Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach

Afrand Agah[1] and Sajal K. Das[2]
(Corresponding author: Afrand Agah)

Computer Science Department, West Chester University of Pennsylvania[1]
West Chester, PA 19383, USA. (Email: aagah@wcupa.edu)
Center for Research in Wireless Mobility and Networking (CReWMaN)[2]
Department of Computer Science and Engineering, University of Texas at Arlington
Arlington, TX 76019-0015, USA. (Email: das@cse.uta.edu)

(Received Jan. 27, 2006; revised and accepted May 7, 2006)

Abstract

In this paper we formulate the prevention of Denial of Service (DoS) attacks in wireless sensor networks as a repeated game between an intrusion detector and nodes of a sensor network, where some of these nodes act maliciously. We propose a protocol based on game theory which achieves the design objectives of truthfulness by recognizing the presence of nodes that agree to forward packets but fail to do so. This approach categorizes different nodes based upon their dynamically measured behavior. Through simulation we evaluate proposed protocol using packet throughput and the accuracy of misbehaving node detection.

Keywords: Game theory, intrusion detection, security, sensor networks

1 Introduction

Wireless sensor networks can be considered as a special type of ad hoc wireless networks, and there are already some proposals addressing security in general ad hoc networks, but sensor networks have some additional concerns that limit the applicability of those traditional security measures. Sensor networks are very limited in local memory and calculation capacity [4], and so security mechanism for sensor networks can not require each sensor node to store long-sized key to run very complex cryptology protocols. They have low power consumption and so sensor network protocols must focus on power conservation. Usually sensor networks consist of large number of communication nodes, do not have global identification number, and could face easy node failure [4].

In DoS attacks, the attacker's objective is to make target destinations inaccessible by legitimate users [17]. A sensor network without sufficient protection from DoS attacks may not be deployable in many areas. Nodes of a sensor network can not be trusted for the correct execution of critical network functions. Nodes misbehavior may range from simple selfishness or lack of collaboration due to the need for power saving, to active attacks aiming at DoS and subversion of traffic. There are two types of DoS attacks:

Table 1: DoS attacks in sensor networks [17]

DoS attacks	Defense strategy
Radio interference	Use spread-spectrum
Physical tampering	make nodes tamper-resistant
Denying channel	Use error correction code
Black holes	Multiple routing paths
Misdirection	Source authorization
Flooding	Limit the connections

- Passive attacks: selfish nodes use the network but do not cooperate, saving battery life for their own communications; they do not intend to directly damage other nodes.
- Active attacks: malicious nodes damage other nodes by causing network outage by partitioning, while saving battery life is not a priority.

DoS attacks can happen in multiple sensor network protocol layers. Table 1 depicts the typical DoS attacks and the corresponding defense strategies [17].

There is very little work done on the prevention of DoS attacks. Attempts to add DoS resistance to existing protocols often focus on cryptographic authentication mechanism. Aside from the limited resources that make digital signature schemes impractical, authentication in sensor networks poses serious complications. It is difficult to establish trust and identity in large-scale sensor network deployments. Adding security afterward often fails in typical sensor networks. Thus design-time consideration of security offers the most effective defense against DoS attacks.

This paper formulates the prevention of passive denial of service attack at routing layer in wireless sensor networks as a repeated game between an intrusion detector and nodes of a sensor network, where some of these nodes act maliciously. We propose a framework to enforce cooperation among nodes and punishment for non-cooperative behavior. We assume that the rational users optimize their profits over time. Intrusion detector residing at the base station keeps track of other nodes' collaboration by monitoring them. If performances are lower than some trigger thresholds, it means that some nodes act maliciously by deviation. Intrusion detector rates other nodes, which is known as subjective reputation and the positive rating accumulates for each node as it gets rewarded.

This paper is organized as follows. Section 2 reports the related work. Section 3 formulates the game while and discusses the equilibrium and payoff of the game. Section 4 evaluates the performance of proposed protocol, and Section 5 concludes the paper.

2 Related Work

Currently there are four mechanism that could be helpful to overcome DoS attacks in sensor networks.

Watchdog scheme: A necessary operation to overcome DoS attacks is to identify and circumvent the misbehaving nodes [19]. Watchdog scheme attempts to achieve this purpose through using of two concepts: watchdog and path-rater. Every node implements a watchdog that constantly monitors the packet forwarding activities of its neighbors and a path-rater rates the transmission reliability of all alternative routes to a particular destination node. The disadvantages of this scheme are that (1) it is only practical for source routing protocols instead of any general routing protocol and (2) collusion between malicious nodes remains an unsolved problem [17].

