International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Game Theory for Preventing Denial of Service in Wireless Sensor Networks

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

[1]*K.N. Government Arts College for Women, Tamilnadu, India*
RMKCET, Tamilnadu, India

Abstract— **Wireless Sensor Networks are becoming an integral part of our lives. There cannot be widespread applications of WSNs without ensuring WSNs security. This paper provides the security approaches based on game theory in WSNs. In this paper we framed a active defense problem as a non -cooperative nonzero sum two player game between attacker and nodes of wireless sensor network. This game achieves Nash equilibrium and thus leading to defense strategy for the network. Results show that game frameworks increases the chance of success in the defense category for WSNs.**

Keywords—**Keyword are your own designated keyword which can be used for easy location of the manuscript using any search engines. It includes at least 5 keywords or phrases in alphabetical order separated by comma.**

I. Introduction

With the recent advances in wireless communications and digital electronics, WSNs have become increasingly one of the most promising and interesting areas in the past years. Limited memory and battery power of sensor nodes create a number of challenges in terms of the security of wireless sensor networks. In this paper we proposed secure base routing for preventing different types of attacks. In the second part we proposed non cooperative non zero sum game theory where each player is tries to maximize its own payoff. This game achieves Nash equilibrium, thus leading to defense strategy for the network.

II. Related Works

There are many researches that are applying game theory in intrusion detection systems. A game theoretic platform is suitable for modeling security issues such as intrusion prevention and intrusion detection. An example of an intrusion prevention game model is presented in (Liu &Zang, 2005), where the authors propose a game theoretic approach to infer attacker intent, objectives, and strategies (AIOS). In the context of intrusion detection, several game-theatrical approaches have been proposed to wired networks, WLANs, sensor networks, ad hoc networks and mobile ad hoc network.

Kodialam&Lakshman (2003) have proposed a game theoretic framework to model the intrusion detection game between two players: the service provider and the intruder. A successful intrusion is when a malicious packet reaches the desired target. In the game, the objective of intruder is to choose a particular path between the source node and the target node, and the objective of the service provider is to determine a set of links on which sampling has to be done in order to detect the intrusion. Essentially, the game is formulated as a two-person zero-sum game, in which the service provider tries to maximize his payoff, which is defined by the probability of detection, and on the other hand, the intrude tries to minimize the probability of being detected.

Patcha & Park (2006) used the concept of multi-stage dynamic non-cooperative game with incomplete information to model intrusion detection in a network that uses a host based IDS. As long as the beliefs are consistent with the information obtained and the actions are optimal given the beliefs, the model is theoretically consistent. They believe that this game-theoretic modeling technique models intrusion detection in a more realistic way compared to previous approaches.

Otrok et al. (2008) proposed a unified framework that is able to prolong the lifetime of IDS in a cluster by balancing the resource consumptions among all the nodes. This was achieved by truthfully electing the most cost-efficient node

(IDS) that handles the detection process. Incentives were given in the form of reputations to motivate nodes in revealing truthfully their costs of analysis.

Poongothai et al. (2008) presented a model for analyzing misbehaviors using game theory their model focuses on interaction between pair of attacking/regular nodes as a two player non-cooperative non-zero sum game.

Agah& Das (2007) formulated 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.

III. SECURITY TO WSN USING AUCTION THEORY

An auction is a method of allocating scarce goods based on competition. A seller wishes to obtain as much money as possible, and the buyer wants to pay as little as possible. There are different ways to classify auctions. Thee are open auctions as well as sealed auctions. In this we adopt sealed bid mechanism because sealed bid requires little communication or interacion between participants. We propose secure routing protocol in sensor networks which is based on first price sealed auctioning.

