Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks

Mingyan Li, *Member*, *IEEE*, Iordanis Koutsopoulos, *Member*, *IEEE*, and Radha Poovendran, *Senior Member*, *IEEE*

Abstract—We consider a scenario where a sophisticated jammer jams an area in which a single-channel random-access-based wireless sensor network operates. The jammer controls the probability of jamming and the 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 jammed region. The jammer is detected by employing an optimal detection test based on the percentage of incurred collisions. On the other hand, the network defends itself by computing the channel access probability to minimize the jamming detection plus notification time. The necessary knowledge of the jammer in order to optimize its benefit consists of knowledge about the network channel access probability and the 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 each other and the case where the jammer and the network lack this knowledge. The latter is captured by formulating and solving optimization problems where the attacker and the network respond optimally to the worst-case or the average-case strategies of the other party. 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 meaningful heuristic algorithm for an efficient jamming strategy. Our results provide valuable insights about the structure of the jamming problem and associated defense mechanisms and demonstrate the impact of knowledge as well as adoption of sophisticated strategies on achieving desirable performance.

Index Terms—Jamming, security, jamming detection and mitigation, optimization, wireless multiple access, wireless sensor network.

1 Introduction

The fundamental characteristic of wireless networks that renders them more vulnerable to attacks than their wireline counterparts is the open, shared nature of their medium. This exposes them to two fundamentally different attacks: passive and active attacks. In the former ones, the malicious entity does not take any action apart from passively observing the ongoing communication, that is, eavesdropping with the intention to intervene with the privacy of network entities involved in the transaction. On the other hand, in active attacks the attacker is involved in transmission as well. Depending on attacker objectives, different terminology is used. If the attacker abuses a protocol with the primary 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 the cause or the consequences of it.

Misbehavior in wireless networks stems from the selfish inclination of wireless network entities to improve their own derived utility at 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 per 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. The latter case occurs when a node prevents other nodes from accessing the channel [2] [3] or from routing their messages to destinations by selfish manipulation of the access control and routing protocol, respectively. The work in [4] focuses on optimal detection of access layer misbehavior in terms of number of required observation samples to derive a decision. The worst-case attack is found out of the class of most significant attacks in terms of incurred performance losses. The framework captures uncertainty of attacks and the case of intelligent attacker that can adapt its policy to delay its detection.

Jamming can disrupt wireless transmission and occur either unintentionally in the form of interference, noise, or collision at the receiver, or in the context of an attack. A jamming attack is particularly effective from the attacker's point of view since 1) the adversary does not need special hardware to launch it, 2) the attack can be implemented by

- *M. Li is with the Boeing Research & Technology, The Boeing Company, PO Box 3707, MC 7L-69, Seattle, WA 98124-2207, and the Network Security Laboratory (NSL), Department of Electrical Engineering, University of Washington, Seattle, WA. E-mail: myli@u.washington.edu.*
- *I. Koutsopoulos is with the Department of Computer Engineering and Communications, University of Thessaly, Gklavani 37 and 28 Octovriou (Office E1/3), Volos, GR 38221, Greece. E-mail: jordan@uth.gr.*
- *R. Poovendran is with the Network Security Laboratory (NSL), Department of Electrical Engineering, University of Washington, Paul Allen Center, Room AE100R, Box 352500, Seattle, WA 98195-2500. E-mail: rp3@u.washington.edu.*

Manuscript received 16 Dec. 2007; revised 18 Sept. 2009; accepted 3 Dec. 2009; published online 21 Apr. 2010.
For information on obtaining reprints of this article, please send e-mail to: tmc@computer.org, and reference IEEECS Log Number TMC-2007-12-0386. Digital Object Identifier no. 10.1109/TMC.2010.75.

simply listening to the open medium and broadcasting in the same frequency band as the network uses, and 3) 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 in the sense that they are realized by means of a high transmission power signal that corrupts a communication link or an entire area. Conventional defense techniques against physical layer jamming rely on spread spectrum which can be too energy consuming for resource-constrained sensors [5]. Jamming attacks also occur at the access layer, whereby an adversary either corrupts control packets or reserves the channel for the maximum allowable number of slots, so that other nodes experience lower throughput by not being able to access the channel [6]. The work in [7] 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 instances can have impact on the network layer by malicious packet injection along certain routes or at the transport layer by SYN message flooding for instance. The work in [8] presents attack detection in computer networks based on observing the IP port scanning profile prior to an attack and using sequential detection techniques. The work [9] uses controlled authentication to detect spam message attacks in wireless sensor networks launched by a set of malicious nodes and addresses the trade-off between resilience to attacks 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 and Stankovic [5] provide a taxonomy of DoS attacks launched against sensor networks from the physical up to the transport layer. Law et al. [10] present attacks aimed at sensor network protocols that are based on learning protocol semantics such as temporal arrangement of packets, time slot size, or packet preample size. In [11], 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 [12] 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. The links are created through frequency hopping over a channel set either in a predetermined or in an ad hoc fashion. In [13], a physical layer jammer termed constant jammer, and three types of link layer jammer termed deceptive, random, and reactive jammer are studied. The reactive jammer is the most sophisticated one as it launches its attack after sensing ongoing transmission. The authors propose empirical methods based on signal strength and packet delivery ratio measurements to detect jamming. In [14], Channel surfing involves on-demand frequency hopping as a countermeasure against jamming is studied. The case of an attacker that corrupts broadcasts from a base station (BS) to a sensor network is considered in [15]. The interaction between the attacker and the BS is modeled as a zero-sum game with a long-term payoff for the attacker. The attacker selects the number of sensors it will jam and the BS chooses the probability with which it will sample sensor status with regard to message reception.

In this paper, we study controllable jamming attacks that are easy to launch but are difficult to detect and confront, since they differ from brute force attacks. The jammer controls the probability of jamming and the transmission range in order to cause maximal damage to the network in terms of corrupted communication links. We assume that the effect of jammer action ceases when it is detected by one or more monitoring nodes, and a notification message is transferred out of the jamming region. Following this notification message, drastic actions are presumably taken by the network in order to isolate, penalize, localize, and even physically capture the attacker. These actions are, however, not addressed further in this work. The fundamental trade-off faced by the attacker is the following: a more aggressive attack, either in terms of higher jamming probability or larger transmission range increases the instantaneous payoff but exposes the attacker to the network and facilitates its detection and, later on, its isolation. In an effort to withstand the attack, alleviate the attacker benefit, and expose the attacker to the detection system, the network controls the channel access probability of the employed random access protocol. The necessary knowledge of the jammer in order to optimize its benefit consists of knowledge about the network channel access probability and the 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:

1. We derive the optimal attack and optimal defense strategies as solutions to optimization problems that are faced by the attacker and the network, respectively, by including in the formulation energy limitations.
2. For attack detection, we provide a methodology and an optimal detection test that derives decisions based on the percentage of incurred collisions compared to the nominal one.
3. We include in the formulation the attack detection and the transfer of the attack notification message out of the jammed area.
4. We capture the impact of available knowledge of the attacker and the network about the other's strategies. For the case of partial knowledge, the attacker and the network optimize with respect to the worst-case or the average-case strategy of the other.
5. We extend the basic model to the case of multiple monitoring nodes and controllable 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 Sections 2 and 3, we state the adopted network and adversary models, describe the jamming detection and notification mechanism, and derive expressions for the attacker and network payoff functions. In Section 4, we formulate optimization problems and derive optimal jamming attack and defense strategies. We conclude our paper in Section 5. In Table 1, we provide a list of the notations used in this paper.

TABLE 1
A Summary of Notations

Notation	Description
q	probability of jamming in a time slot
γ	channel access probability of a network node
i, j	indices of a network node
n_i	number of neighboring nodes of node i
$\mathcal{N}_i$	set of all neighbors of i
ρ	network density
ν	number of nodes in the jammer's sensing range
E, E_m	energy of a node, and the attacker, respectively
P, P_m	power level of a node, and the attacker, respectively
R, R_m	transmission range of a node, and the attacker
R_s, R_{ms}	sensing range of a node, and that of the attacker
θ_0, θ_1	probability of collision observed in the absence of in the presence of an attacker, respectively
P_M	probability of miss detection
P_{FA}	probability of false alarm
S_k	logarithm of likelihood ratio at stage k
a, b	thresholds used in sequential probability ratio test
$\mathbf{H}_0, \mathbf{H}_1$	Hypothesis
X, Y	general random variables
$\mathbb{E}[X]$	expectation of random variable X
N	No. of samples until a detection decision is made
U_I, U_{mI}	instantaneous payoff of the network, and that of the attacker
U_C, U_{mC}	cumulative payoff of the network, and that of the attacker
U_W, U_{mW}	weighed cumulative payoff of the network and the attacker, respectively
$A = \pi R^2$	transmission range of a network node
$A_m = \pi R_m^2$	jamming range
p_s	probability of a successful transmission in region A
D	jamming detection time (in terms of the number of slots)
W	time to route an alert out of the jamming range
U^0, U_m^0	payoff threshold for the network and the attacker, respectively

2 Modeling Assumptions

2.1 Sensor Network Model

We consider a wireless sensor network deployed over a large area and operating under a single-carrier slotted Aloha type random access protocol [16]. We assume symmetric transmission and reception in the sense that a node i can receive a signal from node j if and only if node j can receive a signal from i. Time is divided into time slots and the slot size is equal to the size of a packet. All nodes are assumed to be synchronized when transmitting with respect to time slot boundaries. Each node transmits at a fixed power level P with an omnidirectional 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 transmitted messages from i, while a node within sensing range can just sense activity due to higher signal strength than noise, but cannot decode the transmitted message. Typically, R_s is a small multiple of R, ranging from 2 to 3 [17]. A node within distance R of a node i (excluding node i itself) is called a neighbor of i. The neighborhood of i, $\mathcal{N}_i$ is the set of all neighbors of i with $n_i = |\mathcal{N}_i|$ being the size of i's neighborhood. Transmissions from node i are received by all its neighbors. The sensor 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 where edge (i, j) denotes that sensor i and j are within transmission range of each other. Sensor nodes are uniformly distributed in an area, with spatial density ρ nodes per unit area and the topology is static, i.e., we assume no mobility. Each node has an initial amount of energy E. We do not consider the energy consumed in reception.

