Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks

Mingyan Li
Network Security Laboratory
Dept. of Electrical Engineering
University of Washington
and Boeing Phantom Works
Seattle, Washington

Iordanis Koutsopoulos
Dept. of Computer and
Communication Engineering
University of Thessaly
Volos, Greece
jordan@uth.gr

Radha Poovendran
Network Security Laboratory
Dept. of Electrical Engineering
University of Washington
Seattle, Washington
rp3@u.washington.edu

***Abstract*— We consider a scenario where a sophisticated jammer jams an area in a single-channel wireless sensor network. The jammer controls the probability of jamming and transmission range to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by a monitoring node in the network, and a notification message is transferred out of the jamming region. The jammer is detected at a monitor node by employing an optimal detection test based on the percentage of incurred collisions. On the other hand, the network computes channel access probability in an effort to minimize the jamming detection plus notification time. In order for the jammer to optimize its benefit, it needs to know the network channel access probability and number of neighbors of the monitor node. Accordingly, the network needs to know the jamming probability of the jammer. We study the idealized case of perfect knowledge by both the jammer and the network about the strategy of one another, and the case where the jammer or the network lack this knowledge. The latter is captured by formulating and solving optimization problems, the solutions of which constitute best responses of the attacker or the network to the worst-case strategy of each other. We also take into account potential energy constraints of the jammer and the network. We extend the problem to the case of multiple observers and adaptable jamming transmission range and propose a intuitive heuristic jamming strategy for that case.**

I. Introduction

The fundamental characteristic of wireless networks that renders them vulnerable to attacks is the broadcast nature of their medium. This exposes them to passive and active attacks, which are different in their nature and objectives. In the former, a malicious entity does not take any action except passively observing ongoing communication, e.g. eavesdropping so as to intervene with the privacy of network entities involved in the transaction. On the other hand, an active attacker is involved in transmission as well. Depending on attacker objectives, different terminology is used. If the attacker abuses a protocol with the goal to obtain performance benefits itself, the attack is referred to as misbehavior. If the attacker does not directly manipulate protocol parameters but exploits protocol semantics and aims at indirect benefits by unconditionally disrupting network operation, the attack is termed jamming or Denial-of-Service (DoS), depending on whether one looks at its cause or its consequences.

Misbehavior stems from the selfish inclination of wireless entities to improve their own derived utility to the expense of other nodes' performance deterioration, by deviating from legitimate protocol operation at various layers. The utility is expressed in terms of consumed energy or achievable throughput on a link or end-to-end basis. The first case arises if a node denies to forward messages from other nodes so as to preserve battery for its own transmissions. The latter case occurs when a node prevents other nodes from accessing the channel [1] or from routing messages to destinations by selfish manipulation of the access control and routing protocol respectively. The work in [2] focuses on optimal detection in terms of number of required observations to derive a decision for the worst-case access layer misbehavior strategy out of the class of strategies that incur significant performance losses. The framework captured uncertainty of attacks and the case of intelligent attacker that can adapt its policy to delay its detection.

Jamming can disrupt wireless transmission and can occur either unintentionally in the form of interference, noise or collision at the receiver side or in the context of an attack. A jamming attack is particularly effective since (i) no special hardware is needed in order to be launched, (ii) it can be implemented by simply listening to the open medium and broadcasting in the same frequency band as the network and (iii) if launched wisely, it can lead to significant benefits with small incurred cost for the attacker. With regard to the machinery and impact of jamming attacks, they usually aim at the physical layer and are realized by means of a high transmission power signal that corrupts a communication link or an area. Conventional defense techniques against physical layer jamming rely on spread spectrum, which can be too energy-consuming to be widely deployed in resource-constrained sensors. Jamming attacks also occur at the access layer; an adversary either corrupts control packets or reserves the channel for the maximum allowable number of slots, so that other nodes experience low throughput by not being able to access the channel [3]. The work in [4] studies the problem of a legitimate node and a jammer transmitting to a common receiver in an on-off mode in a game-theoretic framework. Other jamming attacks influence the network layer by ma-

licious packet injection along certain routes or the transport layer (e.g. SYN message flooding). In [5] attacks in computer networks are detected by observing the IP port scanning profile prior to the attack and by using sequential detection techniques. The work [6] uses controlled authentication to detect spam message attacks and presents a distributed scheme for the trade-off between attack resilience and computational cost.

Sensor networks are susceptible to jamming attacks since they rely on deployed miniature energy-constrained devices to perform a certain task without a central powerful monitoring point. Wood *et.al* [7] provide a taxonomy of DoS attacks for sensor networks from the physical up to the transport layer. The authors in [8] present attacks aimed at sensor network protocols and are based on learning protocol semantics such as temporal packet arrangement, slot size or preample size. In [9], low-energy attacks are analyzed, which corrupt a packet by jamming only a few bits, such that the code error correction capability is exceeded. Low Density Parity Check (LDPC) codes are proposed as a method to defend against these attacks. The work in [10] considers passing attack notification messages out of a jammed region by creation of wormhole links between sensors, one of which resides out of the jammed area. Links are created through frequency hopping over a channel set either in a predetermined or in an ad-hoc fashion. In [11], four types of jammers, namely constant, deceptive, random, and reactive jammer are studied. The authors use empirical methods based on signal strength and packet delivery ratio measurements to detect jamming. In [12], various countermeasures against jamming are assessed. Channel surfing involves on-demand frequency hopping in case of an attack and spatial retreat refers to moving away from jamming region. The case of an attacker that corrupts broadcasts from a base station (BS) to a sensor network is considered in [13]. The interaction between the attacker and the BS is modeled as a zero-sum game in which the attacker selects the number of sensors to jam and the BS chooses the sample rate of sensor status.