Rating scheme: In Rating scheme the neighbors of any single node collaborate in rating the node, according to how well the node execute the functions requested from it [20, 21, 23]. It strikes a resonant chord on the importance of making selfishness pay. Selfishness is different from maliciousness in the sense that selfishness only aims at saving resources for the node itself by refusing to perform any function requested by the others, such as packet forwarding and not at disrupting the flow of information in the network by intension. The disadvantages of this approach are that (1) how an evaluating node is able to evaluate the result of a function executed by the evaluated node, (2) evaluated node may be able to cheat easily and (3) the result of the function may require significant overhead to be communicated to the evaluating node [17].

Virtual currency: This scheme introduces a type of selfish node that are called *nuglets* [9, 11]. To insulate a node's nuglets from illegal manipulation, a tamper-resistant security module storing all the relevant IDs, nuglet counter and cryptographic materials is compulsory. In Packet Purse Model each packet is loaded with nuglets by the source and each forwarding host takes out nuglets for its forwarding services. The disadvantages of this schemes are that : (1) malicious flooding of the network can not be prevented, (2) intermediate nodes are able to take out more nuglets than they are supposed to, and (3) overhead [17].

Route DoS Prevention: It attempts to prevent DoS in the routing layer by cooperation of multiple nodes [8]. It incorporates a mechanism to assure routing security, fairness and robustness targeted to mobile ad hoc networks. The disadvantage of this approach is that misbehaving nodes are not prevented from distributing bogus information on other nodes' behavior and legitimate nodes can be classified as misbehaving nodes [17].

3 Game Formulation of the Proposed Protocol

Here we formulate the prevention of passive denial of service (DoS) attacks in wireless sensor networks as a repeated game between an intrusion detector and nodes of a sensor network, where some of these nodes act maliciously. Intrusion detection systems (IDSs) extend the information security paradigm beyond traditional protective network security. They monitor the events in the system and analyze them for any sign of a security problem [7]. Considering current intrusion detection systems, there is definitely a need for a framework to address attack modeling and response actions.

Game theory addresses problems where multiple players with different objectives compete and interact with each other in the same system; such a mathematical abstraction is useful for generalization of the problem. In order to prevent DoS, we capture the interaction between a normal and a malicious node in forwarding incoming packets, as a non-cooperative N player game [24]. The intrusion detector residing at the base station keeps track of nodes' collaboration by monitoring them. If performances are lower than some trigger thresholds, it means that some nodes act maliciously by deviation. The IDS rates all the nodes, which is known as subjective reputation [20], and the positive rating accumulates for each node as it gets rewarded.

Our proposed framework enforces cooperation among nodes and provides punishment for non-cooperative behavior. We assume that the rational users optimize their profits over time. The key to solve this problem is when nodes of a network use resources, they have to contribute to the network life in order to be entitled to use resources in the future. The intrusion detector keeps track of other nodes behavior, and as nodes contribute to common network operation their reputation increases.

To understand the concept of repeated games, let us start with an example, which is known as the Prisoner's

Dilemma [28], in which two criminals are arrested and charged with a crime. The police do not have enough evidence to convict the suspects, unless at least one confesses. The criminals are in separate cells, thus they are not able to communicate during the process. If neither confesses, they will be convicted of a minor crime and sentenced for one month. The police offers both the criminals a deal. If one confesses and the other does not, the confessor one will be released and the other will be sentenced for 9 months. If both confess, both will be sentenced for six months. This game has a unique Nash equilibrium in which each player chooses to cooperate in a single-shot setting.

However, in a more realistic scenario a particular one shot game can be played more than once, in fact a realistic game could even be a correlated series of one shot games. So what a player does early on can affect what others choose to do later on. In particular, one can strive to explain how cooperative behavior can be established as a result of rational behavior. This does not mean that the game never ends; we will see that this framework is appropriate for modeling a situation when the game eventually ends but players are uncertain about exactly when the last period is.

Now in the prisoner's dilemma, suppose that one of the players adopts the following long-term strategy: (1) choose to cooperate as long as the other player chooses to cooperate, (2) if in any period the other player chooses to defect, then choose to defect in every subsequent period. What should the other player do in response to this strategy? This kind of games is known as repeated games with sequences of history-dependent game strategies.

We model the interaction between nodes (normal or malicious) and IDS in a sensor network as a repeated game. N players play a non-cooperative game at each stage of the game, where players of the game are an IDS residing at the base-station and N sensor nodes. We first define the stage game, then define the uncertainty that players have about the game. Finally, we define what strategies the players can have in the repeated game.

Consider a game G, which will be called the stage game. Let the players/nodes set to be $I = \{1, \cdots, N\}$, and refer to a node's stage game choices as *actions*. So each node has an action space A_i. If it is a malicious node then sometimes its action is dropping of the incoming packets.