Each node is equipped with a single 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 generated by higher layers of a node, or they may come from other nodes and need to be forwarded or they may be previously sent and collided packets 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 slotted Aloha type random access protocols that are characterized by a *common* channel access probability γ for all network nodes in each slot. This provides us with a straightforward means to quantify the network effort to withstand and confront the attack by regulating the amount of transmitted traffic and essentially exposing the attacker to the detection system, as will become clear in the sequel. 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 for node j or for other nodes. Thus, the probability of collision at node j in a slot is

$$\theta_0 = 1 - (1-\gamma)^{n_j} - n_j\gamma(1-\gamma)^{n_j-1}. \quad (1)$$

If node j attempts to transmit at a slot while it receives a message, a collision occurs as well. In that case, the receiver is not in position to tell whether the collision is due to its own transmission or whether it would occur anyway. In the sequel, we will term collision an event addressing the case of multiple simultaneous transmissions received by (not necessarily intended to) a node and no transmission attempt by that node. Note that, if we include the possibility that the receiver also attempts to access the channel, the probability of collision is the same as the one above with n_j substituted by $n_j + 1$. Whenever a 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., it is $n_j = 0$), then this node does not receive any packets and does not experience collisions.

2.2 Attacker Model

We consider one attacker, the jammer, in the sensor network area. The jammer is neither authenticated nor associated with the network. The objective of the jammer is to corrupt legitimate transmissions of sensor nodes by causing intentional packet collisions at receivers. Intentional collision leads to retransmission, which is translated into additional energy consumption for a certain amount of attainable throughput or equivalently reduced throughput for a given amount of consumed energy. In this paper, we do not consider the attacker that is capable of node capture.

The jammer may use its sensing ability in order to sense ongoing activity in the network. Clearly, sensing ongoing network activity prior to jamming is beneficial for the attacker in the sense that its energy resources are not aimlessly consumed and the jammer is not needlessly exposed to the network. The jammer transmits a small packet which collides with legitimate transmitted packets at their

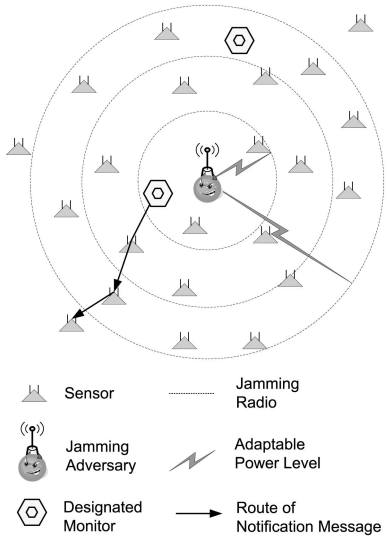

Fig. 1. Illustration of jamming attack. The jamming adversary can jam with different transmit power levels to disrupt network operation while avoiding detection. We assume that there exist designated monitoring nodes for detecting the jamming attack. Upon detection, a notification is routed out of the jammed region in a multihop fashion. The jammer can prolong the transfer of such a notification message by continuing jamming after detection.

intended receivers. As argued in [11], a beacon packet of a few bits suffices to disrupt a transmitted packet in the network. The jammer is assumed to have energy resources denoted by E_m, yet the corresponding energy constraint in the optimization problems of the next section may be redundant if the jammer adheres to the policy above. The jammer uses an omnidirectional antenna with circular sensing range R_{ms} and adaptable transmission range R_m that is realized by controlling transmission power P_m as illustrated in Fig. 1. 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, therefore, specified by set $\mathcal{P} \times (0, 1)$, where $\mathcal{P}$ is the discrete set of employed power levels. The attacker attempts to strike a balance between short- and long-term benefits, as a more aggressive attack increases instantaneous benefit but exposes the attacker to the detection system, while a milder attack may prolong detection time.

If the jammer senses the channel prior to deciding whether to jam or not, collision occurs at node j if the jammer jams and at least one neighbor transmits. Thus, conditioned on existence of a jammer, the probability of collision at node j is

$$\theta_1 = 1 - (1-\gamma)^{n_j} - (1-q)n_j\gamma(1-\gamma)^{n_j-1}.$$

On the other hand, if jamming occurs without prior channel sensing, the probability of collision is

$$\theta_1' = [1-(1-\gamma)^{n_j}]q + \theta_0(1-q) = \theta_1.$$

Thus, the probability of collision is the same regardless of channel sensing prior to jamming. This implies that jamming can be viewed as a multiple access situation between a network of 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 energy by a factor of $1-(1-\gamma)^{\nu}$, where ν denotes the number of legitimate nodes in the jammer's sensing range. For large ν, $1-(1-\gamma)^{\nu} \approx 1$. Namely, for a dense sensor network, it is very likely that some transmission will always occur in the network and, therefore, it does not really make a difference whether the attacker will sense the channel or not. In the sequel, we will not consider the energy saving factor $1-(1-\gamma)^{\nu}$.

We will subsequently assume that the adversary possesses different amounts of knowledge about the network, ranging from full knowledge about network parameters such as access probability γ and the neighborhood of a monitor node to no knowledge at all. Network's differing levels of knowledge about an attacker will be considered as well.

2.3 Attack Detection Model

The network employs a mechanism for monitoring network status and detecting potential malicious activity. The monitoring mechanism consists of: 1) determination of a subset of nodes $\mathcal{M}$ that act as monitors, and 2) employment of a detection algorithm at each monitor node. The assignment of the role of monitor to a node is affected by potential existing energy consumption and node computational complexity limitations, and by detection performance specifications. In this work, we consider a fixed set $\mathcal{M}$, and formulate optimization problems for one or several monitor nodes.

We fix attention to a specific monitor node and the detection scheme that it employs. First, we need to define the quantity to be observed at each monitor. In our case, the readily available metric is the 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 limit of the ratio of number of slots where there was collision over total number of slots of the training period. Now let the network operate in the open after the training period has elapsed and fix attention to a time window much smaller than the training period. An increased percentage of collisions in the time window compared to the learned long-term ratio may be an indication of an ongoing jamming attack that causes additional collisions. However, it may happen as well that the network operates normally and there is just a temporary irregular increase in the percentage of collisions compared to the learned ratio for that specific interval. A detection algorithm is part of the detection module at a monitor node; it takes as input observation samples obtained by the monitor node (i.e., collision/not collision) and decides whether there is an attack or not. On one hand, the observation window should be small enough, such that the attack is detected in a timely manner 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 reduced.

The sequential nature of observations at consecutive time slots motivates the use of sequential detection techniques. A sequential decision rule consists of: 1) a stopping time, indicating when to stop taking observations, and 2) 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 trade-offs 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 average delay) to reach a decision among all sequential and nonsequential tests for which P_{FA} and P_M do not exceed the predefined values above is Wald's Sequential Probability Ratio Test (SPRT) [18]. When SPRT is used for sequential testing between two hypotheses concerning two probability distributions, SPRT is optimal in that sense as well [19].

SPRT collects observations until significant evidence in favor of one of the two hypotheses is accumulated. After each observation at the kth stage, we choose between the following options: accept one or the other hypothesis and stop observing, or defer decision for the moment and obtain another observation $k+1$. In SPRT, there exist two thresholds a and b that aid the decision. The computed figure of merit at each step is the logarithm of the likelihood ratio of the accumulated sample vector until that step. In our case, the test is between hypotheses H_0 and H_1 that involve Bernoulli with probability mass functions (p.m.fs.) f_0 and f_1 defined by $Pr(c=1)=\theta_i=1-Pr(c=0)$ where $c=1$ denotes the event of collision in a slot. That is, H_0 concerns the hypothesis about absence of jamming with Bernoulli p.m.f. f_0 with parameter θ_0, while H_1 corresponds to the hypothesis of jamming with a Bernoulli p.m.f. f_1 with parameter θ_1. Thus, 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 probability mass function of sequence $(x_1,\ldots,x_k)$ based on hypothesis H_i, for $i=0,1$. 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:

$$\begin{aligned} S_k\geq a &\Rightarrow \text{accept}\quad H_1,\\ S_k< b &\Rightarrow \text{accept}\quad H_0,\\ b\leq S_k< a &\Rightarrow \text{take another observation.}\end{aligned} \tag{4}$$

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 the detection rule is to minimize the number of required observation samples to derive a decision about existence or not of jamming. The detection performance is quantified by the average sample number (ASN), $\mathbb{E}[N]$, needed until a decision is reached, where the expectation is with respect to the distribution of the observations. From Wald's identity and conditioned on hypothesis H_i being true [18] we have $\mathbb{E}[S_N|H_i]=\mathbb{E}[N|H_i]\times\mathbb{E}[\Lambda|H_i]$, where $\mathbb{E}[\Lambda|H_i]$ is the expected value of the logarithm of likelihood ratio, conditioned on hypothesis H_i. By using a similar derivation as the one in [20, pp. 339-340], we derive the inequalities:

$$1-P_M\geq e^a P_{FA}\quad\text{and}\quad P_M\leq e^b\,(1-P_{FA}), \tag{5}$$

where a and b are the thresholds of SPRT. When the expected number of required observations is large, the increments Λ_j in the logarithm of likelihood ratio are small. Therefore, when the test terminates with selection of hypothesis H_1, the expected value of cumulative likelihood ratio, $\mathbb{E}[S_N|H_1]$ will be slightly larger than a if the attack is detected and very close to b if the attack is missed and declared as absent. Then, inequalities (5) hold with a good approximation as equalities [18], [20]. Under this assumption, the decision levels a and b that are required for attaining performance (P_{FA},P_M) are

$$a=\ln\frac{1-P_M}{P_{FA}}\quad\text{and}\quad b=\ln\frac{P_M}{1-P_{FA}}. \tag{6}$$

Furthermore, it is $\mathbb{E}[S_N|H_1]=aP_D+b(1-P_D)=C$, where $P_D=1-P_M$ is the probability of detection of SPRT. Hence, the expected number of samples for detecting jamming is

$$\mathbb{E}[N|H_1]=\frac{\mathbb{E}[S_N|H_1]}{\mathbb{E}[\Lambda|H_1]}=\frac{C}{\theta_1\log\frac{\theta_1}{\theta_0}+(1-\theta_1)\log\frac{1-\theta_1}{1-\theta_0}}. \tag{7}$$

Note that $\mathbb{E}[N|H_1]$ is a function of the jamming probability q and the network channel access probability γ, denoted also by $D(q,\gamma)$.

