Secure Packet Transfer in Wireless Sensor Networks – A Trust-based Approach

Yenumula B. Reddy
Grambling State University
Grambling, LA 71245, USA
ybreddy@gram.edu

Rastko Selmic
Louisiana Tech University
Ruston, LA 71270, USA
rselmic@latech.edu

***Abstract*—Trust is very important in wireless sensor networks to transfer the data from source to destination. The Dynamic Source Protocol calculates the alternate path, if any node fails to transfer the data. The Dynamic Source Protocol does not have any built-in functionality to calculate an alternate path if the path has a malicious node. With the expense of an intruder detection system we can detect the malicious node and alter the data/packet transfer path. However, intruder detection system is very expensive for wireless sensor networks and there is no guarantee in detecting a malicious node. In the current research a trust-based approach is recommended to minimize the overheads of intruder detection system and it also detects the abnormal behavior nodes. The proposed model uses the repeated games to detect faulty nodes through the cooperative effort in the sensor network and further judges the trust of successive nodes. Simulations were presented for normalized payoff of packet dropping, average discount payoff, and trust relation.**

Keywords-wireless sensor networks; repeated games; packet transfer; trust-based approach; secure transferof data.

I. INTRODUCTION

Wireless sensor networks (WSN) are used in a variety of applications including structural health monitoring (SHM), industrial automation (IA), civil structure monitoring (CSM), military surveillance (MS), and monitoring the biologically hazardous places (BHP). In CSM, MS, and BHP the data is transferred over a number of nodes and any malicious node in the path leads to a dangerous situation. The Dynamic Source Protocol (DSR) cannot detect the malicious node and the IDS package has overheads as well as more false alarms. Hence, we need an alternative approach to detect the malicious node on the communication path with minimum overheads. The alternative approach includes trusting the next node in the path generated by DSR. Here, trust means transferring the packets above expected percentage (for example more than 95%) of packets that were received by that node.

The sinkhole detection, selective forwarding attacks, acknowledgement spoofing, detection of malicious node, and utility-based decision making were discussed in [1-4, 15-19, 21-22]. None of these researchers attempted to verify that the next node in the path was malicious or trustworthy to transfer the data. Failure to transfer the packets depends upon the normal failure of node (communication path or battery loss or node was destroyed) or if the node is compromised. The research of selective forward attacks and detection of malicious nodes provides an extra effort if the data does not reach the destination. But we need a trusted path at the time of transferring the data (packets).

Perrig et al. [1] introduced the modified TESLA [2] protocol for sensor networks and named it μTESLA. The new protocol (μTESLA) is designed to show that security is possible in sensor networks by usage of a simple model to authenticate and transfer the data that is required. Therefore, it is necessary to develop a simple model that eliminates unnecessary checks, avoids sinkholes, detect selective forward packet drops, and improve processing time. The checkpoint-based multi-hop acknowledgement scheme (CHEMAS) [3] identifies the localization of the suspected node that requires extra processing to detect a malicious node. The authors claim that the scheme (CHEMAS) has a high detection rate with communication overhead.

Isolating misbehavior and stabling trust routing in wireless sensor networks was studied in [4]. The trust routing algorithm uses the μTESLA scheme to form the chain of trust. The chain of trust is an expensive process and has more overheads compared to trusting the next successive node. However, it is difficult to keep track of the complete communication path particularly in WSN. The authors in [4] discussed various search methods to detect the insecure locations and isolate those locations from communication paths.

Zhang and Huang [5] used reinforcement learning to establish a secure path for packet transfer from source to base-station. They concluded that adaptive spanning trees can maintain the best connectivity for transferring the packets between source and destination. The authors further discussed the energy-aware and congestion-aware problems for successful delivery of packets.

Carmen et al. [13] discussed the trust management in wireless sensor networks. A trust management system helps to detect the node (faulty or malicious) behaving in an unexpected way. Liu et al. [23] presented a dynamic trust model for ad hoc networks, where each node is

 ISBN:978-1-61208-113-7

assigned a trust value according to its identity. Sometimes trust level is also calculated by evaluation of nodes over other nodes. Evaluation of trust factor is done with IDS data and statistical data of packet transfer rate. Rebahi et al. [9] discussed a reputation based trust mechanism in ad hoc networks, where each node monitors the neighboring nodes activities, sends the information to the reputation manager, and stores it in a matrix for evaluation of nodes.