Let a_i^t refer to the action of the stage game G which node i executes in period t. The action profile played in period t is just the n-tuple of individuals' stage game actions $a^t = (a_1^t, \cdots, a_n^t)$. We want to be able to condition the nodes' stage game action choices in later periods upon actions taken earlier by other nodes. To do so, we need the concept of *history* which is a description of all the actions taken up through the previous periods. We define the history at time t as $h^t = (a^0, a^1, \cdots, a^{t-1})$. In other words, the history at time t specifies which stage game action profile was played in each previous period. So we write node i's period-t stage game as the function s_i^t, where $a_i^t = s_i^t(h^t)$ is the stage game action it would play in period t if the previous play had followed the history h^t. When the game starts, there is no past play, every node executes its a_i^0 stage game. This zero-th period play generates the history $h^1 = (a^0)$, which will be recorded at the base station, where $a^0 = (a_1^0, \cdots, a_n^0)$. This history is then revealed to the IDS so that it can condition its period-1 play upon the period-0 play. It means that if a node is acting maliciously, by keeping history of the game, the IDS is able to notify neighboring nodes of a malicious one. Each node chooses its $t = 1$ stage game, strategy $s_i^1(h^1)$. Consequently, in the $t = 1$ stage game the stage game strategy profile $a^1 = s^1(h^t) = (s_1^1(h^1), \cdots, s_n^1(h^1))$ is played.

Each node i has a von Neumann-Morgenstern utility function defined over the outcomes of the stage game G, as $u_i : A \rightarrow \Re$, where A is the space of action profiles. Let G be played several times and let us award each node a payoff which is the sum of the payoffs it got in each period from playing G. Then this sequence of stage games is itself a game, called a *repeated game*. Here,

$$u_i^t = \alpha r_i^t - \beta c_i^t,$$

where r_i^t is the gain of node i's reputation, c_i^t is the cost of forwarding a packet for the node, and α and β are weight parameters. We assume that measurement data can be included in a single message that we call a packet. Packets all have the same size. The transmission cost for a single packet is a function of the transmission distance. In particular, we assume $c_i^t = c'.d^\mu$, where c' is a constant that includes antenna characteristics, d is the distance of the transmission and μ is the path loss exponent [27].

By assuming that in each period the same stage game is being played, two statements are implicit:

- For each node, the set of actions available to it in any period in the game G is the same regardless of which period it is and regardless of what actions have taken place in past.
- The payoffs to the nodes from the stage game in any period depend only on the action profile for G which was played in that period, and this stage game payoff to a node for a given action profile for G is independent of which period it is played.

We now define the players' payoff functions for the repeated game. When studying repeated games, we are concerned about a player who receives a payoff in each of many periods. In order to represent the performance over various payoff streams, we want to meaningfully summarize the desirability of such a sequence of payoffs by a single number. A common assumption is that the player wants to maximize a weighted sum of its per-period payoffs, where it weights later periods less than earlier periods. For simplicity this assumption often takes the particular form that the sequence of weights forms a geometric series for some fixed $\delta \in (0, 1)$, each weighting factor is δ times the previous weight. δ is called discount factor.

If in each period t, player i receives the payoff u_i^t, then we could summarize the desirability of the payoff stream $u_i^0, u_i^1, \cdots$ by the number:

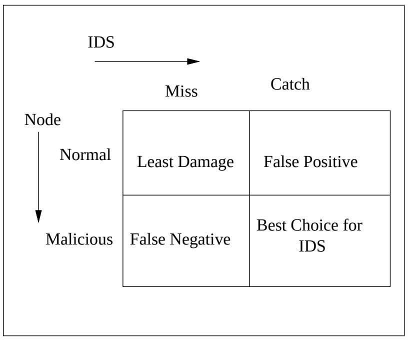
$$(1-\delta)\sum_{t=0}^{\infty}\delta^t u_i^t.$$

Such a preference structure has the desirable property that the sum of the weighted payoffs will be finite. It is often convenient to compute the average discounted value of an infinite payoff stream in terms of a leading finite sum and the sum of a trailing infinite stream. For example, suppose that the payoffs v_i^t a player receives are some constant payoff v_i' for the first t periods, and thereafter it receives a different constant payoff v_i'' in each period. The average discounted value of this payoff stream is:

$$\begin{aligned}(1-\delta)\sum_{\tau=0}^{\infty}\delta^\tau v_i^\tau &= (1-\delta)(\sum_{\tau=0}^{t-1}\delta^\tau v_i^\tau + \sum_{\tau=t}^{\infty}\delta^\tau v_i^\tau)\\ &= (1-\delta)v_i'\sum_{\tau=0}^{t-1}\delta^\tau + (1-\delta)v_i''\frac{\delta^t}{1-\delta}\\ &= (1-\delta)v_i'\frac{1-\delta^t}{1-\delta} + \delta^t v_i''\\ &= (1-\delta^t)v_i' + \delta^t v_i''.\end{aligned}$$