In first-price sealed auction always the bidder with the highest bid wins and reaches equilibrium and thereafter the truth bidding is a dominant strategy for sensors. With suitably designed rules, auctions can achieve efficient allocations with minimal a priori information. One of the essential reasons to use auction is to speed up the sale and ignite competition between buyers, which is the main reason to adopt the first-price sealed auction mechanism in the approach presented in this chapter. The absence of pre-existing infrastructure in sensor networks means that most of the nodes will serve as routers for through traffic. Sensor nodes, either malicious or truthful, compete against each other in order to forward incoming packets and by doing so each node improves its reputation among other nodes. Bidding is done to gain a better reputation in the network and instead of paying money, the winner of the bid disinherits some of its initial energy power. Participation in an auction is a decision that is completely up to the sensor node, whereas a malicious node tries its best to win the bid and then drops the packets and corrupts the network.

IV. PROTOCOL DESCRIPTION

In the proposed Secure Auction-based routing (SAR) protocol, a node sends out a Route request message. All nodes receiving this message 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 and the bid price that it is willing to pay. After receiving one or several routes, the source selects the best one having the highest bid; stores it and sends messages along that path. In the SAR protocol, the path is chosen by picking the path from the cache of available paths to the packet's destination with the highest bid, as depicted in Figure 4.1. Once a route request reaches its destination, the path that this route request has taken is reversed and sent back to the sender.

This protocol proposes an auction on routes to ensure a view on which nodes will provide likely service due to their commitment. Note that a malicious node could agree to the auction and still subvert the route, so a watch-list facilitates recognizing such faulty nodes. How can we determine if a node is acting maliciously? Destination nodes can send back messages, and when one destination node gets notified of the winning path, it sets a timeout timer. In order to implement the timeout at the receiving node, once the auction ends, the sending node sends a Winning route packet to the destination node, which stores this route and the source. Once the destination node gets a packet from the source (that is not a control message), it removes the source from its list of pending links. If the pending link times out, then the destination node sends abed route packet to the base station, which updates its list with the nodes in the route (excluding the source and destination). If a node is placed on the watch-list more often than a pre-defined threshold, the base station sends out a Watch list ignore broadcast, and all of the nodes add that node into their ignore lists. The threshold is high enough to distinguish deliberate malicious behavior from simple selfishness of a node. All nodes prefer not to communicate with a node in their ignore list.

V. THE BID

In strategic games, players first make their decision and subsequently the outcome of the game is determined. The outcome can be either deterministic or contain uncertainties. The decisions are made without knowledge of other player's decisions. In sensor network consisting of N sensors, where occasionally some of them act maliciously, there are N players that compete to bid against each other.

Definition 1

The strategic game called (bidding) consists of

- a finite set of N sensor nodes
- for each node $i \in$ {1, ...,N} a nonempty set A_i of actions available to node i .
- for each node $i \in$ {1, ...,N} a von Neumann-Morgenstern utility function $u_i : A_i \to R$

where R is the set of real numbers.

A sealed-bid auction is a typical strategic game with incomplete information A player/node knows its own valuation of the packet but does not know the valuation of other bidders.

The solution of a strategic game is a Nash equilibrium. Every strategic game with a finite number of players, each with a finite set of actions has an equilibrium This Nash equilibrium is a point from which no single player wants to deviate unilaterally.

Definition 2

A Nash equilibrium of a strategic game $\langle N,(A_i),u_i\rangle$ is a profile $a*=(a_1^*,a_2^*,a_3^*,.........a_N^*\ )$ of actions with the property that for every player $i\in\{1,2,.....N\}$

$$u_i(a^*)\geq u_i(a_1^*,a_2^*,a_3^*......a_N^*)\ \forall a_i\in A_i$$

When a game is played, the rationality assumption will force the game into a Nash equilibrium outcome.

If the outcome is not a Nash equilibrium, at least one player would gain a higher pay off by choosing another action. If there are multiple equilibria, more information about the behavior of the players is needed to determine the outcome of the game. We present the model of our proposed framework for secure routing as an auction game. Players of this game are the nodes of the network who bid against each other in order to obtain better reputations in the network.