The belief-based packet forwarding model in mobile networks using repeated games was discussed in [6]. The authors described the belief-based packet forwarding model as being dependent upon past history of other nodes' information transfer. The model enforces cooperation in the ad hoc networks with noise and imperfect observation. Enforcing the cooperation slightly degrades the performance of packet transfer compared to unconditionally cooperative outcomes. The model further provides the ad hoc networks and needs to modify for WSN.

The rest of the paper introduces the repeated games to model the trust level of successive node and then formulate the trust-based model in a cooperative environment. Further, we calculate the trust-based packet forwarding and discuss the future research.

II. TRUST MANAGEMENT

Trust is subjective term used for reliability of an entity. It is a subjective probability of an individual A expects another individual B to perform a given task. The trust management model helps to detect the intruders (malicious nodes) and discard them from the communication path [9, 11, 12, 13]. The concept of reputation (collecting the data about status of a successive node) linked to trustworthiness [10] depends upon trusting a person (node). In the current situation trust depends upon the ratings of successive the node. If the ratings of the successive node are above the expected value (threshold) then the node will be trusted for transfer of data. Further, relaying on self detecting misbehavior nodes (intruders) is dangerous and collaborating between neighboring nodes is required.

Figure 1 shows the data transfer scenario from node A through node D and establishing the trust of node D for future data transfer. For example, node A sends data to node D and node D receives the data and acknowledges to node A. There is no guarantee that node D transfers the data to the next node in the path. If node A knows that node D transferred the data successfully, then node A assumes that node D can be trusted. After repeated transfers (successive node activity), if the trust factor reaches below the threshold, then node A compares the trust factors of its neighboring node B and node C that are transferring their data through node D. If nodes B and C trust node D, then node A establishes a new route for successful transfer of data and avoids node D. Trust of the next successive node in data path is a kind of watchdog approach to detect the malicious node.

In the proposed approach, each node maintains a rating of its successive node (number of successful pack transfer) in the path. If the ratings of a successive node are above the threshold (minimum error rate) then the current node continues to transfer the packets. The current approach does not expect to calculate all ratings (packet transfer, noise, jamming, and infection factor) of its neighboring nodes and selects the path of highest ratings [1]. Selecting a highest rating path requires more processing time and is a waste of energy in the sensor node. The proposed approach detects the malicious node using the trust factor. For example, if node D only selectively drops the packets from node A but not from nodes C and D then node A concludes that the path from node A through node D cannot be trusted and node A establishes the alternative path. The alternate path is selected only if the successive node is not trusted.

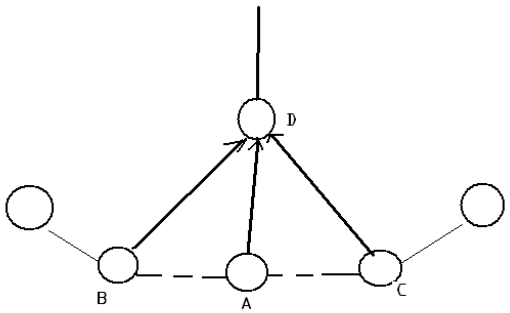

Figure 1. Scenario for node 'A' establishing trust of node 'D'.

III. GAME MODEL

In games [8, 20] the interaction between the players is inherently dynamic, so players always observe the actions of other players and decide their optimal response. Many times, the game is played repeatedly and decisions depend upon the previous actions or conclusion of previous actions. In repeated games, players have more opportunity to learn to coordinate their actions depending upon the previous outcome. In Figure 1, Player 1 and Player 2 (node A and node D) are involved in transferring the information where Player 1 transfers data to Player 2. Player 1 then waits for successful transfer of data packets from Player 2 to the next step in the path. Player 1's trust on Player 2 depends upon Player 2's successful transfer of data packets. The problem is how these two players coordinate their actions.

The outcome of Player 1 depends upon the actions (repeated outcome conclusion) of Player 2. In the cooperative effort, we must consider the outcome of neighboring players (within communication distance) of Player 1; that is, Player 3 and Player 4 (node B and node C in Figure 1) and have the similar interaction with Player 2. If the outcomes of Player 3 and Player 4 are the same as Player 1 (no better than Player 1) then the Player 1

 ISBN:978-1-61208-113-7

concludes either to transfer the future packets or chooses an alternative path. If the trust relation of Player 1on Player 2 is consistent and depends upon the outcome of its neighbors then we say it reaches to Pareto optimality.

