Far East Journal of Electronics and Communications

http://www.pphmj.com
http://dx.doi.org/10.17654/0973700622001
Volume 25, 2022, Pages 1-36 **P-ISSN: 0973-7006**

A SURVEY ON JAMMING AND FRIENDLY JAMMING TECHNIQUES

Kiriakos Gavouchidis and Dimitrios Efstathiou

Department of Informatics, Computers and Telecommunications Engineering
International Hellenic University
Serres Campus, Greece

Abstract

Wireless communication is the most growing area in the field of communications and wireless networks as their key components become increasingly important in our life. Despite the great advancement of wireless networks in recent years, most wireless networks are vulnerable to *jamming attacks* because of the openness of the wireless channel. The purpose of jamming is to cause interference with the adversary's or enemy's effective use of electromagnetic spectrum [1]. In contrast to jamming, which is typically used for attack purposes, friendly jamming is a technique used to protect against attacks. We start by introducing the basic jamming concepts and fields of use. The focus of our review is based on jamming and friendly jamming techniques, their application fields,

Received: May 6, 2022; Accepted: June 28, 2022

Keywords and phrases: jamming, friendly jamming, confidentiality, authentication, access control.

How to cite this article: Kiriakos Gavouchidis and Dimitrios Efstathiou, A survey on jamming and friendly jamming techniques, Far East Journal of Electronics and Communications 25 (2022), 1-36. http://dx.doi.org/10.17654/0973700622001

Published Online: August 17, 2022

their limitations, and challenges for different kinds of networks such as WLANs, 5G radio networks, cognitive radio networks, vehicular wireless networks and fly ad-hoc networks.

1. Introduction

There are many kinds of wireless communication, e.g., cell phone, wireless computer, data links, weapon-firing links, or unmanned aerial vehicle (UAV) links communication. Communication jamming, or more precisely radio frequency jamming, is also known in literature as electromagnetic countermeasures (ECM) or as electronic attack (EA). The subject of communication jamming, hereinafter jamming, is to prevent the transfer of information [2]. Typical communication systems consist of a transmitter that sends the information and a receiver that receives the information. Jamming refers to jamming the receiver, not the transmitter, considering that the signal on the receiver side is weaker to attack [3]. Jamming usually causes an undesired signal with the objective to prevent the receiver to demodulate the desired information from the signal it is trying to receive. The disruption of wireless communication takes place at the physical layer, and it is therefore hard to remove it. Some parameters that play a role in jamming are signal power of the transmitted signal, signal modulation as well as geometry of the link.

On the other hand, the interruption of communication through jamming can be used to the advantage of a wireless network. This concept referred to as friendly jamming. Two different use cases for friendly jamming are referenced in the literature. The first one is blocking unauthenticated communication (e.g., in access points). The second one is the prevention of eavesdropping on communication. Friendly jamming can be enabled using more than one jammer which cooperate [4].

Although friendly jamming is believed to be a simple and effective way to protect wireless devices with limited resources, there are several challenges in using friendly jamming. The characteristics of the wireless channel, like attenuation and multipath effects contribute to a dynamic

environment. Friendly jamming effectiveness in such an environment is a challenge. A second challenge is the achievement of pervasiveness in means of availability for the most wireless protocols at low cost. Finally, a third challenge friendly jamming must deal with, is to be minimally invasive, it must block off attack transmissions and at the same time protect the legitimate transmissions. Friendly jamming must have minimal impact to the transmissions it is designed to protect.

We discuss in Section 2 jamming attacks and friendly jamming in Section 3. Section 4 presents related work and Section 5 concludes our paper.

2. Jamming Attacks

In the literature we do not find a uniform definition of the term jamming attacks. NIST, the U.S. National Institute of Standards and Technology of the U.S. Department of Commerce in its glossary [5] define *jamming* in four different publications as the following:

Definition 1. An attack that attempts to interfere with the reception of broadcast communications.

Definition 2. An attack in which a device is used to emit electromagnetic energy on a wireless network's frequency to make it unusable.

Definition 3. A deliberate communication disruption meant to degrade the operational performance of the RF subsystem. Jamming is achieved by interjecting electromagnetic waves on the same frequency that the receiver to tag uses for communication.

Definition 4. The deliberate radiation, re-radiation, or reflection of electromagnetic energy for the purpose of preventing or reducing the effective use of a signal.

In addition to the terms mentioned in the introduction, jamming is also referred to as 'soft kill'. The attacked communication infrastructure becomes

temporarily ineffective or no longer functions, but it is not destroyed. Due to its effects a jamming attack is a form of Denial of Service (DoS) attack. The legacy IEEE 802.11 standard does not provide defense functionality against jamming attacks. This is the reason why jamming, e.g., in WLANs, is difficult to defend.

Jamming sometimes happens unintended; for example, if devices (e.g., cordless telephone or microwave oven which operates within the unlicensed spectrum) share bandwidth they can make one or more nearby wireless networks unusable.

2.1. How does jamming work? Main principles

We propose an adversary model where a sender (e.g., enemy) sends information with a transmitter to a receiver as a wireless signal, called the *desired signal*, and an adversary uses a jamming attack to prevent the receiver to reconstruct the signal. A jamming attack can prevent the recovery of the desired signal in two different ways: (a) the power of the jamming signal overwhelms the content of the desired signal, or (b) the characteristics of the combined signal, consists of desired and jamming signal, do not allow the receiver hardware to separate the two signals and use the information in the desired signal. There are many different strategies and models for jamming attacks and defenses against them with different effectiveness. Xu et al. describes some jamming attack models [6]. These are the *constant jammer*, the *deceptive jammer*, the *random jammer*, the *reactive jammer*, the *go-next jammer*, and the *control channel jammer*.

- A *constant jammer* sends out constantly random bits as a radio signal without waiting for the channel to become free. Using the constant jammer and applying a signal strength that is higher than a fixed threshold the constant jammer can prevent the legitimate receiver from getting hold the channel.

- A *deceptive jammer* sends out constantly regular packets, or parts of regular packets, e.g., a continuous stream of preamble bits. The attacker prevents this way the receiver to change to the send mode.

- Through a *random jammer* an attacker implements an alternating radio-sleeping and radio-jamming mode instead to emit a continuous signal as in constant and deceptive jammers. The time the jammer stays at radio-sleeping or radio-jamming mode is either random or fixed. Random jammers are used if energy for jamming is available to a limited extent. Constant, deceptive, and random jammers are called *active jammers* since they send their jamming signal just independent from the communication between transmitter and receiver. They are very effective, but their detection is easy.

- A *reactive jammer* implements a reactive strategy, which means that jamming becomes active when the attacked system is active. The reactive jammer cannot save energy, as it must regularly check whether the transmitter and receiver are communicating with each other. Its advantage is that it is harder to detect it.

- A *go-next jammer* attacks each time one frequency channel. If the transmitter detects the jammer activity in the radio channel, it hops to the next frequency. In this case the go-next jammer continues to attack the receiver changing also to the next frequency. Because the jammer attacks every time only one frequency channel, we can say that go-next jammers store up their energy. On the other hand, if the transmitter carries out fast rate frequency hopping, the jammer also performs a fast rate frequency hopping and waste energy.

- A *control channel* jammer targets the control traffic between transmitter and receiver attacking the control channel before communication starts.

2.2. Interference, types of interference, jamming, and application fields of jamming

Jamming and interference are two related terms. To what extent? In Definition 1 jamming is mentioned as an attack that attempts to interfere with the reception of broadcast communications. Interference in this definition is used in terms of *Radio Frequency* (*RF*) *Interference*. The

International Telecommunication Union's (*ITU*) defines RF interference as *the effect of unwanted energy due to one or a combination of emissions*, *radiations*, *or inductions upon reception in a radiocommunication system*, *manifested by any performance degradation*, *misinterpretation*, *or loss of information which could be extracted in the absence of such unwanted energy* (RR-2020-00013-Vol.I-EA5). Devices based on Radio Frequency (RF) including cellular, radio, radar, Wi-Fi, Global Positioning System (GPS), unmanned aircraft system (UAS) communications and control systems, satellite, and other technologies are potentially vulnerable to interference. ITU's Radio Regulations (RR) distinguishes between three types of interference: the permissible interference, the accepted interference, and the harmful interference.