Now we need to specify the strategies for each of these players. Each node makes the decision whether to (1) accept a packet and forward it to improve its own reputation in the network, we call this action "Normal"; or (2) do not cooperate and save battery life and stay selfish, we call this action "Malicious". On the other hand, IDS always wants to catch a malicious node but it depends on how well it can detect an intrusion. Thus the output of IDS actions are either (1) "Catch" a node as malicious, or (2) "Miss" it. As depicted in Figure 1, in cases of false positives and false negatives, payoff of one player is the maximum when it is the minimum for the other player. The most important case (rewarding for IDS) is when a node acts maliciously and IDS is able to catch it. IDS has different utility values based on which case happens and how we would like to give different weights to false positives and false negatives detections. For simplicity, we assume $U(Miss, Normal) = v'$, $U(Catch, Normal) = v''$, $U(Miss, Malicious) = v'''$, and $U(Catch, Malicious) = v''''$.

At each stage game, the IDS concurrently plays an N-person game with N different nodes and several possible strategies can be described for it. We want a strategy that punishes it even for its own past deviations (false negatives). We define the utility of IDS as: $U_{IDS} = \gamma_1 v'''' - \gamma_2 v''' - \gamma_3 v''$, where each γ_i represents the number of occurrences of case i. We consider the following retaliation strategy for IDS: in the initial period every node plays cooperatively and so IDS does not catch anyone; in later periods, IDS does not catch if the node has always played normal. However, if a node acts maliciously, then the IDS catches it for the remainder of the game. More formally, the IDS has the following strategy:



	Miss	Catch
Normal	Least Damage	False Positive
Malicious	False Negative	Best Choice for IDS

Figure 1: Possible cases of interaction between IDS and a node

$$s_{IDS}(h^t) = \begin{cases} Miss & \text{if } t = 0\\ Miss & \text{if } a_i^{t-1} = Normal\\ Catch & \text{otherwise.}\end{cases}$$

Each node in the initial period plays normally and so IDS does not catch anyone, in later periods, a node does not act maliciously if the IDS has missed it. However, if the IDS catches a node, then the node acts maliciously for the remainder of the game. More formally for a node i, we have the following strategy:

$$s_i(h^t) = \begin{cases} Normal & \text{if } t = 0\\ Normal & \text{if } a_i^{t-1} = Miss\\ Malicious & \text{otherwise.}\end{cases}$$

3.1 Equilibrium

First, we show that the above strategies reach to Nash-equilibrium of the repeated game. Both players (sensor nodes and IDS) play cooperatively at $t = 0$. Therefore at $t = 1$, the history is $h^1 = (Miss, Normal)$; so they both play cooperatively again. Therefore at $t = 2$, the history is $h^2 = ((Miss, Normal), (Miss, Normal))$, and so on. The repeated game payoff to each player corresponding to this path is trivial to calculate.

Can IDS gain from deviating from the repeated game strategy given that a sensor node is faithfully following it? Let t be the period in which IDS first deviates. It receives a payoff of v' in the first t periods and in period t, IDS plays "Catch" while sensor node played "Normal", yielding IDS a payoff of v'' in that period. This defection by IDS triggers "Malicious" always response from node. The best response of IDS to this strategy is to "Catch" in every period itself. Thus it receives v'''' in every period $t+1, t+2, \cdots$.

To calculate the average discounted value of this payoff stream, we see that the player receives v_i' for the first t periods, then receives v_i'' only in period t and receives v_i'''' every period thereafter. Therefore, the average discounted value of this stream is:

$$(1-\delta^t)v_i' + \delta^t[(1-\delta)v_i'' + \delta v_i''''].$$

By solving the above inequality for δ and calculating the average discount value of this payoff, while substituting $v'''' > v'' > v' > v'''$, one possible discount factor necessary to sustain cooperation is $\delta \geq 1/2$. In other words, for $\delta \geq 1/2$, the deviation is not profitable. This means that if IDS is sufficiently patient (i.e., if $\delta \geq 1/2$) then the strategy of retaliation is a Nash equilibrium of the infinitely repeated game. We see that with this strategy the optimal response for IDS is to cooperate and not deviate. In other words, in any stage game reached by some player having "defected" in the past, each player chooses the strategy "defect always". Therefore, the repeated game strategy profile is a sequence of Nash-equilibria.

3.2 Payoff and Reputation

The problem of generating reliable information in sensor networks can be reduced to one basic question: How do sensor nodes trust each other? Embedded in every social network is a web of trust with a link representing the amount of trust between two individuals. Here IDS monitors the behavior of other nodes, based on which it builds up their reputation over time. It uses this reputation to evaluate their trustworthiness and in predicting their future behavior. At the time of collaboration, a node only cooperates with those nodes that it trusts. Here the objective is to generate a group of trustworthy sensor nodes.

