Security in wireless networks: A tutorial

Authors

Introduction

Wireless networks have gained more importance over the past few years. Wireless networks have found their applications in inventory management and price marketing in retail stores over a decade ago in the 1990s when the cost of radio cards were expensive. Now a days when the cost of radio cards have reduced drastically from $1500 to $50, the companies now are reaping benefits of investment and cost savings for collecting data and in logistics applications[1]. Companies and enterprises are also using wireless networks for easy collaboration with other colleagues through emails and voice over calls across the globe for low costs. Wireless networks with location based technology helps companies to advertize their product depending on the physical location of the user. For example, if a user is sitting in an airport would see the advertisement of the nearest coffee shop on his/her wireless device, using the location based technology of wireless networks. Not only commercial, wireless networks have found a place in the home and residential areas too [1]. The installation and use of wireless is easy as compared to running cables through the walls and the mobility provided by wireless network has become an instant hit in homes [1]. The boon of using wireless network also comes with a few concerns in the form of security issues. Wireless network are susceptible to various attacks because they use air as a common medium to transmit and receive data. The most commonly studied attacks on wireless networks are jamming attacks, denial of service attacks, Sybil attack etc. Security issues have been studied and different solution approaches to cope with the different attacks are provided [2, 3, 4, 5, 6, 7]. Wireless networks and their issues are a major research area in the field of electrical engineering (EE) and most of the papers published are from an electrical engineering point of view. The security issues of wireless networks can be thought of and modeled as a resource allocation problem [8, 9]. Resource allocation problems [10, 11] have a been solved using methods and concept of operations research. The classic traveling salesman problem [12] is one of the oldest resource allocations problem solved using operations research. So, although security in wireless networks is not a classical problem from a operations research prospective, there are a few papers from an operations research view point [8, 13]. Surveys [14, 15, 16, 17] found in literature are more centered towards the EE community and make it difficult for the non-EE to getter a better understanding of the topic. The main aim of this paper is to introduce the topic of network security in wireless networks with more emphasis on jamming attacks to the non-electrical engineering community. We start by discussing the different types of wireless networks studied extensively in literature. We also highlight the main issues and defense mechanism in wireless networks. Also some of the important definitions to better understand wireless networks and the security issues

in them are discussed. And finally a few modeling examples are also provided. We believe that the examples provided along with the definitions will give a good start for the operations research community to see and better understand potential research areas in wireless network security.

The rest of the paper is organized as follows; in Section 2 we introduce wireless networks and different types of wireless networks are discussed in Section 2.1. In Section 3 we provide different modeling constructs, and define some performance metrics. Section 4 provides some modeling examples from literature for better understanding wireless network security problems from an operations research view. We conclude this paper in Section 5.

1. About wireless networks

Ethernet cables or wires that connect computer in the same network and the internet are most commonly used method for communication in local areas like schools, offices etc. The data requested by the user is sent through these cables. Although, local area networks (LAN) are useful for fast communication of data in a small area, it restricts mobility of the user. To overcome the limitations of movement wireless means of transmitting data using air as the medium is becoming more and more popular these days. Wireless method of sending data finds its applications not only in offices and schools but also used by medical practitioners and military among the other applications. The data received or transmitted goes thorough the following abstract layers and each layer has a particular function as described:

1. *Physical Layer:* Describes the characteristics of the physical connection between devices on the network. The physical connection between devices can be cables, fibers, wires, and air in the case of wireless network. The transmission and reception of data is managed by the physical layer. In case of wireless network the binary data between computers in translated into electrical signals and use radio frequency to send and receive data, and all this is done by this layer. This layer suffers from radio jamming attacks.
2. *Data Link Layer:* Responsible for communication between the network layer and the physical layer. Also, segments the packets sent by the higher layer to frames that can be sent by the physical layer below. This layer also provides error checking and formatting of the frames of data being sent. The MAC (Medium Access Control) layer 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. A channel in a wireless network is a frequency at which the nodes send their data. The MAC sublayer uses MAC protocols to ensure that signals sent from different stations across the same channel don't collide. This layer is susceptible to much more sophisticated jamming energy efficient jamming than the physical layer jamming attacks.
3. *Network Layer:* Responsible to figuring out the network topology and assigning address and in concerned with the routing of the data. It acts as a link between the transportation layer above and thee data link layer below.
4. *Transport Layer:* Recovers any lost data and also responsible for retransmission of data. Provides data encryption and reliable data transfer capabilities.

5. *Application Layer:* This layer is responsible for defining the specifications of the data requested by the both the end user and the node in a network.

1.1. Types of wireless networks and applications

1.1.1. WLAN

The most widely used wireless network is the wireless local area network (WLAN), more commonly known as Wi-Fi. WLAN is available these days at home, schools, offices, coffee shops, etc., which allows for easy access to the Internet whenever needed as long as it is possible to connect to the Wi-Fi signal. The computers connect to an access point (AP) through wireless means, which connects to the Internet and allows the users to move freely within the rage of the Wi-Fi signal. Figure 1 gives a example of a WLAN with one AP and four computers which communicate with the AP using a wireless medium.

Figure 1. Wireless LAN .

1.1.2. WSN

Wireless Sensor Network (WSN) is a collection of a large number of individual autonomous nodes that share information among themselves. In WSN the data collected is not directly sent to the user, rather the result of all the data is sent i.e., only the goal of the sensor network is sent to the user and the intermediate data is not sent [18]. WSN consists of a gateway (base station) that connects the sensor nodes to other sensor networks or to the end user see 2. The data at the sensor nodes is compressed and transmitted to the base station from where the results are presented to the end user [19]. The data packets are sometimes sent to the destination via many intermediate nodes. This transmission by hopping from one node to another is called multihop. Figure2 shows a WSN with sensors in a sensing area for some information which are transmitted between the sensors and final result of all the data is sent to the base station which forwards the data to the end user.

Applications [14]**:**

- *Security:* The WSNs are used in security applications such as surveillance in sensitive areas to detect any threats (biological or chemical attacks) and false alarms.
- *Environment and habitat monitoring:* WSNs also help in getting information about the areas where it is difficult to setup infrastructure to monitor and environment and habitats.

- *Medical monitoring:* Doctors and medical practitioners can monitor the health of the patients with the use of proper WSNs.
- *Object tracking:* WSN can be used to track moving objects if suitable sensors are used.
- *Assistive environments:* Individuals with disabilities can be more independent and improve functional capabilities with the use of WSN. WSNs can enable cost effective self care and a better quality of life.