Permissible interference (No. 1.167 in ITU RR 2020): Observed or predicted interference which complies with quantitative interference and sharing criteria contained in these (ITU RR 2020) Regulations or in ITU-R Recommendations or in special agreements as provided for in these Regulations.

Accepted interference (No. 1.168 in ITU RR 2020): Interference at a higher level than that is defined as permissible interference, and which has been agreed upon between two or more administrations without prejudice to other administrations.

Harmful interference (No. 1.169 in ITU RR 2020): Interference which endangers the functioning of a radio-navigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with Radio Regulations (CS).

Harmful interference can be caused through different sources. We differentiate between sources according to whether the interference they cause is intentional or unintentional. Unintentional interference sources can be for example degraded, outdated, or improperly installed signal boosters, solar flares, lighting ballasts, or Universal Serial Bus chargers. Intentional

interference sources are for example radios that use unauthorized frequencies, or illegal jamming devices like phone jammers or GPS blockers. Radio frequency interference effects depend on source location in relation to the target location. RF interference in public safety communications can be categorized in internal or self-interference, in external interference, and intentional jamming. The reasons for internal interference are wrong settings inside the communication infrastructure, e.g., through upgrades of hubs, "non-linear mixing" of external signals in a receiver, or inadequate filtering of radio equipment. External interference is unintentional RF interference. External interference is caused from neighbor communication systems or space weather events. Examples of external interference are, e.g., space weather events like northern lights, and solar flares as well as hurricanes and floods. Other examples of external interference are in case of improper frequency coordination of transmitters communicating on the same channel, or if transmitter energy spills over on adjacent channels.

What is the relation between jamming and RF interference? Jamming is intentional interference noise that is used to weaken or even disrupt the receiver from receiving information or degrade communication. The term jamming is used to describe a *Penetration of DoS attack* [7] threatening availability that affects one or more users [8]. By using jamming an attacker can easily (low effort) generate interfering transmissions to prevent communication within their reception range. The network coverage area can be well-defined, e.g., along a highway, and therefore an attacker through a jamming attack can disrupt the communication in the neighbourhood. This happens using limited transmission power and without compromising any cryptographic protocols that are in use [9].

The application of jamming is mainly divided into two areas, civilian and military use. Civilian applications are, e.g., mobile jamming, internet jamming (partly or fully), radio station jamming or satellite TV stations jamming. Military applications of jamming are, e.g., *communication jamming*, *radar jamming*, *radar deceptive jamming*, *cover jamming*, or *decoy jamming*. Communication jamming prevents the transmitted

information to be passed over the enemy communication link. Radar jamming causes radar to find or lose its target. Deceptive jamming of radar results in delivery of false information (e.g., changed angle) in the radar response signal. Cover jamming damages the desired signal quality. The information cannot be recovered. Decoy jamming deceives the enemy, so the enemy attacks the decoy instead of the originally envisaged target.

2.3. Communication jamming performance considerations

The links that we consider in the context of using jamming are digital links. One of the most important units of measurement in case of jamming is the jamming-to-signal-ratio (J/S or JSR). Jamming-to-signal-ratio is 'the ratio of the received jamming signal power to the received desired signal power in the receiver' [10]. The jamming-to-signal ratio (in dB) is given by the formula

$$J/S = ERP_J - ERP_S - LOSS_J + LOSS_S + G_{RJ} - G_{RS}, \quad (1)$$

where ERP_J is the effective radiated power of the jamming transmitter in the direction of the target receiver (in dBm), ERP_S is the effective radiated power of desired signal from transmitter in the direction of the target receiver (in dBm), $LOSS_J$ is the transmission loss from jamming transmitter to target receiver (in dB), $LOSS_S$ is the transmission loss from desired signal transmitter to target receiver (in dB), G_{RJ} is the gain of the receiver's antenna in the direction of the jammer (in dB), and G_{RS} is the gain of the receiver's antenna in the direction of the desired signal transmitter (in dB). In case of use of a nondirectional antenna on the target receiver side, the last two terms of the formal are equal and cancel out each other. Digital signal communications can be stopped applying a jamming duty cycle of 20% to 30% and a J/S of 0 dB. Successful jamming depends also on the nature of the information carried by the link. Bit error rate (BER) refers to the number of bit errors per unit time. A high bit error rate results to nonrecoverable digital signals. An increase in J/S results in an increase in BER. When the

jammer achieves 0 dB J/S, the number of possible bit errors reaches its maximum value. Increasing jamming power after $J/S = 0$ will result to only very few additional errors [10].

2.4. Jamming attacks in WLANs and mitigation

Due to the open nature of the wireless medium, wireless networks are vulnerable to several security threats such as jamming attacks. An important characteristic of different adversarial models is the extent of network knowledge by the attacker. We differentiate between attacker models with zero knowledge and models with knowledge awareness of the network. Attackers having zero knowledge of the network usually adapt the so called always-on jamming strategy [11]. They fire permanent high-power jamming signals such as frequency modulated noise or wave tones to interfere the communication. From the attacker point of view this strategy is not beneficial. A lot of energy must be consumed for the permanent jamming signals to attack the desired frequencies. Another disadvantage is that the attacks based on zero knowledge of the network can be easily mitigated by localization and elimination of the jamming nodes, using spread spectrum, or applying spatial retreat on user communication side. Jamming attacks in networks usually adapt the network knowledge awareness model. The attacker in this model uses his network knowledge and targets or selects in real time important *Transmission Control Protocol* (*TCP*) packets to attack before these packets arrive to receiver.

This is where the term *selective jamming attack* came about. The real-time selected TCP packets can now be classified as *relevant* or *not relevant* for the attack. Attack relevant packets are corrupted before they reach the receiver. The classification of packets can be done on ISO/OSI layer 2, the link layer through decoding of the control field of the MAC frame. To mitigate selective jamming, it is necessary to prevent real-time packet classification. Lazos et al. [11] proposes three schemes that combined with physical layer attributes to defend selective jamming by transforming a selective jammer into a *random* one. The three schemes that are used are

based on cryptographic primitives such as *Commitments*, *Cryptographic Puzzles*, and *All-or-nothing Transformations*. Their goal is to overwhelm the attacker's computational ability of real-time classification.

Wi-Fi (Wireless Fidelity) as a WLAN technology is due to its increasing importance target of jamming attacks. Packet transmission in Wi-Fi consists of three phases: Data encoding, OFDM symbol generation, and waveform shaping which includes the upconversion of the OFDM modulated signals to the channel's carrier frequency and the signal transmission by the RF front end. Interleaving is part of the data encoding phase and is a technique that is used to combat burst bit errors in the packet transmission process. A burst error is a contiguous symbol sequence, received in such way, that the first and last symbols as well as the symbols between them in the signal are in error. Interleaving scatters the bits received from the convolution encoder by separating consecutive bits (also the burst error bits) to larger distances and vice versa. Vo-Huu et al. [12] investigates the coding scheme of IEEE 802.11a/g/n with special consideration of its interleaver/convolutional structure. Using short burst bit errors in deliberately selected sub-carriers leads to overwhelming of the possibilities offered by the error correction of the Wi-Fi. One interesting observation is that in the coding scheme of IEEE 802.11a/g/n the interleaving pattern of the coded bits is deterministic and predictable for all frames. Additionally, the deterministic property of interleaving applies across OFDM subcarriers. Especially the analysis of the first and second round interleaver permutations leads to the development of jamming patterns across the OFDM subcarriers. The de-interleaving of these jamming patterns in turn leads to interference burst, enabling in this way efficient interleaving jamming attacks. With an energy cost of 2 to 4 magnitude orders than that used by regular communication nodes an attacker can degrade over 95% of or even destroy the packets. Vo-Huu et al. prove that for IEEE 802.11 non-BPSK transmissions, adjacent bits at positions K and K' in the original coded data sequence are interleaved into separate data subcarriers, whose distance in the spectrum is a multiple of 3. For example, in a 64-Quadrature Amplitude Modulation (QAM) interleaving divides the

data packet into multiple 288-bit groups where every 6 bits are embedded into one data subcarrier (DSC) and bits that followed each other before interleaving are now in DSCs that are three times apart. The interleaving jamming strategy based on the fact that if we cause interference to a group of n DSCs that are separated from each other by a multiple of 3, we can create a sequence of n consecutive bit errors. Interleaving jamming is a *multi-carrier jamming strategy* because it generates interference on DSCs i, $i + 3$, $i + 6$, $i + 3(n - 1)$ with i anyone of the DSCs, and n the number of subcarriers the attacker wants to jam. The authors implemented a real time interleaving jammer on the HackRF One software defined radio. Wi-Fi has no mechanisms to protect against malicious interference. For this reason, countermeasures against interleaving attacks require modifications to the standard. One possible countermeasure is the application of cryptography to randomize interleaving mapping. A second countermeasure is to introduce a frame dependent interleaving structure and permute over frequency and time subcarriers.

