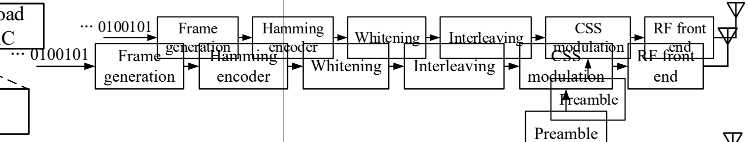
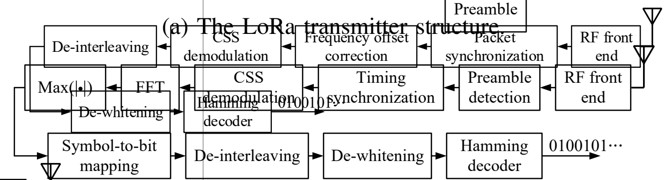


Fig. 17: The structure of LoRa frame.



(a) The LoRa transmitter structure.



(b) The LoRa receiver structure.

Fig. 18: The schematic diagram of LoRa transceiver.

VII. Jamming and Anti-Jamming Attacks in LoRa Networks

A. A Primer of LoRaWANs

LoRa is a low power wide area networking (LPWAN) technology. It recently becomes popular thanks to its promising features such as open-source development, easy deployment, flexibility, security, cost effectiveness, and energy efficiency. LoRa has been widely used in diverse IoT applications such as smart parking, smart lighting, waste management services, life span monitoring of civil structures, and air and noise pollution monitoring. Compared to other low-power wireless technologies (e.g., ZigBee and Bluetooth), LoRa offers a large coverage (5km–15km). LoRa is a lightweight communication system with low-complexity signal processing and low-complexity MAC protocols. It consumes only 120–150 mW power in its transmission mode. The lifetime of a LoRa device varies in the range from 2 to 5 years, depending on its in-use duty cycle [157].

LoRa uses chirp spread spectrum (CSS) modulation for its data transmission. It supports a data rate from 980 bps to 21.9 kbps and spreading factors (SF) from 6 to 12. In the CSS modulation, data is carried by frequency modulated chirp pulses. The CSS modulation scheme appears to be resilient to both interference and Doppler shift, making it particularly suitable for long-range mobile applications.

LoRa operates in sub-GHz ISM bandwidth in North America. On 902.3 MHz–914.9 MHz spectrum, 64 channels are defined for LoRa, each of 125 kHz bandwidth. On 1.6 MHz spectrum, 8 channels are defined for LoRa's uplink transmission, each of 500 kHz bandwidth. On 923.3 MHz–927.5 MHz spectrum, 8 channels are defined for LoRa's downlink transmission, each of 500 kHz bandwidth. Typically, LoRa operates in a star-network topology, where one or multiple LoRa devices are served by a central gateway connected to a network server.

Packet Structure: Fig. 17 shows the structure of a LoRa packet. The preamble comprises a sequence of upchirps and a sequence of downchirps. The number of upchirps in the preamble depends on the data rate and spreading factor. The downchirps in the preamble is used for packet detection and clock synchronization.

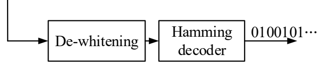
The PHY header and its CRC fields are optional and transmitted to indicate the length of PHY payload. The PHY payload consists of MAC header, MAC payload, and message integrity code (MIC). Depending on the selected data rate, the maximum user payload size varies in the range of 11 to 242 bytes. MAC header is 1-byte data, specifying MAC message type (MType), such as uplink/downlink data, join request, and accept request. LoRa supports both "*confirmed*" data transmission and "*unconfirmed*" data transmission. The former requires a receiver to acknowledge the frame reception, while the latter requires no ACK feedback. The MAC payload consists of a frame header (FHDR), an optional port field (FPort), and frame payload, as shown in Fig. 17. The frame header (FHDR) mainly carries the end-device address, and the frame payload carries the application-specific end-device data.

LoRa supports bi-directional communications. That is, when a LoRa device sends an uplink packet, it waits for two window time slots for downlink data. This means that the downlink transmission requires a LoRa device to send the uplink packets first. In a LoRaWAN, the ALOHA scheme is used as the medium control protocol for LoRa devices to access the channel for their uplink transmissions.

Transceiver Structure: Fig. 18 shows the schematic diagram of a LoRa transceiver structure. At the transmitter side, the bits to be transmitted are first encoded using a Hamming encoder. The encoded bits are fed into the whitening module to avoid transmitting a long sequence of consecutive zeros/ones. Following the whitening module, the interleaving module is applied to the scrambled bits. The preamble sequence is attached to the processed bits, and all are modulated on the carrier frequency using the CSS modulation. At the receiver side, the frame is detected and synchronized using the preamble and PHY header symbols. The received chirps are decoded using the CSS demodulation block, FFT operation, and peak detection in the frequency domain. Finally, the decoded bits are fed into the deinterleaving block, dewhitening block, and hamming decoder, sequentially.

B. Jamming Attacks

In this subsection, we overview the jamming attacks on LoRa communications. In [158], Hou et al. studied the vulnerability of LoRa communications in the face of constant noise-like jamming attacks. The experimental measurements in [158] show that a LoRa receiver can achieve 100% packet reception rate when SJNR is -2 dB, the spreading factor is 8, and the bandwidth is 250 kHz. When SJNR drops below -6 dB, the LoRa communications are completely disrupted. The authors further studied the destructiveness of jamming attackers that send synchronous data chirps to interfere with



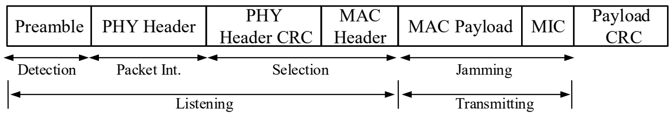


Fig. 19: Illustration of selective jamming attack on LoRa packet transmissions [162].

the desired chirps. It was argued that the existing collision recovery and interference cancellation techniques (e.g., [159]–[161]) are incapable of defeating synchronous chirp jamming attack. The proposed scheme was implemented on a USRP-based testbed and evaluated in a real-world scenario. The experimental results showed that a synchronous chirp jamming attacker, with 20$\sim$30 dBm transmission power, could completely disrupt LoRa communications in indoor environments.

In [162], Aras et al. investigated the vulnerabilities of LoRa communications under triggered jamming attack and selective jamming attack. The authors showed that, despite using spreading spectrum scheme at low data rate, LoRaWAN is still highly susceptible to jamming attacks.

- *Triggered jamming:* Triggered jamming attack is similar to reactive jamming attack. Once the jammer detects the preamble transmitted by a LoRaWAN device, it will broadcast jamming signal. [162] conducted experiments to evaluate the performance of LoRaWAN under triggered jamming attack, where a commodity LoRa end-device is used as triggered jammer. The experimental results show that the packet reception rate of a legitimate LoRa device drops to 0.5% under the triggered jamming attack.
- *Selective jamming:* Fig. 19 shows the basic idea of selective jamming attack studied in [162], where a jammer sends jamming signal upon decoding the MAC header and the end-device address. The selective jamming attack can block a particular device's communications in a LoRaWAN while causing no interference to other devices in the network. The authors ran experiments to evaluate the performance of selective jamming attack in a LoRaWAN. They used two commodity LoRa devices and programmed the jammer such that it targets one of their communications. Experimental results show that the packet reception rate at the victim LoRa device drops to 1.3% under the selective jamming attack.

In [163], Huang et al. built a prototype of a reactive jammer against LoRaWAN communications using a commodity LoRa module. The proposed algorithm jointly use the LoRa preamble detection and the signal strength indicator (RSSI) for efficiently detecting LoRa channel activity. The authors evaluated the performance of the proposed jammer in LoRaWAN via conducting real-world experiments. They considered the impact of the SF and the jammer's bandwidth on signal detection. The packet delivery rate was used to measure the performance of the victim LoRa device under the proposed jamming attack. Their results demonstrate that a jammer can achieve more than 90% accuracy in LoRa packet detection when the jammer's SF and bandwidth are matched with the legitimate LoRa signal. Moreover, the results show that, for most scenarios, when jamming signal is 3 dB stronger than LoRa signal, a LoRa receiver fails to decode the received packets and the packet delivery rate drops to zero.

C. Anti-jamming Techniques

The spreading spectrum technique is the main approach used in the LoRa technology to secure its communications against jamming attacks and unintentional interference signals. As mentioned earlier, LoRa uses the CSS modulation scheme for its data transmissions, in which every bit to be transmitted is mapped into the sequence of 2^{SF} chips and modulated onto the chirp waveform.

Per [164], a LoRa receiver is capable of recovering the received packets (i.e., yielding zero packet error rate) with the RSSI as low as -121 dBm when working at 125 KHz bandwidth and SF = 8. Comparing to conventional FSK modulation scheme, it is shown that, for a given data rate of 1.2 Kbps, a LoRa receiver achieves 7 dB to 10 dB lower receiving sensitivity. Moreover, a LoRa receiver achieves up to 15 dB gain in the packet reception ratio compared to conventional FSK receivers.

In [165], Danish et al. proposed a jamming detection mechanism in LoRaWANs using Kullback Leibler divergence (KLD) and Hamming distance (HD) algorithms. The KLD-based jamming detection scheme uses the likelihood of jamming-free received signal's probability distribution and the received signal's probability distribution under jamming attack. Particularly, the authors used join request transmissions to determine a mass function of the LoRa device signaling. If the similarity of the received signal's distribution and the acquired mass function is below a certain threshold, the presence of an undesired interference signal or a jamming signal will be claimed. Similarly, in the Hamming distance scheme, the algorithm finds the average Hamming distance between the received signal and the training signal. If the calculated distance diverges from a certain threshold, the algorithm claims the presence of jamming attacks. The authors evaluated the performance of their proposed schemes via a real-world system implementation. The results show 98% and 88% accuracy in jamming detection for the KLD-based and HD-based algorithms, respectively.

A Summary of Anti-Jamming Techniques: Thus far, very limited progress has been made in securing LoRaWANs against jamming attacks. As discussed above, LoRa uses chirp spreading spectrum (CSS) techniques to enable long-rang, low-power communications. CSS allows LoRa devices to decode the received packets even below the noise floor. It somehow protects the LoRa communications in the face of jamming attacks.

VIII. Jamming and Anti-Jamming Attacks in Vehicular Wireless Networks

In this section, we survey the jamming attacks and anti-jamming mechanisms in vehicular wireless communication networks, including on-ground vehicular ad-hoc network (VENET) and in-air unmanned aerial vehicular (UAV) network. In what follows, we first provide an introduction of vehicular wireless communication networks and then review

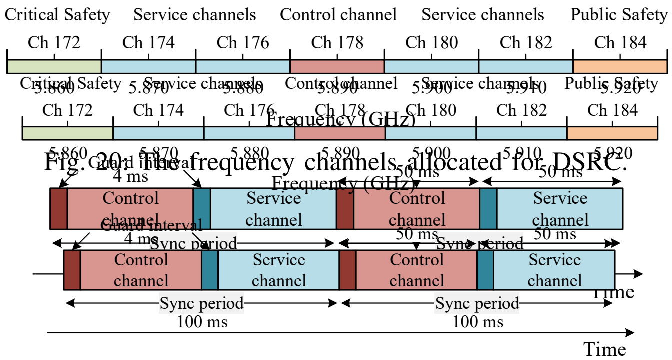


Fig. 20: The frequency channels allocated for DSRC.

Fig. 21: The time intervals in 802.11p communications.

the jamming/anti-jamming strategies uniquely designed for vehicular wireless networks.

A. A Primer of Vehicular Wireless Networks

On-Ground VANET: Every year thousands of deaths occur in the U.S. due to traffic accidents, about 60 percent of which could be avoided by vehicular communication technologies. To reduce vehicular fatalities and improve transportation efficiency, the U.S. Department of Transportation (USDOT) launched the Connected Vehicle Program that works with state transportation agencies, car manufacturers, and private sectors to design advanced wireless technologies for vehicular communications. It is a key component of network infrastructure to realize the vision of an intelligent transportation system (ITS) by enabling efficient vehicle-to-vehicle (V2V) communications and/or vehicle-to-infrastructure (V2I) communications. Compared to stationary and semi-stationary wireless networks such as Wi-Fi networks, VANETs face two unique challenges in their design and deployment. First, vehicles are of high speed. The high speed of the vehicles continuously changes the network topology in terms of both the vehicles' positions and the number of connected vehicles. Second, VANET is a delay-sensitive communication network. Reliable and timely packet delivery is of paramount importance for applications such as collision avoidance in real-world transportation systems.

Dedicated short-range communications (DSRC) is a communication system that enables wireless connectivity for VANETs. At the PHY and MAC layers, DSRC deploys IEEE 802.11p standard. 802.11p uses the same frame format as legacy Wi-Fi (Fig. 4(a)) for its data transmission. However, the channel bandwidth is reduced to 10 MHz to provide higher link reliability against channel impairments caused by users' mobility. DSRC operates in the 5.9 GHz frequency band, where seven distinct channels of 10 MHz are available for the users' access, as shown in Fig. 20. The center channel (control channel) and the two on-edge channels are used to carry safety messages such as critical information on road crashes or traffic congestion, while the service channels can be used for both safety messages and infotainment data such as video streaming, roadside advertising, and road map and parking-related information. In the time domain, the resources are separated into equally-sized time intervals of 100 ms, known as sync period, as shown in Fig. 21. Every sync period is divided into two 50 ms intervals. Every user needs to listen to the control channel within the first 50 ms interval to receive the safety messages as well as obtain the information required for accessing the available services. In the second 50 ms interval, the user will switch to the intended service channel to send/receive infotainment data.

In a VANET, the vehicles, also known as on-board units (OBUs), and roadside units (RSUs) can communicate in three different network settings: i) An RSU, similar to a Wi-Fi AP, serves a set of OBUs having the same basic service set (BSS) ID. ii) The units with the same BSSID communicate with each other within an ad-hoc mode, where there is no dedicated central unit. iii) The out-of-network units can hear each other, in which the units use a so-called wildcard BSSID to communicate with each other. The wildcard BSSID allows the units from different networks to communicate in a critical moment. While the first two network settings are already deployed in Wi-Fi communications, the third mode is specifically designed for VANETs, as they require all units to be able to receive critical and safety messages.

At the MAC layer, similar to legacy Wi-Fi, 802.11p uses carrier sensing for channel access. However, on top of the 802.11p MAC mechanism, DSRC takes advantage of an enhanced MAC-layer technique, known as enhanced distributed channel access (EDCA) in IEEE 1609.4, as a prioritized medium access mechanism to enable critical message exchanging.

