# Agent-based Trust Calculation in Wireless Sensor Networks

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* - Cooperation in wireless sensor networks to detect the malicious node without any infrastructure is a recent trend in research. The current models need more storage, computation, security tools, and communication requirements. They fail in wireless sensor networks due to limitation of resources. Trust-based approach does not need high-end resource requirement. The proposed agent-based approach eliminates the computations in the sensor nodes with appropriate trust factor. The proposed approach uses an agent-based collaborative concept to ensure the trust in the successive node in the path. The proposed agent-based framework uses reputation of neighboring nodes as part of trust calculation in its successive node. The simulations were presented to calculate the trust of a node.**

***Keywords: agent-based approach, packet transfer, wireless sensor networks, protocols, trust-based approach, resource.***

## I. INTRODUCTION

Sensors are small in size, limited computational power, and capabilities. Wireless sensor networks are based on these small form-factor nodes transmitting the collected information to the base station. Since safe transmission of information is important, the path of transmission must be trustworthy. Therefore, each node must trust the successive node in the path. If any node in the path is suspicious, the decision node must calculate the alternative path.

There are varieties of methods to calculate the trust of a successive node. The methods include the reputation-based trust management, event-based trust management, collaborative trust management, and agent-based trust management. In reputation-based trust management, the node stores the number of packets transfer from the node and calculate the success rate of packets transferred from its successive node. In the event-based trust management system, the trust rate is calculated at particular or specific time events or periodically. In collaborative models, the business models are used to calculate the trust similar to product trust management. In agent-based trust management systems, an agent node is introduced to store the packet transfer information from a cluster of nodes within communication distance. The agent-based systems relieve the most of the processing time of nodes and the nodes concentrate on transfer of information. Trust-based systems will help to detect the malicious nodes and eliminate them from the communication path.

A trusted node must transmit the minimum acceptable number of packets. The minimum acceptable number is called threshold. The threshold is used to rate the node. The ratings will be updated and maintained using Sporas formula [7] or Molina's fuzzy reputation model [5] or proposed agent-based model. The proposed model reduces the overheads on sensor nodes and helps to improve the life time expectancy and efficiency.

Figure 1 show the WSN with nodes, neighbor nodes, and an agent to collect and process trust information. The agent's responsibility is to collect the node ratings update the trust of each node within communication distance of successive node in the path. The agent also provides the level of trust and recommends alternative path if the trust is below the threshold value.

The remaining part of the paper discusses the related work, reputation based trust, agent-based trust calculation. The reputation based trust model uses Sporas formula and Molina's fuzzy model and comparison of these models to update the rates. Finally, the paper presents concluding remarks and 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. Trust calculation and update the node ratings uses reputation-based trust calculation [1, 4], event-based trust management [3], and agent-based trust management [7-9]. Repeated games help to detect the trustworthiness of a node in the path [1].

Ganeriwal et al. [2] discussed the reputation-based framework for high integrity sensor networks. The model

 ISBN: 978-1-61208-144-1 

evaluates the trustworthiness of the nodes and various type of misbehavior of nodes in the network. The model uses the Bayesian formulation and updates the trust with direct and indirect trust calculations.

Trust is not consistent. It varies from time to time and event to event. In sensor networks, a series of events happens. Data collection, data routing, location report, identifying neighbor, reorganizing the network, and time synchronization are very common. In event-based systems [2], the behavior of sensors and collection of trust rating from neighbor nodes is done through agents. The agent decides the trustworthiness of sensor and path reestablishment.

The agent-based system [7-9] uses various methods of sensor node ratings and calculation of trust of nodes. In agent-based models, an agent is created with a set of nodes within the communication distance. The agent is responsible to calculate the trust and reputation of the nodes using various formulas.

Collaborative reputation in an electronic market [3] uses the Sporas formula to calculate the ratings of a node on Web. The ratings will conclude the trust in WSN. Bio-inspired technique based on ant colony system. The most worthy path is detected by using the pheromone traces deposited by ants.