In repeated games the behavior of Player 1 depends upon its opponent's (Player 2) actions (behavior). Further, no threat, punishment, or revenge is considered. The strategy is that Player 2 must transfer the packets received from Player 1. The trigger strategy is that the malicious behavior of Player 2 will permanently disconnect the path from Player 1 and its neighbors that have the current path through player 2. For example, the Stage game G is of the form

$$G = (N, A, U) \quad (1)$$

where N is a set of users (set of sensor nodes), A is a set of pure strategy profiles (actions – action may be the missing packets for each transmission), and U is a vector of payoffs. If Ω is the common discount payoff and $g_i(a^t)$ is the per-period payoff of the i[th] node related to current action a^t, then the normalized payoff β (relation to utility of sequence $a^0, a^1, .., a^T$) at any node is given by [20]

$$\beta = \frac{1-\Omega}{1-\Omega^{T+1}} t \sum_{t=0}^{t=T} g_i(a^t) \quad (2)$$

The trust of the player depends upon the outcome of β. The Figure 2 shows that the payoff is higher with a lower number of packets dropped in the same time period. But the average payoff will be very close in a large time period. Therefore it is necessary to consider frequent averages for packet dropping for appropriate decision.

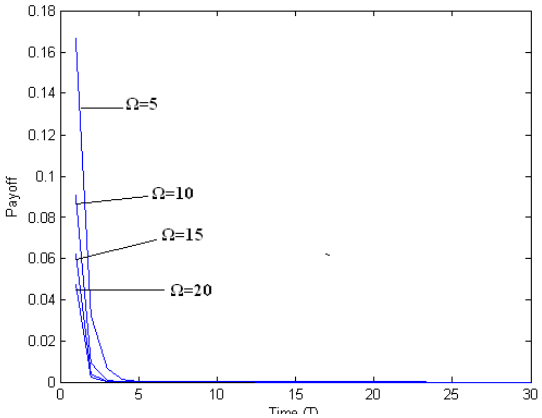

Figure 2. Payoff β verses packet dropping in a given time period

IV. Trust Model and Game Application

Each node in the sensor network maintains a dynamic table to store the information about packet transfer of the successive node in the path. The values in the table include the packets transmitted from the node and packets transferred from the successive node (recorded through over hearing). These values are used for trust calculation of the successive node. The values are also used to calculate the risk involved in order to carry out packet transfer. In other words trust value is a simple mathematical representation. The problem with no successive node will be dealt with different models [14, 15].

Consider a sensor network of N nodes deployed in a field. Let the nodes be connected as shown in the Figure 3 and represented through a matrix of equation (3). The filled nodes are existing nodes and unfilled are drawn to complete the matrix. Unfilled means no node exists or a dead node. The equation (3) helps to verify the isolated node (blackhole).

$$M = [M_{i,j}] = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} \quad (3)$$

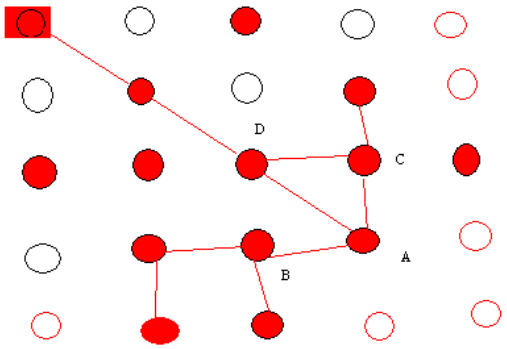

Figure 3. Sensor Network Nodes and their relation with neighboring nodes

Reputation is used to predict the behavior of the node. We create a table at node i (values stored in table at node i are over hearing from Node 2) to predict the behavior of the node j. Let $R_{i,j}$ represents the reputation of node j represented by node i. The reputation table RT_i stores the reputations maintained by node i and represented as:

$$RT_i = \{R_{i,j}\} \quad (4)$$

The periodic quantification of reputations at node j is $Q_{i,j}$ and is stored at RT_i as part of node j. The missing is calculated as (1 - $Q_{i,j}$). Further, each node has direct and indirect observations of reputations. Direct observation is the reputations stored at node i and indirect observations are received from neighboring node (s). The indirect

observations are represented as $IQ_{i,j}$. The trust prediction of the node j depends upon the $Q_{i,j}$ and $IQ_{i,j}$.

