Available online at www.elixirpublishers.com (Elixir International Journal)

Adoc Network

Elixir Adoc Network 43 (2012) 6746-6750

ISSN: 2229-712X

A novel approach for jamming detection and avoidance in wireless sensor networks

Ajesh.F[1] and Aneesh S Perumpurath[2]
Musaliar College of Engineering and Technology, Pathanamthitta.

ARTICLE INFO

Article history:
Received: 5 January 2012;
Received in revised form:
25 January 2012;
Accepted: 7 February 2012;

Keywords
Jamming,
Security,
Optimization,
Wireless sensor network.

ABSTRACT
Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission. A jamming attacker launches jamming attacks easily by transmitting high-power signals and all legitimate sensor nodes interfered by jamming signals suffer corrupted packet transmissions. In this paper, model the interaction between the sensor network model and the attacker model as a non-cooperative non-zero-sum static game. In such a game, the sensor network has a set of strategies of controlling its probability of accessing the wireless channel and the attacker manipulates its jamming by controlling its jamming probability after sensing a transmission activity. The jammer action ceases when it is found by a monitoring node in the network, and an intimation of jamming message is transferred out of the jamming region. In this paper implements, algorithm for computing jamming attack and network defense. A critical issue is that there may exist a number of possible strategy profiles of Nash equilibria and its solve by applying Pareto-dominance and risk dominance.Results provide valuable insights about the structure of the jamming attack problem and associated defense policies and the adoption of sophisticated strategies on achieving desirable performance.

Introduction

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 [2] 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 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 [1].

In this paper, interaction between the sensor network model and the attacker model it as a non-cooperative non-zero-sum static game. The attacker employs a smart jamming attack technique that it transmits jamming signals after it senses a transmission activity. It manipulates its jamming by controlling its jamming probability. The sensor network employs monitors for finding jamming attacks by using an optimal sequential probability hypothesis test. It has a set of strategies of controlling its probability of accessing the wireless channel [9].

In this paper implements an efficient algorithm for computing jamming attack and network defense policies [1], respectively. An issue is that there may exist a number of possible strategy profiles of Nash equilibria and its solve by applying Pareto-dominance and risk dominance. Our numerical results demonstrate that the strategies chosen by Pareto-dominance and risk dominance achieve the expected performance. Results provide valuable insights about the structure of the jamming attack problem and associated defense policies and the adoption of sophisticated strategies on achieving desirable performance.

In the paper we have made the following contributions.

1. To study the attack-defense model interaction between the sensor network model and jamming attacks.
2. Derive the interaction between the sensor network and the jammer as a non-cooperative game and design an efficient algorithm for computing the network defense and jamming attack.
3. To solve with the issue of multiple Nash equilibria by applying Pareto-dominance and risk-dominance techniques.
4. The formulation the attack detection and the transfer of the attack notification message out of the jammed area.

The remainder of the paper is organized as follows. The next section presents model describing the network model, the attacker model and the defense model, the non-operative non-zero-sum game played by the sensor network and the attacker is explained and the problem for attack and defense is defined [4]., we prose algorithm and techniques for computing and describes in Section 3 and the experimental results shown in Section 4.

Model

Network Model

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[2]. Sensor nodes are uniformly distributed in an area, with spatial density ρ nodes per unit area. The Summary of Notations is shown in table 1.

A transmission on edge (i,j) is successful if and only if no node in $Nj \in \{j\}\backslash\{i\}$ transmits during that transmission. In this work, we consider the class of slotted Aloha type random access protocols that are characterized n by a common channel access probability γ for all network nodes in each slot. For analysis simplification, we let the accessing probability be selected from a set of all possible probabilities $\gamma = \{\gamma_0, \gamma_1, ...\gamma_{n-1}\}, 0 < \gamma_i \leq 1, 0 \leq i \leq n-1$

Probability of collision at node j in a slot i

Tele:
E-mail addresses: ajeshf@gmail.com

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

Attacker Model

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 [3]. The jammer transmits a small packet which collides with legitimate transmitted packets at their intended receivers. 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.