In-Air UAV Network: With the significant advancement of robotic and battery technologies in the past decades, UAV communication networks have drawn an increasing amount of research interest in the community and enabled a wide spectrum of applications such as photography, film-making, newsgathering, agricultural monitoring, crime scene investigations, border surveillance, armed attacks, infrastructure inspection, search and rescue missions, disaster response, and package delivery. Depending on the applications, UVAs of different sizes can be deployed in the network. Small UAVs are generally used to form swarms, while large UAVs are likely used in critical military or civilian missions. The speed of UAVs in different scenarios may vary from 0 m/s to 100 m/s, depending on the applications [166].

Most UAVs operate in the unlicensed 2.4 GHz and 5.8 GHz ISM bands. Depending on the application requirements, UAV networks can be configured to operate in one of the following network topologies: i) star topology, where each UAV directly communicates with a ground control station; and ii) mesh network topology, in which UAVs communicate with each other as an ad-hoc network, and a small number of them may communicate with ground control station [167]. Moreover, heavier UAVs can be designed to take advantage of satellite communication (SATCOM) for routing. UAVs are typically pre-programmed for this service to follow a flight route using global navigation satellite system (GNSS) signals. In recent years, many standards have been drafted to address the challenges regarding UAV communications. Cellular networks are currently considered as a promising infrastructure for UAV activities due to their wide coverage. 3GPP in its release 15 have enhanced the LTE capability to

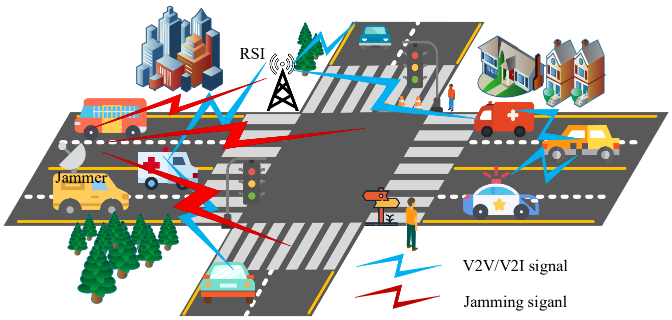


Fig. 22: Illustration of jamming attacks in a vehicular network.

support UAV communications [168].

B. Jamming Attacks

Given the openness nature of wireless medium for vehicular communications, both VENET and UAV networks are vulnerable to generic jamming attacks (see Section II-B), such as constant jamming, reactive, deceptive, and frequency-sweeping jamming attacks. In this subsection, we focus on the existing jamming attacks that were dedicatedly designed for vehicular wireless networks. Table IX presents a summary of existing jamming attacks in vehicular networks.

VANET-Specific Jamming Attacks: Jamming attacks are of particular importance in VANETs as the connection loss caused by the jamming attacks may lead to car collision and road fatality. A jamming attacker can adopt different strategies (e.g., constant, reactive, and deceptive jamming) to cause the loss of wireless connection for V2V and V2I communications in VANETs. Fig. 22 shows an instance of jamming attack on a VANET, where the destructiveness of existing jamming attack strategies has been studied in literature.

In [169], Azogu et al. studied the impact of jamming attacks on IEEE 802.11p-based V2X communications, where the jammers were designed to dynamically switch to in-use channels. The authors conducted experiments in a congested city area using 100 vehicles and 20 RSI, and placed multiple radio jammers with the range of 100 m in the proximity of RSIs. They used two 802.11p channels for V2X communications and packet send ratio (PSR) as the evaluation metric, where the PSR is the number of packets sent per total number of queued messages for transmission. The experimental results show that 10 radio jammers can degrade the network PSR to 0.4.

In [170] and [171], Punal et al. evaluated the achievable throughput of V2V communications under constant, periodic, and reactive jamming attacks using real-world software-defined radio implementation. The authors conducted several real-world experiments in both indoor and outdoor environments. Particularly, their experiments in an outdoor scenario show that the packet delivery rates in 802.11p communications drop to zero when SNJR is less than 9 dB under constant jamming attack, when SNJR is less than 55 dB under periodic jamming attack with the duty cycle of 86% and 74 μs period, and when SNJR is less than 12 dB under reactive jamming attack with the packet detection duration of 40 μs and jamming signal duration of 500 μs.

UAV-Specific Jamming Attacks: While UAV networks are vulnerable to the generic jamming attacks in Section II-B, we focus on those jamming attacks that were deliberately designed for satellite-based UAV networks. Since most UAVs rely on GPS signals for positioning and navigation, a jamming attacker may target on their GPS communications to dysfunction UAV networks. This class of jamming attacks can pose a severe threat to military UAV networks.

In [172], another UAV-specific jamming attack, called control command attack, was studied. In this attack, a jammer attempts to interrupt the control commands issued by UAVs' ground control station. Control command attacks can be realized using conventional jamming attacks to block the desired received signal or by sending fake information to lure UAVs following incorrect commands. The control command attack can cause the loss of UAVs and mission failure.

C. Anti-Jamming Techniques

In this subsection, we review the anti-jamming techniques that were dedicatedly designed for VANETs and UAV networks. Table IX presents a summary of existing anti-jamming mechanisms in vehicular networks. We elaborate on them in the following.

VANET-Specific Anti-Jamming Techniques: Thus far, very limited work has been done in the design of anti-jamming techniques for VENETs. Given that most VENETs are using IEEE 802.11p (DSRC) for V2V and V2I communications, a straightforward anti-jamming strategy for VENETs is to switch to another available wireless network (e.g., cellular), provided that such an alternative network is available.

In [173] and [174], the authors proposed to cope with jamming attacks for VANETs by leveraging UAV devices. They studied smart jamming attacks in a VANET, where a jammer continuously changes its attack strategy based on the network topology. To salvage the vehicular communications, a UAV was utilized to relay data for vehicles to the alternative RSUs when the serving RSU is under jamming attacks. In this work, a game theory approach was employed to model the interactions between jammer and UAV, where the jammer adaptively selects its transmission power, and the UAV makes decisions for relaying the data.

In [177], Pirayesh et al. proposed a new architecture for multi-antenna 802.11p receiver, called JammingBird, to secure vehicular communications against high power constant jamming attacks. The authors leveraged the unused resource elements within the IEEE 802.11p frame structure and constructed a spatial filter for each subcarrier to cancel jamming signal. The proposed receiver was implemented on a wireless USRP testbed, and its feasibility was demonstrated in practice. In particular, the performance of the new receiver was evaluated on parking lot, local streets, and highway scenarios. The experimental results showed that the proposed receiver can decode 802.11p packets in the face of 25 dB stronger jamming signal and achieve 83% throughput of the jamming-free scenario on average.

TABLE IX: A summary of jamming attacks and anti-jamming strategies for vehicular wireless networks.

		Ref.	Description	Strengths	Weaknesses
Jamming attacks	VANETs	[169], [170]	Constant jamming attack on 802.11p-based V2V	Highly effective	Energy efficient
		[170], [171]	Periodic jamming attack on V2V communications	Energy efficient	Less effective
		[170], [171]	Reactive jamming attack on V2V communications	Highly effective	Hardware constraint
	UAV	[172]	Jamming attack on UAVs' control command.	Highly effective	Less stealthy

		Ref.	Description	Application scenario
Anti-jamming techniques	VANETs	[173], [174]	Traffic rerouting to alternative RSUs using UAVs	Smart jamming attack
		[175]	Mobile jammers detection using unsupervised learning algorithm	Periodic jamming attack
		[176]	Learning-based jammer localization in VANETs	Periodic jamming attack
		[177]	JammingBird; MIMO-based jamming resilient receiver design	Constant jamming attack
		[178]	Massive MIMO RSUs combined with network coding	Constant noise-like jamming attack
		[179], [180]	Jamming detection by real-time tracking the received PDR	Low-power constant jamming attack
		[181]	Differentiating jamming attack, interference signal, and collision in VANETs	Reactive jamming attack
		[182]	Jamming detection for vehicle platooning using data-mining techniques	Random and ON/OFF jamming attacks
	UAVs	[183]	Power control game modeling for UAV communications	Low-power constant jamming attack
		[184]–[186]	Bayesian Stackelberg game modelling for UAV ad-hoc network	Power-optimized jamming attack
		[187]	Learning-based frequency, motion, and antenna selection for UAV swarms	Fixed and mobile constant jamming attack

In [178], Okyere et al. studied the robustness of massive MIMO RSUs (RoadSide Units) under constant jamming attacks in VANETs. Network coding scheme was considered for RSUs to serve multiple vehicles. The RSU leverages a sum-difference matrix to transform the uplink channel matrix and cluster the received symbols into correlated pairs to estimate the superimposed symbols received from multiple vehicles. The performance of the network coding scheme was evaluated under noise-like jamming attacks for both sub-6 GHz and mmWave channel models. Simulation results showed that for the same network setting and the same SJNRs, RSU using network coding can achieve double spectral efficiency for both channel models compared to that without network coding.

Attacker detection and localization are an alternative approach that has been studied in literature as an effort to thwart jamming attacks in VANETs [175], [176], [179]–[182]. In [179] and [180], the authors proposed a fast-convergent algorithm to detect jamming attacks in VANETs by real-time tracking the received packet deliver ratio (PDR) changes. The authors simulated a VANET consisting of 100 vehicles moving at 10 m/s. It was assumed that RSU and jammer are stationary, and one vehicle enters into the jammed area at a time. Simulation results show that the proposed algorithm can detect reactive jamming in less than 40s.

In [181], Benslimane et al. proposed an MAC-layer mechanism that is capable of differentiating jamming attack, interference signal, and collision in VANETs. The proposed algorithm monitors the collided beacon frames transmitted within the control channel intervals and detects the jamming attacks by a low false alarm probability. In [182], Lyamin et al. proposed a jamming detection mechanism for vehicle platooning applications in cooperative intelligent transportation systems. In the studied vehicle platooning, a group of smart cars pursue a leading human-driven vehicle. The proposed algorithm combines prior knowledge of the platoon communications with the monitored collided messages and leverages data-mining techniques to detect an anomaly transmission within the network. The authors studied the performance of their proposed scheme in jamming detection under two types of on-off and random jamming attacks. Simulation results showed that the jamming detection probability is higher than 0.7 when the number of vehicles is 25 with 10% jamming probability. Moreover, the authors demonstrated that the algorithm could be run in real time as the measured decision delay is less than 50ms.

In [175], Karagiannis et al. proposed to use an unsupervised learning algorithm for detecting mobile jammers in vehicular networks. The key component of the proposed scheme is to use a newly-defined parameter that measures the relative speed of victim vehicles and the jammer vehicle for training a learning algorithm. They evaluated the performance of the detection algorithm in two jamming attack scenarios: i) the jammer periodically sends jamming signal and maintains a safe distance from the victim vehicle; and ii) the jammer is unaware of the possible detection mechanism and sends constant jamming signal at any distance from the victim vehicle. Their simulation results show that their proposed algorithm can classify the attacks with the accuracy of 98.9% under constant jamming attack and 44.5% under periodic jamming attack.

In [176], Kumar et al. employed a machine learning-based approach to estimate the location of jammers in a vehicular network. Particularly, a foster rationalizer was used to detect any undesired frequency changes stemming from jamming attacks on legitimate V2V communications. Following the rationalizer, a Morsel filter was applied to remove the noise-like components from jammed signal. The filtered signal was then injected into a Catboost algorithm to estimate the jammer's vehicle location. Their simulation results show that the proposed scheme can predict the jamming vehicle's position with an accuracy of 99.9%.

UAV-Specific Anti-Jamming Techniques: Despite having attracted more research efforts, UAV networks are still in its infancy, and the research on UAV-specific anti-jamming strategies remains rare. In [183], the authors performed a theoretical study on anti-jamming power control game for UAV communications in the presence of jamming attacks, where the interactions between a jammer and a UAV are modeled as a Stackelberg game. An optimal power control policy for UAV transmissions under jamming attack was obtained using a reinforcement learning algorithm. In [184] and [185], Xu et al. studied the jamming problem in a UAV ad-hoc network, in which a transmitter tends to send the data towards its desired receiver while causing interference to other communication links (refers to the co-channel mutual interference). The problem was formulated as a Bayesian Stackelberg game, in which a jammer is the leader, and UAVs are the followers of the game. The optimal transmission power of UAVs and jammer were analytically derived using their utility functions optimization. In [186], a model was developed to take into account the flying process of UAV. Based on the model, the flying trajectory and transmission power of the UAV were optimized. In [187], Peng et al. investigated the jamming attacks in a UAV swarm network, where a jammer network consisting of multiple nodes attempts to block the communication between the swarm and its ground control station. Multiple parameters were taken into account to provide high flexibility for UAV communications to deal with jamming attacks. In particular, the UAVs exploited the degrees of freedom in the frequency, motion, and antenna-based spatial domains to optimize the link quality in the reception area. A modified Q-learning algorithm was proposed to optimize this multi-parameter problem.

A Summary of Anti-Jamming Techniques: Table IX summarizes the jamming attacks and anti-jamming strategies in vehicular networks. As it can be seen from the table, a wide range of anti-jamming strategies, including relay-aided, MIMO-based, network coding, learning-based jammer detection, power control, and channel hopping techniques, have been designed to secure vehicular networks against different jamming attacks. The prosperity of research in this area underscores the jamming threats in vehicular networks, especially in intelligent transportation systems with autonomous driving vehicles. Among the proposed anti-jamming strategies, MIMO-based approaches were mainly designed to thwart constant jamming attacks; game-theory approaches were mainly proposed to cope with low-power jamming attacks; learning-based approaches were mainly developed to detect and localize periodic and random jamming attacks.

IX. Jamming and Anti-Jamming Attacks in RIFD Communication Systems

In this section, we first provide a primer of Radio-frequency identification (RFID) communication and then provide a review on RFID-specific jamming and anti-jamming attacks.

A. A Primer of RFID Communication

As we enter into the Internet of Everything (IoE) era, RFID emerges as a key technology in many industrial domains with an exponential increase in its applications. In RFID communications, an interrogator (reader) reads the information stored in simply-designed tags attached to different objects such as humans, animals, cars, clothes, books, grocery products, jewelry, etc. from short distances using electromagnetic waves. An RFID tag can be either passive or active. Passive tags do not have a battery and use energy harvesting for their

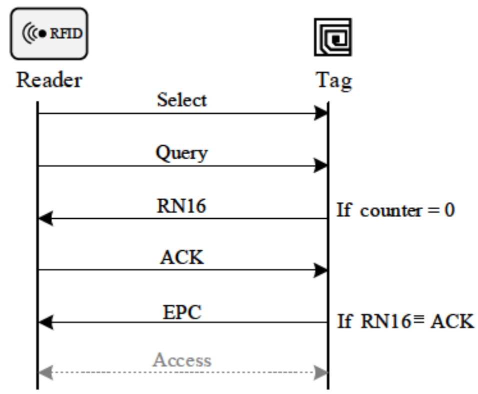


Fig. 23: RFID tag inventory and access processes.

computation and RF signal transmission. Active tags, on the other hand, use battery to drive their computation and RF circuits.

