A Communications Jamming Taxonomy

Marc Lichtman, Jeffrey D. Poston, SaiDhiraj Amuru, Chowdhury Shahriar,
T. Charles Clancy, R. Michael Buehrer, Jeffrey H. Reed
Wireless@VT, Virginia Tech
Blacksburg, Virginia, USA
Corresponding Email: marcll@vt.edu

***Abstract*—With the now widespread availability of software defined radio technology for wireless networks, the distinction between jamming in the original electronic warfare sense and wireless cyber security attacks becomes hazy. In order to delineate these concepts in the rapidly expanding field of wireless security, we propose a jammer taxonomy to classify the theoretical behaviors and characteristics of communications jammers. In contrast to the historical emphasis of categorizing jammers by specific signal types, this paper organizes jammers by the information they possess and their capacity to act on it. Key jammer capabilities include whether or not the jammer is time correlated, protocol-aware, uses spoofing, and/or able to learn. Second tier characteristics include jammer parameters such as relative bandwidth, duty-cycle, modulation, antenna pattern, and whether the antenna is steerable. We then sample jamming techniques that exist in literature and discuss how they fall into our proposed classification system.**

***Index Terms*—Jamming, Taxonomy, Classification, Wireless Communications, Anti-jamming, Electronic Warfare.**

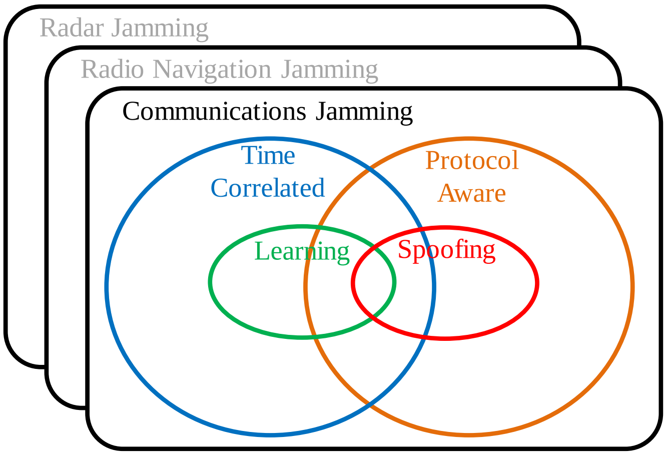

Fig. 1. Key capabilities of a jammer and how they relate.

I. Introduction

The inherent openness of the wireless medium makes it susceptible to adversarial attacks. The vulnerabilities of a wireless system can be largely classified based on the capability of an adversary: a) an eavesdropping attack in which the eavesdropper (passive adversary) can listen to the wireless channel and try to infer information b) a jamming attack in which the jammer (active adversary) can transmit energy to disrupt reliable data transmission and c) a higher-layer active attack that threatens *integrity* and *confidentiality* of a link. In this paper, we study jamming attacks, principally those at the physical (PHY) layer, intended as a Denial of Service (DoS) to one or more users, thus compromising the *availability* of a link.

Jammers may employ a wide range of behaviors to cause DoS, and a sampling of literature related to jamming will show numerous jamming models and assumptions. These models or behaviors can span in complexity from a constant source of continuous wave interference to an intelligent jammer that has the capability of sensing and making decisions in real-time to increase effectiveness and covertness of the attack.

In this paper, we propose a taxonomy that covers the communications side of jamming (as opposed to radar jamming or attacks against radio navigation). Research on electronic warfare (EW) and jamming dates to World War II, an era when jammers needed to be categorized by signal type, because each signal type had to be constructed from distinct radio circuitry. In the present era of software defined radio (SDR), however, the historical approach burdens the understanding of jamming with unnecessary restrictions. Today, the important questions to answer are what information does the jammer possess and what is the jammer's capacity to act on that information.

The intent of this jamming taxonomy is to help researchers place newly discovered jamming or anti-jamming strategies within a larger context of known strategies in a way that is consistent with modern electronic warfare.

