Denial of Service Attacks in Wireless Networks: The Case of Jammers

Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy

***Abstract*—The shared nature of the medium in wireless networks makes it easy for an adversary to launch a Wireless Denial of Service (WDoS) attack. Recent studies, demonstrate that such attacks can be very easily accomplished using off-the-shelf equipment. To give a simple example, a malicious node can continually transmit a radio signal in order to block any legitimate access to the medium and/or interfere with reception. This act is called jamming and the malicious nodes are referred to as jammers. Jamming techniques vary from simple ones based on the continual transmission of interference signals, to more sophisticated attacks that aim at exploiting vulnerabilities of the particular protocol used. In this survey, we present a detailed up-to-date discussion on the jamming attacks recorded in the literature. We also describe various techniques proposed for detecting the presence of jammers. Finally, we survey numerous mechanisms which attempt to protect the network from jamming attacks. We conclude with a summary and by suggesting future directions.**

***Index Terms*—Wireless DoS, jamming, wireless security, anti-jamming.**

I. Introduction

SECURITY is one of the critical attributes of any communication network. Various attacks have been reported over the last many years. Most of them, however, target wired networks. Wireless networks have only recently been gaining widespread deployment. At the present time, with the advances in technology, wireless networks are becoming more affordable and easier to build. Many metropolitan areas deploy public WMANs for people to use freely. Moreover, the prevalence of WLANs as the basic edge access solution to the Internet is rapidly becoming the reality. However, wireless networks are accompanied with an important security flaw; *they are much easier to attack than any wired network.*

The shared and easy to access medium is undoubtedly the biggest advantage of wireless networks, while at the same time is its *Achilles' heel*. In particular, it makes it extremely easy for an adversary to launch an attack. The goal of traditional DoS attacks is to overflow user and kernel domain buffers [1]. However, in wireless networks there are many occasions where the attack can be much easier for an adversary. For example, in carrier sensing based networks (e.g. 802.11, sensor networks, etc.), a saboteur might continually transmit electromagnetic energy on the medium, achieving the following two results: **(a)** the transmissions at the sender are deferred because the medium is sensed to be busy, and/or **(b)** the reception at the receiver is interfered with due to the jamming signals. Both these effects degrade the wireless network performance significantly. As another example, in the context of mobile phone devices, one can use a compromised mobile device to broadcast huge volumes of SMS messages in its vicinity in order to flood all nearby devices [2]. With such malicious techniques, it is feasible to block any communication between two wireless capable nodes.

However, such "brute-force" jamming techniques, which mainly exploit PHY and MAC layer vulnerabilities, can be detected easily. Jammers have responded by employing more intelligent ways to accomplish jamming task in order to evade detection. They exploit vulnerabilities at the higher layers of the network stack. A typical example is detecting the transmission of specific control packets and preferentially corrupting such packets by injecting interference. In order to address these threats, security experts must deploy more efficient methods for detecting and preventing such "smart" (stealthy) attackers. A fascinating arms-race, thus, begins between adversaries and network administrators.

Nowadays many commercial jamming devices are readily available for attacking all kinds of wireless networks (e.g. 802.11, 3G, GSM, radar communications, etc) [3] [4] [5] [6]. This, in conjunction with the large number of jamming attack strategies reported in the literature [2] [7] [8] [9], makes jamming a big threat for wireless networks.

In this survey paper, we describe some of the most harmful attacks that can be launched by a jammer. Having established various jamming threats, we report the most important research on detecting and preventing such scenarios. Our survey is organized as follows. In Section II, we provide definitions useful for understanding the concept of jamming, as well as metrics used for quantifying the effectiveness of a jammer. In Section III, we expand on known jamming techniques and attack models. In particular, we study attacks confined to the PHY and MAC layers. Section IV deals with intelligent jamming techniques targeting the MAC and higher layers. In Sections V and VI, we study ways of detecting and defending against the various jamming attacks. We highlight future directions and further reading for the interested reader in Section VII. Section VIII summarizes the topics presented in the paper.

II. Definitions and Metrics

First, we start by formally defining jammers. We will adopt the definition given by Xu *et al* [10]: *"We define a jammer to be an entity who is purposefully trying to interfere with the*

Manuscript received 3 March 2009; revised 1 September 2009 and 19 January 2010.

The authors are with the University of California, Riverside (e-mail: {kpele, marios, krish}@cs.ucr.edu).

Digital Object Identifier 10.1109/SURV.2011.041110.00022

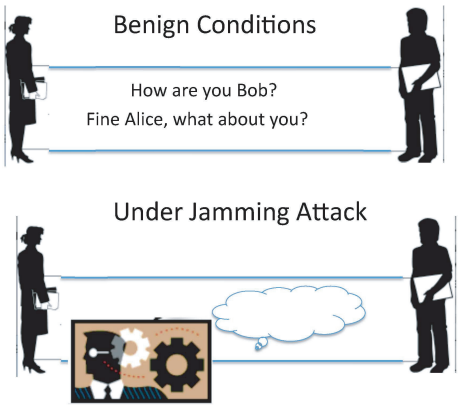

Fig. 1. Pictorial representation of a jamming entity.

physical transmission and reception of wireless communications". A pictorial representation of the jammer is given in Figure 1.

Before describing the various jamming models, it is important to refer to some criteria and metrics that are used to characterize the attack model.

A. Jamming Efficiency Criteria

Acharya *et al* [11] enumerate the following list of widely used jamming efficiency criteria:

- *Energy efficiency*
- *Probability of detection*
- *Level of DoS*
- *Strength against physical layer techniques such as FHSS, DSSS, CDMA.*

An ideal jamming attack should have **high energy efficiency** (i.e., consume low power), **low probability of detection** (preferably close to 0), achieve **high levels of DoS** (i.e., disrupt communications to the desired (or maximum possible) extent) and be **resistant to PHY layer anti-jamming techniques** (i.e., do not allow signal processing techniques to overcome the attack). Often, the criteria of interest are jamming scenario dependent. In other words, the jamming scenario dictates the most suitable criteria for use. For example, when malicious nodes have limited energy resources, energy efficiency will be their prime goal. Of course, in all cases jammers may attempt to be effective in as many of the aforementioned criteria as possible. As a simple example, in order to maintain a low probability of detection, the jammer can adopt techniques that are consistent with MAC layer behaviors. More details on jamming techniques will be provided in the following sections.

B. Jamming Efficiency Metrics

In order to quantify the extent to which the jammer satisfies the above criteria, we need to define metrics that capture the jammer's behavior. For describing these metrics, we will use simple scenarios with one transmitter (T_x) and one receiver (R_x).

Xu *et al* [10] introduce the following two, widely used, metrics (PSR and PDR).

Packet Send Ratio (PSR): Lets assume that the MAC layer of T_x has n packets for transmission. Due to jamming interference, only m ($n \geq m$) of these packets can eventually be transmitted. PSR is then defined to be:

$$PSR = \frac{m}{n} = \frac{Packets\ Sent}{Packets\ Intended\ To\ Be\ Sent} \tag{1}$$

PSR is an easily computed measure which intuitively captures the effectiveness of the jammer towards a transmitter employing carrier sensing as its medium access policy. The jamming signals can render the medium busy due to carrier sensing and as a result the transmission queues of T_x will get filled up quickly. Packets arriving at a full queue will be dropped. Moreover, depending on the semantics of the MAC protocol employed, transmissions for packets at the head of the queue can eventually *expire* and the packets themselves get discarded. The PSR metric can quantify such jamming effects.

Packet Delivery Ratio (PDR): Lets suppose that R_x receives m packets sent out from T_x. However, from these m packets only q were successfully delivered to the higher layers of R_x. A successful reception means that the packet successfully passed the CRC (Cyclic Redundancy Codes) check. In contrast to PSR, PDR captures the effectiveness of the jamming attack towards R_x. The PDR is defined as follows (note that if $m = 0$ then PDR is defined to be zero):

$$PDR = \frac{q}{m} = \frac{Packets\ That\ Pass\ The\ CRC}{Packets\ Received} \tag{2}$$

In addition to the simple metrics described above, there are other sophisticated measures used in order to quantify the jammer's effectiveness.

