Proceedings of the 2014 Industrial and Systems Engineering Research Conference
Y. Guan and H. Liao, eds.

A Bi-Level Programming Model for the Wireless Network Jamming Placement Problem

Satish Vadlamani[1], Hugh Medal[1], Burak Ekşioğlu [1], Pan Li[2]
[1]Department of Industrial and Systems Engineering,
Mississippi State University, Starkville, MS
[2]Department of Electrical and Computer Engineering,
Mississippi State University, Starkville, MS

Abstract

Wireless networks, used extensively in military applications, are susceptible to jamming attacks. In this paper, we study a network interdiction problem on a multi-hop multi-channel wireless network in which an attacker places jamming devices in order to minimize the expected throughput of the network. We model this problem as a bi-level attacker-defender mixed integer program. The objective of the attacker is to locate a limited number of jamming devices and determine an optimal channel hopping strategy while the defenders objective is to determine an optimal channel hopping strategy. The defender seeks to maximize the equilibrium network throughput, and the attacker seeks to minimize it. In the defender's problem, the attacker and defender play a Nash Equilibrium channel hopping mixed strategy.

Keywords
Wireless networks, network interdiction, jamming, integer programming

1. Introduction

Military strategists are always looking for better ways to protect a communication wireless network from attacks of terrorists. The use of air as a medium for data transfer makes wireless networks susceptible to various attacks. Of these attacks, jamming and denial of service attacks are most commonly occurring and hence are widely studied. The type of attack where the attacker transmit electromagnetic waves using a jamming device, so as to disrupt legitimate transmission is called jamming attack (see section 3 for details). In denial of service attacks, the attacker sends multiple data requests to the nodes in the network. This keeps the network busy continuously, preventing legitimate transmission from being sent through the network. Wireless networks, as the name suggests, are computer or mobile networks that send and receive data without the use of wires. The ease of installation and the added benefit of mobility (e.g., Laptops) within the area covered, make wireless networks very popular, especially in homes [1]. Wireless networks are also used in military applications and disaster situations. There are three main types of wireless networks: Wireless Local Area Network (WLAN), more commonly called Wi-Fi; Wireless Sensor Networks (WSN); and Wireless Ad-Hoc Networks (AHN). Wi-Fi networks are mostly found in homes, coffee shops, malls etc., while WSNs are used for collecting data or information from places where it is difficult for the human to be physically present (e.g., hot deserts) [2]. AHNs are mostly used in military applications and disaster situations [3, 4] where it is not feasible to build an infrastructure for communications. Wireless networks can also be classified as single-hop and multi-hop networks. A network is called single-hop when the data from one node is sent directly to the other node without any intermediate nodes. In a multi-hop network the data is sent from the source node to the destination node via one or more intermediate nodes. This process of sending data from source to destination via intermediate nodes is called hopping. The data is sent through a shared channel between nodes. In wireless networks, data can often be sent on multiple channels, or bands of frequency. A wireless network can be a single-channel or a multi-channel network.

In this paper we study the wireless network jamming problem in multi-hop, multi-channel wireless networks. The problem is solved from the attacker's point of view to place jamming devices in such a way that the throughput of the network is minimized. In addition to the jamming placement problem, our model also considers channel hopping, in which the attacker and operator (defender) switch channels randomly. We provide a min-max formulation where the

attacker tries to minimize the throughput and the operator tries to maximize the throughput. We linearize the non-linear terms in min-max formulation and give an integer programming model for calculating the optimal throughput of the network. Numerical experiments of different problem instances are solved using CPLEX solver and the results are reported. The results clearly show the damage jamming attacks can cause to mission critical wireless networks by reducing the throughput of the network.

The rest of the paper is organized as follows: in Section 2 a brief literature review is provided. In Section 3.1 we describe the problem and a mathematical model is provided in 3.2. Section 4 and Section 5 gives the solution and the numerical experiments. A conclusion is provided in Section 6 in the end.

