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

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

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

***Abstract*—Trust is an important factor in transferring data from the source to destination in wireless sensor networks. If any sensor node fails to transfer the data, the Dynamic Source Protocol calculates the alternate path. Currently, the Dynamic Source Protocol does not have any built-in functionality to calculate an alternate path if the path has a malicious node. Intruder detection system can detect the malicious node. 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 detect the abnormal behavior nodes. The proposed model uses the repeated games to detect faulty (malicious) nodes through the cooperative effort in the sensor network and judges the trust of successive nodes. Further, the research includes the trust model with reliable neighbors and query-based trust calculation. 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 transfer of data.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are used to collect important data in sensitive areas including military surveillance, fire monitoring dangerous forests, and hazardous places including biological and chemical areas [42-46]. Secure communication is required for these applications, since sensors are deployed massively and unorganized way [1-6]. Due to the unorganized massive deployment, the black holes are common and malicious nodes will be created through hackers. Most of the times, eliminating the malicious nodes or further deployment of sensors at sink holes is very difficult [37].

WSNs are used in different applications including Structural Health Monitoring (SHM), Industrial Automation (IA), Civil Structure Monitoring (CSM), Military Surveillance (MS), and monitoring the Biologically Hazardous Places (BHP) [47-52]. 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. Due to the WSN topology, injecting bad nodes is not difficult. Therefore, there is a need to create a secure transmission model with minimum overheads and transmit the data securely.

Design of secure communication model with minimum overheads is very difficult [53]. The information security models (Intruder Detection System (IDS) and cryptography techniques) for wireless communications are not suitable to WSNs due to resource (processing and memory) limitations. Further the WSNs topology changes dynamically due to failure of nodes and the distance between the nodes is limited. Due to limited distance, frequent failure of nodes, and possible injection of malicious nodes, the trust of successive nodes and cooperation of neighboring nodes is very important.

The trust depends upon the predictable behavior of successive nodes [1]. The Dynamic Source Protocol (DSR) cannot detect the malicious node, and the IDS package has overheads as well as more false alarms [54]. 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. Trust means transfer the packets above expected percentage (for example more than 95%). The trust level is calculated as the difference of packets received to transfer of packets by that node.

The trust depends upon the predictable behavior of nodes within communication distance with their continuous positive behavior. The trust is the degree of belief, which is based upon the continuous or repeated experience. Trust is non-transferable, reputation-based, time dependent, subjective, contextual, and unidirectional. Due to the nature of the trust, researchers are recently diverted towards these simple models (trust base models).

Since trust depends upon the closeness, the successive and neighboring nodes are included in the trust model. The successive node in the path is to communicate the data and the neighboring nodes (cooperation) are useful to confirm the trust factor, if the trust of successive node in the path is below the threshold (below the dependable value).

Trust-based packet transfer uses the Belief-Based Packet Transfer (BBPT) [7]. The BBPT uses the history of the other nodes transferring the data through its successive node. The BBPT requires the cooperation of its neighbors. The BBPT works better with agent-based systems, where

the agent collects the history of nodes, sets the neighborhood, and processes the data.

The rest of the paper introduces the related work, trust management, repeated games to model the trust level of successive nodes, and formulates the trust-based model in a cooperative environment. The paper further discusses the trust based packet forwarding, trust interaction with neighbor nodes, query-based trust calculation, conclusions, and the future research.

II. Related Work

Trust management is not a new concept in the electronic market. Reputation and trust are the basics of product sales. Establishing trust on a product manufacture industry and reputation of a product is the source of sales. Similarly, establishing trust on a node transferring the packets and reputation of the node is very important to keep the sensor node on data transfer path. In recent applications, trust calculation and update the node ratings uses reputation-based trust calculation [37], [40], event-based trust management [39], and agent-based trust management [30-32]. Further, repeated games help to detect the trustworthiness of a node in the path [37].