Momani et al. [10] proposed the secure data aggregation scheme to detect the inside attack (within networks) and trustworthiness of a node in the WSN. Further, trust establishment in ad hoc network using distributed environment was studied in [12].

*Contribution*: Trust ratings with Sporas formula and fuzzy reputations of Molina's formula were derived and compared. The two methods used to calculate the trust of a node. It is concluded that the learning rate and most recent trust rate helps in detecting the malicious node quickly. Further, the agent in each cluster minimizes the computational overhead of the nodes. The simulations were presented to illustrate the theoretical analysis.

## III. TRUST AND REPUTATION

The reputation-based models use the rate of a number of packets received to transfer by a node [1]. The event-based models calculate the trust on the rate of transfer of packets at any particular event [2]. Further, business (collaborative) models are used to calculate the trust of a node depending upon the rating by neighboring nodes [3]. All models were used to calculate the trust and detect the malicious node, so that they can avoid the malicious node from the data transfer path. These calculations show that trust is calculated on the behavior of a node in the data transfer path.

Molina et al. used the fuzzy reputation to calculate the trust of a node [5, 6]. The trust depends upon the reputation of a node $R_{i-1}$ at the time $i-1$, current rating $C_i$ and remembrance weight $\omega$. The maximum value of remembrance is 1. Therefore, $0 \le \omega \le 1$. The current reputation is calculated as [5]:

$$R_i = \frac{R_{i-1}.\omega + C_i.(2-\omega)}{2} \quad (1)$$

If $\omega = 0$ then $R_i = C_i$. If the node does not remember the previous reputation, then current rating is the reputation value. It shows that a new node entering into network does not have previous value. If $\omega = 1$ then the new reputation is equal to average of previous reputation and current rating. The maximum value of $\omega$ provides the excellent reputation and more trustworthy. Therefore, the equation (1) becomes

$$R_i = \frac{R_{i-1} + C_i.}{2} \quad (2)$$

The equation (2) shows that if a node is added with the best possible rating, it should not be given more than half of reputation. The reputation must be established.

The reputation of a node is updated with current ratings. The current ratings are obtained using the following Sporas formula [7].

$$R_i = R_{i-1} + \frac{1}{\theta}\phi(R_{i-1})(C_i - R_{i-1}) \quad (3)$$

$$\phi(R_{i-1}) = 1 - \frac{1}{1 + e^{-(R_{i-1}-D)/\sigma}} \quad (4)$$

where:

$\theta$ - effective number of ratings taken into account ($\theta > 1$). The change in rating should not be very large.

$\phi$ - helps to slow down the incremental change

$C_i$ - represents the rating given by the node $i$

$D$ - range or maximum reputation value

$\sigma$ - the acceleration factor to keep the $\phi$ above certain value (> threshold).

 ISBN: 978-1-61208-144-1 

If the node compromises, the rating will be smaller and $(C_i - R_{i-1})$ become negative. Therefore the current reputation slowly crosses below threshold and node declared as malicious.

The equations (1) and (3) calculate the new reputation of a node. Substituting equation (1) in (3), we obtain.

$$\frac{R_{i-1}.\omega + C_i.(2-\omega)}{2} = R_{i-1} + \frac{1}{\theta}\phi(R_{i-1})(C_i - R_{i-1}) \quad (5)$$

Assume the remembrance weight $\omega$ =1 or $\omega$ =0 the equation (5) simplifies

$$C_i = R_{i-1} \quad (6)$$

The equation (6) shows that if the remembrance $\omega$ =1 or $\omega$ =0 the ratings given by a node $i$ is equal to reputation of the node. That is, a long term excellent reputation node and recent added good node assumes to be trustworthy.

Further, in equation (1), if the remembrance $\omega$ =1, then current reputation is average of previous reputation and current ratings. Figure 2a shows the relation between reputation of a node and current reputation. In normal conditions, the current reputation is proportional to previous reputation.