In repeated games, expected payoff depends upon the action profile and its observation. The action profile is given by

$$U_i = (\frac{1}{Q_{i,j}})\lambda \quad (5)$$

where λ is the difference between $Q_{i,j}$ and $IQ_{i,j}$. If λ =0 then the packets transferred at a node and its neighbor node is the same. The trust of the node depends upon the factor β. Further we calculate the average discount factor to calculate the stable state of the node. The average discount payoff is given by

$$UA_i = \beta(\sum_{t=1,n} \Omega_i(t).U_i(t)) / n \quad (6)$$

If the average discount payoff is above the threshold then node is in trust state and if trust state is consistent then we say it reaches Nash equilibrium. If the Nash Equilibrium exists in repeated games, then it satisfies Folk theorem [7] and sufficiently the player reaches to Pareto optimal payoff in Nash equilibrium. The simulations for average discount payoff are shown in Figure 4.

For a small value of λ (0.001) and probability of more than 90% successful packet transfer rate, the payoff increases in a smaller period of time (if lower number of packets is dropped). In average discount payoff, the number of packets dropped is set approximately the same. The number of packets transmitted is numbered in small or many. The average discount pay of increases initially (from 100 packet transmission to 900 packet transmission) and settles after it reaches a transmission rate of 1000 packets with the same number of drops. This shows, for a selected action strategy of a player, the game reaches Nash equilibrium at action profile during the time period of higher number of packet transmission with lower dropouts. That means the successive node can be trusted at current state.

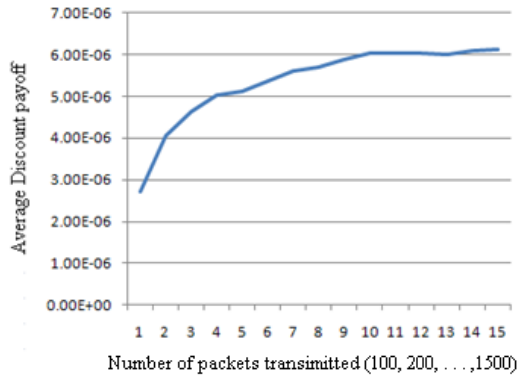

Figure 4. Average discount payoff verses number of packets dropped

V. TRUST-BASED PACKET FORWARDING

In trust-based systems, we begin to believe all nodes in the path are trusted. Trust of node 2 at node 1 will be developed after repeated transfer of packets from node 1 (n_i) to node 2 (n_j) and then successfully transferred from node 2. The trust of interaction between these nodes is

$$T_{i,j}^t = (n_j, s_k, TE_{i,j,t}) \quad (7)$$

where $T_{i,j}^t$ is a trust of node n_i on node n_j at time t , s_k is a set of possible specifications to perform task at n_j where $s_k \in S$, and $TE_{i,j,t}$ is the set of tasks.

Further, the node n_i , the initiator node must store the data about the reliability of node n_j when the packets are transferred repeatedly. The node n_i experience in repeated operation of packet transfer is

$$R_{i,j}^t = (n_j, s_k, P_{i,j,t}) \quad (8)$$

where $P_{i,j,t}$ is satisfaction achieved by node n_i at node n_j at any time t and $P_{i,j,t} \in (0,1)$.

The experience of each particular task will be updated at n_i and represented as

$$I^t(n_j, s_k) = (n_j, w_j) \quad (9)$$

where w_j is the response from n_j in the interaction. By updating the process combinations of I^t and storing the experiences of $T_{i,j}^t$ and $R_{i,j}^t$ we get the quality satisfaction measurements.

The equations (2), (6), and (9) will provide the needed information to trust the node n_i for future transformation of information.

To create trust level we generated random data to test the equation (9). In the test process, 100 random samples were generated for node n_j . If node n_j is trusted more than 90%, we note that the trust level is above threshold. This process was repeated 100 times to reach correct trust level. The process was repeated and the percentage of trust in hundred attempts is shown in Figure 5.

The random generation of trust data is not a correct process but it helps in simulations. The average trust of a hundred samples in Figure 5 is approximately 90.42. The average hundred samples each time is approximately 90.42. The threshold was set as 90 and above and satisfies the simulation results. Therefore, we can assume that if the transfer rate is above 90% the node can be trusted.