2.4.1. The wireless network jamming problem

The *wireless network jamming problem* (*WNJP*) is the problem to find out the optimal number of a set of jamming devices and their individual placement to neutralize communication on the wireless network. Clayton et al. investigate the problem in known enemy network environments [13] and in uncertain enemy network environments [14] without information about the network to be jammed.

2.5. Jamming attacks in 5G New Radio and mitigation

5G networks operate from below 1 GHz to 100 GHz and are vulnerable to jamming attacks, which are serious threats to public safety [15]. The main characteristics of the architecture of 5G New Radio (5G NR) are network flexibility, multi-connectivity, high level security, massive MIMO/beamforming, and new radio spectrum. 5G NR architecture combines LTE components with not backward LTE-compatible new radio access technology and supports frequency division duplexing (*FDD*) and time

division duplexing (*TDD*). In 5G NR, the downlink (*DL*) uses orthogonal frequency-division multiplexing (*OFDM*) with a cyclic prefix. Cyclic Prefix in OFDM is used to correct the offset in the transmitter/receiver in the frequency-time domain, as well as to correct multipath effects or to make corrections when the transmitter or receiver is moving. 5G NR uplink (UL) uses OFDM just like the downlink or DTF spread OFDM (*DTF-s-OFDM*). The DTF-s-OFDM mode does not allow multiple-transmissions. Several different physical channels are used in 5G. For the downlink there are the *broadcast channel* (*PBCH*), the *downlink control channel* (*PDCCH*), and the *downlink shared channel* (*PDSCH*). For the uplink there are the uplink control channel (PUCCH), the *random-access channel* (*PRACH*), and the *uplink shared channel* (*PUSCH*). One subcarrier over one OFDM symbol interval in LTE is a resource element (RE). Jamming vulnerability of a channel depends on [16]:

- The sparsity of the channel in relation to the time-frequency resource grid (percentage of resource elements in the time-frequency domain).

- The power of jamming needed to successfully attack the channel (measured using J/S_{CH}).

The operation of 5G NR in the millimeter wave band (> = 24 GHz) improves robustness to jamming. Therefore, we focus on operation for frequencies less than 24 GHz. Jammers attacking 5G NR systems that operate in the millimeter band are expensive and their construction is complex. 5G NR users use devices such as cell phones, dongles, or tablets. These devices are called *user equipment* (*UE*). A UE accesses the LTE base station called *evolved NodeB* (*eNodeB*). Typically, a UE connects to one eNodeB at a time or if its home network is not available it roams in other 2G, 3G or 4G networks. The 5G NR downlink and uplink signals are implemented by physical signals and physical channels that are multiplexed together in frequency and time and mapped onto the time-frequency frame grid. This mapping takes place in the broadcast messages sent by each base station. This kind of information mapping allows jammers to target specific

parts of the frequency-time frame grid and attack information in specific resource elements or jam with specific physical downlink channels or signals.

2.5.1. Jamming synchronization signals

5G NR uses two synchronization signals, the *Primary Synchronization Signal* (*PSS*) and the *Secondary Synchronization Signal* (*SSS*). Both are used to transfer the Physical Cell ID as well for symbol/slot/frame timing. For an attacker it is more efficient to spoof the PSS and SSS signals instead to jam them. Jamming PSS or SSS selectively in time requires synchronization to the cell in time and identification of the subcarrier space. Spoofing of PSS or SSS does not require cell synchronization.

2.5.2. Vulnerability of PBCH

The transmission of physical broadcast channel (PBCH) takes place in the same slots as the slots where PSS and SSS are transmitted. The difference is that PBCH includes more subcarriers than PSS or SSS. While both PSS and SSS are made up of a set of 127 subcarriers each of them, PBCH is mapped into a set of 240 subcarriers. Below the frequency of 3 GHz the associated resource elements (one subcarrier by one OFDM symbol) are distributed in 12 symbols following one another in the time axis. Above the limit of 3 GHz the associated elements in the 240 subcarriers are distributed in 24 symbols following one another in the time axis of the frequency-time grid. The PBCH transfers the *Master Information Block* (*MIB*). The MIB information enables the successful initial access of a UE to a cell eNodeB and therefore, is essential. Some parameters of MIB are downlink system bandwidth, control information, and information for frame synchronization. Jamming PBCH will prevent the UEs to access the MIB and thereafter to connect to one or more cell eNodeBs. If we assume that the jammer can synchronize to the target cell eNodeB, PBCH jamming can be used in a time-selective way. If synchronization is not possible the jammer could jam the subcarriers that include PBCH using a duty cycle of 100%. Considering that the PBCH region occupies 240 subcarriers a 15 MHz

downlink with 15 kHz subcarriers (1000 subcarriers) means jamming of 24% of the downlink signal.

2.5.3. Vulnerability of PDCCH

The PDCCH is used to organize modulation, uplink transmissions, downlink transmissions, and transmission coding format. Using the information carried over the PBCH the UEs determine the location of the system information block (SIB) messages, which are carried over the PDCCH. The SIB messages contain critical mobile network information, including cell configuration, the eNodeB's idle timer, the physical random-access channel (PRACH) configuration and the paging channel (PCH) configuration. *CORESET* is a group of parameters to carry PDCCH as well a set of physical resources, e.g., a particular area in the 5G NR Downlink Resource Grid. CORESET maps a set of physical resources using a set of parameters (e.g., *CORESET-freq-dom*, and *CORESET-time-duration*). These parameters are used to carry PDCCH. LTE PDCCH and 5G NR PDCCH are equivalent. Their difference is that while in the LTE CORESET area PDCCH spread across the whole channel bandwidth, in the 5G NR CORESET PDCCH is in a special region of the frequency domain. To jam the PDCCH channel is a bigger challenge than to jam the PBCH channel. PDCCH can occupy any subcarrier. If the attacker has no knowledge of CORESET-freq-dom, then the jammer must take into account all possible areas in which PDCCH can be located. It could be easier for an attacker to jam PDCCH if the attacker knows the CORESET freq-domain. To achieve that the jammer needs access to the frequency domain resource parameters. The jammer must intercept and decode the CORESET freq-domain. PDCCH that is QPSK modulated starts directly in the first symbol in every slot. To successfully jam all regions in the frequency-time grid that include the PDCCH, CORESET-freq-dom must be known, and the jammer should jam every subcarrier using a duty cycle that depends on the value of the CORESET-time-duration parameter. The number of OFDM symbols per slot that PDCCH occupies is set in the parameter CORESET-time-duration that takes values 1, 2 or 3. Jammer could jam with 7% duty cycle if CORESET-

time-duration is 1, with 14% duty cycle if CORESET-time-duration is 2, and with 21% duty cycle if CORESET-time-duration is 3. The attack success depends on whether and how long the attacker needs to intercept and decode CORESET.

