International Journal of Advanced Technology in Engineering and Science
Vol. No.4, Issue No. 09, September 2016
www.ijates.com
ijates
ISSN 2348 - 7550

A GAME THEORY APPROACH IN PREVENTING FALSE NODES IN WSN

Vinoba.V[1], Hema.P[2]

[1]*Department of Mathematics, K.N. Government Arts College, Tamil Nadu*

[2]*Department of Mathematics, RMKCET, Tamil Nadu*

ABSTRACT

In this paper we formulate the prevention of false nodes 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 , Repeated game theory.

I. INTRODUCTION

1.1 Description Abour Repeated Game Theory

Repeated games are an important tool for understanding concepts of “reputation” and “punishment” in game theory. This section introduces the setting of the repeated game, the strategies available to repeated game players, and the relevant notions of equilibria.

In a repeated game formulation, players participate in repeated interactions within a potentially infinite time horizon. Players must, therefore, consider the effects that their chosen strategy in any round of the game will have on opponents’ strategies in subsequent rounds. Each player tries to maximize her expected payoff over multiple rounds. A wireless sensor network (WSN) is a network of thousands of resource-constrained sensors whose communications with a central station are conveyed by means of wireless signals. A sensor node is generally comprised of four basic elements, including a sensing unit, a processing unit, a transceiver unit, and a power unit. The WSN is frequently deployed for sensing the area of interest where data captured encompass light, pressure, sound, and others. Sensor nodes in WSN mainly use a broadcast communication paradigm where the sensor signals are used in further analyses of the sensed environment. WSN is preferred as the sensor system architecture with regard to its inherent redundancy but is susceptible to disadvantages caused by limited operation life-time. Differ from other wired networks, the use of WSNs are usually restricted by energy stored, computation capability, memory, plethoric information flow, and short communication distance . Since the sensor nodes are often densely deployed in a sensing field, it is difficult and costly to replace faulty sensor nodes manually. Furthermore, sensor nodes may have no global information of the whole network and the topology of a WSN varies frequently . The game types for preventing DoS attacks include non-cooperative game cooperative game and repeated game The jamming and anti-jamming issues are modeled as a zero-sum stochastic game in literature to defend DoS attack. In this game, the actions of the sensor and jammer are dependent on the current system state. A quadratic function is used as the payoff function, thus facilitating the LQG control of the power system. The NE of the game is analyzed, including the existence and the corresponding computation. Numerical simulations are carried out for a seven-dimensional linear system of power grid and demonstrate the increase of reward when proper anti-jamming actions are taken established an attacking-defending gaming model which can detect active DoS attacks effectively, where the strategy space and payoff matrix are given to both the IDS and the maliciousnodes.

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 . 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 . 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 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.

1.2 Prisoner’s Dilemma

To understand the concept of repeated games, let us start with an example, which is known as the Prisoner's Dilemma 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 con- fesses. 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 we'll call the *stage game* or the *constituent game*). As usual we let the player set be I={1,…,n}. In our present repeated-game context it will be clarifying to refer to a player's stage game choices as *actions* rather than strategies. (We'll reserve "strategy" for choices in the repeated game.) So each player has a pure-action space A_i. The space of action profiles is $A = X_{i \in i} A_i$. Each player has a von Neumann-Morgenstern utility function defined over the outcomes of G, $u_i : A \rightarrow R$. Here we use "U" for the payoff to the entire repeated game.)

Let G be played several times (perhaps an infinite number of times) and award each player a payoff which is the sum of the payoffs she got in each period from playing G. Then this sequence of stage games is itself a game: a *repeated game* or a *super game.* Two statements are implicit when we say that in each period we're playing the same stage game:

a. For each player the set of actions available to her 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 the past.

b. The payoffs to the players 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 player for a given action profile for G is independent of which period it is played.

Statements a and b are for our repeated game is *stationary* (or, alternatively, independent of time and history). This does *not* mean the actions themselves must be chosen independently of time or history.

Then we interpret a and b above as saying that the payoff matrix is the same in every period.

We make the typical "observable action" or "standard signaling" assumption that the play which occurred in each repetition of the stage game is revealed to all the players before the next repetition. Therefore even if the stage game is one of imperfect information (as it is in simultaneous-move games)—so that during the stage game one of the players doesn't know what the others are doing/have done that period—each player *does* learn what the others did before another round is played. This allows subsequent choices to be conditioned on the past actions of other players.