In this paper we study controllable jamming attacks that are easy to launch and difficult to detect and confront, since they differ from brute force attacks. The jammer controls probability of jamming and transmission range in order to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by the network, namely by a monitoring node, and a notification message is transferred out of the jamming region. The fundamental tradeoff faced by the attacker is the following: a more aggressive attack in terms of higher jamming probability or larger transmission range increases the instantaneously derived payoff but exposes the attacker to the network and facilitates its detection and later on its isolation. In an effort to withstand the attack and alleviate the attacker benefit, the network adapts channel access probability. The necessary knowledge of the jammer in order to optimize its benefit consists in knowledge about the network channel access probability and number of neighbors of the monitor node. Accordingly, the network needs to know the jamming probability. With this work, we contribute to existing literature as follows: (i) We derive the optimal attack and defense strategies as solutions to optimization problems that are faced by the attacker and the network respectively by including in the formulation energy limitations, (ii) for attack detection, we provide an optimal detection test that derives decisions based on the measurable percentage of incurred collisions, (iii) we include in the formulation attack detection and transfer of the attack notification message out of the jammed area, (iv) we formulate optimization problems that capture the impact of available knowledge of the attacker and the network about the strategies of each other. For the case of lack of knowledge, the attacker and the network respond optimally to the worst-case strategy of the other, (v) we extend the basic model to the case of multiple monitoring nodes and varying jamming transmission range and suggest a simple efficient jamming strategy. In the sequel, we use the equivalent terms "attacker", "adversary" and "jammer" to refer to the malicious node. The rest of the paper is organized as follows. In section II, we state our network and adversary models, and describe the jamming detection mechanism. In section III, we formulate jamming and defense problems and derive the optimal solutions. We conclude our paper in section IV.

II. Modeling Assumptions

A. Sensor network model

We consider a wireless sensor network deployed over a large area and operating under a single-carrier slotted Aloha type access control protocol. We assume symmetric transmission, namely a node i can receive signal from node j if and only if node j can receive signal from i. The network is represented by an undirected graph $G = (S, E)$ where S is the set of sensor nodes and E is the set of edges. Time is divided into time slots and the slot size equals the size of a packet. All nodes are assumed to be synchronized with respect to slot boundaries. Each node transmits with a fixed power level P with an omni-directional antenna and its transmission range R and sensing range R_s are circular with sharp boundary. Transmission and sensing ranges are defined by two thresholds of received signal strength. A node within transmission range of node i can correctly decode messages from i, while a node within sensing range can just sense activity due to higher signal strength, but cannot decode a message. Typically, R_s is a small multiple of R ranging from 2 to 3. A node within distance R of a node i is called neighbor of i, and the neighborhood of i, $\mathcal{N}_i$ is the set of all neighbors of i. Also, $n_i = |\mathcal{N}_i|$ is the size of i's neighborhood. Transmissions from a node i are received by all its neighbors. Sensor nodes are uniformly distributed in a region with spatial density ρ nodes per unit area and the topology is static, i.e, we assume no mobility. Each node has an amount of energy E.

Each node has one transceiver, so that it cannot transmit and receive simultaneously. All nodes are assumed to be continuously backlogged, so that there are always packets in each node's buffer in each slot. Packets can be either generated by higher layers of a node or come from other

nodes and need to be forwarded, or they may result from previous unsuccessful transmission attempts due to collision and need to be retransmitted. A transmission on edge (i,j) is successful if and only if no node in $\mathcal{N}_j \cup \{j\} \setminus \{i\}$ transmits during that transmission. In this work, we consider the class of multiple access protocols that are characterized by a common channel access probability γ for all nodes in a slot. Each node i uses uni-cast transmission and chooses the destination equally likely, that is, the probability that a packet is transmitted to $j \in \mathcal{N}_i$ is γ/n_i. Provided that it remains silent in a slot, a receiver node j experiences collision if at least two nodes in its neighborhood transmit simultaneously, regardless of whether the transmitted packets are destined to node j or to other nodes. Hence, the probability of collision at node j in a slot is $\theta_0 = 1 - \Pr\{\text{only one or no neighbor transmits}\} = 1-(1-\gamma)^{n_j} - n_j\gamma(1-\gamma)^{n_j-1}$. If node j attempts to transmit at a slot while it receives a message, a collision occurs as well. In that case, the receiver cannot find out whether the collision is due to its own transmission, or it would occur anyway. Hence, in the sequel, collision will refer to the case of multiple simultaneous transmissions to a node and no transmission attempt by that node. Whenever packet collision occurs at a receiver, the packet is retransmitted in the next slot if the transmitter accesses the channel again. If a node does not have any neighbors, i.e $n_j = 0$, this node does not receive any packets and does not experience collisions.

B. Attacker model

We consider one attacker in the area, which is not authenticated and associated with the network. The objective of the jammer is to corrupt transmissions of legitimate nodes by causing packet collisions at receivers. Intentional collision leads to retransmission and thus additional energy consumption for a certain amount of throughput, or equivalently reduced throughput for a given amount of consumed energy.

Upon sensing the channel, the attacker transmits a small packet which collides with legitimately transmitted packets at their intended receivers. As argued in [9], a jammer beacon packet of a few bits suffices to disrupt a transmitted packet in the network. The jammer is assumed to have energy resources E_m, but the corresponding constraint in the optimization problems of the next section can be considered redundant if the jammer adheres to the aforementioned policy. The jammer uses an omni-directional antenna with circular sensing range R_{ms} and adaptable transmission range R_m, realized by controlling transmission power P_m. The jammer also controls the probability q of jamming the area within its transmission range in a slot, thus controlling the aggressiveness of the attack. The attack space is specified by $\mathcal{P} \times (0,1)$, where $\mathcal{P}$ is a discrete set of power levels. The attacker attempts to strike a balance between short and long-term benefits in the following sense: an aggressive attack increases instantaneous benefit at the risk of being detected faster, while a mild attack may prolong the detection time.

Collision occurs at node i if the jammer jams and at least a neighbor transmits. The probability of a collision at node i is

$$\begin{aligned}\theta_1 &= 1 - \Pr\{\text{no neighbor transmits}\} - \\ &\quad \Pr\{\text{one neighbor transmits while adversary does not}\} \\ &= 1 - (1-\gamma)^{n_i} - (1-q)n_i\gamma(1-\gamma)^{n_i-1}.\end{aligned}$$

If jamming occurs without sensing, the collision probability is

$$\begin{aligned}\theta_1' &= (1 - Pr\{\text{no neighbor transmits}\})q + \theta_0(1-q) \\ &= \theta_0 + qn_i\gamma(1-\gamma)^{(n_i-1)} = \theta_1\end{aligned}$$

Thus, the probability of collision is the same regardless of whether the jammer senses the channel before jamming. This implies that jamming can be viewed as multiple access among a network of ν legitimate nodes, each with access probability γ and the jammer with access probability q. Nevertheless, by using sensing, the adversary does not waste energy on empty slots and conserves transmission energy by a factor of $1-(1-\gamma)^{\nu}$. For large ν, $1-(1-\gamma)^{\nu} \approx 1$, which means that in a dense sensor network, it is very likely that some transmission occurs at each time. Note however that energy expenditure due to sensing is non-negligible [11]. In the sequel, we will not consider the energy saving factor $1-(1-\gamma)^{\nu}$.