Figure 2b is drawn for the remembering weights $\omega = 0,\ 0.7,\ 1.0$. Once the system get updated continuously, the node rate constantly increases (stabilizes). If the reputation is random (reputation may be low or high) and ratings are increasing or decreasing, the node is not trustworthy. The node drops the packets randomly. The Figure 2c and Figure 2d shows that if the nodes are dropping packets randomly, the increasing reputation is better than decreasing reputation.

In the agent based systems, it is recommended to use the Sporas formula to update the ratings, so that the fuzzy reputation formula of equation (1) provides better results. The reliability of the nodes in WSN is temporary. The continuous update of ratings is required in the WSN.

## IV. AGENT-BASED APPROACH

Agent-based trust approach is similar to cluster-based approach or watchdog approach [5, 7, 9]. The cluster forms with the nodes that are within communicating distance. Each cluster has an agent to collect the reputation of nodes. The reputation of a node includes two factors.

- Trust of each node in the cluster transmitting the packets through same node and must be within communicating distance.
- Trust of a node (constant and less than 1) to its neighboring node(s).

The agent keeps the above information of each node within communicating distance and calculates the trust of a node in the transmitting path. The trust value decides the trust of node in the communication path. Therefore, the trust depends upon the direct observations of a node plus the indirect observations received from its neighboring nodes. The reputation of a node is calculated in two ways.

**Case 1:** From the Figure 1, the reputation of a node D at node A is a sum of the observations of node A, node C with respect node A, and node B with respect to node A. The reputation of node D at node A is given by

$$R_{A,D} = \alpha.R_{A,D} + \beta.R_{C,D} + \gamma.R_{B,D} \quad (7)$$

and $$\alpha + \beta + \gamma = 1 \quad (8)$$

where

$R_{A,D}$ reputation of node D at node A

$R_{C,D}$ reputation of node D at node C

$R_{B,D}$ reputation of node D at node B

The nodes C and B are neighbors of node A. The direct reputations are at decision node and indirect reputations are from its neighboring nodes. Initially, the constant factor at decision node carries higher value than other nodes. The values of $\beta$ and $\gamma$ are based on the trust of node A with respect to nodes C and B. Figure 3a shows that the higher value of alpha lower the confidence of a node that was put in trust test. If the value of $\beta$ and $\gamma$ are larger, then the indirect observations provide better results. That is, the neighbor nodes receive more confidence on the successive node with respective to the testing node (node A is a testing node in the current case).

Therefore, it is better to adjust the alpha value at lower level (<0.5). Figure 3b shows the collaborative trust calculation at Node A as trust value decreases. Collaborative effort helps and confirms the trust status. In the current problem (Figure 3a and 3b), it is clearly shown that, the node A to D has communication problem and D is not a malicious node. Furthermore, node A can confirm from node B and node C the confidence or reputation of

 ISBN: 978-1-61208-144-1 

node D using their original trust values which are stored at the agent.

In agent-based systems, the agent has the trust and reputation values of all nodes. The agent also has the level of belief on its neighbors. The level of belief is the multiplication factor ( $\beta$ or $\gamma$ ) that helps to calculate its belief factor on a specific node. The trust at any node is calculated using the equation (7). Further, the agent-based system eliminates the computations required at each node and saves the energy of nodes. Saving the energy increases the life of sensor nodes.

**Case 2:** The trust of node D with respect to node A $(R_{A,D})$ is calculated using the trust of node D at B with respect to node A and trust of node D at C with respect to node A.