Jamming-to-Signal Ratio: Traditionally, jamming strength (mostly referring to PHY layer jamming) is measured by the jamming-to-signal ratio given by the following equation [12], [13]:

$$\frac{J}{R} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j} \tag{3}$$

where with the subscript j we refer to the jammer, with r to the receiver and with t to the transmitter. P_x is the transmission power of node x, G_{xy} is the antenna gain from node x to y, R_{xy} is the distance between nodes x and y, L_r is the communication link's signal loss, L_j is the jamming signal loss and B_x is node's x bandwidth.

Obviously, a high jamming-to-signal ratio implies a successful jamming attack. From the mitigation perspective, an attack countermeasure would try to reduce this ratio. Equation 3 points to several directions towards this goal. For example, by reducing the distance between the legitimate transceiver pair, one can reduce the jamming-to-signal ratio and make the link more robust to jamming attacks. Section VI provides a more detailed discussion on these issues.

Connectivity index: The presence of jammers in an ad hoc wireless network can hurt connectivity (i.e., disrupt the existence of routes between all wireless nodes in the network). To capture the effect of jamming on the connectivity of a wireless ad hoc network, Noubir *et al*. [12] introduce the connectivity index.

We start by defining a non-jammed link [12]. Let R be the communication range of the nodes, JS be the set of jammers, and JR be the jammer's range. A link from node A to node B is said to be non-jammed if and only if:

$$d(A,B) < R \wedge \forall J \in JS : d(J,B) > JR \tag{4}$$

where $d(A,B)$ denotes the Euclidean distance between the locations of node A and node B[1]. Having defined the non-jammed links we can now define the connectivity index as follows.

Let $G = (V,E)$ be the directed connectivity graph representing the multi-hop ad hoc network after removing the jammed links. Let $G' = (V,E')$ be the transitive closure of G. The connectivity index of G is defined to be:

$$Connectivity\ Index = \frac{|E'|}{\frac{|V|(|V|-1)}{2}} \tag{5}$$

From the definition of the transitive closure, E' contains all the pair of nodes of the graph for which, there exists a path that connects them. The connectivity index is simply the ratio of the number of such pairs to the number of all possible pairs of nodes in the network. As a result, a connected graph has a connectivity index of 1, while a graph partitioned in two connected graphs of equal size, has a connectivity index 0.5.

Other metrics that are traditionally used to capture the performance of a wireless network can also be used to measure the efficiency of a jammer. For example, the *long term throughput* of a link (which suffers from the presence of a jammer) can be used as such a metric; the lower the throughput the higher the jamming efficiency. In the following section we proceed by describing jamming techniques reported in the literature.

III. PHY AND MAC LAYER JAMMING MODELS

In this section, we present four *basic* jamming models [10] [14] [15] [16]; a jamming model captures the strategy followed by the malicious attacker. The key attributes of these models lies in their simplicity and effectiveness.

A **constant jammer** [10] continually emits radio signals on the wireless medium. The signals can consist of a completely random sequence of bits; electromagnetic energy transmissions do not have to follow the rules of any MAC protocol. The goal of this type of jammer is twofold: (a) to pose interference on any transmitting node in order to corrupt its packets at the receiver (lower PDR) and (b) to make a legitimate transmitter (employing carrier sensing) sense the channel busy, thereby preventing it from gaining access to the channel (lower PSR).

Similar to the constant jammer is the **deceptive jammer** [10]. Their similarity is due to the fact that both constantly transmit bits. The main difference is that with the deceptive jammer, the transmitted bits are not random. The deceptive jammer continually injects regular packets on the channel without any gaps between the transmissions. This makes an overhearing user believe that there is a legitimate transmission going on. Consequently, every node will remain in the listening state even if it has data to transmit. An important difference from the constant jammer is that deceptive jamming is harder to be detect using network monitoring tools, since these tools will sense legitimate traffic on the medium.

One disadvantage of both of the aforementioned jamming strategies is their power efficiency. Emitting signals continually on the wireless medium limits their ability to be autonomous and to not depend on an external power source. A more power efficient jamming strategy, is the use of **random jammer** [10]. An attacker employing random jamming, jams for t_j seconds and then sleeps for t_s seconds. During the jamming intervals, the jammer can follow any of the approaches that we have described so far, or any of the tactics that we will describe in the following sections. By changing t_j and t_s, we can achieve different levels of aggressiveness and power savings; t_j and t_s can be different in different jamming cycles. For instance, t_j and t_s can be samples of two random variables T_j and T_s, respectively, following (different) uniform distributions.

Constant and deceptive jamming try to both interfere with the reception of a packet as well as try to hinder transmission (if CSMA is used). However, this reduces the power efficiency of the jammer. A smarter and more power efficient approach would be to only target the reception of a packet. This jamming model is called the **reactive jammer** [10]. This jammer is constantly sensing the channel and upon sensing a packet transmission immediately transmits a radio signal in order to cause a collision at the receiver[2].

Note that current standards for wireless data communications work in favor of the jammer [17]! For example, the PHY layer of IEEE 802.11 does not support error correction. As a result, the jammer can send just enough power to corrupt a single bit to cause a received packet to fail the CRC check. The reason for this protocol specification is that wireless systems have been designed only to be resilient to non-malicious interference and to noise. A jammer can exploit this and efficiently use low power in order to disrupt the entire communication.

IV. INTELLIGENT JAMMING MODELS

The jamming strategies presented in the previous section, can be thought as naive (or very basic) jamming attacks. These jamming models try to break down the communication between two nodes. While they can achieve a high degree of denial of service, they exhibit (in general) low energy efficiency and high probability of detection. However, orthogonal to physical layer jamming, several WDoS attacks can be launched by exploiting higher protocol layers' semantics. For example with IEEE 802.11, a saboteur can manipulate the back-off functionality to gain continuous access to the medium. This, in turn, would force the rest of the nodes to defer their transmissions resulting in a significant throughput drop. As another example with the MAC layer protocol used with Bluetooth technology, an adversary can selectively destroy specific control packets disrupting ongoing communications. At the routing layer, in a wireless ad hoc network, one

[1]In a CSMA/CA network one should extend the definition and include the constraint: $d(J,A) > JR$.

[2]The underlying assumption here is that the sensing functionality is less costly in terms of energy compared to the transmission functionality.

can inject erroneous messages or destroy legitimate routing control packets. Similarly, at the transport layer a jammer can force TCP to invoke multiplicative decreases in order to keep the congestion window small. In the rest of this section we present in more detail, several "intelligent" jamming models reported in the literature.

A. Goals of Intelligent Jamming

Intelligent jamming tries to exploit upper layer protocol vulnerabilities in order to achieve three main goals [18]:

- maximized jamming gain
- targeted jamming, and
- reduced probability of detection.

Next we describe each of these goals in more detail.

Jamming Gain: We define the jamming gain of a jammer to be the *"inverse ratio of the amount of power used to achieve a desired effect with the jammer under consideration to the amount of power that is used to achieve the same effect with the constant jammer"* [18]. Later in this survey, we will describe jamming models with jamming gains as high as 40db.

Targeted Jamming: Naive jammers (as an example constant jammers) emit a radio signal on the wireless medium and break down the communications without paying any attention to which nodes are being jammed. Further jamming gains can be accomplished if the attacker jams specific victims (e.g. a relay node for many flows in an ad-hoc network).

Reduced Probability of Detection: As we will discuss in Section V, strategies like constant jamming are easy to detect. By adding intelligence to the jamming strategy, one can force the victim network to believe that the degradation in network performance is due to congestion or poor link conditions and not due to the presence of a jammer. This can lead to a reduced probability of detection.

We must emphasize that jamming is not a transmit-only activity and most of the time could be spent sensing the wireless channel as well. Given the fact that sensing also requires energy, energy preservation is in general a very desirable property for jammers.

B. A Layered Model for Jamming

Encryption is commonly used in order to prevent unauthorized access to transmitted data. This can obfuscate control packets from malicious nodes. Brown *et al* [18] present a layered jamming strategy that can work very well towards disrupting encrypted wireless networks[3]. Brown *et al* propose a three layered approach to jamming. We briefly describe this approach here. We refer the reader to the original paper for more details [18].

The approach spans the three layers of the protocol stack with each layer offering services to its immediate upper layer; namely the application, transport and link/physical layer. Each of the layers has two different modules: the sensing module and the jamming module. We begin from the lowest, i.e. link/physical layer, which interacts directly with the wireless medium. The sensing module senses the channel and for every packet measures the packet transmission duration and its starting time. The jamming module performs the actual jamming.