We focus on different cases of attacker knowledge about the network, such as full knowledge about network parameters such as access probability γ and neighborhood size of a monitor node or no such knowledge. Different instances of network knowledge about the attacker strategy will be studied as well.

C. Attack detection model

The network employs a monitoring mechanism for detecting potential malicious activity by a jammer. The monitoring mechanism consists of the following: (i) determination of a subset of nodes $\mathcal{M}$ that will act as network monitors, and (ii) employment of a detection algorithm at each monitor node. The assignment of the role of monitor to a node can be affected by energy limitations and detection performance specifications. In this work, we fix $\mathcal{M}$ and formulate optimization problems for one or more monitor nodes.

We now fix attention to detection at one monitor node. First, we define the quantity to be observed at each monitor node. In our case, the readily available metric is probability of collision that a monitor node experiences, namely the percentage of packets that are erroneously received. During normal network operation, and in the absence of a jammer, we consider a large enough training period in which the monitor node "learns" the percentage of collisions it experiences as the long-term average of the ratio of number of slots in which there was a collision over total number of slots of the training period. Assume now the network operates in the open after the training period and fix attention to a time window much smaller than the training period. An increased percentage of collisions over this time window compared to the learned long-term average may be an indication of an ongoing jamming attack or only a temporary increase of percentage of collisions compared to the average during normal network operation. A detection

algorithm takes observation samples obtained at the monitor node (i.e, collision or not collision) and decides whether there exists an attack. On one hand, the observation window should be small enough, such that the attack is detected on time and appropriate countermeasures are initiated. On the other hand, this window should be sufficiently large, such that the chance of a false alarm notification is minimized.

The sequential nature of observations at consecutive time slots motivates use of sequential detection techniques. A sequential decision rule consists of (i) a stopping time indicating when to stop taking observations, and (ii) a final decision rule that decides between the two hypotheses (i.e, occurrence or not of jamming). A sequential decision rule is efficient if it can provide reliable decision as fast as possible. The probability of false alarm P_{FA} and probability of missed detection P_M constitute inherent tradeoffs in a detection scheme, in the sense that a faster decision unavoidably leads to higher values of these probabilities while lower values are attained at the expense of detection delay. For given values of P_{FA} and P_M, the detection test that minimizes the average number of required observations (and thus the average delay) to reach a decision among all sequential and non-sequential tests for which P_{FA} and P_M do not exceed the predefined values above is Wald's Sequential Probability Ratio Test (SPRT) [14]. When SPRT is used for sequential testing between two hypotheses concerning two probability distributions, SPRT is optimal in that sense as well [15].

SPRT collects observations until significant evidence in favor of one of the two hypotheses is accumulated. After each observation at the k-th stage, we choose between the following options: accept one or the other hypothesis and stop observing, or defer decision and obtain another observation $k+1$. There exist thresholds a and b that aid in the decision. The computed figure of merit at each stage is the logarithm of likelihood ratio of the accumulated sample vector until that stage.

In our case, the test is between hypotheses $\mathbf{H}_0$ and $\mathbf{H}_1$ that involve Bernoulli probability mass functions (p.m.f's) with f_0 and f_1, where f_i, $i = 0, 1$ are defined as p.m.f's:

$$\Pr\{Y = 1\} = \theta_i = 1 - \Pr\{Y = 0\} \tag{1}$$

where $Y = 1$ denotes the event of collision in a slot. That is, $\mathbf{H}_0$ means absence of jamming and thus the corresponding p.m.f f_0 is Bernoulli with parameter θ_0, while $\mathbf{H}_1$ corresponds to jamming with a Bernoulli p.m.f f_1 with parameter θ_1. The logarithm of likelihood ratio at stage k with accumulated samples $x_1, \ldots, x_k$ is

$$S_k = \ln \frac{f_1(x_1, \ldots, x_k)}{f_0(x_1, \ldots, x_k)}, \tag{2}$$

where $f_i(x_1, \ldots, x_k)$ is the joint p.m.f of sequence $(x_1, \ldots, x_k)$ based on hypothesis $\mathbf{H}_i$, $i = 0, 1$. If observation samples are statistically independent, then

$$S_k = \sum_{j=1}^{k} \Lambda_j = \sum_{j=1}^{k} \ln \frac{f_1(x_j)}{f_0(x_j)}\,. \tag{3}$$

The decision is taken based on the following criteria:

$$\begin{aligned} S_k \geq a \quad &\Rightarrow \quad \text{accept } \mathbf{H}_1, \\ S_k < b \quad &\Rightarrow \quad \text{accept } \mathbf{H}_0, \\ b \leq S_k < a \quad &\Rightarrow \quad \text{take another observation.} \end{aligned} \tag{4}$$

Thresholds a and b depend on the specified values of P_{FA} and P_M, as will be explained in the sequel.

The objective of a detection rule is to minimize the number of required observation samples to derive a decision about existence or not of attack. The detection performance is quantified by the average sample number (ASN) $\mathbb{E}[N]$ needed until a decision is reached, where the average is taken with respect to the distribution of the observations. From Wald's identity [14], it is

$$\mathbb{E}[S_N|H_i] = \mathbb{E}[N] \times \mathbb{E}[\Lambda|H_i], \tag{5}$$

where $\mathbb{E}[\Lambda|\mathbf{H}_i]$ is the expected value of the logarithm of likelihood ratio, conditioned on hypothesis $\mathbf{H}_i$. By using a similar derivation as the one in [16], we obtain the inequalities

$$1 - P_M \geq e^a P_{FA} \;\text{ and }\; P_M \leq e^b\,(1 - P_{FA}). \tag{6}$$

When the average number of required observations is very large, the increments Λ_j of the logarithm of likelihood ratio are also small. Therefore, when the test terminates with selection of hypothesis $\mathbf{H}_1$, S_N is slightly larger than a, while when it terminates with selection of $\mathbf{H}_0$, S_N is very close to b. Therefore, the above inequalities hold with good approximation as equalities. Under this assumption, the decision levels a and b that are required for attaining performance (P_{FA}, P_M) are given by

$$a = \ln \frac{1 - P_M}{P_{FA}} \;\text{ and }\; b = \ln \frac{P_M}{1 - P_{FA}}\,. \tag{7}$$

Furthermore, due to the above and [14], [16], it is $\mathbb{E}[S_N|H_1] = aP_D + b(1 - P_D)$, where $P_D = 1 - P_M$ is the probability of detection of SPRT. Hence, the average number of samples needed for detecting jamming is

$$\mathbb{E}[N|\mathbf{H}_1] = \frac{\mathbb{E}[S_N|\mathbf{H}_1]}{\mathbb{E}[\Lambda|\mathbf{H}_1]} = \frac{C}{\theta_1 \log \frac{\theta_1}{\theta_0} + (1 - \theta_1) \log \frac{1-\theta_1}{1-\theta_0}} \tag{8}$$

Observe that the above is a function of q and γ, denoted also by $D(q, \gamma)$.