Closer to the technological theme of this paper, the Common Attack Pattern Enumeration and Classification (CAPEC) [1] is a catalog and taxonomy of cyber-attack patterns, created to assist in the building of secure software. Each attack pattern provides a challenge that the attacker must overcome, common methods used to overcome that challenge, and recommended methods for mitigating the attack. The taxonomy is organized at the top-level by mechanisms of attack (e.g., abuse of functionality, exploitation of authentication, malicious code execution) and domains of attack (e.g., hardware, software, social engineering). While the jamming taxonomy proposed in this paper is fundamentally different in structure, CAPEC represents a cyber security equivalent.

There are general similarities in the strategies of EW and cyber-attack. An early jamming technique included *barrage* jamming (explained in Section IV) that, qualitatively, resembles the approaches of early Internet DoS flooding attacks. More recently, however, both EW and cyber-attack often begin with a reconnaissance phase in order to better understand the technical characteristics of the target and craft a tailored attack.

The EW literature, reflecting its military heritage, referred to this preliminary stage as *signals intelligence* (SIGINT). As holds true for cyber-attacks, jamming can serve a larger purpose than just denying communications. For example, it could deny wireless users access to a network with strong authentication and privacy mechanisms, but permit association with another network having inadequate security measures, thereby setting the stage for breaches of confidentiality, integrity, and identity. The full discussion of all of these parallels between EW and cyber-attack, however, is beyond this paper's scope of introducing a new jamming taxonomy.

As this taxonomy only covers jamming, we distinguish between a jammer and cyber-attack based on the intended mode of failure, and the type of attack vector used by the adversary. Traditionally, jamming is performed using an RF vector while a cyber-attack is launched through a network vector. The blurry area occurs when dealing with correlated jamming, described in Section III-A, where the jammer both receives and transmits a signal. We will assume that a jamming signal is *not* a valid frame or packet, because such attacks are rarely classified as jamming. However, we make no limitations to the receiving capabilities of the jammer. For example, the jammer could process the received waveform at the media access control (MAC) and network (NET) layers, in order to target a certain type of frame or packet. However, to remain within the common definition of jamming, the transmitter portion of the jammer must either inject noise into the communications link, or transmit what looks like a real PHY-layer signal (as discussed in Section III-D). Otherwise the attack should be classified under the cyber security domain. This classification is not meant to limit the capability of jammers, but rather to put a label on a given attack and better define the scope of this taxonomy.

It is important to note that this paper does not discuss malicious node detection, anti-jamming strategies, jammer detection, or jammer localization. Likewise, it does not cover radar jamming or radio navigation (a.k.a. positioning navigation and timing) jamming or spoofing such as attacks on GPS. The goal of the paper is to shed light on the broad characteristics that the jammer may possess and also provide the right references for someone interested in pursuing research related to jamming.

This paper is organized as follows. Section II highlights related works. In Section III we identify key capabilities that distinguish major classes of jamming, which forms the core basis for the jammer taxonomy and also provides a parametric framework that covers the second tier jammer characteristics. Section IV samples several jamming attacks found in open literature, and finally conclusions are provided in Section V.

II. Related Works

The comprehensive references of Adamy [2] and Poisel [3] for the most part reflect the historical tradition of distinguishing jamming by signal type (e.g., noise, tone, pulse). Poisel's work has more of a communications focus than Adamy's and includes *smart jamming* techniques that, in this paper, we term *protocol-aware* jamming. In contrast to [2, 3], this paper emphasizes behaviors and attributes a jammer could have and then discusses specific jamming techniques characterizing a given behavior. Consequently, in this paper's view, a jammer having one tone versus multiple tones is just expressing an adjustable parameter within the same overall jamming behavior.

Another categorization of jammers is provided in [4], where the authors use the categories of: constant jammer, deceptive jammer, random jammer, and reactive jammer. The authors describe a constant jammer as one that sends out random bits without following any media access control (MAC)-layer protocols. Their deceptive jammer (termed as *spoofing* in this paper) is one that transmits regular packets into the channel, following the PHY and MAC layer protocol used by the target. They define random jamming as the jammer turning on and off with a random or fixed period. Lastly, reactive jamming (termed as correlated jamming in this paper) is a jammer that senses the target channel and only transmits when there is activity. While these categories are well-suited for the analysis performed by the authors, they omit distinctions for whether or not the jammer is adapting its signal based on information it has *a priori* or has acquired. A similar concern applies to jamming literature surveys such as [5].