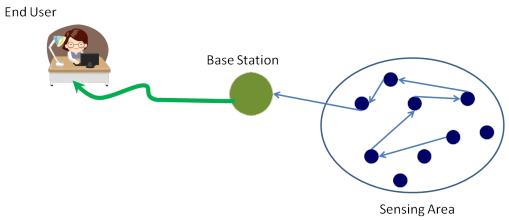

Figure 2. Wireless Sensor Network .

1.1.3. Ad hoc

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 routing of data independently by forwarding data from one to another without any centralized management equipment like access point. The nodes in the ad hoc network dynamically decide which node to send the data next depending on the network connectivity. Figure 3 shows a basic setup of an ad hoc network between laptops and phones, which communicate among themselves without an AP.

Applications [20, 21] **:**

- Military units (e.g.; soldiers, tanks) and ships can communicate even in the absence of well defined wireless infrastructure by forming an ad hoc network.
- Ad hoc networks can also be used for emergency, law enforcement, and rescue missions.
- Ad hoc networks are also used in conferences/lectures/meetings and other commercial areas where the load on the network can be very high (e.g., football games stadiums to check scores of other games)

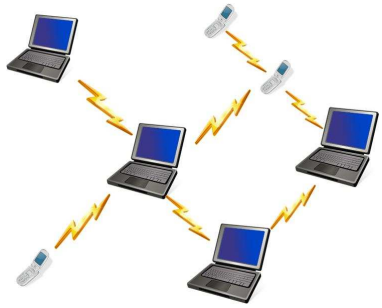

Figure 3. Wireless ad hoc network .

2. Modeling Constructs

In this section we discuss some of the modeling constructs like data collections and performance metrics found in literature. When the word 'jammer' is used we mean a device that has the capacity to jam a network and when used by the adversary can damage a legitimate network.

2.1. Data

Collecting data on security issues in wireless network is not an easy task for modeling a problem. It is difficult to get real world data about jamming strategy, defense strategy, and the location information of both the jammers and the network. Moreover it is not practical to test the attack and defense models in existing networks. Researchers therefore, have sought to simulations and experiments [22, 23, 24, 25] to test the attacks and provide defense strategies to those attacks. There are legal and ethical issues with collecting and publishing for research in cyber security [26]. These issues make it easy to create realistic data and run simulations or experiments to support the claim.

2.2. Objectives (performance metrics)

2.2.1. SINR

Signal to Interference plus Noise Ratio (SINR) is the ratio of the power of the signal of interest to the power of all other interfering signal including other nodes in the network and jammer and the power of background noise in the channel. The power of a signal (signal of interest, interference from other nodes, and signal from jammer) attenuates in the air with distance. The rate at which electromagnetic waves attenuates in free space is $\frac{1}{d_{ij}^2}$,where d_{ij} is the distance from the transmitting node i to receiver node j where i, j can be any node in the network or a jamming device. The power of node i experienced at node j denoted by p_{ij} is given by:

$$p_{ij} = \frac{\lambda}{d(i,j)^2} \tag{1}$$

and $\lambda \varepsilon \mathbb{R}$ is a proportionality constant; without loss of generality, we can set $\lambda = 1$. Now, the SINR in the channel at the receiver node D is:

$$\text{SINR} = \frac{p_{TD}}{I_D + \nu_D} \tag{2}$$

where p_{TD} is the power of node T at node D and I_D is the interference from concurrent transmissions of other nodes in the network and the power from the jammer; all these power follow the path loss property shown by Eq. (1). ν_D is the background noise in the channel. Higher the SINR the better is the quality of the data being transferred and vice-verse. The jammer tries to increase the interference power to decrease the SINR and thereby achieve its goal of disrupting the network. There could also be some selfish nodes in the network other than the jammer that try to decrease the SINR by increasing their power of concurrent transmission.

2.2.2. *Packet Send Ratio (PSR)*

This metric was introduced by Xu et al. [27]. PSR is defined as ratio of the number of packets that successfully sent by the legitimate transmission node T and the number of nodes it actually intended to send. If the transmission node intended to send n packets and the receiving node D receives only m ($m \leq n$) packets, then the PSR is given by 3.

$$PSR = \frac{m}{n} = \frac{\text{Packets Sent}}{\text{Packets Inteded to be sent}} \tag{3}$$

This loss in some packets is due to jamming interference. T senses the channel to be busy before transmitting any data because of the presence of a jamming signal. This busy channel leads to the filling up of the queue at T and no new packets are accepted and eventually the packets already in queue are discarded. Different MAC protocols have different ways of calling a channel busy. One way a channel is defined as busy is; if the signal strength of the channel is more than a predetermined threshold level. PSR also measures the efficiency of a transmitter that uses carrier sensing protocol to send data. PSR is easily calculated just by keeping track of the number of packets intended to send and the number of packet that have been successfully sent [15, 27].

2.2.3. *Packet Delivery Ration (PDR)*

Consider D receives n packets and from that only q packets pass the CRC (Cyclic Redundancy Codes) check, then the PDR is given by 4

$$PDR = \frac{q}{n} = \frac{\text{Packets that pass the CRC check}}{\text{Packets Recieved}} \tag{4}$$

So, the Packet Delivery Ratio (PDR) is the ratio of the number of packets received by the receiver to the number of packets that pass the CRC check. CRC is an error detecting technique used mainly in computer networks. This method finds the error between the data that is received and the data that is supposed to be received. In the presence of a jammer the data packets received will not pass the CRC, thereby reducing the PDR. PSR which captures the effectiveness of jamming at the transmitter, PDR measures the effectiveness at the receiver. It is also to be noted that if no packets are received, i.e., $n = 0$ the PDR is defined to be zero [15, 27].