III. Optimal jamming attack and defense policies as solutions to optimization problems

An aggressive attack, namely one with large q has a large potential to corrupt links in several time slots. Nevertheless, this attack will be detected relatively fast due to the large percentage of incurred collisions. Following detection, a notification message will be passed out of the jammed region and hence it can be assumed that the damage caused to the network is mitigated or ceased. On the other hand, a milder attack, namely one with smaller q may turn out to be more beneficial for the attacker, provided of course that the attacker does not need to jam links urgently. The objective of an adversary is to

increase the total number of corrupted links before the attack is detected and the notification alarm is propagated.

The network performance metric is the number of successful transmissions in each slot, namely the throughput. As a first line of defense the network can select the access probability γ so as to (i) increase the number of successful transmission links under given energy limitations, (ii) "expose" the potentially existing jammer by reducing the number of required samples to make a decision. Another constraint for the network is to maintain a certain minimum throughput in the presence of an attack, if possible.

A. Attacker Payoff

The payoff of the attacker is measured in terms of number of incurred corrupted links. The *instantaneous payoff of the attacker* U_{mI}, is the *average* number of *additionally* corrupted links in a slot, not counting those due to legitimate contention. It depends on jamming probability q and network access probability γ and is denoted as $U_{mI}(q,\gamma)$. In order to obtain an analytic expression for $U_{mI}(q,\gamma)$, we first find the probability of successful transmission in the absence of jamming.

Since nodes are uniformly distributed with spatial density ρ, and each node independently transmits with probability γ at each slot, the transmitters are uniformly distributed with density $\rho\gamma$ and the total number of transmitters in the jammed area $A_m = \pi R_m^2$ is Poisson distributed with spatial density $\lambda = \rho\gamma$ [17]. Since nodes are continuously backlogged and a node cannot transmit and receive at the same time, the potential receivers are uniformly distributed in the same area with density $\rho(1-\gamma)$. Equivalently, in area A the number of transmitters and receivers is Poisson distributed with parameter $A\rho\gamma$ and $A\rho(1-\gamma)$, respectively. A transmission is successful if there is no other transmitter in a receiver's transmission range of area $A = \pi R^2$ and there is at least one receiver in the transmitter's transmission range of area A. The probability of success of an attempted transmission, p_s is

$$\begin{aligned} p_s &= \Pr\{\text{only one transmitter in area } A\} \\ &\quad \times \Pr\{\text{at least one potential receiver in area } A\} \\ &= \rho\gamma A e^{-\rho\gamma A} \times \left(1 - e^{-\rho(1-\gamma)A}\right) \\ &= \rho\gamma A \left(e^{-\rho\gamma A} - e^{-\rho A}\right). \end{aligned}$$

Conditioned on a fixed total number of transmitters $X = x$, and since each transmission succeeds with probability p_s, the number of successful transmission links Y follows the binomial distribution with parameters (x, p_s). The conditional mean is $\mathbb{E}[Y|X=x] = xp_s$. Since the adversary launches an attack after sensing a transmission and all transmission links within its range will be corrupted, the payoff for the jammer in a slot will be $\mathbb{E}[Y]$. Recall now that X is Poisson distributed with parameter $A_m\rho\gamma$. We have

$$\begin{aligned} \mathbb{E}[\,Y\,] &= \mathbb{E}_X[\,\mathbb{E}_Y[\,Y|X=x\,]\,] = \mathbb{E}_X[\,Xp_s\,] \\ &= p_s\rho\gamma A_m \\ &= A_m A(\rho\gamma)^2\left(e^{-\rho\gamma A} - e^{-\rho A}\right). \end{aligned}$$

The instantaneous payoff for the attacker that jams with probability q after sensing a transmission is

$$U_{mI}(q,\gamma) = q\,\mathbb{E}[\,Y\,] = qA_m A(\rho\gamma)^2\left(e^{-\rho\gamma A} - e^{-\rho A}\right), \quad (9)$$

and is linearly increasing with q.

The *instantaneous payoff for the network* in the absence of jammer is

$$U_I(\gamma) = \mathbb{E}[\,Y\,] = A_m A(\rho\gamma)^2\left(e^{-\rho\gamma A} - e^{-\rho A}\right),$$

which has global maximum with respect to γ. For large enough values of ρ, $\mathbb{E}[\,Y\,]$ has a maximum at approximately $\gamma = \frac{2}{A\rho}$. In the presence of a jammer, the instantaneous payoff for the network is $U_I(\gamma,q) = (1-q)A_m A(\rho\gamma)^2(e^{-\rho\gamma A} - e^{-\rho A})$.

The *cumulative payoff* U_{mC} for the attacker is the number of jammed links until the jammer is detected and the notification message is transferred out of the jammed area. Having assumed a single-channel system, we assume there does not exist a control channel for signalling notification. Hence, the transfer of the notification message from the monitor node out of the jammed region in a multi-hop fashion still undergoes the effects of jamming. Having obtained an expression of detection time as a function of q and γ, we compute the average time needed for the notification message to be carried out of the jammed area. The probability of successful channel access for a node i on the route of the notification message in the presence of jamming is $p_a = (1-q)\gamma(1-\gamma)^{n_i-1}$. Hence, the average waiting time for node i before successful transmission is $\sum_{j=1}^{\infty} j(1-p_a)^{j-1}p_a = 1/p_a$ slots. Let the average number of hops needed to deliver the alarm out of area A_m be H. Assuming a dense sensor deployment, the route followed by the notification message can be roughly approximated by a straight line. Then, $H \approx R_m/(2R)$, namely the average distance of the monitor from the boundary of the jamming area divided by node transmission range R. We adhere to this approximation since exact calculation of H relies on knowledge about network topology and location of the monitor. Such knowledge is rather unrealistic to assume for the attacker and even for the network itself. The average time needed for the alarm to propagate out of the jamming area is

$$W(q,\gamma) = \frac{H}{p_a} = \frac{H}{(1-q)\gamma(1-\gamma)^{\bar{n}-1}}, \quad (10)$$

where $\bar{n} = \rho A - 1$ is the average number of neighbors of a node along the path. It can be shown that $W(q,\gamma)$ is convex and monotonically increasing in terms of q. It is also convex in terms of γ and the minimum is achieved at $\gamma = 1 - \exp[-1/\bar{n}]$.