As noted above, most of the previous work only studied specific aspects of the jamming problem and did not provide a complete overview of the potential jamming attacks that can be performed depending on the information available to the jammer. In this regard, our taxonomy is not only more comprehensive than those in the above references, but unique in the sense that it is based on the information the jammer possesses and the jammer's capacity to act on that information.

III. Key Jammer Capabilities

The primary delineation of the taxonomy is by jammer capabilities that define the fundamental behavior of the jammer. A secondary refinement of the taxonomy by parameters is explained in the next section. A jammer can have one or more of the following major capabilities:

1) Time Correlated
2) Protocol-Aware
3) Ability to Learn
4) Signal Spoofing

Figure 1 shows how the jammer capabilities are interrelated.

These four capabilities were chosen based on a survey of jammer models that exist in literature, with an emphasis on complex forms of jamming. For example, a learning jammer (a.k.a. cognitive jammer) may not represent the majority of what is found in current-day operations, but it is a topic of interest in recent research and will likely become more prevalent over the next decade. We discuss correlation in the time domain specifically, because it is implicit that a jammer's signal needs to have some correlation in the frequency domain with the victim's desired signal to be successful (i.e., at least be aware of the spectrum being used by the victim and thereby perform jamming attacks over this spectrum). Thus, for the remainder of this paper we will refer to correlated as time correlation. The remainder of this section provides more details about each capability.

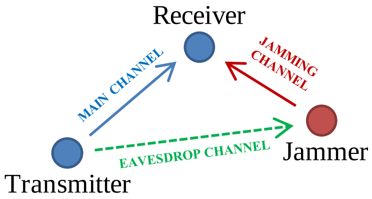

Fig. 2. Geometrical configuration of a correlated jamming scenario, showing the three channels involved.

A. Time Correlated

A time correlated jammer (a.k.a. reactive jammer in some literature) is one that transmits a jamming signal that is correlated to the target signal in time, in some fashion. A correlated jammer implies the jammer can listen to the transmitter's signal, leading to the geometrical configuration shown in Figure 2. The implementation of this capability may be by alternately receiving then transmitting or, for simultaneous receive and transmit operation, the jammer may cancel its own signal or use separate directional antennas.

This class of jammer could take on a wide range of specific models. For example, it may sense a block of subchannels and jam those that contain energy significantly above the noise floor, or the jammer may retransmit a manipulated replica of what it receives for its attack as in the case of a Digital RF Memory (DRFM) or repeater jammer. While correlated jamming is a very broad category of jamming, it acts as a good characteristic to quickly identify the complexity of the jammer, as a correlated jammer must have some form of a receiver. Because there is significant engineering that goes along with receiving capability (e.g., a full RF chain, sampling, processing), any correlated jamming attack corresponds to a more complex attack. For the remainder of this paper we will refer to a jammer that isn't time correlated as "non-correlated".

One may ask how jamming is possible without a receiver; how does a jammer know which signals to jam? When we discuss a jamming attack, we are referring to the specific attack being launched against a signal. Before any attack is launched, the following steps must occur (see below). The time correlation capability comes into play during the actual attack, not the signal awareness step. Obtaining signal awareness surely requires receiving capability, but a time correlated attack consists of the jammer being tightly synchronized to the target signal.

