Jamming Attacks on Wireless Networks: A Taxonomic Survey

Author information blinded

Abstract

Defense against jamming attacks has been an increasing concern for the military and disaster response authorities. The military uses jamming attacks as a tool to attack and disrupt terrorist's communications, because the open nature of wireless networks makes them vulnerable to various attacks. Many studies and a few survey papers are available in the literature, but none of these papers classify the attacks or the defense strategies by the type of wireless network affected, the attacker or defender's perspective, the type of game used to model the problem, such as Bayesian game, Stackelberg game, or the type of solution methodology, such as mathematical programming model and algorithm. This paper provides a comprehensive survey and a taxonomic classification to help interested researchers find the gaps in the literature and guide them to research areas that need to be explored.

Keywords: Jamming attack, wireless networks, survey, taxonomy

1. Introduction

1.1. Introduction to wireless networks

Wireless networks refers to computer networks where communication between two devices like laptops is done without the use of cables or wires. The most widely used wireless network is the wireless local area network (WLAN), more commonly known as Wi-Fi. WLAN is available in homes, schools, offices, coffee shops, etc., which allows for easy access to the Internet whenever needed, as long as the device can connect to the Wi-Fi signal. The computers connect to an access point (AP) through wireless means to connect to the Internet and allow the users to move freely within the range of the Wi-Fi signal. Figure 1 shows an example of a WLAN with one AP and six computers that communicate with the AP via a wireless medium. Another type of wireless network, used mostly in the military and disaster situations, is the wireless ad hoc network (AHN). The network is called *ad hoc* because it does not need any pre-existing infrastructure, like cables or access points. Here, each node, e.g. laptop, cellphones, participates in the networks routing of data by forwarding it from one node to another without any centralized management equipment like an AP. The nodes in an AHN dynamically decide to which node to send the data depending on network connectivity. Figure 2 shows a basic setup of an AHN between laptops and phones that communicate among themselves without an AP. Some of the most important application [75, 110] of AHNs are:

- Military units, such as soldiers, tanks, and ships can communicate even in the absence of well defined wireless infrastructure by forming an AHN.
- AHNs can also be used for emergency, law enforcement, and rescue missions.
- AHNs are also used in conferences, lectures, meetings, and other commercial areas where the network loads can be very high.

Another type of wireless network is the Wireless Sensor Network (WSN), which is a collection of a large number of individual autonomous nodes that share information among themselves. In a WSN the data collected is not directly sent to the user, rather, it is first aggregated and then sent [72]. A WSN consists of a gateway or base station, that connects the sensor nodes to other sensor networks, or to the end user. (See Figure3.) The data at the sensor nodes is compressed and transmitted to the base station, which presents the results to the end user [88]. The data packets are sometimes sent to the destination via several intermediate nodes. This transmission by hopping from one node to another is called multi-hop. Figure 3 shows a WSN with a sensing area gathering information that is transmitted among the sensors, and the final result of all the data is sent to the base station to forward the data to the end user. One application of WSN is environment and habitat monitoring.

Other than the above mentioned WLAN, AHN, and WSN there exist numerous other networks that serve a variety of purposes. Wireless personal area networks (WPAN) are networks that connect devices within a very small area, for example, a Bluetooth enable computer mouse connects to the laptop via Bluetooth. Wireless wide area networks (WWAN) are present in large public areas and perform long-haul connectivity, e.g. connecting two cities. Wireless mesh networks are wireless networks that consists of nodes that are arranged in a mesh topology. A mesh topology is a network topology, in which the the data from the source to the destination node is relayed by intermediate nodes in the network. Wireless mesh networks are sometimes also considered to be AHN networks. Wireless metropolitan area networks (WMAN) connect multiple WLANs and provide a coverage ranging from a few blocks within the city to the entire city. And finally, cellular networks provide communication among cellular phones or mobile phones. In this paper, we study WLAN, AHN and WSN because these networks are more commonly used to carry critical information and the focus of the attention of the academic literature is on these networks.

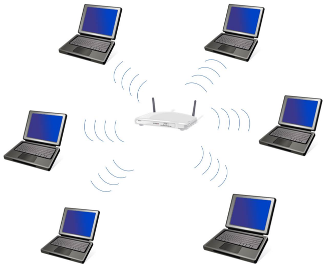


Figure 1: Wireless LAN (adapted from [89])

Even though wireless networks are easy to use, they have been exposed to security threats, because use of air as a medium to transmit data has made wireless networks susceptible to jamming attacks. A jamming attack is the transmission of radio signals that disrupt communications by decreasing the Signal-to-Inference-plus-Noise ratio (SINR) Berg [14]. SINR is the ratio of the signal power to the sum of the interference power from other interfering signals and noise power. A ratio greater than 1 indicates the desirable state of more signal than noise. A jamming device, tuned to the same frequency as the opponent's receiving equipment and with the same type of modulation, can, with enough power, override any signal at the receiver. Wireless signal jamming devices are most often used to interfere with wireless networks, a type of denial of service (DoS) attack. DoS attacks deny legitimate users sending data because of the illegitimate users presence. Advanced and more expensive jamming devices may jam satellite communications. A wireless signal jamming device can be used to stop transmission temporarily and short out or turn off the power of device or units like radios, televisions, microwaves, or any unit that receives electrical signals to operate.

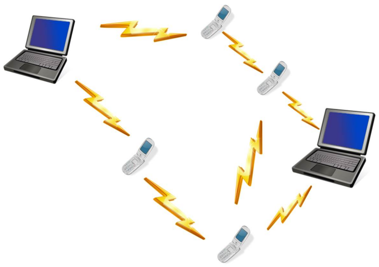


Figure 2: Wireless Ad Hoc Network (adapted from [89])

The internal function of a wireless communication system is divided into the following abstract layers, each having a specific function. The abstract layers are:

1. *Physical Layer* [61, 92]*:* The transmission and reception of data via a physical connection like cables,

fibers, wires, or air among devices on the network is managed by the physical layer; in wireless networks, the binary data among computers is translated into electrical signals and uses radio frequency to send and receive data. Radio jamming attacks can impact the physical layer.

2. *Data Link Layer* [61, 92]*:* Responsible for segmenting the data packets sent by the network layer to frames that can be sent by the physical layer and is responsible for communication between the network layer and the physical layer . The formatting of frames of data sent and error checking are the additional responsibilities of this layer. A sublayer which is a part of the data link layer and is responsible for moving data packets to and from one node to another across a shared channel is the Medium Access Control (MAC) layer. A channel in a wireless network is the frequency at which nodes send their data. Another, responsibility of the MAC sublayer is to ensure that the signal sent from different nodes across the same channel do not collide. This layer is susceptible to much more sophisticated jamming and energy efficient jamming than physical layer jamming attacks.
3. *Network Layer*[61, 92]*:* Links between the transportation layer and the data link layer and also responsible for figuring out the network topology, assigning address, and routing the data.
4. *Transportation Layer* [61, 92]*:* Responsible for reliable data transfer and recovers any lost data, retransmits data, and provides data encryption.
5. *Application Layer* [61, 92]*:* Defines the specifications of the data requested by the end user in the network.

Five abstract layers mentioned above are arranged in a hierarchy starting from the *physical layer* at the bottom to the *application layer* on top. Data packets are sometimes sent to the destination via several intermediate nodes. Mesh networking is a type of network topology where each node must not only capture and disseminate its own data, but also serve as a relay for other nodes and collaborate to propagate the data in the network. A wireless mesh network is a communications network made up of radio nodes in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers, and gateways. The mesh clients are often laptops, cellphones and other wireless devices, and the mesh routers forward traffic to and from the gateways which may, but do not need to, connect to the Internet.

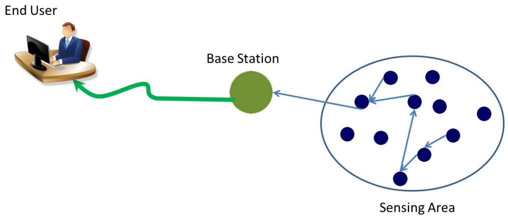


Figure 3: Wireless Sensor Network (adapted from [89])

1.2. *Definition of game theory*

Jamming attacks on wireless networks have been widely studied by researchers, and different solution approaches have been proposed for this attack. Of the methods proposed to solve the jamming problem, game theoretical approaches are increasingly being used by researchers. Game theory is a study of strategic decision making, or "the study of mathematical models of conflict and cooperation between intelligent rational decision-makers"[62]. To be fully defined, a game must specify the following elements: the players of the game, the information and actions available to each player at each decision point, and the payoffs for each outcome. A game theorist typically uses these elements, along with a choice solution concept, to deduce a set of equilibrium strategies for each player such that, when these strategies are employed, no player can profit by unilaterally deviating from their strategy, the Nash equilibrium. Different varieties of games include the non-zero-sum game, zero-sum game, cooperative and non-cooperative games. Among these, researchers have widely applied zero-sum games to the jamming problem. A zero-sum game is a mathematical interpretation of a situation in which a participant's gain in payoff is exactly equal to the loss in the utility of the other participant, and vice-versa. If the total gains of the participants are added up and the total losses subtracted, the sum will be zero. In the literature there are many studies in finding the Nash equilibrium for a jamming game between the attacker and defender with each trying to increase and decrease the throughput respectively, but researchers have previously concentrated on single channel networks with only one communication frequency among network nodes.

1.3. Related literature and motivation

This section briefly discusses some of the survey papers available in the jamming attack literature. Pelechrinis et al. [67] survey different DoS jamming attacks papers. They discuss intelligent jamming attacks with different objectives, such as *jamming gain, targeted jamming,* and *reduced probability of detection.* They also discuss jamming efficiency metrics like *packet delivery ratio, packet send ratio,* and *connectivity index.* Young et al. [105] present the different papers that deal with different types of jammers like *constant jammers, random jammers* etc., and they compare the adversarial models presented. A survey on different game theoretic classification of the problems on network security as a whole is presented in Roy et al. [74]. They provide a taxonomy for classifying the different game theoretic approaches listed in the literature. Mpitziopoulos et al. [61] provide a survey on the different attack countermeasure strategies for WSNs in literature. Along with presenting the different papers in the literature, they also provide a taxonomy to distinguish the countermeasure schemes. The taxonomy divides the different countermeasures as (i) detection techniques, (ii) proactive countermeasures, (iii) reactive countermeasures, and (iv) mobile agent countermeasures. These survey papers are restricted to one type of wireless network or give a general overview of the types of attack and defense strategies, but they do not provide a clear picture of the types of attacks and the defense strategies employed.

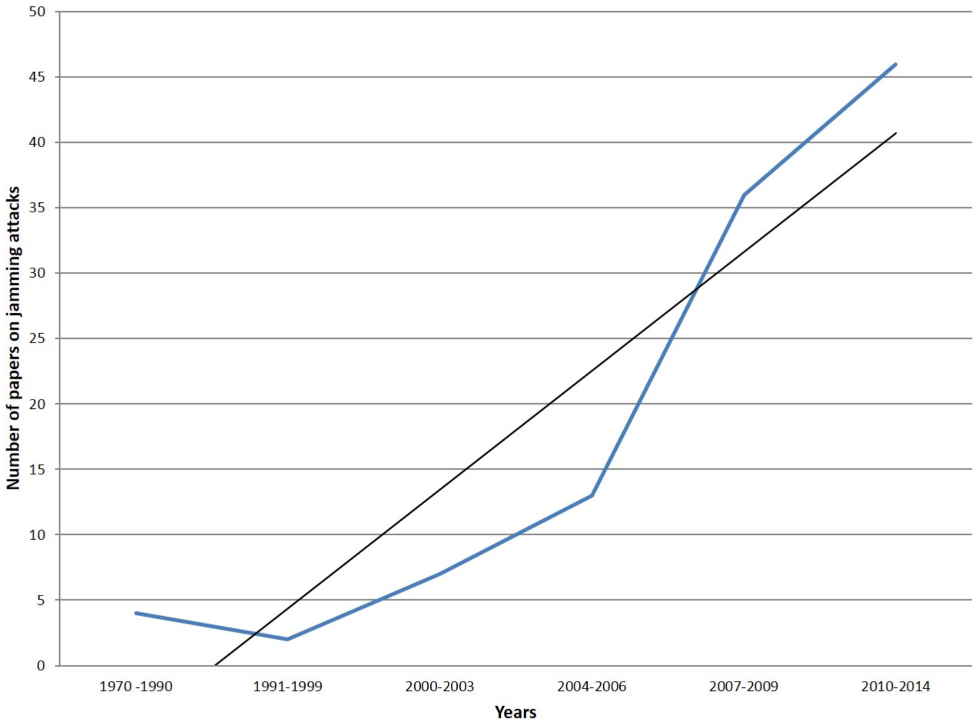


Figure 4: Publications from 1970 to 2014.