The total time until the jamming activity stops is $D(q,\gamma) + W(q,\gamma)$ and becomes infinite in the following cases:

- $q = 0$, which essentially means no jamming, hence no difference between normal and abnormal conditions and hence infinite detection time.
- $q = 1$, namely the scenario of continuous jamming, where the notification time approaches infinity.
- $\gamma = 0$, namely the case of absence of network transmissions, where no collision is observed and the detection time approaches infinity.

- $\gamma = 1$, where all network transmissions fail due to excessive contention regardless of existence of an adversary.

Then, the cumulative reward for the jammer for $q > 0$ is

$$\begin{aligned} U_{mC}(q,\gamma) &= U_{mI}(q,\gamma)[D(q,\gamma)+W(q,\gamma)] \\ &= qU_I(\gamma)\frac{C}{\theta_1 \log\frac{\theta_1}{\theta_0}+(1-\theta_1)\log\frac{(1-\theta_1)}{(1-\theta_0)}} \\ &\quad +qU_I(\gamma)\frac{H}{(1-q)\gamma(1-\gamma)^{\bar{n}-1}}\,. \end{aligned} \tag{11}$$

The cumulative payoff $U_{mC}(q,\gamma)$ goes to infinity at $q = 0$ and $q = 1$. For $q \to 0$, the jammer is almost undetectable and the number of disrupted links over an infinite time adds up to infinity. When $q \to 1$, although the detection time is minimized, the channel is completely occupied by the adversary and nodes are prevented from accessing it and flag the attack and hence the damage caused also goes to infinity. Similarly, the cumulative payoff for the network is

$$U_C(q,\gamma) = (1-q)U_I(\gamma)[D(q,\gamma)+W(q,\gamma)]. \tag{12}$$

and is increasing with γ.

B. Problem formulation and solution

1) Constant jamming power and one monitor node: In this section we formulate optimization problems to derive optimal strategies from the point of view of the jammer and the network with one designated monitor node. The objective function is the total delay $D(q,\gamma)+W(q,\gamma)$. An adversary tries to maximize it by controlling q and the network tries to minimize it by selecting γ. Both entities select parameters subject to energy limitations and payoff threshold constraints.

Problem 1:

The attacker problem is:

$$\begin{aligned} \max_{0<q\le 1}\quad & D(q,\gamma)+W(q,\gamma) \\ \text{s.t.}\quad & qP_m\left[D(q,\gamma)+W(q,\gamma)\right] \le E_m \quad (13) \\ & U_{mC}(q,\gamma) \ge U_m^0 \quad (14) \end{aligned}$$

where cumulative payoff $U_{mC}(q,\gamma)$ is defined in (11). The payoff threshold U_m^0 denotes a minimum required payoff for the jammer and captures the case where the jammer receives benefit by corrupting communication in a certain time frame.

The corresponding problem from the network's point of view is:

$$\begin{aligned} \min_{0\le\gamma\le 1}\quad & D(q,\gamma)+W(q,\gamma) \\ \text{s.t.}\quad & \gamma P\left[D(q,\gamma)+W(q,\gamma)\right] \le E \quad (15) \\ & U_C(q,\gamma) \ge U^0 \quad (16) \end{aligned}$$

where the network cumulative payoff $U_C(q,\gamma)$ is given by (12) and U^0 is the payoff threshold for the network. Threshold U^0 serves the purpose of avoiding network defense policies with small γ and accounts for the fact that the network aims at achieving a certain minimum level of throughput.

These optimization problems obtain different twists depending on the amount of knowledge of the attacker and the network about each other. We distinguish and study two cases:

- **Case 1:** the attacker knows the network policy, namely the access probability γ and the networks knows the jamming probability q.
- **Case 2:** Lack of the knowledge above at both sides.

Case 1: We start with the attacker's problem. Since the detection time approaches infinity at $q = 0, 1$, the solution is determined by the energy and payoff constraints, which can be written as:

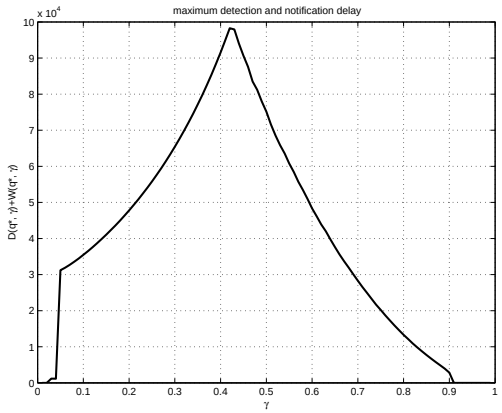
$$\begin{aligned} q\left[D(q,\gamma)+W(q,\gamma)\right] &\le E_m/(P_m) \\ q\left[D(q,\gamma)+W(q,\gamma)\right] &\ge U_m^0/U_{mI}(\gamma) \end{aligned}$$

Function $F(q) = q(D(q,\gamma)+W(q,\gamma))$ approaches infinity at $q = 0$ and $q = 1$ and can be shown to have one minimum in [0,1]. We omit the proof due to space constraints. Let $f_{\min}$ be the minimum of $F(q)$. We can distinguish three cases about the solution:

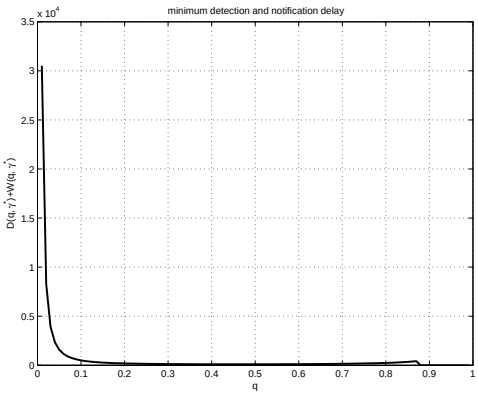
1) If $E_m/P_m < \max\{U_m^0/U_I(\gamma), f_{\min}\}$, there exists no feasible solution q. This reflects the fact the attacker cannot cause a certain level of damage due to energy limitations.
2) If $E_m/P_m \ge U_m^0/U_I(\gamma) \ge f_{\min}$, the energy constraint (13) restricts the value of q to an interval $[q_1, q_2]$, where q_1 and q_2 are obtained by making the energy constraint an equality. Similarly, the payoff constraint (14) yields a range of feasible values for q, $(0, q_3]$ and $[q_4, 1]$. Note that since $E_m/P_m \ge U_m^0/U_I(\gamma)$, the following must hold: $q_1 \le q_3$ and $q_2 \ge q_4$, i.e. the two ranges of feasible values for q overlap. Hence, the feasible ranges for q are $[q_1, q_3]$ and $[q_4, q_2]$. Since $D(q,\gamma)+W(q,\gamma) = F(q)/q$ and $F(q_1) = F(q_2) \ge F(q_3) = F(q_4)$ with $q_1 \le q_3 \le q_4 \le q_2$, we have $F(q_1)/q_1 > \max\{F(q_2)/q_2, F(q_3)/q_3, F(q_4)/q_4\}$, hence $q^* = q_1$.
3) If $E_m/P_m \ge f_{\min} \ge U_m^0/U_I(\gamma)$, the payoff constraint (14) is automatically satisfied for $q \in (0, 1]$. Hence the solution q^* is defined by the energy constraint. Since $F(q_1)/q_1 > F(q_2)/q_2$, it is $q^* = q_1$.