2.4 Notification Delay

Following detection of an attack, the network needs to be notified in order to launch appropriate countermeasures. The transfer of the notification message out of the jammed area is performed with multihop routing from the monitor node to a node out of the jammed region. The same random access protocol with channel access probability γ is employed by a node to forward the message to the next node. Having assumed a single-channel sensor network, we implicitly exclude the existence of a control channel that is used for signaling attack notification messages. Hence, the transfer of the notification message out of the jammed will take place in the same channel and will still undergo jamming. Clearly, the time that is needed for the notification message to be passed out of the jammed area depends on the jamming strategy as well as the network channel access probability. For that reason, we use the sum of detection and notification delay as a metric that captures the objective of the attacker and the network. It is understood that if there exists a control channel for signaling notification messages that is not jammed, then only the detection delay is needed as a performance objective. If this control channel is jammed, then one needs to consider the notification time but also assess the cost incurred by jamming an additional channel. We discuss briefly this issue in the last section as part of future work.

We now 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 along the route of the notification message in the presence of jamming is $p_a=(1-q)\gamma(1-\gamma)^{n_i-1}$. Hence, the expected number of transmission attempts before successful

transmission, which also denotes expected delay for node i before successful transmission is $\sum_{j=1}^{\infty} j(1-p_a)^{j-1}p_a = 1/p_a$ slots. In a single-channel network, the adversary can cause additional disruption to the network by jamming the alert message even after being detected. In order to find the average delay for transmitting an alert out of the jammed region, let us first denote the average number of hops to deliver the alarm out of jammed area A_m by H. Clearly, the expected notification delay depends on the expected number of hops it takes for the notification message to leave the jammed area which in turn depends on the position of the monitor node. We assume dense sensor deployment and, thus, roughly approximate the route followed by the notification message with an almost straight line. This means that $H \approx R_m/(2R)$, namely, H is equal to the average distance of a monitor from the boundary of the jammed area ($R_m/2$) divided by the node transmission range R. We adhere to this approximation since the exact expression for the distribution of H depends on knowledge about the network topology and the 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, also referred to as notification delay, is

$$W(q,\gamma) = \frac{H}{p_a} = \frac{H}{(1-q)\gamma(1-\gamma)^{\bar{n}-1}}, \tag{8}$$

where we substituted in the expression above the average number of neighbors of a node along the path, $\bar{n}$ in order to eliminate dependence on the specific monitor i. Note that $\bar{n} = \rho A - 1$. 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 $\gamma^* = 1/\bar{n}$ since $\partial W(q,\gamma^*)/\partial\gamma = 0$ and $\partial^2 W(q,\gamma^*)/\partial\gamma^2 > 0$. As argued before, the total time until the activity of the jammer is assumed to stop is $D(q,\gamma) + W(q,\gamma)$ and goes to infinity when:

- $q = 0$, which essentially means no jamming and hence infinite detection time,
- $q = 1$, namely in the scenario of continual jamming, where the notification time is infinite,
- $\gamma = 0$, namely in absence of network transmissions, where no collision can be observed and detection time goes to infinity.
- $\gamma = 1$, where all network transmissions fail due to excessive contention regardless of existence of an adversary.

In Fig. 2, we plot the detection delay $D(\cdot)$ and notification delay $W(\cdot)$ as functions of jamming probability q, for $0.001 \le q \le 0.999$. Since the values of delay are large, we show results in logarithmic scales. Fig. 2 verifies our remark that the total delay $D(q,\gamma) + W(q,\gamma)$ approaches infinity as q approaches 0 and 1. It can also be observed from Fig. 2 that there can be two different values of q that achieve the same total delay $D(\cdot) + W(\cdot)$. Smaller values of q correspond to larger detection delays but smaller notification delays, while larger values of q result in faster detection and slower notification.

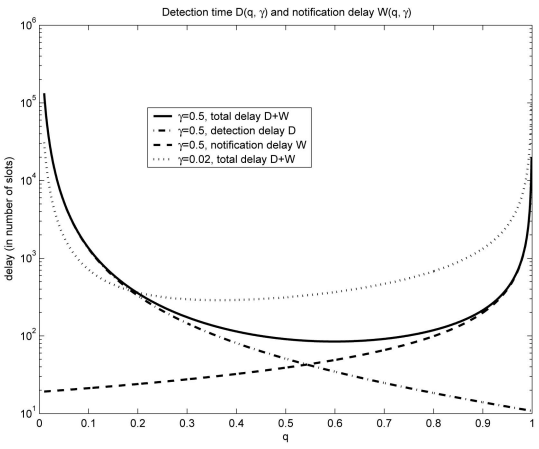

Fig. 2. The detection delay $D(\cdot)$, notification delay $W(\cdot)$, and total delay $D(\cdot) + W(\cdot)$ as functions of jamming probability q for $0.001 \le q \le 0.999$.

3 Attacker and Network Payoffs

In the sequel, we define various forms of payoffs for the attacker and the network.

3.1 Instantaneous Payoff

The payoff of the attacker is measured in total number of corrupted links. The *instantaneous payoff* for the attacker, U_{mI}, is defined as the *expected number of additionally corrupted links* in a slot besides the ones due to legitimate contention. This payoff depends on jamming probability q and access probability γ and we denote it as $U_{mI}(q,\gamma)$. To obtain an analytic expression for $U_{mI}(q,\gamma)$, we first derive an expression for 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 $\rho\gamma$. Moreover, total number of transmitters X in the jammed area $A_m = \pi R_m^2$ is Poisson distributed with spatial density $\lambda = \rho\gamma$ [21]. 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 region A the number of transmitters and receivers are Poisson distributed with mean $A\rho\gamma$ and $A\rho(1-\gamma)$, respectively. A transmission is successful if there is no other transmitter in a receiver's transmission range area $A = \pi R^2$ and there is at least one receiver in the transmitter's transmission range area A. The success probability of an attempted transmission, p_s is

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

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 and p_s and its conditional mean is $\mathbb{E}[Y|X=x] = xp_s$. Since the adversary launches an attack after sensing and all transmission links in its transmission range will be corrupted, the

payoff for the jammer in a slot will be $\mathbb{E}[Y]$. Recall that X is Poisson distributed with mean $A_m\rho\gamma$. We have

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

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

$$U_{mI}(q,\gamma) = q\,\mathbb{E}[\,Y\,] = qA_mA(\rho\gamma)^2\big(e^{-\rho\gamma A} - e^{-\rho A}\big), \qquad (9)$$

and is linearly increasing with q.

The network performance metric is the throughput measured in total number of successful transmissions in each slot. The network *instantaneous payoff* in the absence of jammer is

$$U_I(\gamma) = \mathbb{E}[\,Y\,] = A_mA(\rho\gamma)^2\big(e^{-\rho\gamma A} - e^{-\rho A}\big), \qquad (10)$$

which has a global maximum with respect to γ. For sufficiently large values of ρ, it is $\mathbb{E}[\,Y\,] \approx A_mA(\rho\gamma)^2e^{-\rho\gamma A}$, which has a maximum at $\gamma = \frac{2}{A\rho}$.

In the presence of a jammer, the instantaneous payoff for the network is $U_I(q,\gamma) = (1-q)\mathbb{E}[Y]$. Regardless of a jammer's existence, this network payoff is zero for $\gamma = 0$ as no node delivers messages in the network; the payoff is also zero for $\gamma = 1$ as all transmissions are blocked due to high contention.

3.2 Cumulative Payoff

The *cumulative payoff* U_{mC} for the attacker is the number of achieved jammed links until the jammer is detected and the notification message is transferred out of the jammed area. The cumulative payoff of the jammer for $q > 0$ is

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

The cumulative payoff $U_{mC}(q,\gamma)$ goes to infinity for $q \to 0$ and $q \to 1$. For $q \to 0$, the jammer tends to become undetectable and the number of disrupted links over an infinite time adds up to infinity. For $q \to 1$, although the detection time is minimal, the channel is completely occupied by the adversary and nodes are prevented from accessing it and transferring the attack message out of the jammed area, and hence the damage caused also goes to infinity.

The cumulative payoff for the network is

$$U_C(q,\gamma) = (1-q)U_I(\gamma)\times[D(q,\gamma)+W(q,\gamma)] \qquad (12)$$

and is increasing with γ.

3.3 Weighted Cumulative Payoff

Oftentimes sensor networks are *event driven* in the sense that a large amount of network traffic is generated upon detection of an event. In such scenarios, traffic is time critical, namely, the less the latency experienced until the intended destination, the higher its value. On the other hand, information that is not delivered in time becomes obsolete and of less use to the network. In that case, the goal of the adversary is to jam the messages sooner as it will cause larger disruption to the network. To model the time dependence of the payoff, we introduce a weighting factor r, with $0 \le r \le 1$. As in [15], the reward of the adversary in future slots become less important by applying such a discounting factor. The instantaneous payoff for the adversary at slot $k+1$ is recursively given as $U_{mI}(q,\gamma,k+1) = rU_{mI}(q,\gamma,k) = r^kU_{mI}(q,\gamma)$, for $k > 0$ and $U_{mI}(q,\gamma)$ defined in (9). The adversary *weighted cumulative payoff* up to slot k is defined as

$$\begin{aligned}U_{mW}(q,\gamma,k) &= \sum_{\tau=0}^{k-1} r^\tau U_{mI}(q,\gamma) \qquad (13)\\ &= \frac{1-r^k}{1-r}U_{mI}(q,\gamma), \qquad \text{for } 0 \le r < 1,\\ &= k \times U_{mI}(q,\gamma), \qquad \text{for } r = 1. \qquad (14)\end{aligned}$$

The weighted cumulative payoff is a general representation of the payoff and reduces to instantaneous payoff when $r = 0$ and to cumulative payoff when $r = 1$.