(a) Trust of node D at node B with respect to node A $(R_{B_A,D})$ is the sum of the trust of node B on node D and trust of node B on node A $(R_{BA})$ :

$$R_{B_A,D} = R_{A,D}.R_{BA} + (1 - R_{BA})R_{B,D} \quad (9)$$

(b) Trust of node D at node C with respect to node A $(R_{C_A,D})$ is the sum of the trust of node C on node D and trust of node B on node A $(R_{CA})$ :

$$R_{C_A,D} = R_{A,D}.R_{CA} + (1 - R_{CA})R_{C,D} \quad (10)$$

Find the average of trust of node A on D, trust of node B on node D with respect A, and trust of node C on node D with respect A.

$$R_{A,D} = (R_{A,D} + R_{B_A,D} + R_{C_A,D})/3 \quad (11)$$

Figure 4a shows the slow decrease of trust calculated through equations (9) to (11). The confidence factor helps to confirm the successive node status. The Figure 4a is drawn with higher reputation of neighbor nodes and trust of node A on node D is decreasing. Figure 4b is drawn for higher reputation of node D at node A (above the threshold value) and lower reputation of nodes B and C on D. The results show that the lower reputation of node D at neighboring nodes effects the decision at node A.

The equations (7) and (11) approximately produce the same result. The results show that if the node D is malicious and temporarily produces better reputation at A, the collaborative effort will give warning to drop the node from the communication path.

## V. CONCLUSIONS

Trust-based packet transfer has been taken significant importance in recent years. The secure transfer of information with low cost is still a debatable problem in WSN. In this paper, we first presented the fuzzy rating models and Sporas formula for node rating. An agent-based approach was introduced to calculate the trust using the collaborative approach. The ratings of a node and its neighbors with respective to the node help for better decision on trust calculation of successive node in the path. A similar approach was used to lower the burden of computational work on the node. Lowering the computational work at node increases the life of sensor node.

The future research includes the event-based trust calculation. The event-based trust is recently introduced, and very little work was done in this line. Event-based trust models depend upon the specific events in the surroundings of a sensor node. It will be easier to detect the malicious node in the communication path using the data of specific events in the surroundings of a node.

## 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, pp. 218-223.

[2] 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, pp. 359-364.

[3] Zacharia, G., Moukas, A, and Mae, P., "Collaborative Reputation Mechanisms for Electronic Marketplaces", Decision Support Systems, Vol. 29, Issue 4, December 2000, pp. 1-7.

[4] 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, pp. 66-77.

[5] Carbo, J., Molina, J.M., and Davila, J., "Trust Management through Fuzzy Reputation",

 ISBN: 978-1-61208-144-1 

International Journal of Cooperative Information Systems", Vol. 12, Issue 1, 2003, pp. 135-155.

[6] Carbo, J., Molina, J.M., and Davila, J., "Comparing Predictions of Sporas vs. a Fuzzy Reputation System", 3rd International Conference on Fuzzy Sets and Fuzzy Systems, 2002 (last accessed on May 24, 2011: www.wseas.us/e-library/conferences/switzerland2002/papers/456.pdf

[7] 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(last accessed: May 24, 2011), URL: http://earticle.net/article.aspx?sn=105974)

[8] 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, pp.119-124.

[9] Boukerche, A., and Li, X., "An Agent-based Trust and Reputation Management Scheme for Wireless Sensor Networks", IEEE GLOBECOMM, 2005.2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), October 2004, pp 66-77,.

[10] Momani, F. G., and Perez, G. M., "Providing Trust in Wireless Sensor Networks using a Bio-Inspired Technique", NAEC 2008, pp. 1-16.

[11] Momani, M. and Challa, S., "Probabilistic Modelling and Recursive Bayesian Estimation of Trust in Wireless Sensor Networks," submitted to Ad Hoc Networks, 2007, pp. 381-403.

[12] Aivaloglou, E., Gritzalis, S., and Skianis, C., "Trust Establishment in ad hoc and Sensor Networks", Lecture notes in computer science, 2006, vol. 4347, pp. 179-194.