Each bidder submits a sealed bid of b_i. A winner i will be charged the price Ω_i which is its battery power loss. Only one path wins a bid, and nodes on this path are assumed to be cooperative. If the nodes on the winning path cooperate, then their reputation will be raised, otherwise another path will be chosen. In order to model the player's strategy, their perception of the bid needs to be presented. Our analysis relies on the fact that players, along with their own absolute profit, are also motivated by the relative profit, which indicates how their standing compares to the profit of other players. The utility of a node is not solely based on the absolute payoff but also on the relative payoff compared to the overall payoff of all nodes. We use the theory of Equity, Reciprocity and Competition (ERC) model presented in [10] as follows: $v_i=\alpha_i u(y_i)+\beta_i r(\sigma_i\ )$ where α_i,β_i are positive constants and u(.) is differentiable strictly increasing concave and r(.) is differentiable, concave and has its maximum at $\sigma_i=\frac{1}{N}$. Here v_i is the ERC global utility function, y_i is the absolute profit and $u(y_i)$ is the absolute utility function for player i.

The total amount of bid that each node is willing to pay is v_i. The absolute profit value of a node depends on the node's battery power (Ω_i) and its reputation (Φ_i) which will be discussed in section

VI. The Equilibrium Strategy

Each of the N > 1 potential bidders knows how much it is willing to pay (v_i). Each node's decision problem can be viewed as of choosing a bid b(v_i) and probability ρ of winning. Suppose $b*$ is the equilibrium bid strategy, one can show that $b*$ is monotonically increasing in v which guarantees that the bidder with the highest evaluation would win the auction .

Proposition 1 For the given utility structure of the bidding game, there is always a Nash equilibrium at $b^*(v)(1-\frac{1}{N})v.$

Proof: If the bidder i bids the amount $b=b^*(v)$), he wins with probability

$$\rho(b)=pr\{b^*(v_1,v_2,....v_{i-1,}\ v_{i+1}....v_N\ )<b\}$$

$$=\rho(b)=pr\{b^*(v_1,v_2,....v_{i-1,}\ v_{i+1}....v_N\ )<\delta(b)\}$$

where is $\delta(b)$ the inverse of $b*(v_i)$. This indicates the valuation that leads to bidding the amount b if strategy $b*$ is played and v_i is the ith order statistic of the sample of N random valuations. In equilibrium, the bid b must be a best-response to bids. Therefore, b must be a maximize of the expected gain: $\rho(b)(v_i-b)$ leading to the condition $\rho'(b)(v-b)-\rho(b)=0$ where ρ' is the derivative of ρ _. By using the fact that $v=\delta(b^*(v)),$ the differential equation will have the solution of $\delta(b)=\frac{N}{N-1}b.$ finally solving this for b the equilibrium bid strategy is given by: $b^*(v)=(1-\frac{1}{N})v.$

One can also prove that this equilibrium is unique. For, $N = 2$, $\delta(b) = \frac{1}{2\delta^2} + \delta(0)$ Since, $b = 0$ one has $\delta(0) = 0$ and thus $\delta(b) = 2bv$ where v is the price that bidder is willing to pay. Hence, the unique equilibrium strategy is $b^*(v) = \frac{1}{2v}$. In order to generalize the proof to $N > 2$, one can apply a transformation of variables, from (δ, b) to (z, b), where $z = \frac{\delta}{b}$, and by separating variables and uniquely solving the differential equation by integration.

The intuition behind this proposition is that, for the defined bidding game, a Nash equilibrium exists. This is a point from which no other node wants to deviate. The maximum amount that each node is able to truthfully bid is its utility. Now that we know where the equilibrium is (which depends on the payoff values calculated at the moment), the network will take the corresponding biding acceptance based on the payoffs calculated. In other words, the equilibrium tells us about the most rational choice for each bidder in the game in certain situation and the network follows that.