The Transport/Network layer gets information from the Link/ Physical layer and offers services to the Application layer. In more detail, its sensing module reads the measurements from the lower layer and employs a statistical algorithm to classify each packet. Based on the classification results, the jamming module stimulates the link/physical layer to attack a specific node in order to achieve the greatest possible jamming gain with minimum detection probability.

Finally, the Application layer, operates at a higher level. The sensing module senses entire sessions (e.g. HTTP session) and targets processes running at specific nodes in the network. The jamming module uses the session information and defines when jamming should take place in order to maximize the degradation in the performance given the targeted protocol (e.g., HTTP).

One practical consideration is the ability of the system to work online or offline. The ideal mode of operation would be to be online; however, since some packets need to be considered along with future packets in order to be interpreted correctly, offline classification is more realistic. This limitation lowers the maximum achievable jamming gain. The offline classification can be easily achieved in multi-hop wireless ad hoc networks as explained in [18].

The classification of the packets can be achieved by using a probabilistic model of the packet size and a historical analyzer. The entire procedure involves the computation of basic statistics and can be accomplished in a fairly easy way, as described in [18]. This jamming strategy can achieve significant jamming gains compared to a naive constant jammer. In particular, as shown in [18], gains in the order of 400 are viable.

C. Intelligent Jamming in IEEE 802.11

The models presented thus far have not explicitly taken into account any protocol specific parameters. In the remainder of this section, we present jamming techniques that involve jamming of 802.11 control packets in order to corrupt communications with the minimum possible energy consumption. These techniques require a good knowledge and understanding of the IEEE 802.11 standard. Readers that are not familiar with the protocol specifics can find an overview in [19].

1) CTS Corruption Jamming: The malicious node senses the channel and waits for an RTS packet. After the transmission of an RTS, it waits for a SIFS time interval and sends a short jamming pulse which will result in corrupting the CTS packet. This strategy will result in zero throughput, since no data will be successfully transmitted.

2) ACK Corruption Jamming: Using a similar approach (as in CTS corruption jamming), the adversary senses the medium for the DATA packet. Upon sensing a DATA packet, it waits for a SIFS time interval at the end of the transmission and then jams the channel. This will result in the corruption of the MAC layer ACK. The ACK is not received from the sender and there will be several retransmissions, until the sender gives up and drops the packet from its MAC layer queue. It is easy to see that this technique will result in zero throughput as well.

[3]A naive jamming model - e.g. constant jammer - can simply jam the medium and destroy packets on the air irrespective of whether they are encrypted or not. However in order to achieve the goals of intelligent jamming an adversary should be able to identify and jam specific (control) packets.

3) DATA Corruption Jamming: Similar to the previous jamming approaches the jammer waits for the CTS packet and then counts down a time equal to DIFS before jamming the DATA packet.

4) Narrow-band Jamming: Gummadi *et al* [20] found that 802.11 devices are vulnerable to specific patterns of narrow-band interference, relating to time recovery, dynamic range selection and PLCP-header processing. They show that due to these limitations, an intelligent jammer with a 1000 times weaker signal (than that of the legitimate transceiver) can still corrupt the reception of packets.

5) DIFS Waiting Jamming: Jammers belonging to this class wait until they sense the channel idle for a DIFS time period. After this period the saboteur jams the channel. This corrupts the communication that follows the DIFS idle time. The jammer will corrupt either the DATA packet, or the RTS packet if the RTS/CTS exchange is employed.

By comparing the previous five intelligent jamming strategies, we can see that strategies 1 and 3 work only when RTS/CTS is used. In addition, "DIFS waiting jamming" can be energy inefficient as compared to the other strategies, since after the idle DIFS time there might not be any communication. This jamming strategy works well on networks that carry high traffic loads. In [21] the authors compare the total energy that various jamming approaches consume for achieving the (same) result. Their findings demonstrate that intelligent jamming models can be a lot more energy efficient compared to simplistic continuous jamming.

6) Identity Attacks: Bellardo *et al* [22], present the so called identity attacks. There are various types of DoS attacks that belong to this category. First, we present the **de-authentication attack**, where the attacker spoofs the deauthentication message; this is a special message with which a mobile user or an AP (Access Point) explicitly requests a deauthentication. Spoofing this packet will cause the AP or the mobile client to exit the authentication phase and refuse any further packets until re-authentication. Similar to this attack is the **disassociation attack**. In this case, the malicious entity spoofs association messages. This attack is less effective than the de-authentication attack strategy, since the latter forces the victim to do more work to return to an authentication state. Another possible identity attack is the **power saving attack**. In this case the attacker spoofs the pooling messages or the TIM messages, which are related to the power conservation functionality of a mobile node using IEEE 802.11. This will result in the discarding of data. More details on these types of attacks are found in [22].

7) Greedy Behavior: The authors in [23] [24] [25] and [26] describe examples of greedy behavior of a selfish user that wants to gain more throughput than the other users of the network[4]. The greedy node can scramble the CTS, ACK or DATA frames - just like with the previous jamming models. The congestion windows of the legitimate nodes will increase and as a consequence they will defer their transmissions, thereby achieving a much lower throughput than their fair share. The greedy node can also increase the duration value in the frame header of RTS or DATA. As a consequence, its neighbors will have a long busy period indicated in their NAVs; for the period shown to be busy by the NAV they will not contend for the medium. As a result the cheating node can send multiple data packets (if the NAV is set to a large enough value) with one medium access instance. In the case of an adversarial node, there will not be any data exchange during the NAV period; however the legitimate nodes will not be able to contend for the channel. Another greedy strategy is related to the backoff functionality of 802.11. In particular, the greedy user can reduce its backoff time (or consistently use the minimum value for the backoff congestion window) and/or use another distribution for the congestion window. This translates to more frequent access to the channel than the other, legitimate nodes. As a final example, a node can increase its CCA threshold and ignore signals from other nodes. After an initial period with collisions, the legitimate users will enter the back off states with larger congestion window values, while the greedy user will gain more frequent access to the channel. The greedy user will be able to count down its back off window faster, even when other nodes get temporary access to the channel. This is because it will not sense such transmissions due to the increased CCA value. Such greedy behaviors can be called ***active jamming***, since they resemble jamming attacks. However, the attackers' goal is to gain more throughput than their fair share, which is in stark contrast with (passive) jamming attacks where goal is to disrupt ongoing communications. More details on these types of attacks can be found in the references provided.

8) Wireless Ad Hoc DoS: There is a class of WDoS attacks that are specific to 802.11 networks operating in the *ad hoc* mode. These malicious behaviors target layers above the MAC and in particular the routing layer. They take advantage of the fact that these type of networks operate without any infrastructure [27]. In order for two nodes in this network to communicate, a route should first be discovered. An adversary can flood the network by sending a large number of route requests, causing high levels of congestion which in turns disrupts routing. However, note that the large number of requests could be a consequence of normal network operations. For example when the network exhibits high mobility and/or there is a large number of poor quality links, the *route discovery* phase can be legitimately triggered very often, making the detection of such attacks challenging. In addition, the saboteur can spoof the source IP addresses of the route request packets and flood a victim node with requests. These requests seemingly originate at different users, and cause a DDoS at that node. This class of attacks does not fall into the same category as jamming attacks. However, given their importance, we will briefly survey techniques for detecting and preventing such attacks in the following sections.

V. Intrusion Detection Schemes

Traditional techniques directly borrowed from Intrusion Detection Systems (IDS) for wire line networks, face practical limitations when considered for wireless networks. For example, signature based IDSs will not be efficient, since many WDoS attacks take place at the MAC layer. Thus, it is difficult to isolate sequences of packets and feed them as an input is

[4]However, these techniques can be also used from an adversary that wants to interrupt the normal operation of the wireless network.

such systems. In addition, the power constraints of a mobile user are such that make it relatively difficult to build such an IDS, which is required to store a great number of attack signatures. The rest of this section presents studies related to intrusion detection in wireless networks.

A. PHY layer Intrusion Detection

The PHY layer jamming is the most easy to implement jamming technique. The basic idea for detecting such attacks is very simple: *the presence of jamming radio signals at the receiver can effect the received signal strength*. Along these lines, the authors in [10] and [14] propose a series of basic detection methods.