2.5.4. Vulnerability of PRACH

When a UE wants to connect to an eNodeB it initializes a cell search. First UE receives PSS, SSS, and PBCH and synchronizes to the cell eNodeB in time and frequency. After the synchronization with the cell eNodeB the UE initiates the *random access* (*RA*) procedure to establish a network connection. With the help of the RA procedure, an uplink transmission, the UE transmits a preamble to the eNodeB using the *physical random-access channel* (*PRACH*). The UE transmission of the preamble makes use of the Zadoff-Chu encoded modulation scheme and has the form of a Zadoff-Chu sequence. A special value in the preamble clearly (temporarily) specifies the UE and the eNodeB becomes aware of the presence of the UE and that the UE wants to connect to the cell. The base station receives the preamble, allocates radio resources for the desired communication with the UE, makes an estimation of some temporal synchronization parameters and broadcasts all this information on PRACH. The base station also broadcasts the candidate locations of the PRACH for the case that UE wants to connect to the network. Due to the considerable number of possible locations and due to the complexity of the process for their real-time discovery (decode positions in real-time), it is difficult to jam PRACH, however it is not impossible. If the jammer cannot determine these locations, it can flood the channel using invalid preambles as in 5G NR there is no specification to manage this scenario.

2.5.5. Vulnerability of PUCCH

UE uses the *physical uplink control channel* (*PUCCH*) to send scheduling requests, control information, and channel state information to the base station. Five different PUCCH formats with different parameters and options are in use. PUCCH uses a defense mechanism named intra-slot

hopping. This mechanism can provide some protection against selective jammers although all information about intra-slot hopping in 5G is a public standard. The announced security depends on the hopping rate. If the jammer knows the intra-slot hopping, a jamming attack against PUCCH is easy. PUCCH is modulated with MPSK, $m = 2$ (BPSK) or 4 (QPSK) and uses polar code, repetition code, simplex code, or Reed Muller code as an error coding scheme, depending on the number of bits should be transmitted. Polar codes do not offer sufficient security against jamming attacks. Jamming only the PUCCH will not block all uplink control information because uplink control information can be transferred on the PUSCH. We conclude that PUCCH is a complicated physical channel and difficult to jam.

2.5.6. Vulnerability of Massive MIMO

One feature in 5G NR networks is the use of massive multiple input multiple output (MIMO) antennas to enhance coverage and capacity of wireless base stations. It is generally known that massive MIMO systems are vulnerable to jamming. Miller et al. [17] describes different jamming attacks against SVD-based MIMO systems. These attacks are valid also for 5G NR networks. The target of jamming in MIMO systems is the channel estimation. An attacker can establish active jamming attacks against ingenuous users. Under jamming conditions accurate channel estimation is important to achieve the desired performance for which MIMO systems were designed. Extensive research is necessary for design and implementation of techniques for accurate channel state estimation that cannot be influenced from the presence of jammers.

2.5.7. Vulnerability of low-density-parity-check-coding (LDPC) and polar coding

Regarding the coding schemes, as already mentioned, 5G NR can use polar coding for the control channel. Use of polar coding is efficient with large portions of data (performance close to the Shannon limit). For error correction in the data channel 5G NR uses low-density parity check (LDPC). In contrast to polar code, LDPC performs well for small portions of data. Polar coding and LDPC are both vulnerable to jamming.

2.5.8. Detection and mitigation of jamming attacks in 5G NR

The detection of jamming attacks can be implemented in three main ways.

Machine learning based. Different machine learning techniques have been investigated for effectiveness regarding the detection of jamming attacks, e.g., support vector machines, decision trees, expectation maximization, or deep learning. Deep learning is more suitable for detecting jamming attacks (high accuracy) in an experimental environment but not in real systems because of the lack of public real-word datasets to train the machine learning models.

Statistical based detection. This detection method uses historical data and tries with the creation of statistics to differ between jammed and not jammed signals. Statistical based detection of jamming can be very accurate in the case of constant jammers.

Monitoring excessive energy on a physical channel or very large change in its performance. Excessive energy in a physical channel or very large performance change in the communication can be an indication of jamming. This detection method uses a threshold considering performance metrics like signal-to-noise ratio (SNR), packet drop ratio (PDR), bit error rate (BER), and packet delivery ratio (PDR). The threshold is set after monitoring the performance values with and without jamming attacks. Jamming attacks can be detected (high false alarm) in the case of constant jammers.

Typical frequencies in 5G NR networks will be higher than 30 GHz. For a jammer this means that a lot of energy must be available to jam the signal. Aside from that 5G NR offers techniques such as frequency hopping (FH), and direct sequence spread spectrum (DSSS). Next, we analyze the capabilities of these techniques to prevent jamming in 5G NT networks.

Direct sequence spread spectrum (*DSSS*). Signal spreading is a method to protect against jamming attacks. The nature of our data signal is a narrow band signal. Direct sequence spread spectrum (DSSS) is a modulation

technique to increase the bandwidth of a baseband signal, in case of our data signal. This can be done by multiplying the data signal with a wideband pseudo-noise (PN) sequence that can be viewed as a spreading code. Spreading code can be considered as a pre-shared secret key between a transmitter and a receiver to expand a data signal. The multiplication of both signals results into several small-time increments called *chips*. The product (modulated) signal is a new signal having spectrum nearby the wideband of the PN. The data signal is propagated in this way through the channel, and it is difficult for an adversary to detect it. DSSS is a powerful countermeasure against jamming attacks, and it performs attack 'camouflaging' method. DSSS techniques are powerful but have limitations due to the capabilities of the physical devices used to generate the PN sequence. The processing gain of a system that is used to countermeasure jamming attacks is a function of the PN sequence period. The smaller the chip duration of the PN sequence the larger the processing gain and the greater transmission bandwidth with more chips per bit is possible. But physical devices do not have unlimited possibilities to generate the PN spread spectrum, and repeatedly to always increase the processing gain and to overcome jammers. Alternative methods are therefore also in demand [18].

Frequency-hopping spread spectrum (*FHSS*). One other method is Frequency-hopping spread spectrum (FHSS). In FHSS the data-modulated carrier randomly hops from one frequency to the next. This forces the jammer to try to attack a larger spectrum area. In FHSS the transmitted signal spectrum is spread sequentially (one frequency hop after the other) and not instantaneously. FHSS systems use M-ary frequency-shift keying (MFSK) as modulation. One of the FH characteristics is the hopping rate. A distinction is made between *Slow Frequency Hopping (SFH)* and *Fast Frequency Hopping (FFH)*. In SFH with each frequency hop more than one symbol should be transmitted. In FFH the carrier frequency changes several times during the transmission of one symbol. The use of FHSS is subject to certain restrictions. SFH is not suitable if jammers are used that find the next frequency hop faster than the time the transmitter needs to switch to the next frequency. FFH could have an impact on the performance of communication

between transmitter and receiver because the synchronization between transmitter and receiver becomes more difficult. Sender and receiver must agree on the pattern according to which they will operate frequency hopping. To do this, they need to exchange a pre-shared key. The key exchange can be intercepted by an eavesdropper.

Some other technologies for jamming mitigation in 5G NR networks. There are some other approaches to countermeasure jamming attacks:

- *Game theory*: Jamming defense can be viewed as a game between adversary and legal user, e.g., where legal users can proactively implement frequency hopping to minimize the payoff function. Game theory can find the optimal strategy to defend against a jammer (find the Nash equilibrium) [19-21] and [22].

- *Timing channel*: Another approach is to use the timing channel. This approach consists of two steps. The first one is the detection of the jammer(s) and the second one is the creation of a time channel to take advantage and to send and receive in the period where jammers are inactive [23].

- *SDN*, *NFV and deep learning*: The increasing demand for high-quality multimedia services created a new paradigm in network administration regarding separation, abstraction, and mapping of management aspects of services. 5G supports programmable control and management of network resources using Software-Defined Networking (SDN) and Network Function Virtualization (NFV) [24]. With the help of SDN and NFV, the physical network can be divided into multiple isolated logical networks with different sizes and structures which are dedicated to different types of services. SDN, NFV in combination with deep learning can contribute to build intelligent radio resource allocation and user scheduling, learn the jammer master plan, reduce jamming attacks, and maximize network performance [25].

- *Massive MIMO suppression of jammers*: This approach includes the creation of robust channel coding schemes with the goal to correct corrupted packets and to exhaust the adversary jammers [26].

- *Use of machine learning and UAVs*: UAV aided 5G NR wireless communication in combination with reinforcement learning on UAV side is an additional approach to avoid jamming attacks. When a base station is attacked, UAVs can be used as relays. The optimal relay policy for 5G NR users can be learned using deep reinforcement learning techniques [27]. A challenge of this approach is the vulnerability of UAVs to jammer attacks.