The sinkhole detection, selective forwarding attacks, acknowledgement spoofing, detection of malicious node, and utility-based decision making were discussed in [3], [5], [8], [9], [12], [13], [15], [16], [17], [21], [22]. None of these results 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 a node (communication path or battery loss or complete node failure) or a node compromises. The research of selective forward attacks and detection of malicious nodes provides an extra effort if the data does not reach the destination. A trusted path is needed at the time of transferring the data (packets).

Perrig et al. [17] introduced the modified TESLA protocol [16] 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. 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) [22] 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 [21]. 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 [21] discussed various search methods to detect the insecure locations and isolate those locations from communication paths.

Zhang and Huang [24] used reinforcement learning to establish a secure path for packet transfer from source to the base-station. They concluded that adaptive spanning trees could 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.

The trust management in wireless sensor networks was discussed by Carmen et al. [4]. A trust management system helps to detect the node (faulty or malicious) behaving in an unexpected way. Liu et al. [10] presented a dynamic trust model for ad-hoc networks, where each node is 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. [19] 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. Probst and Kasera [18] developed a distributed, statistical method for reputation-based trust in sensor networks. The method computes statistical trust based on sensor nodes behavior in terms of experiences in order to isolates faulty sensor nodes.

The belief-based packet-forwarding model in mobile networks using repeated games was discussed in [7]. The authors described the belief-based packet-forwarding model as being dependent upon history of other nodes' information transfer. The model further enforces cooperation in the ad hoc networks. The performance of packet transfer slightly degrades due to enforcing the cooperation of nodes compared to unconditionally cooperative outcomes. The model further provides the ad hoc networks and needs to modify for WSNs.

In this research, role of repeated games to detect the malicious or faulty node through a cooperative effort is discussed. The trust relation model and simulations were presented. Further, we discussed the trust model with reliable neighbors and query-based trust model.

III. Trust Management

Trust is used differently in different fields. A person is trustworthy, if he/she is dependable and reliable. That is, if a person completes the work on time, with satisfaction then we say the person is trust worthy. Trust depends upon the satisfaction of completing work repeatedly and as expected. The concept is used in credit cards, bank loans, and work places. Different procedures are used at different places. Sensor networks do not deviate much from the original concept.

The conceptual differences between trust, security, and reputation were explained in [29]. Further, the authors explained the WSNs security issues and innovative approaches. The authors suggested the future researchers may use these approaches to model the trust in respective fields. The suggestions conclude that the research needs to divert to create innovative approaches for trust-based WSNs.

Task-based trust management, event-based trust management and an agent-based trust management were studied in [30-34]. In [30], a general approach for task-based trust management is used similar to economics to detect the malicious node. The event-based approach [31] uses several trust ratings to enforce the security in WSN. The agent-based trust models in [31-34] discuss the attacks on WSN, packet dropping, and local storage management using the trust policy. The models can further discusses the trust aggregation, Hello flood attack, and detect the malicious nodes.

Hur et al. [35] presented a trust-based approach to distinguish illegal nodes from legal nodes. They claim that their approach detects insider attacks and uses trust evaluation model. The trust management model in [36] uses the Bayesian probabilistic approach. The model calculates the trust factor by using the current trust factor plus the second hand information received from its neighboring nodes.

Trust is a subjective term used for reliability of an entity. It is a subjective probability of an individual A that 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 [4], [6], [14], [19]. The concept of reputation (collecting data about the status of a successive node) linked to the trustworthiness [2] of a person's example. 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 of nodes is dangerous. Therefore, collaborating between neighboring nodes is suggested.

The data transfer scenario from node A through the node D (Figure 1) establishes the trust of node D for future data transfers. 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 successive node in the communication path. If the node A knows that node D transferred the data successfully, then the node A assumes that the 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 the node C that are transferring their data through node D. If nodes B and C trust the node D, then node A establish 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.