1) Signal Strength Measurements Xu *et al*. [10] [14] show that simple statistical metrics, such as the average received signal power, are not useful in discriminating between the jamming scenarios and the normal states of the network. In particular, it is hard to select a threshold that can distinguish between jamming and normal network conditions (e.g., congestion). Xu *et al* [10] [14] use spectral discrimination techniques in order to enhance detection. However, as shown in the paper, their scheme can detect only some types of jammers. In particular, it can detect the constant and the deceptive jammers, but it fails to detect the reactive and the random jammers.

2) Carrier Sensing Time In a CSMA network - e.g. 802.11 - the MAC protocol requires a node to first sense the channel to be idle for a specific amount of time prior to transmitting. Under normal conditions and for a specific network, the distribution of this *carrier sensing time* is known and can be acquired either theoretically or empirically. Monitoring for deviations from the *benign* distribution, can be used for jamming detection [10] [14]. However, the effectiveness of this scheme is similar to that of the scheme that relies on signal strength measurements; it can detect a constant and a deceptive jammer, but not a random or a reactive jammer. The random jammer spends time sleeping without affecting the carrier sensing time (during these periods), while the reactive jammer is not affecting transmissions at all.

3) Measuring the PDR In [10] and [14] the authors show that PDR measurements can help detect all types of PHY layer jammers. It is shown that even in a highly congested network the PDR remains as high as 78%. On the other hand, under a jamming attack, the PDR drops significantly. Therefore, a simple threshold can be set to distinguish between a congested network state and a state induced by a PHY layer jammer. However, there are still situations where PDR measurements can lead to false alarms. For example, such scenarios may arise when there is a network failure (such as a battery failure); the node under consideration stops sending packets and PDR drops to 0. In addition, poor link quality at the receiver (i.e. low SNR) can drastically reduce PDR. Clearly, PDR measurements can not always distinguish between jamming and network failures and/or poor link conditions.

4) Consistency Checks Xu *et al* [10] [14] introduce two detection techniques based on consistency checks. With these methods, one is able to detect all types of jammers and overcome the problem of distinguishing between network dynamics and jamming attacks. The two schemes are the following:

Signal Strength Consistency Check: The detection system measures both the PDR and the RSS (received signal strength). The key idea is that if we measure low PDR and high RSS then it is most likely that the node is jammed. On the other hand, if we measure low PDR with low RSS, then this can be due to a network failure or poor link quality.

Location Consistency Check: Similar to the RSS consistency check, the detection system measures the PDR, along with the location of the neighbors of the node under consideration. The thesis here is that if we measure low PDR and the distances to the neighbors are small, then with high probability the node is being jammed. On the other hand, if we have low PDR and the distances between the nodes are high, then this is likely due to nodes getting out of range or experiencing poor link quality (e.g., due to long separation distances[5]).

In [10], the authors show that both schemes can (i) detect all types of PHY jammers and (ii) distinguish the state induced from normal congested network states or dynamic failures in the network. However, there are still open issues. For example, the frequency of the location advertisements can significantly affect the performance of the location consistency check system. In addition, wireless propagation effects (e.g. fading) should be taken into consideration for accurately computing the false alarm rate of the IDS.

Li *et al*. [28] study the case of optimal PHY layer jamming in wireless sensor networks. Here, the goal of the jammer is to corrupt the maximum number of links while keeping the probability of detection low. In order to achieve this, it tunes the jamming probability and its transmission range. The goal of the IDS is to detect the jammer and notify the sensor nodes in a short time. The detection system utilizes monitor nodes and is based on measuring the *percentage of incurred collisions*. A training period, which can be large, is required in order for the detection algorithm to operate efficiently. The algorithm itself is based on Wald's Sequential Probability Ratio Test [29] and the reader is referred to [28] for more details.

B. Detection of MAC layer DoS/misbehavior

As described in Section IV-C7, selfish users can launch *active jamming attacks* in order to gain illegitimate frequent access to the medium, causing starvation to the other nodes. The most widely known selfish behavior detection system for WLANs is DOMINO (Detection Of greedy behavior in the MAC layer of IEEE 802.11 Networks) [23] . Its name seems to imply that it can only address greedy "legitimate" users. However, given the similarity of greedy behaviors to jamming attacks, DOMINO can be modified to be used as a jamming IDS. The main advantage of DOMINO is that it does not require any modifications to the existing infrastructure.

DOMINO consists of three modules. The first module is responsible for the collection of traffic traces. These traces are

[5]Note here that even if two nodes are close to each other, wireless propagation effects, such as fading, can significantly degrade the quality of the (short) link, and as a result the effectiveness of this detection scheme.

used as input to the second module which performs various tests, each specialized to detect a particular attack. The current version of DOMINO supports six such tests as described in [23]. Each test comprises of two components: the deviation estimation algorithm, which determines the deviation from the expected model, and the anomaly detection component which uses the previously estimated deviation in order to decide if a station is a well behaved node or not. The third and last module, is the decision making component, which aggregates all the results derived from the previous tests and decides if the station is an adversary. The decision making component is also divided into the aggregation component and the behavior classification component. The former can use several functions to aggregate the results from the tests. In the current implementation, this function is a simple logical OR operation. However, more complicated functions with weights can be used instead. The behavior classification component performs the actual classification using the result from the aggregate test.

Complementary to DOMINO, the authors in [26], design a detection scheme (called CMD for Carrier sensing Misbehavior Detection) for users who selfishly exploit CCA tuning. The key idea behind the detection, is that user who increase their CCA to gain more frequent access to the medium will treat signals that arrive at their circuitry with RSSI smaller than the CCA threshold, as noise[6]. Consequently, the authors propose a challenge-response scheme, where the AP transmits low power probes to nodes that obtain higher throughputs than their fair share. A detailed analytical and experimental evaluation of the proposed scheme shows that CMD can efficiently detect misbehaving nodes, with low probabilities of false alarm [26].

The most widely considered selfish strategy is the manipulation of the 802.11 backoff mechanism. Kyasanur *et al*. [24] propose a scheme that can detect a user that tries to access the channel more often by deviating from the standard exponential backoff mechanism. The motivation for such an adversarial strategy can be either to get higher share of the bandwidth or just to prevent other users from accessing the medium.

The proposed detection scheme consists of three modules that *modify* IEEE 802.11. The high level idea is that when a receiver sends a CTS or ACK packet to a sender, explicitly indicates to the sender the next, randomly selected, backoff time that it has to use. The first module of the system is used to identify deviations from the protocol. The receiver monitors the channel to check whether the sender is using the correct backoff time or not. The second module of the system uses the knowledge acquired by the first module to penalize the sender if it misbehaved in the last transmission; a larger backoff time proportional to its deviation is assigned for the next transmission. In some cases, a deviation might be falsely determined due to, for example, hidden terminal problems. However, in such instances the deviation, and consequently the penalty, will be small leading the system to an overall satisfactory performance in the long term. The last module of the system is the diagnosis module. It monitors the deviations using a sliding window of length W. If the sum of the deviations exceeds a threshold, the node is classified as malicious.

Despite the reasonable performance achieved with the above scheme, there are some issues that need to be further examined. It is interesting to examine what happens when colluding attackers exist; what are the changes required in order to prevent the attack? Furthermore, how can one avoid extended misdiagnosis? Extensions of the above system are found in [25].

Radosavac *et al* [31] propose a theoretical framework for detecting misbehaving nodes that deviate from the backoff mechanism. They consider the case of an intelligent attacker, which adapts its strategy trying to avoid detection for as long as possible. The authors formulate the detection problem within a minmax robust detection framework and they prove that the optimal detection rule is a Sequential Probability Ratio Test (SPRT). Nodes observe the backoff times used by the other legitimate users and using SPRT they try to detect misbehaving entities. In contrast with the schemes in [24] [25], it does not require changes to the 802.11 protocol. However, it comes with some assumptions that can make its deployment hard; accurate node synchronization is needed and constantly backlogged nodes are assumed. In addition, issues related to inaccurate measurements due to interference and/or colluding nodes need to be addressed.

C. A Wireless Distributed IDS

Aime *et al*. propose a distributed IDS [32]. The basic concept is that a node by itself cannot decide if an observed degradation in performance is due to a network failure or due to a jamming attack. In order to make a correct decision, all nodes need to cooperate. Every node in the network monitors the ongoing traffic and creates a list of evidence, relating to events that take place on the wireless medium. Such events include the number of packets sent, the duration of idle periods, the number of corrupted packets, etc. When every user has created its own list, nodes exchange them and try to match events. This combination leads to a better understanding of what happens in the network and more importantly it can distinguish between jamming attacks and channel failures. The corresponding two network states have the same basic *signature* - packets transmitted but never received - but they differ in their position in the event list. As an example, an attack will result in a number of packets lost sequentially, while channel failures will have packets lost here and there. The whole process resembles to a large extent, data fusion techniques which have been traditionally used in wired IDSs; data from many different sensors are combined in order to support evidence [33].