Fig. 23 shows the medium access protocol used in GEN2 UHF RFID communications [188]. Generally speaking, in an RFID system, a reader (interrogator) manages a set of tags following a protocol that comprises the following three phases:

- *Select:* The reader selects a tag population by sending *select* commands, by which a group of tags are informed for further inquiry process.
- *Inventory:* In this phase, the reader tries to identify the selected tags. The reader initializes the inventory rounds through issuing *Query* commands. The reader and RFID tags communicate using a slotted ALOHA medium access mechanism. Once a new-selected tag receives a Query command, it sets its counter to a pseudo-random number. Every time a tag receives the Query command, it decreases its counter by 1. When the tag's counter reaches zero, it responds to the reader with a 16-bit pseudo-random sequence (RN16). The reader acknowledges the RN16 signal reception by regenerating the same RN16 and sending it back to the tag. When a tag receives the replied RN16 signal, it compares the signal with the original transmitted one. If they are matched, the tag will broadcast its EPC, and the reader will identify the tag.
- *Access:* When the inventory phase is completed, the reader can access the tag. In this phase, the reader may write/read to/from the tag's memory, kill, or lock the tag. From a PHY-layer perspective, an UHF RFID readers use pulse interval encoding (PIE) and DSB-ASK/SSB-ASK/PR-ASK modulation for its data transmission, while a UHF RFID tag uses FM0 or Miller data encoding and backscattering for carrier modulation. Moreover, the required energy for the tag's backscattering is delivered via the reader's continuous wave (CW) transmissions [189].

B. Jamming Attacks

Since RFID communication is a type of wireless communications, it is vulnerable to generic jamming attacks such as constant, reactive, and deceptive jamming threats. In [190], Fu et al. investigated the impact of constant jamming attack on UHF RFID communications and evaluated the system performance through a simulation model. The results in [190] showed that when the received RFID reader signal power is 0 dBm, the received jamming signal power of -15 dBm will be sufficient to break down the RFID communications.

Per [191], Zapping attack is one of the well-known security attacks to RFID tags, in which an attacker aims to disable the function of RF front-end circuits in RFID tags. In a Zapping attack, a malicious attacker produces a strong electromagnetic induction through the tag's circuit by generating a high-power signal in the proximity of the tag's antenna. The large amount of energy a tag receives may cause permanent damage to its RF circuits.

RFID tags are recently used for electronic voting systems in many countries across the world. In such voting systems, the votes are written through electronic RFID tags instead of conventional ballot voting papers. Electronic voting systems were originally designed to improve the accuracy and speed of the vote-counting process. Given the importance of voting services, research on RFID security receives a large amount of attention from academia and industry. In [192] and [193], Oren et al. studied two main security threats on RFID communications: jamming and zapping attacks. The authors studied these two jamming attacks and evaluated their performances in terms of their maximum jamming ranges. The author also investigated the impact of a jammer's antenna type on its jamming effectiveness. It was shown that a helical antenna yields a larger jamming range compared to a hustler or 39 cm loop antenna.

C. Anti-Jamming Techniques

Unlike other types of wireless networks, securing RFID communication against jamming attacks is a particularly challenging task due to the passive nature of RIFD tags or low-energy supply of RFID tags. Generic anti-jamming techniques (e.g., MIMO-based jamming mitigation, spectrum spreading, and frequency hopping) appear ineffective or unsuitable for RFID systems.

In [194], Patel et al. proposed a jamming detection algorithm for RFID communications. The proposed algorithm traces the packet delivery ratio, the packet sent ratio, and the received signal strength to identify the jamming attack. Most of existing works focus on authentication issues in RFID networks. For example, Wang et al. in [195] proposed an authentication scheme to cope with RFID replay attack. Avanco et al. in [196] proposed a low-power jamming detection mechanism in RFID networks. The proposed mechanism detects malicious activities within the network by exploiting side information such as the received signal power in adjacent channels, the received preamble, and the tag's uplink transmission response.

X. Jamming and Anti-Jamming Attacks in GPS Systems

In this section, we survey jamming and anti-jamming attacks in the Global Positioning System (GPS). By the same token, we first offer a primer of GPS communication system and then review existing jamming/anti-jamming attacks deliberately designed for GPS systems.

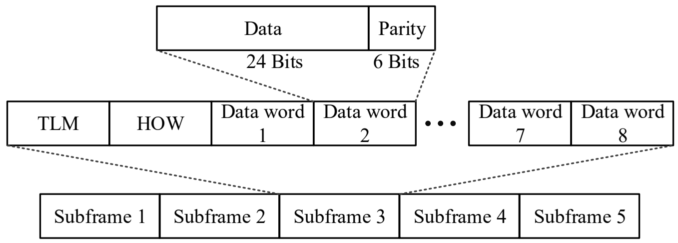


Fig. 24: GPS navigation message frame structure.

A. A Primer of GPS Communication System

GPS was designed to provide on-earth users with an easy way of obtaining their location and timing information by establishing a set of satellites that continuously orbit around the earth and broadcast their location and timing information. In GPS, an on-earth user first acquires a satellite's time and location information and then estimate the distance (a.k.a. pseudo-range) from the satellite to itself by calculating the time of signal travel. The on-earth user's geographical location can be determined mathematically, considering the locations and estimated pseudo ranges of multiple satellites. As such, wireless communication in GPS is one-way communication.

Fig. 24 shows the structure of a GPS navigation message, which consists of 5 equally-sized subframes. Each subframe is composed of 10 data words, consisting of 24 raw data bits followed by 6 parity bits. The first data word in each subframe is the telemetry (TLM) word, which is a binary preamble for subframe detection. It also carries administrative status information. Following the TLM word is Handover (HOW) word and carries GPS time information, which is used to identify the subframe. Subframe 1 carries the information required for clock offset estimation. Subframes 2 and 3 consist of satellite ephemeris data that can be used by the users to estimate the satellite's location at a particular time accurately. Subframes 4 and 5 carry almanac data that provides information on all satellites and their orbits on the constellation.

The navigation message is sent at 50 bps data rate. All GPS satellites operate in 1575.42 MHz (L1 channel) and 1227.60 MHz (L2 channel) and use one of the following signaling protocols:

- *Course Acquisition (C/A) Code:* C/A signal uses a direct sequence spread spectrum (DSSS) with a 1023-chip pseudo-random spreading sequence, which is replicated 20 times to achieve higher spreading gain. The main lobe C/A signal bandwidth is 2 MHz and the spreading gain is $10 \times \log_{10}(20 \times 1023) \approx 43$ dB. The C/A signal is transmitted over the L1 frequency channel and is mainly used to serve civilian users.
- *P-Code:* P-code signal also uses spreading spectrum. The length of its spreading code is $10,230$ chips per bit. P signal is more spread over the frequency and can achieve higher spreading gain (≈ 53 dB) than the C/A signal. The signal bandwidth is 20 MHz for the P-code signal. P

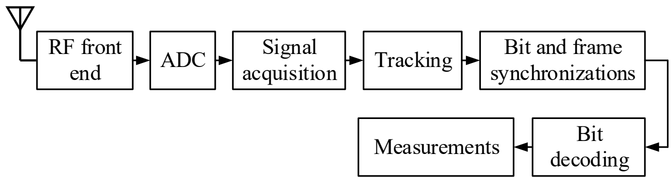


Fig. 25: The schematic diagram of a GPS receiver [197]

signal can be transmitted over both L1 and L2 channels and used by the US Department of Defense to serve authorized users.

Fig. 25 shows the structure of a GPS receiver. When a GPS device receives GPS signal from satellites, it uses a signal acquisition module to identify the corresponding satellites. The signal acquisition will be made using C/A code correlation and exhaustive search over a possible range of Doppler frequencies. The tracking module modifies the coarse changes in the phase and frequency of the acquired signal. Following the phase and frequency tracking, the received chips are synchronized and demodulated into bits that are used for measurement.

B. Jamming Attacks

Given that GPS is a one-way communication system, the potential jamming threat in GPS is mainly posing on on-earth GPS user devices. Since GPS satellites are very far from earth, on-earth GPS signals can be easily drowned by jamming signals. Table X summarizes some jamming attacks on GPS communications. We divide the jamming attacks on GPS communications into three categories: *jamming in vehicular networks*, *jamming in maritime systems*, and *jamming in phasor measurement units (PMUs)*. We elaborate them in the following.

Vehicular Systems: In [198], Mitch et al. studied the characteristics of 18 COTS GPS jammers through an extensive experiment. The studied GPS jammers were classified into three categories: *Cigarette Lighter Jammers*, *SMA-Battery Jammers*, and *NonSMA-Battery Jammers*. *Cigarette Lighter Jammers* are powered by the 12V vehicle cigarette lighter. They are designed to send jamming signals on L1 frequency. The frequency sweeping range varies from 3.2 MHz to 5.9 MHz to investigate the jammers in this class. And the measured in-band power ranges from 0.1 mW to 23 mW depending on the signal bandwidth. *SMA-Battery Jammers* are powered by battery and equipped with SMA antennas. This class of GPS jammers are designed to work on L1 frequency. The frequency sweeping range varies from 0.8 MHz to 23.2 MHz, and the maximum transmission power is 642 mW for 10 jammers in this class. *NonSMA-Battery Jammers* are also powered by battery but are not equipped with external antennas. This type of GPS jammers is designed to work on both L1 and L2 frequencies. The measured in-band powers are, however, much lower than the SMA-Battery jammers. Their maximum power is 4.95 mW on L1 frequency and 7.74 mW on L2 frequency.

Maritime Systems: In [199], Glomsvoll studied the performance of a maritime GPS receiver in the face of jamming attacks. A wide-band commercial off-the-shelf radio jammer on L1 carrier frequency has been used to jam an on-board GPS signal. The jamming signal bandwidth was set to 60 MHz, and its transmit power was measured to -35 dBW. Carrier-to-Noise Ratio (CNR) was used to measure the received GPS signal strength. CNR is a bandwidth-independent metric expressed as the ratio of carrier power to noise power per hertz. It was shown that, for stationary and semi-stationary GPS receivers, a CNR ranging from 30 to 35 dB/Hz suffices for signal detection. In a jamming-free scenario, it was measured that the CNR is 44 dB/Hz at a GPS receiver. In [200], Grant et al. summarized results of the experiments conducted by General Lighthouse Authorities (GLA) on the performance of a Northern Lighthouse Board (NLB) vessel GPS receiver under jamming attacks. In the experiments, the jammer sends constant jamming signals on L1 frequency over 2 MHz bandwidth. The maximum jammer's power is 2 dB. The experimental results showed that the receiver cannot successfully decode the GPS signal when the vessel moves within the jamming signal main lob and its distance is less than 25 m.

Phasor Measurement Units (PMUs): In addition to global localization, the GPS system provides a time reference for GPS receivers. This time information provides a time source in the range of microsecond to seconds for interoperability of many applications and system components such as phasor measurement units (PMUs) [201]. PMUs are GPS-synchronized systems that real-time measure and analyze electrical signal flows in power grids. Per [202], jamming attacks on GPS communications introduce a security vulnerability for PMUs, as they rely on GPS communications for timing synchronization. In [203], Hoffer et al. studied the impact of GPS connection loss on PMUs caused by jamming attacks. Per [203], PMUs cannot successfully extract a model for the electric power system under jamming attacks, thereby failing to allocate resources for operating system. This may result in power outage in specific areas.

C. Anti-Jamming Attacks

Since the GPS communication system employs the spectrum spreading technique for data transmission, it bears 43 dB spreading gain for C/A code (civilian use) and 52 dB spreading gain for P-code (military use). The spreading gain enables a GPS receiver to combat jamming attacks to some extent. In addition to its inherent spectrum spreading technique, other anti-jamming techniques (e.g., MIMO-based jamming mitigation) can also be used to improve its resilience to jamming attacks. In what follows, we review existing anti-jamming attacks for GPS in the literature, which are summarized in Table X.

Jamming Signal Filtering: In [204], Zhang et al. proposed to enhance a GPS receiver's resilience to jamming attack by designing a filtering mask in both time and frequency domains. Such a filtering mask uses the time and frequency distributions of the jamming signal to suppress its energy while allowing GPS signals to pass. In [205], an adaptive notch filter was designed to detect, estimate, and block single-tone continuous jamming signals. Their proposed notch filter used a second-order IIR filter designed in the time domain. In [206], Rezaei

TABLE X: A summary of jamming attacks and anti-jamming strategies in GPS systems.

	Ref.	Description	Strengths	Weaknesses
Jamming attacks	[198]	Cigarette lighter COTS GPS jammers	Cheap	Less effective
		SMA-battery COTS GPS jammers	Highly effective	Working on L1 only
		Non SMA-battery COTS GPS jammers	Working on L1/L2	Less effective
	[199], [200]	Wide-band COTS GPS jamming attacks on maritime systems	Highly effective	Less stealthy
	[201]–[203]	GPS jamming attack on PMUs	Highly effective	Less stealthy

	Ref.	Description	Application scenario
Anti-jamming techniques	[204]	Time-frequency mask design using distributions of jamming signals	Narrowband FM radio jamming signal
	[205]	Adaptive notch filter design for jamming detection and blocking	Single-tone continuous jamming attack
	[206]	STFT-based notch filter design	Single-tone continuous jamming attack
	[207]	Approximate conditional mean and discrete wavelet transform filters design	Narrowband FM radio jamming signal
	[208]	Adaptive antenna array design	Wideband/narrowband constant jamming attacks
	[209]	Adaptive antenna system design based on pattern and polarization diversity	Wideband constant jamming attack
	[210]	Adaptive array-based design with negligible phase distortion	Continuous wave/broadband jamming attacks
	[211]	Analog beamforming design using inherent self-coherence feature of the GPS signals	Broadband binary jamming attack
	[212]	Self-coherence beamforming design	Noise-like constant jamming attack
	[213]	Signal projection onto the orthogonal space of jamming signal	Noise-like constant jamming attack
	[214]	Spatial-temporal interference projection mechanism	Narrowband FM radio jamming signal
	[215]	Regret minimization framework	Constant jamming attack
	[216]	Multi-sensor fusion and Kalman filtering	Noise-like constant jamming attack
	[217], [218]	Position-information-aided vector tracking approach	Constant jamming attack

et al. aims to enhance the capability of notch in jamming mitigation filter for a GPS receiver. The authors proposed to use the short-time Fourier transform (STFT) to increase the time and frequency domain resolution.