The jammer's weighted cumulative payoff for $r < 1$ is

$$U_{mW}(q,\gamma,D+W) = \frac{qU_I(\gamma)\big[1-r^{[D(q,\gamma)+W(q,\gamma)]}\big]}{1-r}. \qquad (15)$$

When $q \to 0$ or $q \to 1$, the total delay $D(q,\gamma)+W(q,\gamma)$ goes to infinity. Then, $r^{(D(q,\gamma)+W(q,\gamma))} \to 0$ and $U_{mW}(\cdot)$ approximates $\frac{qU_I(q,\gamma)}{1-r}$. Unlike the cumulative payoff $U_{mC}(\cdot)$, the weighted cumulative payoff $U_{mW}(\cdot)$ with $r < 1$ approaches 0 when $q \to 0$, and $U_I(1,\gamma)/(1-r)$ when $q \to 1$. When $q \to 0$, the instantaneous payoff is minimal and the payoff is discounted with time, so the weighted sum is close to 0. When $q \to 1$, the future payoff is diminished with time and, hence, the total payoff approaches a value that is independent of q rather than infinity.

In Fig. 3, we present the adversary's cumulative payoff $U_{mC}(\cdot)$ (i.e., with $r = 1$) and weighted cumulative payoff $U_{mW}(\cdot)$ (with $r < 1$) with respect to detection and notification delay for different values of γ. The range of total delays is obtained by varying the jamming probability q in the range $0.001 \le q \le 0.999$. Since the delay and payoff values are large, we show results in logarithmic scales. Fig. 3a shows that $U_{mC}(\cdot)$ tends to increase with the total delay, which indicates that if the adversary can prolong detection and/or notification time, then its payoff will increase. As reported above, there exist two different values of q that attain the same total delay $D(q,\gamma)+W(q,\gamma)$: the larger such value of q yields a larger payoff as $U_{mC}(q,\gamma) = qU_I(\gamma)[D(q,\gamma) + W(q,\gamma)]$. Unlike $U_{mC}(\cdot)$, $U_{mW}(\cdot)$ (with $r < 1$) either decreases or increases with total delay depending on the values of q. The payoff around the larger of the two values of q tends to increase with total delay. Finally, for a given total delay and decaying factor r ($0 \le r \le 1$), the adversary's payoff increases with respect to the network access probability γ, as illustrated in Figs. 3a and 3b.

The weighted cumulative payoff for the network is

$$U_W(q,\gamma,D+W) = \frac{(1-q)U_I(\gamma)\big[1-r^{[D(q,\gamma)+W(q,\gamma)]}\big]}{1-r}. \qquad (16)$$

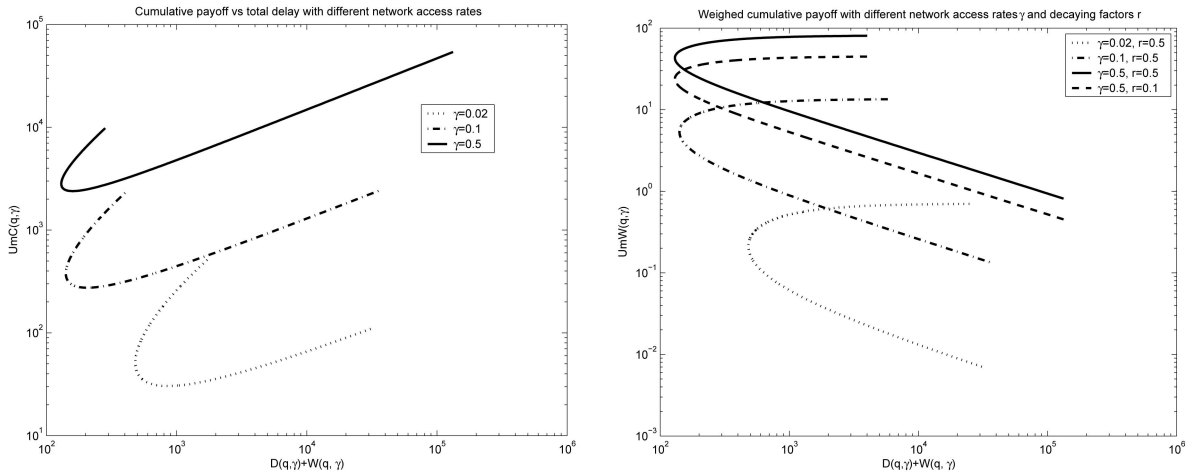

Fig. 3. The adversary's cumulative payoff $U_{mC}(\cdot)$ and weighted cumulative payoff $U_{mW}(\cdot)$ with respect to total delay $D(\cdot)+W(\cdot)$ when jamming probability $0.001 \leq q \leq 0.999$. As a numerical example, we consider a sensor network with the following parameters: node density $\rho = 0.0025$, sensor transmission range $R = 20$ m, and jammer transmission range $R_m = 200$ m. Unless otherwise stated, these parameters are used throughout the paper. (a) Cumulative payoff versus delay (i.e., decaying factor $r = 1$). (b) Weighted cumulative payoff versus delay.

4 Optimal Jamming Attack and Defense Policies as Solutions to Optimization Problems

The objective of the adversary is to increase the total number of corrupted links before the attack is detected and the notification alarm is propagated. Following detection, a notification message needs to be passed out of the jammed area and, hence, the damage caused to the network is ceased. An aggressive attack, namely one with large q has a potential to corrupt more links in successive time slots. Nevertheless, this will be detected relatively quickly due to the large percentage of incurred collisions compared to the nominal one. On the other hand, a milder attack, namely one with smaller q may turn out to be more beneficial for the attacker. A significant incentive for the attacker to expedite link jamming is when jamming time-critical information. This situation is captured by the weighted cumulative payoff. As a first line of defense, the network selects the access probability γ to control the number of successful transmissions given its energy limitations and at the same time expose the attacker by reducing the number of required samples to obtain a decision. Another useful network constraint is to attempt to maintain a certain minimum level of throughput in the presence of an attack.

We formulate optimization problems to derive optimal strategies of the jammer and the network. For both the adversary and the network, the following performance metrics are meaningful: the total delay $D(q,\gamma)+W(q,\gamma)$, the payoff, and the energy consumption. In the formulation of an optimization problem, we may define one of the above as the problem objective and choose the other two as constraints. We define the total delay as objective for the jammer and the network.

4.1 Constant Jamming Power and One Monitor Node

We study the scenario where the adversary has constant jamming power and the network has one designated monitor node. The objective function is total delay $D(q,\gamma)+W(q,\gamma)$. The adversary tries to maximize it by controlling its strategy q, while the network tries to minimize it by selecting γ. Both entities select their strategies subject to energy limitations and payoff constraints.

The problem faced by the attacker is:

$$\begin{aligned} \max_{0<q\leq 1} \quad & D(q,\gamma)+W(q,\gamma) \\ \text{s.t.} \quad & qP_m[D(q,\gamma)+W(q,\gamma)] \leq E_m \\ & U_{mW}(q,\gamma,D(q,\gamma)+W(q,\gamma)) \geq U_m^0, \end{aligned} \tag{17}$$

where the payoff threshold U_m^0 denotes a minimum required payoff for the jammer.

Remark. A note about constraint (17) is necessary here. This constraint accounts for the scenario where, at the point when detection and notification message passing has occurred, the adversary's consumed energy is less than its initial energy E_m. That is, the formulation above implies that the adversary has sufficient energy to cause damage to the network. However, it might happen as well that the adversary chooses to induce disruption to the network and its energy is depleted before detection, in which case it will not be detected. The corresponding problem formulation is:

$$\begin{aligned} \max_{0<q\leq 1} \quad & D(q,\gamma) \\ \text{s.t.} \quad & qP_m D(q,\gamma) \geq E_m, \end{aligned} \tag{18}$$

$$U_{mW}\left(q,\gamma,\frac{E_m}{qP_m}\right) \geq U_m^0. \tag{19}$$

Further, the payoff constraint (19) is:

$$q\frac{E_m}{qP_m} \geq U_m^0/U_I(\gamma) \text{ for } r=1, \tag{20}$$

$$q\left[1-r^{\left(\frac{E_m}{qP_m}\right)}\right] \geq (1-r)U_m^0/U_I(\gamma) \quad \text{for } 0 \leq r < 1. \tag{21}$$

We first consider the case with $r = 1$. Function $qD(q,\gamma)$ is decreasing in q; therefore, the energy constraint (18) limits the solution q^* to be in interval $(0, q_1]$, where q_1 is obtained as solution after taking (18) to be equality. Observe that the

payoff constraint reduces to $E_m/P_m \geq U_m^0/U_I$ and q vanishes. Depending on the values of γ, the inequality $E_m/P_m \geq U_m^0/U_I$ may not hold, which implies the adversary energy is insufficient to achieve its preassigned payoff, and then there exists no feasible q. Otherwise, if $E_m/P_m \geq U_m^0/U_I$, the payoff constraint can be satisfied for the given energy, and the optimal solution $q^* \to 0$ as the objective function $D(q,\gamma)$ decreases with q.

For $0 \leq r < 1$, the payoff constraint (21) gives the lower bound on q^*, which is approximately $(1-r)U_m^0/U_I(\gamma)$ (assuming the exponent of r is fairly large). If the lower bound $(1-r)U_m^0/U_I(\gamma) \geq 1$, which indicates the payoff goal is too excessive for the jammer to satisfy, then no feasible solution exists. If the lower bound $(1-r)U_m^0/U_I(\gamma) < 1$ and the upper bound $q_1 \geq (1-r)U_m^0/U_I(\gamma)$, then the optimal strategy $q^* = (1-r)U_m^0/U_I(\gamma)$, which is given by the payoff constraint. Otherwise, there is no feasible solution q that can avoid detection while still achieving the predetermined payoff U_m^0. This payoff captures the jammer payoff within a certain time frame. By concentrating its efforts on this time frame, the jammer corrupts time-critical information transmission in the network.