In summary, it can be said that the security requirements of 5G must become part of the design of 5G, e.g., base stations should offer jamming defense mechanisms. A mechanism for preventing jamming in 5G NR that requires further research is the use of deep learning techniques under the consideration of different jammer types and the use of large data set for training to identify legitimate user signals from jamming signals. A significant part of this technique is sensing for jammer strategy detection and use of frequencies and channels that are not jammed. The direct spread spectrum approach as jamming countermeasure offers high protection; however, the corresponding solutions are complex. Due to the possibility of jammers to detect the next hopping frequency, this technique is not suitable to countermeasure jamming. Timing channels in combination with detection techniques for the attacker timing can be a solution against jamming. The discussed machine learning approach is impractical because of the long time it takes to train for some 5G applications. Use of UAVs against jamming is a very promising approach that needs further consideration. More research is needed to increase the 5G NR defense ability against jamming.

2.6. Jamming attacks in cognitive radio networks and mitigation

The *Cognitive Radio Networks* (*CRN*) technique addresses the spectrum shortage problem. CRN enables the coexistence of primary users (*PUs*) and secondary users (*SUs*) in licensed spectrum bands. Primary users are licensed (incumbent) users and secondary users are unlicensed (cognitive) users. With *Cooperative Spectrum Sensing* (*CSS*), we understand the combination of spectrum sensing results from multiple cognitive users used to autonomously identify unused portions of the radio spectrum, to improve spectrum utilization, and thus to avoid interference to PU's. The CSS

process consists of: (1) spectrum sensing for signal detection, (2) the hypothesis analysis if medium is busy, and (3) the data fusion of the results of the hypothesis analysis from the SUs that are part of the CRN. Signal detection can be implemented, e.g., through matched filtering or energy detection. Matched filtering uses the knowledge of the PU's protocols, e.g., packet format, to detect if PU transmissions are present. Energy detection cannot differentiate between PU signal transmission, interference, or noise signals, and thus this reduces sensing accuracy. Using hypothesis analysis SUs decide if the sensed medium is busy or not. Hypothesis analysis can be implemented, e.g., through the sequence probability ratio test, or the Bayesian test. In the third step the SU decisions are integrated (data fusion) using a centralized or decentralized setting.

Four types of attacks against CRNs are known. These are:

- *learning-based jamming attacks*
- *false-report attacks*
- *jamming attacks on secondary network and common control channel*
- *primary user emulation* (*PUE*) *attacks*.

Learning-based jamming attacks on cognitive radio networks are based on deep learning classifiers. Deep learning classifiers consider recent sensing results, and they are used from cognitive radio transmitters as pre-trained classifiers to predict the current channel status. Jammers used for attacks take advantage of deep learning classifiers and select channel status information (CSI) and ACKs to build a deep learning classifier that can predict signal transmissions in the spectrum and jam them afterwards. Erpek et al. [28] found out that learning-based jamming attacks are more effective than random or sensing-based jamming.

In case of use of a centralized setting in step three (data fusion) in the CSS process, a *false-report attack* is a method to send misleading channel sensing reports to the fusion center. This false report information leads to false decisions regarding the sending activity of PUs. This kind of attack is

also known as spectrum sensing data falsification (SSSDF) attack or Byzantine Attack [29]. False-Report Attacks can be initiated through a malicious attack or through a selfish attack. In both the attacks, the malicious network or the attacker respectively injects or reports into the fusion center misleading sensing results to cause false decisions about the used spectrum.

Jamming Attacks on Secondary Network and Common Control Channel are aimed at causing denial of service to the secondary network in CRNs. Common Control Channel is used by secondary nodes for sharing their channel sensing reports. The attack overwhelms the secondary network by fake MAC control frames, and it is difficult to detect it due to the small number of control packets it needs to transfer and due to the injection of MAC control frames that correspond to the secondary networks protocol.

Primary User Emulation (*PUE*) *Attacks*. The process of a SU leaving the channel due to a PU signal sending and the SU re-sense of the spectrum to find other idle channels is known as *spectrum hand-off*. Through the new re-sense SUs waste time and this means a performance degradation of the spectrum use. This concept can be misused by an adversary to prevent SUs to access the channel. In the Primary User Emulation (PUE) Attack, an attacker emulates the PU and causes the SU to leave the channel. Here too, the attack can be initiated as a malicious attack or a selfish attack.

Usual countermeasures against jamming attacks apply also against CRN attacks. A countermeasure type that is uniquely designed for CRNs is the *Random channel hopping*.

2.7. Jamming attacks in vehicular wireless networks and mitigation

In this section, we introduce jamming attacks and countermeasures in on-ground vehicular ad-hoc networks (*VANET*). Two challenges in the design of VANETs are: (1) their delay-sensitive communication network, and (2) their high traveling speed of the vehicle. In this context, we meet the terms vehicle-to-vehicle (V2V) communications and vehicle-to-infrastructure (V2I) communications. The *Dedicated short-range communication* (*DSRC*) is a system for the wireless connectivity of

VANETs. DSRC is based onto IEEE 802.11p standard. This standard uses for data transmission the same frame format as Wi-Fi. A VANET consists of *on-board units* (*OBUs*) and *roadside units* (*RSU*). Every RSU is an access point in VANET, like a Wi-Fi access point. 802.11p applies at the Link Layer (or MAC layer) carrier sensing for channel access. The protocol includes the *enhanced distributed channel access* (*EDCA*) technique to make critical message exchanging possible.

While detecting jamming attacks is important towards enhancing road safety (e.g., car collision), it is challenging because VANET operates in outdoor environment with highly changeable road conditions and atmospheric phenomena and encompasses volatile topology and high mobility of vehicles (travelling speed and directions) [30]. Azogu et al. [31] deal with the impact of jamming attacks on V2V and V2I IEEE 802.11p-based communications. In the study the jammer switches dynamically to in-use channels. The authors proved that 10 radio jammers can decrease the packet sent ratio (PSR) to 0.4.

Punal et al. in [32] and in [33] analyze the throughput of V2V communications applying different kinds of jamming attacks, e.g., reactive, periodic, and constant jamming attacks in combination with a real software defined radio (SDR) implementation. In their experiments they found that when *signal-to-noise-plus-jamming ratio* (*SNJR*) is less than 9 dB applying a constant jamming attack, then the packet delivery rate in 802.11p communications tends to 0. In case of a periodic jamming attack and SNJR less than 55 dB, 74 microseconds period, and duty cycle of 86% the packet delivery rate drops to 0 as well. The same also in case of a reactive jamming attack with SNJR less than 12 dB with 40 microseconds as packet detection duration, and 500 microseconds jamming signal duration. Countermeasure against jamming in VANETs is a research area that is not well explored. One strategy against jamming is to switch to a second wireless network, e.g., to a cellular one, assuming there is one. Also, the use of frequency hopping and data relaying common techniques against jamming is an additional option. A countermeasure against jamming in VANETs is presented in [34] and [27].

The authors use UAV devices against a jammer, which continuously changes its attack strategy. When a RSU is under jamming attack, the UAV is used to relay the vehicle data to another alternative RSU.

2.8. Jamming attacks in Fly Ad-hoc networks and mitigation

In this section, we introduce jamming attacks and countermeasures in in-air unmanned aerial vehicular (*UAV*) ad-hoc networks. UAVs have a wide application range. For the different applications of UAVs, there exist different UAV sizes. Small UAVs are used for example in film-making or agricultural monitoring. Bigger UAVs are used for armed attacks, disaster response, or rescue missions. UAVs can be deployed in a network. Their speed can be up to 100m/s depending on the application. Most of them operate in the 2.4 GHz and 5.8 GHz ISM bands. As network topologies, star topology and mesh network topology are in use. Star topology is used when every UAV communicates with a ground control station. The mesh network topology is used when all UAVs build with each other an ad-hoc network, while a small number of them communicate directly with the ground control station. Bigger UAVs can use satellite communication (SATCOM) to manage their routing. UAVs are vulnerable to constant, to reactive, to deceptive, and to random and periodic jamming attacks. Jammers of satellite-based UAV networks target GPS communications to disturb UAV networks. Hartman et al. [35] consider this as a possible reason regarding the loss of a military UAV (RQ-170 Sentinel) to Iranian military forces. A GPS-spoofing attack might have carried out, spoofing the position estimation of the UAV, and hijacking the UAV's routing decision. Rudinskas et al. [36] investigates the control command attack, an UAV jamming attack. The jammer in this attack tries to interrupt the control commands sent by the ground control station to the UAV. Jamming takes place using conventional jamming attacks to block the received signal. In research, one rarely finds techniques against jamming on UAVs.