In [207], Rao et al. proposed to secure GPS communications against FM radio jamming signals using an approximate conditional mean (ACM) filter followed by a discrete wavelet transform (DWT) filter. Their simulation results demonstrated that the designed DWT filter is capable of delivering above 30 dB SNR when the JSR (jamming-to-signal power ratio) keeps sweeping from 15 dB to 55 dB. The designed ACM filter also could achieve at least 15 dB SNR when JSR increased to 55 dB.

Antenna Array Design: Antenna array processing is another technique that is used by GPS receivers to enhance their jamming resilience [208]. In [209], Rezazadeh et al. designed an adaptive antenna system by leveraging the antenna's pattern and polarization diversity to nullify the jamming signal in airborne GPS applications. The authors built a prototype of the designed antenna and evaluated its performance in the presence of jamming attack. Their experimental results showed that the implemented antenna is capable of achieving up to 38 dB jamming suppression gain. In [210], Zhang et al. studied the challenges associated with the antenna array design for GPS receiver. The authors proposed an array-based adaptive anti-jamming algorithm to suppress jamming signal with negligible phase distortion. In [211], Sun et al. harnessed the inherent self-coherence feature of GPS signal to mitigate the jamming signal, as the GPS signal repeats 20 times within each symbol. In [212], a beamforming technique was designed as an anti-jamming solution for GPS communications. A spectral self-coherence beamforming technique was proposed to design a weight vector to nullify the jamming signal and improve the desired signal detection.

A similar idea was explored in [213], where the received signal is first projected onto the jamming signal's orthogonal space, and a so-called CLEAN method [219] was used to extract the received GPS signals. The CLEAN method is a classical approach that iteratively computes the beamforming vectors to identify the arrival direction of the signals of interest. It uses the repetitive pattern of the C/A code to construct the beamforming vectors. The authors evaluated the performance of their proposed anti-jamming technique via both computer simulations and real-world experiments. They considered four GPS signals arriving at different directions and a continuous wave jamming signal. The simulation results demonstrated that their proposed algorithm could successfully acquire the 4 GPS signal streams when jamming signal power to noise power ratio (JNR) is 40 dB. Their experimental results show that, using a 4-antenna array plane, the proposed receiver can correctly determine its position when JNR is 20 dB.

In [214], Amin et al. designed a spatial-temporal interference projection mechanism to secure GPS C/A signal against FM jamming signal. The proposed scheme jointly estimates the jamming instantaneous frequency (IF) and orthogonal jamming signal subspace to suppress the jamming signal. The authors showed that the temporal correlation coefficient between FM jamming signal and GPS C/A code is small due to differences in their signal characteristics, which allows multi-sensor receiver to mitigate jamming signal regardless of its angle of arrival.

Game-Theoretical Approaches:

Unlike other wireless technologies, satellite communications suffer from significant delay as the signal travels a long distance from a satellite to a ground station (or vice versa). Such large propagation delays pose grand challenges in the spectrum sensing for cognitive users. In [215], Sagduyu et al. studied the spectrum access problem in satellite communications under jamming attacks. The authors formulated a regret minimization framework and developed a game-theoretical approach to model the interactions between the parties. In the studied model, the users update their strategies based on random defined functions that reflect the impact of delay randomness on reward and cost functions in channel reservation. It was shown that the proposed regret minimization framework can achieve a low-complex and fast-convergence solution to the studied problem. The authors built an emulation testbed using USRP radios and a channel emulator, and validated the performance of the proposed scheme in terms of throughput.

Anti-jamming Strategies for Maritime Systems and PMUs:

In [220], Medina et al. studied the potential countermeasures for maritime GPS systems against jamming attacks. They divided the techniques into three categories. First, an alternative terrestrial system can be used to provide navigation information for the receivers. A backup navigation system, called R-Mode, has already been devised to serve as an alternative solution for maritime applications. Second, the signal processing approaches can be adopted to suppress the jamming signal. Such techniques have been discussed earlier in this section. Third, the received signal from multiple sensors can be fused to mitigate the impact of jamming signal. Per [220], Kalman filter is a well-known technique to realize a multi-sensor fusion system. In [216], Caron et al. proposed a multi-sensor fusion scheme using Kalman filter to detect and reject false inputs, thereby increasing the reliability of the system. The authors used two sensors, one GPS sensor and one inertial navigation system (INS), in their design. The simulation results showed that the proposed scheme can improve the positioning accuracy by more than 60%.

In [217] and [218], the authors proposed a position-information-aided (PIA) vector tracking approach to secure PMUs against jamming attacks. In the proposed scheme, multiple co-located receivers are connected to a common clock source to synchronize the clock frequency at the receivers. The receivers independently process the signals and feed the results into a Kalman filter for navigation estimation. Then, a PIA Vector Tracking Loop was used to estimate the final clock solution. The authors implemented their approach on a USRP-based testbed and measured the clock error values when an artificial noise is added into the system. They used four USRPs (sensors) each connected to a GNSS navigation antenna and placed them on a roof top. The results demonstrated that the clock error in their proposed scheme increases from 1.5ns to 7ns when 11 dB noise figure is added, while a single receiver stops working after adding 8 dB noise. The clock errors for their proposed scheme and the single sensor scenario are 2ns and 20ns when 4 dB noise is added to the system, respectively.

A Summary of Anti-Jamming Techniques: Table X summarizes existing jamming attacks and anti-jamming strategies for GPS communications. The proposed anti-jamming techniques can be classified into three categories: *filtering (masking) design*, *antenna phase array techniques*, and *signal-processing-based multi-sensor fusion*. The filtering and masking techniques were designed to secure GPS communications against narrow-band or single-tone jamming attacks. Antenna phase array and analog beamforming techniques could deliver significant gains in jamming nullification. They, however, rely on training phases and time-frequency signal properties such as operating carrier frequency and channel bandwidth. Multi-sensor fusion techniques used Kalman filtering and were implemented for PMUs and maritime systems to secure their GPS connections.

XI. Jamming and Anti-Jamming Attacks in Emerging Wireless Systems

In this section, we overview jamming attacks and anti-jamming strategies in emerging wireless technologies. We first present jamming and anti-jamming for learning-based wireless systems and learning-based adversarial jamming attacks on wireless communications. Second, we study jamming attacks and anti-jamming techniques in mmWave communications.

A. Jamming and Anti-Jamming for Learning-Assisted Wireless Systems

The vulnerability of learning-based communication systems to physical adversarial attacks have been studied in [221]–[224], where the attacker attempts to add a well-optimized signal to the input of machine learning systems to break learning model. In [221], Sadeghi et al. proposed an algorithm to design physical adversarial perturbations against an end-to-end auto-encoder wireless system. The authors showed that the designed adversarial attack is more destructive compared to noise-like constant jamming attacks. In [222], Kim et al. studied an adversarial attack on a learning-based classifier of wireless signal modulation. Specifically, the authors considered a wireless link between a legitimate transmitter and a receiver, and proposed two adversarial attacks that attempt to alter the classifier outputs by falsifying modulation labels.

In [223], Sagduyu et al. proposed a learning-based adversarial attacker that attempts to interrupt the spectrum sensing of a legitimate transmitter. The proposed attacker learns the behavior of the legitimate transmitter in accessing the medium and attempts to jam the ACK transmissions, thereby forcing the legitimate transmitter to make wrong decisions or retrain its model. In addition, a defense mechanism was proposed to secure the legitimate link against the designed attack. The proposed countermeasure scheme adopts false strategies in the chosen time slots to fool the learning model of the attacker.

In [225], Zhong et al. proposed two learning-based adversarial attacks to minimize the performance of a legitimate user in channel access. In the proposed framework, the user implements a dynamic channel access mechanism using an actor-critic deep reinforcement learning (DRL). The attacker sends a jamming signal to a single channel in each time slot to reduce the accuracy of the user's channel selection. The authors used a feed-forward neural network (FNN) and a DRL method to design the attacker's strategies for jamming signal transmissions. In the DRL-based attack, the attacker has no prior knowledge about the user's channel selection policies and updates its strategies based on its observations. The simulation results showed that the proposed FNN-based and DRL-based jamming attacks decrease the accuracy of the user's channel selection by 50% and 20%, respectively.

In [226], Abuzainab et al. proposed a learning-based solution for a distributed wireless network that allows users to cooperatively maximize network performance in terms of throughput, delay, and energy efficiency while securing them against jamming and eavesdropping attacks. The key enabler of the proposed scheme is a deep reinforcement learning approach that selects the users' actions so the performance of the networks will be optimized. The authors defined three actions that a user can apply in different scenarios: i) it may participate in data transmissions; ii) it may attack the eavesdropper by sending a jamming signal; and iii) it may secure the network. In order to secure the network against jamming attacks, the authors proposed a routing protocol that allows the users to create new paths for jamming avoidance.

B. Jamming and Anti-Jamming on mmWave Communications

Research on mmWave has recently received tremendous attention from both academia and industry, as it features a wide bandwidth and promises multi-Gbps data rate over a single link. Despite its huge potential for network capacity, mmWave is of unique over-the-air propagation characteristics that introduces new security challenges. In what follows, we provide ab overview of jamming attacks and anti-jamming strategies in mmWave systems.

In [227], Zhu et al. studied jamming attacks on mmWave MU-MIMO systems and proposed a hybrid beamforming design that allows users to recover their intended signals in the face of jamming signal. In particular, analog beamforming vectors are designed to nullify jamming signal at each user while digital beamforming vectors are designed to cancel inter-user interference. The authors formulated the hybrid beamforming design as a sum-rate maximization problem and proposed a sub-optimal solution. Their simulation results showed that the achievable sum rate of the system is not affected when the received jamming SNR is swept from 0 dB to 30 dB and the received user's SNR is 25 dB.

In [228], Xiao et al. studied the performance of the mmWave massive MIMO systems under smart jamming attacks. The authors proposed a learning-based power allocation mechanism for massive-antenna BS and evaluated the impact of the number of transmit antennas on network achievable sum rate. Particularly, the authors considered downlink MU-MIMO mmWave communications. They formulated the interaction between the BS and smart jammer as a Markov decision process and adopted a reinforcement learning approach to pursue an optimal anti-jamming power control solution.

In [229], Cai et al. proposed a joint beamforming and jamming design for a mmWave surveillance system, where a surveillance controller monitors and jams a suspicious communication link. The authors formulated the controller's analog monitoring and jamming beamforming design as an optimization problem to maximize the non-outage probability of the controller's monitoring and minimize its jamming signal power. The authors employed a penalty dual decomposition (PDD)-based mechanism to solve the optimization problem.

In [230], Bagherinejad et al. proposed to use directional information of users to detect and suppress jamming attacks in mmWave massive MIMO systems. In particular, the authors took advantage of the high angular resolution achieved by massive MIMO base stations to accurately detect the existence and direction of jammer. In this scheme, when a jammer uses one of legitimate pilots in the training phase, the base station will receive that pilot from two different directions. This fact is then used for designing a robust receiver at the base station that can successfully mitigate the jammer's effect.

XII. Open Problems and Research Directions

In this section, we first highlight the lessons and experience we learned, and then list some important open problems facing the design of effective anti-jamming techniques. Finally, we point out some promising research directions towards securing wireless communications against jamming attacks.

A. Lesson Learned

Table XI summarizes the existing anti-jamming strategies, their weaknesses, and their main applications. Despite the advancement of wireless technologies and the research efforts on the design of anti-jamming techniques, real-world wireless network systems are still vulnerable to jamming attacks. In other words, there are no effective anti-jamming techniques that are ready for deployment in real-world wireless systems. For example, commercial WiFi and cellular Internet services can be easily disrupted by malicious jamming emitters. This reality motivates us to rethink the missing parts in this field. Some lessons we learned from this survey and our own anti-jamming design are presented below.

Anti-Jamming Design is beyond Signal Detection: A wireless receiver has several key components of both analog and digital circuits to decode the data packets in the presence of jamming signals. The analog components include power amplifiers, mixer, filters, ADC; and the digital components include packet detection, frequency synchronization, timing recovery, and signal detection. In the literature, the majority of anti-jamming work focuses solely on the anti-jamming signal detection. The impacts of jamming signals on the analog components and other digital components are highly overlooked. For example, in the analog domain, when the jamming signal is strong, it will saturate the dynamic range of ADC, resulting in a significant quantization noise for the useful signal in the digital domain. In the digital domain, the frequency and timing offsets of a packet should be accurately estimated and compensated in order to decode this packet. However, these digital components are vulnerable to jamming signals. Therefore, jamming-resilient frequency/timing recovery digital modules are needed to decode the packets, which are not well studied in the literature. Simply put, securing wireless communications against jamming attacks cannot be limited to a single component (signal detection); rather, it needs a holistic and systematic design of a receiver to mitigate the impacts of jamming signals in its analog and digital components.

Computational Complexity is a Key Factor: Different from other attacks, jamming attacks must be coped with at the physical layer by a wireless receiver. Since the digital signal processing modules of a radio transceiver is typically implemented through ASIC, computational complexity must be taken into account for massive production. Therefore, it is desired to have anti-jamming solutions of a low/acceptable

TABLE XI: A summary of anti-jamming strategies in the literature.

Anti-jamming Strategies	Ref.	Limitations	Applications
Frequency-Hopping Spread Spectrum	[152], [153] [154]–[156]	Vulnerable to broadband jamming attack Vulnerable to key establishment procedure Spectrum inefficient	Bluetooth
Chirp Spread Spectrum	[157], [164], [231]	Spectrum inefficient	LoRa
Direct Sequence Spread Spectrum	[133], [138] [137], [139]	Spectrum inefficient	ZigBee/802.11b
MIMO-based Techniques	[46], [47], [77] [108], [137], [177]	Extra hardware required	Cellular/WLANs/VANETs/ZigBee
Antenna Phase Array & Analog Beamforming Techniques	[208], [209], [232] [212]–[214]	Extra hardware required	GPS
Rate Adaptation Algorithms	[66], [80] [81]	Ineffective against high-power jamming attacks	Cellular/WLANs
Power Control Mechanisms	[80], [81]	Ineffective against high-power jamming attacks	Cellular/WLANs/ VANETs/CRNs
Relay Aided Strategies	[96], [173], [174]	Alternative infrastructure requirements	Cellular/VANETs
Channel Re-selection Mechanisms	[120]–[122] [123], [124]	Ineffective against broadband and sweeping jamming attacks	CRNs
Packet Fragmentation & Fragment Replication	[50], [142], [199]	Ineffective against constant jamming attacks	WLANs/GPS/ ZigBee
Channel Coding Schemes	[78], [79]	Ineffective against high-power jamming attacks	Cellular/WLANs/ VANETs/LoRa
Filtering & Masking Techniques	[204]–[206]	Effective for single-tone jamming attacks only	GPS

computational complexity. Sophisticated digital signal processing schemes, albeit offering superior performance, may not be suited for real-world wireless transceivers.