The corresponding objective for the network is:

$$\begin{aligned} \min_{0\leq\gamma\leq 1} \quad & D(q,\gamma) + W(q,\gamma) \\ \text{s.t.} \quad & \gamma P[D(q,\gamma) + W(q,\gamma)] \leq E \qquad (22) \\ & U_W(q,\gamma, D(q,\gamma) + W(q,\gamma)) \geq U^0, \qquad (23) \end{aligned}$$

where the network cumulative payoff $U_W(q,\gamma)$ is given by (16), U^0 is a network payoff threshold and E is the amount of network energy reserve denoting that sensor nodes should have spare energy during the detection and notification interval. Threshold U^0 serves the purpose of avoiding network defense policies with small γ and accounts for the fact that the network aims at a certain minimum amount of throughput while defending itself against the attack by essentially trying to make the attacker more visible to the detection system.

The attacker and network optimization problems above obtain different twists depending on the amount of knowledge of the attacker and the network about each other. In the sequel, we study two cases reflecting different instances of knowledge.

4.1.1 Case 1: Perfect Knowledge of Attacker and Network

First, we assume that the attacker possesses all necessary knowledge that allows it to compute the optimal strategy q. That is, the attacker knows the network strategy, namely the access probability γ. Another piece of information in the disposal of the jammer is the number of neighbors of the monitor node that enables comparison of the collision pattern caused by its strategy q to the nominal collision pattern. Although the perfect knowledge assumption is quite strong and restrictive, it is interesting to study for benchmarking purposes. We start with the attacker problem. Since the detection time tends to infinity at $q = 0$ and 1, the attacker's strategy is determined by the energy and payoff constraints as:

$$q[D(q,\gamma) + W(q,\gamma)] \leq E_m/P_m, \qquad (24)$$

$$q[D(q,\gamma) + W(q,\gamma)] \geq U_m^0/U_I(\gamma) \quad \text{for } r = 1; \qquad (25)$$

$$q\Big(1 - r^{[D(q,\gamma)+W(q,\gamma)]}\Big) \geq (1-r)U_m^0/U_I(\gamma) \quad \text{for } 0 \leq r < 1. \qquad (26)$$

Observe that the left-hand sides of inequalities (24) and (25) are the same, and let us denote it by $F(q) = q(D(q,\gamma) + W(q,\gamma))$. Function $F(q)$ approaches infinity at $q = 0$ and $q = 1$ and has a minimum in [0, 1], as shown in Fig. 2. A proof for that fact is included in the Appendix. Let $f_{\min}$ be the minimum value of $F(q)$. By comparing $f_{\min}$, E_m/P_m, and $U_m^0/U_I(\gamma)$, we distinguish three cases for the solution when $r = 1$ as follows:

1. If $E_m/P_m < \max\{U_m^0/U_I(\gamma), f_{\min}\}$, there is no feasible solution q, since the attacker cannot cause a given level of damage due to energy limitations.
2. If $E_m/P_m \geq U_m^0/U_I(\gamma) \geq f_{\min}$, the energy constraint (17) or (24) 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. Recall from Fig. 2 that total delay tends to infinity for $q \to 0$ or $q \to 1$. However, the finite energy E_m cannot sustain the infinite delay. Therefore, the energy constraint bounds the value of q to be away from either 0 or 1. On the other hand, the payoff constraint (25) yields a range of feasible values for q, $[0, q_3]$, and $[q_4, 1]$. Note that since $E_m/P_m \geq U_m^0/U_I(\gamma)$, the following must hold: $q_1 \leq q_3$ and $q_2 \geq q_4$, i.e., there are two ranges of feasible values for q, $[q_1, q_3]$, and $[q_4, q_2]$. We have $D(q,\gamma) + W(q,\gamma) = F(q)/q$ and $F(q_1) = F(q_2) \geq F(q_3) = F(q_4)$ with $q_1 \leq q_3 \leq q_4 \leq q_2$ and also $F(q_1)/q_1 > \max\{F(q_2)/q_2, F(q_3)/q_3, F(q_4)/q_4\}$, hence $q^* = q_1$.
3. If $E_m/P_m \geq f_{\min} \geq U_m^0/U_I(\gamma)$, the payoff constraint (25) is automatically satisfied for $q \in [0,1]$. Hence, the solution q^* is determined 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 (17) with equality. From the solution, it follows that optimal strategies for the attacker tend to be rather mild and long term.

When $0 \leq r < 1$, the adversary needs to focus on short-term payoff as the payoff decays with time. The payoff constraint (26) imposes a lower bound on the optimal value of q assuming that $r^{(D(q,\gamma)+W(q,\gamma))} \approx 0$ when $D(q,\gamma) + W(q,\gamma)$ is sufficiently large. The lower bound approximates $(1-r)U_m^0/U_I(\gamma)$. Recall that the energy constraint limits values of q in interval $[q_1, q_2]$. The following cases appear:

- If $q_2 < (1-r)U_m^0/U_I(\gamma)$, there is no feasible solution that satisfies both the energy and payoff constraints.
- If $q_2 \geq (1-r)U_m^0/U_I(\gamma) \geq q_1$, then $q^* = q_2$. The optimal strategy for the adversary when $r < 1$ is rather aggressive, short-term one.
- If $(1-r)U_m^0/U_I(\gamma) < q_1$, then $q^* = q_1$ and the optimal solution is the same as the one with $r = 1$.

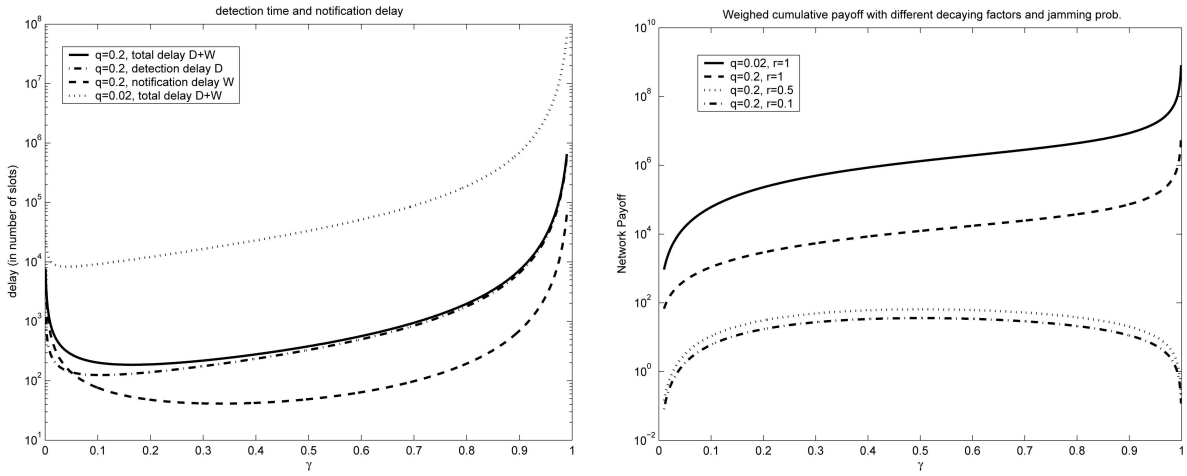

Fig. 4. The detection delay $D(\cdot)$, notification delay $W(\cdot)$, total delay $D(\cdot)+W(\cdot)$, and network payoff $U_W(\cdot)$ as functions of network access probability γ for $0.001 \leq \gamma \leq 0.999$. (a) Total delay versus γ. (b) Network payoff versus γ.

We conclude that regardless of the weighting factor, the optimal strategy for the adversary, if it exists, is determined by the energy constraint.

We now proceed to the network problem. The network knows the jamming strategy q and jammer factor r and it needs to find transmission probability γ^* that minimizes the sum of detection plus notification time. Recall that the objective function $D(\cdot)+W(\cdot)$ is infinite for $\gamma=0$ and $\gamma=1$. Similar to the approach of proving the claim in the Appendix, it can be shown that the total delay has a minimum at a point γ, denoted as $\gamma_{\min}$.

As $\gamma[D(q,\gamma)+W(q,\gamma)]$ is monotonically increasing in γ, the energy constraint (22) imposes an upper bound on feasible values of γ, denoted by γ_u, which is obtained by making the energy constraint an equality. The network payoff (23) can be rewritten as in (12) for $r=1$ and (16) for $0 \leq r < 1$. In the sequel, we differentiate the case of $r=1$ from that of $0 \leq r < 1$ in the network problem.

For $r=1$, the network cumulative payoff given by (12) and appearing in the left-hand side of inequality (23) is monotonically increasing with γ. Therefore, the payoff constraint (23) imposes a lower bound on γ denoted as γ_l. By comparing the γ_l, γ_u, and $\gamma_{\min}$, we derive three cases for the solution:

- If $\gamma_l > \gamma_u$, there is no feasible solution, since the network has a high payoff requirement and limited energy.
- If $\gamma_l < \gamma_u$ and $\gamma_{\min} \in [\gamma_l, \gamma_u]$, the optimal $\gamma^* = \gamma_{\min}$.
- Otherwise, $\gamma^* = \gamma_l$ or $\gamma^* = \gamma_u$ and the solution is dictated by the payoff or the energy threshold.

When $0 \leq r < 1$, the network weighted cumulative payoff is

$$U_W(q,\gamma) \approx \frac{(1-q)U_I(\gamma)}{1-r}.$$

The approximation is due to the fact that $D(q,\gamma)+W(q,\gamma)$ are sufficiently large (as demonstrated in Fig. 4a) and hence $r^{[D(q,\gamma)+W(q,\gamma)]} \approx 0$. It follows that $U_W(\cdot,\gamma) = \mu U_I(\gamma)$, where μ is some value independent of γ. Similar to $U_I(\gamma)$ given in (10), $U_W(\cdot,\gamma)$ has a global maximum with respect to γ, denoted as $U_{W_{\max}}$. Payoff $U_W(\cdot,\gamma)$ is zero for $\gamma=0$ and $\gamma=1$. If $U_{W_{\max}} < U^0$, the constraint (23) cannot be satisfied and hence there is no solution of γ for such a high payoff requirement. Otherwise, the constraint $U_W(\cdot,\gamma) > U^0$ specifies the values of γ to be $[\gamma_{pl}, \gamma_{pu}]$. Similar to the case with $r=1$, there exist three cases for the solution.