VII. THE PAYOFF

Each node's payoff is calculated based on two parameters, namely, battery power and reputation. In order to compute the required power for each sensor node, communication and computation of sensor nodes are being considered. The communication energy usage is much higher than the computation energy usage. Communication in sensor networks is dependent on the connectivity of the network, where connectivity is defined as the ability to link between any pair of nodes. The connectivity cost is function of the number of hops, latency, etc.. In a path containing k nodes, we measure the connectivity energy usage as a function of available energy at each node and the total number of en-route hops. So we define the energy consumption as : defined as

$$\Omega_i(t) = \frac{pow_i(t)}{k} \, where$$

$$pow_i\ (t) = N_T \left\lfloor P_{iT}(T_{on}(t) + T_{st}(t) + P_{i_o\,ut}(T_{on}(t)) \right\rfloor + N_R \left[P_{iR}(R_{on}(t) + R_{st}(t)) \right]$$

where P_T is the power consumed by the transmitter, P_R is the power consumed by the receiver, P_{out} is the output power of the transmitter, T_{on} is the transmitter on time, R_{on} is the receiver on time, T_{st} t is the transmitter start-up time, R_{st} is the receiver start-up time, N_T is the number of times the transmitter is switched on per unit time, and N_R is the number of times the receiver is switched on per unit time, which depends on the medium access control scheme used. A node that acts maliciously or saves its internal memory and power by not forwarding incoming packets and dropping them for its selfishness, should suffer from bad reputation and be isolated from the rest of the network. On the other hand, when anode does not act selfishly, then it must be rewarded; and the reward it gets is the good reputation. By doing a service for the network, each node will improve its reputation. As time passes, more nodes recognize a node with good reputation.

Definition: **3:**Let $P_i^f(t)$ and $P_i^r(t)$ be respectively the number of packets forwarded and received at sensor node i at time t. The reputation of node i, denoted as $\phi_i(t)$ is defined as the ratio of the number of packets forwarded to the total number of received packets at time t at node. Thus $\phi_i(t)$ is a measure of throughput experienced at each node and calculated as, $\phi_i(t) = \frac{P_i^f(t)}{P_i^T(t)}$ The reputation value decreases when misbehavior is detected. For any given node, the payoff is given by $\phi_i(t)$. Which is the reputation that it gains over time. But it also must bear some additional cost $\Omega_i(t)$ which is the energy loss. Therefore, the payoff is calculated as, $y_i(t) = \alpha\phi_i(t) - \beta\Omega_i(t)$. where α and β are weight parameters.

VIII. NON COOPERATIVE NON ZERO-SUM GAME

A two-player game is the most basic form of games, but also a powerful tool for solving problems with conflicting goals. In such games, each player has a set of strategies, which are all the possible choices he has in the game.

A two-player game consists of players p1 and p2, where p1 has n strategies numbered as {1, 2, ..., n} and p2 has m strategies numbered {1, 2, ...,m}. In a game defined by the payoff matrices $A=\lfloor a_{ij} \rfloor$ and $B=\lfloor b_{ij} \rfloor$, a pair of strategies $\left(rowi^{*}, column\ j^{*}\right)$is said to constitute a non-cooperative pure strategy (Nash) equilibrium solution to the game if the following pair of inequalities is satisfied: $a_{i^{*}j^{*}} \le a_{ij^{*}}$ *and* $b_{i^{*}j^{*}} \le b_{i^{*}j}$ $\forall i = 1,2,.......n \text{ and } \forall j = 1,2,.......m.$ It has been shown in that a two-player non zero-sum game may or may not have a pure strategy Nash equilibrium.

Game Formulation Of The Proposed Protocol

In our two-player game consisting of sensor nodes, players are Intrusion Detection System (IDS), which can reside at the base station, and the attacker. With respect to one fixed node, say k, which itself is a cluster-head, the attacker node has the following two strategies as depicted in following figure.

- AS1: attack node k ,
- AS2: attack a node different than k .

The attacker chooses a strategy to attack a node. The network predicts the attacker's strategy by finding the most vulnerable node.

The sensor network also has two strategies:

- SS1: defend node k ,
- SS2: defend a different node.

The payoffs of these two players are expressed in the form of 2×2 matrices, A and B, where a_{ij} and b_{ij} denote the sensor network's and the attacker's payoff, respectively.