## Graphs

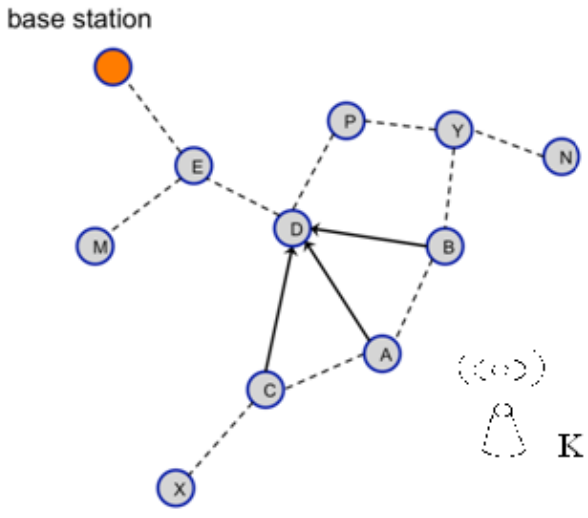


Figure 1: Wireless sensor network communication topology.

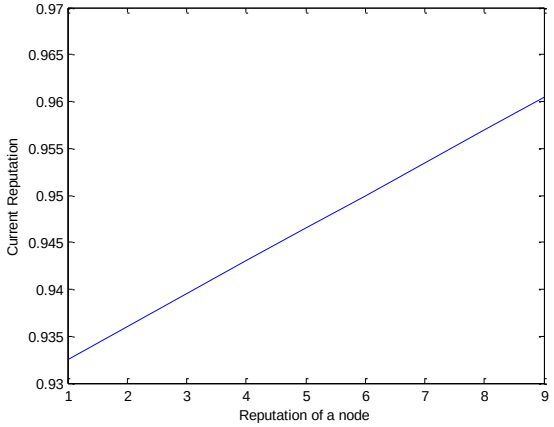


Figure 2a: Relation between the reputation of a node and current reputation

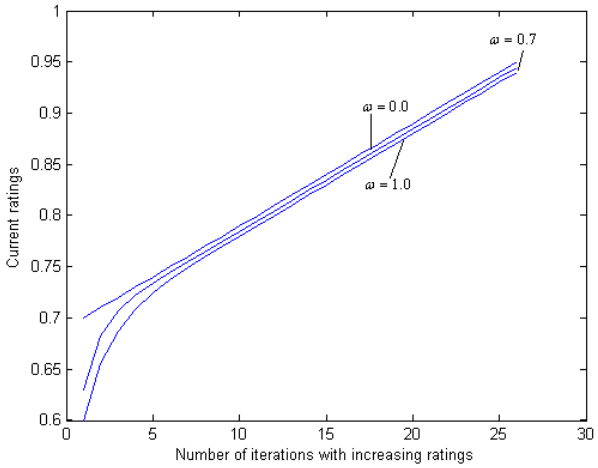


Figure 2b: Relation between the reputation of a node and current reputation

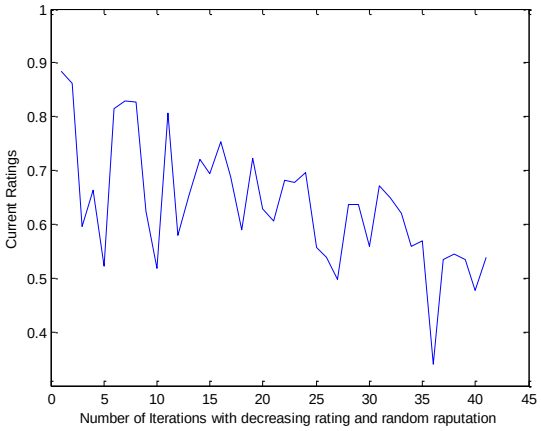


Figure 2c: Relation between the reputation of a node and current reputation

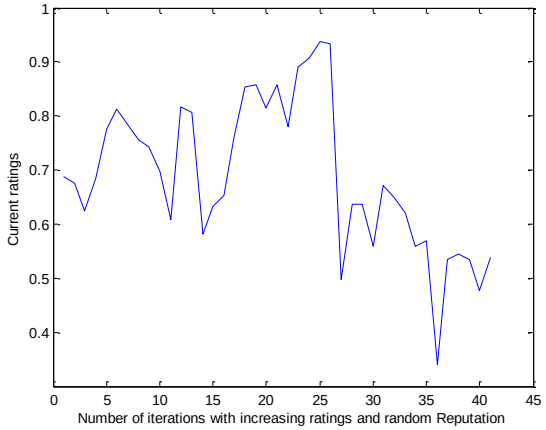