If jamming occurs without prior channel sensing, the probability of collision is

$$\theta_1 = 1-(1-\gamma)^n - (1-q)n\gamma(1-\gamma)^{n-1} \quad (2)$$

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. For analysis simplification [8], we let the jamming probability be selected from a set of all possible probabilities, $Q = \{q_0, q_1, ...q_{n-1}\}, 0 < q_i \le 1, 0 \le i \le n-1$

Defense Model

The sensor network uses a mechanism for detecting jamming attacks. A set of nodes are employed as monitors that try to detect jamming. For each monitor node, it watches its collisions and detects a jamming attack by checking if the collisions happened show abnormal. We focus on the situation of one monitor. The monitor observes the probability of collision it has experienced. When the monitor is jammed by an attacker, the probability of collision it experiences would be different from what it experiences under normal situations. An increased probability of collision usually results from a jamming attack. The monitor takes observations for each time slot (collided or not collided) and decides whether there has appeared jamming. The monitor prefers to use a short time window of observation so that a jamming attack can be detected as quickly as possible. Meanwhile, it takes long enough time so as to minimize the false alarm rate.

The specific algorithm for jamming detection is Wald's Sequential Probability Ratio Test (SPRT) [7]. The algorithm minimizes the average number of required observations while the false alarm and detection missing rate do not exceed the given thresholds above.

Let H_0 and H_1 denote the two hypotheses, meaning absence and presence of jamming, respectively. According to the algorithm, the mean number of time slots for jamming detection is given by

$$E[N \mid H_1] = \frac{C}{\theta_1 \log \frac{\theta_1}{\theta_0} + (1-\theta_1)\log \frac{1-\theta_1}{1-\theta_0}} \quad (3)$$

In θ_0 and θ_1, is the neighborhood size of the monitor. In the following, let D (q, γ) denote E[N|H_1]which is the expected delay for jamming detection.

Notification Message

The transfer of the notification message out of the jammed area is performed with multi hop 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.

The probability of successful channel access for a node i along the route of the notification message in the presence of jamming is

$$P_a = (1-q)\gamma(1-\gamma)^{n-1} \quad (4)$$

The expected number of transmission attempts before successful transmission, and calculated delay is shown in Fig1 which also denotes expected delay for node i before successful transmission is

$$t_a = \sum_{j-1}^{\infty} j(1-a)^{j-1} P_a = 1/P_a \quad (5)$$

The message is sent hop by hop. The mean number of hops that the message needs to be forwarded is H=R_m /2R Therefore, the average time needed for notification broadcast is

$$W(q,\gamma) = \frac{H}{P_a} = \frac{R_m}{2R(1-q)\gamma(1-\gamma)^{n-1}} \quad (6)$$

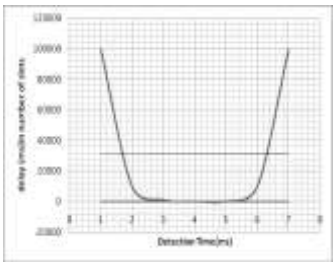

Fig 1. The detection delay D (.), notification Delay W (.), and total delay D (.) + W (.) As Functions of jamming probability q. Total time until the activity of the jammer is assumed to Stop is D (q, γ) + $W(q,\gamma)$ (ms), and goes to infinity When:

- q = 0, which essentially means no jamming and hence infinite detection time [10].
- q = 1, namely in the scenario of continual jamming, where the notification time is infinite
- γ = 0, namely in absence of network transmissions, where no collision can be observed and detection time goes to infinity.
- γ =1 where all network transmissions fail due to excessive contention regardless of existence of an adversary.

Materials and method

non-zero game formulation

The performance gain for the attack is dependent on the action that taken by the senor network and the performance gain of the sensor network is related to the jamming action of the attacker. This interaction between the senor network and the attacker is a non-cooperative game.

Attacker Payoff

The payoff function for the jammer (denoted by U_{mC}) is defined by the number of incurred corrupted links. Note this number does not include those caused by legitimate contention. Let the instantaneous payoff U_{mI} (q, γ)

In order to get the value of U_{mI} (q, γ) we first derive the mean number of successful transmissions in a time slot. Let X and Y denote the number of attempted transmissions and the number of successful transmission links, respectively. It is not difficult to find success the probability of an attempted transmission, as follows

P_s = Pr {Only one transmitter in A}

× Pr {At least one potential receiver in A}

$$= \rho\gamma A(e^{-\rho\gamma A} - e^{-\rho A}) \quad (7)$$

This payoff depends on jamming probability q and access probability γ and denote as U_{mI} (q, γ).A transmission is successful if there is no other transmitter in a receiver's transmission range area and there is at least one receiver in the transmitter's transmission range area A= πR^2. By conditioning on X, we can derive the mean number of successful transmission links,

$$E[Y] = E_x[E_y[Y \mid X = x]] \quad (8)$$

$$E[Y] = A_m(A(\rho\gamma)^2(e^{-\rho\lambda A} - e^{-\rho A}) \quad (9)$$

Where A_m is the area covered by the transmission range of the jammer. The instantaneous payoff for the attacker that jams with probability q after sensing a transmission is

$$U_{mi}(q,\gamma) = q \times E[Y]$$

$$U_{mi}(q,\gamma) = qA_m(A(\rho\gamma)^2(e^{-\rho\lambda A} - e^{-\rho A})) \quad (10)$$