2. Literature Review

The jamming problem has been studied widely in many wireless network settings, including wireless LAN networks [5–7], sensor networks [8, 9], and multihop networks [10, 11]. Other general wireless networks have also received their fair share of attention [12–16].

Commander et. al [17] studied the problem of determining the optimal number and placement of a set of jamming devices in order to neutralize communication of the network. This is known as the Wireless Network Jamming Problem (WNJP). The jamming devices were 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 connects two nodes if they are within a certain communication threshold. 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 model for finding a minimum number of jamming devices needed to meet a certain threshold on the area that can be jammed.

For a system which has multiple channels, the interactions of the transmitter and jamming device is formulated as a game of transmitting randomly over multiple channels [18]. The jamming problem was studied by [19] as an intrusion detection problem. The problem of multi-hop networks with packet forwarding was studied in [10] and [11]. Zorzi et.al [20] and [21] studied jamming problems and showed that a successful transmission by a transmitter depends on the probabilities of choosing the channel via probabilistic capture model.

To the best of our knowledge the WNJP has not been studied in wireless multi-hop, muti-channel networks. In this paper we formulate the WNJP as a network interdiction problem, using directional antennas instead of the omni-directional antennas used in Commander et. al [17]. We also model random channel selection for both the jammer and the operator.

3. Problem Description and Mathematical Model

Before we describe the problem, we will define some of the important terms needed to better understand the problem:

- ***Jamming Attacks:*** The act of deliberately transmitting electromagnetic waves to a wireless network with the intention of disrupting or forestalling the legitimate transmission of the network is called a jamming attack. The word "jammer" is used to denote a device or an adversary with a device emitting electromagnetic waves to disrupt the network. In WSN and AHN the jammer disrupts the legitimate transmission by using the same radio frequency or the same channel that the legitimate nodes in the network use. Since WSN and AHN are mostly used in military applications and disaster situations where the data or information is critical, jamming attacks can prove to be a serious threat. The higher the power of the jammer, the greater the damage to the network. However, there is a maximum limit on how much power the jammer can use.
- ***Constant Jammer:*** In this paper we study multi-hop wireless networks like AHN and WSN under the attack of a constant jammer. A constant jammer is a type of jammer which continuously emits electromagnetic waves or random sequences of bits through the channel. If the channel on which the jammer transmits is same as that of the nodes in the network, the channel is jammed, reducing the throughput on that channel.
- ***Channel Hopping:*** The attacker and operator choose channels with a particular probability to disrupt the network and to evade the jamming attack respectively. Once a channel is chosen all the power of the jammer is used on that channel to disallow the legitimate flow of data through that channel. The operator tries to change the channels to evade jamming and this technique has proved to be effective [22]. In this paper we assume that the jammer and operator do not have information about each other's channel access probabilities as in [8]. In

such a case, when there is no channel access information, the operator and jammer choose each channel with the same probability to reduce maximum damage and to cause maximum damage, respectively [8].

- ***Directional Antennas:*** Directional antennas used in wireless networks transmit and receive signal only from one direction. Noubir [23] proposed the use of directional antennas in AHN to reduce the effect of jamming attacks. The other more commonly used antennas in the literature are the omni-directional antennas. Unlike directional antennas, omni-directional antennas transmit and receive data from all directions. So, the use of directional antennas reduce interference from other concurrent transmission around it because it only transmits and receives in the direction of the other node. In this paper we assume that the nodes in the network use directional antennas. In other words, each node has as many directional antennas as the number of other nodes it is communicating with. This assumption of the operator using directional antennas is justifiable because in military applications, the position and direction of nodes (e.g. laptop, cell phone) is planned ahead of time. On the other hand, we assume that the jammer uses omni-directional antennas to maximize the range of damage it can cause. For a jammer to jam communication between two nodes using directional antennas, the jammer has to be located exactly in the direction of the receiving or transmitting directional antenna of the node.
- ***Signal to Interference plus Noise Ratio (SINR):*** Signal to interference plus noise ratio is defined as the ratio of the power of the signal of interest to the power of the interference from all other signals including the power from all the other nodes in the network transmitting, the power of the jammer transmitting and the white noise in the network. The higher the value of SINR the better the quality of the signal received and hence the operator would like to increase the, SINR. The jammer on the other hand will try to increase the interference, thereby decreasing the SINR and hence disrupting the network.
- ***Throughput:*** In computer networks throughput is defined as the average rate of successfully transmitting data over a channel used in communication. The throughput is measured in bits/sec.