- If $\gamma_u < \gamma_{pl}$, no feasible solution exists, as the network cannot achieve the high payoff threshold with given energy budget.
- If $\gamma_{pl} \leq \gamma_{\min} \leq \min(\gamma_u, \gamma_{pu})$, the optimal solution is $\gamma^* = \gamma_{\min}$.
- Otherwise, $\gamma^* = \min(\gamma_u, \gamma_{pu})$ or $\gamma^* = \gamma_{pl}$ and the optimal network access probability is defined by the energy constraint or the payoff constraint.

In Fig. 4, we plot the total delay and network payoff $U_W(\cdot)$ as functions of γ for $0.001 \leq \gamma \leq 0.999$ and for different values of jamming probability q and weighting factors r. Logarithmic scale is again used for delays and payoffs. Fig. 4a depicts the convexity of total delay as a function of γ and the fact that it approaches infinity for $\gamma \to 0$ and $\gamma \to 1$. As shown in Fig. 4b, the network cumulative payoff $U_C(\cdot)$ (which equals U_W if $r=1$), monotonically increases with respect to γ. In contrast for $r<1$, $U_W(\cdot)$ is a concave function of γ. It has several maxima and it reaches zero at $\gamma \to 0$ and $\gamma \to 1$. From Fig. 4b, it is clear that smaller q's result in larger network payoff as expected, since fewer transmissions are corrupted due to jamming in that case.

4.1.2 Case 2: Lack of the Knowledge of Attacker and Network

We now proceed to the case where the perfect knowledge assumption of the previous subsection does not hold. In the sequel, we focus on the payoffs $U_{mW}(\cdot)$, $U_W(\cdot)$ with $r=1$, namely the cumulative payoffs $U_{mC}(\cdot)$ and $U_C(\cdot)$. The treatment for $r<1$ is similar.

Suppose that the attacker and the network do not know the other's strategy but know essential topology information such as the number of neighbors of the monitor node. One approach for the attacker may be to choose q so as to respond optimally to the worst-case (for the adversary) scenario of

network defense, namely to the scenario where the network operates with a γ that minimizes the attacker objective function. Admittedly, this approach is rather conservative. The attacker payoff in that case is a lower bound for the set of incurred attacker payoffs over all network defense policies. The problem to be solved by the attacker is:

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

In order to approximately compute the solution of the max-min problem above, the adversary can start with a large number, M of candidate values of γ, $\gamma_j \in [0,1]$, for $j = 1\ldots, M$. For example, we use $M = 100$ in the subsequent computations. For each γ_j, the adversary finds the q_j^* that maximizes $D(q,\gamma_j)+W(q,\gamma_j)$ subject to the problem constraints. The attacker chooses among all the q_j^*'s the one that corresponds to the smallest value of $D(q_j^*,\gamma_j)+W(q_j^*,\gamma_j)$, for $j = 1\ldots, M$. Clearly, the approximation of the solution becomes better with larger values of M.

Similarly, the network takes the conservative approach that the attacker performs the optimal attack and solves the following problem for responding to this attack:

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

and applies the methodology outlined above to derive an approximate solution. The solution to this problem is an upper bound for resulting 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 $U^0 = 500$, attacker transmission range $R_m = 200$ m, energy constraint $E_m/P_m = 1{,}000$ units, target attacker payoff $U_m^0 = 500$, and probabilities of false alarm and detection $p_{FA} = 0.02$ and $p_D = 0.98$.

Taking the solution approach outlined above, we obtain the numerical solution for the adversary as $q^* = 0.87$ with an estimated minimum total delay of 1.137×10^3 slots for lack of knowledge about γ. The solution for the network is $\gamma^* = 0.026$ with the estimated maximum delay equal to 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 optimal $q^* = 0.828$ and cause delay 1.506×10^3, which is larger than the minimum delay estimated by the adversary when having no knowledge about γ. Thus, to incur the largest delay subject to its 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 detection and notification delay to just 414 slots. We note that the delay of 414 slots is less than 1.206×10^3, which is obtained if the adversary and the network do not know each other's transmission probability and solve their own max-min or min-max problem independently. We also note that 414 is less than the minimum delay 1.137×10^3 as 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.

Besides the aforementioned min-max and max-min approaches, an alternative formulation can model lack of knowledge of the attacker and the network about each other. The attacker (or the network) average over the (unknown) strategy of the other. The adversary (or network, respectively) can assume that the network access probability (jamming probability, respectively) is uniformly distributed in $[0,1]$ if no further prior knowledge is available. The attacker problem is formulated as

$$\begin{aligned} \max_{0<q\le 1} \quad & \int_0^1 [D(q,\gamma)+W(q,\gamma)]d\gamma \\ \text{s.t.} \quad & qP_m \int_0^1 [D(q,\gamma)+W(q,\gamma)]d\gamma \le E_m \\ & \int_0^1 U_{mC}(q,\gamma)d\gamma \ge U_m^0. \end{aligned}$$

If some knowledge about the distribution and range of network strategy γ is available, it can be incorporated in the problem formulation. The corresponding problem for the network is:

$$\begin{aligned} \min_{0\le\gamma\le 1} \quad & \int_0^1 [D(q,\gamma)+W(q,\gamma)]dq \\ \text{s.t.} \quad & \gamma P \int_0^1 [D(q,\gamma)+W(q,\gamma)]dq \le E \\ & \int_0^1 U_C(q,\gamma)d\gamma \ge U^0. \end{aligned}$$

These problems can be approximately solved with numerical methods due to the difficulty in some of the expressions in the integrals. In the sequel, we provide one such approach for the attacker problem. We start with a large number of candidate values for q, say q_i, $i = 1,\ldots, M$. For each q_i the adversary approximates $\int_0^1 [D(q_i,\gamma) + W(q_i,\gamma)]d\gamma$ by a summation and chooses among all q_i the one that maximizes total delay while satisfying the constraints. The network can take a similar approach. Using the numerical method above, we have approximated the solution for the adversary as $q^* = 0.341$ with an average delay of 2.931×10^3 slots, and the solution for the network as $\gamma^* = 0.139$ with average delay of 660 slots. If the network knows $q = 0.341$, it can solve for $\gamma^* = 0.232$ which results in a delay of 111 slots. When compared to a minimum delay of 414 slots guaranteed by the max-min approach (i.e., with $q^* = 0.87$), the solution for the adversary that is obtained by averaging over the unknown strategy of the network yields worse performance, as the minimum delay with $q^* = 0.341$ can be as small as 111 units. This result of the comparison is expected, as solutions using max-min and min-max approaches provide conservative performance guarantees for the worst-case strategy of the opponent.

The adversary may obtain knowledge about the network parameters by simply observing network operation (without launching jamming) and estimating γ. However, the approaches above that model lack of knowledge can be

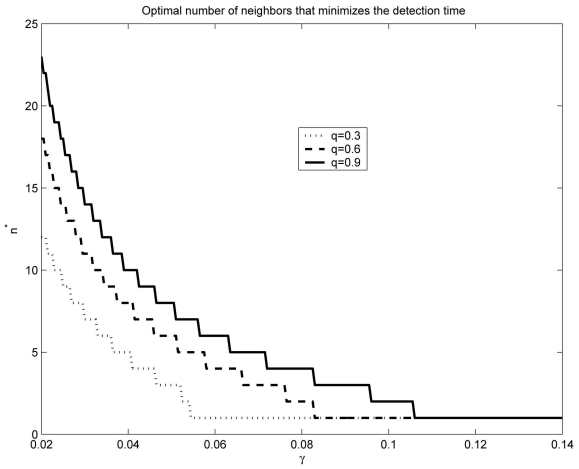

Fig. 5. The optimal number of neighbors n, n^* that minimizes the detection time versus γ for different values of q.

adopted by the adversary if the network strategy γ varies with time. On the other hand, more often than not, the network will have no knowledge of the strategy of the jammer and hence the min-max and averaging approaches are applicable.

4.2 Constant Jamming Power and Multiple Monitor Nodes

We extend the problem for the case where there exist several monitor nodes to provide measurement diversity. Here, arises the issue that different monitor nodes have different perceptions of the probability of collision under normal conditions, as they have different numbers of neighbors. As a result, monitors which have different numbers of neighbors reach a determination of whether or not an attack exists at different times. That is, detection delay is highly dependent on the monitor node. Nodes can be classified in classes $\mathcal{C}_1, \ldots, \mathcal{C}_K$, such that nodes of class $\mathcal{C}_n$ have n neighbors for $1 < n \leq n_{\max}$. Clearly, we would like to assign the role of a monitor to nodes of an appropriate class with n^* neighbors so as to minimize detection time. In Fig. 5, we plot the number of neighbors that minimizes detection time as a function of γ for different jamming probabilities $q = 0.3$, $q = 0.6$, and $q = 0.9$, as numerically computed using MATLAB. We observe that as γ increases from zero, the optimal number of neighbors approaches $n^* = 1$. This is quite intuitive since in the case of one neighbor, a small amount of collisions are caused in nominal network operation and hence the monitor can quickly distinguish an increased percentage of collisions due to attack. However, when γ is extremely small, a larger number of neighbors than $n^* = 1$ are needed in order for the monitor to observe transmissions and collisions so to detect jamming quickly.

Given the conclusion above, the attacker should choose its strategy so as to *balance* detection delays of different monitors. For sufficiently large values of γ which will usually be the case, the attacker needs to focus only on class $\mathcal{C}_1$ of monitors with one neighbor. When γ is small, e.g., $\gamma < 0.05$, the detection delay balancing problem of different monitors is meaningful and can be stated as:

$$\max_{0<q\leq 1} \min_{i\in\{1,\ldots,K\}} D(q, \gamma, \mathcal{C}_i), \tag{27}$$

where notation $D(q, \gamma, \mathcal{C}_i)$ denotes the dependence of detection delay on the monitor class. Since detection delay is decreasing with q regardless of number of neighbors, the smallest feasible q is the solution for the attacker.