Let us first define some notations:

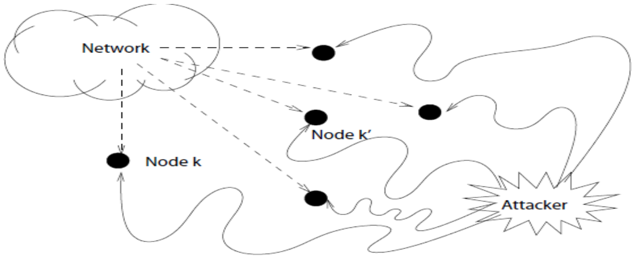
- $U(t)$: the payoff of the network at time t .
- L_k : the cost of losing a malicious node k .
- C_k : the cost of defending a node k .
- N_k : the number of sensor nodes in the cluster, where node k is the cluster-head & the number of sensor node

Communicating with a node k

$Cost_{wait}$: the cost of waiting and deciding to attack in the future.

$Cost_{\text{int}}$: The cost of intrusion for attacker

$P(t)$: Profit of each attack



Two payoff matrices $A=\lfloor a_{ij} \rfloor$ and $B=\lfloor b_{ij} \rfloor$, are defined such that a_{ij} denotes player p_1's payoff when player p_1 chooses strategy i and player p_2 chooses strategy j ;whereas b_{ij} denotes player p_2's payoff when player p_1 chooses strategy i while player p_2 chooses strategy j. We define the network's payoff matrix as follows:

$$A=\left[a_{ij}\right]_{2x2} = \begin{bmatrix} U(t)-C_k & U(t)-C_k-E(\sum_{i\neq k} L_i \\ U(t)-C_{k'}-\sum_{i\neq k'} L_i & U(t)-C_{k'} \end{bmatrix}$$

Here a_{11} represents the payoff if the players follow the strategy pair (AS_1, SS_1),which is when the attacker chooses to attack node k and the network chooses to defend the same node k. Thus, for the network, its original utility value of $U(t)$ will be deducted by the cost of defense C_k. The term a_{12} represents the payoff corresponding to the strategy pair (AS_2, SS_1) ,which is when the attacker attacks a different node k', but the network still defends node k . In this case we subtract the cost of defending one node from the original utility, as well as deducting the expected value of losing another node, which can be any other node than k. The term a_{21} represents the payoff of strategy pair (AS_1, SS_1) ,that is the attacker and the network choose two different nodes to attack and to defend, respectively. The term a_{22} represents the payoff of strategy tuple (AS_2, SS_2), which is when the attacker attacks a node other than k and the network defends another node. In this case we subtract the cost of defending one node, from the original utility, as well as deducting the loss of losing another node.

We define the attacker's payoff matrix as follows:

$$B = \left[b_{ij}\right]_{2x2} = \begin{bmatrix} Cost_{\text{int}} & P(t) - Cost_{\text{int}} \\ P(t) - Cost_{\text{int}} & Cost_{\text{int}} \end{bmatrix}$$

For the network, the cost of defense is the price it must pay to protect a node that is most likely to be under attack. We assume it is dependent on two parameters:

(i) the cost of protecting a node which is more important in the network, like an aggregation point, must be higher than the cost of protecting a normal node, and

(ii) the cost must be dependent on the number of nodes communicating with that node.

*Definition 4:*The cost of intrusion for the network is given by: $C_i = \varsigma\gamma_i + \eta N_i$ where γ_i is the weight of a node i where ς and η are weight parameters and $\varsigma + \eta$ =1.Depending upon the sensor applications, there value can be varied, assume that $\varsigma >> \eta$.

We define cost of waiting for the attacker as: $Cost_{wait} = \delta\gamma_i'$ where δ is a weight parameter and γ_i' is the number of previous unsuccessful attack attempts. Profit of each attack for the attacker and the loss of losing a node for the network are dependent to the density of nodes that are communicating with the node, and the reliability of each node $r_i(t)$. The density can range from few sensor nodes to few hundred sensor nodes, density μ can be calculated according as $\mu(R) = \dfrac{N\pi R^2}{A}$ where N is the number of scattered sensor nodes in the region A, and R is the radio transmission range. The node density depends on the application in which the sensor nodes are deployed.