3.1 Problem Description

In wireless multi-hop networks, the data travels from the source node to the destination via multiple intermediate nodes. The jammer places the devices in locations such that the entire networks is rendered useless. Figure 1 shows a wireless multi-hop, multi-channel network with six nodes; with node 1 as the source, and 6 the destination, and all other nodes as intermediate nodes. The main purpose of the intermediate nodes is to relay data sent from the source to the destination without sending data of their own. The figure shows three channels denoted by solid, dotted and dashed lines each of different frequency 2.41 GHz, 2.42 GHz, and 2.40 GHz respectively. The triangles on arcs (1,2) and (1,4) represents the location of jamming devices. We assume that all nodes use directional antennas and hence the jamming devices have to be placed in the direction of transmission from node 1 to node 2. We assume that there is no concurrent transmission from the other nodes in the network, i.e., there is only one source node and one destination node. It can be seen that jamming the arcs going out of the source node or jamming the arcs going into the destination node will jam the entire network. The objective of the jammer is to place the jamming devices on the arcs such that throughput of the network is minimized. The objective of the operator is to maximize the throughput of the network. We assume that jammer can place the jamming device at midpoint of the arc between two nodes. There is also a limit on the number of jamming devices that are available. The operator and jammer play a zero-sum simultaneous channel hopping game, and at equilibrium both select a channel with equal probability, i.e., in Figure 1 the probability of the operator selecting a channel is $\frac{1}{k} = \frac{1}{3}$, where k is the number of channels. The channel hopping probability helps the operator to still use the network for transmitting data by choosing a channel different from the one used by the jammer. The operator uses channel hopping only for the arcs under jamming attack. The jammer and the operator can transmit data only on one channel at any given time. We assume that the attacker and the operator do not know each other's channel hopping probabilities, thus, the channel hopping can be modeled as a simultaneous game in choosing channels. The mixed strategy Nash Equilibrium of the game is that both the jammer and the operator select channels with equal probabilities. So the probability for each player to choose a channel in Figure 1 is $\frac{1}{3}$. A game theorist typically uses a set of elements, along with a solution 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, this equilibrium is known as Nash equilibrium [24]. The probability of the operator and the jammer choosing a channel are independent, and hence the probability of a channel being jammed is $\frac{1}{3^2}$ and the probability of a channel not being jammed is $1 - \frac{1}{3^2} = \frac{8}{9}$.

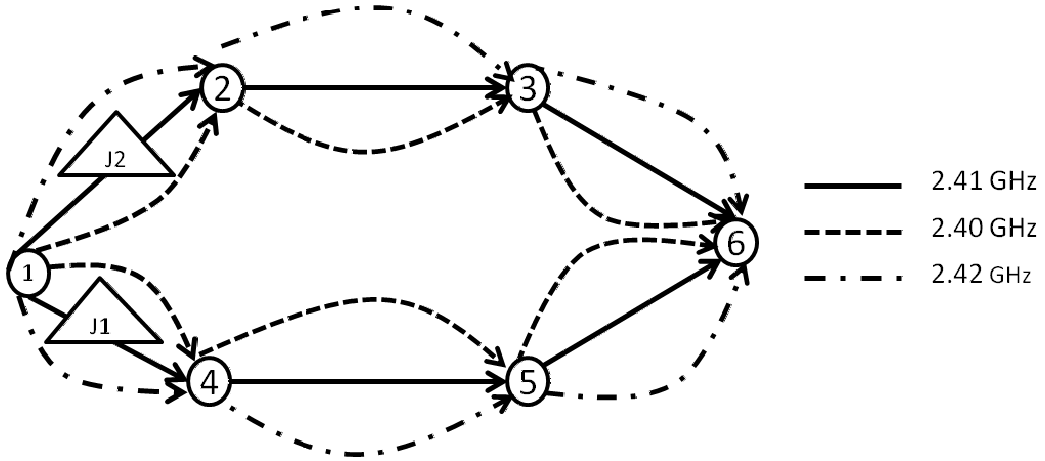

Figure 1: Example of jamming in a network.