 ISBN:978-1-61208-113-7

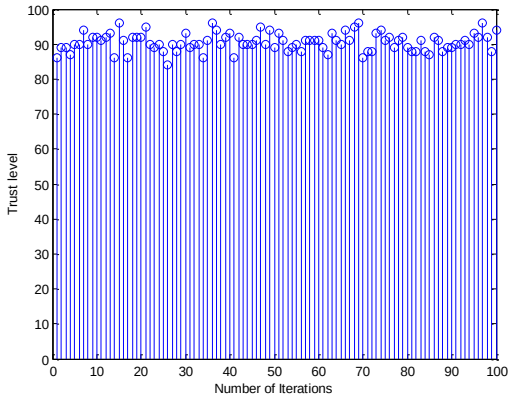

Figure 5. Trust relation generated in 100 iterations

VI. TRUST REPUTATION AND INTERACTING WITH NEIGHBORS

To confirm the trust of the successive node the node interacts with its neighbors. The neighbors of node n_i can be represented as:

$$N_i = \{n_k \mid n_k \in N, then eighbor(n_i, n_k) = true$$

In Figure 1, nodes B and C are neighbors of node A, if the Boolean function value is true. Similarly, the current node A interacts with several of its neighbors to create trusted neighbors and keeps the superior nodes and ignores the inferior nodes. For example, if we denote ζ_i as the inferior neighbor node and ζ_s as the superior neighbor node then their values will vary as $0 \leq \zeta_i \leq \zeta_s \leq 1$. For the stronger neighbor, the relational value must be close to 1. Therefore, the representation of most trusted node is

$$NT^t_{\sup}(n_i, s_k) = \{n_k \mid n_k \in N, \quad if\ trust\ of\ \ n_k \geq threshold \qquad (10)$$

Similarly, the set of nodes with doubtful confidence is given by

$$NT^t_{\inf}(n_i, s_k) = \{n_k \mid n_k \in N, \quad if\ trust\ of\ \ n_k < threshold \qquad (11)$$

The most reputed nodes (established complete trust over time) will be grouped into reliable nodes and represented as

$$NR^t_{\sup}(n_i, s_k) = \{n_k \mid n_k \in N, \quad if\ trust\ of\ \ n_k \geq threshold \qquad (12)$$

The reliable nodes will be used as a reference to verify the trust of successive nodes. If the reliable node is not available, it will verify with a trusted node before it transfers the packets.

The calculation of the threshold value is very important and will be calculated using equation (8). The threshold value will be updated in preset timings by the agent.

VII. CONCLUSIONS AND FUTURE RESEARCH

The current available research models deal with secure transfer of packets, intruder detection, sinkholes, and similar approaches. All these methods need a lot of processing, storage, and energy. There is no literature available for a simple security model for wireless sensor networks that confirms the successive node to transfer the packets. The proposed model is a unique approach to transfer the data securely and at the same time confirms the trust of next level nodes. We are working on the following research ideas that transfer the packets securely from source to destination.

a) What happens if an intruder at successive node level acts as a real node and acknowledges to the preceding node with 100% success of packet transfer and then transfers the packets to the sinkhole?
   - *This problem was solved using the NS2 package by creating a table at the previous node and observing the successive node. The experiment will be useful for detecting the sinkhole. The results will be presented in the next conference.*

b) What happens if the intruder modifies the packets and forwards them to the next level and then these corrupted packets reach the destination?
   - *This is an open problem and will be attempted and solved soon.*

c) What happens if the intruder stores the packet forwarding table appropriately (as the preceding node requires for successful transformation) and never forwards the packets (acts as an intelligent sinkhole).
   - *This problem will be solved with (a) before we publish the results.*

We are working on the above problems by modifying the node level code of the NS 2 package. In the first step, a large size sensor network with 1000 nodes was created and experienced heavy dropping of packets due to overloading at the node. We then minimize the size of the network to 500, 400, 300, 200, and 100 sensor nodes and succeeded partial control of dropping the packets. So, we decided to start with less than 25 nodes for simulations and the packet dropping was controlled. Further, the proposed model is more realistic compared to the previous models in the research [4, 5, 6] and is simple to implement.

ACKNOWLEDGEMENT

The research work was supported by the ONR with award No. N00014-08-1-0856. The first author wishes to express

appreciation to Dr. Connie Walton, Grambling State University and Dr. S. S. Iyengar, LSU Baton Rouge for their continuous support.