In order to compute the values of a node's gain, we turn our attention to the work proposed in [20]. In this work the authors proposed the concept of subjective reputation, which reflects the reputation calculated directly from the subject's observation. In order to compute each node's gain at time t, we use the following formula:

$$r_i^t = \sum_{k=1}^{t-1} \rho_i(k),$$

where $\rho_i(k)$ represents the ratings that the IDS has given to node i, and $\rho_i \in [-1, 1]$. If the number of observations collected since time t is not sufficient, the final value of the subjective reputation takes the value 0. IDS increments the ratings of nodes on all actively used paths at periodic intervals. An actively used path is one on which the node has sent a packet within the previous rate increment interval. Recall that reputation is the perception that a person has of another's intentions. When facing uncertainty, individuals tend to trust those who have a reputation for being trustworthy. Since reputation is not a physical quantity and only a belief, it can be used to statistically predict the future behavior of other nodes and can not define deterministically the actual action performed by them. Table 2 depicts the notations that were used throughout this paper.

Table 2: Parameters and Notations

Cost of forwarding packet at node i	c_i
History at node i	h_i
Rating of node i	ρ_i
Reputation at node i	r_i
Utility at node i	u_i
Weight Parameters	α_i, β_i

3.3 Protocol Description

In the proposed protocol, a node sends out a *Route_request* message. All nodes receiving this message compute their utility based on their local reputation and cost, place themselves into the source route and forward it to their neighbors, unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a *Reply* message containing the full source route with the total utility.

After receiving one or several routes, the source selects the best one having the highest utility, which means this route consists of the most reputed possible nodes; stores it and sends messages along that path. Once a route request reaches its destination, the path that this route request has taken is reversed and sent back to the sender. As the destination notifies the base station of the receipt of the packet, the base station gives a higher reputation value to every node on the route, and broadcasts the new reputation values to nodes. As each node is aware of its neighboring node (in its transmission range), it will update the reputation table.

This protocol ensures a view on which nodes will provide likely service due to their commitment, as they want to increase their reputation in the network. IDS also wants to recognize the malicious nodes and isolates them from participating in network functions, but it would prefer not to risk it and have the least amount of false detections, to increase its own utility. The benefit of using a framework based on repeated games is that, the base station has a history of the previous games and when a node is malicious it gets a negative reputation when the total reputation accumulates, a path consisting of less number of malicious nodes is chosen to be the wining path. This results in isolation of malicious nodes.

4 Performance Evaluation

For simplicity we assume the following: (1) sensors are scattered in a field, (2) in the beginning each battery has the same maximum energy, (3) two sensors are able to communicate with each other if they are within transmission range, (4) sensors perform a measurement task and periodically report to a base station, and (5) IDS is present at the base station and constantly monitors all nodes for any sign of maliciousness. The sensor network consists of some malicious nodes which occasionally launch DoS attacks.

4.1 Metrics

Number of hops for received packets: Malicious behavior affects performance in a number of ways. We consider different topologies, and see the effect of starving multi-hop flows and giving all the capacity to one-hop flows.

Throughput: This measure characterizes the total number of forwarded packets over the total number of received packets.

4.2 Implementation

Figure 2 illustrates throughput as a function of the percentage of attackers. The figure indicates that without any attacking node, legitimate nodes spend 60% of their time successfully transmiting, and the remaining 40% having broken routes and trying to re-establish routes due to the quality of routes. We can observe the scalability of the attack for 5 hop nodes: with 10% of attacking nodes, the throughput drops to 52%, whereas with 20% of attacking nodes, the throughput drops to 35%. We belive that the impact of the attacker is even more prominent in large-scale networks in which a longer path length is increasingly likely to include an attacking node.

Figure 3 depicts the average hop length for received packets. Without attack, the mean is 7 indicating that a significant number of packets are received on long routes. Yet, as the number of malicious nodes grows, the average path length for a received packet diminishes: fewer and fewer packets are able to traverse long routes leading to increased capacity for one-hop flows.