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.

We'll refer to the action of the stage game G which player i executes in period t as a_i^t. The *action profile* played in period t is just the n-tuple of individuals' stage-game actions $a_t = \left(a_1^t, a_2^t, \ldots\ldots a_n^t\right)$............ (1)

We want to be able to condition the players' stage-game action choices in later periods upon actions taken earlier by other players. To do this we need the concept of a *history*: a description of all the actions taken up through the previous period. We define the history at time t to be $h^t = \left(a^0, a^1, \ldots\ldots a^{t-1}\right)$ …………..(2)

In other words, the history at time t specifies which stage-game action profile (i.e., combination of individual stage-game actions) was played in each previous period. Note that the specification of h^t includes within it a specification of all previous histories $\left(h^0, h^1, \ldots\ldots h^{t-1}\right)$. For example, the history h^t is just the concatenation of h^{t-1} with the action profile a^{t-1}; i.e. h^t =(h^{t-1} , a^{t-1}) The history of the entire

game is $h^{T+1} = \left(a^0, a^1, \ldots\ldots a^T\right)$Note also that the set of all possible histories h^t at time t is just

$$A^t = \underset{t=0}{\overset{t-1}{X}} A \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \quad (3)$$

To condition our strategies on past events, then, is to make them functions of history. So we write player i's period-t stage-game strategy as the function s_i^t, where $a_i^t = s_i^t(h^t)$

is the stage-game action would play in period t if the previous play had followed the history h^t. A player's stage-game action in any period and after any history must be drawn from her action space for that period, but is the stage-game action would play in period t if the previous play had followed the history h^t. A player's stage-game action in any period and after any history must be drawn from her action space for that period, but because the game is stationary her stage-game action space A_i does not change with time. Therefore we write:

$(\forall i \in I)(\forall t)(\forall h^t \in A^t)s_i^t(h^t) \in A_i$. Alternatively, we can write $(\forall i \in I)(\forall t)\, s_i^t : A_i^t \to A_i$

The period-t stage game strategy profile s^t is $s^t = (s_1^t, s_2^t.......s_n^t)$

This profile can be described by $s_i^t : s^t ; A^t \to A$ (i.e) $\forall h^t \in A^t, s^t(h^t) = (s_1^t(h^t), s_2^t(h^t)..........s_n^t(h^t))$

Let a^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^i *n*-tuple of individuals' stage game actions $a^t = (a_1^t, a_2^t, ...a_n^t)$.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 $h^t = (a^0, a^1, ...a^{t-1})$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^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 We now define the players' payoff functions for the repeated game. When studying will be recorded at the base station, where $a^0 = (a_1^0, a_2^0, ...a_n^0)$. The history is then revealed to the IDS so that it can condition its period-1 play upon the period-o play. It means that if a node is acting maliciously, by keeping history of game, the IDS is able to notify neighbouring nodes of a malicious one. Each node chooses its t=1 stage game, strategy $s^1(h^1)$. Consequently, in the $t = 1$ stage game the stage game strategy profile $a^1 = s^1(h^t) = (s^1(h^1), \cdots, s^1$ $(h^1))$ is played.

Each node *i* has a von Neumann-Morgenstern utility function defined over the outcomes of the stage game *tt*, as $u_i : A \to$ R, 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 $c^t = c^r.d^\mu$, where c^r is a constant *i* that includes antenna Characteristics, *d* is the distance of the transmission and μ is the path loss exponent

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.

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 pay- offs, 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^t, then we could summarize the desirability of the payoff stream

$u_i^0, u_i^1 ....$, by the number:

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

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^t a player receives are some constant payoff v^{r} for the first *t* periods, and thereafter it receives a different constant payoff v^{rr} in each period. The average discounted value of this payoff stream is:

$$(1-\delta)\sum_{\tau=0}^{\tau=\infty}\delta^t v_i^t = (1-\delta)\left[\sum_{\tau=0}^{t-1}\delta^t v_i^t + \sum_{\tau=t}^{\infty}\delta^t v_i^t\right]$$

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 de- pends 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:

$UIDS\ = \gamma_1 v'''' \ -\gamma_2 v''' \ -\gamma_3 v''$, where each γi 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:

$$s_{IDS}\left(h^t\right)=\begin{cases} miss\ \ if & t=0 \\ miss\ \ if & a_i^{t-1}=normal \\ catch & otherwise \end{cases}$$

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,

$$s_{IDS}\left(h^t\right)=\begin{cases} normal\ \ if & t=0 \\ normal\ \ if & a_i^{t-1}=miss \\ malicious & otherwise \end{cases}$$

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 pay-off stream, we see that the player receives v' for the first t periods, then receives v'' only in period t and receives $_i$ every period thereafter. Therefore, the average dis- counted value of this stream is:

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

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 in- finitely 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.

1.3 Payoff and Reputation

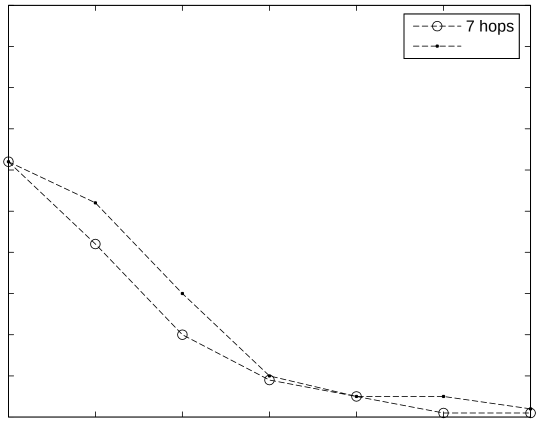
The problem of generating reliable information in sensor networks can be reduced to one basic question: How do sensor nodes trust each other? Embedded in every social network is a web of trust with a link representing the amount of trust between two individuals. Here IDS monitors the behavior of other 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:

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

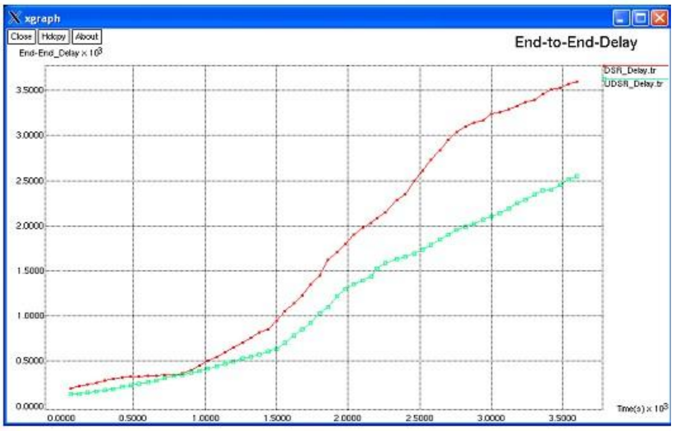
where $\rho i(k)$ represents the ratings that the IDS has given to node i, and $\rho i \in [-1, 1]$. If the number of observations collected since time t is not sufficient, the final value of the subjective reputation takes the value 0. IDS increments the ratings of nodes on all actively used paths at 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.

1.4 Protocol Description

In this proposed protocol a node sends out a route request message. All route receiving the 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 be- fore. 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