3.2 Mathematical Model

The objective of the operator is to maximize the throughput of the network and the objective of the jammer is to minimize the throughput of the network. Wood [25] proposed a network interdiction problem for the flow of drugs in the South America. They provide a $\min-\max$ formulation in which the enemy tries to maximize the flow and the drugs while the interdictor tries to minimize the flow by interdicting the drugs flow. In this paper the jammer tries to interdict and minimize the flow of the legitimate data by placing jamming devices in the network while the military or operator tries to maximize the flow by channel hopping. We present a $\min-\max$ formulation. Given a directed graph $G=(V,A)$, the data from the source node s flows to the sink node d via intermediate nodes. The data is sent using electromagnetic waves via air from one node to another. The binary data consisting of ones and zeros are converted to electromagnetic waves and transmitted using a directional antenna, in the direction of the next node. Electromagnetic waves attenuate in free space at a rate $\frac{1}{t_{ij}^2}$, where t_{ij}, is the distance between nodes i and j in the network. The electromagnetic waves from the jamming device ℓ and node j also attenuates in free space with the rate $\frac{1}{t_{\ell j}^2}$, where $t_{\ell j}$, is the distance between jamming device ℓ and node j in the network. The power p_{ij} is the power of node i received at node j and is given by:

$$p_{ij} = \frac{\lambda}{t_{ij}^2} \tag{1}$$

where $\lambda \in \mathbb{R}$ is a proportionality constant; and without loss of generality, we set $\lambda = 1$. The power $p_{\ell j}$ between jamming device ℓ and node j can be calculated using Equation (1) by replacing i with ℓ. The SINR for a given channel is given by :

$$SINR_{ij} = \frac{p_{ij}}{I_j + v} \tag{2}$$

where I_j is the total interference from all other concurrent transmissions from the jamming device ℓ received at node j and is given by

$$I_j = \sum_{\ell, j \in A} p_{\ell j} \tag{3}$$

v is the white noise in the channel. The throughput of the channel used in communication is given by the Shannon's rate [16]:

$$C_{ij} = B(\log(1 + SINR_{ij})) \tag{4}$$

where C is the maximum theoretical throughput of the channel and B is the bandwidth of the channel measured in Hertz. In the presence of a jammer, the throughput decreases because jammer increases the noise. We assume that the bandwidth $B = 1\ Hertz$. We fixed the power values for the signal and the interference from the jammer at 5 $Watts$ each. The values of v is fixed to be a very small value close to zero. Let u_{ij} be the throughput of a non-jammed

channel $(i, j) \in A$ between nodes i and j as is calculated using Equation (4) with I_j=0. Let w_{ij} be the throughput of the jammed the channel (i, j), and is calculated using Equation (4) with I_j given by Equation (3). Here, $i, j \in V$ and $i, j = 1, 2, 3, ...m$, m is the total number of nodes in the network. Let q_{ij} be the expected throughput of a channel between (i, j), given arc (i, j) is not jammed. There is no channel hopping when there the arc is not jammed and hence q_{ij}=u_{ij}. Let v_{ij} be the expected throughput of an arc between (i, j) given arc (i, j) is jammed. Let s_{ij}=ku_{ij} be expected throughput of the arc between (i, j). The expected throughput v_{ij} for a mixed strategy Nash Equilibrium channel hopping game between the operator and attacker is given by $v_{ij} = (1 - \frac{1}{k^2})u_{ij} + \frac{1}{k^2}w_{ij}$, where k is the number of channels. The min − max mathematical model is shown in *Model*1.