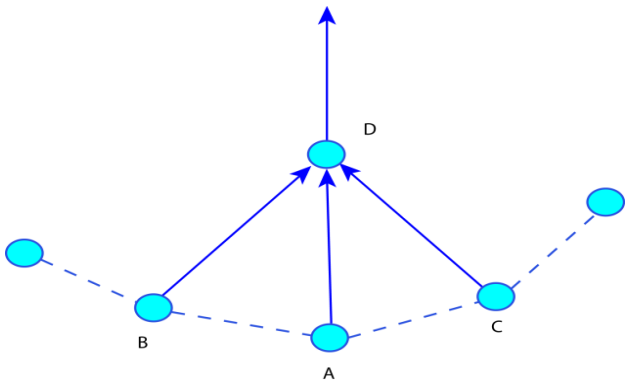

Figure 1: Scenario for node *A* establishing a trust of node *D*.

In the proposed approach, each node maintains a rating of its successive node (number of successful packet transfers) in the path. If the ratings of a node are above the threshold (expected 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 [17]. Selecting the highest rating path requires additional processing time and is a burden on the energy budget in the sensor node. The proposed approach detects the malicious node using the trust factor. For example, if node D 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. Since the communication path from node A to the node D is not trusted, node A establishes the alternative path. The alternate path is selected only if the successive node is not trusted.

IV. GAME MODEL

In games [11][23], the interaction between the players is inherently dynamic, so players always observe the actions of other players and decide their optimal response. Often, the game is played repeatedly to conclude the outcome. 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; i.e., Player 3 and Player 4 (node B and node C in Figure 1) and have the similar interaction with Player 2. If Player 3 and Player 4 have same outcomes as Player 1 that is no better than Player 1, then the Player 1 concludes its decision to select communication path. If the trust of Player 1 on Player 2 depends upon the outcomes of its neighbor nodes and consistent, then we say it reaches 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

$$G = (N, A, U) \tag{1}$$

where N is a set of users (set of sensor nodes), A is a set of pure strategy profiles (action may be the missing packets for each transmission), and U is a vector of payoffs.

A simple stage game is defined with two players. If the two players n_1 and n_2, $(n_1, n_2 \in N)$, played with set of strategies $a_i, a_j (a_i, a_j \in A)$ in time unit t_i. In a repeated game, a player n_i plays with strategy a_i in time unit t_i to generate payoff u_i, $(u_i \in U)$. Let τ be the missing number of packets in a time period $T(t_1, t_2, \ldots, t_n)$. The number of missing packets in a unit time is τ / T.

The payoff β at node *D* in a period *T* is given by [7]

$$\beta = \frac{1 - \tau / T}{1 - (\tau / T)^{T+1}} \tag{2a}$$

Equation (2a) represents the normalized payoff. If $\beta > threshold$ then the player is trustworthy. Figure 2a is drawn for the dropping of packets at different time period. The Figure 2a shows that, the payoff is better if the packet dropping slot is in a larger time period. Consider an example with the threshold value is fixed at 95%. Figure 2a concludes that the larger time periods are suggested for better payoff (Figure 2a). The same may not be true in a smaller time period for the current random data. Therefore, the time period is very important to calculate the trust of a node. If we consider the smaller time periods, then the trust value must be kept at a lower rate.

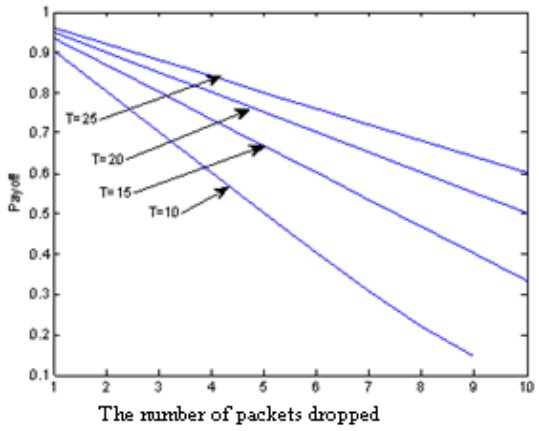

Figure 2a: Variation of time units and packet dropping

The payoff can also be calculated using a different method. 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 $(a^0, a^1, \ldots . a^T)$ at any node is given by [11]

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

The trust of the player depends upon the outcome of β. Figure 2b is drawn using Equation 2b.