To the best of our knowledge, Commander et al. [23] is the only study in the operations research (OR) literature that examines physically placing a jamming device in a strategic location to cause maximum damage. The authors solve for the jamming device placement but do not try to find the best (X, Y) coordinates, rather, they choose from a set of available discrete locations of the jamming device and assume that a jamming device can jam all the channels between two nodes. Increased usage of wireless networks and their applications in military and critical time-sensitive environments has led researchers to find ways to make the wireless networks more reliable. Jamming attacks have gained more attention from researchers than other types of attacks.

Figure 4 shows an increase in the number of papers published in the literature in the years 2010-2014. However, there are only a few papers that survey the literature available on jamming attacks. For instance Young and Boutaba [105] and Pelechrinis et al. [67] each develop a survey on different types of jamming attacks, methods to detect jamming attacks, and mechanisms to protect against attacks. Lazos and Krunz [42] survey selective jamming along with detection and protection. Our survey complements the previous surveys by categorizing different jamming attacks and solution methodologies based on the network type (WLAN, AHN, WSN).

1.4. Contribution

The major contribution of this work is to provide a classification scheme for the literature by identifying the different jamming attacks launched by the jammer, different defense, detection and prevention techniques against the jamming attacks and classifying them by the type of wireless networks they mainly affect and the defense against such attacks. After establishing the types of attacks classified by the type of network, the different attack strategies, defense strategies, detection and prevention strategies, and game theoretic strategies described in the literature are surveyed. An analysis of the gaps in the jamming attack literature is provided to better understand the importance of filling the gaps. A goal of this paper is to give the OR community a better understanding of the existing research in wireless network jamming and areas where it can contribute to find better jamming attacks and ways to defend against jamming attacks. This survey also identifies new areas of research in jamming attacks for the OR community.

The rest of the paper is organized as follows : Section 2 provides the classification scheme for the survey, Section 3 provides a simple example of the jamming problem in wireless networks, Section 4.1 discusses the literature available for WLANs. Section 4.2 describes the literature available for WSNs. Section 4.3 describes the literature available for AHNs. Section 4.4 provides a summary and comparison of the results of the various papers discussed in this taxonomy. Finally, Section 5 discusses gaps in the literature and suggests areas for future research, and Section 6 concludes the paper.

2. Boundaries of study and classification scheme

2.1. Boundaries of study

The keywords used to search papers include “jamming,” “anti-jamming,” “wireless networks,” and “game theory.” These keywords were listed in the title, abstract, or body of text of journal articles or conference proceedings published in English. The data bases included in our search were Science Direct, Springer, IEEE libraries, and ACM libraries. We limited the time period of the search to 1980 forward because the first instance of jamming was explored in the literature in 1982.

2.2. Classification scheme

We provide a classification method for a one-stop easy reference for the jamming research available so far. Tables 1 - 3 show the classification schema provided in this paper. There are four major columns: *Papers, Types of Network, Problem Perspective,* and *Methodology. Papers* classifies and groups the papers published by year, with all the papers that fit the search criteria from 1980 to June 2014. *Types of network* further divides into the three wireless network types considered in this work, and each of these network types are further divided into single channel and multichannel networks. *Problem Perspective* further divides into *Attacker, Defender*, *Both,* and *Game Theory.* For example, a paper discussing a new set of jamming attacks would be classified as *Attacker* , and a new anti-jamming or defense mechanism would be *Defender.* Some authors solve both the attacker and defender problem using game theory; these papers are classified as *Both.* The papers that propose a game theoretic approach are classified as *Game Theory. Game Theory* further divides into *Non-Cooperative, Bayesian, Stackelberg,* and *Other* depending on the type of game studied. The fourth major column in the classification is the *Methodology*, and this column further divides into *Protocol Design/Algorithm* and *Mathematical Programming Model.* The papers that provide a protocol design and/or an algorithmic approach are categorized under the column *Protocol Design/Algorithm*, and the papers providing a mathematical programming model come under the *Mathematical Programming Model* column. The x’s in the above described columns are the categories each of the papers at the left fall into.

Table 1: Classification scheme

Papers	Types of network						Problem Perspective							Methodology	
	WLAN		WSN		AHN					Game theory					
	Single Channel	Multi Channel	Single Channel	Multi Channel	Single Channel	Multi Channel	Attacker	Defender	Both	Non-Cooperative	Bayesian	Stackelberg	Other	Protocol Design/Algorithm	Mathematical Programming Model
2010-2014															
Vadlamani et al. [90]						x			x					x	x
Yang et al. [104]					x	x			x			x			x
Wang et al. [91]			x					x						x	x
Liu et al. [54]		x						x						x	
Li and Dai [46]				x		x		x						x	
Zhang et al. [108]				x		x		x						x	
Chen and Leneutre [19]	x								x				x		x
Liu et al. [50]			x					x						x	
Liu et al. [56]			x					x						x	
Sagduyu et al. [78]	x	x							x	x					x
Sagduyu et al. [79]	x								x		x				x
Altman et al. [9]	x								x				x		x
Garnaev et al. [28]	x								x						x
Wang and Wyglinski [92]	x								x					x	
Xu et al. [103]				x					x	x					x
Liu et al. [49]	x								x			x			x
Clark et al. [22]			x						x	x		x		x	x
Wilhelm et al. [93]	x						x							x	
Zhu et al. [111]			x						x	x					x
Lu et al. [57]	x								x				x	x	
DeBruhl and Tague [24]	x								x				x		x
Liu and Ning [55]				x				x						x	
Hanawal and Altman [30]					x				x				x		x
Richa et al. [73]	x							x						x	
Lee et al. [45]			x				x							x	
Lee et al. [44]			x											x	
Kim et al. [37]		x					x							x	
2007-2009															
Commander et al. [23]					x		x							x	
Altman et al. [8]	x								x				x		x
Sagduyu and Ephremides [80]	x								x	x					x
Sagduyu et al. [77]	x								x	x	x				x
Sagduyu and Ephremides [81]	x								x	x					x

Table 2: Classification scheme

Papers	Types of network						Problem Perspective							Methodology	
	WLAN		WSN		AHN					Game Theory					
	Single Channel	Multi Channel	Single Channel	Multi Channel	Single Channel	Multi Channel	Attacker	Defender	Both	Non-Cooperative	Bayesian	Stackelberg	Other	Protocol Design/ Algorithm	Mathematical Programming Model
Altman et al. [6]	x								x				x		x
Pelechrinis et al. [68]		x							x				x		x
Theodorakopoulos and Baras [85]	x								x				x		x
Xu et al. [101]	x							x						x	
Dong et al. [27]		x						x						x	
Chiang and Hu [21]	x							x						x	
Islam et al. [32]			x					x						x	
Zhang et al. [109]					x				x					x	
Çakiroğlu and Özcerit [17]			x					x						x	
Khattab et al. [36]		x						x						x	
Lazos et al. [43]						x			x					x	
Khattab et al. [35]		x						x						x	
Krikidis et al. [39]			x					x						x	
Navda et al. [63]		x						x						x	
Alnifie and Simon [4]				x				x						x	
Chan et al. [18]		x						x						x	
Xu et al. [100]				x				x						x	
Chiang and Hu [20]		x						x						x	
Wood et al. [96]				x				x						x	
Dolev et al. [26]		x						x						x	
Xu [98]	x							x						x	
Liu et al. [52]		x							x	x					x
Wu et al. [97]		x							x				x		x
Tague et al. [84]		x					x								x
2004-2006															
Sagduyu et al. [76]	x								x	x					x
Liu et al. [53]					x				x		x				x
Kashyap et al. [34]		x							x	x					x
Shafiee and Ulukus [82]	x								x	x					x
Alpcan and Basar [5]	x								x	x					x
Noubir [64]					x			x						x	
Law et al. [41]			x				x							x	

Table 3: Classification scheme

Papers	Types of network						Problem Perspective							Methodology	
	WLAN		WSN		AHN					Game Theory					
	Single Channel	Multi Channel	Single Channel	Multi Channel	Single Channel	Multi Channel	Attacker	Defender	Both	Non-Cooperative	Bayesian	Stackelberg	Other	Protocol Design/ Algorithm	Mathematical Programming Model
Xu et al. [102]	x								x					x	
Brown et al. [15]					x		x							x	
Xu et al. [99]				x					x					x	
Pathan et al. [66]			x						x					x	
Thuente and Acharya [86]	x						x							x	
Acharya and Thuente [2]	x						x							x	
2000-2003															
Agarwal et al. [3]					x			x						x	
Wood and Stankovic [94]			x						x					x	
Maxim and Pollino [59]	x						x							x	
Mallik et al. [58]	x								x				x		x
Wood et al. [95]			x					x						x	
1980-1999															
Pronios and Polydoros [70]	x								x					x	
Medard [60]	x						x							x	
Zander [106]	x								x				x		x

3. Example of wireless network jamming problem

Military strategists are always looking for better ways to improve their force's effectiveness while reducing the number of causalities. In any adversarial situation, the attacker aims to neutralize the military's communications. The military would like to make sure it can maintain communication by working around the adversaries' attempts to neutralize communication. In a war situation, as it is not possible to have infrastructure for communication, the military needs to setup an AHN. In a wireless AHN, each node transmits data using one channel from a number of available channels. The jamming device seeks to choose a location such that, by choosing the same channel nodes are using, the data is blocked from successful transmission. The main aim of the jamming device is to en-sure that the nodes cannot use the network, and on the other hand nodes try to maximize the usage of the network. Both the jamming device and the node are playing a game. Think of it as a two player game, and the players are attacker/terrorist and defender/military. Figure 5 shows the network consisting of six nodes (n1-n6) and one jamming device (j1). Three communication channels of different frequencies, continuous, dotted, and dashed line, exist between each node. A channel is not a physical cable or connection, but a frequency at which the nodes communicate through air. Figure 5, assumes that nodes 5 and 6 are communicating using the 2.41 GHz (dotted) frequency channel. The attacker chooses it's location and chooses a frequency; in this case, it chooses 2.41 GHz (dotted), which is the same as the nodes. The communication channel between nodes 5 and 6 is in the radius of the jamming device's power range. Since the jammer chose a location with the available power and a frequency on which node 5 and 6 were communicating, the jamming is successful.

Figure 5: Example of jamming in a network

In the sections below we introduce the readers to some of most commonly used attack and defense strategies studied in literature. These lists of attack and defense strategies will help reader understand the 4 section better, as most of the papers discussed in this section use one more of these attack and defense strategies.

3.1. Types of jamming strategies

There are four types of jamming strategies most commonly studied in literature. In this section, we briefly discuss these different jamming strategies [61, 67, 92, 102]:

- ***Constant Jammer:*** Constant jammers continuously emit electromagnetic waves or radio signals or random sequence of bits that interfere with the legitimate transmission of the network. In the presence of a constant jammer the transmission channel of the legitimate network appears busy therefore disallowing legitimate transmission. The disadvantage of constant jammer is that, the continuous emission of signals drains the energy fast and require high amount of power.