Tradeoff Between Spectrum Efficiency and Jamming Resiliency: Spectrum efficiency and jamming resiliency are two conflicting factors in the design of jamming-resilient wireless communication systems. For example, spectrum spreading tends to offer a better resiliency to jamming attacks if a larger spreading factor is used. But using a large spreading factor will reduce the spectrum efficiency. This is the same for frequency hopping techniques. Therefore, spectrum efficiency should be taken into account when analyzing an anti-jamming technique, and a tradeoff between these two should be sought in the course of anti-jamming design.

B. Open Problems

Despite the significant advancement of wireless communication and networking technologies in the past decades, real-world wireless communication systems (e.g., Wi-Fi, cellular, Bluetooth, ZigBee, and GPS) are still vulnerable to malicious jamming attacks. As wireless services become increasingly important in our society, the jamming vulnerability of wireless Internet services poses serious security threats to existing and future cyber-physical systems. This vulnerability can be attributed to the lack of practical, effective, and efficient anti-jamming techniques that can be deployed in real-world wireless systems to secure wireless communication against jamming attacks. One may argue that Bluetooth is equipped with the frequency hopping technique, and ZigBee/GPS is equipped with spectrum spreading technique, and (therefore) these networks can survive in the presence of jamming attacks. This argument, however, is not valid. Bluetooth can only work in the face of narrow-band jamming attack, and ZigBee/GPS can only work under a low-power jamming attack. These wireless systems as well as the most prevailing Wi-Fi and cellular networks, can be easily paralyzed by a jamming attack using commercial off-the-shelf SDR devices.

In what follows, we describe some open problems in the design of anti-jamming techniques, with the aim of spurring more research efforts on advancing the design of jamming-resistant wireless communication systems.

1) Effectiveness of Anti-Jamming Techniques: One open research problem is to design effective anti-jamming techniques for wireless networks. Existing anti-jamming techniques (e.g., frequency hopping, spectrum spreading, retransmission, and MIMO-based jamming mitigation) have a limited ability to tackle jamming attacks. For example, neither frequency hopping nor spectrum spreading technique is able to salvage wireless communication services when jamming signal is covering the full spectrum and stronger than useful signal. The state-of-the-art MIMO-based technique can offer at most 30 dB jamming mitigation capability for two-antenna wireless receivers. This indicates that if jamming signal is 22 dB stronger than the useful signal, the receivers in a wireless network will not be capable of decoding their packets under jamming attacks. Therefore, a natural question to ask is how to design effective anti-jamming techniques for wireless networks so that those wireless networks can be immune to jamming attacks, regardless of jamming signal power, bandwidth, sources, and other configuration parameters.

2) Efficiency of Anti-Jamming Techniques: Another open problem is to improve the efficiency of anti-jamming techniques. For example, frequency hopping can cope with narrow-band jamming attacks, but it significantly reduces spectral efficiency. Bluetooth uses frequency hopping to be immune to unknown interference and jamming attack, at the cost of using only one of 79 channels at one time. Spectrum spreading technique has been used in ZigBee, GPS, and 3G cellular networks. It allows these networks to be immune to low-power jamming attacks. However, their jamming immunity does not come free. It significantly reduces the spectral efficiency by expanding the signal bandwidth using a spreading code. Retransmission may be salvage wireless communication, but it also reduces the communication efficiency in the time domain. MIMO-based jamming mitigation also lowers the spatial degrees of freedom that can be used for useful signal transmission. Therefore, a question to ask is how to improve the communication efficiency of wireless networks when they employ anti-jamming techniques to secure their communications. As expected, the jamming resilience will not come for free. A more reasonable question is how to achieve the tradeoff between communication efficiency and jamming resilience of a wireless network.

3) Practicality of Anti-Jamming Techniques: An important problem that remains open is to bridge the gap between theoretical study (or model-based analysis) and practical implementation. In the past decades, many research works focus on the theoretical investigation of anti-jamming techniques using approaches such as game theory and cross-layer optimization. Despite offering insights to advance our understanding of anti-jamming design, such theoretical results cannot be deployed in real-world wireless network systems due to their unrealistic assumptions (e.g., availability of global channel information, prior knowledge of jamming actions) and prohibitively high computational complexity. Securing real-world wireless networks (e.g., Wi-Fi, cellular, ZigBee, Bluetooth, and GPS) calls for the intellectual design of anti-jamming strategies that can be implemented in realistic wireless environments where computational power and network-wide cooperation are limited. Particularly, PHY-layer anti-jamming techniques have a stringent requirement on their computational complexity. This is because PHY-layer anti-jamming techniques should have an ASIC or FPGA implementation in modern wireless chips, which have a strict delay constraint for decoding each packet.

4) Securing Wireless Communication System by Design: A conventional anti-jamming approach for wireless communication systems is composed of the following three steps: i) wireless devices detect the presence of jamming attacks, ii) wireless devices temporarily stop their communications and invoke an anti-jamming mechanism, and iii) wireless communication resumes under the protection of its anti-jamming mechanism. This approach, however, is not capable of maintaining constant wireless connection under jamming attack due to the separation of jamming detection and countermeasure invocation, and the disconnection of wireless service may not be intolerable in many applications such as surveillance and drone control on the battlefield. Realizing this limitation, securing wireless communication *by design* has emerged as an appealing anti-jamming paradigm and attracted a lot of research attention in recent years. The basic idea behind this paradigm is to take into account the anti-jamming requirement in the original design of wireless systems. By doing so, a wireless communication system may be capable of offering constant wireless services without disconnection when suffers from jamming attacks. For this paradigm, many problems remain open and need to be investigated, such as the way of designing anti-jamming mechanisms and the way of striking a balance between communication efficiency and jamming mitigation capability.

C. Research Directions

Jamming attack is arguably the most critical security threat for wireless communication networks as it is easy to launch but hard to thwart. The limited progress in the design of jamming-resilient wireless systems underscores the grand challenges in the innovation of anti-jamming techniques and the critical need for securing wireless networks against jamming attacks. In what follows, we point out some promising research directions.

1) MIMO-based Jamming Mitigation: Given the potential of MIMO technology that has demonstrated in Wi-Fi and 4/5G cellular networks, the exploration of practical yet efficient MIMO-based jamming mitigation techniques is a promising research direction towards securing wireless networks and deserves more research efforts. The past decade has witnessed the explosion of MIMO research and applications in wireless communication systems. With the rapid advances in signal processing and antenna technology, MIMO has become a norm for wireless devices. Most commercial Wi-Fi and cellular devices such as smartphones and laptops are now equipped with multiple antennas for MIMO communication. Recent results in [77] show that, compared to frequency hopping and spectrum sharing, MIMO-based jamming mitigation is not effective in jamming mitigation but also efficient in spectrum utilization. In addition, the existing results from the research on MIMO-based interference management (e.g., interference cancellation, interference neutralization, interference alignment, etc.) can be leveraged for the design of MIMO-based anti-jamming techniques. In turn, the findings and results from the design of MIMO-based anti-jamming techniques can also be applied to managing of unknown interference (e.g., blind interference cancellation) in Wi-Fi, cellular, and vehicular networks.

2) Cross-Domain Anti-Jamming Design: Most existing anti-jamming techniques exploit the degree of freedom in a single (time, frequency, space, code, etc.) domain to decode in-the-air radio packets in the presence of interfering signals from malicious jammers. For instance, channel hopping, which is used in Bluetooth, manipulates radio signals in the frequency domain to avoid jamming attack; spectrum spreading employs a secret sequence in the code domain to whiten the energy of narrow-band jamming signal to enhance a wireless receiver's resilience to jamming attacks; MIMO-based jamming mitigation aims to project signals in the spatial domain so as to make useful signal perpendicular to jamming signals. However, these single-domain anti-jamming techniques appear to have a limited ability of handling jamming signals due to a number of factors, such as the available spectrum bandwidth, the computational complexity, the number of antennas, the resolution of ADC, the nonlinearity of radio circuit, and the packet delay constraint. One research direction toward enhancing a wireless network's resilience to jamming attacks is by jointly exploiting multiple domains for PHY-layer signal processing and MAC-layer protocol manipulation. This direction deserves more research efforts to explore practical and efficient anti-jamming designs.

3) Cross-Layer Anti-Jamming Design: For constant jamming attacks, most existing countermeasures rely on PHY-layer techniques to avoid jamming signal or mitigate jamming signal for signal detection. With the growth of smart jamming attacks that target on specific network protocols (e.g., preamble/pilot signals in Wi-Fi network and PSS/SSS in cellular network), cross-layer design for anti-jamming strategies becomes necessary to thwart the increasingly sophisticated jamming attacks. It calls for joint design of PHY-layer signal processing, MAC-layer protocol design, and network resource allocation as well as cross-layer optimization to enable efficient wireless communications in the presence of various jamming attacks.

4) Anti-Jamming techniques for mmWave Networks: With the depletion of sub-6GHz spectrum, pushing wireless communications onto mmWave spectrum is an inevitable trend, which has already produced a large amount of research results, industry development, and commercial applications. Compared to sub-6GHz communications, mmWave communications have very different channel characteristics and very different system settings (e.g., analog beamforming, directional antennas, and large bandwidth). Therefore, it is important to understand the effectiveness and destructiveness of various jamming attacks in mmWave networks, as well as develop and experimentally validate new anti-jamming solutions to secure mmWave communications in both indoor and outdoor environments.

5) Machine Learning for Anti-Jamming Design: Machine learning has become a powerful technique and has been applied to many real-world applications such as image recognition, speech recognition, traffic prediction, product recommendations, self-driving cars, email spam, and malware filtering. It is particularly useful for solving complex engineering problems whose underlying mathematical model is unknown. In recent years, machine learning techniques have been used to secure wireless communications against jamming attacks (e.g., [174], [233]) and produced some pioneering yet exciting results. Therefore, the design of learning-based anti-jamming techniques is a promising research direction that deserves more research efforts for an in-depth investigation.

6) Intelligent Reflecting Surface (IRS) for Anti-Jamming Applications: IRS is widely regarded as a promising technology to improve the quality of wireless links. It can reconstruct over-the-air wireless channels using reconfigurable passive or active electronic components to control radio-wave reflection. In mmWave communication systems, the presence of IRS makes it possible to constructively combine the incident signals to the surface at the user side, achieving a 3D beamforming gain, by carefully adjusting the phase shifts of a large number of low-cost passive elements [234]. Recently, IRS-assisted techniques have been proposed to mitigate the impact of jamming signals for a wireless link (e.g., [235], [236]). It would be interesting and important to explore the potential of IRS techniques for securing wireless communications against jamming attacks.

XIII. Conclusion

This survey article provides a comprehensive review of jamming attacks and anti-jamming techniques for Wi-Fi, cellular, cognitive radio, ZigBee, Bluetooth, vehicular, RFID, and GPS wireless networks, as well as for emerging learning-based and mmWave wireless systems. For each network, we first offered a primer of its PHY and MAC layers and then elaborated on its vulnerability under jamming attacks, followed by an in-depth review on existing jamming strategies and defense schemes. Particularly, we offered informative tables to summarize existing jamming attacks and anti-jamming techniques for each network, which will help the audience to grasp the fundamentals of jamming and anti-jamming strategies. We also listed some important open problems and pointed out the promising research directions toward securing wireless networks against jamming attacks. We hope such a survey article will help the audience digest the holistic knowledge of existing jamming/anti-jamming research results and facilitate the future design of jamming-resilient wireless communication systems.

References

[1] C. Condo, V. Bioglio, H. Hafermann, and I. Land, "Practical product code construction of polar codes," *IEEE Transactions on Signal Processing*, vol. 68, pp. 2004–2014, 2020.

[2] V. Bioglio, C. Condo, and I. Land, "Design of polar codes in 5G new radio," *IEEE Communications Surveys & Tutorials*, 2020.

[3] M. A. Albreem, M. Juntti, and S. Shahabuddin, "Massive MIMO detection techniques: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3109–3132, 2019.

[4] E. Björnson and L. Sanguinetti, "Scalable cell-free massive MIMO systems," *IEEE Transactions on Communications*, 2020.

[5] L. Liu and W. Yu, "Massive connectivity with massive MIMO—part ii: Achievable rate characterization," *IEEE Transactions on Signal Processing*, vol. 66, no. 11, pp. 2947–2959, 2018.

[6] X. Wang, L. Kong, F. Kong, F. Qiu, M. Xia, S. Arnon, and G. Chen, "Millimeter wave communication: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1616–1653, 2018.

[7] X. Shen, Y. Liu, L. Zhao, G.-L. Huang, X. Shi, and Q. Huang, "A miniaturized microstrip antenna array at 5G millimeter-wave band," *IEEE Antennas and Wireless Propagation Letters*, vol. 18, no. 8, pp. 1671–1675, 2019.

[8] P. Kheirkhah Sangdeh, H. Pirayesh, Q. Yan, K. Zeng, W. Lou, and H. Zeng, "A practical downlink NOMA scheme for wireless LANs," *IEEE Transactions on Communications*, vol. 68, no. 4, pp. 2236–2250, 2020.

[9] B. Makki, K. Chitti, A. Behravan, and M.-S. Alouini, "A survey of NOMA: Current status and open research challenges," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 179–189, 2020.

[10] Y. Yuan, Z. Yuan, and L. Tian, "5G non-orthogonal multiple access study in 3GPP," *IEEE Communications Magazine*, vol. 58, no. 7, pp. 90–96, 2020.

[11] X. Chen, G. Liu, Z. Ma, X. Zhang, P. Fan, S. Chen, and F. R. Yu, "When full duplex wireless meets non-orthogonal multiple access: Opportunities and challenges," *IEEE Wireless Communications*, vol. 26, no. 4, pp. 148–155, 2019.

[12] A. Goyal and K. Kumar, "LTE-advanced carrier aggregation for enhancement of bandwidth," in *Advances in VLSI, Communication, and Signal Processing*, pp. 341–351, Springer, 2020.

[13] N. Naderializadeh, M. A. Maddah-Ali, and A. S. Avestimehr, "Cache-aided interference management in wireless cellular networks," *IEEE Transactions on Communications*, vol. 67, no. 5, pp. 3376–3387, 2019.