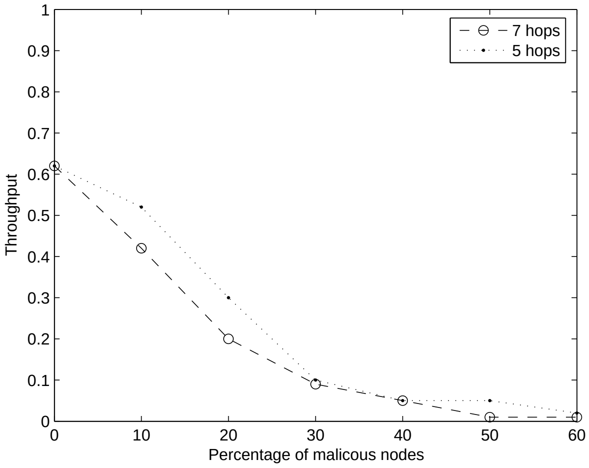


Figure 2: Throughput vs. number of malicious node

Figure 4 indicates the throughput of a node versus time. As the figure depicts, when a node acts maliciously its average throughput drops compared to when it acts normally. The reason behind increase in the throughput over time is that for simulating packet drop, we manually switched off the power switch on the board, and malicious nodes were turned off for shorter duration of time as we proceed with this experiment.

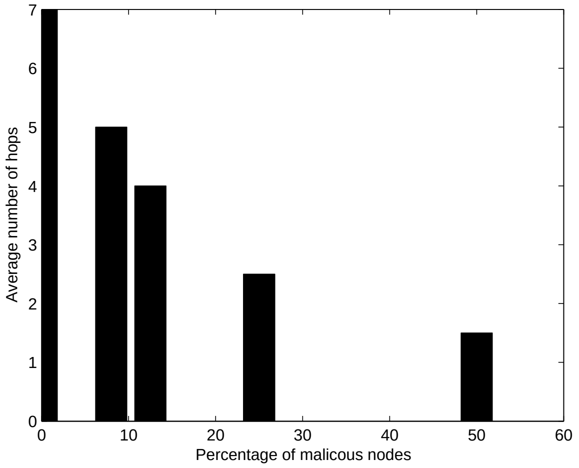


Figure 3: Average number of hops for received packets

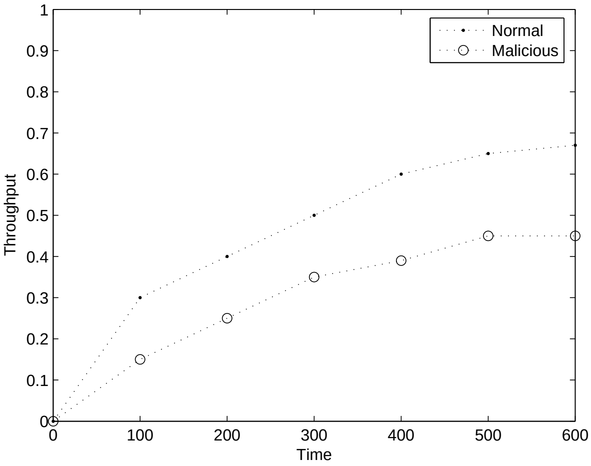


Figure 4: Throughput

In the original case, we consider a $2m \times 2m$ topology with 18 real sensor nodes. Here we also consider a scenario with half the density. Figure 5 shows that for very low densities the average number of hops is relatively low in spite of the large dimensions of the topology. In fact, due to the low density, the network is not fully connected such that long-range flows are unlikely to exist.

Also, we explore the effect of system size (number of nodes) on successfully attack detection in Figure 6. We can observe that with the presence of 60% malicious nodes, the IDS is able to detect correctly 60% of the time, but as we have a large number of nodes present in the area the rate of success degrades.

Finally, Figure 7 depicts the percentage of malicious node detection by IDS. We run the experiments for 100 times for two scenarios, (1) 30% of nodes are malicious and (2) 60% of nodes are malicious. As predicted, when