Model 1:

$$\min_{\gamma} \max_{x} \quad x_{ds} \tag{5}$$

$$\text{s.t.} \quad \sum_j x_{sj} - \sum_j x_{js} - x_{ds} = 0 \tag{6}$$

$$\sum_j x_{ij} - \sum_j x_{ji} = 0 \ \forall i \in V \backslash \{s, d\} \tag{7}$$

$$\sum_j x_{dj} - \sum_j x_{jd} + x_{ds} = 0 \tag{8}$$

$$x_{ij} - s_{ij}(1 - \gamma_{ij}) - v_{ij}\gamma_{ij} \leq 0 \ \forall (i, j) \in A \tag{9}$$

$$\sum_{(i,j)\in A} \gamma_{ij} \leq n \tag{10}$$

$$x_{ij} \geq 0 \ \forall (i, j) \in A \cup \{(d, s)\} \tag{11}$$

$$\gamma_{ij} \in \{0, 1\} \ \forall (i, j) \in A \tag{12}$$

where x_{ij} is the flow on the arc (i, j) and γ_{ij} is 1 if a jammer is located on arc (i, j) and 0 otherwise. The objective function is to minimize the expected throughput of the network from the attackers perspective, and maximize the throughput from the operator's perspective. The internal max problem is the max flow problem objective. In the classic max flow problem, the objective is to maximize the flow possible through a capacitated graph. This can be thought of as the objective of the operator, to flow maximum data in the capacitated graph. Equations (6-8) are the flow balance constraints of the max flow problem. Let α_s, α_d and α_j ($j \neq s, d$) be the dual variables associated with Equations (6-8), respectively. We assume that the attacker has a limited number of jamming devices denoted as n in Equation (10). Let θ_{ij} be the dual variable associated with Equation (9), $(i, j) \in A$. We can write the dual of the internal maxflow problem as shown in *Model*2.

Model 2:

$$\min_{\gamma} \min_{\alpha,\theta} \quad \sum_{(i,j)\in A} s_{ij}(1 - \gamma_{ij})\theta_{ij} - v_{ij}\gamma_{ij}\theta_{ij} \tag{13}$$

$$\text{s.t.} \quad \alpha_i - \alpha_j + \theta_{ij} \geq 0 \ \forall (i, j) \in A \tag{14}$$

$$-\alpha_s + \alpha_d \geq 1 \tag{15}$$

$$\sum_{(i,j)\in A} \gamma_{ij} \leq n \tag{16}$$

$$\alpha_i \in \{0, 1\} \ \forall i \in V \tag{17}$$

$$\theta_{ij} \in \{0, 1\} \ \forall (i, j) \in A \tag{18}$$

Equation (13) in *Model*2 has a non linear term $\gamma_{ij}\theta_{ij}$, we linearize this equation by replacing $\beta_{ij} = \gamma_{ij}\theta_{ij}$ and adding related constraints to the model. *Model*3 shown below is the linearized form of *Model*2:

Model 3:

$$\min \quad \sum_{(i,j)\in A} s_{ij}\theta_{ij} - s_{ij}\beta_{ij} - v_{ij}\beta_{ij} \tag{19}$$

$$\text{s.t.} \quad \alpha_i - \alpha_j + \theta_{ij} \geq 0 \ \forall (i,j) \in A \tag{20}$$

$$-\alpha_s + \alpha_d \geq 1 \tag{21}$$

$$\beta_{ij} \leq \gamma_{ij} \tag{22}$$

$$\beta_{ij} \leq \theta_{ij} \tag{23}$$

$$\beta_{ij} \geq \theta_{ij} + \gamma_{ij} - 1 \tag{24}$$

$$\sum_{(i,j)\in A} \gamma_{ij} \leq n \tag{25}$$

$$\alpha_i \in \{0,1\} \ \forall i \in V \tag{26}$$

$$\theta_{ij}, \beta_{ij}, \gamma_{ij} \in \{0,1\} \ \forall (i,j) \in A \tag{27}$$

Equation (25) sets the upper limit on the number of jamming devices that can be placed in the network. Equations (21-23) are the linearization constraints.