[14] P. Yu, F. Zhou, X. Zhang, X. Qiu, M. Kadoch, and M. Cheriet, "Deep learning-based resource allocation for 5G broadband TV service," *IEEE Transactions on Broadcasting*, pp. 1–14, 2020.

[15] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, "A joint learning and communications framework for federated learning over wireless networks," *arXiv preprint arXiv:1909.07972*, 2019.

[16] P. Kheirkhah Sangdeh and H. Zeng, "DeepMux: Deep-learning-based channel sounding and resource allocation for IEEE 802.11ax," *IEEE Journal on Selected Areas in Communications*, 2021.

[17] A. M. Wyglinski, R. Getz, T. Collins, and D. Pu, *Software-Defined Radio for Engineers*. Artech House, 2018.

[18] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A survey on software-defined networking," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 27–51, 2014.

[19] Y. Miao, X. Liu, K.-K. R. Choo, R. H. Deng, H. Wu, and H. Li, “Fair and dynamic data sharing framework in cloud-assisted Internet of everything,” *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 7201–7212, 2019.

[20] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, “A survey on jamming attacks and countermeasures in WSNs,” *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[21] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey,” *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.

[22] Y. M. Amin and A. T. Abdel-Hamid, “A comprehensive taxonomy and analysis of IEEE 802.15.4 attacks,” *Journal of Electrical and Computer Engineering*, vol. 2016, 2016.

[23] D. R. Raymond and S. F. Midkiff, “Denial-of-service in wireless sensor networks: Attacks and defenses,” *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, 2008.

[24] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, “Jamming attacks on wireless networks: A taxonomic survey,” *International Journal of Production Economics*, vol. 172, pp. 76–94, 2016.

[25] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: attack and defense strategies,” *IEEE network*, vol. 20, no. 3, pp. 41–47, 2006.

[26] R. Di Pietro and G. Oligeri, “Jamming mitigation in cognitive radio networks,” *IEEE Network*, vol. 27, no. 3, pp. 10–15, 2013.

[27] R. P. Jover, “Security attacks against the availability of LTE mobility networks: Overview and research directions,” in *Proceedings of international symposium on wireless personal multimedia communications (WPMC)*, pp. 1–9, 2013.

[28] K. Grover, A. Lim, and Q. Yang, “Jamming and anti-jamming techniques in wireless networks: a survey,” *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.

[29] C. Shahriar, M. La Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, “PHY-layer resiliency in OFDM communications: A tutorial,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 292–314, 2014.

[30] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” *IEEE Communications surveys & tutorials*, vol. 13, no. 2, pp. 245–257, 2010.

[31] M. Vanhoef and F. Piessens, “Advanced Wi-Fi attacks using commodity hardware,” in *Proceedings of Computer Security Applications Conference*, pp. 256–265, 2014.

[32] M. Ettus, “Universal software radio peripheral (USRP),” *Ettus Research LLC http://www.ettus.com*, 2008.

[33] WARP: Wireless Open Access Research Platform, “Warp v3,” 2020. Available at: https://warpproject.org/trac/wiki/HardwareUsersGuides/WARPv3 [Online; accessed 2020-09-17].

[34] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, “Byzantine attack and defense in cognitive radio networks: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342–1363, 2015.

[35] D. Das and S. Das, “Primary user emulation attack in cognitive radio networks: A survey,” *IRACST-International Journal of Computer Networks and Wireless Communications*, vol. 3, no. 3, pp. 312–318, 2013.

[36] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, “A survey on security threats and detection techniques in cognitive radio networks,” *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 428–445, 2012.

[37] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. Leung, “A survey of security challenges in cognitive radio networks: Solutions and future research directions,” *Proceedings of the IEEE*, vol. 100, no. 12, pp. 3172–3186, 2012.

[38] “IEEE standard for information technology–telecommunications and information exchange between systems—local and metropolitan area networks–specific requirements–part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications–amendment 4: Enhancements for very high throughput for operation in bands below 6 GHz.,” *IEEE Std 802.11ac(TM)-2013*, pp. 1–425, 2013.

[39] E. Perahia and R. Stacey, *Next generation wireless LANs: 802.11n and 802.11ac*. Cambridge university press, 2013.

[40] B. Bellalta, “IEEE 802.11ax: High-efficiency WLANs,” *IEEE Wireless Communications*, vol. 23, no. 1, pp. 38–46, 2016.

[41] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, “A tutorial on IEEE 802.11ax high efficiency WLANs,” *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 197–216, 2019.

[42] T. Karhima, A. Silvennoinen, M. Hall, and S.-G. Haggman, “IEEE 802.11 b/g WLAN tolerance to jamming,” in *Proceedings of IEEE Military Communications Conference (MILCOM)*, vol. 3, pp. 1364–1370, 2004.

[43] L. Jun, J. H. Andrian, and C. Zhou, “Bit error rate analysis of jamming for OFDM systems,” in *wireless telecommunications Symposium*, pp. 1–8, IEEE, 2007.

[44] Y. Cai, K. Pelechrinis, X. Wang, P. Krishnamurthy, and Y. Mo, “Joint reactive jammer detection and localization in an enterprise WiFi network,” *Computer Networks*, vol. 57, no. 18, pp. 3799–3811, 2013.

[45] S. Prasad and D. J. Thuente, “Jamming attacks in 802.11g—a cognitive radio based approach,” in *Proceedings of IEEE Military Communications Conference (MILCOM)*, pp. 1219–1224, 2011.

[46] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, “MIMO-based jamming resilient communication in wireless networks,” in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, pp. 2697–2706, 2014.

[47] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, “Jamming resilient communication using MIMO interference cancellation,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1486–1499, 2016.

[48] M. Schulz, F. Gringoli, D. Steinmetzer, M. Koch, and M. Hollick, “Massive reactive smartphone-based jamming using arbitrary waveforms and adaptive power control,” in *Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 111–121, 2017.

[49] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, “Performance of IEEE 802.11 under jamming,” *Mobile Networks and Applications*, vol. 18, no. 5, pp. 678–696, 2013.

[50] I. Broustis, K. Pelechrinis, D. Syrivelis, S. V. Krishnamurthy, and L. Tassiulas, “FIJI: Fighting implicit jamming in 802.11 WLANs,” in *Proceedings of International Conference on Security and Privacy in Communication Systems*, pp. 21–40, Springer, 2009.

[51] S. Gvozdenovic, J. K. Becker, J. Mikulskis, and D. Starobinski, “Truncate after preamble: PHY-based starvation attacks on IoT networks,” in *Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 89–98, 2020.

[52] S. Bandaru, “Investigating the effect of jamming attacks on wireless LANs,” *International Journal of Computer Applications*, vol. 99, no. 14, pp. 5–9, 2014.

[53] M. J. La Pan, T. C. Clancy, and R. W. McGwier, “Jamming attacks against OFDM timing synchronization and signal acquisition,” in *Proceedings of IEEE Military Communications Conference (MILCOM)*, pp. 1–7, 2012.

[54] M. J. La Pan, T. C. Clancy, and R. W. McGwier, “Physical layer orthogonal frequency-division multiplexing acquisition and timing synchronization security,” *Wireless Communications and Mobile Computing*, vol. 16, no. 2, pp. 177–191, 2016.

[55] C. Shahriar, S. Sodagari, R. McGwier, and T. C. Clancy, “Performance impact of asynchronous off-tone jamming attacks against OFDM,” in *Proceedings of IEEE ICC*, pp. 2177–2182, 2013.

[56] S. Zhao, Z. Lu, Z. Luo, and Y. Liu, “Orthogonality-sabotaging attacks against OFDMA-based wireless networks,” in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1603–1611, 2019.

[57] M. J. La Pan, T. C. Clancy, and R. W. McGwier, “Phase warping and differential scrambling attacks against OFDM frequency synchronization,” in *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 2886–2890, 2013.

[58] T. C. Clancy, “Efficient OFDM denial: Pilot jamming and pilot nulling,” in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 1–5, 2011.

[59] C. Shahriar, S. Sodagari, and T. C. Clancy, “Performance of pilot jamming on MIMO channels with imperfect synchronization,” in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 898–902, 2012.

[60] S. Sodagari and T. C. Clancy, “Efficient jamming attacks on MIMO channels,” in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 852–856, 2012.

[61] S. Sodagari and T. C. Clancy, “On singularity attacks in MIMO channels,” *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 3, pp. 482–490, 2015.

[62] A. L. Scott, “Effects of cyclic prefix jamming versus noise jamming in OFDM signals,” tech. rep., Air Force Institute of Technology Graduate School of Engineering and Management, 2011.

[63] G. Patwardhan and D. Thuente, “Jamming beamforming: a new attack vector in jamming IEEE 802.11ac networks,” in *Proceedings of IEEE*

Military Communications Conference (MILCOM), pp. 1534–1541, 2014.

[64] D. Thuente and M. Acharya, “Intelligent jamming in wireless networks with applications to 802.11b and other networks,” in *Proceedings of IEEE Military Communications Conference (MILCOM)*, vol. 6, p. 100, 2006.

[65] M. Acharya, T. Sharma, D. Thuente, and D. Sizemore, “Intelligent jamming in 802.11b wireless networks,” *Proceedings of OPNETWORK. Washington DC, USA: OPNET*, 2004.

[66] G. Noubir, R. Rajaraman, B. Sheng, and B. Thapa, “On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming,” in *Proceedings of ACM conference on Wireless network security*, pp. 97–108, 2011.

[67] C. Orakcal and D. Starobinski, “Rate adaptation in unlicensed bands under smart jamming attacks,” in *Proceedings of IEEE International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, pp. 1–6, 2012.

[68] C. Orakcal and D. Starobinski, “Jamming-resistant rate adaptation in Wi-Fi networks,” *Performance Evaluation*, vol. 75, pp. 50–68, 2014.

[69] P. Kheirkhah Sangdeh, H. Pirayesh, A. Mobiny, and H. Zeng, “LB-SciFi: Online learning-based channel feedback for MU-MIMO in wireless LANs,” in *Proceedings of IEEE International Conference on Network Protocols (ICNP)*, pp. 1–11, 2020.

[70] S. Biaz and S. Wu, “Rate adaptation algorithms for IEEE 802.11 networks: A survey and comparison,” in *Proceedings of IEEE Symposium on Computers and Communications*, pp. 130–136, 2008.

[71] J. He, W. Guan, L. Bai, and K. Chen, “Theoretic analysis of IEEE 802.11 rate adaptation algorithm samplerate,” *IEEE Communications Letters*, vol. 15, no. 5, pp. 524–526, 2011.

[72] J. He, Z. Tang, H.-H. Chen, and S. Wang, “Performance analysis of ONOE protocol—an IEEE 802.11 link adaptation algorithm,” *International Journal of Communication Systems*, vol. 25, no. 7, pp. 821–831, 2012.

[73] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, “Using channel hopping to increase 802.11 resilience to jamming attacks,” in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, pp. 2526–2530, 2007.

[74] J. Jeung, S. Jeong, and J. Lim, “Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN,” in *Proceedings of IEEE Military Communications Conference (MILCOM)*, pp. 1231–1236, 2011.

[75] I. Harjula, J. Pinola, and J. Prokkola, “Performance of IEEE 802.11 based WLAN devices under various jamming signals,” in *Proceedings of IEEE MILCOM*, pp. 2129–2135, 2011.

[76] W. Shen, P. Ning, X. He, H. Dai, and Y. Liu, “MCR decoding: A MIMO approach for defending against wireless jamming attacks,” in *Proceedings of IEEE Conference on Communications and Network Security*, pp. 133–138, 2014.

[77] H. Zeng, C. Cao, H. Li, and Q. Yan, “Enabling jamming-resistant communications in wireless MIMO networks,” in *Proceedings of IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, 2017.

[78] G. Noubir and G. Lin, “Low-power DoS attacks in data wireless LANs and countermeasures,” *Proceedings of ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, pp. 29–30, 2003.

[79] G. Lin and G. Noubir, “On link layer denial of service in data wireless LANs,” *Wireless Communications and Mobile Computing*, vol. 5, no. 3, pp. 273–284, 2005.

[80] K. Pelechrinis, I. Broustis, S. V. Krishnamurthy, and C. Gkantsidis, “Ares: an anti-jamming reinforcement system for 802.11 networks,” in *Proceedings of international conference on Emerging networking experiments and technologies*, pp. 181–192, 2009.

[81] K. Pelechrinis, I. Broustis, S. V. Krishnamurthy, and C. Gkantsidis, “A measurement-driven anti-jamming system for 802.11 networks,” *IEEE/ACM Transactions on Networking*, vol. 19, no. 4, pp. 1208–1222, 2011.

[82] C. Orakcal and D. Starobinski, “Jamming-resistant rate control in Wi-Fi networks,” in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, pp. 1048–1053, 2012.

[83] E. Garcia-Villegas, M. Gómez, E. López-Aguilera, and J. Casademont, “Detecting and mitigating the impact of wideband jammers in IEEE 802.11 WLANs,” in *Proceedings of International Wireless Communications and Mobile Computing Conference*, pp. 57–61, 2010.

[84] A. Richa, C. Scheideler, S. Schmid, and J. Zhang, “A jamming-resistant MAC protocol for multi-hop wireless networks,” in *International Symposium on Distributed Computing*, pp. 179–193, Springer, 2010.

[85] O. Puñal, I. Aktaş, C.-J. Schnelke, G. Abidin, K. Wehrle, and J. Gross, “Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation,” in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pp. 1–10, 2014.

[86] K. Davaslioglu, S. Soltani, T. Erpek, and Y. Sagduyu, “DeepWiFi: Cognitive WiFi with deep learning,” *IEEE Transactions on Mobile Computing*, 2019.

[87] E. U. T. R. Access, “Physical channels and modulation,” *3GPP TS*, vol. 36, p. V8, 2009.

[88] E. Dahlman, S. Parkvall, J. Sköld, and P. Beming, “3G evolution: HSPA and LTE for mobile broadband,” *Jordan Hill, Oxford, UK*, 2007.

[89] G. Romero, V. Deniau, and O. Stienne, “LTE physical layer vulnerability test to different types of jamming signals,” in *Proceedings of International Symposium on Electromagnetic Compatibility-EMC EUROPE*, pp. 1138–1143, 2019.

[90] S. Zorn, M. Gardill, R. Rose, A. Goetz, R. Weigel, and A. Koelpin, “A smart jamming system for UMTS/WCDMA cellular phone networks for search and rescue applications,” in *Proceedings of IEEE/MTT-S International Microwave Symposium Digest*, pp. 1–3, 2012.