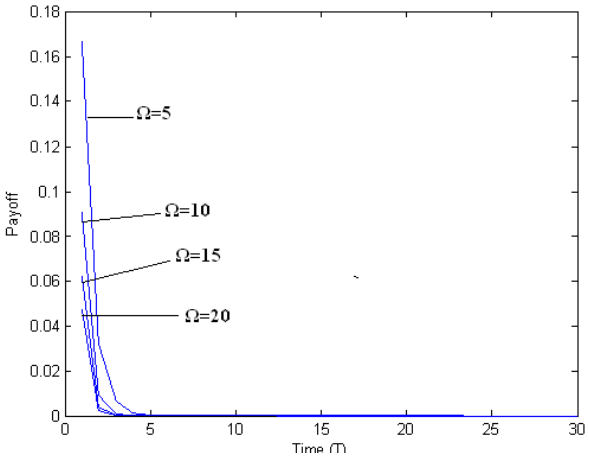

Figure 2b: Payoff β verses packet dropping in a given time period.

The Figure 2b 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.

From Figures 2a and 2b, we conclude that larger periods must be considered to calculate the trust of a node. The smaller periods will panic the system, since small number of packet dropping will show the trust below the threshold.

V. TRUST MODEL AND GAME APPLICATION

Each node in the sensor network maintains a dynamic table to store the information about packet transfers 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 calculations 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 [20].

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 (black-hole).

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

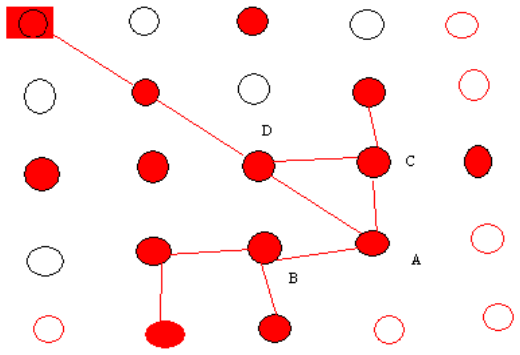

Figure 3: Sensor network nodes and their relation with neighboring nodes.

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 overhearing 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 is 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 nodes. The indirect observations are represented as $IQ_{i,j}$. The trust prediction of the node j depends upon $Q_{i,j}$ 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 $\lambda = 0$ then the packets transferred at a node and its neighboring node are the same. The trust of the node depends upon the factor β. Further we calculate the average discount factor in order to calculate the stable state of the node. The average discount payoff is given by

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

If the average discount payoff is above the threshold then node is trustworthy. If the trust state is consistent, then we say it reaches Nash equilibrium. If the Nash equilibrium exists in repeated games, then it satisfies the Folk theorem [1] and Pareto optimality (payoff in Nash equilibrium). The simulations for average discount payoff are shown in Figure 4a and Figure 4b.

Figure 4a shows the number of packets transmitted to average discount payoff. The system stabilizes after transmission reaches 1500 and above. The trust calculation in large time periods and packets transfer provides the stable results. In Figure 4b, average discount payoff is better in larger period of time.