2.2.4. *Connectivity Index*

In wireless ad hoc networks the presence of a jammer can disrupt the routes between the nodes in the network, thereby reducing the connectivity. *"A graph is said to be connected if there exists at least one path between any two nodes"* Noubir [28]. Connectivity index was first introduced by *Noubir [28]* to study the effect of jamming on the connectivity of ad hoc networks. Noubir [28] start by defining a non-jammed link. Now, let us assume R be range of communication between the nodes in the network, JS is the set of all the jammers, and JR is the range of jammers. A link between nodes T and D is said to be non-jammed if and only if Noubir [28]

$$d(T,D) < R \wedge \forall J \in JS : d(J,D) > JR \tag{5}$$

where $d(T,D)$ and $d(J,D)$ represents the Euclidean distance between nodes T and D and distance between jammer J and node D. Now let us define the connectivity index as

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

$$\text{Connectivity Index} = \frac{|E^{'}|}{\frac{|V|(|V|-1)}{2}} \tag{6}$$

The definition of transitive closure $|E^{'}|$ contains the node pairs in the graph that have a connection between them. So, the connectivity index is nothing but the ratio between such pair of nodes that have a connection between them to the number of all possible pairs of nodes in the network. We can see that a connected graph has a connectivity index of 1, while a graph partitioned in two connected graphs of equal size, has a connectivity index 0.5 [15].

2.2.5. Throughput

Throughput in business and manufacturing is defined as the rate at which the product or inputs and outputs leaves a system or a production line. In computer networks throughput is defined as the average rate of successful message delivery in a network over a communication channel. The throughput of a communication channel is given by the Shanon's rate [29]:

$$C = B log(1 + SINR) \tag{7}$$

where C is the channel capacity or maximum theoretical throughput measured in bits/sec, B is the bandwidth of the channel in Hertz and SINR is give by Eq. 2. The throughput of a channel is affected in the presence of a jammer or selfish node because the SINR is reduced as discussed above.

2.2.6. Utilization

In queuing systems if the rate of arrival (λ) of products/customers to a system follows a Poisson process and the rate of departure (μ) follows an exponential distribution then the utilization of the system is given by Little's Law [30]:

$$\rho = \frac{\lambda}{\mu} \tag{8}$$

In wireless networks the throughput is measured as the ratio of the rate of arrival of packets at a node to the service rate of the packets at that node. The presence of a jammer reduces the utilization of the node and overall network by jamming the channels and increasing the service rate.

2.3. Players and Strategies

The ease of movement and flexibility that wireless network (discussed above) although very convenient, comes with a threat to the security of the data being sent. The wireless

networks because of their nature of sharing a common medium like air to transmit and receive data makes them susceptible to attacks. The wired network on the other hand although is less flexible, suffers less attacks. The use of air makes it easy for the attacker to become part of the legitimate network and damage it by either compromising the secure data or by just not allowing legitimate data from flowing in the network. Below are discussed a few of the attacks common in wireless networks. We consider two players attacker; one who tries to disrupt the network and defender who tries to defend the network from the attacker.

2.3.1. Attack Strategies

Types of Attacks

- ***Sink Hole Attack:*** In sink hole attacks the adversary node would make a malicious node attractive and lure the traffic in that area through this compromised node. The adversary fakes the routing table values and makes the compromised nodes look attractive, they also try show higher quality link to reach the base station. With the neighboring nodes send the data thought the compromised node improves the routing tables baiting other nodes to use that malicious node to route data to the base station. This routing of data from all the nodes in the area increases the "strength of influence" [31] of the adversarial node. The adversary can either eavesdrop or even corrupt the data or read any secret messages making this very dangerous in wireless networks [31].
- ***Sybil Attack:*** In this type of attack, a single node displays multiple identities to other nodes in the network. This attack reduces the efficiency of the network by causing problems with routing protocols. The authorized packets sent by a node that uses multi path routing, or routes using disjoint nodes will be actually using a single attacker node portraying itself as multiple users.
- ***Worm hole Attack:*** In worm hole attacks the attacker tunnels the data received from one point in the network over a link with less delays and replays the data from another point in the network. Worm holes attacks include two distant malicious nodes colluding together to downplay the actual distant from each other and thereby attracting data to be sent through them. The malicious nodes could be very far from the network and be out of bound from a single hop, but they still pretend to be close to by using a single long range directional link. An adversary could be multiple hops from the base station but, they can completely convince the other nodes that they are just one or two hops from the base station if they use the wormhole. Here the malicious could eavesdrop or even form a sink hole [32, 31].
- ***Jamming Attack:*** The act of intentionally transmitting electromagnetic waves towards a communication network to either disrupt or preclude signal transmission in wireless networks is called jamming attack. In WSN and ad hoc networks jamming attacks interfere with legitimate transmission by using the same radio frequency that the nodes in the network use. The more powerful jammer can cause greater damage to the normal functionality of the network. In case of military and security applications where WSN and ad hoc networks are extensively used jamming attack could mean losing secure information to attackers or terrorists. This makes it important to use effective countermeasures against such attacks. The nodes in WSN and ad hoc networks have limited power, memory resources and low computational capacity, making them easy targets for an attacker with mediocre intelligence. Moreover these networks some-

times even have to use insecure channels to transmit data, in the case of an event like disaster where establishing a secure channel could be infeasible, allowing attackers to get easy access to the data by jamming the link the data is being transferred on. Jamming attacks are sometimes referred to as a special case of Denial of Service (DoS) attack [14]. Denial of service attack denies legitimate users from sending data because of the presence of an illegitimate user who transmits false data or radio frequency through the network, giving an impression to the legitimate nodes that the network is busy, and forcing them to stop sending any data until the network is free again. 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 DoS attack. Advanced and more expensive jamming devices are used to jam satellite communications. A wireless signal jamming device can be used to temporarily stop transmission and short out or turn off the power during the usage of units. Examples of such units are radios, televisions, microwaves, or any unit that receives electrical signals for operation.

Types of jammers Here we discuss four basic types jammers that have been studied in literature Xu et al. [27], Pelechrinis et al. [15], Mpitziopoulos et al. [14].