1) **Signal Awareness:** sensing and detecting signals across the spectrum of interest
2) **Threat Assessment:** for each signal, a decision must be made as to whether or not it will be jammed
3) **Attack Selection:** for each signal to be jammed, the best attack must be selected

B. Protocol-Aware

The term protocol-aware simply means the jammer is aware of the protocol of the target signal. Information about the signal's protocol is obtained during the **Signal Awareness** step and used in the **Attack Selection** decision-making. For example, the jammer may identify that a particular signal is a Wi-Fi or LTE signal, which due to the open nature of specifications allows the jammer to know almost everything about the PHY and MAC layers. A jammer could use *a priori* knowledge of the protocol to exploit weaknesses in the protocol, and launch a jamming attack that is more effective and may be harder to detect than non-protocol-aware jamming. We note that a signal does not have to belong to a specific technology to be open to a protocol-aware attack. For example, the jammer may only know a signal uses orthogonal frequency-division multiplexing (OFDM) with pilots in certain locations, which would be considered protocol-aware if it knew exactly where the pilots were placed.

As discussed in literature, if a jammer knows the specific protocol being used, it can increase in effectiveness by jamming a PHY or MAC layer mechanism instead of data directly. In most wireless protocols, the data takes up the largest portion of time and frequency resources. Thus, if a jammer targets something besides the data, it will likely result in an attack that uses less power and is harder to detect (as long as the targeted mechanism is essential for communications). Possible mechanisms that could be targeted in a protocol-aware attack (taken from open literature) include:

- Control channels/subchannels
- Control frames or packets (e.g., ACKs)
- Pilots (a.k.a. reference symbols)
- Synchronization signals
- Cyclic prefix in OFDM

For a survey of protocol-aware jamming attacks against Wi-Fi and LTE we refer the reader to [6] and [7], respectively.

C. Ability to Learn

In this paper, we will define the term "learning" in the Machine Learning (ML) sense: "systems that can learn from data, rather than follow only explicitly programmed instructions". A jammer that has the ability to learn is one that may modify its behavior in real-time in response to its experiences (i.e., instances of successful or unsuccessful jamming actions/decisions) [8]. However, a learning system has capabilities beyond an adaptive system that is limited to following a pre-programmed sequence of change in response to stimulus. A simple test to determine if a given jammer has the ability to learn is to see if it evolves its behavior in response to a target's behavior and adaptation. Learning jammers go beyond simply detecting the target's waveform type and choosing from a pre-programmed set of jamming waveforms. Rather, a jammer that learns may detect that the target has initiated an anti-jam strategy, and then the jammer can explore different strategies of its own to circumvent this anti-jam defense. This category corresponds to some of the most complex jammers, for the following two reasons:

1) Learning algorithms (e.g., supervised learning algorithms such as the popular Support Vector Machine (SVM) or artificial neural networks (ANNs)) are complex, with high computational complexity during training.
2) Determining the success of a certain jamming attack may be difficult for the jammer, as it may not have

access to the channel feedback information. This is an area where traffic analysis may be used.

Often the ability to learn leads to the label of “cognitive”. However, a cognitive jammer that is capable of learning should not be confused with “cognitive radio jamming”, i.e., a jammer designed to deny a cognitive radio network (e.g., the primary user emulation attack [9]). In some cognitive radio jamming literature, the term “cognitive jammer” is used, even though the primary user emulation attack rarely involves learning and often is not even correlated.

In some situations a learning jammer may target radios that are also capable of learning, such as cognitive radios in the Mitola sense [10] (as opposed to dynamic spectrum sharing radios). The jammer can exploit this fact using a belief manipulation attack thereby causing the targeted system’s adaptation processes to seek a poor operating point [11]. If you can metaphorically convince a radio that “up is down”, and “down is up”, you can severely impact how it behaves and reacts to particular situations.

In terms of how presence of learning relates to the other key capabilities, a jammer capable of learning is almost surely correlated because learning involves observing the target signal. We consider learning and protocol-aware as independent features, leading to the relationship shown in Figure 1.

D. Spoofing (a.k.a. Protocol Emulation)

Spoofing is broadly defined as a situation in which one entity successfully masquerades as another by falsifying data and/or signals in order to gain an illegitimate advantage. Typically spoofing targets a PHY-layer mechanism by emulating a signal. In terms of jamming, which is assumed to be a physical layer adversary, we will define spoofing as **the action of transmitting a signal that is meant to look like a legitimate signal**. To distinguish physical layer spoofing from, for example, transmitting fake frames or packets, we will confine spoofing to be on the physical layer. In other words, the spoofed signal need not have any properties that make it look like a valid frame or packet. Rather, the spoofed signal must be intended to fool the signal processing level of the target. Spoofing may or may not be correlated, although in literature it is more often *not* correlated.