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

$$U_{mc} = U_{mi} \times (D(q,\gamma) + W(q,\gamma))$$

$$U_{mc} = qA_m(A(\rho\gamma)^2(e^{-\rho\lambda A} - e^{-\rho A})) \times \left(\frac{C}{\theta_1 \log\frac{\theta_1}{\theta_0} + (1-\theta_1)\log\frac{1-\theta_1}{1-\theta_0}} + \frac{R_m}{2R(1-q)\gamma(1-\gamma)^{n-1}}\right) \quad (11)$$

Network Payoff

Let U_I be the payoff of the sensor network in a time slot. It is the number of successful transmission links in the presence

$$U_C(q,\gamma) = (1-q)A_m(A(\rho\gamma)^2(e^{-\rho\lambda A} - e^{-\rho A}) \times \left(\frac{C}{\theta_1 \log\frac{\theta_1}{\theta_0} + (1-\theta_1)\log\frac{1-\theta_1}{1-\theta_0}} + \frac{R_m}{2R(1-q)\gamma(1-\gamma)^{n-1}}\right) \quad (12)$$

Optimal method for jamming

Defense

In this section we derive the optimal jamming strategy for the attacker and the optimal defense strategy for the sensor network.

Computing Optimal Strategies

According to game theory, a strategy is dominant if it provides the player with a larger payoff than any other regardless what strategies the other players take. However, after analysis, we find that there do not exist dominant strategies for both sides, as shown in the following theorem.

THEOREM 1: *In the jamming-defense game, there are no dominant strategies for either the attacker or the network.*

Proof. We first prove that there is no dominant strategy for network defense. It can be proved in a similar way that there is no dominant strategy for the attacker. We prove it by contradiction. Suppose there is a dominant strategy for network defense and denote the defense strategy with γ^*. Then it follows that we have the proposition γ^* must be unique. We select two different jamming probabilities $_1$ and q_2. When the jamming probability is given, the payoff of the network U_c(q, γ) then become a function of only one variable, i.e., accessing probability γ. It is not difficult to find γ_1^* and γ_2^* that maximizes the network payoff when the jamming probability takes q_1 and q_2, respectively. By supposing a configuration instance of the network and the attacker, we compute γ_1^* and γ_2^* and find that they are not the same. This is contradictory to the previous proposition that γ_1^* must be unique. We design the optimal strategy profile algorithm for computing the strategy profiles of Nash equilibrium. The central idea of this algorithm is as follows. All possible strategy profiles define a payoff matrix. For each player, it finds the maximum payoff for each of this strategy and marks the strategy profile. If a strategy profile has been marked twice, then it corresponds to a Nash equilibrium. The detail pseudo code of the optimal strategy profile algorithm is shown in the algorithm figure.

Optimal Strategy Profile Algorithm

Input:

$Q = \{q_0, q_1, ..., q_{n-1}\}$: Jammer's strategy set

$M_{jam} = (U_{mC}(q_i, \gamma_j))_{n\times n}$: Jammer payoff matrix

$\gamma = \{\gamma_0, \gamma_1, ..., \gamma_{n-1}\}$: Network's strategy set

$M_{network} = (U_C(q_i, \gamma_j))_{n\times n}$: Network payoff matrix

Output:

(q_*, γ_*): Nash equilibria

Main procedure:

for each $q_i \in Q$

for each $\gamma_j \in \gamma$

$U_{mC}(q_i, \gamma_j) = \max(M_{jam}(q_i, \gamma_j))$;

$S_1 \leftarrow (q_i, \gamma_j)$

end for

end for

For each $\gamma_j \in \gamma$

for each $q_i \in Q$

$U_C(q_i, \gamma_j) = \max(M_{net}(q_i, \gamma_j))$;

$S_2 \leftarrow (q_i, \gamma_j)$;

end for

if $(q_*, \gamma_*) \in S_1$ && $(q_*, \gamma_*) \in S_2$

return (q_*, γ_*);

end if

Nash-Pareto dominant Algorithm

Input:

$\{(q_i, \gamma_i) \mid 0 \le i \le k-1\}$: k Nash equilibriums

$M_{jam} = (U_{mC}(q_i, \gamma_j))_{n\times n}$: Jammer payoff matrix

$M_{net} = (U_C(q_i, \gamma_j))_{n\times n}$: Network payoff matrix

Output:

(q_*, γ_*) : Pareto-dominated equilibrium

Main procedure:

$(q_*, \gamma_*) = (q_0, \gamma_0)$;

for i=1 to k-1

if $M_{jam}(q_i,\gamma_i) > M_{jam}(q_*,\gamma_*)$ && $M_{net}(q_i,\gamma_i) > M_{net}(q_*,\gamma_*)$

$(q_*,\gamma_*) \leftarrow (q_i,\gamma_i)$;

end if

end for

return (q_*,γ_*);

Nash-Risk dominant Algorithm

Input:

$\{(q_i,\gamma_i) \mid 0 \le i \le k-1\}$: k Nash equilibriums

$M_{jam} = (U_{mC}(q_i,\gamma_j))_{n\times n}$: Jammer payoff matrix

$M_{net} = (U_C(q_i,\gamma_j))_{n\times n}$: Network payoff matrix

Output:

(q_*,γ_*) : Risk-dominated equilibrium

main procedure:

for $i = 0$ to $k-1$

$$t_i = \left(\frac{1}{n} \times \sum_{j=1}^{n} M_{jam}(q_i,\gamma_j)\right);$$

end for

$t_m = \max(t_0, t_1, ..., t_{k-1})$;

$q_* \leftarrow q_m$;

for $j = 0$ to $k-1$

$$S_j = \left(\frac{1}{n} \times \sum_{i=1}^{n} M_{jam}(q_i,\gamma_j)\right);$$

end for

$S_l = \max(S_0, S_1, ..., S_{k-1})$;

$\gamma_* \leftarrow \gamma_l$;

return (q_*,γ_*)

This algorithm contains two double-loops. The time complexity of each double-loop is $O(n^2)$. As the time complexity of the other part of the algorithm is $O(n\log_2 n)$ the total time complexity of the algorithm is $O(n^2)$.We have to store the elements of S_1 and S_2. The number of the elements in S_1 or S_2 is less than n. Thus, the total space complexity of the algorithm is O(n).

Dealing with Multiple Nash Equilibria

The optimal strategy profile algorithm outputs a number of Nash equilibria. The existence of multiple equilibria creates difficulty in understanding the jamming-defense game in wireless sensor network [6]. It is apparent that for each computed equilibrium, when the other player fixes its strategy, the player's best strategy is to follow the one defined by the strategy profile of the Nash equilibrium. In the following, we present two possible equilibria that may be applied in the jamming-defense game of wireless sensor networks [5].

Pareto-Dominated Equilibrium

In multiple Nash equilibria earns larger payoffs for all players simultaneously, than any other equilibria. It is highly probable that all players will have unanimous tendency to this equilibrium. That is all players in this game will choose the strategy defined by this equilibrium and also predict that other players will do the same. The approach to selecting Nash equilibrium is based on the Pareto efficiency. The equilibrium selected by Pareto efficiency is called Pareto-dominated equilibrium. We develop the Nash-Pareto dominant Algorithm for computing the Pareto-dominated equilibrium and the corresponding optimal strategy profile for the attacker and the network. Note that it is unnecessary that a game always has a Pareto-dominated equilibrium.

Risk-Dominated Equilibrium

In practice, the strategies defined by the Pareto-dominated equilibrium are not the best choice, because there is uncertain with how the opponent player chooses its strategy. The possible reasons are incompleteness of information or the limited rational degree of the opponent player. Nash equilibrium is risk-dominated if it has the largest basin of attraction, which means that the more uncertainty players have about the actions of the other player(s), the more likely they will choose the strategy corresponding to it. A risk-dominated equilibrium defines the optimal strategy for a player in the sense that the strategy results in the best expected payoff on the condition that the opponent player may choose its strategy with certain randomness. We develop the Nash-risk dominant Algorithm for computing the optimal risk-dominated strategies for jamming attack and network defense.

Experimental Results

The following simulation results show that the proposed system is more efficient than current system.

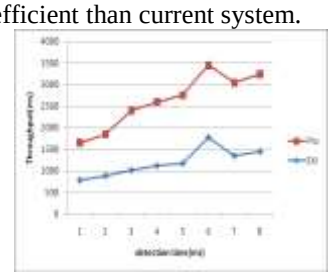

Fig 2: Throuput Graph

Fig 2. Shows throughput graph for without applying game formulation (exi) and with game formulation th (pros) w.r.t throughput (maximum number of successful transmission) and jamming detection time(ms).