- ***Deceptive Jammer:*** Deceptive jammer like the constant jammer emits signals continuously, but unlike constant jammers does not emit random bit sequence, but emits a legitimate bit sequence which gives the network an impression of presence of a legitimate node. This impersonation makes deceptive jammers more effective than constant jammers.

- ***Random Jammer:*** Unlike constant and deceptive jammers random jammer conserves energy by alternating between random jamming and sleep states. Random jammers do not use energy in the sleep state therefore, reducing power consumption.
- ***Reactive Jammer:*** Reactive jammers like the random jammers conserve power by not emitting signals continuously. Reactive jammers listen to the transmission channel and react by emitting signals in the presence of data transfer. The amount of power required to listen to a channel is much less compared to the power required for jamming.

3.2. Types of defense against jamming attacks

In this section we briefly describe some of the most common defense strategies against jamming attacks found in literature.

- ***Transmission power:*** The use of low transmission power can be a defense strategy against jamming attacks in that, with the use of low transmission power makes it difficult for the jamming devices to detect legitimate transmission. However, use of low power can undesirably decrease SINR. It is important for the nodes in the network to vary their transmission power.
- ***Frequency Hopping Spread Spectrum (FHSS):*** Spread Spectrum (SS) a modulation technique spreads data across the entire band of the transmission channel although the entire band of the transmission channel is not required. This spreading of data in the entire channel band ensures that the transmitted signal is resistant to interference. FHSS a spread spectrum technique evades jamming by rapidly switching between different transmission channel frequencies. The channel switching algorithm is shared between the sender and receiver prior to the actual data transmission. This technique works as long as the shared algorithm is kept secret from the attacker.
- ***Directional Antennas:*** Jamming attacks can be evaded by using directional antennas. Directional antennas can transmit and receive data only in one direction, unlike traditional omni directional antennas, which can transmit and receive data from all directions, making omni directional antennas an easy target for the jammers. But, with directional antennas, the jammer has to be placed in the same direction of the directional antenna for it to successfully jam the signal. Sectored antennas a special type of directional antennas have proved to help improve the connectivity of wireless networks and help combat jamming attacks. Sectored antennas, like directional antennas, serve only in one direction and more specifically at an angle forming a geometric sector shaped radiation pattern.
- ***Channel Surfing:*** Channel surfing like FHSS evades jamming by quickly switching between channels. But, the difference between the two is that, FHSS, unlike, channel surfing requires specialized antennas for transmitting and receiving signals. The major difference between the two is that in channel surfing sharing of a secret algorithm between the sender and receiver is not required.

4. Discussion of literature

The first knowledge of jamming attack dates back to when it was used against military radios. The first countries to engage in jamming were Germany and Russia. The first time jamming attacks were used during a war situation was during World War II, when radio operators misled pilots by feeding them false instructions in their own language. The operators who started such an attack were known by the code name Raven, which was soon changed to Crow. During World War II radars were jammed, which was considered an invention at that time. Jamming attacks on foreign radio broadcasts stations were more common during tense international relations and wars, and they prevented listening to the radio transmission of enemy countries. The jamming of foreign radio signals could be avoided by changing the transmission frequency or by the power of transmission [61]. When jamming attacks were used for the first time, a new technology SS (discussed above) was invented by the military to cope.

SS received attention from early researchers after World War II . Although jamming attacks were popular during the war, the word “jamming” was used for the first time by Basar and Basar [12] in 1982 in “*Robust linear coding in continuous-time communication systems in the presence of jamming and with noisy side information at the decode*r.” The authors in [70] study dynamic jamming in 1988. The authors study the throughput/delay performance of the Slotted Aloha type network under dynamic jamming. They use Markovian decision model to find the optimal decision rules for the jamming device. The authors assume that the jamming is the ON-OFF type and has a finite amount of power. Zenko [107] provide uses and application of SS, and the authors in [1] analyze SS technology. Medard [60] develops an information-theoretic approach. The authors in [106] study the multi-hop packet radio networks in the presence of active interference. They also consider power constraints for both the jamming device and the network nodes. The authors formulate the problem as a two player constant sum game.

The jamming problem has been studied widely in many wireless network settings, including wireless LAN networks [13, 29, 40], sensor networks [15, 47, 102], and multi-hop networks [85, 106]. Other general wireless networks have also received attention [7, 10, 16, 34, 58, 80]. Researchers assume the location of a jamming device and the effect of the locating a jamming device to solve the problem. But in [23] the authors solve the jamming device location problem, but they assume the effect a jamming device has on the wireless network to decide the location of the jamming device. The readers are recommended to read the tutorial by Vadlamani et al. [89] to better understand jamming attacks and their defense mechanism available in literature.

4.1. Wireless Local Area Network (WLAN)

4.1.1. Single Channel

In this section, we further classify the literature as below:

A. Attack Strategies

Thuente and Acharya [87] show that normal jamming attacks, where the attacker constantly or periodically emits signals to jam the network, are inefficient in terms of energy consumption, and introduce intelligent jamming attacks that enables the jamming attacker to corrupt the Clear To Send (CTS), Request To Send (RTS), and Acknowledge (ACK) packets. Acharya and Thuente [2] extend the work in Thuente and Acharya [87] to propose another intelligent attacking strategy called the fake RTS jamming attack. They also propose countermeasures to prevent such attacks as well as methods to overcome the proposed countermeasures. Wilhelm et al. [93] develop a software-based reactive jamming attack and show that reactive jamming should be considered a real threat, and new defense mechanisms must be developed to cope with such attacks. The jamming attack as a DoS attack in wireless communication is discussed by Maxim and Pollino [59]. The authors classify jamming attacks as *client jamming* or *base station jamming.* In client jamming, a mischievous client takes over and impersonates the legitimate client. The mischievous client can even jam the network so that the legitimate client cannot use the network. In base station jamming attacks the jamming device impersonates the legitimate base station or deprives the client of service. Pronios and Polydoros [70] study the throughput/delay performance of the Slotted Aloha type network under dynamic jamming using a Markovian decision model to find the optimal decision rules for the jamming device. The authors assume that the jamming is the ON-OFF type and has a finite amount of power. Since, the jammer assumed is of the ON-OFF type the life of the jamming device is longer, as the power is not consumed when the jamming device is in the OFF state. An information-theoretic approach is developed in Medard [60]. Finally, Xu et al. [102] studied jamming attack from both the attackers and defenders point of view. They provide four different models and show the problems associated with an effective attack. They also provide different measures that help the network to detect the attack. The authors find that signal strength and carrier sensing time are not enough to determine whether a poor connection is due to jamming or because of the mobility of the nodes. They also determine which measures give a better understanding about the poor quality of network’s connection.

B. Detection and Prevention Strategies

Xu et al. [102] introduce two methods of detecting jamming attack: 1) Packet Send Ratio (PSR) and 2) Packet Delivery Ratio (PDR). PSR is the ratio of the number of packet sent to the number of packets intended to be sent. If the number of packet sent is less than the number of packets intended to be sent, it can indicate the presence of a jamming device. PDR is the ratio of the number of received packets that pass the completeness of data to the number of packets actually received. If only a few of the received packets pass the completeness check, it can indicate the presence of a jamming device. These PSR and PDR methods of detecting jamming attacks opened new gates for research on jamming attacks. Wang and Wyglinski [92] combine some of the existing approaches such as PSR and PDR to detect jamming attacks and measure the PSR and PDR to evaluate the accuracy of their approach. The authors use a ns-2 simulation platform and the results obtained confirm that the approach of combining existing jamming detection approaches increases the accuracy of detecting jamming attacks.

C. Defense Strategies

Richa et al. [73] propose a local medium access control protocol called, JADE, that can protect a multi-hop wireless network with a single channel against an adaptive jamming device which can adapt its attack for its benefit . Here, the authors model the interference and transmission as a unit disk graph. The jamming strategies change from node to node and, hence, make it difficult to defend. The results of this work shows that JADE achieves an asymptotically optimal throughput. An anti-jamming strategy based on creating a timing channel: an extra channel overlaying the already existing physical and link layer channel, between users of a network in the presence of jamming attack, is developed by Xu et al. [101]. Studies by Pronios and Polydoros [70], Medard [60], and Xu et al. [102] are discussed in 4.1.1. Chiang and Hu [21] discuss a binary key tree and a dynamic tree-remerging method to evade broadcast jamming attacks. Finally, Xu [98] studies the issues associated with controlling the transmission power for improving the successful transmission of data under a jamming attack.

D. Game Theoretic Strategies

Chen and Leneutre [19] provide a game theoretic framework for the jamming attacks in wireless networks. The authors provide a defense strategy to fight the jamming device actively by draining the jamming device of energy. The authors also show that their strategy eliminates undesired equilibrium and increased the energy consumption at the jamming device without negatively affecting the performance of the network. Liu et al. [49] propose a dynamic jamming attack in which the attacker dynamically adjusts the jamming period, to increase the attacker's utility. The authors provide a method where the network will change the re-transmission mechanism to defend against the jamming attacks. The authors modeled the problem as a Stackelberg game and derive the Nash equilibrium.

Sagduyu et al. [79] deal with jamming games in the MAC layer of the wireless network. They assume that each of the nodes in that network knows only its type, i.e., a selfish user type or a malicious user type that tries to jam the communication channel. The authors model the jamming game as a multi-stage two-player Bayesian game. The action set of a node is a set of transmission probabilities to choose from at random. The utility function of a selfish user is the difference of its reward function, which is an increasing function of the SINR, and the energy cost function, which is an increasing function of the node's own power. The utility function of a malicious node is the difference of its reward function and its energy cost function. The reward function of the malicious user is the opposite of the function of the other user if that user is a selfish user, and zero if the other user is a malicious node. The authors also consider the Bayesian Nash equilibrium as the expected strategies of the nodes. Sagduyu et al. [77] present a game-theoretic model for the jamming problem at the MAC layer of the wireless network. They present different models based on power control and random access. They also derive the Nash equilibrium strategies depending on the degree of the type of uncertainty. Throughput rewards, transmission energy cost, and malicious attack incentives are used as performance measures. Random access games are studied in Sagduyu and Ephremides [80], and the jamming device and transmitter balance the throughput rewards and energy cost. Sagduyu and Ephremides [81] and [6] introduced different energy objectives based on power control with different utility functions, depending on throughput rewards and energy costs. Sagduyu et al. [76] explore the effects of dynamic traffic on jamming attacks in a power controlled MAC, i.e., each transmitter chooses its power to transmit. MAC channels with two users in the presence of a jamming device is studied by Shafiee and Ulukus [82].

The effects of random channels were studied in Altman et al. [9] for jamming games based on the throughput rewards and energy costs. Garnaev et al. [28] discuss the impacts of incomplete information related to fading channel gains on transmission parameters. For the purpose of solving this problem, the authors consider the Orthogonal Frequency Division Multiplexing (OFDM) network with transmitters and jamming devices. A Bayesian approach is presented by the authors and SINR is the metric used to optimize the problem. The authors show that incomplete information about the jamming device channel gains leads to utilization of same channels by different jamming devices under the equilibrium condition. The study also shows that, under the equilibrium conditions, incomplete information about the transmitter leads to users sharing channels. The authors provide a closed form expression for the equilibrium. Altman et al. [8] studies how the increase in the number of jamming devices impacts the transmission game. The objective function of the node they consider is the SINR. The authors also analyze a zero-sum game scenario and an optimization scenario to show that the jamming device equalizes the quality of the best sub carrier.

Lu et al. [57] model jamming attacks as a gambler, and a new performance metric message invalidation ratio is introduced for time critical traffic networks. A two player game theoretic framework for an adaptive jamming attack and anti-jamming defense is modeled by DeBruhl and Tague [24]. Zander [106] study multi-hop packet radio networks in the presence of active interference. They also consider power constraints for both the jamming device and the network nodes, and the authors formulate the problem as a two player constant sum game. Multi-hop networks with packet forwarding are studied in [85]. From a game theoretic prospective of jamming in wireless networks, the transmission strategies may also include randomized power selection; see Mallik et al. [58]. The jamming problem that Alpcan and Basar [5] study is an intrusion detection problem. Sagduyu et al. [78] discussed in Section 4.1.2 study both single channel and multichannel WLANs.