The main drawback of this system is the need for an event list exchange. If a node is being jammed it will not be able to perform this exchange in real-time (during the attack period), but the evidence will be shared only at later time. Therefore, this scheme is not appropriate for real time detection. Moreover, the system should be augmented by a trust/reputation mechanism; some nodes might intentionally report wrong lists in order to mislead the detection scheme. More details on the protocol used to share lists and the

[6]Most commodity cards set their CCA threshold to be equal to the receiver sensitivity [30].

algorithm are beyond the scope of this work, and can be found in [32].

D. Wireless Ad Hoc Networks Intrusion Detection

As mentioned before, mobile ad hoc networks (MANETs) are more susceptible to attacks due to the lack of infrastructure. Features such as, open medium, dynamic topological changes, limited bandwidth, distributed cooperation and constrained energy resources are some of the characteristics that make MANETs more vulnerable.

Recently there has been an increased interest in wireless MANET intrusion detection. A brief overview of these works can be found in [27]. In particular Zhang *et al*. [34] describe a distributed IDS for MANETs, where an IDS agent operates at each mobile node of the network. This scheme is further extended in [35] by trying to enhance the security of the AODV routing protocol. A local IDS is proposed in [36]; the system is based on mobile agents which collect existing data from the Management Information Base (MIB) using the SNMP protocol. Collecting such information does not incur much cost for an agent running SNMP and mobile agents can reach remote nodes. Both of the above factors, constitute two important advantages of the proposed IDS. The authors in [37] propose an IDS based on Support Vector Machines. The SVM data mining technique is very powerful and is used for classification when there are previously unseen events. In their work, an SVM is being used in order to classify the traffic that is being collected as normal or abnormal. More studies on ad hoc IDSs can be found in [38] [39] [40], and a detailed comparison of these systems can be found in [27].

VI. Intrusion Prevention Schemes

As their name suggests, Intrusion Prevention Systems try to prevent jamming by either *avoiding* or *fighting* against the malicious entities.

A. Frequency Hopping

Frequency hopping has been traditionally employed in order to overcome the presence of a jammer [14] [41] [42]. Frequency hopping can be either reactive or proactive. In the reactive case, when a node detects that it is jammed it switches to a different channel and sends a beacon message on the new channel, announcing its presence. Its non-jammed neighbors will sense its absence and will change their bands of operation to check if their lost neighbor has sent beacons announcing its presence on a different channel. If not, then they assume that the node just moved away. Conversely, if they sense a beacon, they will inform the other nodes in the network to change channels. At this point, there are two possible approaches. The first approach would be for the entire network to eventually migrate to the new, non-jammed channel. Alternatively, only the boundary nodes of the jammed region will change their frequency of operation; these nodes will be then used as relays between the non-jammed and the jammed areas of the network.

Navda *et al*. [42] implement a proactive frequency hopping protocol with pseudo-random channel switching. They compute the optimal frequency hopping parameters, assuming that the jammer is aware of the frequency hopping procedure that is followed. They show that their scheme can retain up to 60% of the throughput achieved under benign conditions; in addition there is no significant degradation when there is no jammer.

Gummadi *et al* [20] propose a rapid frequency hopping scheme in order to avoid narrow-band jamming. The authors first show - as mentioned earlier - that 802.11 devices are vulnerable to specific patterns of narrow-band interference relating to time recovery, dynamic range selection and PLCP-header processing. A jammer exploiting this vulnerability, can cause a significant number of packets to be corrupted with even an 1000 times weaker signal than that of the legitimate transceivers. In order to overcome this problem a rapid frequency hopping scheme is proposed. Frequency hopping is based on the premise that operating on an orthogonal channel of that of the jammer, suppresses the jamming interference. However, frequency hopping techniques try to avoid the malicious node (and in particular its band of operation), rather than fighting against the latter. Taking into account that current commercial systems, use only a small number of orthogonal bands, and that adjacent orthogonal channel interference exists, frequency hopping has been shown to be rather ineffective. In particular, the authors in [43] have shown that adjacent orthogonal channels are not fully *separated*, that is, a jammer residing on a channel can still harm communications on adjacent (orthogonal) channels. The authors after quantifying this effect through measurements, model the interactions between a jammer and a link as a zero-sum, two person game, obtaining bounds on the anti-jamming performance of frequency hopping. Multiple jamming devices operating on different bands can effectively block the entire spectrum. Note that, multi-channel jamming attacks canbe launched by utilizing cognitive radios. In such a scenario, with one radio, one can jam multiple channels [44]. Concluding, anti - jamming schemes that try to fight against a co-channel jammer (instead of simply avoiding it) are of interest due to the above deficiencies of frequency hopping. As an example, the preliminary work in [45], tries to fight against co-channel jamming utilizing rate and power control techniques. In addition, it can be potentially used, in conjunction with frequency hopping for enhanced performance.

B. Spatial Retreats

Mobile nodes affected by the jammer can move away from their initial positions to avoid jamming signals. In brief, when a node detects that it is being jammed, it tries to (a) *escape* from the jammed area (*evasion phase*) and (b) *stay connected* with the rest of the network (avoiding partition with the rest of the network - *reconstruction phase*) [14] [41]. In particular, when a node senses that it is being jammed, it starts moving out of the jammed region; at the same time it executes a detection algorithm trying to stay connected with its previous neighbors. The latter is achieved by moving along the boundary of the jammed area. If the evading node was blindly moving away from the jammed area, the connectivity of the network could be significantly affected.

C. Fighting Reservation Based DoS attacks

As mentioned earlier, an adversary can send an RTS packet, requesting the medium for a period of M slots, while it does not have actual data to send. This results in the under-utilization of the medium; no packets are on the air but the legitimate users cannot access it. Negi *et al*. [46] propose the usage of a new control packet, called CTSR, to address this attack. More specifically, in a WLAN setting, the access point can periodically (e.g. every K slots) sense the channel to deduce if there is an ongoing transmission, as should be the case. If the medium is not busy, the AP revokes it by sending out a CTS packet with $NAV\_DURATION = 0$ (CTSR packet).

However, the jammer can adapt its strategy in order to overcome the above prevention scheme. The adversary can send out a jamming packet every K slots, in order to deceive the AP into sensing an ongoing transmission. However, given that for early detection it is required that $K \ll M$, the jammer will have to spend a lot of energy in order to keep deceiving the AP. Thus, its power efficiency will be reduced.

D. Securing our Network from a Layered Jamming Attack

In section IV-B a simple model of a layered jamming attack was presented. This model tries to exploit existing patterns in protocols related to the size, the interframe time periods and the sequence of the packets being exchanged. A simple way to make a network resilient against such intelligent jamming attacks is to obfuscate these patterns when possible. As an example, for obfuscating the packet size consistencies a simple padding technique can be used; every control packet can be made to be of the same size, making it more difficult for a jammer to recognize such packets. This padding only has a very small impact on throughput as explained in [18]. The authors of [18] also suggest that protocols based on overly precise timing should be modified in such a way that additional delays are added. These delays could be indicated in the packet headers.

Finally, obfuscating the packet sequence is more challenging. A technique proposed in [18] for this purpose is that of *packet aggregation*; multiple packets can be aggregated to perturb the sequence relating to packet consistency. The authors do not provide a specific implementation, giving only guidelines for the properties that the system needs to satisfy. They state that the system should be able to aggregate data packets transmitted between one or more sessions on a source system and one or more sessions on a target system. In particular, the system must (a) collect and multiplex packets from the system session(s) of the source into one aggregated packet and (b) demultiplex the latter at the destination system, delivering the original packets at the corresponding sessions. This procedure affects also the interpacket timing and the size of packets. At the same time the precise number of packets that are exchanged is hidden. Thus, packet aggregation can be deployed against sophisticated layered jamming attacks.

E. PHY layer anti-jamming techniques

In this section we present anti-jamming techniques that are built entirely at the PHY layer [47] [48].