4. Solution Approach

In this section we discuss the solution methodology. Consider a graph with one source node, one destination and nine other intermediate nodes as shown in Figure 2. This graph is the optimal solution obtained by solving $Model3$ using a commercial solver CPLEX for a graph with 9 intermediate nodes, 2 jammers, 3 arcs and 3 channels. The source node has three arcs $(0,1)$, $(0,2)$, $(0,3)$ connecting to nodes 1, 2, and 3. We assume that there are three channels between every node pair. The attacker can place a maximum of two jammers in the network to minimize the throughput. The operator and the attacker strategies are modeled as a mixed strategy Nash Equilibrium channel hopping sequential zero sum game. The operator and attacker both use their Nash equilibrium channel hopping probabilities of $\frac{1}{k}$=$\frac{1}{3}$. We assume that the jammer and the nodes in the network transmit with a power of 5 *Watts*. The signal to interference noise ratio is given by Equation (2). The numerator is the signal strength (i.e., 5 *Watts*), while the denominator is the interference caused by the jammer placed in the direction of the signal being sent from one node to another is also 5 *Watts*. In the absence of jamming, the denominator value of the jammer power is zero. The value of the noise that exists in the channel in the presence and absence of a jammer is a very small close to zero. The throughput of a channel can be calculated by Equation (4). The operator's objective is to maximize the throughput of the network and the jammer objective to minimize the throughput are considered by $Model3$. If there are multiple arcs going out of a node, even if the jammer is placed on one arc, the data is transferred through the other arc. Using multiple channels allow the operator to reduce the effect of jamming attack by choosing a different channel (see channel hopping above). The optimal solution for a jammer is to jam either the arcs going out of the source or the arcs going in to the destination node to cause maximum damage by reducing the throughput. From optimal solution shown in Figure 2, the jammer places the jamming devices on the arcs $(0,1)$ and $(0,2)$ and is denoted by dotted lines. But since the network has a node degree of three , the throughput of the network is not reduced greatly as the operator can use the other arc $(0,3)$ (denoted by a solid line to show non jammed arc) arc to send data.

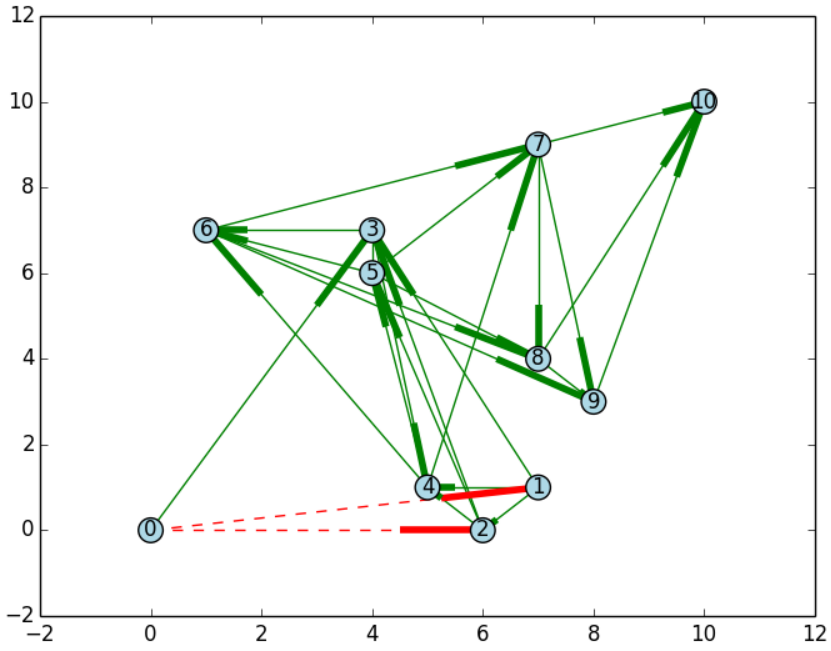

Figure 2: Jamming in a network of 9 intermediate node.