Combining cases 2 and 3, we have that $q^* = q_1$ if $E_m/P_m > \max\{U_m^0/U_I(\gamma), f_{\min}\}$, where q_1 is the smallest value of q that satisfies the energy constraint (13) with equality. From the solution, it follows that optimal strategies for the attacker tend to be rather mild and long-term.

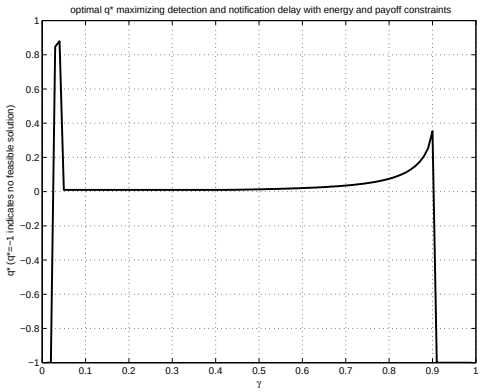
Next, we consider the network problem. The network needs to find access probability γ^* that minimizes the detection plus notification time. Recall that the objective function is not of finite value at $\gamma = 0$ and $\gamma = 1$. Similar as before, it can be shown that the total delay has a minimum at some point γ, $\gamma_{\min}$. The energy constraint (15) is written as $\gamma(D(q,\gamma)+W(q,\gamma)) \le E/P$ with $\gamma(D(q,\gamma)+W(q,\gamma))$ being monotonically increasing in γ. Therefore, the energy constraint (15) imposes an upper bound on γ, denoted by γ_{ub}, which is obtained by making the energy constraint an equality. Meanwhile, the network cumulative payoff $U_C(q,\gamma)$ is also increasing with γ. Hence, the payoff constraint imposes a lower bound on γ, γ_{lb}. There are now four cases for the solution:



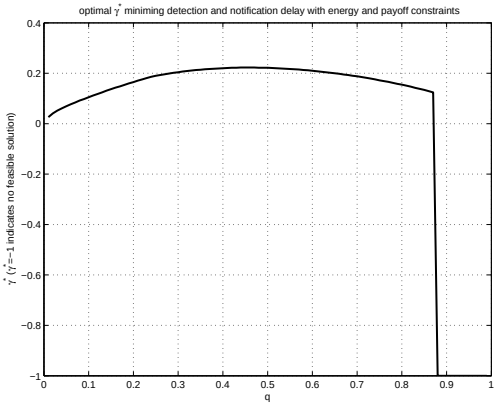
(a1) Attacker: maximum detection and notification delay for different γ's.



(b1) Network: minimum detection and notification delay for different q's.



(a2) Attacker: optimal q^* for different γ's.



(b2) Network: optimal γ^* for different q's.

Fig. 1. Numerical results for Case 2 of Problem 1 (lack of knowledge by attacker and network about the strategy of each other. Note that $q^* = -1$ (or $\gamma^* = -1$) in the plots indicate the non-existence of a feasible solution.

- If $\gamma_{\text{lb}} > \gamma_{\text{ub}}$, there exists no feasible solution, since the network has a high payoff requirement and limited energy.
- If $\gamma_{\text{lb}} < \gamma_{\text{ub}}$ and $\gamma_{\text{min}} \in [\gamma_{\text{lb}}, \gamma_{\text{ub}}]$, the optimal solution is $\gamma^* = \gamma_{\text{min}}$.
- If $\gamma_{\text{min}} < \gamma_{\text{lb}} < \gamma_{\text{ub}}$, then $\gamma^* = \gamma_{\text{lb}}$, and the solution is dictated by the payoff threshold.
- If $\gamma_{\text{lb}} < \gamma_{\text{ub}} < \gamma_{\text{min}}$, then $\gamma^* = \gamma_{\text{ub}}$ and the solution is defined by the energy threshold.

Case 2: Suppose now that the attacker and the network do not know the strategy of each other. One approach for the attacker is to choose q so as to respond optimally to the worst scenario (for the attacker) of network defense, namely to the case where the network selects γ to minimize the objective function. Admittedly, this approach is rather conservative. The attacker payoff in that case is a lower bound on attacker payoffs over all network defense policies. The attacker problem is:

$$\begin{aligned} \max_{0<q\leq 1} \min_{0\leq\gamma\leq 1} \quad & D(q,\gamma) + W(q,\gamma) \\ \text{s.t.} \quad & qP_m \left[D(q,\gamma) + W(q,\gamma)\right] \leq E_m \\ & U_{mC}(q,\gamma) \geq U_m^0 \end{aligned}$$

To approximate the solution of the max-min problem above, the attacker starts with a large number of M candidate values of γ, $\gamma_j \in [0,1]$, $j = 1...M$. For each γ_j, the attacker finds q_j^* that maximizes $D(q,\gamma_j) + W(q,\gamma_j)$ subject to the constraints. The attacker chooses among all the q_j^*'s the one that corresponds to the smallest value of $D(q_j^*,\gamma_j) + W(q_j^*,\gamma_j)$, $j = 1...M$. Clearly, the approximation of the solution becomes better with a larger number M.