[91] S. Zorn, M. Maser, A. Goetz, R. Rose, and R. Weigel, “A power saving jamming system for E-GSM900 and DCS1800 cellular phone networks for search and rescue applications,” in *Proceedings of IEEE Topical Conference on Wireless Sensors and Sensor Networks*, pp. 33–36, 2011.

[92] R. Krenz and S. Brahma, “Jamming LTE signals,” in *Proceedings of IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, pp. 72–76, 2015.

[93] F. M. Aziz, J. S. Shamma, and G. L. Stüber, “Resilience of LTE networks against smart jamming attacks: Wideband model,” in *Proceedings of IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1344–1348, 2015.

[94] J. Kakar, K. McDermott, V. Garg, M. Lichtman, V. Marojevic, and J. H. Reed, “Analysis and mitigation of interference to the LTE physical control format indicator channel,” in *Proceedings of IEEE Military Communications Conference (MILCOM)*, pp. 228–234, IEEE, 2014.

[95] M. Lichtman, T. Czauski, S. Ha, P. David, and J. H. Reed, “Detection and mitigation of uplink control channel jamming in LTE,” in *Proceedings of IEEE Military Communications Conference (MILCOM)*, pp. 1187–1194, 2014.

[96] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, “LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation,” *IEEE Communications Magazine*, vol. 54, no. 4, pp. 54–61, 2016.

[97] F. Girke, F. Kurtz, N. Dorsch, and C. Wietfeld, “Towards resilient 5G: Lessons learned from experimental evaluations of LTE uplink jamming,” in *Proceedings of IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, 2019.

[98] M. Lichtman, J. H. Reed, T. C. Clancy, and M. Norton, “Vulnerability of LTE to hostile interference,” in *Proceedings of IEEE Global Conference on Signal and Information Processing*, pp. 285–288, 2013.

[99] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, “5G NR jamming, spoofing, and sniffing: threat assessment and mitigation,” in *Proceedings of IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1–6, 2018.

[100] F. M. Aziz, J. S. Shamma, and G. L. Stüber, “Resilience of LTE networks against smart jamming attacks,” in *Proceedings of IEEE Global Communications Conference*, pp. 734–739, 2014.

[101] Y. Arjoune and S. Faruque, “Smart jamming attacks in 5G new radio: A review,” in *IEEE Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 1010–1015, 2020.

[102] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, “Survey on threats and attacks on mobile networks,” *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[103] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, “What will 5G be?,” *IEEE Journal on selected areas in communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[104] Y. E. Sagduyu, T. Erpek, and Y. Shi, “Adversarial machine learning for 5G communications security,” *arXiv preprint arXiv:2101.02656*, 2021.

[105] B. Kim, Y. E. Sagduyu, T. Erpek, and S. Ulukus, “Adversarial attacks on deep learning based mmwave beam prediction in 5G and beyond,” in *Proceedings of IEEE Statistical Signal Processing Workshop (SSP)*, pp. 590–594, 2021.

[106] Y. Shi, Y. E. Sagduyu, T. Erpek, and M. C. Gursoy, “How to attack and defend 5G radio access network slicing with reinforcement learning,” *arXiv preprint arXiv:2101.05768*, 2021.

[107] A. Sheikhi, S. M. Razavizadeh, and I. Lee, "A comparison of TDD and FDD massive MIMO systems against smart jamming," *IEEE Access*, vol. 8, pp. 72068–72077, 2020.
[108] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, "Jamming-resistant receivers for the massive MIMO uplink," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 210–223, 2017.
[109] J. Vinogradova, E. Björnson, and E. G. Larsson, "Detection and mitigation of jamming attacks in massive MIMO systems using random matrix theory," in *Proceedings of IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–5, 2016.
[110] H. Akhlaghpasand, S. M. Razavizadeh, E. Björnson, and T. T. Do, "Jamming detection in massive MIMO systems," *IEEE Wireless Communications Letters*, vol. 7, no. 2, pp. 242–245, 2017.
[111] H. Akhlaghpasand, E. Björnson, and S. M. Razavizadeh, "Jamming suppression in massive MIMO systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 1, pp. 182–186, 2019.
[112] H. Akhlaghpasand, E. Björnson, and S. M. Razavizadeh, "Jamming-robust uplink transmission for spatially correlated massive MIMO systems," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3495–3504, 2020.
[113] J. Pinola, J. Prokkola, and E. Piri, "An experimental study on jamming tolerance of 3G/WCDMA," in *Proceedings of IEEE Military Communications Conference (MILCOM)*, pp. 1–7, 2012.
[114] B. Makarevitch, "Jamming resistant architecture for WiMAX mesh network," in *Proceedings of IEEE Military Communications conference (MILCOM)*, pp. 1–6, 2006.
[115] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks," *EURASIP Journal on Information Security*, vol. 2014, no. 1, p. 7, 2014.
[116] Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi, and N. Kaabouch, "A novel jamming attacks detection approach based on machine learning for wireless communication," in *Proceedings of IEEE International Conference on Information Networking (ICOIN)*, pp. 459–464, 2020.
[117] Q. Wu, G. Ding, J. Wang, and Y.-D. Yao, "Spatial-temporal opportunity detection for spectrum-heterogeneous cognitive radio networks: Two-dimensional sensing," *IEEE Transactions on Wireless Communications*, vol. 12, no. 2, pp. 516–526, 2013.
[118] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Proceedings of Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers*, vol. 1, pp. 772–776, 2004.
[119] P. K. Varshney, *Distributed detection and data fusion*. Springer Science & Business Media, 2012.
[120] G.-Y. Chang, S.-Y. Wang, and Y.-X. Liu, "A jamming-resistant channel hopping scheme for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 10, pp. 6712–6725, 2017.
[121] Y. Wu, B. Wang, K. R. Liu, and T. C. Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *IEEE journal on selected areas in communications*, vol. 30, no. 1, pp. 4–15, 2011.
[122] B. F. Lo and I. F. Akyildiz, "Multiagent jamming-resilient control channel game for cognitive radio ad hoc networks," in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 1821–1826, 2012.
[123] B. Wang, Y. Wu, K. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE journal on selected areas in communications*, vol. 29, no. 4, pp. 877–889, 2011.
[124] A. Asterjadhi and M. Zorzi, "JENNA: A jamming evasive network-coding neighbor-discovery algorithm for cognitive radio networks," *IEEE Wireless Communications*, vol. 17, no. 4, pp. 24–32, 2010.
[125] E. Altman, K. Avrachenkov, and A. Garnaev, "A jamming game in wireless networks with transmission cost," in *International Conference on Network Control and Optimization*, pp. 1–12, Springer, 2007.
[126] Y. E. Sagduyu, R. A. Berryt, and A. Ephremidesi, "Wireless jamming attacks under dynamic traffic uncertainty," in *8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, pp. 303–312, IEEE, 2010.
[127] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Jamming games in wireless networks with incomplete information," *IEEE Communications Magazine*, vol. 49, no. 8, pp. 112–118, 2011.
[128] L. Xiao, J. Liu, Q. Li, N. B. Mandayam, and H. V. Poor, "User-centric view of jamming games in cognitive radio networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2578–2590, 2015.
[129] K. Bian and J.-M. Park, "MAC-layer misbehaviors in multi-hop cognitive radio networks," in *Proceedings of US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006)*, pp. 228–248, 2006.
[130] T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep learning for launching and mitigating wireless jamming attacks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 1, pp. 2–14, 2018.
[131] H. Li and Z. Han, "Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems," in *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–6, 2009.
[132] Q. Zhu, H. Li, Z. Han, and T. Basar, "A stochastic game model for jamming in multi-channel cognitive radio systems," in *IEEE International Conference on Communications*, pp. 1–6, 2010.
[133] IEEE 802 Working Group, "IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (LR-WPANs)," *IEEE Std*, vol. 802, pp. 4–2011, 2011.
[134] J. Rewienski, M. Groth, L. Kulas, and K. Nyka, "Investigation of continuous wave jamming in an IEEE 802.15.4 network," in *Proceedings of International Microwave and Radar Conference (MIKON)*, pp. 242–246, 2018.
[135] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?," in *Proceedings of ACM conference on Wireless network security*, pp. 47–52, 2011.
[136] Z. Chi, Y. Li, X. Liu, W. Wang, Y. Yao, T. Zhu, and Y. Zhang, "Countering cross-technology jamming attack," in *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 99–110, 2020.
[137] H. Pirayesh, P. Kheirkhah Sangdeh, and H. Zeng, "Securing ZigBee communications against constant jamming attack using neural network," *IEEE Internet of Things Journal*, pp. 1–1, 2020.
[138] S. Fang, S. Berber, A. Swain, and S. U. Rehman, "A study on DSSS transceivers using OQPSK modulation by IEEE 802.15.4 in AWGN and flat Rayleigh fading channels," in *Proceedings of IEEE TENCON*, pp. 1347–1351, 2010.
[139] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1–9, 2010.
[140] J. Heo, J.-J. Kim, S. Bahk, and J. Paek, "Dodge-jam: Anti-jamming technique for low-power and lossy wireless networks," in *Proceedings of IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1–9, 2017.
[141] J. Heo, J.-J. Kim, J. Paek, and S. Bahk, "Mitigating stealthy jamming attacks in low-power and lossy wireless networks," *Journal of Communications and Networks*, vol. 20, no. 2, pp. 219–230, 2018.
[142] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in *Proceedings of IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 60–69, IEEE, 2007.
[143] B. DeBruhl and P. Tague, "Digital filter design for jamming mitigation in 802.15.4 communication," in *Proceedings of International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–6, 2011.
[144] Y. Liu and P. Ning, "BitTrickle: Defending against broadband and high-power reactive jamming attacks," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, pp. 909–917, 2012.
[145] S. Fang, Y. Liu, and P. Ning, "Wireless communications under broadband reactive jamming attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 3, pp. 394–408, 2015.
[146] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "Detection of reactive jamming in DSSS-based wireless communications," *IEEE Transactions on Wireless Communications*, vol. 13, no. 3, pp. 1593–1603, 2014.
[147] K. M. Haataja and K. Hypponen, "Man-in-the-middle attacks on Bluetooth: a comparative analysis, a novel attack, and countermeasures," in *Proceedings of International Symposium on Communications, Control and Signal Processing*, pp. 1096–1102, 2008.
[148] C. Gehrmann, J. Persson, and B. Smeets, *Bluetooth security*. Artech house, 2004.
[149] C. T. Hager and S. F. MidKiff, "An analysis of Bluetooth security vulnerabilities," in *Proceedings of IEEE Wireless Communications and Networking (WCNC)*, vol. 3, pp. 1825–1831, 2003.
[150] M. Jakobsson and S. Wetzel, "Security weaknesses in Bluetooth," in *Proceedings of Cryptographers' Track at the RSA Conference*, pp. 176–191, 2001.

[151] S. Köppel, "Bluetooth jamming," *Bachelor's Thesis supervised by Michael König and Roger Wattenhofer, ETH Zurich*, 2013.

[152] M. Strasser, C. Pöpper, and S. Čapkun, "Efficient uncoordinated FHSS anti-jamming communication," in *Proceedings of ACM international symposium on Mobile ad hoc networking and computing*, pp. 207–218, 2009.

[153] E.-K. Lee, S. Y. Oh, and M. Gerla, "Randomized channel hopping scheme for anti-jamming communication," in *Proceedings of IEEE IFIP Wireless Days*, pp. 1–5, 2010.

[154] C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE journal on selected areas in communications*, vol. 28, no. 5, pp. 703–715, 2010.

[155] A. Liu, P. Ning, H. Dai, and Y. Liu, "USD-FH: Jamming-resistant wireless communication using frequency hopping with uncoordinated seed disclosure," in *Proceedings of IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2010)*, pp. 41–50, 2010.

[156] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using uncoordinated frequency hopping," *IEEE transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 297–309, 2011.

[157] J. P. S. Sundaram, W. Du, and Z. Zhao, "A survey on LoRa networking: Research problems, current solutions, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 371–388, 2019.

[158] N. Hou, X. Xia, and Y. Zheng, "Jamming of LoRa PHY and countermeasure," in *Proceedings of IEEE Conference on Computer Communications*, pp. 1–10, 2021.

[159] R. Eletreby, D. Zhang, S. Kumar, and O. Yağan, "Empowering low-power wide area networks in urban settings," in *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*, pp. 309–321, 2017.

[160] X. Xia, Y. Zheng, and T. Gu, "FTrack: Parallel decoding for LoRa transmissions," *IEEE/ACM Transactions on Networking*, vol. 28, no. 6, pp. 2573–2586, 2020.

[161] X. Wang, L. Kong, L. He, and G. Chen, "MLoRa: A multi-packet reception protocol in LoRa networks," in *Proceedings of IEEE 27th International Conference on Network Protocols (ICNP)*, pp. 1–11, 2019.

[162] E. Aras, N. Small, G. S. Ramachandran, S. Delbruel, W. Joosen, and D. Hughes, "Selective jamming of LoRaWAN using commodity hardware," in *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 363–372, 2017.

[163] C.-Y. Huang, C.-W. Lin, R.-G. Cheng, S. J. Yang, and S.-T. Sheu, "Experimental evaluation of jamming threat in LoRaWAN," in *Proceedings of IEEE Vehicular Technology Conference*, pp. 1–6, 2019.

[164] A. SEMTECH and M. Basics, "AN1200.22," *LoRa Modulation Basics*, vol. 46, 2015.

[165] S. M. Danish, A. Nasir, H. K. Qureshi, A. B. Ashfaq, S. Mumtaz, and J. Rodriguez, "Network intrusion detection system for jamming attack in lorawan join procedure," in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 1–6, 2018.

[166] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3417–3442, 2019.

[167] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123–1152, 2015.

[168] ATIS-I-0000060, "Unmanned aerial vehicle (UAV) utilization of cellular services–enabling scalable and safe operation," *Alliance for Telecommunications Industry Solutions*, 2017.

[169] I. K. Azogu, M. T. Ferreira, J. A. Larcom, and H. Liu, "A new anti-jamming strategy for VANET metrics-directed security defense," in *Proceedings of IEEE Globecom Workshops (GC Wkshps)*, pp. 1344–1349, 2013.

[170] O. Puñal, A. Aguiar, and J. Gross, "In VANETs we trust? characterizing RF jamming in vehicular networks," in *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications*, pp. 83–92, 2012.

[171] O. Punal, C. Pereira, A. Aguiar, and J. Gross, "Experimental characterization and modeling of RF jamming attacks on VANETs," *IEEE transactions on vehicular technology*, vol. 64, no. 2, pp. 524–540, 2014.