A total of 31 papers provided in this study classified as WLAN single channel are discussed in this section; including 7 papers classified as *Attack Strategies,* 2 papers as *Detection and Prevention Strategies,* 7 papers as *Defense Strategies*, and 19 papers as *Game Theoretic Strategies.*

4.1.2. Multichannel

In this section, we further classify the literature as below:

A. Attack Strategies

To the best of our knowledge, among the papers in WLAN multichannel networks, only Tague et al. [84] and Kim et al. [37] study jamming problem from an attackers perspective. Tague et al. [84] were the first to introduce the problem of flow-jamming attack and model flow-jamming attack as a linear programming model. Kim et al. [37] provide stochastic search algorithms like iterative improvement, simulated annealing, and genetic algorithm and provide a stochastic optimization approach for flow-jamming attacks in multi-channel wireless networks. Flow is defined as the data that is sent on a path between two nodes in a network. So, flow-jamming attack is an intelligent attack where the jamming devices are located in such a way, that the amount of flow jammed in the network is maximized and at the same time the power used to jam the flow is minimum. In a flow-jamming attack, the attacker has knowledge about the network layer and hence, is different from general jamming attacks. Since, there are not many papers discussing the different types of attack strategies in multichannel WLAN, it is important that more research is done in this area.

B. Detection and Prevention Strategies

To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with detection and prevention strategies for multichannel WLAN and more research in this areas is needed.

C. Defense Strategies

Liu et al. [54] propose a two-slot cooperative relay scheme to maximize the secrecy rate in a one source, one destination, on eavesdropper, and multiple decode-and-forward relays wireless network. In the first slot the source and destination work together to jam the eavesdropper. In the second slot one optimally selected node transmits the signal from the source and cooperates with the source to jam the eavesdropper without causing interference at the destination. Dong et al. [27] consider cooperative jamming in a multiple antenna scenario as well as methods to maximize the system's secrecy subject to a transmission power constraint. Reactive and proactive channel hopping techniques to evade jamming are studied in Khattab et al. [35]. Navda et al. [63] study channel hopping in 802.11 networks. Chan et al. [18] discuss the jamming of broadcast control channels in the presence not only in external jamming attacks, but also in relation to an internal traitor who has information about the channels in the network. Chiang and Hu [20] discuss a binary code tree technique which works with any SS communication technology. Khattab et al. [36] introduce the problem of maximizing network goodput under jamming attacks through a combination of channel hopping and error correction coding. The gossip problem considered as jamming problems in wireless multichannel networks is presented by Dolev et al. [26], and a deterministic algorithm based on Turan's theorem is developed.

From our taxonomy, it is apparent that, there is not one defense mechanism that works for all the type of jamming attacks in multichannel WLAN. Hence, it there is not a common technique that is better than the other. Finding a metric or standard to measure the effectiveness of one defense mechanism over the other is important. Mutlichannel WLAN provide an advantage to both the attacker and defender, as both can use the available channels to their advantage. And with the increase in the use of multichannel networks, it becomes important that there is more research in this area. To the best of our knowledge, not all the defense strategies developed for a single channel WLAN will work for multichannel WLAN and vice-versa. Hence, there needs to be more research in finding defense mechanisms that will work for both single channel and multichannel networks.

D. Game Theoretic Strategies

Sagduyu et al. [78] explore a non-cooperative game between a jamming device and a transmitter in which both choose their transmission probabilities to access the collision channels with random packet capture. They consider random errors in the queue state for the jamming device and add a channel sensing capability to the jamming device. They provide the Nash Equilibrium with packet delay and energy constraints. The authors extend the game to multiple transmitters, jamming devices, sub-channels, and channel access points. A non-cooperative game is proposed for Multiple Input Multiple Output (MIMO) fading channels in Kashyap et al. [34]. Pelechrinis et al. [68] explore a system with multiple channels, where the interactions of the transmitter and jamming device are formulated as game transmitting randomly over multiple channels. SPREAD, a multilayer mechanism hopping technique discussed in [52] based on using the frequency hopping technique for preventing jamming as a DoS attack. Liu et al. [52] formulate SPREAD as a non-cooperative game. Finally, a multi-path routing game-theoretic framework to evade jamming attack is proposed in Wu et al. [97].

A total of 14 papers provided in this study classified as WLAN multichannel are discussed in this section; including 1 paper classified as *Attack Strategies,* 0 papers as *Detection and Prevention Strategies,* 8 papers as *Defense Strategies*, and 6 papers as *Game Theoretic Strategies.*

4.2. Wireless Sensor Network (WSN)

4.2.1. Single Channel

In this section, we further classify the literature as below:

A. Attack Strategies

Lee et al. [44] derive the optimum relay amplifying matrices for wireless networks and introduce the topic of node geometry in wireless networks. The authors conclude that node geometry can have an impact on the network. They use bit error rate to measure the impact on the network. Lee et al. [45] consider wireless relay networks under jamming attacks, and node geometry with received power constraints. The authors consider minimum square error and amplify forward relay strategy, and calculate the diagonal relay amplifying matrix, to minimize the mean square error between the received signal and the transmitted signal. Law et al. [41] develop jamming attacks that can work on encrypted packets. They expose the shortcomings of semantics of the data link layer and show that some of the MAC protocols are susceptible to a jamming attacks.

B. Detection and Prevention Strategies

The ideal way to stop a jamming attack is to detect the location of the jamming device, although this may not be feasible. However, finding the device would be would be very cost effective as compared to other methods of designing protocols for escaping jamming attacks. Wood et al. [95] provide a mapping detection approach to provide feedback to the base station about further jamming areas and power management strategies for the nodes that are under jamming attack or within the range of the jamming device. The protocol consists of two parts: 1) the jamming detection module and 2) a mapping module. The jamming detection module monitors radio and MAC layers and then applies heuristics to determine whether the node is jammed or not. The mapping module groups the nodes that are jammed, based on the information received from the jamming detection module. Liu et al. [56] address the problem of locating a jamming device in a wireless network. They propose a least square (LSQ) based localization algorithm that estimates the location of the jamming device by using the changes in neighboring nodes caused by the device. The approach used by the authors does not depend on the signal strength in the jammed area, nor does it depend on delivering information out of the jammed area. They also study the LSQ based algorithm in the shadowing model. The authors show that the LSQ method significantly reduces the computational cost of locating the jamming device. Liu et al. [50] propose a method to find the location of multiple jamming devices in a network even when the jamming areas overlap. The method proposed by the authors, unlike other methods, does not depend on the signal strength to find the position, but uses distributed network communication instead. Islam et al. [32] study optimal DoS attack detection sensor placement problem to minimize the number of sensor required to detect the DoS attack and the cost for locating such sensors. Finally, in Çakiroğlu and Özcerit [17], two detection mechanisms distinguish between legitimate and adversary nodes under a DoS attack are discussed.

C. Defense Strategies

Wang et al. [91] propose an optimal relay and jammer selection scheme with power allocation to maximize the secrecy rate subject to a total transmission power constraint. Secrecy rate is defined as the rate at which the data in the network is transmitted without being leaked to an eavesdropper. In this paper, the authors use jamming attack to attack the existing eavesdroppers in the network. Wood and Stankovic [94] study DoS attacks and various types of defenses and their drawbacks against such attacks in WSN. The authors provide a classification of different type of DoS attacks and their known defense methods in the different abstract layers of the Internet. The authors study two different protocols that are used by WSNs that did not consider security initially. From the examples provided by the authors, they conclude that considering security during protocol design is essential. The authors describe jamming attacks as one of the major attacks on the physical layer, and the jamming attack is very effective if the network is using a single frequency. A constant jamming attack will not allow the nodes to communicate if they are under attack, but it would not last long because the jamming device might use all its energy. SS is good for defending jamming attacks but it has high power and cost requirements; thus, the authors conclude that SS is not efficient in the case of sensors networks. The other defense strategy discussed is that the nodes should transmit data when the jamming device is not transmitting and using high power. But, this defense is possible only if the attack is intermittent. Pathan et al. [66] discuss the holistic view of the security threats faced by the WSN and available defense strategies such as, secure routing of packets under an attack and power management schemes for extending the life of the of network under an attack. Finally, the selection of relay nodes that increase the security of the WSN by protecting the destination node from eavesdropping and jamming attack is discussed in [39]. The authors provide a hybrid technique to switch between jamming and non-jamming relay scheme, where an eavesdropper is intelligently attacked by the jammer without corrupting the data being sent through the network, which is an improvement on the paper by Wang et al. [91], where in an attempt to jam the eavesdropper the data could be corrupted.

D. Game Theoretic Strategies

Clark et al. [22] study the proactive defense technique against jamming attacks in multi-hop relay networks. The network nodes send a deceptive flow along a routing path, so the attacker will use all its resources on the deceptive flow, which will reduce the impact of jamming on the real traffic. This strategy, although good against jamming attacks, requires efficient energy usage by the source nodes in the network. The authors consider two types of source nodes, namely: selfish node and altruistic node. The selfish node aims to maximize its energy consumption efficiency while the altruistic node teams up with other source to improve overall energy efficiency. The authors provide a two stage non-cooperative game with Stackelberg equilibrium model for both the selfish and altruistic nodes versus the jamming attacker. Zhu et al. [111] provide a non-cooperative game theoretic model played between the network node and a malicious node. The aim of the network nodes is to maximize the network capacity by choosing a relay node, keeping in mind the interference from other network nodes and the presence of a malicious node. While the malicious nodes aims to minimize capacity of the network and also choose either to be a jamming node or an eavesdropper to improve the payoff.

A total of 14 papers provided in this study classified as WSN single channel are discussed in this section; including 3 papers classified as *Attack Strategies,* 5 papers as *Detection and Prevention Strategies,* 4 papers as *Defense Strategies*, and 2 papers as *Game Theoretic Strategies.*

4.2.2. Multichannel

In this section, we further classify the literature as below:

A. Attack Strategies

To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with attack strategies for multichannel WSN and more research in this areas is needed.

B. Detection and Prevention Strategies

To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with detection and prevention strategies for multichannel WSN and more research in this areas is needed.

C. Defense Strategies

Channel surfing is switching between channels or frequencies to avoid jamming by the attacker. Xu et al. [99] propose two different versions of channel surfing methods: coordinated channel switching and spectral multiplexing, both of which combat jamming attacks in multichannel WSNs. Liu and Ning [55] study a new method called BitTrickle, an anti-jamming scheme that allows communication in the presence of a reactive broadband high power jamming device. This wireless scheme exploits the reaction time of a reactive jamming device. The results show that the BitTrickle scheme works better than SS technology because it allows communication under a reactive jamming attack. Li et al. [48] study adaptive anti-jamming techniques in wireless WSNs, in which the sensors can choose the best solution among the defense techniques available . The authors also propose a method where the strengths of several anti-jamming techniques are combined, and the decision of a choosing a defense technique depending on the jamming condition is left to the sensors to decide. MULtichannel Exfiltration PROtocol (MULEPRO), a protocol that rapidly exfiltrate data from a large distributed network, is explored by Alnifie and Simon [4]. In [100] two different channel surfing methods are discussed: one where all the nodes in the networks change their channels and one in which the nodes in the jammed area change their channels to escape jamming. Wood et al. [96] propose DEEJAM , a novel protocol that has four layers of defense 1) frame masking, 2) channel hopping, 3) packet fragmentation, and 4) redundant encoding, that protects the network communication from jamming and reduces the impact of damage caused by jamming attacks. Zhang et al. [108] study and propose a cooperative anti-jamming scheme designed to enhance the quality of the links degraded by jamming. In this scheme legitimate users cooperate among themselves to improve the quality of the links jammed in both WSN and AHNs. Jamming attackers need not be illegitimate users or nodes outside the network. Sometimes, previously legitimate network nodes could change sides and become an attacker, such attackers are called insider attacker. These insider attackers do not reveal their malicious nature to the rest of the network. Finally, Li and Dai [46] investigate the connectivity of a multi-hop multichannel WSN and AHNs network subject to insider jamming attacks. They use uncoordinated frequency hopping technique, where the transmitter and receiver switch channel randomly without the use of a common strategy to choose channels. The authors study the impact on the connectivity of the network when the communication links in the network switch between the normal transmission and uncoordinated frequency hopping transmission when attacked by an insider jamming attack.