Along the same lines, the network takes the conservative approach that the attacker performs the optimal attack and solves the following problem as response to this attack:

$$\begin{aligned} \min_{0\leq\gamma\leq 1} \max_{0<q\leq 1} \quad & D(q,\gamma) + W(q,\gamma) \\ \text{s.t.} \quad & \gamma P \left[D(q,\gamma) + W(q,\gamma)\right] \leq E \\ & U_C(q,\gamma) \geq U^0. \end{aligned}$$

The resulting total delay for the network in that case is an upper bound on incurred delays over all jamming policies. We have numerically evaluated the max-min and min-max problems for the following scenario: sensor node transmission range $R = 20$m, node density $\rho = 0.0025$, energy constraint $E/P = 500$ (i.e., a sensor can continuously transmit in 500 slots), payoff threshold $U^0 = 500$ transmissions, attacker

transmission range $R_m = 200$m, energy constraint $E_m/P_m = 1000$, target payoff $U_m^0 = 500$, $p_{FA} = 0.02$ and $p_D = 0.98$. The results are presented in Figure 1.

From Figure 1, we obtain the solution for the adversary as $q^* = 0.87$ with corresponding total delay of 1.137×10^3 slots. The solution for the network is $\gamma^* = 0.026$ with corresponding total delay 3.089×10^4. In fact, when $q = 0.87$ and $\gamma = 0.026$, $D(q,\gamma) + W(q,\gamma) = 1.206 \times 10^3$. If the adversary knows $\gamma = 0.026$, it can choose an optimal $q^* = 0.828$ and cause delay 1.506×10^3, which is larger than the one obtained without knowledge of γ. In order to incur the largest delay subject to energy and payoff constraints, the adversary needs to know γ. On the other hand, if the network knows $q = 0.87$, the optimal γ^* is 0.124 which reduces the detection and notification delay to just 414 slots, which is much faster than 1.206×10^3. Note that 414 is faster than the minimum delay 1.137×10^3 estimated by the adversary. This can be explained by the fact that the adversary and the network each solve the max-min and min-max problems subject to their own constraints. Similar problems can be formulated and solved with the cumulative payoff as the objective function.

2) Constant jamming power and several monitor nodes: We now consider the extension for multiple monitor nodes. Different monitor nodes have different perception of the probability of collision under normal conditions due to different neighborhood sizes and therefore reach a decision as to occurrence or not of attack at different times. Nodes can be classified in different classes $\mathcal{C}_1, \ldots, \mathcal{C}_K$ such that nodes in class $\mathcal{C}_n$ have n neighbors, $1 < n \leq n_{\max}$. Clearly, we would like to assign the role of monitor to nodes of a class with n^* neighbors to minimize detection time. The optimal neighborhood size n^* as a function of γ is depicted in Figure 2 for jamming probabilities $q = 0.3$, $q = 0.6$ and $q = 0.9$. We observe that as γ increases, n^* approaches 1, which is the case of a monitor with only one neighbor. This is explained as follows: when γ is not small, multiple neighbors can cause collision, thus negatively affecting detection delay. When γ is small, a larger number of neighbors are needed in order for the monitor to observe collision.

The attacker would like to choose its strategy so as to balance the detection delays of different monitors. For sufficiently large values of γ, we concluded above that it needs to focus only on the class $\mathcal{C}_1$. When γ is small, e.g. $\gamma < 0.05$, the detection delay balancing problem is meaningful and can be stated as:

Problem 2

$$\max_{0<q\leq 1} \min_{i\in\{1,\ldots,K\}} D(q,\gamma,\mathcal{C}_i),$$

where we stress dependence of detection delay on different monitor classes. Since detection time is decreasing in q regardless of number of neighbors, the smallest feasible q imposed by the energy constraint is the solution for the attacker.

3) Controllable jamming power and several monitor nodes: We now consider the problem where the jammer can choose transmission power level $P_{m,j}$ out of a set of L ordered discrete values $\{P_{m,1}, \ldots, P_{m,L}\}$ with probability q_j such that $\sum_{j=1}^{L} q_j = q$. With probability $q_0 = 1-q$ the jammer remains silent. Without loss of generality and to avoid the trivial solution $q_0 = 1$, we let $q_0 < 1$, i.e. $0 < \sum_{j=1}^{L} q_j \leq 1$. Different jamming power levels P_j lead to different jamming areas $A_{m,j}$ with radii $R_{m,j}$. Define zone j to be the ring determined by $R_{m,j}$ and $R_{m,j-1}$, i.e. the area covered by power level $P_{m,j}$ but not $P_{m,j-1}$. The average number of transmission links in $A_{m,j}$ is $T_j = A_{m,j}A(\rho\gamma)^2(e^{-\rho\gamma A} - e^{-\rho A})$. We assume that the network is dense enough such that there always exists a monitor in each of the zones. A node in zone j perceives jamming with probability $\sum_{\ell=j}^{L} q_\ell$. The average number of hops to traverse zone j based on a previously stated assumption is approximately $(R_{m,j+1} - R_{m,j})/2$.

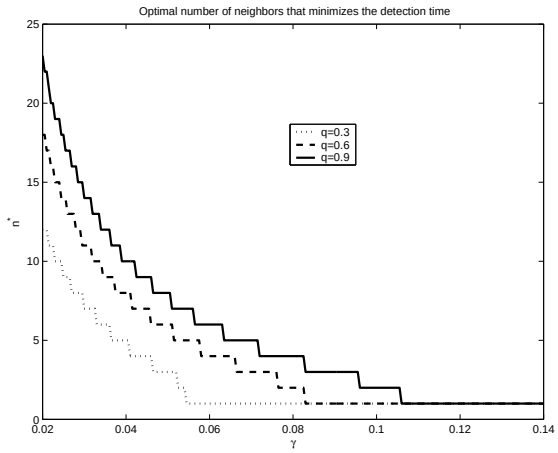


Fig. 2. The optimal number of neighbors n to minimize the detection time vs. γ for three different q's.

An interesting tradeoff arises here. Monitor nodes located in outer zones perceive lower jamming probability and hence the detection time can be large. However, they are close to the boundary of the jammed area and thus they can pass a notification message out of the area in fewer hops, namely faster. Monitors located in inner zones experience a more aggressive attack and can detect it faster, but they delay in passing the message out of the jammed area. The goal of the attacker is to find jamming strategy so as to maximize the detection plus notification delay. The strategy consists in choosing vector $(q, \{q_j\}_{j=1,\ldots,L})$. We now show a simple and intuitive heuristic for the attacker. For ease of notation, denote detection and notification times by $D(q)$ and $W(q,\bar{R})$, where $\bar{R}$ is the average distance of a monitor from the boundary of the jammed region. Symbolize $R_{m,j}$ by R_j.