3. Friendly Jamming

3.1. What is friendly jamming?

Friendly Jamming (*FJ*) is a mechanism that enables message authentication and access control and protects confidentiality of transmitted data in wireless networks [37]. Intention of the implementation of message authentication and access control through friendly jamming is to block attacker communication with a protected device. Using friendly jamming, we can also implement confidentiality protection to degrade attacker's channel in a way that user message decoding through the attacker is unachievable. Thus, friendly jamming is used to: (i) prevent attacker communication with protected devices, and (ii) prevent an attacker to eavesdrop messages.

3.2. How does friendly jamming work?

The working principle of friendly jamming to achieve confidentiality is based on superimposition of the confidential message and the jamming signal, e.g., a relay node, of a friendly jammer at the attackers' antennas. Friendly jamming scenarios consist of a transmitter (the data source for the creation of the confidential message), a receiver (receives the protected data message), the friendly jammer for placing the jamming signal, and the attacker. The use of the jammer intends to degrade the channel between transmitter and attacker in a way that the attacker cannot decode the transmitter messages. Nevertheless, the legitimate receiver must not be influenced and must be able to continue to receive the signal sent by the transmitter. Whether an attacker will be able to decode the received superimposed signal depends on the following factors:

- the respective distances between data source, jammer device, and attacker antenna(s)
- the configured environment itself
- the message signals, and the jamming signals.
- the respective locations of the attacker, the data source, and the jamming device.

Two types of friendly jammers exist:

- *Nearby jammers*. In nearby jammer systems, the distance between the jammer and the transmitter is less than a half of the carrier wavelength. This type of jammers assumes that there is a high correlation between the message and the jamming signal envelope, and therefore both signals cannot be separated through an attacker.

- *Remote jammers*. In remote jammer systems, the distance between the jammer and the transmitter is larger than a half of the carrier wavelength. This type of jammers assumes, that the attacker uses a single omni-directional antenna and due to this assumption attacker cannot separate in his antenna the two messages.

3.3. Reactive vs. Proactive jamming

Proactive friendly jamming presupposes emitting a continuous and high-power signal through the jammer device. In reactive friendly jamming, the signals can be analysed. The jamming signal is generated after the detection of certain type of signals that must be interfered. Reactive jamming is energy-efficient [6]. It is more regulatory-compliant than proactive friendly jamming. A challenge that the reactive friendly jamming faces is the strict timing constraints for its application. Reactive friendly jamming first senses the channel to detect target frames and decode them. The efficient detection of the target frames depends on the position of the jammer device with respect to the target frames transmitter and additionally on present environmental conditions. After detection and decoding the jammer analyses the signals and must decide very fast if the sensed signals are legitimate frames or target frames. After that, target frames must be jammed with a maximal jamming hit ratio (number of jammed frames/number of sent frames), while legitimate frames should be minimally exposed on jamming. After sensing and analyzing the received signal the jammer device switches from receive to transmission mode and emits the jamming signals. Successful friendly jamming depends on the modulation and coding scheme of the target frames, as well as on the power of the jamming signal. High power jamming signal leads to high jamming access but otherwise high-

power jamming signal is subject to legal regulations and has negative effects on legitimate wireless network traffic. A success factor for reactive jamming is the use of concurrent jammers to improve target frame detection and power level of the jamming signal. The role of power is described by the *Power Design Problem*.

3.4. Power design problem

Secrecy capacity is defined as "the difference between the capacity of the intended communication channel and the capacity of the eavesdropper channel" [37]. The *Power Design Problem* is an optimization problem and can be described as maximization of the achievable secrecy capacity under the preconditioning of a limitation of the total transmission power. The same optimization problem can be described as minimization of the total transmission power under the preconditioning of a limitation of the achievable secrecy capacity.

3.5. Friendly jamming application fields

In the last fifteen years some important fields of application of friendly jamming have been established:

- *Protection of implantable device*: An application example is the protection of implantable medical devices (IMDs) described by Gollakota et al. [38].

- *Development of* '*firewall*' *functionality in IEEE* 802.15.4 *wireless networks using reactive jamming*: An implementation on a USRP2 software-defined radio platform is presented by Wilhelm et al. [39].

- *Detection of impersonated and unauthenticated wireless transmissions*: Martinovic et al. describe in [40] the so-called attack cancelation, a friendly jamming method for detection and destroying fake frames in wireless sensor networks.

- *Solve the hidden terminal problem.* Cai et al. use friendly reactive jamming to solve the hidden terminal problem. The hidden terminal problem occurs when a node A and a node B can communicate with an Access Point (AP) but cannot directly communicate with each other [41].

• *Protection of networks with a variety of protocol types*, *e.g.*, *like smart homes* [42]: Many different communication protocols are used in home automation. Most of them lack basic security features. Friendly jamming can be a sensible alternative security method.

• *Build walled wireless coverage or secure Wi-Fi zones in WLANs*: Kim et al. [43] propose an approach to forge secure zones and protect WLANs from information leakage.

• *Physical layer key generation*: Gollakota et al. [44] demonstrate a physical-layer approach for secret key generation. The presented approach is fast and independent of channel variations.

• *Confidentiality improvement* (will be analysed in the next section).

• *Improvement of authentication and access control* (will be analysed in the next section).

In traditional radio frequency jamming attacks, the goal of the attacker is to block legitimate communication. Friendly radio frequency jamming implements the requirement of *minimal invasiveness* [45], it targets only specific transmissions and legitimate communication is not or minimal affected. To achieve minimal invasiveness friendly jamming techniques, deploy reactive and frame-selective jamming.

3.6. Using friendly jamming for improving confidentiality (secrecy of communications)

Confidentiality protection normally can be achieved by encryption at the upper layers of the protocol architecture. Due to different circumstances, (e.g., shared keys cannot be distributed or used, encryption cannot always take place) the application of friendly jamming is a feasible mechanism to achieve in such cases the confidentiality. Friendly jamming is also used as a second layer of protection additionally to encryption. Friendly jamming can be used for the protection of the initial key establishment. Tippenhauer et al. [37] construct a MIMO-based attack against data sources that protect their data by friendly jamming based on the nearby jammers scheme and shows

that friendly jamming is not always a strong guarantor for confidentiality, (e.g., friendly jamming fails to ensure confidential communication in the Medical Implant Communication Service (MICS) band).

3.7. Using friendly jamming for improving authentication and access control (blocking unauthorized communications)

Shen et al. [46] introduced in their paper the concept of *Ally Friendly Jamming*. Ally Friendly Jamming is a mechanism to disable unauthorized (e.g., enemy) wireless devices and at the same time to allow authorized wireless devices to communicate, even if all these devices operate at the same frequency. The core idea of Ally Friendly Jamming is continuous jamming of the wireless channel and use of secret keys to control the jamming signals. Unauthorized devices interpret the sensed jamming signals as unpredictable interference. Authorized devices provided with the secret keys can recover the friendly jamming signals, remove them from the mixed signals and get the jamming-free messages.

3.8. Use of friendly jamming in different networks

Friendly jamming is a research area with increasing interest in recent years. This subsection describes the use and the technical challenges of Friendly Jamming for some scenarios and examples.