Protocol-aware jamming may or may not involve spoofing, but if spoofing occurs then the jammer is almost surely protocol-aware, because it needs to know what to spoof. Determining whether a given adversary is spoofing is rather simple. One must check whether it is transmitting noise, or transmitting something that looks legitimate to the target’s PHY layer. The difference between physical layer spoofing and higher layer spoofing is less clear, although if the adversary is transmitting what looks like a valid packet or frame, then the attack is definitely not confined to the PHY layer, and the attack would fall under the category of cyber-attack.

Cognitive radio jamming techniques, such as primary user emulation, may be considered spoofing depending on the specific waveform the jammer transmits. In forms of primary user emulation where the secondary users only utilize an energy detector, the jammer must only transmit noise at a particular frequency for the secondary users to evacuate the band and avoid using the spectrum. Other forms of primary user emulation could involve the jammer transmitting a signal meant to look like the primary user’s signal (e.g., the pilots associated with a radio station), in which case it is PHY layer spoofing.

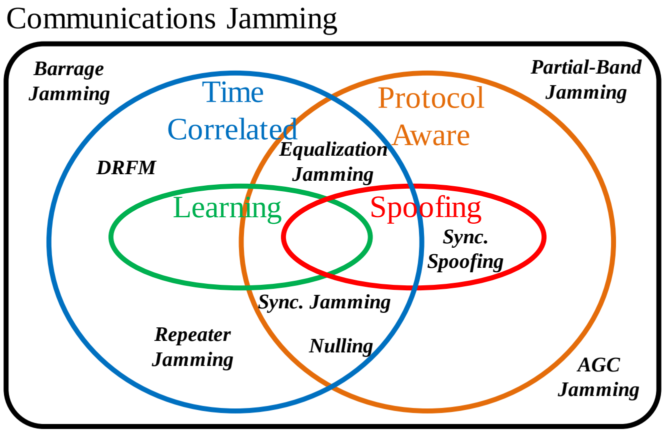

Fig. 4. Specific jamming techniques discussed in literature, mapped according to key jammer capabilities.

E. Jammer Parameters

Building upon the definition of major categories of jammer capabilities, a second tier refinement comes from the choice of physical parameter values. As illustrated in Fig. 3, example parameters include frequency, time overlap with jamming target, antenna directionality, and the jammer’s waveform or modulation. In this way, jammer types that, in early literature, were treated as distinct technologies can be understood now as minor variations on a common algorithm.

IV. A Sampling of Specific Jamming Attacks

In this section we provide several example jamming attacks that can be found in open literature, and discuss how they are classified with respect to the taxonomy we have developed in the previous two sections, as shown in Figure 4.

A. Barrage Jamming

Barrage jamming is the simplest form of jamming and is usually defined as a jammer which transmits noise-like energy across the entire portion of spectrum occupied by the target with 100% duty cycle in time. Thus, it is non-correlated and non-protocol-aware. Barrage jamming has been shown game theoretically and information theoretically to be the best a jammer can do in the absence of any knowledge of the target signal [12].

B. Partial-band Jamming

When jamming a single-carrier signal, it has been shown that jamming gains can be achieved by not jamming the entire signal in the frequency domain, but rather jamming a fraction of the signal. This is known as partial-band jamming, and it