We note than in the formulation above, we considered the detection delay rather than total delay since the notification delay depends heavily on the location of the monitor which may not be known to the attacker. On the other hand, our assumption is valid for a dense sensor network where monitor nodes with one neighbor are mostly located close to the boundary of the jammed area. Hence, the notification time is negligible and the total delay is well approximated by only the detection delay.

4.3 Controllable Jamming Power and Multiple Monitor Nodes

We now consider the more general problem where the jammer can choose a 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 $\sum_{j=1}^{L} q_j = q$. Thus, the jammer jams with some power with probability q and remains idle with probability $q_0 = 1 - q$. Without loss of generality and to avoid the trivial solution $q_0 = 1$, we let $q_0 < 1$ so that $0 < \sum_{j=1}^{L} q_j \leq 1$. Different jamming power levels P_j lead to different jamming areas $A_{m,j}$ of radii $R_{m,j}$. Define zone j to be the ring bounded by circles with radii $R_{m,j}$ and $R_{m,j-1}$, i.e., the area covered by power level $P_{m,j}$ but not by $P_{m,j-1}$. The average number of transmission links in $A_{m,j}$ is

$$S_j = A_{m,j} A (\rho\gamma)^2 (e^{-\rho\gamma A} - e^{-\rho A}).$$

We assume that the network is dense enough such that there always exists a monitor node in each zone. A node in zone j perceives jamming with probability $\sum_{\ell=j}^{L} q_\ell$. The average number of required hops to traverse zone j is approximately $(R_{m,j+1} - R_{m,j})/2$ according to our previous assumptions.

An interesting trade-off arises here. Monitors in different zones exhibit different detection and notification delays for a given jamming strategy. Monitors located in outer zones perceive lower jamming probability and hence the detection delay 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 faster. On the other hand, monitors located in inner zones perceive a more aggressive attack and may detect it faster, but they need more time to pass the notification message out of the jammed area. The goal of the attacker is to find a jamming strategy that optimally addresses this trade-off. The attacker strategy consists of choosing vector $\mathbf{q} = (q_0, q_1, \ldots, q_L)$ to maximize the minimum of total delays experienced by monitors in different zones. Denote by $W(q, \gamma, d)$ the notification delay experienced by a message starting from a monitor node in a zone of average length d with perceived jamming probability q and network access probability γ. We also denote $R_{m,j}$ by R_j. Then, clearly the total notification time equals the sum of notification times through the traversed zones from the monitor to the boundary of the jammed area. The attacker objective is formulated as follows:

$$\max_{0\le q_j\le 1}\min_{j=1,\ldots,L} T_j(\mathbf{q},\gamma), \tag{28}$$

where

$$T_j(\mathbf{q},\gamma)=D\left(\sum_{\ell=j}^{L} q_\ell,\gamma\right)+\sum_{i=0}^{L-j} W\left(\sum_{\ell=j+i}^{L} q_\ell,\gamma,\frac{R_{j+i}-R_{j+i-1}}{2}\right).$$

The first term denotes the detection delay by a monitor in zone j. The second term denotes the total delay in transferring the notification message out of the jammed area starting from zone j, where the average length of message traversal through zone j (averaged over the location of the monitor) is taken to be $(R_j - R_{j-1})/2$. We define variable $T=\min_{j=1,\ldots,L} T_j(\mathbf{q},\gamma)$. The problem constraints are a generalization of the energy and payoff constraints for constant jamming power as:

$$T\sum_{j=1}^{L} q_j P_{m,j}\le E_m, \tag{29}$$

$$T\sum_{j=1}^{L}\left(\sum_{\ell=j}^{L} q_\ell\right)(S_j-S_{j-1})\ge U_m^0, \tag{30}$$

and $\sum_{j=0}^{L} q_j = 1$, $q_0 < 1$. The constraint

$$T_j(\mathbf{q},\gamma)\ge T,\ \text{ for }\ j=1,\ldots,L, \tag{31}$$

emerges with definition of new variable $T(\cdot)$.

We now show a simple and intuitive heuristic for the attacker to tackle the problem above. For ease of notation, we 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. The algorithm goes as follows: Start with jamming the largest region and find the probability of jamming $q_L^*=q$ by solving problem $\max_{q_L} D(q_L,\gamma)+W(q_L,R_L/2)$ subject to the constraints. Let a be the maximum value of the objective. Now assume that two power levels with ranges R_{L-1} and R_L are employed. The attacker needs to deduce whether the use of two power levels is more beneficial to it than the use of a single power level. Fix the jamming probability to q and solve

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

where the notification terms denote the required time for a monitor in the *inner* circle to pass the alarm through the two zones. Let the optimal value of the objective be a_1. Compare with 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 in that case be a_2. The value $\min\{a_1,a_2\}$ is the total delay for two power levels. Let q_{L-1}^* be the jamming probability that achieves this delay. If $\min\{a_1,a_2\}>a$, 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 profitable.

We solve the problem numerically with $\rho=0.0025$, $R=20$ m, $U_m^0=500$, and $L=2$ power levels corresponding to ranges $R_{m,1}=100$ m and $R_{m,2}=200$ m. Also $E_m/P_{m,1}=500$ and $E_m/P_{m,2}=250$. The network access probability $\gamma=0.3$ is known to the attacker. We also assume different minimum number of neighbors per zone. In zones 1 and 2 (zone 1 being the inner one) the minimum numbers of monitors' neighbors are 3 and 7. For this scenario, the optimal strategy is $q_1^*=0.013, q_2^*=0.002$ with detection plus notification delay equal to 2.92×10^4. In addition to the scenario above, we also consider the following two scenarios: 1) The attacker energy is double, so $E_m/P_{m,1}=1{,}000$, $E_m/P_{m,2}=500$ and 2) The minimum number of neighbors of monitors in the two zones is 7 and 3, respectively. For the additional scenario 1 we found $q_1^*=0.027, q_2^*=0.000$ with total delay 3.44×10^4. For scenario 2 we got $q_1^*=0.000, q_2^*=0.027$ which yields a total delay of 9.93×10^3. The scenarios above reveal the impact of energy budget and of the number of neighbors of monitor nodes on the optimal jamming policy and resulting delay.

5 Discussion

In this work, we studied controllable jamming attacks against wireless sensor networks, and derived the optimal solutions that dictate optimal jamming attack and network defense strategies. On one hand, the attacker attempts to find an optimal trade-off between the severity of the attack and the extent to which it becomes detectable. On the other hand, the network aims at alleviating the effect of the attack and exposing the attacker to detection. Without loss of generality, we considered an Aloha type of protocol characterized by a common access probability for all sensor nodes. The reason for adhering to this admittedly simple protocol is to abstract out the protocol specifics and focus on the collective impact of network defense (captured through a single parameter) when confronting the attack. It is understood that a similar approach can be applied when the network operates under other channel access protocols such as CSMA that leverage more composite mechanisms such as back-off and contention window adaptation to regulate the amount of transmitted traffic. Jamming and defending strategies under these composite channel access protocols are left as a future research direction.

Although we adhere to a model with continuously backlogged nodes, sparse traffic patterns that do not follow this assumption can be handled by our models, as the sparse traffic scenarios only rely on observed samples that indirectly reveal the attacker. The difference is that for sparser network traffic the action of the jammer and the observation samples will be less frequent, yet our sequential algorithms capture this scenario as well. The payoff functions also capture different types of information data in terms of time criticality. Of particular interest is also the comparison between the case of perfect knowledge and a lack of knowledge of the attacker and the network about the other's strategy and the impact of knowledge availability on performance.

Our work is a first step toward understanding the structure of these problems, the interaction of opposing parties, the trade-offs between various forms of attacks, and the impact of different parameters on performance. There exist several directions for future study. A natural extension of this work is to study other forms of payoff functions, such as attacker's payoff modeled as the number of packets that fail to reach the destination, or the amount of network lifetime reduced by the attacker. These payoff functions will likely result in different optimal jamming and antijamming

strategies. In this paper, we solved the optimization problems separately from the viewpoints of the attacker and the network. The game-theoretic formulation that call for strategy pairs (q, γ) so that no party can benefit by deviating from that point is worth investigating.

Interesting issues arise in multichannel networks. In that case, the defense strategy space has an additional dimension, that of channel switching. On the other hand, the jammer should find the optimal trade-off between jamming costs when jamming more channels and jamming reward in terms of higher chances to corrupt ongoing communication. Another interesting issue is to formalize and model lack of knowledge for the attacker and the network besides the min-max, max-min, and strategy averaging approaches we mentioned. More enhanced versions of attacks can also be considered, such as the one with dynamic control of jamming probability as response to the network strategy, and the one modeled by a discrete or continuous set of jamming probabilities and a (discrete or continuous) probability distribution on that set.

Finally, mobility is a dimension that gives an interesting twist in the problem and has a direct impact on network performance. In a network of mobile nodes, one would expect the detection performance to deteriorate since potential attackers move in and out of range of an observer node with a detection system, hence the sequence of observations is intermittent. In that case, interesting topics to consider would be the impact of specific mobility patterns on detection performance and how to engineer mobility patterns of defender nodes in order to alleviate the impact of attacks.

APPENDIX

Claim 1. *Function $F(q) = q[D(q,\gamma) + W(q,\gamma)]$ has a minimum with respect to q, for $q \in [0,1]$.*

Proof. We first show that $(qD(q,\cdot))' \leq 0$, i.e., $qD(q,\cdot)$ is a decreasing function in q. Let

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

where C is defined in (2.3). As $\theta_1 \geq \theta_0 \geq 0$, it is easy to prove that $g(q) \geq 0$. Based on (7), $qD(q,\cdot) = \frac{Cq}{g(q)}$ and $C > 0$.

We have $(\frac{q}{g(q)})' = \frac{g(q)-qg'(q)}{g^2(q)}$. As $g^2(q) \leq 0$ always holds, the problem of proving the nonpositiveness of $(qD(q,\cdot))'$ is reduced to proving $g(q) - qg'(q) < 0$. Let $h(q) = g(q) - qg'(q)$.