5. Numerical Experiments

In order to demonstrate the advantages of the proposed model (*Model*3) to solve the network interdiction of wireless networks, we provide some case studies. The experiments were performed on a computer with a 2.5 *GHz* Intel i7 processor with 8 Gb RAM, Microsoft Windows 7 operating system. The problems are solved using a commercial solver CPLEX 12.5. We assume that the strategists can locate nodes randomly in a given area.We generate random graphs of 3, 4, and 9 intermediate nodes. Random graph topology can be justified by the fact that in military applications, the military strategist (operators) do not have well established infrastructure to locate the wireless devices, for communication. The operator has to locate wireless devices in feasible areas. The source node and destination node have fixed locations and the other intermediate node locations are generated randomly. For example, in the case where there are 9 intermediate nodes in the network, the source node is located at coordinate $(0,0)$ and the destination node at coordinate $(10,10)$, the rest of intermediate nodes are randomly located at coordinates in the area divided into a grid of 10 x10. Five replications for each of the problem instances were run and the average throughput of the five runs is reported. The running time of all the experiments are less than 1 sec and hence are not reported. Table 1, Table 2, and Table 3 show the optimal solution for 3, 5 and 9 intermediate nodes with different values of jammers, channels, and the node degree. The number of jammers are always strictly less than number of arcs from each node, this is to make sure that the jammers are not placed on all the nodes going out of the source node which otherwise would make the problem trivial.

Table 1: 3 Intermediate Nodes

No. Intermediate Nodes	No. Jammers	Arcs from each node	No. Channels	Average of 5 Replications
3	1	2	1	161.47
3	1	2	2	279.85
3	1	2	3	301.96
3	1	3	1	321.08
3	1	3	2	437.93
3	1	3	3	461.05
3	2	3	1	162.89
3	2	3	2	399.27
3	2	3	3	442.47

Table 2: 5 Intermediate Nodes

No. Intermediate Nodes	No. Jammers	Arcs from each node	No. Channels	Average of 5 Replications
5	1	2	1	162.92
5	1	2	2	279.37
5	1	2	3	300.47
5	1	3	1	317.67
5	1	3	2	437.07
5	1	3	3	459.59
5	2	3	1	161.21
5	2	3	2	398.41
5	2	3	3	441.33

Table 3: 9 Intermediate Nodes

No. Intermediate Nodes	No. Jammers	Arcs from each node	No. Channels	Average of 5 Replications
9	1	2	1	158.22
9	1	2	2	277.76
9	1	2	3	299.92
9	1	3	1	317.22
9	1	3	2	436.31
9	1	3	3	460.17
9	2	3	1	159.13
9	2	3	2	394.07
9	2	3	3	438.48

From the experimental results shown above, it is clear that as the number of arc out of a node increase, the throughput of the network also increases and this is intuitive because more arcs provide alternate paths for the the maxflow problem. We can also see that as the number of channels increases the throughput also increases, this result is also intuitive because as the number of channels increase, the probability of jamming the channel which the nodes uses to transmit data is reduced. It is also observed that irrespective of the number of intermediate nodes $(3,5,9)$ if the number of jammers increase the throughput of the network reduces. For example in the case of 9 intermediate nodes with no jamming attack, 3 arcs, and 3 channels the throughput of the network is 474.79 $bits/sec$. The throughput for the problem instance with 9 intermediate nodes, 1 jammer, 3 arcs, and 3 channels is 460.17 $bits/sec$, i.e., the reduction in throughput of the network is about 4%. The throughput for 9 intermediate nodes, 2 jammers, 3 arcs, and 3 channels (see Table 3), obtained by solving $Model3$, is 438.48 $bits/sec$. From this it is clear by having two jammer in place, the attacker can reduce the throughput of the network by 7%. In military and disaster situations where data transferred is very important reduction in throughput can be critical and prove to be dangerous.