- ***Constant Jammer:*** The constant jammer continuously emits signals in the wireless network. The signal emitted can be a simple electromagnetic wave or even bits of data. The electromagnetic waves or bits of data transmitted by the jammer does not follow any protocol or rule that the legitimate nodes in the network follow. This kind of jammer reduces the PDR by corrupting the bits at the receiver node by interfering with the transmission of a transmitter node. The other objective of the constant jammer can be to reduce the PSR by keeping the channels busy and not allowing legitimate nodes to transmit data [15].
- ***Deceptive Jammer:*** Deceptive jammers are very similar to constant jammer in the sense both continuously transmit signals or data through the network, but, the difference is deceptive jammers unlike constant jammers they do not random bits. The deceptive jammers inject packets into the network continuously without any gap between transmissions and since they are not random bits, the legitimate nodes in the network believe these bits of data to be legitimate and hence cannot use the network anymore [15].
- ***Random Jammer:*** The jammers discussed above which continuously transmit signals or data and hence not very efficient with power management and have be connected to an external power source reducing their capability of moving. The random jammers on the other hand have sleep cycle and a jamming cycle both of which could follow any distribution like the uniform distribution or could be entirely random. Let τ_s and τ_j be the sleep time and the jamming time. In the sleep phase the jammer conserves energy and in the jamming phase can behave like any of the jammers discussed above [15].
- ***Reactive Jammer:*** Another energy efficient jammer is the reactive jammer. Reactive jammers unlike constant and deceptive jammers do not continuously jam the network; rather they jam the channel when any transmission is made. These jammers constantly listen to the channel and when they sense a packet transmission they immediately send a radio signal that jams the channel. The amount of power need to sense the channel is very less [15].

2.3.2. Defense strategies

The defense strategies most popular in literature for each type of attack strategies discussed above.

Defense against Sybil Attack

- ***One-way key chains:*** In sensor networks defense against Sybil attacks is done by a redundancy mechanism [33]. The set up server before assigns each sensor a unique information. The server subsequently assigns each of the unique information a unique id and binds the sensor with that unique id and unique information. The server creates a certificate of binding, and downloads the certificate and the unique information to the sensor node. To successfully receive/ transmit data the node should first show its unique id and the unique information to the demand node. If this check is complete then the data is transferred. This way no node can display multiple identities and hence Sybil attack fails [33].
- ***Radio Resource Testing:*** In this approach to defend against Sybil attack, the node n assigns each of its neighbors a different channel to broadcast some message on. The node n then randomly chooses a channel to listen to, if the neighbor that was assigned that channel is legitimate then the node n can hear the message. If the on other hand if s of $n's$ neighbors are Sybil identities then probability of the channel chosen is not transmitting any data, and hence detecting the Sybil attack is $\frac{s}{n}$. Conversely the probability of not detecting a Sybil attack is $\frac{n-s}{n}$. And if this procedure is repeated r times, the probability of not detecting a Sybil attack is $(\frac{n-s}{n})^r$. The more the number of rounds, the lower the probability of not detecting the attack [34].

Defense against Sink hole Attacks

- ***Trust Management System:*** Trust management and Dynamic Trust Management Systems (DTMS) have been used to protect both ad hoc and wireless networks receptively from attacks. In trust management system the nodes in the ad hoc network broadcast a vector of trust vector of length of N (number of nodes in the network) and a value of $+0.5$. The trust vector is broadcasted to all nodes in the network at regular time intervals. But, the value in vector changes depending on the experience of the other nodes in the network. If a node drops packets then its trust value is reduced at a very high rate. If a node transfers packets without much loss to the packets being it earns a positive trust value, but in this case the rate of increase of trust value is very small. This process is repeated and each node knows the trust value of other, so the nodes with a bad trust value are ignored from the routing [35]. Roy et al. [36] provide a dynamic trust management system to counter sink hole attacks in WSN. Unlike ad hoc network where there is no central manager who controls the flow of data, in sensor networks the trust vector is sent to the base station at regular intervals, where the decision of which node to trust is made and then routing plan is decided.

Defense against Wormhole Attack

- ***Packet Leash:*** The packet leash method is has two different variants; 1) geographic leash, 2) temporal leash. The geographic leash is location based and the temporal leash is time based. In geographic leash the sender sends his location p_s, and time of sending t_s along with the packet. At the receiver the node compares its location p_r and the time of receiving t_r, both the clocks at transmitter and receiver are loosely

synchronized. Now, using the time and the location values and knowing the speed of packets, the receiver can calculate the upper bound of the distance between the transmitter and receiver. So, in the presence of a worm hole, the distance would seem very far from the actual reported value by the transmitter and hence eliminating the route [32]. In temporal leash the transmitter and the receiver clocks have to be tightly synchronized. The transmitter node includes the time of sending in the packet and the receiver on receiving the packet, notes the time. Now using the time values and the speed of light, the receiver calculates the distance, to see if the packet has traveled a longer distance than it should have. There is another variation of temporal leash, in which the transmitter includes the time of sending and a expiration time in the packet after which the receiver should not accept the packet. Both, these method provide a good defense strategy against wormhole attacks [32].

Defense against Jamming Attack

- ***Transmission power:*** Transmitter can use low power to transmit data in the network making it difficult for the jammer to detect the source of transmission to jam the channel being used. But on the other hand it is better to have a stronger signal power to combat jamming by increasing the SINR (Eq. 2). The nodes therefore should have a control over the power used for transmission to evade jamming attacks [14].
- ***Frequency Hopping Spread Spectrum (FHSS):*** Spread Spectrum (SS) is a modulation technique that spreads the transmitting data across the entire band even though the entire band is not needed to send that data. The spreading of the data beyond the needed limit in entire band makes the signal resistant to noise, interference and eavesdropping. FHSS is a spread spectrum technique where the transmitting radio rapidly switches between frequency channels. The channel change is done by an algorithm that is shared between both the transmitter and the receiver prior to exchanging data. The jammer is kept in the dark about the channel switching algorithm and hence cannot jam the channel that is being used for transmission [14].
- ***Directional Antennas:*** Directional antennas unlike omni directional antennas transmit and receive data from one direction; this reduces the interference and increases the performance of the network. Directional antennas provide better protection from jamming and eavesdropping. Wireless ad hoc networks use two types of directional antennas; sectored and beamforming antennas [14] . Noubir [28] proposed sectored directional antennas for WSN.
- ***Channel Surfing:*** Channel Surfing is similar to FHSS in that both evade jamming attack by quickly changing channels to transmit and receive data between the transmitter and receiver. The difference between the two is that FHSS is on the physical layer and needs special transceivers, where as the channel surfing is a link layer technology and can be applied to wireless nodes. The other difference is that FHSS needs the transmitter and receiver to share an algorithm prior to sending data (as discussed above), and this is not need in channel surfing [37].