Figure 2d: Relation between the reputation of a node and current reputation

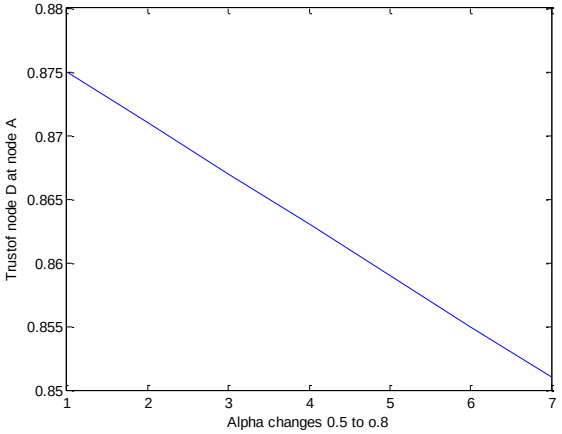


Figure 3a: Trust of node D at A with collaborative effort

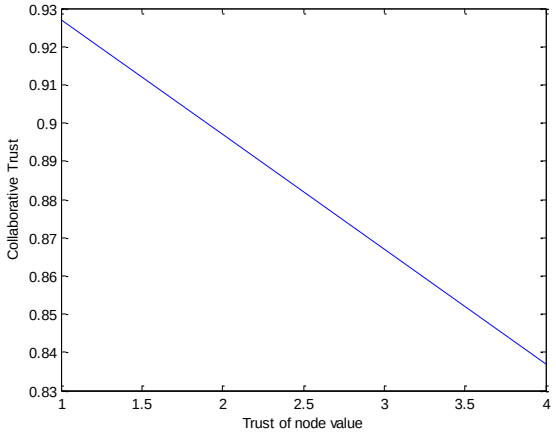


Figure 3b: Trust of node D at A with collaborative effort

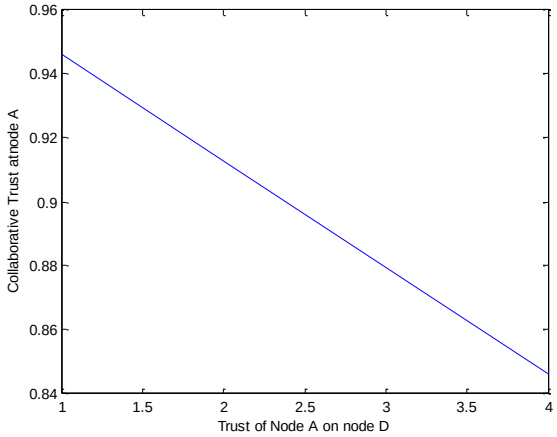


Figure 4a: Trust of node D at A with collaborative effort for Case 2.

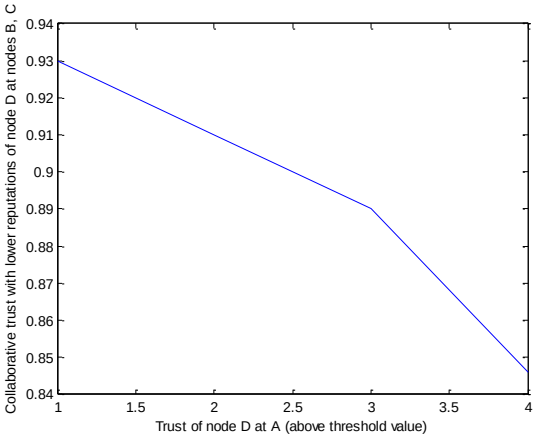


Figure 4b: Trust of node D at A with collaborative effort with lower confidence at nodes B and C (for Case 2).