Note that $\theta_1 = \theta_0 + cq$, where $c = n_i\gamma(1-\gamma)^{(n_i-1)} > 0$ is a linear function of q. Hence, $g''(q) = c \cdot g''(\theta_1) = c \cdot (\log\frac{\theta_1}{\theta_0} - \log\frac{1-\theta_0}{1-\theta_1})' = c \cdot \frac{1}{\theta_1(1-\theta_1)} \geq 0$. Furthermore, $h'(q) = (g(q) - qg'(q))' = -qg''(q) < 0$. We also note that $g(0) = 0$ and $g'(0) = 0$; therefore, $h(0) = 0$. We can conclude that $h(q)$ is a decreasing function with the maximum 0 achieved at $q = 0$, and hence $h(q) \leq 0$.

Furthermore, we note that $\lim_{q\to 0}(qD(q,\cdot))' = \frac{g(q)-qg'(q)}{g^2(q)} = \lim_{q\to 0}\frac{-qg''(q)}{2g(q)g'(q)} = -\infty$. Evaluation of $(qD(q,\cdot))'$ at $q = 1$ yields a finite value. To this end, we have proven that $(qD(q,\cdot))'$ is no greater than 0 with a finite value at $q = 1$ and approaches $-\infty$ at $q = 0$.

Next, we prove that $(qW(q,\cdot))' \geq 0$, i.e., $qW(q,\cdot)$ is increasing with q. From (8), we have that

$$qW(q,\cdot) = \frac{qH}{(1-q)\gamma(1-\gamma)^{\bar{n}-1}}.$$

The first derivative $(qW(q,\cdot))' = \frac{H}{(1-q)^2\gamma(1-\gamma)^{\bar{n}-1}} > 0$ for $q \in [0,1]$ and it approaches $+\infty$ at $q = 1$.

Now, we prove that $F'(q)$ should have at least one point q^* such that $F'(q^*) = 0$. We have so far proven the following: 1) $(qD(q,\cdot))' \leq 0$ for $q \in [0,1]$ approaches $-\infty$ at $q = 0$ and attains a finite value at $q = 1$, and 2) $(qW(q,\cdot))' \geq 0$ takes a finite value at $q = 0$ and approaches $+\infty$ at $q = 1$. Therefore, we have $F'(q) = (q(D(q,\cdot) + W(q,\cdot)))'$ equal to $-\infty$ at $q = 0$ and equal to $+\infty$ at $q = 1$. As $F'(q)$ is a continuous function, there must exist at least one point q^* such that $F'(q^*) = 0$ which is local minimum of $F(q)$. □

ACKNOWLEDGMENTS

This work was supported in part by the following grants: ARO PECASE, W911NF-05-1-0491; ARL CTA, DAAD19-01-2-001; and ARO MURI, W911NF-07-1-0287. This document was prepared through collaborative participation in the Communications and Networks Consortium sponsored by the US Army Research Laboratory under the Collaborative Technology Alliance Program, DAAD19-01-2-0011. I. Koutsopoulos acknowledges the support of the European Commission through STREP project OPNEX (FP7-ICT-224218) and NoE NEWCOM++ (FP7-ICT-216715). The US Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the US Army Research Laboratory, the US Government, or The Boeing Company. Part of the material in this paper was presented in [1] at INFOCOM 2007, Anchorage, Alaska.

REFERENCES

[1] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal Jamming Attacks and Defense Policies in Wireless Sensor Networks," *Proc. IEEE INFOCOM*, 2007.

[2] M. Raya, J.-P. Hubaux, and I. Aad, "DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots," *Proc. Second Int'l Conf. Mobile Systems, Applications and Services (MobiSys '04)*, 2004.

[3] P. Kyasanur and N. Vaidya, "Selfish MAC Layer Misbehavior in Wireless Networks," *IEEE Trans. Mobile Computing*, vol. 4, no. 5, pp. 502-516, Sept./Oct. 2005.

[4] S. Radosavac, I. Koutsopoulos, and J.S. Baras, "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks," *Proc. ACM Workshop Wireless Security (WiSe)*, 2005.

[5] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," *Computer*, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[6] R. Negi and A. Perrig, "Jamming Analysis of MAC Protocols," Carnegie Mellon Technical Memo, 2003.

[7] R. Mallik, R. Scholtz, and G. Papavassilopoulos, "Analysis of an On-Off Jamming Situation as a Dynamic Game," *IEEE Trans. Comm.*, vol. 48, no. 8, pp. 1360-1373, Aug. 2000.

[8] J. Jung, V. Paxson, A.W. Berger, and H. Balakrishnan, "Fast Portscan Detection Using Sequential Hypothesis Testing," *Proc. IEEE Symp. Security and Privacy*, 2004.

[9] V. Coskun, E. Cayirci, A. Levi, and S. Sancak, "Quarantine Region Scheme to Mitigate Spam Attacks in Wireless Sensor Networks," *IEEE Trans. Mobile Computing*, vol. 5, no. 8, pp. 1074-1086, Aug. 2006.
[10] 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," *ACM Trans. Sensor Networks*, vol. 5, no. 1, pp. 1-38, Feb. 2009.
[11] G. Lin and G. Noubir, "On Link-Layer Denial of Service in Data Wireless LANs," *Wiley J. Wireless Comm. and Mobile Computing*, vol. 5, no. 3, pp. 273-284, May 2005.
[12] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti-Jamming Techniques in Sensor Networks," *IEEE Trans. Mobile Computing*, vol. 6, no. 1, pp. 1-15, Jan. 2007.
[13] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," *Proc. ACM MobiHoc*, 2005.
[14] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel Surfing: Defending Wireless Sensor Networks from Interference," *Proc. IEEE Int'l Conf. Information Processing in Sensor Networks (IPSN)*, 2007.
[15] J.M. McCune, E. Shi, A. Perrig, and M.K. Reiter, "Detection of Denial-of-Message Attacks on Sensor Network Broadcasts," *Proc. IEEE Symp. Security and Privacy*, 2005.
[16] D.P. Bertsekas and R.G. Gallager, *Data Networks*, second ed. Prentice Hall, 1992.
[17] C.D.M. Cordeiro and D.P. Agrawal, *Ad Hoc and Sensor Networks: Theory and Applications.* World Scientific, 2006.
[18] A. Wald, *Sequential Analysis.* Wiley, 1947.
[19] V.P. Dragalin, A.G. Tartakovsky, and V.V. Veeravalli, "Multihypothesis Sequential Probability Ratio Tests—Part I: Asymptotic Optimality," *IEEE Trans. Information Theory*, vol. 45, no. 7, pp. 2448-2461, Nov. 1999.
[20] C.W. Helstrom, *Elements of Signal Detection and Estimation.* Prentice-Hall, 1995.
[21] A.M. Mathai, *An Introduction to Geometrical Probability.* Gordan and Breach Science Publishers, 1999.

Mingyan Li received the doctor of philosophy degree from the Network Security Laboratory in the Department of Electrical Engineering (EE) at the University of Washington (UW) in 2006. She is an advanced computing researcher at Boeing Research and Technology (BR&T) and an affiliated assistant professor in the EE Department at the UW. Her research interests are in the area of network security and user privacy, with applications to ubiquitous computing, sensor networks, RFID applications, software distribution systems, medical security systems, vehicular ad hoc networks (VANET), distributed storage, and secure multicast. She has led Boeing-Siemens collaborative projects on wireless and RFID security. She was a recipient of the BR&T silver teamwork award in 2008, the IEEE PIMRC best student paper award in 2007, the UW EE Departmental Chair's Award in 2006, and the outstanding Society of Women Engineer (SWE) Graduate award in 2003. She is a member of the IEEE.

Iordanis Koutsopoulos received the diploma in electrical and computer engineering from the National Technical University of Athens, Greece, in 1997, and the MSc and PhD degrees in electrical and computer engineering from the University of Maryland, College Park (UMCP), in 1999 and 2002, respectively. He is an assistant professor in the Department of Computer and Communications Engineering, University of Thessaly, Greece, since 2009, and was a lecturer in the same department from 2005 to 2009. He is also affiliated with the Institute for Telematics and Informatics of the Center for Research and Technology Hellas (CERTH). From 1997 to 2002, he was a Fulbright fellow and a research assistant with the Institute for Systems Research (ISR) of UMCP. He held internship positions with Hughes Network Systems, Germantown, Maryland, Hughes Research Laboratories LLC, Malibu, California, and Aperto Networks, Inc., Milpitas, California, in 1998, 1999, and 2000, respectively. In the summer of 2005, he was a visiting scholar with the University of Washington, Seattle. From 2005-2007, he was awarded a Marie Curie International Reintegration Grant (IRG). His research interests are in the area of network control and optimization, with emphasis on wireless network cross-layer design and performance analysis, peer-to-peer, and sensor networks. He is a member of the IEEE.

Radha Poovendran received the PhD degree in electrical engineering from the University of Maryland, College Park, in 1999. He is a professor and a founding director of the Network Security Lab (NSL) in the Electrical Engineering Department of the University of Washington. His research interests are in the areas of applied cryptography for multiuser environment, wireless networking, and applications of information theory to security. He is a recipient of the NSA Rising Star Award, Faculty Early Career Awards including the US National Science Foundation (NSF) CAREER (2001), ARO YIP (2002), ONR YIP (2004), and PECASE (2005) for his research contributions to multiuser security, the Graduate Mentor Recognition Award from the University of California, San Diego in 2006, and was invited to the Kavli Frontiers of Science Symposium organized by the National Academy of Sciences in 2007. He has recently organized and cochaired the 2008 National Workshop on High Confidence Transportation Cyber-Physical Systems (CPS) and chaired the 2009 Army Research Office Workshop on CPS security at the University of Washington. He is a co-editor of the Springer Verlag book *Secure Localization and Time Synchronization in Wireless Ad Hoc and Sensor Networks* and a guest editor of an upcoming special issue on cyber-physical systems in the *Proceedings of the IEEE*. He is a senior member of the IEEE.