The algorithm goes as follows: start by jamming the largest region, solve problem $\max_{q_L} D(q_L,\gamma)+W(q_L,R_L/2)$ subject to the constraints, and find $q_L^* = q$. Let a be the maximum value of the objective function. Assume now two power levels with ranges R_{L-1} and R_L. Solve:

$$\max_{q_{L-1}} D(q_{L-1})+W(q_{L-1},\frac{R_{L-1}}{2})+W(q-q_{L-1},\frac{R_L-R_{L-1}}{2}),$$

where the notification terms are the required time for a monitor in the inner circle to pass the alarm through the two zones. Let the optimal value be a_1. Compare with the detection plus notification time required for a monitor in the outer zone,

$$\max_{q_{L-1}} D(q - q_{L-1}) + W(q - q_{L-1}, (R_L - R_{L-1})/2)$$

and let the optimal value be a_2. Then, $\max\{a_1, a_2\}$ is the total delay for two power levels. If $\max\{a_1, a_2\} > a$, the attacker adopts strategy (q_L^*, q_{L-1}^*), otherwise it uses strategy q. Continuing in that fashion, the attacker adds more power levels to its strategy if this is beneficial.

We solved numerically the problem with $\rho = 0.0025$, $R = 20$m, $U_m^0 = 500$, $L = 2$ power levels with ranges $R_{m,1} = 100$m and $R_{m,2} = 200$m, and $E_m/P_{m,1} = 1000$, $E_m/P_{m,2} = 2000$. We also assumed different minimum number of neighbors per zone. In zone 1, the minimum number of neighbors of monitors is 2 and in zone 2 it is 7. The network transmission probability $\gamma = 0.3$ is known to the attacker. We consider the following scenarios: (i) the adversary knows the neighborhood of monitors (ii) the adversary has no knowledge of monitor locations and neighborhoods, hence it uses the average number of neighbors $\rho\pi * R^2 - 1 = 2$ in finding the optimal q_j's. For case (i) the optimal jamming strategy is $q_1^* = 0$, $q_2^* = 0.07$, which yields the detection and notification delay 1.33×10^5. For case (ii) the jamming strategy is $q_1^* = 0.02$, $q_2^* = 0$, i.e. to jam only the smaller zone, zone 1. The detection and notification delay is 1.05×10^5, which is less than the delay the attacker can cause with full knowledge. From the numerical solutions for different γ's, we observed that the optimal solution without knowledge of monitor neighborhood is to jam the inner region. The theoretical proof or disproof of this observation is deferred for future study.

IV. Conclusions

We studied controllable jamming attacks in wireless sensor networks, which are easy to launch and difficult to detect and confront. The derived solutions to the optimization problems dictate optimal attack and network defense strategies. Of particular interest is the comparison between the case of perfect knowledge and that of lack of knowledge of the attacker and the network about the strategy of each other. In the latter, the attacker and the network respond optimally to the worst-case strategy of the other.

Our work is a first step towards understanding the structure of these problems, identifying tradeoffs and capturing the impact of different parameters on performance. There exist several directions for future study. Interesting issues arise in multi-channel networks. In that case, the defense strategy space has an additional dimension, channel switching, while the jammer has higher energy costs when jamming more channels. Another interesting issue is to find alternatives for modeling lack of knowledge for the attacker and the network. An idea would be to average over all strategies of the opponent. More enhanced versions of attacks can be considered, such as the one with dynamic control of jamming probability to extend detection time. Likewise, the network can adapt channel access probability. Finally, the issue of multiple, potentially co-operating attackers gives a whole new flavor to these problems and is worth further attention.

Acknowledgments

This work is supported in part by the following grants ONR N00014-04-1-0479 and ARO PECASE W911NF-05-1-0491. This document was prepared through the collaborative participation in the Communication and Networks Consortium sponsored by the U.S. Army Research Laboratory under the Collaborative Technology Alliance Program DAAD19-01-2-0011. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon. The views and conclusions contained in this documents are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government.

I. Koutsopoulos acknowledges support of the European Commission NoE CRUISE (IST-4-027738) and the Marie Curie Grant SAINT-W (IRG-017267).

References

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

[2] S. Radosavac, I. Koutsopoulos and J.S. Baras, "A framework for MAC protocol misbehavior detection in wireless networks," in *Proc. ACM Workshop on Wireless Security (WiSe)*, 2005.

[3] R. Negi and A. Perrig, "Jamming analysis of MAC protocols," *Carnegie Mellon Technical Memo*, 2003.

[4] R. Mallik, R. Scholtz, and G. Papavassilopoulos, "Analysis of an on-off jamming situation as a dynamic game," *IEEE Trans. Commun.*, vol. 48, no. 8, pp. 1360-1373, Aug. 2000.

[5] J. Jung, V. Paxson, A.W. Berger and H. Balakrishnan, "Fast portscan detection using sequential hypothesis testing," in *Proc. IEEE Symposium on Security and Privacy*, 2004.

[6] V. Coskun, E. Cayirci, A. Levi, and S. Sancak, "Quarantine region scheme to mitigate spam attacks in wireless-sensor networks", *IEEE Trans. on Mobile Computing*, vol. 5, no. 8, pp. 1074-1086, August 2006.

[7] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, vol. 35, no. 10, pp. 54-62, 2002.

[8] Y. W. Law, L. van Hoesel, J. Doumen, P. Hartel and P. Havinga, " Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," in *Proc. ACM Security Sensor Ad-hoc Networks (SASN)*, 2005.

[9] G. Lin and G. Noubir, "On link-layer denial of service in data wireless LANs," *Journal on Wireless Comm. and Mob. Computing*, August 2004.

[10] M. Cagalj, S. Capkun, J.-P. Hubaux, "Wormhole-based anti-jamming techniques in sensor networks," *IEEE Trans. on Mobile Computing*, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[11] W. Xu, W. Trappe, Y. Zhang and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *Proc. ACM MobiHoc*, 2005.

[12] W. Xu, T. Wood, W. Trappe and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," *Proc. Workshop on Wireless Security (WiSe)*, 2004.

[13] J. M. McCune, E. Shi, A. Perrig and M. K. Reiter, "Detection of denial-of-message attacks on sensor network broadcasts," *Proc. IEEE Symposium on Security and Privacy*, 2005.

[14] A. Wald, *Sequential Analysis*, Wiley 1947.

[15] Vladimir P. Dragalin, A. G. Tartakovsky and V. V. Veeravalli. "Multihypothesis Sequential Probability Ratio Tests - Part I: Asymptotic optimality," *IEEE Trans. Inf. Theory*, Vol. 45, No. 7, Nov. 1999.

[16] C. W. Helstrom, *Elements of signal detection and estimation*, pp. 339-340, Prentice-Hall, 1995.

[17] A. M. Mathai, *An introduction to geometrical probability*, Gordan and Breach Science Publishers, 1999.