Definition 5: Profit of attack for the network are defined as:

$$P(t) = \sum_{i=1}^{N} L_i = \mu \Pi i_{i=1}^{N} r_i(t)$$

In a zero-sum game everything that someone wins must be lost by someone else. Our defined game is non zero-sum. In order to justify this, let us assume that the game is zero sum in the sense that the increase in one player's payoff implies the decrease in the other player's payoff. However, this may not be true for our system.

For instance, networking is always protecting itself but if attacker does not attack, payoff of one party is decreasing while payoff of other party is steady, which is conflicting with the zero-sum assumption. So this game have to be modeled as non-zero sum. Now we study the equilibrium solution for the game. Let us first introduce the concept of dominant strategy in the game theory. Given a matrix game defined by two mxn matrices, A and B , which are the payoffs of player p_1 and p_2 respectively. We say that "row i " dominates "row " k " if $a_{ij} \geq a_{kj}$, for $j = 1,2,....n$ "row i " is called dominant strategy for player p_1. For p_1, selecting the dominating "row i " is at least as good as selecting the dominated "row k ". So "row k " actually can be removed from game because p_1 as a rational player would not consider this strategy at all.

Theorem: The defined game has Nash equilibrium at strategy pair (AS_1, SS_1).

In the network's payoff matrix $A = \left[a_{ij}\right]_{2x3}$ and the attacker's payoff matrix $B = \left[b_{ij}\right]_{2x3}$, SS_1 is dominating strategy and so SS_2 can be eliminated. A and B become 1x3 matrices. Obviously $a_{11,}\ a_{12} \geq a_{13}$. Now there are 4 possible cases to consider:

- If $N_k > N_{k'}$ *and* $\gamma_k > \gamma_{k'}$ *then* $C_k > C_{k'}$ so $U(t) - C_k < U(t) - C_{k'}$ and therefore $a_{12} \geq a_{11}$
- If $N_k < N_{k'}$ *and* $\gamma_k > \gamma_{k'}$ *as* $\varsigma >> \eta$ *then* $C_k > C_{k'}$ and so $U(t) - C_k < U(t) - C_{k'}$ and therefore $a_{12} \geq a_{11}$
- If $N_k < N_{k'}$ *and* $\gamma_k > \gamma_{k'}$ *then* $C_k < C_{k'}$ and so $U(t) - C_k > U(t) - C_{k'}$ and therefore $a_{11} \geq a_{12}$.
- If $N_k > N_{k'}$ *and* $\gamma_k < \gamma_{k'}$ *then* $C_{k'} = \varsigma'(\gamma k + \alpha_0) + \eta'(N_k - \beta_0)$ *as* $\varsigma' >> \eta'$, *so* $C_k < C_{k'}$ and then $U(t) - C_k > U(t) - C_{k'}$ and therefore $a_{11} \geq a_{12}$.

Obviously $b_{11}, b_{13} \geq b_{12}$. and $b_{11} = b_{13}$, which implies equilibrium for the game is at a_{11} and b_{11}

From the definition of Nash equilibrium, we conclude that strategy pair (AS_1, SS_1) constitutes the Nash equilibrium to this game. So the equilibrium of the network is when it chooses the node with the highest value of $U(t)-C_k$ for protection.

The intuition behind the above discussion is that for the network the best strategy is finding the best node to defend, which the one with maximum value is of $U(t)-C_k$ and for the attacker the best strategy is finding the right node to attack, as $P(t)-Cost_{\text{int}}$ is always more than $Cost_{wait}$, so attacker is always encouraged to attack.

In our proposed protocol UDSR where the nodes send out a route request message all the nodes that receive this message, calculate their utility value, put themselves and their utility value into the source route and forward it to their neighbors, unless they have received the same request before. If the receiving node is in the destination, or has a route to destination, it does forward the request, but sends a REPLY message containing the full source route and the total utility value.

IX. CONCLUSION

In this paper we proposed two protocols. Our objective was to measure the effectiveness of these schemes in Detecting malicious behavior. The experimental results shows that by including the utility value of each route Which is based on cooperation and reputation of en-route nodes, we can guarantee a more reliable delivery.

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