2.4. Constraints

The major issues with using wireless network, other than being susceptible to attacks, have a limitation on the amount of energy they can use. In case of WLAN laptop computers have a limited battery life and need to be recharged when necessary. This

might not seem like a problem, in case of a WLAN (laptops), but, in WSN and ad hoc networks battery power and energy are major issues. WSN and ad hoc networks are used in places where it is hard for humans to be, and in military situations where a node failing due lack of power or energy could prove dangerous. Researchers have fairly recently included power constraint [7] in their models. It is also important to note that power constraints from the attacker point of view have also been considered [7]. The transmission cost [38] for both attacker and defender is important constraint. The number of channels that can be used to transfer data are also limited depending on the frequency range used ($2.4GHz$, $5GHz$ etc.). For setting up a wireless network with all the defense capabilities involves or for an attacker to have maximum capacity involves a lot of cost [39] and is even infeasible due to the limitations from existing technologies.

2.5. Decision Variables

Here some of the decisions the attacker and defender take to increase the damage and to decrease the damage to the network.

2.5.1. Attacker

- ***Select Channel Probabilities:*** The jammer is successful in jamming a channel if and only if she chooses the channel on which data is transferred. Sweep jamming [14] is a jamming technique in which the jammer shifts its full power rapidly from channel to another. This is effective because jam multiple channels in quickly but has a disadvantage of jamming only one channel at time. It would better for the jammer to choose a channel which has higher chances of sending data with higher probability rather than simply wasting its power on channels with low probability of transmission.
- ***Jammer Location:*** The location of the jammer is very important, because the farther the jammer from the nodes the less the impact or damaged caused Eq.1. Commander et al. [8] 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).
- ***Jamming Power Level:*** Jammers like nodes in the wireless network, have restriction on the amount of power they can use. Using the power wisely is also an important decision that jammer have to take [40]. In a war situation, the jammer might not get time to recharge the jammer without losing critical information or even getting caught.

2.5.2. Defender

- ***Select Channel Probabilities:*** Changing channels to evade jamming attack is effective [37]. If the channel access probability of the jammer is known the node can choose channels in such a way that it can avoid jamming. Without knowing the channel access probability of the jammer, the node chooses the channel with probability to reduce the maximum damage caused by the jammer 41.
- ***Transmission Power Level:*** The limitation on the power usage influences [40] the decision of the node in the network. More the power better the range of transmission Eq.1 and higher the SINR Eq.2, but, increases attack probability and reduces the lifetime of the node. A regulated power usage is very important for nodes in wireless networks and is important for WSN and ad hoc networks [14].

- ***How to design networks:*** [42]The network should be designed being aware of the fact that there is always going to be someone try to attack. Metrics should be put in place to detect an attack even before deploying a network. Some of metrics like PDR, PSR, and SINR are good, but not the only metrics, the network designer should also think better metrics to detect an attack. A low PDR does not necessarily always mean that the network is under attack, it could be a genuine case of congestion in the network. So, good methods or more sophisticated methods should be thought and implemented. Once the attack is detected, the nodes should be take counteractions to protect the data and the network. Cryptographic measures should also be taken to protect against intelligent attacks.

3. Modeling Examples

In this section we provide a few examples of models from literature for each of the types of wireless networks discussed in section 2.

3.1. WLAN

[9] Consider a single channel access point network with one transmitter and one jammer as shown in Figure 4. The transmitter is called Node 1 and Jammer is Node 2. Let λ be the arrival rate of packets in the queue at node 1. Node 2 does not have any messages or queue of its own. Assume that for each packet transmission from the transmitter or jammer consumes one unit of energy. The objective of node 1 is to minimize the average energy cost. The probability of node 1 transmitting p_1 only if there is a packet in the queue. The transmission is successful if the jammer does not transmit. If node 2 transmits in the same time slot as node 1 the packet is captured by the network (safely kept in memory) with a probability q. Assume that the node 2 transmits at a fixed probability $p_2 \in [0,1]$. The service rate of node 1's queue is :

$$\mu(p_1, p_2) = p_1((1-p_2)+p_2q) \tag{9}$$

The transmission of node 1 is successful if and only if the node 1 transmits when node 2 does not or the packet is captured with a probability q if node 2 transmits at the same time. The model of node 1 is given as

$$\begin{aligned} max_{p_1 \in [0,1]} u(p_1, p_2) &= -\frac{\lambda}{\mu(p_1, p_2)} p_1 \\ s.t.\ \mu(p_1, p_2) &\geq r(\lambda, D) \end{aligned} \tag{10}$$

The objective is to minimize the average cost of transmission, given the cost of one transmission is one unit energy. Eq.10 is the targeted minimum rate constraint and D is the quality of service parameter. The objective of node 2 is to maximize the average energy consumed by node 1 is given:

$$max_{p_2 \in [0,1]} u(p_1, p_2) = \frac{\lambda}{\mu(p_1, p_2)} p_1$$
$$s.t.\ p_2 \leq E_2 \tag{11}$$

where 11 is the average energy constraint and $0 < E_2 < 1$. Sagduyu et al. [9] provided a game theoretic solution and also provide a Nash Equilibrium for the above model.

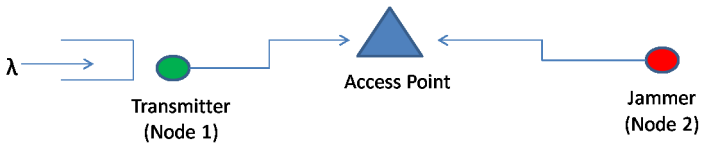

Figure 4. Single Channel Access Point with one transmitter and one jammer.

3.2. WSN

[41] Given an undirected graph $G = (S, E)$ where S is the set of sensor nodes and E is the set of edges. Every node or sensor transmit with a power level P and has a range of transmission R. Let N_i is the set of all neighbors of node i, and $n_i = |N_i|$ is the number of nodes in the set N_i. Also E is the total amount of energy at each node. γ is the channel access probability common for all nodes in the network. The transmission from node i to node j is successful only if node i transmits and no other neighboring nodes transmit at the same time. The probability of collision at node j is $\theta_0 = 1 - Pr\{\text{only one or no neighbors transmit}\} = 1 - (1-\gamma)^{n_j} - n_j\gamma(1-\gamma)^{n_j-1}$. Jammer has energy level of E_m and the transmission power. The jammer also jams the area with a probability q within its transmission range R_m. Collision occurs at node i if the jammer jams and at least a neighbor transmits. The probability of a collision at node i is $\theta_1 = 1 - Pr\{\text{no neighbor transmits}\} -$ $Pr\{\text{one neighbor transmits while adversary doesnot}\} =$ $1 - (1-\gamma)^{n_i} - (1-q)^{n_i}\gamma(1-\gamma)^{n_i-1}$. The average number of samples needed for detecting jamming (refer [41] for details) is

$$D(q, \gamma) = \frac{C}{\theta_1 log\frac{\theta_1}{\theta_0} + (1-\theta_1) log\frac{1-\theta_1}{1-\theta_0}} \tag{12}$$