REFERENCES

[1] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", MOBICOM 2001, Rome, Italy, June 2001.

[2] Perrig, A., Canetti, R., Tygar, J. D., and Song, D., "Efficient authentication and signing of multicast streams over lossy channels", IEEE Symposium on Security and Privacy, May 2000.

[3] Xiao, B., Yu, B., and Gao, C., "CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks", Journal of Parallel Distributed Computing, Vol 67, 2007.

[4] Tanachaiwiwat, S., Dave, P., Bhindwale, R., and Helmy, A., "Location-centric Isolation of Misbehavior and Trust Routing in Energy-constrained Sensor Networks", IEEE IPCC, October 2004.

[5] Zhang, Y., and Huang, Q., "A Learning-based Adaptive Routing Tree for Wireless Sensor Networks", J. of Communications, 1 (2), 2006.

[6] Ji, Z., Yu, W., and Liu, K. J., "Belief-based Packet Forwarding in Self-organized Mobile Ad Hoc Networks with Noise and Imperfect Observation", IEEE WCNC 2006.

[7] Abreu, D., Dutta, P., and Smith, L., "The Folk Theorem for Repeated Games: A NEU Condition", Econometrica, Vol. 62, 1996.

[8] Yuan, J., and Yu, W., "Distributed cross-layer optimization of wireless sensor networks: a game theoretic approach", Proc. of IEEE Global Telecommunications Conference, 2006.

[9] Yacine R., Vicente E., Mujica V., and Dorgham Sisalem., "A Reputation-Based Trust Mechanism for Ad Hoc Networks", 10th IEEE Symposium on Computers and Communications (ISCC'05), 2005.

[10] Audun J., Roslan I., and Colin B., "A survey of Trust and Reputation Systems for Online Service Provision", Decision Support Systems, 2006.

[11] Mohammad M., and Subhash C., "Trust management in Wireless Sensor Networks", 5th IEEE/ACM international conference on Hardware/software codes and system synthesis, 2007.

[12] Junbeom H., Yoonho L., Seongmin H., and Hyunsoo, Y., "Trust-based secure aggregation in Wireless Sensor Networks", Sensor and Ad Hoc Communications and Networks (SECON '06), 2006.

[13] Fernandez-Gago, M. C., Rodrigo, and R., Javier L., "A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks", 3rd International workshop on Security, Privacy, and Trust in Parvasive and Ubiquitous Computing, July 2007.

[14] Reddy, Y. B., "Potential Game Model to Detect Holes in Sensor Networks", IFIP/NTMS 2009.

[15] Kanno, J., Buchart, J. G., Selmic, R. R., and Phoha, V., "Detecting coverage holes in wireless sensor networks," 17th Mediterranean Conference on Control and Automation, June, 2009.

[16] Mark F., Jean-Pierre H., and Levente B., "Cooperative Packet Forwarding in Multi-Domain Sensor Networks", PERCOM 2005.

[17] Garth V. C., and Niki P., "Evolution of Cooperation in Multi-Class Wireless Sensor Networks", LCN 2007.

[18] Narayanan, S., Mitali S., and Bhaskar K., "Decentralized utility-based sensor network design", Mobile Networks and Applications, June 2006.

[19] Kannan, R., and Iyengar, S.S., "Game-theoretic models for reliable path-length and energy-constrained routing with data aggregation in wireless sensor networks", IEEE J. of selected areas in communications, Aug 2004

[20] Machado, R., and Tekinay, S., " A survey of game-theoretic approaches in wireless sensor networks", Comput. Netw. 52, 16, Nov. 2008.

[21] John, B., and Gabriel, N., "Utility-based decision-making in wireless sensor networks", Proc. of the 1st ACM international symposium on Mobile ad hoc networking & computing, November 20, 2000.

[22] Miller, D.A., Tilak, S., and Fountain, T., "Token equilibria in sensor networks with multiple sponsors", Collaborative Computing: Networking, Applications and Worksharing, 2005.

[23] Zhaoyu L., Anthony W. Joy., and Robert A. T., "A Dynamic Trust Model for Mobile Ad Hoc Networks", IEEE International workshop on Future Trends of Distributed Computing Systems (FTDCS) 2004.

 ISBN:978-1-61208-113-7