D. Game Theoretic Strategies

Xu et al. [103] provide power control methods in their study of a non-cooperative zero-sum game to detect and avoid energy efficient jamming attacks in wireless WSNs . They also model a one stage game between an intrusion detection system and an attacker, and provide a Nash equilibrium for both games.

A total of 9 papers provided in this study classified as WSN multichannel are discussed in this section; including 0 papers as *Attack Strategies*, 0 papers as *Detection and Prevention Strategies,* 8 papers classified as *Defense Strategies,* 1 papers as *Game Theoretic Strategies.*

4.3. Ad hoc Network (AHN)

4.3.1. Single Channel

In this section, we further classify the literature as below:

A. Attack Strategies

Commander et al. [23] study the problem of determining the optimal number and placement for a set of jamming devices in order to neutralize communication on the network. This is known as the Wireless Network Jamming Problem (WNJP). The jamming devices are assumed to have omni-directional antennas. The communication nodes are also assumed to be outfitted with omni-directional antennas and function as both receivers and transmitters. An undirected edge would connect two nodes if they are within a certain communication threshold. The study considers the transmitting nodes which emit radio signals and, correspondingly, the jamming devices which emit electromagnetic waves. The jamming effectiveness of a device depends on the power of its electromagnetic emission, which is assumed to be inversely proportional to the squared distance from the jamming device to the node being jammed. The authors provide an integer programming (IP) model for finding the minimum number of jamming devices needed to ensure a certain threshold is met. Further, they solve the Optimal Network Covering Problem (ONCP): The objective is to minimize the number of jamming devices used while achieving some minimum level of coverage at each node. They also solve the Connectivity Index Problem (CIP): The objective of this formulation of the WNJP is to minimize total jamming cost, subject to a constraint that the connectivity index of each node does not exceed some pre-described level. They consider a deterministic formulation. Instead of finding the connectivity as in the previous variant of the problem, the authors show that it is sufficient to jam some percentage of the total number of nodes in order to acquire effective control over the network. The Value-at-Risk (VaR) and Conditional Value-at-Risk (CVaR) are used to solve CIP. VaR is a measurement and controls the level of risk an individual/group can undertake, and it is used mostly in financial risk analysis. CVaR is a percentile risk measure for estimating and controlling risks in stochastic and uncertain environments [23]. Commander et al. [23] to the best of our knowledge are the first to study and introduce jamming attacks to the OR community. Brown et al. [15] show that in a jamming attack, the jammer can jam a AHN even if the data is encrypted.

B. Detection and Prevention Strategies

To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with detection and prevention strategies for single channel AHN and more research in this areas is needed.

C. Defense Strategies

Noubir [64] studies the problem of maintaining connectivity in a multi-hop AHN. The study introduces a connectivity index, which is the probability that a path exists between two nodes. From the results, the authors show that connectivity can be reduced even with a small number of jamming devices. And as a solution to the connectivity problem, the authors show that using sectored antennas improves the connectivity even in the presence of a high number of jamming devices. A network is said to be connected if there exists at least one path between any two nodes. Agarwal et al. [3] propose methods to reduce the energy consumption of the low power batteries in wireless AHNs. The authors provide a power control loop similar to that found in cellular networks and use it in AHNs. The use group mobility, group communication, terrain blockage models are provided and the jamming attack problem is implicitly added into the terrain blockage model as a moving enemy jamming device in the battlefield and in inclement weather. The power consumption of the network under such blockages (jamming attack) is studied. The power control loop proposed by the authors reduced the energy consumption per transmitted byte by 10-20% and also increased the throughput of the network by 15%. Zhang et al. [109] study a jamming acknowledgment (JACK) attack, and the work explores the weakness of many MAC schemes of wireless networks to transmit an acknowledgment (ACK) from the data receiver to the data sender to announce the successful arrival of a packet. In this attack, the attacker transmit data to block the ACK sent from the data receiver before it reaches the data sender. Since, the data sender does not receive the ACK, the data sender will resend the data and therefore using the available limited power. So, this attack drains the legitimate users battery. The advantages of JACK attack are lower power consumption by the attacker, attack stealthiness, and damage the victim node. The Extended Network Allocation Vector scheme is proposed to combat such a JACK attack in Zhang et al. [109]. In this scheme legitimate users in network extend the time of sending the ACK and so the attacker cannot effectively jam the ACK.

D. Game Theoretic Strategies

Hanawal and Altman [30] study the performance of a mobile AHN in presence of a jamming device. The objective of the jamming device is to degrade the performance of the network, while the objective of the operator is to optimize the network's performance. The authors model this situation as a zero-sum game and define the Nash equilibrium under two cases. In one case, the distance between the receiver and transmitter is fixed, and, in the other, the distance is not fixed. Liu et al. [53] propose a Bayesian game formulation for intrusion detection in wireless AHNs and provide static and dynamic game models. In the static game the defender assumes the type of opponent with a fixed probability. In the dynamic game model developed by the authors, the defender updates his belief about the opponents' type by keeping track of the history of the game. They find a mixed strategy and pure strategy Bayesian Nash equilibrium, and both players try to maximize their payoffs; the attackers' payoff is to maximum damage without being detected, and the defender tries to maximize defending capability while constrained to energy usage. Yang et al. [104] present a Stackelberg game model to study defense against jamming attacks in both single channel and multichannel networks in the presence of a smart jammer, which learns the transmission power of the user and adaptively adjusts its transmission power to maximize the damage.

A total of 8 papers provided in this study classified as AHN single channel are discussed in this section; including 2 papers classified as *Attack Strategies*, 0 papers classified as *Detection and Prevention Strategies,* 3 papers as *Defense Strategies*, and 3 papers as *Game Theoretic Strategies.*

4.3.2. Multichannel

In this section, we classify the literature as defense and game theoretic strategies.

A. Attack Strategies

To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with attack strategies for multichannel AHN and more research in this areas is needed.

B. Detection and Prevention Strategies

To the best of our knowledge, there are no papers in literature within the scope of this survey that deal with detection and prevention strategies for multichannel AHN and more research in this areas is needed.

C. Defense Strategies

Multichannel networks provide higher performance compared to single channel networks and hence there has been an increase in their usage. But, in order increase network throughput most of the important network functions such as channel selection and routing are controlled by sending data over a collaborative channel called the control channel. Lazos et al. [43] address the problem of control channel jamming attacks in multichannel AHNs. A frequency hopping technique, where the communicating nodes do not have a common frequency hopping scheme, is employed to combat such control channel jamming attacks. The papers [46, 108] have been discussed in Section 4.2.2.

D. Game Theoretic Strategies

Vadlamani et al.[90] solve a bi-level model jammer placement problem that accounts for the attacker defender, channel hopping, and Nash equilibrium strategies. In this paper, the authors model the jammer placement problem as a $\min - \max$ problem. The jammer tries to minimize the number of jammers located and at the same time minimize the throughput of the network. The defender tries to solve a max flow problem to maximize the throughput of the network. The attacker and the defender play a mixed strategy channel hopping game. The authors show that, by increasing the number of channels in the network, the throughput of the network increases. If the number of jammers increases, the throughput of the network can be reduced considerably. Yang et al. [104] has been discussed in Section 4.3.1.

A total of 5 papers provided in this study classified as AHN multichannel are discussed in this section; including 0 papers classified as *Attack Strategies,* 0 papers as *Detection and Prevention Strategies,* 3 papers as *Defense Strategies*, and 2 papers as *Game Theoretic Strategies.*

4.4. Summary and Comparison of Results

In this section we will highlight some of the most important insights we derive from this taxonomy. First, it is apparent from the literature related to attack strategies that (see Sections 4.1.1, 4.1.2, 4.2.1, and 4.3.1), there is a multitude of different attack strategies without much commonalities among the strategies. Each of the papers in this area of literature introduce different types of attack strategies. Thus, there is a need for a unifying framework to be developed. Toward this end, we believe that there are several factors that should be fundamental to an attack strategy: power supply available to the jamming device, the rate of power consumption by the jamming device, and the effect of jamming attack on the throughput of the network.

From the literature on attack detection techniques (see Sections 4.1.1 and 4.2.1), we can conclude that, it could be worthwhile to explore ways to combine existing detection techniques to yield higher detection accuracy. Another observation apparent from this taxonomy is that there are not many papers in literature that discuss detection and prevention techniques against jamming attacks (see Sections 4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.3.1, and 4.3.2). Hence, there is also a need for more detection techniques. Of the few detection techniques discussed in literature, currently there is not a way to measure the effectiveness of these techniques. So, developing such a standard or metric to help measure the effectiveness of the detection techniques for jamming attacks in wireless networks is critical. There is currently a shortage of effective prevention techniques in the literature.

As in the case of defense strategies, like the attack strategies, it is clear from the literature that there are many defense strategies (see Sections 4.1.1, 4.1.2, 4.2.2, 4.3.1, and 4.3.2), studied and there is not much in common among the different strategies. The authors introduce different defense mechanisms in each of the papers and there is not a way to find the most commonly studied defense strategy. Among the different defense strategies studied, there is not a metric to measure the effectiveness of these defense strategies. An interested researcher could contribute to the jamming attack literature by providing a combined strategy and a combined metric to measure the effectiveness of defense strategies.

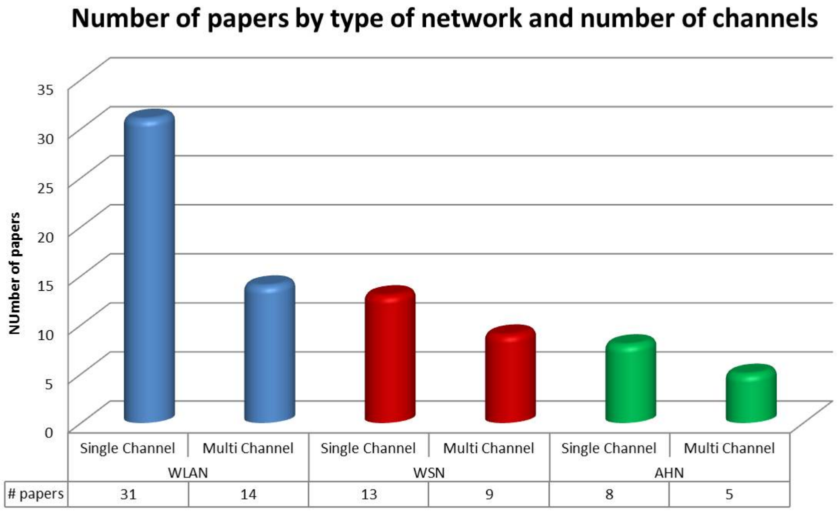
One can see from the taxonomy provided in this paper that many researchers have used game theory as a solution methodology to model jammer-defender interactions on wireless networks. Reviewing the literature, it can be noted that, of the different types of games, Bayesian games, Stackleberg games, and non-cooperative games have been extensively studied for addressing the problem of jamming attack and their defense. A Bayesian game is a game in which the players do not have complete information of the strategies applied by each other. The use of Bayesian game can be justified, in that, in the real world, both the attacker and the defender do not have complete information about each other's attack and defense strategies, respectively. A Stackleberg game is a two player game played sequentially with one player being the leader and the other being the follower. The leader implements his/her strategy first and then followed by the followers strategy who implements his/her strategy next. The Stackleberg model is also justified because in many situations the attacker makes a decision after seeing the actions of the defender, or vice versa. Non-cooperative games as a strategy for solving jamming attack and defense problems can be justified due to the fact that, during a jamming attack and defense against such an attack, the attacker and defender work independent of each other and do not cooperate.