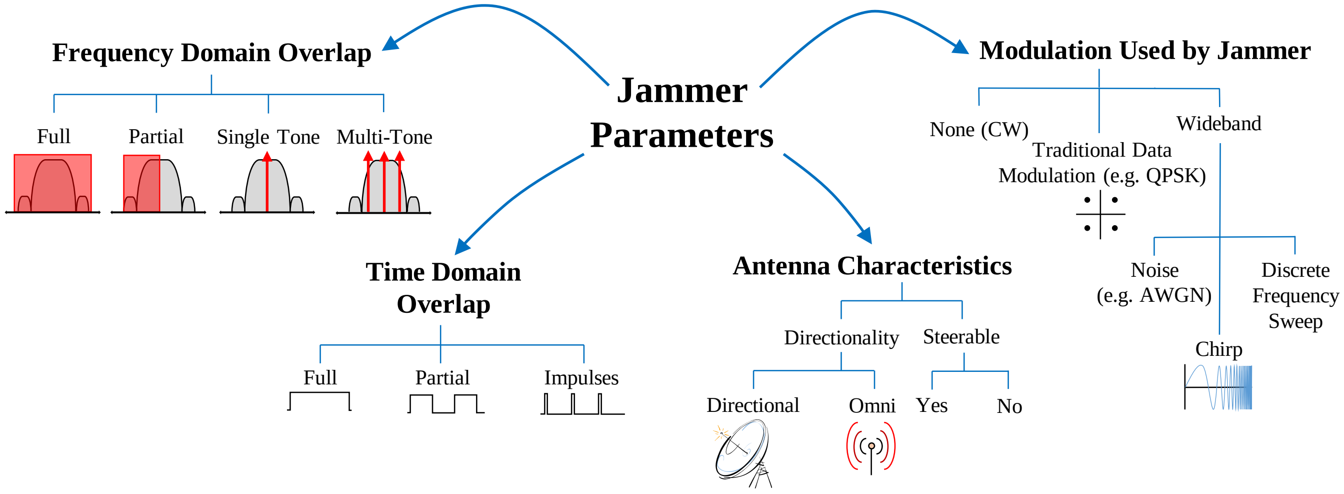

Fig. 3. Jammer parameters organized into trees.

is usually considered a non-correlated jamming attack because the jammer transmits continuously in time. Performing partial-band jamming against an OFDM waveform does not make sense because strong forward error correction could allow the data to be reconstructed from the unjammed subcarriers.

C. Automatic Gain Control Jamming

The automatic gain control (AGC) mechanism in a receiver adjusts the input gain such that the received signal comes in at a proper level to best utilize the range of the analog-to-digital converter(s). A jamming attack that targets the AGC mechanism is one that uses a very low duty cycle (e.g., 2%) but with extremely high instantaneous power. By not transmitting continuously, the jammer can save power and remain harder to detect in some situations [2]. AGC jamming is non-correlated, although the specific period and duty cycle used are important parameters. Aside from the assumption/knowledge that the target receiver uses AGC, it is non-protocol-aware.

D. Equalization Jamming

Equalization jamming involves targeting any mechanism related to equalization. Known data symbols (a.k.a. reference symbols) are inserted into the transmitted waveform to estimate the channel's frequency response and equalize the effect of the channel at the receiver prior to demodulation. These known symbols are called pilot symbols in multicarrier communications such as OFDM or single-carrier frequency-division multiple access (SC-FDMA) and channel sounding symbols in multiple-input and multiple-output (MIMO) systems [13]. For example, in OFDM, pilot tone jamming is simply the process of jamming pilot tones, which may reside on certain subcarriers (in the case of 802.11) or may be multiplexed in time and frequency with data (in the case of LTE). Pilot jamming is protocol-aware because the jammer must know where the pilots are located. If the pilots occur on a dedicated subcarrier then the attack is non-correlated, but if they are multiplexed in time then it must be correlated in order to surgically jam the pilots. It was found that pilot jamming can be energy efficient and similar degradation in target receivers BER can be achieved using roughly one-tenth of the energy [13]. The pilot jamming process is similar in the case of SC-FDMA, which is the single-carrier variant of OFDM and used in the uplink of the LTE air-interface. In MIMO systems, known reference signals are used for channel sounding and thus can be jammed as well as long as they are known by the jammer *a priori*.