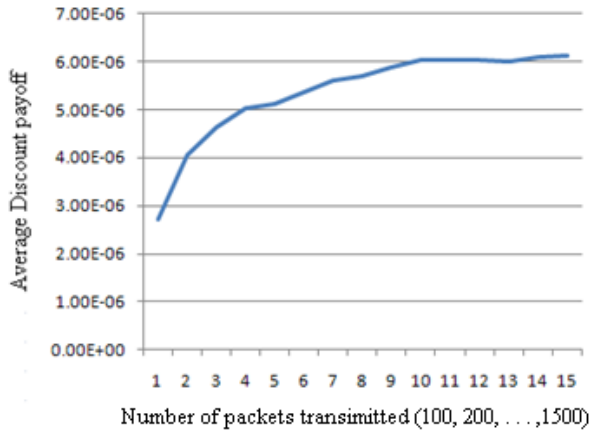

Figure 4a: Average discount payoff verses number of packets dropped

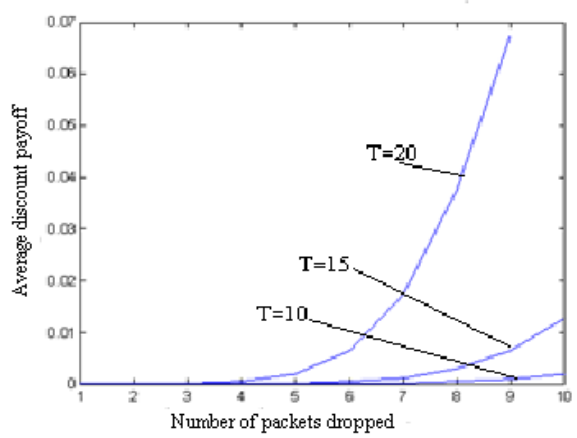

Figure 4b: Average discount payoff verses number of packets dropped

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 transmitted packets is numbered in small or many. In the beginning, the average discount payof increases (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.

VI. 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

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

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

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

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

$$I^{t}(n_j, s_k) = (n_j, w_j) \tag{9}$$

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^t and R^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.

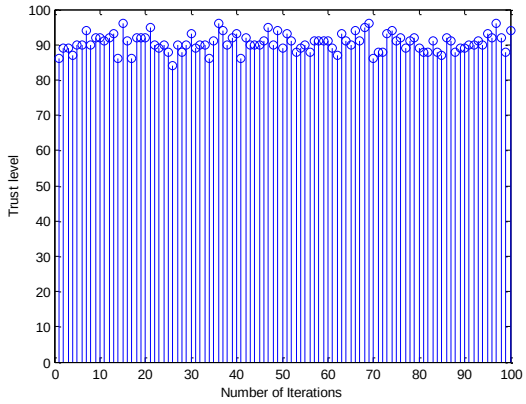

Figure 5: Trust relation generated in 100 iterations.

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 of hundred samples 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.

VII. Trust Model With Reliable Neighbors

The nodes within the communication distance are the neighbors of the node. The neighbor nodes confirm the trust of common successive node. For example, node B and node C are the neighbors of node A (Figure 1). The neighbors of the node n_i can be represented as:

$$N_i = (n_j \mid n_k \in N), \; if \; (n_i, n_k) = true \tag{10}$$

To confirm the neighbor nodes, we use the Boolean function in equation (10). If the Boolean function value is true in equation (10), the nodes are neighbors. Identify trusted neighbors and keeps the superior nodes (trustable nodes) and ignores the inferior nodes, the node A interacts with several of its neighbors (node B and node C). For example, if we denote ζ_i as the inferior neighbor node and ζ_s as the superior neighbor node then their values will be represented as $0 \le \zeta_i \le \zeta_s \le 1$. If ζ_s is close to 1 then the neighbor will be identified as superior. Therefore, the most trusted node is

Therefore, the representation of most trusted node is

$$NT^t_{\sup}(n_i, s_k) = \{n_k \mid n_k \in N\}, \; if \; trust \; of \; n_k \ge threshold \tag{11}$$

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

$$NT^t_{\inf}(n_i, s_k) = \{n_k \mid n_k \in N\}, \; if \; trust \; of \; n_k < threshold \tag{12}$$

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

$$NR^t_{\inf}(n_i, s_k) = \{n_k \mid n_k \in N\}, \; if \; trust \; of \; n_k < threshold \tag{13}$$

The reliable nodes are useful to verify the trust of successive nodes. If the reliable node is not available, it will verify trust of a successive node based on reputation values or node ratings (economic market place) done using economics models [39, 27].

The calculation of the threshold value is very important and will be calculated using equation (8). The agent updates the threshold value in preset time instances.

VIII. Query-based Direct Trust Calculation

The query-based approach is useful to establish the communication path from source nodes to the base station. The query system helps to infer the future status of the trusted communication path. Further, the information obtained through query system will predict the future actions of the nodes in the path.