1) Simple PHY Layer Techniques: The jamming-to-signal ratio, captured by Equation 3, provides various insights on possible ways to fight against jammers. For instance a legitimate transmitter can *increase its transmission power*. As another example the distance between the transmitter and the receiver, i.e., the *length of the link*, can be reduced, thus boosting the received signal strength. Both of this approaches are brute force techniques. They result in a decreased jamming-to-signal ratio and hence, can be expected to improve performance. However, such strategies might not provide significant benefits in CSMA/CA networks (e.g. 802.11, sensor networks, etc.); decreasing the jamming-to-signal ratio will potentially help in cases where only the receiver is affected by the jammer. If the transmitter is able to sense the jammer, packets will not be transmitted at all, causing a severe performance degradation.

2) Directional Antennas: Noubir [12] proposes the use of *directional antennas* as a means for combating the jammer. This results in an increased antenna gain from the transmitter to the receiver and vice versa, decreasing as a consequence the jamming to signal ratio. The same effect can also be achieved by using sectored antennas, or other types of smart antennas that focus the beam's power on the receiver. Using directional antennas, can also help at mitigating jamming effects at a CSMA/CA transmitter. In particular, based on the radiation patterns of the antenna used, jamming interference coming from directions other than the direction of transmission does not stimulate transmission deferrals due to carrier sensing; in other words packets can still be transmitted despite the presence of a jammer.

3) Spread Spectrum: The above methods do not perform any processing of the transmitted signals; they just change the transmission parameters of the signals (e.g. power, directionality, etc.). However, there are PHY layer signal processing techniques used as jamming countermeasures. The most well known techniques are based on the use of *Spread Spectrum communications* [49]. Spread-spectrum communications refer to signal structuring techniques that employ direct sequence, frequency hopping or a combination of these. Spread spectrum can be used for multiple access. These techniques decrease the potential interference to other receivers, by making use of a sequential, noise-like, signal structure to spread the (usually) narrow band information signal over a relatively wider (radio) frequency. The receiver correlates the received signals to retrieve the original information signal. Initially, there were two motivations behind spread spectrum communications: (a) to resist enemy efforts to jam communications (anti-jam, or AJ) and (b) to hide the fact that communication was taking place (sometimes referred as Low Probability of Intercept (LPI)).

However, despite the usage of spread spectrum techniques, the communication link is not totally secured against jammers; the adversary does not have to be aware of the complete spectrum-transition sequence, e.g. the frequency hopping sequence, in order to disrupt communication. For instance, in the case of voice communications between human users, the corruption of a small part of the conversation will have a minor effect on the quality of the communication. However, in the case of data communications (assuming absence of error-correction) the corruption of a single bit is enough to

compromise the whole communication process. In addition, similar to brute force techniques discussed earlier, spread spectrum cannot protect a CSMA/CA transmitter from the presence of a jammer. Finally, the *near far problem* [50] also exists with random 802.11 network deployments, and this might cause spread spectrum systems to be ineffective in coping with jamming.

4) Cyber Mines and FEC: The use of FEC increases overhead but can help in the presence of a jammer. The main drawback of not using any error-correction, is that the attackers need to corrupt just a single bit in a packet to achieve their objective. This requires very low jamming energy. The corruption of a single bit is enough to cause a packet reception failure. Thus, adversaries can achieve high *jamming efficiency* (high energy efficiency with high levels of DoS). Such low-energy long-lived jamming units are called **cyber-mines**.

Handling Cyber mines: The authors in [47] [48] propose a scheme that aims to force the jammer into spending more energy in order to achieve its goal. Simply put, their goal is to eliminate cyber-mines. Towards this, they investigate the performance of various error-correction schemes; they conclude that the most suitable codes for binary modulation in the presence of a jammer are the Low Density Parity Codes (LDPC). The main advantages of LDPC are: (a) they result in a capacity close to Shannon's bound, (b) they perform very well with long packets (of the order of 16,000 bits) which makes them suitable for IP-networks and (c) they are relatively easy to implement. In addition, the authors find that a good alternative to LDPC are Turbo-Codes. Such codes are especially suitable for shorter packets. In practice, in order to improve the error tolerance, an interleaver is used in conjunction with error-correction codes (ECC). The main problem with traditional communication systems is that the structures of the interleaver and the ECC are publicly known. Consequently, the adversary can attack those (critical) bits that result in a burst of errors such that the underlying error correction will fail. To overcome this problem the use of cryptographic-interleaving is proposed. With this, the reordering of bit-blocks in a transmission frame are permuted, known only to the two communicating parties. Such information can be exchanged secretly using any standard encryption scheme.

The price of using ECC is the additional overhead for the transmission of the redundant bits and the additional communication latency; the complete information cannot be retrieved before the reception of all the interleaved information blocks. The gain however, is an increased ambiguity in terms of which bits must be jammed, in order for a packet to fail the CRC check at the receiver. Therefore, the scheme proposed prevents jammers from attacking the network while preserving energy.

5) Use of covert channels in the presence of a jammer: Xu *et al* [51] propose the set up of a covert timing channel that will exist even in the presence of a jammer. The key idea is that in a jamming environment where only the reception of a packet is being affected, the receiver can identify the reception of a (corrupted) packet. By encoding data based on the inter-arrival times between received corrupted packets, a low rate channel under jamming can be established. The authors propose an extension of their scheme, to account for multiple users. They propose a time-slotting system that makes use of optical orthogonal codes [52]. The reader is referred to [51] for more details.

We would like to reiterate, that most of the PHY layer anti-jamming schemes try to mitigate the jamming effects at the receiver. There is an implicit assumption that packets can be transmitted by the sender. However, as discussed above, many wireless systems employ carrier sensing to define their medium access policy; this makes packet transmissions vulnerable to jamming as well.

F. Wormholes

Until recently wormholes were thought to be a threat for a wireless network [53] [54] [55]. Cagalj *et al* [56] though, proposed a reactive anti-jamming scheme for wireless sensor networks using wormholes. The basic idea is that jammed nodes can use channel diversity, to establish communication with another user outside the jammed area. There are 3 proposed types of wormholes:

- ***Wired pairs of sensors:*** A sensor network can be enhanced by connecting a subset of node pairs that are through wires. It is shown in [56] that in order to be able to arbitrarily form a wormhole pair between the exposure region and a non-jammed area with high probability, a large number of wired pairs is required.
- ***Frequency hopping pairs:*** The pairs are created by utilizing nodes with frequency hopping capabilities. All pairs deployed use frequency hopping and thus links are resistant to jamming[7]. However this technique requires synchronization in order for the frequency hopping scheme to operate.
- ***Uncoordinated channel-hopping:*** In this scenario, sensor nodes that are capable of hopping between radio channels that span a large frequency band try to create uncoordinated wormholes among themselves. The difference as compared to the previous solution is that now an entire packet is being transmitted on a single channel. As a result the hops between the different channels occur at a much slower timescale as compared to classical frequency hopping.

More information and a detailed probabilistic analysis on the formation of the wormholes can be found in [56].

The frequency/channel hopping wormhole pairs suffer from the same deficiencies of frequency hopping anti-jamming schemes. For example, the presence of a wide band jammer can completely disable the formation of these types of wormholes. In addition, establishing wired connections between pairs of sensors can be unrealistic in real world deployments. As a result there are still open research problems with respect to using wormholes as a jamming countermeasure.

G. Protocol Mechanism Hopping

As mentioned earlier, intelligent jammers take advantage of specific protocol parameters (at any layer of the protocol stack). Once a vulnerability is identified, the intelligent

[7]The authors assume that the jammer cannot harm frequency hopping communications.

TABLE I
Characteristics of various jamming models (Poor, Low, Medium, Average, High).