The average time needed for a signal after the attack is detected to propagate in the network (refer [41] for details) is

$$W(q, \gamma) = \frac{H}{(1-q)\gamma(1-\gamma)^{\bar{n}-1}} \tag{13}$$

where H is the number of hops needed for the signal to be delivered outside the area of a jamming attack and $\bar{n}$ is the average number of neighbors of a node along the path of the signal. The objective function of the jammer is to maximize the total delay of the signal to be delivered outside the area of the jamming attack.

$$max_{0<q\leq 1} \quad D(q,\gamma)+W(q,\gamma)$$
$$s.t.\ qP_m[D(q,\gamma)+W(q,\gamma)] \leq E_m \tag{14}$$
$$U_{mC}(q,\gamma) \geq \quad U_m^0 \tag{15}$$

where 14 is the energy constraint and $U_{mC}(q,\gamma)$ and U_m^0 is the cumulative and the minimum payoff for the jammer for corrupting the communication (for details [41]). The objective of the network is to minimize the total delay:

$$min_{0\leq\gamma\leq 1} \quad D(q,\gamma)+W(q,\gamma)$$
$$s.t.\ \gamma P[D(q,\gamma)+W(q,\gamma)] \leq E \tag{16}$$
$$U_C(q,\gamma) \geq \quad U^0 \tag{17}$$

where 16 is the energy constraint and $U_C(q,\gamma)$ and U^0 is the cumulative and the minimum payoff for the network for avoiding the attack (for details [41]). Li et al. [41] solve the above problem as an optimization problem. They also solve the problem as *minmax* when there no information between the jammer and the attacker about each others strategy.

3.3. Ad hoc

[43] Consider a mobile ad hoc network (MANET) model called the Poisson bipolar model. Each transmitter node in the network (Operator) has a particular receiver node and the transmitter node have infinite packets to send. Nodes in the network are scattered in the Euclidean space according to a homogeneous Poisson point process of intensity λ_1[43]. Jammer are also has jamming nodes scattered in the Euclidean space according to a homogeneous Poisson point process of intensity λ_2. The probability that a node transmits is q_1 and the intensity of a pair of independent Poisson process for nodes that transmit is $q_1\lambda_1$. Let P_1 and P_2 be the fixed power of transmission of the nodes and the jammer respectively. The transmitters of the Jammer form a Poisson point process of intensity $q_2\lambda_2$, where $q_2$is the probability that the jammer transmits. Thus a typical node gets interference from the other nodes that form a Poisson point process of intensity $q_1\lambda_1+q_2\lambda_2$. The average density of power dissipated among the nodes of the Operator is $q_1\lambda_1P_1$ and the let the cost of transmission of an Operator node be ρ_1. Similarly, the average energy dissipated among the nodes of the jammer is $q_2\lambda_2P_2$ and the cost of transmission is ρ_2. The strategy of the Operator nodes is to choose $q_1 \in [0,1]$ with which each of the nodes can access the channel. The strategy of the jammer is to choose $q_2 \in [0,1]$ such that the transmission of the jammer is turned ON at the same time slot as the nodes. The utility function of the nodes in the network is the density of successful transmission considering the average cost of transmission among the nodes:

$$U_1(q_1,q_2) = d(q_1,q_2) - \rho_1 q_1 \lambda_1 P_1 \tag{18}$$

The utility function of the jammer such that the density of successful transmission of the nodes is minimized considering the average cost of transmission:

$$U_2(q_1, q_2) = -d(q_1, q_2) - \rho_2 q_2 \lambda_2 P_2 \tag{19}$$

where is the density of successful transmission of the Operator nodes (refer [43] for details)

$$d(q_1, q_2) = \lambda_1 q_1 p_s(q_1, q_2) \tag{20}$$

Now the objective of the nodes in the network is to choose q_1^*, such that the density of successful transmission is maximized

$$q_1^* \in argmax_{q_1 \in [0,1]} U_1(q_1, q_2) \tag{21}$$

the objective of jammer is to choose q_2^*, such that the density of successful transmission of the nodes is minimized

$$q_2^* \in argmax_{q_2 \in [0,1]} U_2(q_1, q_2) \tag{22}$$

Hanawal and Altman [43] solve the above problem as a zero-sum game and also find a Nash Equilibrium solution.

4. Conclusion

In this paper we provide a detailed introduction to security issues in wireless networks with more importance to jamming attacks to the operations research community. We provide a tutorial on the types of wireless networks, types of attacks strategies and defense strategies for each of the attack described. Then modeling constructs like data collection, performance metrics are also discussed. The a few modeling examples from literature are also provided for each type of network.

References

[1] Jim Geier. The state of wireless LANs. Technical report, 2004. URL `http://networkworld.com/whitepapers/nww/Intel_SR_071104.pdf`.

[2] Tansu Alpcan and T. Basar. A game theoretic analysis of intrusion detection in access control systems. In *Decision and Control, 2004. CDC. 43rd IEEE Conference on*, volume 2, pages 1568–1573 Vol.2. IEEE, December 2004. ISBN 0-7803-8682-5. doi: 10.1109/cdc.2004.1430267. URL `http://dx.doi.org/10.1109/cdc.2004.1430267`.

[3] Eitan Altman, Konstantin Avrachenkov, and Andrey Garnaev. A Jamming Game in Wireless Networks with Transmission Cost. In Tijani Chahed and Bruno Tuffin, editors, *Network Control and Optimization*, volume 4465 of *Lecture Notes in Computer Science*, pages 1–12. Springer Berlin Heidelberg, 2007. doi: 10.1007/978-3-540-72709-5_1. URL `http://dx.doi.org/10.1007/978-3-540-72709-5_1`.

[4] Andrey Garnaev, Y. Hayel, and E. Altman. 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*, pages 41–48. IEEE, May 2012. ISBN 978-1-4673-2294-2. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6260494.

[5] N. Pronios and A. Polydoros. 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*, pages 709–713 vol.2. IEEE, October 1988. doi: 10.1109/milcom.1988.13468. URL http://dx.doi.org/10.1109/milcom.1988.13468.