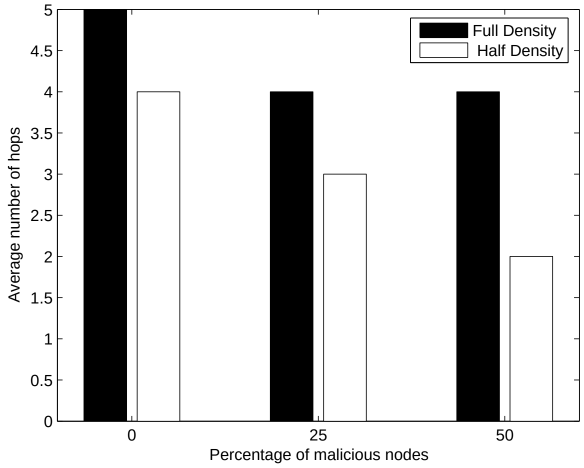


Figure 5: Percentage of malicious nodes vs. number of hops

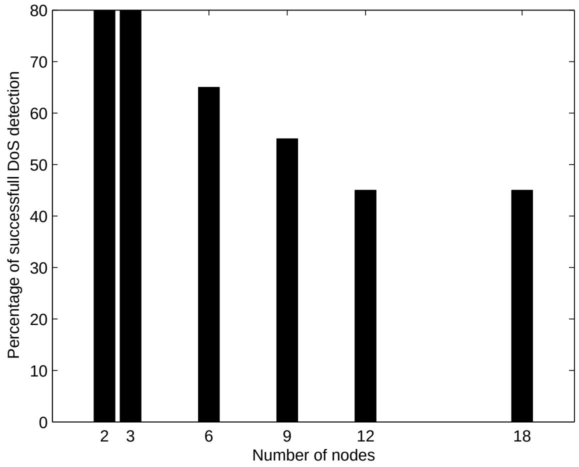


Figure 6: Percentage of malicious nodes vs. number of nodes

we have more malicoius nodes present in the network the success rate of IDS degrades. This is due to the fact that IDS prefers to maximize its own utility and so it has to lower the rate of false positives and flase nagatives detection and eventually it misses more malicious nodes.

5 Conclusion

Infinite repetition can be the key for obtaining behavior in the stage games which could not be equilibrium behavior if the game were played once or a known finite number of times. In the proposed protocol, IDS rates nodes through a monitoring mechanism. The observations collected by the monitoring mechanism are processed to evaluate reputation of each node. We ensure the finiteness of the repeated-game payoffs by introducing *discount* of future payoffs relative to earlier payoffs.

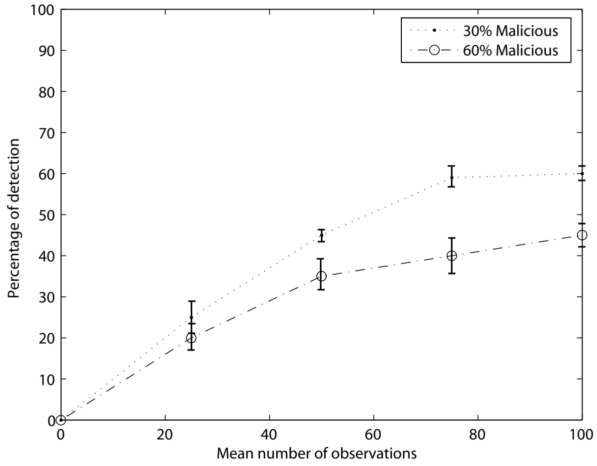


Figure 7: Percentage of correct detection

References

[1] A. Agah, K. Basu, and S. K. Das, "A game theory based approach for security in sensor networks," *International Performance Computing and Communications Conference* (IPCCC), pp:259-263, Phoenix, AZ, Apr. 2004.

[2] A. Agah, S. K. Das and K. Basu, "Preventing DoS attack in sensor and actor networks: A game theoretic approach," *IEEE International Conference on Communications (ICC)*, pp:3218-3222, Seoul, Korea, May 2005.

[3] A. Agah, S. K. Das, and K. Basu, "Enforcing security for prevention of DoS attack in wireless sensor networks using economical modeling, " Proceedings of 2nd IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS), Washington, D.C., Nov. 2005.

[4] I. F. Akyldiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, 2002, pp:393-422.

[5] R. Bace and P. Mell, "Intrusion detection systems," NIST Special Publication on Intrusion Detection systems, http://www.snort.org/docs/nistids.pdf.

[6] G. E. Bolton, A. Ockenfels, "ERC a theory of equity, reciprocity, and competition," *The American Economic Review*, vol. 90, 2000.

[7] S. Buchegger and J. L. Boudec, "Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes-Fairness In Dynamic Ad-hoc NeTworks," *International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2002.

[8] S. Buchegger and J. L. Boudec, "Nodes bearing grudges: toward routing security, fairness and robustness in mobile ad hoc networks," *Proceedings of the 10th Euronicro Workshop on parallel, Distributed and Network-based Processing*, Canary Islands, Spain, January 2002.

[9] L. Blazevic, L. Buttyaan, S. Capkun, S. Giordano, J. P. Hubaux, J. LeBoudec, "Self-organization in mobile ad hoc networks: the approach of terminodes," *IEEE Commun.Mag.*, vol. 39, no. 6, 2001, pp:161-174.

[10] L. Buttyaan, J. P. Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Networks," Mobile Computing and communications Review, vol.6, no.4, 2002.

[11] L. Buttyaan, J. P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks, " Technical Report DSC/2001/001, Department of Communication Systems, Swiss Federal Institute of Technology, 2001.

[12] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," *IEEE Computer*, vol.36, no.10, 2003, pp:103-105.

[13] C. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenge," *Proceedings of the IEEE, special issue on sensor networks and application*, vol. 91, no. 8, 2003, pp:1247-1256.

[14] J. Deng, R. Han, S. Mishra, "INSENS:Intrusion-tolerant routing in wireless sensor networks," *Technical Report TR CU-CS-939-02*, Dept. of Computer Science, University of Colorado, 2002.