Jamming Model	Implementation Complexity	Energy Efficiency	Stealthiness	Level of DoS	Anti−Jamming Resistance
Constant [10]	Low	Low	Low	High	Medium
Deceptive [10]	Low	Low	Low	High	Medium
Random [10]	Low	Adjustable	Medium	Adjustable	Medium
Reactive [10]	High	High	Medium	High	Low
Packet Corruption [11], [21]	Average	High	Average	High	Low
Narrow-band [20]	High	High	High	High	Average
DIFS Waiting [11], [21]	Medium	Medium	Medium	High	Low
Identity Attacks [22]	Medium	Average	Average	High	High
Layered Attacks [18]	High	Low	Average	High	Medium

jammer can consistently exploit it and significantly degrade the performance. Liu *et al* [57] propose a game-theoretic framework for modeling the interactions between a smart jammer and protocol specific functions. Based on this framework they propose SPREAD (Second-generation Protocol Resiliency Enabled by Adaptive Diversification), a system to provide robustness against intelligent jamming attacks. In a nutshell, SPREAD chooses and hops across various protocol parameters based on the strategy being used by the jammer. SPREAD hinders the effectiveness of the jammer by hiding the underlying vulnerabilities that the jamming entity tries to exploit. The authors provide as an example a game where packet sizes are tuned, using their game theoretic framework. Their approach can be thought as a generalization of the frequency hopping schemes. However, there is a significant effort needed in order to bridge the gap between the theoretical formulation of SPREAD and a practical anti-jamming system implementation.

VII. Discussion, Future Work and Further Reading

Effectively addressing the jamming problem clearly requires a cross-layer approach; different jamming models exploit parameters of different protocols/functionalities. Thus, anti-jamming methods discussed in this survey can operate in complementary way to each other. A combination of the proposed schemes can be used in an appropriate way, in order to implement a unified anti-jamming system that caneffectively address the problem. Researchers should always keep in mind that adversaries often come up with more intelligent ways of launching jamming attacks and as a result we need to act proactively. Furthermore, most of the existing work is theoretical and in many instances make *unrealistic* assumptions. Future research on jamming could benefit from system implementation. Two very recent works, following this path, combine ideas and techniques from optimization theory in a practical system implementation. In particular, Broustis *et al* [58], acting proactively, identify a new, intelligent jamming attack on WLANs. After demonstrating its malicious effects, they implement a cross-layer detection and mitigation system. In particular, they alleviate the attack via traffic shaping based on the solutions to a set of optimization problems. The authors of [59], utilize the main idea of gradient descent optimization algorithm to design and implement a jammer localization system. Despite similar research efforts, the gap between theory and practice in wireless networks, and as a consequence in jamming research as well, is still big. However, researchers should focus on closing this gap in the future and having more practical systems implemented towards *fighting* with real world adversaries. Finally, on a different note, jamming has been recently proposed, for augmenting security systems for communications in sensor networks. In particular, Martinovic *et al* [60] propose the use of jamming in order to destroy unauthenticated packets on the air. This way, nodes will not need to receive and authenticate these packets and this translates to a lower energy consumption overall. Nevertheless, there are still open research issues that accompany such an approach. For example, one needs to be sure that the packets that are jammed are fake packets. The trade off between the energy spent to jam and the one required to receive and authenticate a packet needs to be carefully examined. Despite these issues, using jamming for the benefit of the network is a novel and yet an unexplored research area which will attract a lot of attention during the next years.

Further reading: A reader interested in jamming attacks on wireless sensor networks can further refer to the work by Mpitziopoulos *et al* [61]. Work on attacks and on wireless networks in general and on countermeasures thereof are found in [62] [63] [64] [65] [66] [67]. These studies present surveys on security issues in wireless networks.

VIII. Conclusions

Jamming is still an open and important research problem. In this paper, we tried to gather together the majority of the research on this area. We present:

- a plurality of jamming models that have been considered in the literature,
- various jammer detection strategies that have been proposed and,
- anti-jamming schemes.

Table I summarizes the characteristics of the various jamming models examined in this paper. Every solutionthat has been proposed exhibits limitations and there are more things that need to be done in order for the problem to be solved satisfactorily. For example, frequency hopping techniques assume that rapid hopping between channels is possible. However this might depend on the hardware used. A prior work [68] has reported that *switching from one channel to another and the subsequent restoration of a data session may take from 600 to 1000 msec*. During the switching period, there is no traffic flowing from/to the node, and this decreases the long-term

throughput. However, even if such delays can be minimized with driver's modifications [69], multiple jammers residing on different channels as well as wide-band jammers can easily overcome the use of frequency hopping techniques [43].

Other prevention schemes require properties that might not be applicable in realistic scenarios. For example evasion techniques require the mobility of the nodes, which might not be possible, while other solutions require modifications of the current protocols. Given the already widespread deployment of wireless systems, solutions that require large scale changes (and cannot be applied for example through a software patch) are unrealistic. We have tried to gather the most important studies existing on the jamming-related research. We believe that this survey will help future studies on comparing, challenging and, most importantly, improving currently existing solutions to cope with jamming.

REFERENCES

[1] Q.Huang, H.Kobayashi, and B.Liu. "Modeling of distributed denial of service attacks in wireless networks," in *IEEE Pacific Rim Conf. Commun., Computers and Signal Process., vol. 1, pp. 113-127, 2003*.

[2] L.Sherriff, "Virus launches DDoS for mobile phones," [Online]. Available: http://www.theregister.co.uk/content/l/12394.html

[3] SESP jammers. [Online]. Available: http://www.sesp.com/.

[4] ISM Wide Band Jammers. [Online]. Available: http://69.6.206.229/e-commerce-solutions-catalog1.0.4.html.

[5] ISA: "Users fear wireless networks for control," [Online]. Available: http://lists.jammed.com/ISN/2007/05/0122.html

[6] Mobile Device Jammer. [Online]. Available: http://www.phonejammer.com/home.php

[7] "Jamming attack in Hackers' Conf.," [Online]. Available: http://findarticles.com/p/articles/mi_m0EIN/is_2005_August_2/ai_n14841565.

[8] Techworld news. [Online]. Available: http://www.techworld.com/mobility/news/index.cfm?newsid=10941.

[9] RF Jamming attack. [Online]. Available: http://manageengine.adventnet.com/products/wifi-manager/rfjamming-attack.html.

[10] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *MobiHoc 05*, May 25-27, 2005, Urbana-Champaign, Illinois, USA, pp 46-57.

[11] M. Acharya and D. Thuente, "Intelligent jamming attacks, counterattacks and (counter)2 attacks in 802.11b wireless networks," in *Proc. OPNETWORK-2005 Conf.*, Washington DC, USA, Aug. 2005.

[12] G.Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility," *Technical Report, Dec. 2003*.

[13] C. D. Schleher, "Electronic Warfare in the Information Age," 1999, Norwood, Artech House.

[14] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attacks and defense strategies," in *IEEE Netw., May/June 2006*.

[15] Y. Law *et al*., "Link-layer jamming attacks on S-Mac," in *Proc. 2nd Euro. Wksp. Wireless Sensor Netw.*, 2005, pp. 21725.

[16] A. Wood and J. Stankovic, "Denial of service in sensor networks," *IEEE Comp.*, vol. 35, no. 10, Oct. 2002, pp. 5462.

[17] G.Noubir and G.Lin, "Low power DoS attacks in data wireless LANs and countermeasures," in *Proc. Poster: ACM MobiHoc 2003*. Annapolis, MD: ACM Press.

[18] T.X.Brown, J.E.James, and A.Sethi, "Jamming and sensing of encrypted wireless ad hoc networks," in *MobiHoc06*, 22-25 May, Florence, Italy.

[19] B. O'Hara and A. Petrick, "IEEE 802.11 Handbook. A designer's companion," 2nd edition, Standards Information Network, IEEE Press.

[20] R. Gummadi, D. Wetheral, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of RF interference on 802.11 networks," in *ACM SIGCOMM, 2007*.

[21] M. Acharya, T. Sharma, D. Thuente, and D. Sizemore, "Intelligent jamming attacks in 802.11b wireless networks," in *Proc. OPNETWORK-2004 Conf.*

[22] J.Bellardo and S.Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proc. USENIX Security Symposium03*, Aug. 03.

[23] M.Raya, I.Aad, J-P.Hubaux, and A. El Fawal, "DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots," in *Proc. ACM MobiSys, Boston (MA), USA, 2004*.

[24] P.Kyasanur and N.Vaidya, "Detection and handling of MAC layer misbehavior in wireless netwoks," in *Proc. International Conf. Dependable Syst. Netw.*, June 2003.

[25] P.Kyasanur and N.Vaidya, "Selfish MAC layer misbehavior in wireless networks," in *IEEE Trans. Mobile Comput.*, vol. 4, no. 5, Sept./Oct. 2005.

[26] K. Pelechrinis, G. Yan, S. Eidenbenz and S.V. Krishnamurthy, "Detection selfish exploitation of carrier sensing in 802.11 networks," in *IEEE INFOCOM 2009*, Apr. 2009.