3.8.1. Friendly jamming in an IEEE 802.11 network and on access points

The fast reaction time in IEEE 802.11 based devices is a challenge in enabling friendly jamming. Bayraktaroglu et al. [47] conclude, that it is not possible to target high data rate IEEE 802.11 due to fast reaction time which is in order of milliseconds. This is the reason for the use of IEEE 802.15.4 to evaluate friendly jamming, which is slower. Access Points are used in IEEE 802.15.4 and at the same time are natural candidates to implement friendly jamming functionality with the goal to block malicious or unauthenticated communication. There are many reasons to implement friendly jamming in APs. Nodes in a wireless network apply the IEEE 802.1 or 802.15.4 protocol and they do not offer any security functionality. APs are placed in suitable

locations to ensure coverage of all nodes in the wireless network. Additionally, network state information is mainly located at the APs to control wireless network operations. Finally, APs keep up to date with current and future standards to meet the regulations. Implementation of friendly jamming in APs can take place through AP software modification /upgrade and that brings some challenges. The real-time requirements of friendly jamming necessitate its implementation in network interface card (NIC). The NIC firmware must be able simultaneously to receive and to analyze the network frames as well as to stop reception, change to transmit mode and start to (friendly) jam. The last requirement is opposite to the current IEEE 802.11 collision avoidance scheme and therefore it is a challenge.

3.8.2. Using friendly jamming and Fly Ad-hoc networks

Friendly jamming using stationary located jammers have some limitations, (e.g., high construction costs, effect of legitimate communications due to improper placement and use for only specific application scenarios). Drone small cells (DSCs) are aerial base stations used to support communications in the air. DSCs that are composed of multiple UAVs can be deployed as a relay or can be used for friendly jamming (can e.g., carry device-to-device communication). Wang et al. describe a scheme against eavesdropping which is based on the use of multiple unmanned aerial vehicles (UAVs) and friendly jamming [48] to blind eavesdroppers and to protect Industrial Internet of Things. Legitimate users are randomly distributed and operate only in a so-called protection region with Radius R. Jamming-enabled UAVs flying on the air and transmit jamming signals as artificial noise inside a region called interference region, which is the area protected in the ground. The authors conclude that their simulations show that their model has nearly no impact on legitimate communications, and it effectively mitigates the eavesdropping probability.

3.9. The cost of friendly jamming

Friendly jamming can affect loss of legitimate wireless network traffic and cause loss of *power amplification*. Using multiple jammers for friendly

jamming increases the jammers hit ratio. It can also damage legitimate frames in the air [4]. Especially in a wireless LAN the *Hidden Station Problem* (*HSP*) occurs when two transmitters that are hidden from each other, send signals to a single receiver considering the receiver to be free. The transmitters cause then collisions at receivers' side. The HSP reduces the network capacity. The *power amplification effect* is a new type of HSP and enters when a friendly jammer intentionally blocks an attack but simultaneously and accidentally interfere with legitimate transmissions. The more jammers are active, the more packet losses due to power amplification effect are observed. The power amplification effect induces a significant increase of the interference range of any transmission (for the legitimate transmission as well). Therefore, it can be said that the cost of friendly jamming has its origin to the power amplification effect and should be considered as a cost factor in addition to other traditional metrics and security measurements.

4. Conclusion

In this paper, we presented the main working principles of jamming and its difference to interference as well as a comprehensive survey on jamming techniques, their application fields, their limitations, and challenges for different kinds of networks such as WLANs, 5G New Radio, cognitive radio networks, vehicular wireless networks, and fly ad-hoc networks. We presented the working principles of friendly jamming techniques, their application fields, and described the use of friendly jamming to improve confidentiality as well authentication and access control. Our research moves ahead to analyze and develop friendly jamming, jamming, and jamming detection techniques using Artificial Intelligence methods for Fly Ad-hoc networks, which is a very promising research area.

References

[1] David Adamy, EW 101: A first course in electronic warfare, Artech House radar library, Artech House, 685 Canton Street, Norwood, MA 02062, 2001.

[2] David Adamy, EW 103: Communications electronic warfare, 2008.

[3] Adrian Graham, Communications, Radar and Electronic Warfare, John Wiley & Sons, 2011.

[4] Daniel S. Berger, Francesco Gringoli, Nicolò Facchi, Ivan Martinovic and Jens B. Schmitt, Friendly jamming on access points: analysis and real-world measurements, IEEE Trans. Wirel. Commun. 15(9) (2016), 6189-6202.

[5] National Institute of Standards and Technology, Jamming, 2021.

[6] Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood, The feasibility of launching and detecting jamming attacks in wireless networks, Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc 2005, Urbana-Champaign, IL, USA, May 25-27, 2005 (P. R. Kumar, Andrew T. Campbell and Roger Wattenhofer, eds.), ACM, 2005, pp. 46-57.

[7] Levente Buttyán and Jean-Pierre Hubaux, Security, and Cooperation in Wireless Networks - Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing, Cambridge University Press, Cambridge, 2007.

[8] Marc Lichtman, Jeffrey D. Poston, Sai Dhiraj Amuru, Chowdhury Shahriar, T. Charles Clancy, R. Michael Buehrer and Jeffrey H. Reed, A communications jamming taxonomy, IEEE Secur. Priv. 14(1) (2016), 47-54.

[9] Jean-Pierre Hubaux, Security and Cooperation in Wireless Networks, Security and Privacy in Ad-Hoc and Sensor Networks, Third European Workshop, ESAS 2006, Hamburg, Germany, September 20-21, 2006, Revised Selected Papers (Levente Buttyán, Virgil D. Gligor and Dirk Westhoff, eds.), Lecture Notes in Computer Science, Vol. 4357, Springer, 2006, 1-2.

[10] David L. Adamy, EW 104: Electronic warfare against a new generation of threats -ew100, Artech House, Inc., USA, 2015.

[11] Alejandro Proaño and Loukas Lazos, Selective jamming attacks in wireless networks, Proceedings of IEEE International Conference on Communications, ICC 2010, Cape Town, South Africa, 23-27 May 2010, IEEE, 2010, pp. 1-6.

[12] Triet Dang Vo-Huu, Tien Dang Vo-Huu and Guevara Noubir, Interleaving jamming in wi-fi networks, Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, WISEC 2016, Darmstadt, Germany, July 18-22, 2016 (Matthias Hollick, Panos Papadimitratos and William Enck, eds.), ACM, 2016, pp. 31-42.

[13] Clayton W. Commander, Panos M. Pardalos, Valeriy Ryabchenko, Stan Uryasev and Grigoriy Zrazhevsky, The wireless network jamming problem, J. Comb. Optim. 14(4) (2007), 481-498.

[14] Clayton W. Commander, Panos M. Pardalos, Valeriy Ryabchenko, Oleg V. Shylo, Stan Uryasev and Grigoriy Zrazhevsky, Jamming communication networks under complete uncertainty, Optim. Lett. 2(1) (2008), 53-70.

[15] Youness Arjoune and Saleh Faruque, Smart jamming attacks in 5g new radio: A review, 10th Annual Computing and Communication Workshop and Conference, CCWC 2020, Las Vegas, NV, USA, January 6-8, 2020, IEEE, 2020, pp. 1010-1015.

[16] Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan M. Rao, Vuk Marojevic and Jeffrey H. Reed, Lte/lte-a jamming, spoofing, and sniffing: threat assessment and mitigation, IEEE Commun. Mag. 54(4) (2016), 54-61.

[17] Robert D. Miller and Wade Trappe, On the vulnerabilities of CSI in MIMO wireless communication systems, IEEE Trans. Mob. Comput. 11(8) (2012), 1386-1398.

[18] Simon Haykin and Michael Moher, Communication Systems, Wiley, New York, 2009.

[19] QiweiWang, Thinh Nguyen, Khanh D. Pham and Hyuck M. Kwon, Mitigating jamming attack: a game-theoretic perspective, IEEE Trans. Veh. Technol. 67(7) (2018), 6063-6074.

[20] Beibei Wang, Yongle Wu, K. J. Ray Liu and T. Charles Clancy, An anti-jamming stochastic game for cognitive radio networks, IEEE J. Sel. Areas Commun. 29(4) (2011), 877-889.

[21] Luliang Jia, Yuhua Xu, Youming Sun, Shuo Feng and Alagan Anpalagan, Stackelberg game approaches for anti-jamming defense in wireless networks, IEEE Wirel. Commun. 25(6) (2018), 120-128.