Another special kind of equalization jamming attack involves jamming the cyclic prefix (CP) of a multicarrier waveform such as OFDM or SC-FDMA. These waveforms use a CP to mitigate inter-symbol interference (ISI) and inter-channel interference (ICI). CP also ensures that the convolution of the channel impulse response with the modulated symbols has the form of a circular convolution, which is essential for simple one-tap equalization in the receiver. These crucial roles played by the CP make SC-FDMA particularly vulnerable to jamming attacks through CP.

E. Synchronization Jamming

For a communications link to function, the receiver must synchronize to the incoming signal in both time and frequency. To aid in this task, a synchronization signal, or synchronization symbols, are usually designed into the PHY layer protocol. For example, in LTE there are two different synchronization signals that each appear every 5 ms. Synchronization jamming (a.k.a. synchronization signal jamming) is simply the process of surgically jamming one or more synchronization signals. This jamming technique is unique in the sense that it may only prevent radios from establishing a communications link, and thus it won't cause immediate DOS [7]. However, synchronization signals tend to be very sparse with respect to the entire signal, thus providing a significant jamming gain. Synchronization jamming must be protocol-aware, in order to know where the synchronization signal is located. It must be time-correlated, assuming the synchronization signal is multiplexed in time with data and other signaling.

F. Nulling

Instead of transmitting noise as the jamming waveform, a nulling (a.k.a. phase coherent) attack involves transmitting a structured waveform in such a way that the received energy at the target receiver is driven as close to zero as possible [13]. This is done by causing the jamming signal to be received as the π-radian phase shift of the target signal, thus nulling out the target signal and leaving only channel noise for the demodulator. Nulling attacks are extremely challenging and can be considered infeasible in real-world scenarios because they require extremely accurate knowledge of the channels involved, which can be difficult to achieve considering varying nature of wireless channel. Even if the target signal includes pilots and synchronization symbols, that would only provide accurate knowledge of the channel between the jammer and transmitter (to perform nulling, the jammer would also need to know the jammer-receiver and transmitter-receiver channels, as shown in Figure 2). Nulling also requires *a priori* knowledge of the signal, which is possible in some circumstances (e.g., the value of pilot sequences in Wi-Fi and LTE is openly published). Thus, a nulling attack is protocol-aware, but it is probably impractical to implement due to the need for prior knowledge of what are, in reality, random characteristics of a wireless channel.

Even though they are presently believed to be infeasible in practice, nulling attacks are included in this taxonomy due to their presence in academic literature. Pilot nulling against OFDM, which was introduced in [13], involves nulling the pilots at the target receiver. Channel sounding singularity attacks (another name for nulling sometimes used in literature) against MIMO systems has also been investigated.

G. Repeater Jamming

Repeater jamming (a.k.a. DRFM jamming or follower jamming) is the simplest form of correlated jamming when the jammer has no knowledge of the protocol. In repeater jamming, the jammer transmits when it senses energy on the channel. This may be in the form of the jammer retransmitting what it receives with noise added, or sensing a series of subchannels and transmitting noise when it senses energy on one or more subchannels. Regardless of the specific model used, repeater jamming can "follow" a signal if it hops around in frequency, negating the anti-jam gains associated with frequency-hopping spread spectrum (FHSS).

When there are large distances between the transmitter, receiver, and jammer, a repeater jamming attack may fail to achieve time-correlation with the target signal. However, a repeater jamming attack may still be used in order to decrease probability of detection, because the jamming signal will resemble the target's communications. In addition, simply replaying the target signal can aid in achieving frequency correlation, assuming the target is not hopping or changing channels too quickly. We will refer to this form of repeater jamming, which is too slow to overcome the gain associated with FHSS, as a replay attack.

H. Protocol-Aware Jamming Against Wi-Fi

There are several intelligent jamming attacks against Wi-Fi (IEEE 802.11) found in open literature [6], most likely due to the popularity of Wi-Fi and length of time Wi-Fi has been widely used. *Clear to Send (CTS) Jamming* is when a jammer waits for there to be a Request to Send (RTS) packet transmitted over the channel, and then transmits a burst of noise after waiting for the Short Interframe Space (SIFS) interval which is defined in the specifications [5]. *Acknowledgment (ACK) Jamming* works the same way, except the jammer waits for a data packet to be transmitted, then after waiting for a SIFS interval it transmits a burst of energy with the intent to jam the ACK [5].