Another observation from the literature is that, most of the research concentrated on games with incomplete information, and the effect of such incomplete information is significant. Section 4.1.1 provides more information on the impact of incomplete information on the outcome of such games. Researchers often model players to be rational in their strategies, i.e., they are sure to either maximize or minimize their payoffs. The most common payoffs studied are throughput of the network, power consumption, SINR, and transmission energy cost. Zero-sum games have also been extensively used by researchers. An example of a zero-sum game in a jamming context is when an attacker aims to minimize networks throughput and the defender aims to maximize the throughput of the network (see Sections 4.1.1 and 4.3.1).

5. Next Steps

5.1. Gaps in Literature

As documented above, there is a dearth of papers in the area of wireless multichannel networks, so more research is needed. Figure 6 shows the number of jamming papers published for each wireless network type. Of the 28 papers that study multichannel wireless networks, 14 papers study multichannel WLANs, 9 papers study multichannel WSNs, and 5 papers study multichannel AHNs.



	Single Channel	Multi Channel	Single Channel	Multi Channel	Single Channel	Multi Channel
	WLAN		WSN		AHN	
# papers	31	14	13	9	8	5

Figure 6: Number of papers by wireless network type

Only 13 papers found in the literature study wireless AHNs, and out of them, only 5 papers study AHN multichannel networks. As seen in Figure 7, AHN contributes to only 16% of the total number of papers included in this literature review, and yet AHNs are expected to play an important role in the future civilian and military settings [31]. This absence of papers and increasing importance using AHN networks, highlights the clear need for more research in the areas of AHN as a whole and, more specifically about multichannel AHNs. Some of the research areas could be finding different attacks strategies, and defense against such attacks, in AHN networks.

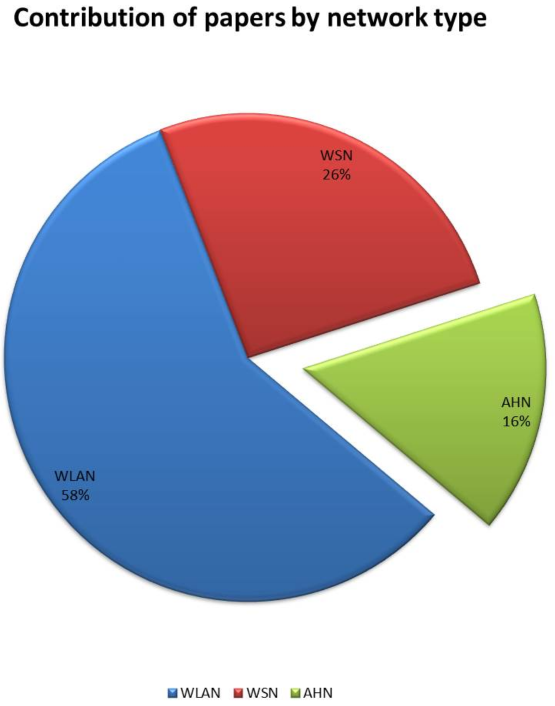


Figure 7: Percentage of the contribution of papers by wireless network type

As discussed earlier in Section 1, WSN and AHN are used in places in critical environments like deserts and war zones. These networks perform a lot of computations to analyze the data available and send the results of the analysis to the final user. Both WSN and AHN use batteries for functioning and the amount of power available is generally low. It is important for researchers to keep in mind power consumption of these networks while designing attack or defense strategies. Designing robust defense mechanisms more often require higher amount of computations, for example, finding paths in the network that are least jammed might take a lot of computation which in turn increases power consumption. From the taxonomy, we can see that researchers have given paramount importance to power levels for both jamming and defense against jamming, especially for WSN and AHN's, but power level was only considered a resource constraint. Hence, finding intelligent attack and defense mechanisms using minimal power can be a major contribution to the jamming literature.

Another potential contribution to the jamming literature is to study the impact and effect of combining some of the existing attack strategies to come up with a robust attack strategy and combine existing defense strategies to come up with a robust defense strategy, e.g., (see Li et al. [48]). A hybrid strategy that takes the positives from several strategies to give a more robust strategy will be a major contribution to the jamming literature. One such idea of combining strategies could be combining the defense strategies is discussed by Xu et al. [99] and Xu et al. [100]. Both these papers propose advanced channel hopping techniques and it would be interesting to see if combining them could give better results.

Another observation apparent from the classification scheme presented above is the 14 papers from the year 2010-2014 that provide a game theoretic approach to solving the jamming problems. The number of game theoretic models provided in literature for years 1980-1999, 2000-2003, 2004-2006 and 2007-2009 are 1, 1, 5, and 9 respectively. Thus, an increasing number of studies are employing mathematical programming modeling and/or game theoretic models to solve complex jamming problems. This trend towards game theory suggests that OR, and specifically mathematical programming and game theory, has an important role to play in future research on jamming wireless networks.

As noted earlier in the paper, most of the researchers have used incomplete information game theoretic approach for addressing the problem of jamming attacks and their defense, but there is no standard metric to measure the impact of incomplete information that is tailored to wireless networks. Interested researchers can contribute to the field of jamming attacks by finding a metric to measure such an impact on wireless networks. As an example, researchers in other fields have developed stochastic frameworks to model incomplete information, and made of use of expected value of perfect information (EVPI), to measure the impact of incomplete information. It would be worthwhile for jamming attack researchers to develop incomplete information games as a stochastic framework based model and use EVPI to measure the impact.

As mentioned earlier, researchers have assumed the players in a jamming attack and defense game to be rational. The assumption of rational players in jamming attacks games might not be completely valid, in that, the lack of information about the network or defense strategies might not enable the attacker to be rational in their decisions and vice-versa, i.e., the defender might not have enough information about the attackers strategies which does not allow the defenders to be rational about their decision. So, more research in developing game theoretic solutions where the players are not rational can be a positive contribution to the jamming literature, e.g., using bounded rationality could be an option (see Paruchuri [65] and Pita et al. [69]).

Another observation as noted before is the use of zero-sum games in defining jamming attack and defense games. Although the zero-sum games representation is common, in reality a gain for one player might not lead to a loss of the other player. For instance, in a min-max formulation the defender would try to minimize the maximum damage caused by the attacker, but in reality the defender might have an objective that is not completely in opposition to the attacker's objective. In this situation a general sum game would be more appropriate. Thus, robust optimization techniques to solve more realistic general sum games for the jamming attack and defense need to be developed.

5.2. Potential Research Problems

Below we discuss several new areas of research at the intersection of wireless network security and operations research.

A. Jammer Placement Problem

The jammer placement problem is an important areas of research for AHNs. The objective of the problem is to locate jamming devices in such a way that would either maximize or minimize the damage caused to the network. This problem is useful to the military; military strategists would like to find a way to locate the jamming devices and disrupt the communication of adversary networks. As discussed before, the jammer placement problem has studied by Commander et al. [23] and Vadlamani et al. [90], but both these papers consider static jammer locations. An interesting problem might be to consider a moving jammer, i.e., what could be the impact of a jammer device that changes locations with time. This problem of moving jammers is realistic in a war scenario or disaster aftermath situation where the jammer constantly moves to increase the impact of the attack. Another, interesting problem could be to include a stochastic model for the dynamic location of moving jammers, and, in response, have a defense mechanism to combat the jamming attack.

B. Anti-Jamming Packet Routing Problem

The anti-jamming packet routing problem is to optimally route the data sent within the network even when the adversary is trying to jam the network. Kim and Tague [38] develop a distributed path selection protocol tool that selects non-jammed paths in a wireless mesh network. Deng et al. [25] introduce an intrusion-tolerant routing protocol for wireless sensor networks. The main objective of this protocol is to protect a WSN whose nodes have been compromised by an attacker. This protocol effectively and securely constructs a tree-structured routing protocol that uses multiple paths to make the network more resilient to intrusion attacks. Pursley and Russell [71] introduce an adaptive decentralized routing protocol, called the least-resistance routing for radio networks. This method considers both interference and jamming in the network. The interference or jamming level determines the resistance of a particular path to transmit or receive data. The protocol chooses the path that has least resistance to transmit the data, thereby improving the throughput of the network. Since these papers provide heuristic solution approaches, it would be useful to develop a mathematical programming model to find optimal solutions for the packet routing problem for wireless networks under jamming attack. An interesting extension to the packet routing problem is the dynamic packet routing problem, in which every node can check to see if the link between it and the next node is jammed, and route packets dynamically using other paths in the network as a defense against jamming attacks.

C. Anti-Jamming Transmission Scheduling Problem

Developing scheduling algorithms that use real time information about the network in the presence of a jamming attack is a very important area of research. The data to be transmitted should be scheduled in such a way that the impact of the jamming attack is minimized. There are many papers in literature that study transmission scheduling problem in wireless networks in general [11, 33, 51, 83], but not for wireless networks under jamming attacks. To the best of our knowledge there is only one paper that addresses the problem of transmission scheduling under jamming attacks. Alnifie and Simon [4] as described above (see *Defense Strategies* in Section 4.2.2) provide a protocol that quickly moves the data from the attacked region to the region that is not under an attack. The scheduling problem they define is to find an assignment that maximizes the use of multiple channels to exfiltrate the data with interference and channel assignment constraints. The authors provide an algorithm to heuristically solve the scheduling problem. Because Alnifie and Simon [4] provide a heuristics solution there is a need for an exact or approximate algorithm to find an optimal solution for the transmission scheduling problem under jamming attacks.

D. Resource Allocation Problem

In AHN's the nodes have a very small amount of power available and efficient use of this power is very important. Many researchers such as Li et al. [47] and Sagduyu et al. [78] have used resource availability as a constraint to solve the jamming problem, but they do not try to optimize the allocation of the resource itself. During a jamming attack, the node in the network may have to reroute the packets or might use a higher signal strength to transmit data, which in turn would increase the power consumption. Hence, it is necessary to find optimization techniques that can improve the efficiency of the resource usage. Resource allocation problems under jamming attacks aim to minimize the total amount of power consumption, cost, etc., used to evade jamming by employing routing techniques or by efficient network node placement.

6. Conclusions

This paper, provides a comprehensive survey on the wireless network jamming problem. We provide a taxonomic classification of the different attack, defense, and detection and prevention techniques in literature by the type of wireless network they affect. Furthermore, different attack, defense, and detection techniques in literature are surveyed, in order to provide the interested researcher an understanding of the research done. This paper, offers a one-stop point for readers to get the complete picture of the research done in the area of wireless jamming attacks, including the type of attack, the solution methodology to counteract the attack, and most importantly, the type of wireless network studied. This classification scheme and analysis on the number of papers available in literature shows a potential gap in the dearth of research in wireless AHN and wireless multichannel networks. The papers shows that there is an increase in the usage of game theoretic strategies to address the problem of jamming attacks and hence points out areas where the OR community can contribute significantly to the wireless jamming literature. Areas and new research problems like jammer placement problem, scheduling, routing, and resource allocation under jamming attacks are identified where the OR community can contribute towards solving jamming problems in wireless network.

References

[1] Abdelmonem, A. H., Saadawi, T. N., Jan. 1989. Performance analysis of spread spectrum packet radio network with channel load sensing. Selected Areas in Communications, IEEE Journal on 7 (1), 161–166.

[2] Acharya, M., Thuente, D., 2005. Thuente, Intelligent Jamming Attacks, Counterattacks and. In: Counter)2 Attacks in 802.11b Wireless Networks, in Proceedings of the OPNETWORK-2005 Conference, Washington DC.

[3] Agarwal, S., Katz, R. H., Krishnamurthy, S. V., Dao, S. K., Sep. 2001. Distributed power control in ad-hoc wireless networks. In: Personal, Indoor and Mobile Radio Communications, 2001 12th IEEE International Symposium on. Vol. 2. IEEE, pp. F–59–F–66 vol.2.