[15] S. Doshi, S. Bhandare, T. Brown, "An On-demand minimum energy routing protocol for a wireless ad hoc networks," *ACM Mobile Computing and Communications Review*, vol. 6, no. 3, July 2002.

[16] M. Felegyhazi, L. Buttyan and J. P. Hubaux, "Equilibrium Analysis of Packet Forwarding Strategies in Wireless Ad Hoc Networks- the Static Case," *Proceedings of Personal Wireless Communications (PWC '03)*, Venice, Italy, September 2003.

[17] F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks," *Ad Hoc Networks*, 2003.

[18] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *In First IEEE International Workshop on Sensor Network Protocols and Applications*, SPNA, 2003.

[19] S. Marti, T. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *in Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM)* 2000.

[20] P. Michiardi, R. Molva, "Core: A Collaborative Reputation mechanism to enforce node cooperation in mobile ad hoc networks," *in Communications and Multimedia Security Conference*, 2002.

[21] P. Michiardi, R. Molva, "Prevention of denial of service attack and selfishness in mobile ad hoc networks," Research Report RR-02-063, Institute Eurécom, France, 2002.

[22] P. Michiardi and R.Molva, "Game theoretic analysis of security in mobile ad hoc networks," *Institute Eurecom*, Research Report, France, 2002.

[23] P. Michiardi and R.Molva, "Simulation-based analysis of security exposures in mobile ad hoc networks," in *European Wireless 2002: Next Generation Wireless Networks: Technologies, Protocols, Services and Applications*, Florance, Italy, February 2002.

[24] G. Owen, *Game Theory*, 3rd ed. New York, NY: Academic Press, 2001.

[25] S. Patil, "Performance Measurement of Ad-hoc Sensor Networks under Threats," *Wireless Communications and Networking Conference (WCNC)*, 2004.

[26] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," *ACM International Conference on Mobile Computing and Networking (MOBICOM)*, July 2001, pp: 189-199.

[27] T. S. Rappaport, "Wireless Communications: Principles and Practice," *2nd Edition*, Prentice Hall, 2002.

[28] J. Ratliff, "Repeated Games," http://www.virtualperfection.com/gametheory, download date Feb. 2005.

[29] E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, A.Chandrakasan, "Physical layer driven protocol and algorithm design for energy efficient wireless sensor networks," *Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM)*, Italy, July 2001, pp:272-286.

Afrand Agah is an Assistant professor at West Chester University of Pennsylvania. She received her doctorate in Computer Science and Engineering from The University of Texas at Arlington in December 2005. Prior to that she received her Master degrees from Azad University, Tehran, Iran and Kansas State University in Manhattan, Kansas. Her research interests include security in wireless sensor networks and mobile ad hoc networks. She is a member of IEEE and society of Woman Engineers (SWE).

Sajal K. Das is the founding director of the University of Texas at Arlington's Center for Research in Wireless Mobility and Networking (CReWMaN). He received his Ph.D. in computer science from the University of Central Florida in 1988 and his M.S. in computer science form the Washington State University in 1986. He received his B.Tech. in computer science form the University of Calcutta in 1983. During 1988-99, he was a faculty member in the Computer Science Department at the University of North Texas, where he founded the Center for Research in Wireless Computing (CReW) in 1997. Dr. Das was a recipient of the Student Association's Honor Professor Award at UNT in 1991 and 1997 for best teaching and scholarly research, and UNT's Developing Scholars' Award in 1996 for outstanding research. He has visited numerous universities and research organizations worldwide for collaborative research and seminar talks. He is also frequently invited as a speaker at international conferences and symposia. Prof. Das has published over 170 research papers in journals and conference proceedings in the areas of wireless networks and protocols, mobile computing, parallel/distributed processing, performance modeling, applied graph theory and interconnection networks. He has also directed numerous funded projects in these areas. He received the Best Paper Awards in the ACM/IEEE Fifth International Conference on Mobile Computing and Networking (MobiCom'99), the Third ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2000), and ACM/IEEE International Workshop on Parallel and Distributed Simulation (PADS'97). Prof. Das serves on the editorial boards of the Journal of Parallel and Distributed Computing (as the subject area editor of mobile computing), Parallel Processing Letters, and the Journal of Parallel Algorithms and Applications. He has guest-edited special issues for many leading journals. He has served on the program committees of numerous conferences including IEEE IPDPS, ICPP, IEEE INFOCOM, and ACM MobiCom. He was general vice-chair of the IEEE International Conference on High Performance Computing (HiPC2000), program vice chair of HiPC'99, and the founding program chair of WoWMoM'98 and WoWMoM'99. Dr. Das also serves on the ACM SIGMOBILE and IEEE TCPP executive committees. He is a member of the IEEE and ACM.