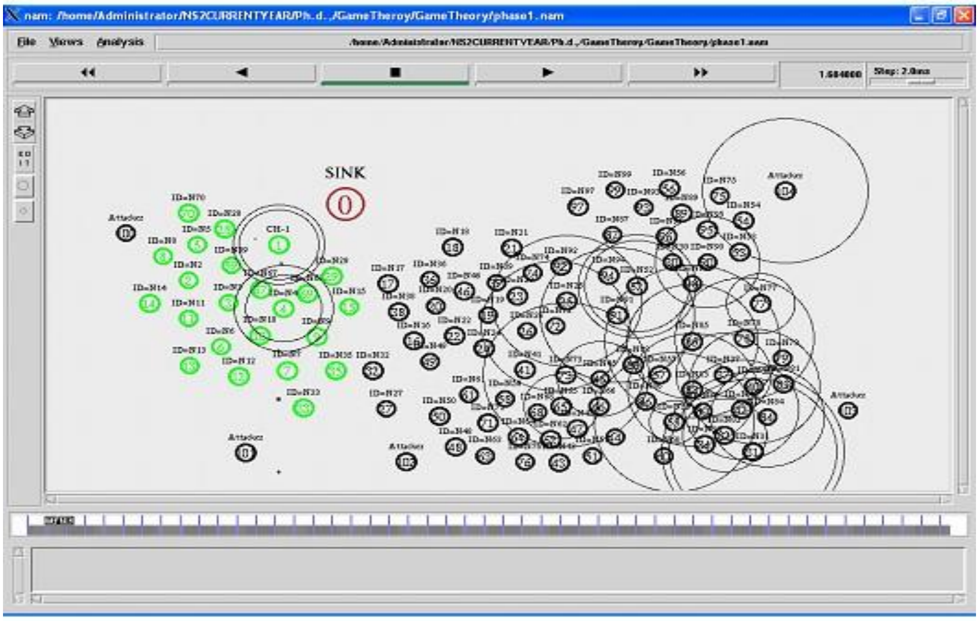
(1) End-End Delay



X-axis represents Times (s) and Y-axis represents End- End Delay (ms)

Percentage of malicious node

Here number of sensor nodes with one base station required.



nam: /home/Administrator/NS2CURRENTYEAR/Ph.d../GameTheroy/GameTheory/phase1.nam
File
Views
Analysis
/home/Administrator/NS2CURRENTYEAR/Ph.d../GameTheroy/GameTheory/phase1.nam
1.684000
Step: 2.0ms
SINK
0
CH-1
Attacker
Attacker
Attacker
Attacker
Attacker

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 pro- vide likely service due to their commitment, as they want to increase their reputation in the network. IDS also want 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.

.

II. 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.

REFERENCES

[1]. I. F. Akyldiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, ―Wireless sensor networks: a survey,‖ Computer Networks, vol.38, pp:393-422

[2]. I. F. Akyildiz and I. H. Kasimoglu, ―Wireless sensor and actor networks:research challenges,‖ to be published Ad Hoc Networks, 2004.

[3]. T. Basar and G. T. Olsder, Dynamic Non cooperative Game Theory, 2nd Ed., Society of Industrial and Applied Mathematics, 1999.

[4]. S. Buchegger and J. L. Boudec, ―Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes-Fairness In Dynamic Ad-hoc NeTworks,‖ MobiHoc, 2002.

[5]. N. Bulusu, D. Estrin, L. Girod and J. Heidemann, ―Scalable coordination for wireless sensor networks: self-configuring localization systems,‖International Symposium on Communication Theory and Applications

[6]. Dan Li, Kerry D. Wong, Yu Hen Hu, Akbar M. Sayeed."Detection, Classification, and Tracking of Targets,"IEEE Signal Processing Magazine, Volume 19, pp: 17-19, (2002).

[7]. 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),

[8]. Wei-Peng Chen, Hou, J.C, Lui Sha. "Dynamicclustering for acoustic target tracking in wireless sensornetworks", IEEE Transactions on Mobile Computing,Volume 3, pp: 258 - 271, (2004).

[9]. L. Buttyan and J.P. Hubaux, ―Nuglets: AVirtual Currency to Stimulate Cooperation in Self organized Mobile Ad-Hoc Networks,‖Technical Report DSC/2001/001,Swiss Fed. Inst. Of Technology, Jan. 2001

[10]. S. Marti, T. Giuli, K. Lai and M. Baker, ―Mitigating routing misbehavior in mobile ad hoc networks,‖ Proceedings of Mobicom 2000, Boston, MA,USA, August 2000.

[11]. A. Perrig, R. Canetti, J. Tygar and D. Song, ―Efficient Authentication and Signing for Multicast,‖ NDSS, 2001.

[12]. A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, ―SPINS: Security Protocols for Sensor Networks,‖ MobiCom, pp: 189-199, July 2001.

[13]. V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. ao,―Cooperation in Wireless Ad Hoc Networks,‖ Proc. IEEEINFOCOM, vol. 2, pp. 808-817, Apr. 2003

[14]. E. Shih, S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang and A.Chandrakasan, ―Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks,‖ Proceedings of ACMMobiCom, Italy, pp:272-286, July 2001

[15]. Nuggehalli, C. F. Chiasserini and R. R. Rao, ―Cooperation in Wireless Ad Hoc Networks,‖ INFOCOM, 20