The performance of node n_j over the (change of) time t depends upon the successful transfer of packets that were received from the node n_i. The reliability of a node n_j is the trust measure associated with the task (packet transfer). Sabater and Sierra [25] stated that the outcome of the reputation measure of node n_i depends upon delivery time, quality, and percent of transfers. Using these factors the trust (T) of the node n_i to the node n_j is

$$T = f(O, \pi, t, R) \tag{14}$$

where O is the outcome, π is variable outcome to be judged, t is recorded time, and R is rating $R \in \{-1, 1\}$. The value -1 is absolutely negative and 1 is positive. Since R is the ratings at time t of outcome π of a task, the equation (14) must satisfy the equation (7). The reliability value is obtained from the number of experiences used to calculate the trust and variability of these ratings experiences.

Using repeated game model, the outcome of node n_j with imperfect history of packet forwarding and dropping is calculated as

$$U_j(\delta) = (1-\delta)\sum_{t=0}^{n} \delta^t u_j^t(a_j^t) \quad (15)$$

where the discount factor $\delta \in (0,1)$, a_j^t is the action part of j^{th} node at time *t*, and u_j^t is expected payoff profile. Folk's theorem for repeated games [1] asserts that there exists $\bar{\delta}$ such that $0 < \bar{\delta} < 1$ will be enforced based on the information shared by the players. Therefore, we rewrite the equation (15) using the Fork's theorem as:

$$U_j(\bar{\delta}) = (1-\bar{\delta})\sum_{t=0}^{n} \bar{\delta}^t u_j^t(a_j^t) \quad (16)$$

The Folk's theorem further assumes that the players share the common information about each other's actions. The strategy can be extended to inference of the other player's future actions. That is, depending upon the current information of successive player, the current player can infer the next (future) actions of successive player. Using this information, the player can decide to recalculate the communication path.

The player n_i shares the common information from other players (Folk's theorem) and the rating of the node n_j will be calculated using Automatic Collaborating Filtering (ACF) [26]. The ACF uses the mean squared difference formula [26] with two users. Let the performance of node n_j is rated by nodes *G* and *H*. Let G_f and H_f denote the ratings of *G* and *H* on a feature (packet transfer) *f* of the node n_j. Let χ be the set of features of the node n_j. Both *G* and *H* are rated the node n_j and $f \in \chi$. The difference between two nodes *G* and *H* in terms of their interests in a node n_j is given by [9]:

$$\Delta = \delta_{U,j} = \frac{1}{|\chi|}\sum_{f \in S}\left(G_f - H_f\right)^2 \quad (16)$$

If Δ is very small, the ratings provided by neighboring nodes are helpful for decision. Otherwise, the node n_i need to collect more facts from other neighbors before any further decision to be made.

There are two types of ACF recommendations: invasive and noninvasive based on the user preferences [27], [28]. The invasive approach uses explicit user feedback having the preferences between 0 and 1. The preferences are interactive and Boolean in noninvasive approach. In the noninvasive approach, the rating 0 means the user not rated and the rating 1 means the user rated. Therefore in noninvasive cases, it requires more data for any decision. In ACF systems, all user recommendations will be taken into account even though they are entered at different times. The ACF system gets more strength with more recommendations and new recommendations depend upon the current data updates in the system.

IX. Conclusion and Future Research

The available security models for packet transfer in wireless networks are useful for intruder detection, sinkholes, and black holes. 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 confirm the trusted 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 node.

The paper discusses the trust models and trust-based approach in sensor net works. The role of repeated game in trust models was introduced and calculated the average discount payoff verses number of packets dropped. The model identifies that large time slots provide better results than observing the packet dropping in a short period of time.

Further, the model for trust relation among the nodes was presented and prediction of a trusted node in the path was discussed using game model and Automatic collaborative filtering approach. The models presented are useful to transfer the data with minimum overheads.