[6] Andrea Richa, Christian Scheideler, Stefan Schmid, and Jin Zhang. Competitive throughput in multi-hop wireless networks despite adaptive jamming. *Distributed Computing*, 26(3):159–171, September 2013. ISSN 0178-2770. doi: 10.1007/s00446-012-0180-x. URL http://dx.doi.org/10.1007/s00446-012-0180-x.

[7] Y. E. Sagduyu and Anthony Ephremides. 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*, pages 1–10. IEEE, April 2007. ISBN 978-1-4244-0960-0. doi: 10.1109/wiopt.2007.4480053. URL http://dx.doi.org/10.1109/wiopt.2007.4480053.

[8] ClaytonW Commander, PanosM Pardalos, Valeriy Ryabchenko, Stan Uryasev, and Grigoriy Zrazhevsky. The wireless network jamming problem. *Journal of Combinatorial Optimization*, 14(4):481–498, 2007. doi: 10.1007/s10878-007-9071-7. URL http://dx.doi.org/10.1007/s10878-007-9071-7.

[9] Y. E. Sagduyu, R. A. Berry, and Anthony Ephremides. 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*, pages 303–312. IEEE, May 2010. ISBN 978-1-4244-7523-0. URL http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5518798.

[10] S. S. Panwalkar, Milton L. Smith, and Christos Koulamas. Review of the ordered and proportionate flow shop scheduling research. *Naval Research Logistics*, 60(1):46–55, February 2013. doi: 10.1002/nav.21518. URL http://dx.doi.org/10.1002/nav.21518.

[11] Hasan Pirkul and Vaidyanathan Jayaraman. A multi-commodity, multi-plant, capacitated facility location problem: formulation and efficient heuristic solution. *Computers & Operations Research*, 25(10):869–878, October 1998. ISSN 03050548. doi: 10.1016/s0305-0548(97)00096-8. URL http://dx.doi.org/10.1016/s0305-0548(97)00096-8.

[12] Marco Dorigo and Luca M. Gambardella. Ant colonies for the travelling salesman problem. *Biosystems*, 43(2):73–81, July 1997. ISSN 03032647. doi: 10.1016/s0303-2647(97)01708-5. URL http://dx.doi.org/10.1016/s0303-2647(97)01708-5.

[13] ClaytonW Commander, PanosM Pardalos, Valeriy Ryabchenko, Sergey Sarykalin, Timofey Turko, and Stan Uryasev. Robust Wireless Network Jamming Problems. In MichaelJ Hirsch, ClaytonW Commander, PanosM Pardalos, and Robert Murphey, editors, *Optimization and Cooperative Control Strate-*

gies, volume 381 of *Lecture Notes in Control and Information Sciences*, chapter 23, pages 399–416. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009. ISBN 978-3-540-88062-2. doi: 10.1007/978-3-540-88063-9_23. URL http://dx.doi.org/10.1007/978-3-540-88063-9_23.

[14] A. Mpitziopoulos, Damianos Gavalas, C. Konstantopoulos, and G. Pantziou. A survey on jamming attacks and countermeasures in WSNs. *Communications Surveys & Tutorials, IEEE*, 11(4):42–56, 2009. ISSN 1553-877X. doi: 10.1109/surv.2009.090404. URL http://dx.doi.org/10.1109/surv.2009.090404.

[15] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *Communications Surveys & Tutorials, IEEE*, 13(2):245–257, 2011. ISSN 1553-877X. doi: 10.1109/surv.2011.041110.00022. URL http://dx.doi.org/10.1109/surv.2011.041110.00022.

[16] David R. Raymond and S. F. Midkiff. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *Pervasive Computing, IEEE*, 7(1):74–81, January 2008. ISSN 1536-1268. doi: 10.1109/mprv.2008.6. URL http://dx.doi.org/10.1109/mprv.2008.6.

[17] M. Young and R. Boutaba. 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, 2011. ISSN 1553-877X. doi: 10.1109/surv.2011.041311.00156. URL http://dx.doi.org/10.1109/surv.2011.041311.00156.

[18] C. S. Raghavendra, Krishna M. Sivalingam, and Taieb Znati. *Wireless Sensor Networks*, chapter 1. Springer US, 2004. ISBN 1-4020-7883-8.

[19] Chris Townsend and Steven Arms. *Wireless Sensor networks: Principles and Applications*, chapter 22. Wilson Inc.

[20] E. M. Royer and Chai-Keong Toh. A review of current routing protocols for ad hoc mobile wireless networks. *Personal Communications, IEEE*, 6 (2):46–55, April 1999. ISSN 1070-9916. doi: 10.1109/98.760423. URL http://dx.doi.org/10.1109/98.760423.

[21] Lidong Zhou and Z. J. Haas. Securing ad hoc networks. *Network, IEEE*, 13 (6):24–30, November 1999. ISSN 0890-8044. doi: 10.1109/65.806983. URL http://dx.doi.org/10.1109/65.806983.

[22] Yongle Wu, Beibei Wang, K. J. R. Liu, and T. C. Clancy. Anti-Jamming Games in Multi-Channel Cognitive Radio Networks. *Selected Areas in Communications, IEEE Journal on*, 30(1):4–15, January 2012. ISSN 0733-8716. doi: 10.1109/jsac.2012.120102. URL http://dx.doi.org/10.1109/jsac.2012.120102.

[23] Wenyuan Xu, Wade Trappe, and Yanyong Zhang. Channel surfing: defending wireless sensor networks from interference. In *Proceedings of the 6th international conference on Information processing in sensor networks*, IPSN '07, pages 499–508, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-638-7. doi: 10.1145/1236360.1236423. URL http://dx.doi.org/10.1145/1236360.1236423.

[24] Zhiguo Zhang, Jingqi Wu, Jing Deng, and Meikang Qiu. Jamming ACK Attack to Wireless Networks and a Mitigation Approach. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, pages 1–5. IEEE, November 2008. ISBN 978-1-4244-2324-8. doi: 10.1109/glocom.2008.ecp.950. URL http://dx.doi.org/10.1109/glocom.2008.ecp.950.

[25] Quanyan Zhu, W. Saad, Zhu Han, H. V. Poor, and T. Basar. Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach. In *MILITARY COMMUNICATIONS CONFERENCE, 2011 - MILCOM 2011*, pages 119–124. IEEE, November 2011. ISBN 978-1-4673-0079-7. doi: 10.1109/milcom.2011.6127463. URL http://dx.doi.org/10.1109/milcom.2011.6127463.