[4] Alnifie, G., Simon, R., 2007. A multi-channel defense against jamming attacks in wireless sensor networks. In: Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks. Q2SWinet '07. ACM, New York, NY, USA, pp. 95–104.

[5] Alpcan, T., Basar, T., Dec. 2004. A game theoretic analysis of intrusion detection in access control systems. In: Decision and Control, 2004. CDC. 43rd IEEE Conference on. Vol. 2. IEEE, pp. 1568–1573 Vol.2.

[6] Altman, E., Avrachenkov, K., Garnaev, A., 2007. A Jamming Game in Wireless Networks with Transmission Cost. In: Chahed, T., Tuffin, B. (Eds.), Network Control and Optimization. Vol. 4465 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 1–12.

[7] Altman, E., Avrachenkov, K., Garnaev, A., 2007. A jamming game in wireless networks with transmission cost. In: Proceedings of the 1st EuroFGI international conference on Network control and optimization. NET-COOP'07. Springer-Verlag, Berlin, Heidelberg, pp. 1–12.

[8] Altman, E., Avrachenkov, K., Garnaev, A., May 2009. Jamming in wireless networks: The case of several jammers. In: Game Theory for Networks, 2009. GameNet, International Conference on. IEEE, pp. 585–592.

[9] Altman, E., Avrachenkov, K., Garnaev, A., Apr. 2011. Jamming in Wireless Networks Under Uncertainty. Mob. Netw. Appl. 16 (2), 246–254.

[10] Awerbuch, B., Richa, A., Scheideler, C., 2008. A jamming-resistant MAC protocol for single-hop wireless networks. In: Proceedings of the twenty-seventh ACM symposium on Principles of distributed computing. PODC '08. ACM, New York, NY, USA, pp. 45–54.

[11] Bao, L., Aceves, G. L., 2002. Transmission Scheduling in Ad Hoc Networks with Directional Antennas. In: Proceedings of the 8th Annual International Conference on Mobile Computing and Networking. MobiCom '02. ACM, New York, NY, USA, pp. 48–58.

[12] Basar, T. U., Basar, T. M., Mar. 1982. Robust linear coding in continuous-time communication systems in the presence of jamming and with noisy side information at the decoder. In: Proceedings of the 16th Annual Conference on Information Sciences and Systems.

[13] Bayraktaroglu, E., King, C., Liu, X., Noubir, G., Rajaraman, R., Thapa, B., Apr. 2008. On the Performance of IEEE 802.11 under Jamming. In: INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, pp. 1265–1273.

[14] Berg, J., 2008. Broadcasting on the Short Waves, 1945 to Today. McFarland, Incorporated Publishers.

[15] Brown, T. X., James, J. E., Sethi, A., 2006. Jamming and sensing of encrypted wireless ad hoc networks. In: Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing. MobiHoc '06. ACM, New York, NY, USA, pp. 120–130.

[16] Buttyan, L., Hubaux, J.-P., 2007. Security and cooperation in wireless networks. Vol. 188. Cambridge University Press Cambridge.

[17] Çakiroğlu, M., Özcerit, A. T., 2008. Jamming detection mechanisms for wireless sensor networks. In: Proceedings of the 3rd international conference on Scalable information systems. InfoScale '08. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium.

[18] Chan, A., Liu, X., Noubir, G., Thapa, B., Jun. 2007. Broadcast Control Channel Jamming: Resilience and Identification of Traitors. In: Information Theory, 2007. ISIT 2007. IEEE International Symposium on. IEEE, pp. 2496–2500.

[19] Chen, L., Leneutre, J., Jun. 2011. Fight jamming with jamming A game theoretic analysis of jamming attack in wireless networks and defense strategy. Computer Networks 55 (9), 2259–2270.

[20] Chiang, J. T., Hu, Y. C., 2007. Cross-layer jamming detection and mitigation in wireless broadcast networks. In: Proceedings of the 13th annual ACM international conference on Mobile computing and networking. MobiCom '07. ACM, New York, NY, USA, pp. 346–349.

[21] Chiang, J. T., Hu, Y.-C., Apr. 2008. Dynamic Jamming Mitigation for Wireless Broadcast Networks. In: INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE.

[22] Clark, A., Zhu, Q., Poovendran, R., Başar, T., 2012. Deceptive Routing in Relay Networks. In: Grossklags, J., Walrand, J. (Eds.), Decision and Game Theory for Security. Vol. 7638 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 171–185.

[23] Commander, C., Pardalos, P., Ryabchenko, V., Uryasev, S., Zrazhevsky, G., 2007. The wireless network jamming problem. Journal of Combinatorial Optimization 14 (4), 481–498.

[24] DeBruhl, B., Tague, P., Jun. 2012. Living with boisterous neighbors: Studying the interaction of adaptive jamming and anti-jamming. In: World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a. IEEE, pp. 1–6.

[25] Deng, J., Han, R., Mishra, S., Jan. 2006. INSENS: Intrusion-tolerant routing for wireless sensor networks. Computer Communications 29 (2), 216–230.

[26] Dolev, S., Gilbert, S., Guerraoui, R., Newport, C., 2007. Gossiping in a multi-channel radio network an oblivious approach to coping with malicious interference. In: Proceedings of the 21st international conference on Distributed Computing. DISC'07. Springer-Verlag, Berlin, Heidelberg, pp. 208–222.

[27] Dong, L., Han, Z., Petropulu, A. P., Poor, H. V., Aug. 2009. Cooperative jamming for wireless physical layer security. In: Statistical Signal Processing, 2009. SSP 09. IEEE/SP 15th Workshop on. IEEE, pp. 417–420.

[28] Garnaev, A., Hayel, Y., Altman, E., May 2012. A Bayesian jamming game in an OFDM wireless network. In: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2012 10th International Symposium on. IEEE, pp. 41–48.

[29] Gupta, V., Krishnamurthy, S., Faloutsos, M., Oct. 2002. Denial of service attacks at the MAC layer in wireless ad hoc networks. In: MILCOM 2002. Proceedings. Vol. 2. IEEE, pp. 1118–1123 vol.2.

[30] Hanawal, M. K., Altman, E., Jan. 2012. Stochastic Geometry based jamming games in Mobile Ad hoc Networks. In: Wireless On-demand Network Systems and Services (WONS), 2012 9th Annual Conference on. IEEE, pp. 91–98.

[31] Hong, X., Gerla, M., Pei, G., Chiang, C. C., 1999. A Group Mobility Model for Ad Hoc Wireless Networks. In: Proceedings of the 2Nd ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems. MSWiM '99. ACM, New York, NY, USA, pp. 53–60.

[32] Islam, M. H., Nadeem, K., Khan, S. A., Dec. 2008. Efficient placement of sensors for detection against distributed denial of service attack. In: 2008 International Conference on Innovations in Information Technology. IEEE, pp. 653–657.

[33] Ju, J.-H., Li, V. O. K., Aug. 1999. TDMA scheduling design of multihop packet radio networks based on latin squares. Selected Areas in Communications, IEEE Journal on 17 (8), 1345–1352.

[34] Kashyap, A., Basar, T., Srikant, R., 2004. Correlated jamming on MIMO Gaussian fading channels. Information Theory, IEEE Transactions on 50 (9), 2119–2123.

[35] Khattab, S., Mosse, D., Melhem, R., 2008. Jamming Mitigation in Multi-Radio Wireless Networks: Reactive or Proactive? In: Proceedings of the 4th international conference on Security and privacy in communication netowrks. SecureComm '08. ACM, New York, NY, USA.

[36] Khattab, S., Mosse, D., Melhem, R., 2008. Modeling of the channel-hopping anti-jamming defense in multi-radio wireless networks. In: Proceedings of the 5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services. Mobiquitous '08. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium.

[37] Kim, Y. S., DeBruhl, B., Tague, P., Jun. 2013. Stochastic optimization of flow-jamming attacks in multichannel wireless networks. In: Communications (ICC), 2013 IEEE International Conference on. IEEE, pp. 2165–2170.

[38] Kim, Y. S., Tague, P., 2012. Jamming-resistant distributed path selection on wireless mesh networks.

[39] Krikidis, I., Thompson, J. S., Mclaughlin, S., Oct. 2009. Relay selection for secure cooperative networks with jamming. Wireless Communications, IEEE Transactions on 8 (10), 5003–5011.

[40] Kyasanur, P., Vaidya, N. F., Jun. 2003. Detection and handling of MAC layer misbehavior in wireless networks. In: Dependable Systems and Networks, 2003. Proceedings. 2003 International Conference on. IEEE, pp. 173–182.

[41] Law, Y. W., van Hoesel, L., Doumen, J., Hartel, P., Havinga, P., 2005. Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. In: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. SASN '05. ACM, New York, NY, USA, pp. 76–88.

[42] Lazos, L., Krunz, M., Jan. 2011. Selective jamming/dropping insider attacks in wireless mesh networks. Network, IEEE 25 (1), 30–34.

[43] Lazos, L., Liu, S., Krunz, M., 2009. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In: Proceedings of the second ACM conference on Wireless network security. WiSec '09. ACM, New York, NY, USA, pp. 169–180.

[44] Lee, K., Kwon, H. M., Ding, Y., Ibdah, Y., Wang, Z., Apr. 2011. Noncooperative distributed MMSE relay schemes under jamming environment and node geometry in wireless relay networks. In: Wireless Telecommunications Symposium (WTS), 2011. IEEE, pp. 1–5.

[45] Lee, K., Kwon, H. M., Ding, Y., Ibdah, Y., Wang, Z., Bi, Y., May 2011. Node geometry and broadband jamming in noncooperative relay networks under received power constraint. In: Sarnoff Symposium, 2011 34th IEEE. IEEE, pp. 1–5.

[46] Li, C., Dai, H., Dec. 2013. Connectivity of multi-channel wireless networks under jamming attacks. In: Global Communications Conference (GLOBECOM), 2013 IEEE. IEEE, pp. 706–711.

[47] Li, M., Koutsopoulos, I., Poovendran, R., Aug. 2010. Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks. Mobile Computing, IEEE Transactions on 9 (8), 1119–1133.

[48] Li, X., Zhu, Y., Li, B., Jun. 2012. Optimal anti-jamming strategy in sensor networks. In: Communications (ICC), 2012 IEEE International Conference on. IEEE, pp. 178–182.

[49] Liu, G., Luo, J., Xiao, Q., Xiao, B., Jun. 2011. EDJam: Effective Dynamic Jamming against IEEE 802.15.4-Compliant Wireless Personal Area Networks. In: Communications (ICC), 2011 IEEE International Conference on. IEEE, pp. 1–5.

[50] Liu, H., Liu, Z., Chen, Y., Xu, W., Jun. 2011. Localizing Multiple Jamming Attackers in Wireless Networks. In: Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, pp. 517–528.

[51] Liu, X., Chong, Shroff, N. B., Sep. 2006. Opportunistic Transmission Scheduling with Resource-sharing Constraints in Wireless Networks. IEEE J.Sel. A. Commun. 19 (10), 2053–2064.

[52] Liu, X., Noubir, G., Sundaram, R., Tan, S., May 2007. SPREAD: Foiling Smart Jammers Using Multi-Layer Agility. In: INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE. IEEE, pp. 2536–2540.

[53] Liu, Y., Comaniciu, C., Man, H., 2006. A Bayesian game approach for intrusion detection in wireless ad hoc networks. In: Proceeding from the 2006 workshop on Game theory for communications and networks. GameNets '06. ACM, New York, NY, USA.

[54] Liu, Y., Li, J., Petropulu, A. P., Apr. 2013. Destination Assisted Cooperative Jamming for Wireless Physical-Layer Security. Information Forensics and Security, IEEE Transactions on 8 (4), 682–694.

[55] Liu, Y., Ning, P., Mar. 2012. BitTrickle: Defending against broadband and high-power reactive jamming attacks. In: INFOCOM, 2012 Proceedings IEEE. IEEE, pp. 909–917.