The future research includes the rating of a successive node using electronic marketplace model [39] to calculate the trusted path. Further, the trusted successive node will be calculated using an agent with a set of nodes (cluster). The cluster-based approach saves the energy at the node level, since calculations are done at agent node. Further, an event-based [38] approach with electronic marketplace concept can be developed depending upon the situation of sensor networks. The mixed approaches are suggested depending upon the topology of sensor networks and type of environment.

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] Y. B. Reddy and Rastko Selmic., "Secure Packet Transfer in Wireless Sensor Networks – A Trust-based Approach", IARIA- ICN 2011, January 23-28, 2011 - St. Maarten.

[2] Audun, J., Ismail, R., and Boyd, C., "A survey of Trust and Reputation Systems for Online Service Provision", *Decision Support Systems*, 2006.

[3] Byers, J., and Nasser, G., "Utility-based decision-making in wireless sensor networks", *Proc. of the 1st ACM International Symposium on Mobile Ad Hoc Networking and Computing*, November 2000, Boston, Massachusetts.

[4] Fernandez-Gago, M., Roman, R., Lopaz, J., "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.

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

[6] Hur, J., Lee, Y., Hong, S., and Yoon, H., "Trust-based secure aggregation in Wireless Sensor Networks", *Sensor and Ad Hoc Communications and Networks (SECON '06)*, 2006.

[7] 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.

[8] 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.

[9] 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.

[10] Liu, Z., Joy, A., and Thomson, R., "A Dynamic Trust Model for Mobile Ad Hoc Networks", *IEEE International workshop on Future Trends of Distributed Computing Systems (FTDCS)*, 2004.

[11] Machado, R. and Tekinay, S., "A survey of game-theoretic approaches in wireless sensor networks", *Computer Networks*, Nov. 2008.

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

[13] Miler, D., Tilak, S., Fountain, T., "Token equilibria in sensor networks with multiple sponsors", *CollaborateCom* 2005.

[14] Momani, M., and Challa, S., "Trust management in Wireless Sensor Networks", *5th IEEE/ACM International Conference on Hardware/Software Codes and System Synthesis*, 2007.

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

[16] 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.

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

[18] Probst, M.J., and Kasera, S.K., "Statistical trust establishment in wireless sensor networks," *Proc. ICPADS '07 the 13th International Conference on Parallel and Distributed Systems*, 2007.

[19] Rebahi, Y., Mujica, V., and Sisalem, D., "A Reputation-Based Trust Mechanism for Ad Hoc Networks", *the 10th IEEE Symposium on Computers and Communications (ISCC'05)*, 2005.

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

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

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

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

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

[25] Sabater, J., and Sierra, C., REGRET: A Reputation Model for Gregarious Societies, *First Int. conf. on Autonomous Agents and Multi-agent Systems*, 2002.

[26] Cunningham, P., Intelligent Support for E-commerce, http://www.cs.tcd.ie/Padraig.Cunningham/iccbr99-ec.pdf, 1999

[27] Hays, C., Cunningham, P., and Smyth, B., A Case-based Reasoning View of Automated Collaborative Filtering, *4th International Conference on Case-Based Reasoning*, 2001.

[28] Sollenborn, M., and Funk, P., Category-Based Filtering and User Stereotype Cases to Reduce the Latency Problem in Recommender Systems, 6th European Conference on Case Based Reasoning, *Springer Lecture Notes*, 2002.

[29] Momani, M., and Challa, S., "Survey of trust models in different network domains", *Int. J. of Ad hoc sensor & Ubiquitous Computing (IJASUC)*, vol. 1, no. 3, September 2010.

[30] Chen, H., Wu, H., Hu, J., and Gao, C., "Agent-based Trust Management Model for Wireless Sensor Networks", *International Conference on Multimedia and Ubiquitous Engineering*, 2008.

[31] Chen, H., Wu, H., Hu, J., and Gao, C., "Agent-based Trust Model in Wireless Sensor Networks," *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2007.

[32] Boukerche, A., and Li, X., "An Agent-based Trust and Reputation Management Scheme for Wireless Sensor Networks", *IEEE GLOBECOMM, 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)*, pp 66-77, October 2004.