[26] Aaron J. Burstein. Conducting Cybersecurity Research Legally and Ethically. In *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, LEET'08, pages 1–8, Berkeley, CA, USA, 2008. USENIX Association. URL http://portal.acm.org/citation.cfm?id=1387717.

[27] Wenyuan Xu, Wade Trappe, Yanyong Zhang, and Timothy Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, MobiHoc '05, pages 46–57, New York, NY, USA, 2005. ACM. ISBN 1-59593-004-3. doi: 10.1145/1062689.1062697. URL http://dx.doi.org/10.1145/1062689.1062697.

[28] Guevara Noubir. On Connectivity in Ad Hoc Networks under Jamming Using Directional Antennas and Mobility. In Peter Langendoerfer, Mingyan Liu, Ibrahim Matta, and Vassilis Tsaoussidis, editors, *Wired/Wireless Internet Communications*, volume 2957 of *Lecture Notes in Computer Science*, pages 186–200. Springer Berlin Heidelberg, 2004. doi: 10.1007/978-3-540-24643-5_17. URL http://dx.doi.org/10.1007/978-3-540-24643-5_17.

[29] Anthony Ephremides, V. Angelakis, and A. Traganitis. SINR-Based Ad-Hoc Networking. In *Personal, Indoor and Mobile Radio Communications, 2006 IEEE 17th International Symposium on*, pages 1–5. IEEE, 2006. ISBN 1-4244-0329-4. doi: 10.1109/pimrc.2006.254188. URL http://dx.doi.org/10.1109/pimrc.2006.254188.

[30] D. Bertsekas and R. Gallager. *Data Networks*. Prentice Hall, Englewood Cliffs, NJ, 1992.

[31] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293–315, September 2003. ISSN 15708705. doi: 10.1016/s1570-8705(03)00008-8. URL http://dx.doi.org/10.1016/s1570-8705(03)00008-8.

[32] Yih-Chun Hu, A. Perrig, and D. B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 3, pages 1976–1986 vol.3. IEEE, March 2003. ISBN 0-7803-7752-4. doi: 10.1109/infcom.2003.1209219. URL http://dx.doi.org/10.1109/infcom.2003.1209219.

[33] Qinghua Zhang, P. Wang, D. S. Reeves, and Peng Ning. Defending against Sybil attacks in sensor networks. In *Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on*, pages 185–191. IEEE,

June 2005. ISBN 0-7695-2328-5. doi: 10.1109/icdcsw.2005.57. URL http://dx.doi.org/10.1109/icdcsw.2005.57.

[34] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil attack in sensor networks: analysis & defenses. In *Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on*, pages 259–268. IEEE, April 2004. ISBN 1-58113-846-6. doi: 10.1109/ipsn.2004.1307346. URL http://dx.doi.org/10.1109/ipsn.2004.1307346.

[35] Subhrabrata Choudhury, SumanDeb Roy, and SnehaAman Singh. Trust Management in Ad Hoc Network for Secure DSR Routing. In Tarek Sobh, Khaled Elleithy, Ausif Mahmood, and MohammadA Karim, editors, *Novel Algorithms and Techniques In Telecommunications, Automation and Industrial Electronics*, pages 496–500. Springer Netherlands, 2008. doi: 10.1007/978-1-4020-8737-0_89. URL http://dx.doi.org/10.1007/978-1-4020-8737-0_89.

[36] S. D. Roy, S. A. Singh, S. Choudhury, and N. C. Debnath. Countering sinkhole and black hole attacks on sensor networks using Dynamic Trust Management. In *Computers and Communications, 2008. ISCC 2008. IEEE Symposium on*, pages 537–542. IEEE, July 2008. ISBN 978-1-4244-2702-4. doi: 10.1109/iscc.2008.4625768. URL http://dx.doi.org/10.1109/iscc.2008.4625768.

[37] Shaxun Chen, Kai Zeng, and P. Mohapatra. Jamming-Resistant Communication: Channel Surfing without Negotiation. In *Communications (ICC), 2010 IEEE International Conference on*, pages 1–6. IEEE, May 2010. ISBN 978-1-4244-6402-9. doi: 10.1109/icc.2010.5502311. URL http://dx.doi.org/10.1109/icc.2010.5502311.

[38] Eitan Altman, Konstantin Avrachenkov, and Andrey Garnaev. 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, pages 1–12, Berlin, Heidelberg, 2007. Springer-Verlag. ISBN 978-3-540-72708-8. URL http://portal.acm.org/citation.cfm?id=1762949.

[39] Yu-Shun Wang, F. Y. S. Lin, Chi-Hsiang Chan, and Jing-Wei Wang. Maximization of Wireless Mesh Networks Survivability to Assure Service Continuity under Intelligent Attacks. In *Advanced Information Networking and Applications (AINA), 2013 IEEE 27th International Conference on*, pages 583–590. IEEE, March 2013. ISBN 978-1-4673-5550-6. doi: 10.1109/aina.2013.31. URL http://dx.doi.org/10.1109/aina.2013.31.

[40] Y. E. Sagduyu, R. Berry, and Anthony Ephremides. 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*, pages 130–139. IEEE, May 2009. ISBN 978-1-4244-4176-1. doi: 10.1109/gamenets.2009.5137394. URL http://dx.doi.org/10.1109/gamenets.2009.5137394.

[41] Mingyan Li, Iordanis Koutsopoulos, and Radha Poovendran. Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks. *IEEE Transactions on Mobile Computing*, 9(8):1119–1133, April 2010. doi: 10.1109/tmc.2010.75. URL http://dx.doi.org/10.1109/tmc.2010.75.

[42] Kemal Bicakci and Bulent Tavli. Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. *Computer Standards & Interfaces*, 31(5):931–941, September 2009. ISSN 09205489. doi: 10.1016/j.csi.2008.09.038. URL http://dx.doi.org/10.1016/j.csi.2008.09.038.

[43] M. K. Hanawal and E. Altman. Stochastic Geometry based jamming games in Mobile Ad hoc Networks. In *Wireless On-demand Network Systems and Services (WONS), 2012 9th Annual Conference on*, pages 91–98. IEEE, January 2012. ISBN 978-1-4577-1721-5. doi: 10.1109/wons.2012.6152245. URL http://dx.doi.org/10.1109/wons.2012.6152245.