[56] Liu, Z., Liu, H., Xu, W., Chen, Y., Mar. 2012. Exploiting Jamming-Caused Neighbor Changes for Jammer Localization. Parallel and Distributed Systems, IEEE Transactions on 23 (3), 547–555.

[57] Lu, Z., Wang, W., Wang, C., Apr. 2011. From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic. In: INFOCOM, 2011 Proceedings IEEE. IEEE, pp. 1871–1879.

[58] Mallik, R. K., Scholtz, R. A., Papavassilopoulos, G. P., Aug. 2000. Analysis of an on-off jamming situation as a dynamic game. Communications, IEEE Transactions on 48 (8), 1360–1373.

[59] Maxim, M., Pollino, D., 2002. WirelessSecurity. The McGraw-Hill Companies.

[60] Medard, M., 1997. Capacity of Correlated Jamming Channels. In: Proc. 35th Annu. Allerton Conf. Communications, Control and Computing.

[61] Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., Pantziou, G., 2009. A survey on jamming attacks and countermeasures in WSNs. Communications Surveys & Tutorials, IEEE 11 (4), 42–56.

[62] Myerson, R. B., 1991. Game theory: analysis of conflict. Harvard University.

[63] Navda, V., Bohra, A., Ganguly, S., Rubenstein, D., May 2007. Using Channel Hopping to Increase 802.11 Resilience to Jamming Attacks. In: INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE. IEEE, pp. 2526–2530.

[64] Noubir, G., 2004. On Connectivity in Ad Hoc Networks under Jamming Using Directional Antennas and Mobility. In: Langendoerfer, P., Liu, M., Matta, I., Tsaoussidis, V. (Eds.), Wired/Wireless Internet Communications. Vol. 2957 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 186–200.

[65] Paruchuri, P., 2008. Playing games for security: An efficient exact algorithm for solving bayesian stackelberg games. In: In AAMAS.

[66] Pathan, A. K., Lee, H.-W., Hong, C. S., Feb. 2006. Security in wireless sensor networks: issues and challenges. In: Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference. Vol. 2. IEEE, pp. 6 pp.–1048.

[67] Pelechrinis, K., Iliofotou, M., Krishnamurthy, S. V., 2011. Denial of Service Attacks in Wireless Networks: The Case of Jammers. Communications Surveys &amp; Tutorials, IEEE 13 (2), 245–257.

[68] Pelechrinis, K., Koufogiannakis, C., Krishnamurthy, S. V., 2009. Gaming the jammer: is frequency hopping effective? In: Proceedings of the 7th international conference on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks. WiOPT'09. IEEE Press, Piscataway, NJ, USA, pp. 187–196.

[69] Pita, J., Jain, M., Tambe, M., Ordóñez, F., Kraus, S., Oct. 2010. Robust solutions to Stackelberg games: Addressing bounded rationality and limited observations in human cognition. Artificial Intelligence 174 (15), 1142–1171.

[70] Pronios, N., Polydoros, A., Oct. 1988. Slotted, ALOHA-type monohop networks under dynamic jamming. In: Military Communications Conference, 1988. MILCOM 88, Conference record. 21st Century Military Communications-What's Possible? 1988 IEEE. IEEE, pp. 709–713 vol.2.

[71] Pursley, M. B., Russell, H. B., Jul. 1993. Routing in frequency-hop packet radio networks with partial-band jamming. Communications, IEEE Transactions on 41 (7), 1117–1124.

[72] Raghavendra, C. S., Sivalingam, K. M., Znati, T., 2004. Wireless Sensor Networks. Springer US, Ch. 1.

[73] Richa, A., Scheideler, C., Schmid, S., Zhang, J., Sep. 2013. Competitive throughput in multi-hop wireless networks despite adaptive jamming. Distributed Computing 26 (3), 159–171.

[74] Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu, Q., Jan. 2010. A Survey of Game Theory as Applied to Network Security. In: System Sciences (HICSS), 2010 43rd Hawaii International Conference on. IEEE, pp. 1–10.

[75] Royer, E. M., Toh, C.-K., Apr. 1999. A review of current routing protocols for ad hoc mobile wireless networks. Personal Communications, IEEE 6 (2), 46–55.

[76] Sagduyu, Y. E., Berry, Ephremides, Jul. 2006. Jamming Games forPower Controlled Medium Access with Dynamic Traffic.

[77] Sagduyu, Y. E., Berry, R., Ephremides, A., May 2009. MAC games for distributed wireless network security with incomplete information of selfish and malicious user types. In: Game Theory for Networks, 2009. GameNets' 09. International Conference on. IEEE, pp. 130–139.

[78] Sagduyu, Y. E., Berry, R. A., Ephremides, A., May 2010. Wireless jamming attacks under dynamic traffic uncertainty. In: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2010 Proceedings of the 8th International Symposium on. IEEE, pp. 303–312.

[79] Sagduyu, Y. E., Berry, R. A., Ephremides, A., Aug. 2011. Jamming games in wireless networks with incomplete information. Communications Magazine, IEEE 49 (8), 112–118.

[80] Sagduyu, Y. E., Ephremides, A., Apr. 2007. A Game-Theoretic Analysis of Denial of Service Attacks in Wireless Random Access. In: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks and Workshops, 2007. WiOpt 2007. 5th International Symposium on. IEEE, pp. 1–10.

[81] Sagduyu, Y. E., Ephremides, A., Jan. 2007. SINR-based MAC Games for Selfish and Malicious Users. In: Proc. Information Theory and Applications Workshop.

[82] Shafiee, S., Ulukus, S., Oct. 2005. Capacity of multiple access channels with correlated jamming. In: Military Communications Conference, 2005. MILCOM 2005. IEEE. IEEE, pp. 218–224 Vol. 1.

[83] Simon, R., Farrugia, E., 2004. Topology Transparent Support for Sensor Networks. In: Karl, H., Wolisz, A., Willig, A. (Eds.), Wireless Sensor Networks. Vol. 2920 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 122–137.

[84] Tague, P., Slater, D., Poovendran, R., Noubir, G., Apr. 2008. Linear programming models for jamming attacks on network traffic flows. In: Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, 2008. WiOPT 2008. 6th International Symposium on. IEEE, pp. 207–216.

[85] Theodorakopoulos, G., Baras, J. S., Sep. 2008. Game Theoretic Modeling of Malicious Users in Collaborative Networks. Selected Areas in Communications, IEEE Journal on 26 (7), 1317–1327.

[86] Thuente, D. J., Acharya, M., 2006. Intelligent jamming in wireless networks with applications to 802.11b and other networks. In: Proceedings of the 2006 IEEE conference on Military communications. MILCOM'06. IEEE Press, Piscataway, NJ, USA, pp. 1075–1081.

[87] Thuente, D. J., Acharya, M., 2006. Intelligent jamming in wireless networks with applications to 802.11b and other networks. In: Proceedings of the 2006 IEEE conference on Military communications. MILCOM'06. IEEE Press, Piscataway, NJ, USA, pp. 1075–1081.

[88] Townsend, C., Arms, S., 2005. Wireless sensor networks. MicroStrain, Inc.

[89] Vadlamani, S., Medal, H., Eksioglu, B., Jun. 2014. Security in Wireless Networks: A Tutorial. Vol. 37 of NATO Science for Peace and Security Series - D: Information and Communication Security. IOS Press, pp. 272–288.

[90] Vadlamani, S., Medal, H., Eksioglu, B., Li, P., 2014. A Bi-Level Programming Model for the Wireless Network Jamming Placement Problem. In: Proceedings of the 2014 Industrial and Systems Engineering Research Conference.

[91] Wang, L., Cao, C., Ma, J. X., Song, M., 2013. Cluster-based cooperative jamming in wireless multi-hop networks. In: Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on. IEEE, pp. 169–174.

[92] Wang, L., Wyglinski, A. M., Aug. 2011. A combined approach for distinguishing different types of jamming attacks against wireless networks. In: Communications, Computers and Signal Processing (PacRim), 2011 IEEE Pacific Rim Conference on. IEEE, pp. 809–814.

[93] Wilhelm, M., Martinovic, I., Schmitt, J. B., Lenders, V., 2011. Short paper: reactive jamming in wireless networks: how realistic is the threat? In: Proceedings of the fourth ACM conference on Wireless network security. WiSec '11. ACM, New York, NY, USA, pp. 47–52.

[94] Wood, A., Stankovic, J. A., Oct. 2002. Denial of service in sensor networks. Computer 35 (10), 54–62.

[95] Wood, A., Stankovic, J. A., Son, S. H., Dec. 2003. JAM: a jammed-area mapping service for sensor networks. In: Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE. IEEE, pp. 286–297.

[96] Wood, A., Stankovic, J. A., Zhou, G., Jun. 2007. DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks. In: Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conference on. IEEE, pp. 60–69.

[97] Wu, Y., Li, X.-Y., Wang, W., 2007. Stochastic Security in Wireless Mesh Networks via Saddle Routing Policy.

[98] Xu, W., Aug. 2007. On Adjusting Power to Defend Wireless Networks from Jamming. In: Mobile and Ubiquitous Systems: Networking &amp; Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on. IEEE, pp. 1–6.

[99] Xu, W., Ma, K., Trappe, W., Zhang, Y., May 2006. Jamming sensor networks: attack and defense strategies. Network, IEEE 20 (3), 41–47.

[100] Xu, W., Trappe, W., Zhang, Y., 2007. Channel surfing: defending wireless sensor networks from interference. In: Proceedings of the 6th international conference on Information processing in sensor networks. IPSN '07. ACM, New York, NY, USA, pp. 499–508.

[101] Xu, W., Trappe, W., Zhang, Y., 2008. Anti-jamming timing channels for wireless networks. In: Proceedings of the first ACM conference on Wireless network security. WiSec '08. ACM, New York, NY, USA, pp. 203–213.

[102] Xu, W., Trappe, W., Zhang, Y., Wood, T., 2005. 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. MobiHoc '05. ACM, New York, NY, USA, pp. 46–57.

[103] Xu, X., Gao, K., Zheng, X., Zhao, T., Aug. 2012. A zero-sum game theoretic framework for jamming detection and avoidance in Wireless Sensor Networks. In: Computer Science and Information Processing (CSIP), 2012 International Conference on. IEEE, pp. 265–270.

[104] Yang, D., Xue, G., Zhang, J., Richa, A., Fang, X., Aug. 2013. Coping with a Smart Jammer in Wireless Networks: A Stackelberg Game Approach. Wireless Communications, IEEE Transactions on 12 (8), 4038–4047.

[105] Young, M., Boutaba, R., 2011. Overcoming Adversaries in Sensor Networks: A Survey of Theoretical Models and Algorithmic Approaches for Tolerating Malicious Interference. Communications Surveys & Tutorials, IEEE 13 (4), 617–641.

[106] Zander, J., Oct. 1991. Jamming in slotted ALOHA multihop packet radio networks. Communications, IEEE Transactions on 39 (10), 1525–1531.

[107] Zenko, W., 1989. Breakthrough in radio technology offers new application options. In: Vehicle Navigation and Information Systems Conference, 1989. Conference Record. IEEE, pp. 384–388.

[108] Zhang, L., Guan, Z., Melodia, T., Apr. 2014. Cooperative anti-jamming for infrastructure-less wireless networks with stochastic relaying. In: INFOCOM, 2014 Proceedings IEEE. IEEE, pp. 549–557.

[109] Zhang, Z., Wu, J., Deng, J., Qiu, M., Nov. 2008. Jamming ACK Attack to Wireless Networks and a Mitigation Approach. In: Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE. IEEE, pp. 1–5.

[110] Zhou, L., Haas, Z. J., Nov. 1999. Securing ad hoc networks. Network, IEEE 13 (6), 24–30.

[111] Zhu, Q., Saad, W., Han, Z., Poor, H. V., Basar, T., Nov. 2011. Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach. In: MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011. IEEE, pp. 119–124.