[33] Marmol, F. G., and Perez, G. M., "Providing Trust in Wireless Sensor Networks using a Bio-Inspired Technique", *NAEC 2008*.

[34] Haiguang Chen, Huafeng Wu, Xi Zhou, Chuanshan Gao, "Agent-based Trust Model in Wireless Sensor Networks", *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2007.

[35] Hur, J., Lee, Y., Hong, S., and Yoon, H., "Trust-based Secure Aggregation in Wireless Sensor Networks", SECON 2006.

[36] Momani, M., and Challa, S., "Trust Management in Wireless Sensor Networks", *3rd International Conference on Intelligent Sensors, Sensor Networks and Information, 2007*.

[37] Y. B. Reddy and Rastko Selmic., "Trust-based Packet Transfer in Wireless Sensor Networks", *Communications and Information Security (CIS2010), IASTED*, Nov 8-10, 2010,USA.

[38] Chen, H., Wu, H., Hu, J., and Gao, C., "Event-based Trust Framework Model in Wireless Sensor Networks", *International Conference on Networking, Architecture, and Storage*, 2008.

[39] Zacharia, G., Moukas, A, and Mae, P., "Collaborative Reputation Mechanisms for Electronic Marketplaces", *Decision Support Systems*, vol. 29, no. 4, December 2000.

[40] Ganeriwal, S., and Srivastava, M. B., "Reputation-based Framework for High Integrity Sensor Networks", *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)*, 2004.

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

[42] Akyildiz, I.F., Weilian Su, Sankarasubramaniam, Y., and Cayirci, E., "A survey on sensor networks", *IEEE Communications Magazine*, Aug. 2002.

[43] Rentala, P., Musunnuri, R., Gandham, S., and Saxena, U., "Survey on Sensor Networks", *Technical report*, University of Texas at Dallas, 2000.

[44] Papageorgiou, P., "Literature Survey on Wireless Sensor Networks", *Technical Report*, University of Texas, Dallas, July 16, 2003.

[45] Bharathidasan, A., and Ponduru, V., "Sensor Networks: An Overview", *Technical report, University of California*, Davis, 2000

[46] Tilak, S., Abu-Ghazaleh, N. B., and Heinzelman, W., "A Taxonomy of Wireless Micro-Sensor Network Models", *ACM SIGMOBILE Mobile Computing and Communications Review*, April 2002.

[47] Goldsmith, A.J., and Wicker, S. B., "Design challenges for energy-constrained ad hoc wireless networks", *IEEE Wireless Communications*, Aug. 2002.

[48] Stark, W., Hua Wang, Worthen, A., Lafortune, S., and Teneketzis, D., "Low-energy wireless communication network design", *IEEE Wireless Communications*, Aug. 2002.

[49] Tilak, S., Abu-Ghazaleh, N. B., and Heinzelman, W., "Infrastructure tradeoffs for sensor networks", *ACM International Workshop on Wireless Sensor Networks and Applications*, 2002.

[50] Chien-Chung Shen, Srisathapornphat, C., and Jaikaeo, C., "Sensor information networking architecture and applications", *IEEE Personal Communications*, Aug. 2001.

[51] Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., and Pister, K., "System architecture directions for networked sensors", *ACM ASPLOS*, 2000.

[52] Da Silva Jr, J. L., Shamberger, J., Ammer, M.J., Guo, C., Li, S., Shah, R., Tuan, T., Sheets, M., Rabaey,J. M., Nikolic, B., Sangiovanni-Vincentelli, A., and Wright, P., "Design methodology for PicoRadio networks", *Proceedings of Design, Automation and Test in Europe*, 2001.

[53] Shenker, S., "Fundamental Design Issues for the Future Internet", *IEEE Journal on Selected Areas in Communications*, Sep. 1995.

[54] Reddy, Y. B., Durand, J., and Sanjeev Kafle, S., "Detection of Packet Dropping in Wireless Sensor Networks", *7th International Conference on Information Technology: New Generations*, 2010.