6. Conclusion

In this paper, we model a jamming problem as a network interdiction problem with the aim of locating jamming devices in a way such that the throughput of the network is minimized from the jammer perspective. The operator's objective is to maximize the throughput of the network by changing the channels to send data. We model this as an attacker-operator mixed strategy Nash Equilibrium channel hopping game. We see that with the increase in the number of channels, the throughput of the network increases, but if the number of jamming devices increase the attacker can reduce the throughput considerably. In the future work, we will consider the effect of having different power levels of transmission by the attacker and the jammer rather than the constant values as considered in this work. We will also develop better techniques for the operator to evade jamming and increase the throughput of the network in the presence of jamming. We will also provide efficient heuristics to solve problems with larger networks.

References

[1] Geier, J., 2004, "The state of wireless LANs. Technical report,"

[2] Mpitziopoulos,A., Gavalas,D.,Konstantopoulos,C., and Pantziou.G.,2009, "A survey on jamming attacks and coun- termeasures in WSNs," Communications Surveys and Tutorials, IEEE,11(4),42-56.

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

[4] Zhou,L., and Haas,Z.J.,1999," Securing ad hoc networks,"Network, IEEE, 13(6),24-30.

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

[6] Gupta,V., Krishnamurthy,S., and Michalis,F.,2002., " Denial of service attacks at the MAC layer in wireless ad hoc networks,"Proceedings in MILCOM,IEEE, October, vol 2, 1118-1123.

[7] Kyasanur,P., and Vaidya,N.F.,2003," Detection and handling of MAC layer misbehavior in wireless net- works," Proceeding In Dependable Systems and Networks, Proceedings,International Conference on,IEEE,June,173-182.

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

[9] Xu,W.,Trappe,W.,Zhang,Y., and 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,New York, NY, USA,46-57.

[10] Theodorakopoulos,G., and Baras,J.S.,2008, "Game Theoretic Modeling of Malicious Users in Collaborative Networks,"Selected Areas in Communications, IEEE Journal on, September,26(7),1317-1327.

[11] Zander,J.,1991,"Jamming in slotted ALOHA multihop packet radio networks,"Communications, IEEE Transactions on, October,39(10),1521-1531.

[12] Altman,E.,Avrachenkov,K., and 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 Berlin,1-12.

[13] Awerbuch,B.,Richa,A., and 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,ACM, New York, NY, USA,45-54.

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

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

[16] Sagduyu,Y.E., and Ephremides,A.,2007, "SINR-based MAC Games for Selfish and Malicious Users," In Proceeding Information Theory and Applications Workshop, January.

[17] Commander,C.W.,Pardalos,P.M., Ryabchenko,V., Uryasev,S., and Zrazhevsky,G., 2007, "The wireless network jamming problem," Journal of Combinatorial Optimization, 14(4),481-498.

[18] Pelechrinis,K., Koufogiannakis,C., and 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,IEEE Press,Piscataway, NJ, USA,187-196.

[19] Alpcan,T., and Basar,T.,2004, "A game theoretic analysis of intrusion detection in access control systems," In Decision and Control,CDC, 43rd IEEE Conference on, December,volume 2,1568-1573.

[20] Zorzi,M., and Rao,R.R.,1994, "Capture and retransmission control in mobile radio," Selected Areas in Communications, IEEE Journal on, October, 12(8),1289-1298.

[21] Nguyen,G.D.,Ephremides,A., and Wieselthier,J.E., 2006, "On Capture in Random-Access Systems," In Information Theory,IEEE International Symposium on, July, 2072-2076.

[22] Chen,S., Zeng,K., and Mohapatra,P.,2010,"Jamming-Resistant Communication: Channel Surfing without Negotiation," In Communications (ICC), IEEE International Conference on,May,1-6.

[23] Noubir,G.,2004, "On Connectivity in Ad Hoc Networks under Jamming Using Directional Antennas and Mobility," In International Conference on Wired /Wireless Internet Communications, Lecture Notes in Computer Science, volume 2957,Springer Berlin Heidelberg,186-200.

[24] Myerson,R.B.,1997, Game Theory: Analysis of Conflict. Cambridge, Mass.: Harvard Univ.,Print.

[25] Wood,R.K., 1993, "Deterministic network interdiction," Mathematical and Computer Modelling, January, 17(2), 1-18.