[22] Dejun Yang, Guoliang Xue, Jin Zhang, Andréa W. Richa and Xi Fang, Coping with a smart jammer in wireless networks: A Stackelberg game approach, IEEE Trans. Wirel. Commun. 12(8) (2013), 4038-4047.

[23] Wenyuan Xu, Wade Trappe and Yanyong Zhang, Anti-jamming timing channels for wireless networks, Proceedings of the First ACM Conference on Wireless Network Security, WISEC 2008, Alexandria, VA, USA, March 31 - April 02, 2008 (Virgil D. Gligor, Jean-Pierre Hubaux and Radha Poovendran, eds.), ACM, 2008, pp. 203-213.

[24] Salvatore D'Oro, Eylem Ekici and Sergio Palazzo, Optimal power allocation and scheduling under jamming attacks, IEEE/ACM Trans. Netw. 25(3) (2017), 1310-1323.

[25] Alcardo Alex Barakabitze, Arslan Ahmad, Rashid Mijumbi and Andrew Hines, 5g network slicing using SDN and NFV: a survey of taxonomy, architectures, and future challenges, Comput. Networks 167 (2020). https://doi.org/10.1016/j.comnet.2019.106984

[26] Hossein Akhlaghpasand, Emil Björnson and S. Mohammad Razavizadeh, Jamming suppression in massive MIMO systems, IEEE Trans. Circuits Syst. II Express Briefs 67-II (1) (2020), 182-186.

[27] Liang Xiao, Xiaozhen Lu, Dongjin Xu, Yuliang Tang, Lei Wang and Weihua Zhuang, UAV relay in vanets against smart jamming with reinforcement learning, IEEE Trans. Veh. Technol. 67(5) (2018), 4087-4097.

[28] Tugba Erpek, Yalin E. Sagduyu and Yi Shi, Deep learning for launching and mitigating wireless jamming attacks, IEEE Trans. Cogn. Commun. Netw. 5(1) (2019), 2-14.

[29] Linyuan Zhang, Guoru Ding, Qihui Wu, Yulong Zou, Zhu Han and Jinlong Wang, Byzantine attack and defense in cognitive radio networks: a survey, IEEE Commun. Surv. Tutorials 17(3) (2015), 1342-1363.

[30] Sharaf J. Malebary, Wenyuan Xu and Chin-Tser Huang, Jamming mobility in 802.11p networks: Modeling, evaluation, and detection, 35th IEEE International Performance Computing and Communications Conference, IPCCC 2016, Las Vegas, NV, USA, December 9-11, 2016, IEEE Computer Society, 2016, pp. 1-7.

[31] Ikechukwu K. Azogu, Michael T. Ferreira, Jonathan A. Larcom and Hong Liu, A new anti-jamming strategy for vanet metrics-directed security defense, 2013 IEEE Globecom Workshops (GC Wkshps), 2013, pp. 1344-1349.

[32] Óscar Puñal, Carlos Pereira, Ana Aguiar and James Gross, Experimental characterization, and modeling of rf jamming attacks on vanets, IEEE Transactions on Vehicular Technology 64(2) (2015), 524-540.

[33] Oscar Puñal, Ana Aguiar and James Gross, in vanets we trust? characterizing RF jamming in vehicular networks, Proceedings of the ninth ACM international workshop on Vehicular internetworking, systems, and applications, Vanet 12, Low Wood Bay, Lake District, UK, June 25, 2012 (John B. Kenney, Javier Gozálvez, Fan Bai and Robin Kravets, eds.), ACM, 2012, pp. 83-92.

[34] Xiaozhen Lu, Dongjin Xu, Liang Xiao, Lei Wang and Weihua Zhuang, Anti-jamming communication game for uav-aided vanets, 2017 IEEE Global Communications Conference, GLOBECOM 2017, Singapore, December 4-8, 2017, IEEE, 2017, pp. 1-6.

[35] Kim Hartmann and Christoph Steup, The vulnerability of uavs to cyber-attacks - an approach to the risk assessment, 5th International Conference on Cyber Conflict, CyCon 2013, Tallinn, Estonia, June 4-7, 2013 (Karlis Podins, Jan Stinissen and Markus Maybaum, eds.), IEEE, 2013, pp. 1-23.

[36] Darius Rudinskas, Zdobyslaw Goraj and Jonas Stanknas, Security analysis of uav radio communication system, Aviation 13(4) (2009), 116-121.

[37] Nils Ole Tippenhauer, Luka Malisa, Aanjhan Ranganathan and Srdjan Capkun, On limitations of friendly jamming for confidentiality, 2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013, IEEE Computer Society, 2013, pp. 160-173.

[38] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi and Kevin Fu, They can hear your heartbeats: noninvasive security for implantable medical devices, Proceedings of the ACM SIGCOMM 2011 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Toronto, ON, Canada, August 15-19, 2011 (Srinivasan Keshav, Jörg Liebeherr, John W. Byers and Jeffrey C. Mogul, eds.), ACM, 2011, pp. 2-13.

[39] Matthias Wilhelm, Ivan Martinovic, Jens B. Schmitt, and Vincent Lenders, Wifire: a firewall for wireless networks, Proceedings of the ACM SIGCOMM 2011 Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, Toronto, ON, Canada, August 15-19, 2011 (Srinivasan Keshav, Jörg Liebeherr, John W. Byers and Jeffrey C. Mogul, eds.), ACM, 2011, pp. 456-457.

[40] Ivan Martinovic, Paul Pichota and Jens B. Schmitt, Jamming for good: a fresh approach to authentic communication in wsns, Proceedings of the Second ACM Conference on Wireless Network Security, WISEC 2009, Zurich, Switzerland, March 16-19, 2009 (David A. Basin, Srdjan Capkun and Wenke Lee, eds.), ACM, 2009, pp. 161-168.

[41] Yifeng Cai, Kunjie Xu, Yijun Mo, Bang Wang and Mu Zhou, Improving WLAN throughput via reactive jamming in the presence of hidden terminals, 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, Shanghai, China, April 7-10, 2013, IEEE, 2013, pp. 1085-1090.

[42] James Brown, Ibrahim Ethem Bagci, Alex King and Utz Roedig, Defend your home! jamming unsolicited messages in the smart home, Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy (New York, NY, USA), HotWiSec' 13, Association for Computing Machinery, 2013, pp. 16.

[43] Yu Seung Kim, Patrick Tague, Heejo Lee and Hyogon Kim, Carving secure wi-fi zones with defensive jamming, 7th ACM Symposium on Information, Computer and Communications Security, ASIACCS' 12, Seoul, Korea, May 2-4, 2012 (Heung Youl Youm and Yoojae Won, eds.), ACM, 2012, pp. 53-54.

[44] Shyamnath Gollakota and Dina Katabi, Physical layer wireless security made fast and channel independent, INFOCOM 2011, 30th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 10-15 April 2011, Shanghai, China, IEEE, 2011, pp. 1125-1133.

[45] Daniel S. Berger, Francesco Gringoli, Nicolò Facchi, Ivan Martinovic and Jens B. Schmitt, Gaining insight on friendly jamming in a real-world IEEE 802.11 network, 7th ACM Conference on Security & Privacy in Wireless and Mobile Networks, WiSec'14, Oxford, United Kingdom, July 23-25, 2014 (Gergely Ács, Andrew P. Martin, Ivan Martinovic, Claude Castelluccia and Patrick Traynor, eds.), ACM, 2014, pp. 105-116.

[46] Wenbo Shen, Peng Ning, Xiaofan He and Huaiyu Dai, Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time, 2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013, IEEE Computer Society, 2013, pp. 174-188.

[47] Emrah Bayraktaroglu, Christopher King, Xin Liu, Guevara Noubir, Rajmohan Rajaraman and Bishal Thapa, On the performance of IEEE 802.11 under jamming, INFOCOM 2008, 27th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 13-18 April 2008, Phoenix, AZ, USA, IEEE, 2008, pp. 1265-1273.

[48] Qubeijian Wang, Hong-Ning Dai, Hao Wang, Guangquan Xu and Arun Kumar Sangaiah, Uav-enabled friendly jamming scheme to secure industrial internet of things, J. Commun. Networks 21(5) (2019), 481-490.