While these previous two attacks are both protocol-aware and correlated, it is possible to have a protocol-aware and non-correlated attack in 802.11, using an attack known as *DIFS Wait Jamming* [6]. This works by transmitting periodic pulses that repeat with a frequency based on the 802.11 DCF Interframe Space (DIFS) duration. This duration determines how long a node senses the channel in order to decide whether or not the channel is idle. Thus, this attack causes a "busy channel" while saving power in a non-correlated manner. A protocol-aware jamming strategy that incorporates learning is proposed in [14].

I. Protocol-Aware Jamming Against LTE

In LTE, data is multiplexed with control information in both time and frequency, due to the use of OFDM. Especially in the downlink, symbols often contain data combined with control information, and control information can be surgically jammed by targeting the specific subcarriers (i.e. frequencies) they occupy. Several protocol-aware jamming against LTE have been investigated in recent literature [7], and were found to be significantly more effective than barrage jamming. To cite one example, there is a downlink control channel called the Physical Control Format Indicator Channel (PCFICH) which only holds two bits of information, but is transmitted every subframe and is vital to the downlink control channel operation [15]. Because the PCFICH is so sparse in time and frequency, jamming it leads to an attack that is about 20 dB more effective in terms of overall jammer-to-signal ratio (J/S) compared to barrage jamming [7]. The PCFICH attack is correlated because the PCFICH is multiplexed in time with other physical channels.

One non-correlated jamming attack against LTE is jamming the Physical Uplink Control Channel (PUCCH), which is always at the edges of the uplink bandwidth, meaning a jammer can use the open specifications to predict where the PUCCH will be in frequency. This is a non-correlated attack because there are no other physical channels multiplexed in time with the PUCCH. For more information on jamming attacks against LTE we refer the reader to [7].

V. Conclusion

As the sophistication of communications systems increases, sophisticated jamming will likely become a bigger threat in public safety, military, and other mission-critical domains. The jammer taxonomy introduced here frames the organization of jammer classes by what information they possess and their capacity to act on that information. This new view of jammers emerges naturally from the way present day wireless technology relies so extensively on software-driven behavior. In addition, understanding the key capabilities that distinguish major classes of jamming, as well as the multidimensional parameter space, can aid in the correct application of anti-jam and detection strategies.

Further research includes the design of a radar jamming taxonomy and radio navigation jamming taxonomy. It may be possible to formulate a taxonomy that applies to all forms of jamming.

References

[1] "Common Attack Pattern Enumeration and Classification (CAPEC)," MITRE. [Online]. Available: https://capec.mitre.org

[2] D. L. Adamy, *EW 101*. Artech House, 2001.

[3] R. Poisel, *Modern Communications Jamming: Principles and Techniques*. Artech House, 2011.

[4] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, 2005.

[5] 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, 2011.

[6] D. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11 b and other networks," in *IEEE MILCOM*, vol. 6, 2006.

[7] M. Lichtman, J. Reed, T. Clancy, and M. Norton, "Vulnerability of LTE to hostile interference," in *IEEE GlobalSIP*, Dec 2013.

[8] S. Amuru and R. M. Buehrer, "Optimal Jamming Strategies in Digital Communications–Impact of Modulation," in *IEEE Global Communications Conference*, Dec. 2014.

[9] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[10] J. Mitola and G. Q. Maguire Jr, "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[11] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, 2008.

[12] T. Basar, "The gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, 1983.

[13] T. C. Clancy, "Efficient OFDM denial: Pilot jamming and pilot nulling," in *IEEE International Conference on Communications (ICC)*, 2011.

[14] S. Amuru and R. M. Buehrer, "Optimal Jamming using Delayed Learning," in *IEEE MILCOM*, Oct. 2014.

[15] S. Sesia, I. Toufik, and M. Baker, *LTE: the UMTS long term evolution*. Wiley Online Library, 2009.