[27] A.Mishra, K.Nadkarni, and A.Patcha, "Intrusion detection in wireless ad hoc networks," *IEEE Wireless Commun.*, Feb. 2004.

[28] M. Li, I. Koutsopoulos, and R. Pooverdan, "Optimal jamming attacks and network defenses policies in wireless sensor networks," in *Proc. IEEE INFOCOM* 2007.

[29] A. Wald, "Sequential Analysis," Wiley 1947.

[30] V. P. Mhatre, K. Papagiannaki, and F. Baccelli, "Interference mitigation through power control in high density 802.11 WLANs," in *IEEE INFOCOM* 2007.

[31] S. Radosavac, J. S. Barras, and I. Koutsopoulos, "A framework for MAC protocol misbehavior detection in wireless networks," in *ACM WiSe*, 2005.

[32] M.D.Aime, G.Calandriello, and A.Lioy, "A wireless distributed Intrusion Detection System and a new attack model," in *Proc. 11th Symp. Comput. Commun.*, 2006, ISCC 06.

[33] V.Chatzigiannakis, G. Androulidakis, K. Pelechrinis, S. Papavassiliou, and V. Maglaris, "Data fusion algorithms for network anomaly detection: classification and evaluation," in *ICNS 2007*, Athens, Greece.

[34] Y.Zhang and W.Lee, "Intrusion detection in wireless ad hoc networks," in *ACM MobiCom 00*, Boston, MA.

[35] S.Bhargava and D.P.Agrawal, "Security enhancements in AODV protocol for wireless ad hoc networks," in *VTC 2001 Fall*, vol. 4, Oct. 7-11, 2001.

[36] P.Albers *et al*. "Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches," in *1st International Workshop Wireless Info., Syst.*, Ciudad Real, Spain, Apr. 3-6, 2002.

[37] H.Deng, Q-A.Zeng, and D.P.Agrawal, "SVM-based intrusion detection system for wireless ad hoc networks," in *VTC*, 2003.

[38] Y.Zhang, W.Lee, and Y.-A.Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *in ACM J. Wireless Net., vol. 9, no. 5, Sept. 2003, pp. 545-56*.

[39] A.B.Smith, "An examination of an intrusion detection architecture for wireless ad hoc networks," in *5th National. Colloq. Inf. Syst. Sec. Education*, May 2001.

[40] O.Kachirski and R.Guha, "Intrusion detection using mobile agents in wireless ad hoc networks," in *Knowledge Media Net., Proc. IEEE Wksp.*, July 10-12, 2002, pp. 153-58.

[41] W.Xu et al, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *Proc. 2004 ACM Wksp. Wireless Security*, 2004, pp.80-89.

[42] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, "Using channel hopping to increase 802.11 resilience to jamming attacks," in *IEEE INFOCOM, Mini-Conf.*, 2007.

[43] K. Pelechrinis, C. Koufogiannakis and S.V. Krishnamurthy, "Gamming the jammer: Is frequency hopping effective?," in *WiOpt*, 2009.

[44] A. Sampath, H. Dai, H. Zheng, and B. Y. Zhao, "Multi-channel jamming attachs using cognitive radios," in *IEEE ICCCN*, 2007.

[45] K. Pelechrinis, I. Broustis, S.V. Krishnamurthy and C. Gkantsidis, "ARES: An anti-jamming reinforcement system for 802.11 networks," in *ACM CoNEXT*, 2009.

[46] R.Negi and A.Rajeswaran, "DoS analysis of reservation based MAC protocols," in *ICC*, 2005.

[47] G.Noubir and G.Lin, "Poster: Low-power DoS attacks in data wireless LANs and countermeasures," in *MobiHoc 03*, June 1-3, Annapolis, MD, USA.

[48] G.Lin and G.Noubir, "On link layer denial of service in data wireless LANs," *Wireless Commun. Mobile Comput.*, May 2003.

[49] A. J. Viterbi, "Principles of Spread Spectrum Communication," Addison-Wesley Wireless Communications Series.

[50] J. Proakis, "Digital Communications," Third Edition, McGraw-Hill, 1995.

[51] W. Xu, W. Trappe, and Y. Zhang, "Anti-jamming timing channels for wireless networks," in *ACM WiSec* 2008.

[52] F. Chung, J. Salehi, and V.Wei, "Optical orthogonal codes: design, analysis and applications," *IEEE Trans. Inf. Theory*, 1989.

[53] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in *INFOCOM*, 2003.

[54] P. Papadimitratos, and Z. Haas, "Secure routing for mobile ad hoc networks," in *Proc. SCS Commun. Netw. Distributed Syst., Modeling Simulation*, 2002.
[55] K. Sanzgiri, B. Dahill, B. Levine, C Shields, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in *ICNP*, 2002, pp.78-89.
[56] M.Cagalj, S.Capkun, and J.-P.Hubaux, "Wormhole-based anti-jamming techniques in sensor networks," *IEEE Trans. Mobile Comput.*, May, 2006
[57] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "SPREAD: Foiling smart jammers using multi-layer agility," in *IEEE INFOCOM, Mini-Conf.*, 2007.
[58] I. Broustis, K. Pelechrinis, D. Syrivelis, S.V. Krishnamurthy and L. Tassiulas, "FIJI: Fighting implicit jamming in 802.11 WLANs," *SecureCom*, 2009.
[59] K. Pelechrinis, I. Koutsopoulos, I. Broustis and S.V. Krishnamurthy, "Lightweight jammer localization in wireless networks: System design and implementation," *Globecom*, 2009.
[60] I. Martinovic, P. Pichota, and J. B. Schmitt, "Jamming for good: A fresh approach to authentic communication in WSNs," *ACM WiSec*, 2009.
[61] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, 2009.
[62] Xiangqian Chen, Kia Makki, Kang Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, 2009.
[63] Y. Zhou, Y. Fang and Y. Zhang, "Securing wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 6-28, 2008.
[64] L. Abusalah, A. Khokhar and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Commun. Surveys and Tutorials, Vol. 10, no. 4, pp. 78-93, 2008.*
[65] T. R. Andel and A. Yasinsac, "Surveying security analysis techniques in MANET routing protocols," *IEEE Commun. Surveys Tuts.*, vol. 9, no. 4, pp. 70-84, 2007.
[66] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2-23, 2006.
[67] P. G. Argyroudis and D. O'Mahony, "Secure routing for mobile ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 3, pp. 2-21, 2005.
[68] R. Vedantham, S. Kakumanu, S. Lakshmanan, and R. Sivakumar, "Component based channel assignment in single radio, multi-channel ad hoc networks," *ACM MobiCom*, 2006.
[69] S. Kandula, K.C-J. Lin, T. Badirkhanli and D. Katabi, "FatVAP: Aggregating AP backhaul capacity to maximize throughput," *USENIX NSDI*, 2008.

Konstantinos Pelechrinis received the diploma of Electrical and Computer Engineering from the National Technical University of Athens, Greece, in 2006 and the MSc degree from the Computer Science department of University of California, Riverside, in 2008. He received his PhD from the Computer Science department of University of California, Riverside, in 2010 and he will be joining the SIS faculty of the University of Pittsburgh in Fall 2010. His research interests include wireless networking, especially security - related issues that span the full protocol stack. He is involved in protocol design, real world experimentation and performance analysis. He is also interested in mathematical foundations of communication networks. He is a student member of IEEE.

Marios Iliofotou received his B.S. degree in Electrical and Computer Engineering in 2005 from the Technical University of Crete in Greece. He received the M.S. degree in Computer Scene from the University of California, Riverside in 2007. He is currently a PhD candidate in the Computer Science department of the University of California, Riverside. His research interesets lay on the area of network monitoring and security.

Srikanth V. Krishnamurthy received his Ph.D degree in electrical and computer engineering from the University of California at San Diego in 1997. From 1998 to 2000, he was a Research Staff Scientist at the Information Sciences Laboratory, HRL Laboratories, LLC, Malibu, CA. Currently, he is a Professor of Computer Science at University of California, Riverside. His research interests are primarily in wireless networks, network security and Internet technologies. Dr. Krishnamurthy is the recipient of the NSF CAREER Award from ANI in 2003. He has also co-edited the book "Ad Hoc Networks: Technologies and Protocols" published by Springer Verlag in 2005. He served as the editor-in-chief for ACM MC2R between 2007 and 2009 and is a senior member of the IEEE.