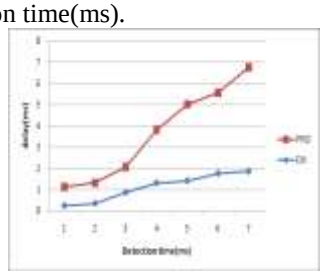

Fig 3:Delay Graph

Fig 3. Shows Delay graph without applying game formulation (exi) and with game formulation (pros) w.r.t detection time (time taken to detect the number of collisions) and delay (delay time for reaching the successful transmission of packets)(ms).

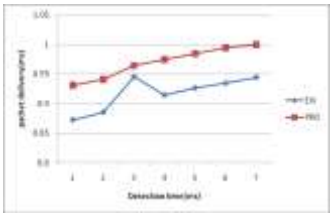

Fig4: Packet Delivery Ratio (PDR

Fig 4. Shows PDR graph applying game formulation (exi) and with game fomulation (Cons) w.r.t packet delivery (successful transmission of packets) and time (ms)

Conclusions

A sensor network under jamming attacks suffer reduced the efficiency of data communication. We studied the optimal strategies for attacking and defense in the framework of non-cooperative non-zero-sum game. The attacker strategically manipulates its jamming probability and the network controls its access probability. For this game, we first prove that there does not exist a dominant strategy for either side of the attacker or the sensor network. We then turn to the find the optimal strategies in the sense of Nash equilibrium. To solve the issue of multiple equilibriums, Pareto-dominance and risk-dominance to find optimal strategies that are useful in real-world situations. Results also demonstrate that the resultant Pareto-dominated strategies provide better payoffs that the strategies defined by other equilibria, and the risk-dominated strategies have better ability of offsetting risk

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. More enhanced versions of attacks can be considered, such as the one with dynamic control of jamming. Mobility is a dimension that gives an interesting twist in the problem and has a direct impact on network performance. Finally, the issue of multiple, potentially co-operating attackers gives a whole new flavor to these problems and is worth further attention.

References

[1] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal Jamming Attacks and Defense Policies in Wireless Sensor Networks," IEEE Transactions On Mobile Computing, Vol. 9, NO. 8. pp 1119-1133,August 2010

[2] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati(2009 "A Survey on Jamming Attacks an Countermeasures in WSNs 'IEEE communications surveys & tutorials, vol. 11, no. 4. Fourth quarter 2009

[3] 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

[4] 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 August 2007

[5] Monti, G.; Moro, G."Multidimensional Range Query and Load Balancing in Wireless Ad Hoc and Sensor Networks" Peer-to-Peer Computing , 2008. P2P '08. Eighth International Conference on IEEE,Page(s): 205 - 214,2008

[6] Frikha, L. Trabelsi, Z. Tabbane, S. Ecole Super. des Commun. de Tunis, Ariana, Tunisia"Simulation, optimisation and integration of Covert Channels, Intrusion Detection and packet filtering systems" Information Infrastructure Symposium, 2009. GIIS '09. Global, pages 1-4 October 2009.

[7] Luo Cuilan"Research on the Access Control Protocol of WiMAX "Electronic Commerce and Security, 2009. ISECS '09. Second International Symposium on Nanchang Page(s): 301 - 304,2009

[8] Bayraktaroglu, E. King, C. Liu, X. Noubir, G. Rajaraman, R. Thapa, B."Jamming Analysis of MAC Protocols" INFOCOM 2008. The 27th Conference on Computer Communications. IEEE Page(s): 1265 - 1273,2008

[9] Peng Luo; DeVol, T.A.; Sharp, J.L"Sequential Probability Ratio Test Using Scaled Time-Intervals for Environmental Radiation Monitoring"Nuclear Science, IEEE Transactions on Volume: 57 , Issue: 3 , Part: 3 Page(s): 1556 - 1562 ,2010.

Guerriero, Willett, Glaz, J"Distributed Target Detection in Sensor Networks Using Scan Statistics"Signal Processing, IEEE Transactions on Volume: 57 , Issue: 7

Table 1
A Summary of Notations

Notation	Description
γ	Channel access probability of network node.
q	Probability of jamming in a time slot.
n_i	Number of neighboring nodes of node i.
ρ	Network density
i,j	Indices of network node
E[x]	Expectation of random variable
U_I, U_{mI}	Instantaneous payoff the network
U_c, U_{mC}	Cumulative payoff of the network
U_w, U_{mW}	Weighted cumulative payoff the network
U^0, U_m^0	Payoff threshold of network and attacker respectively