[172] D. Rudinskas, Z. Goraj, and J. Stankūnas, "Security analysis of UAV radio communication system," *Aviation*, vol. 13, no. 4, pp. 116–121, 2009.

[173] X. Lu, D. Xu, L. Xiao, L. Wang, and W. Zhuang, "Anti-jamming communication game for UAV-aided VANETs," in *Proceedings of IEEE Global Communications Conference*, pp. 1–6, 2017.

[174] L. Xiao, X. Lu, D. Xu, Y. Tang, L. Wang, and W. Zhuang, "UAV relay in VANETs against smart jamming with reinforcement learning," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4087–4097, 2018.

[175] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Vehicular Communications*, vol. 13, pp. 56–63, 2018.

[176] S. Kumar, K. Singh, S. Kumar, O. Kaiwartya, Y. Cao, and H. Zhou, "Delimitated anti jammer scheme for Internet of vehicle: Machine learning based security approach," *IEEE Access*, vol. 7, pp. 113311–113323, 2019.

[177] H. Pirayesh, P. Kheirkhah Sangdeh, S. Zhang, Q. Yan, and H. Zeng, "JammingBird: Jamming-resilient communications for vehicular ad hoc networks," in *Proceedings of IEEE International Conference on Sensing, Communication and Networking (SECON)*, 2021.

[178] B. Okyere, L. Musavian, B. Özbek, S. A. Busari, and J. Gonzalez, "The resilience of massive MIMO PNC to jamming attacks in vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, 2020.

[179] A. T. Nguyen, L. Mokdad, and J. Ben Othman, "Solution of detecting jamming attacks in vehicle ad hoc networks," in *Proceedings of the 16th ACM international conference on Modeling, analysis & simulation of wireless and mobile systems*, pp. 405–410, 2013.

[180] L. Mokdad, J. Ben-Othman, and A. T. Nguyen, "DJAVAN: Detecting jamming attacks in vehicle ad hoc networks," *Performance Evaluation*, vol. 87, pp. 47–59, 2015.

[181] A. Benslimane and H. Nguyen-Minh, "Jamming attack model and detection method for beacons under multichannel operation in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 6475–6488, 2016.

[182] N. Lyamin, D. Kleyko, Q. Delooz, and A. Vinel, "Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining," *IEEE Communications Letters*, vol. 23, no. 3, pp. 442–445, 2019.

[183] S. Lv, L. Xiao, Q. Hu, X. Wang, C. Hu, and L. Sun, "Anti-jamming power control game in unmanned aerial vehicle networks," in *Proceedings of IEEE Global Communications Conference*, pp. 1–6, 2017.

[184] Y. Xu, G. Ren, J. Chen, L. Jia, and Y. Xu, "Anti-jamming transmission in UAV communication networks: a Stackelberg game approach," in *Proceedings of IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 1–6, 2017.

[185] Y. Xu, G. Ren, J. Chen, Y. Luo, L. Jia, X. Liu, Y. Yang, and Y. Xu, "A one-leader multi-follower Bayesian-Stackelberg game for anti-jamming transmission in UAV communication networks," *IEEE Access*, vol. 6, pp. 21697–21709, 2018.

[186] Y. Xu, G. Ren, J. Chen, X. Zhang, L. Jia, Z. Feng, and Y. Xu, "Joint power and trajectory optimization in UAV anti-jamming communication networks," in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 1–5, 2019.

[187] J. Peng, Z. Zhang, Q. Wu, and B. Zhang, "Anti-jamming communications in UAV swarms: A reinforcement learning approach," *IEEE Access*, 2019.

[188] J. Zhang, S. C. Periaswamy, S. Mao, and J. Patton, "Standards for passive UHF RFID," *GetMobile: Mobile Computing and Communications*, vol. 23, no. 3, pp. 10–15, 2020.

[189] G. EPCglobal, "EPC radio-frequency identity protocols generation-2 UHF RFID; specification for RFID air interface protocol for communications at 860 MHz–960 MHz," *EPCglobal Inc., November*, 2013.

[190] Y. Fu, C. Zhang, and J. Wang, "A research on denial of service attack in passive RFID system," in *IEEE International Conference on Anti-Counterfeiting, Security and Identification*, pp. 24–28, 2010.

[191] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Information Systems Frontiers*, vol. 12, no. 5, pp. 491–505, 2010.

[192] Y. Oren, D. Schirman, and A. Wool, "RFID jamming and attacks on israeli e-voting," in *Proceedings of VDE Smart SysTech; European Conference on Smart Objects, Systems and Technologies*, pp. 1–7, 2012.

[193] Y. Oren and A. Wool, "Attacks on RFID-based electronic voting systems.," *IACR Cryptol. ePrint Arch.*, vol. 2009, p. 422, 2009.

[194] D. Patel, N. Soni, G. Dholariya, H. Dalal, A. Razaque, and K. Maheta, "Detection and resolving jamming in RFID wireless network using gauss elimination method," in *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1897–1903, IEEE, 2016.

[195] G. Wang, H. Cai, C. Qian, J. Han, S. Shi, X. Li, H. Ding, W. Xi, and J. Zhao, "Hu-Fu: Replay-resilient RFID authentication," *IEEE/ACM Transactions on Networking*, vol. 28, no. 2, pp. 547–560, 2020.

[196] L. Avanco, A. E. Guelfi, E. Pontes, A. A. Silva, S. T. Kofuji, and F. Zhou, "An effective intrusion detection approach for jamming attacks on RFID systems," in *Proc. IEEE International EURASIP Workshop on RFID Technology (EURFID)*, pp. 73–80, 2015.

[197] M. Karaim, *Ultra-tight GPS/INS Integrated System for Land Vehicle Navigation in Challenging Environments*. PhD thesis, Queen's University (Canada), 2019.

[198] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, J. A. Bhatti, and T. E. Humphreys, "Signal characteristics of civil GPS jammers," in *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, pp. 1907–1919, 2011.

[199] O. Glomsvoll, "Jamming of GPS & GLONASS signals," *Department of Civil Engineering, Nottingham Geospatial Institute*, 2014.

[200] A. Grant, P. Williams, N. Ward, and S. Basker, "GPS jamming and the impact on maritime navigation," *The Journal of Navigation*, vol. 62, no. 2, pp. 173–187, 2009.

[201] Q. Zeng, H. Li, and L. Qian, "GPS spoofing attack on time synchronization in wireless networks and detection scheme design," in *Proceedings of IEEE Military Communications Conference (MILCOM)*, pp. 1–5, 2012.

[202] A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, "Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 886–899, 2016.

[203] J. Hoffer, R. D. S. Lowande, P. Kreuser, and T. A. Youssef, "Educational review: GPS applications and vulnerability implications," in *2020 SoutheastCon*, pp. 1–4, IEEE, 2020.

[204] Y. Zhang, M. G. Amin, and A. R. Lindsey, "Anti-jamming GPS receivers based on bilinear signal distributions," in *Proceedings of IEEE MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No. 01CH37277)*, vol. 2, pp. 1070–1074, 2001.

[205] Y.-R. Chien, "Design of GPS anti-jamming systems using adaptive notch filters," *IEEE Systems Journal*, vol. 9, no. 2, pp. 451–460, 2013.

[206] M. J. Rezaei, M. Abedi, and M. R. Mosavi, "New GPS anti-jamming system based on multiple short-time fourier transform," *IET Radar, Sonar & Navigation*, vol. 10, no. 4, pp. 807–815, 2016.

[207] K. D. Rao and M. Swamy, "New approach for suppression of fm jamming in GPS receivers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 42, no. 4, pp. 1464–1474, 2006.

[208] Q. Li, W. Wang, D. Xu, and X. Wang, "A robust anti-jamming navigation receiver with antenna array and GPS/SINS," *IEEE Communications Letters*, vol. 18, no. 3, pp. 467–470, 2014.

[209] N. Rezazadeh and L. Shafai, "A compact antenna for GPS anti-jamming in airborne applications," *IEEE Access*, vol. 7, pp. 154253–154259, 2019.

[210] Y. D. Zhang and M. G. Amin, "Anti-jamming GPS receiver with reduced phase distortions," *IEEE Signal Processing Letters*, vol. 19, no. 10, pp. 635–638, 2012.

[211] W. Sun and M. G. Amin, "A self-coherence anti-jamming GPS receiver," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3910–3915, 2005.

[212] B. G. Agee, S. V. Schell, and W. A. Gardner, "Spectral self-coherence restoral: A new approach to blind adaptive signal extraction using antenna arrays," *Proceedings of the IEEE*, vol. 78, no. 4, pp. 753–767, 1990.

[213] D. Lu, R. Wu, and H. Liu, "Global positioning system anti-jamming algorithm based on period repetitive CLEAN," *IET Radar, Sonar & Navigation*, vol. 7, no. 2, pp. 164–169, 2013.

[214] M. G. Amin, L. Zhao, and A. R. Lindsey, "Subspace array processing for the suppression of FM jamming in GPS receivers," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 40, no. 1, pp. 80–92, 2004.

[215] Y. E. Sagduyu, Y. Shi, A. B. MacKenzie, and Y. T. Hou, "Regret minimization for primary/secondary access to satellite resources with cognitive interference," *IEEE Transactions on Wireless Communications*, vol. 17, no. 5, pp. 3512–3523, 2018.

[216] F. Caron, E. Duflos, D. Pomorski, and P. Vanheeghe, "Gps/imu data fusion using multisensor kalman filtering: introduction of contextual aspects," *Information fusion*, vol. 7, no. 2, pp. 221–230, 2006.

[217] D. Chou, Y. Ng, and G. X. Gao, "Robust GPS-based timing for PMUs based on multi-receiver position-information-aided vector tracking," in *Proceedings of the International Technical Meeting of The Institute of Navigation*, pp. 600–607, 2015.

[218] Y. Ng and G. X. Gao, "Advanced multi-receiver position-information-aided vector tracking for robust GPS time transfer to PMUs," in *Proceedings of the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015)*, pp. 3443–3448, 2015.

[219] U. Schwarz, "Mathematical-statistical description of the iterative beam removing technique (method CLEAN)," *Astronomy and Astrophysics*, vol. 65, p. 345, 1978.

[220] D. Medina, C. Lass, E. P. Marcos, R. Ziebold, P. Closas, and J. García, "On GNSS jamming threat from the maritime navigation perspective," in *International Conference on Information Fusion (FUSION)*, pp. 1–7, IEEE, 2019.

[221] M. Sadeghi and E. G. Larsson, "Physical adversarial attacks against end-to-end autoencoder communication systems," *IEEE Communications Letters*, vol. 23, no. 5, pp. 847–850, 2019.

[222] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Over-the-air adversarial attacks on deep learning based modulation classifier over wireless channels," in *2020 54th Annual Conference on Information Sciences and Systems (CISS)*, pp. 1–6, IEEE, 2020.

[223] Y. Sagduyu, Y. Shi, and T. Erpek, "Adversarial deep learning for over-the-air spectrum poisoning attacks," *IEEE Transactions on Mobile Computing*, 2019.

[224] D. Adesina, C.-C. Hsieh, Y. E. Sagduyu, and L. Qian, "Adversarial machine learning in wireless communications using RF data: A review," *arXiv preprint arXiv:2012.14392*, 2020.

[225] C. Zhong, F. Wang, M. C. Gursoy, and S. Velipasalar, "Adversarial jamming attacks on deep reinforcement learning based dynamic multichannel access," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, IEEE, 2020.

[226] N. Abuzainab, T. Erpek, K. Davaslioglu, Y. E. Sagduyu, Y. Shi, S. J. Mackey, M. Patel, F. Panettieri, M. A. Qureshi, V. Isler, *et al.*, "QoS and jamming-aware wireless networking using deep reinforcement learning," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*, pp. 610–615, IEEE, 2019.

[227] J. Zhu, Z. Wang, Q. Li, H. Chen, and N. Ansari, "Mitigating intended jamming in mmWave MIMO by hybrid beamforming," *IEEE Wireless Communications Letters*, vol. 8, no. 6, pp. 1617–1620, 2019.

[228] Z. Xiao, B. Gao, S. Liu, and L. Xiao, "Learning based power control for mmWave massive MIMO against jamming," in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, 2018.

[229] Y. Cai, C. Zhao, Q. Shi, G. Y. Li, and B. Champagne, "Joint beamforming and jamming design for mmWave information surveillance systems," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1410–1425, 2018.

[230] S. Bagherinejad and S. M. Razavizadeh, "Direction-based jamming detection and suppression in mmWave massive MIMO networks," *IET Communications*.

[231] N. Hou, X. Xia, and Y. Zheng, "Jamming of lora phy and countermeasure," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2021.

[232] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping—part i: System design," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 70–79, 2012.

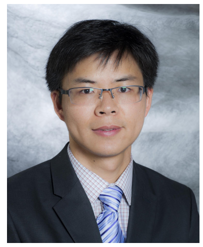
[233] L. Xiao, Y. Li, C. Dai, H. Dai, and H. V. Poor, "Reinforcement learning-based NOMA power allocation in the presence of smart jamming," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3377–3389, 2017.

[234] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5394–5409, 2019.

[235] H. Yang, Z. Xiong, J. Zhao, D. Niyato, Q. Wu, H. V. Poor, and M. Tornatore, "Intelligent reflecting surface assisted anti-jamming communications: A fast reinforcement learning approach," *IEEE Transactions on Wireless Communications*, vol. 20, no. 3, pp. 1963–1974, 2020.

[236] H. Yang, Z. Xiong, J. Zhao, D. Niyato, Q. Wu, M. Tornatore, and S. Secci, "Intelligent reflecting surface assisted anti-jamming communications based on reinforcement learning," in *Proceedings of IEEE Global Communications Conference*, pp. 1–6, 2020.

Hossein Pirayesh received the B.Sc. degree in electrical engineering from Karaj Islamic Azad University, Karaj, Iran, in 2013, and the M.Sc. degree in electrical engineering from the Iran University of Science and Technology, Tehran, Iran, in 2016. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, USA. His research focuses are on wireless communications and networking, including theoretical analysis, algorithm and protocol design, and system implementation.



Huacheng Zeng (Senior Member, IEEE) is an Assistant Professor of Computer Science and Engineering at Michigan State University, East Lansing, MI, USA. He received his Ph.D. degree in Computer Engineering from the Virginia Polytechnic Institute and State University (Virginia Tech), Blacksburg, VA, USA. He was an Assistant Professor of Electrical and Computer Engineering at University of Louisville, Louisville, KY, USA, and a Senior System Engineer with Marvell Semiconductor, Santa Clara, CA, USA. His research interests include broadly in wireless networking and sensing systems. Dr. Zeng was a recipient of the NSF CAREER Award.