TRUST-BASED APPROACH IN WIRELESS SENSOR NETWORKS USING AN AGENT TO EACH CLUSTER

Yenumula B. Reddy

Department of Computer science, Grambling State University, Grambling, LA 71245, USA

ybreddy@gram.edu

Abstract

Detection of malicious node in the neighborhood with minimal infrastructure and computations is a requirement. The existing models require more computation, storage, and complex security calculations. These models are inefficient in wireless sensor networks due to their resource limitations. Therefore, an agent-based approach that maintains the node's current status is proposed in this research. In agent-based approach detection is possible through maintaining the ratings of each node. The ratings of a node will be done through the ratio of packet forwarded by packets received. Further, the ratings can be done using the E-commerce models. In E-commerce models, each node votes the successive node depending upon the ratio of packet forwarded by packets received. The update ratings will be done through Sporas formula or Molina's formula or with a combination of both models. Further, the proposed agent-based framework uses reputation of a node through neighbouring nodes as part of trust calculation. 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.

1. INTRODUCTION

Wireless sensor networks or sensor networks are composed of a large number of sensor nodes deployed densely in a closed proximity to collect data to a specific function. Sensors have limited memory, computational capability, and limited transmission capacity. The sensors primarily preprogrammed to collect the data and forward to the base station through defined communication path. If the information is sensitive, the nodes and communication path must be trust worthy. The sensor network possesses the self-organizing capability if the positions of nodes are not predetermined. Irrespective of the topology, 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.

The low cost small size sensors with more computational power are available in the market. Due to advances in technology the applications span over house hold usage to military. The sensitive applications demand secure transmission at the time of deployment of sensors. The applications include the following items.

- Cars, household items (microwave, refrigerator, washing machine), toys, and office equipment (doors, scanners, printers, and cameras)
- Control of heating, ventilation, detect the presence of biological and chemical presence
- Structural monitoring, tracking of shipment, global positioning system, health monitoring, shopping malls, building entries, remote control to televisions and motor vehicles
- Traffic conditions, status of parking places, status of the hospital room conditions, and unauthorized entries in buildings

The sensor applications in daily life includes from house related to military. Due to these reasons sensor research became very famous.
The algorithms and protocols usage in networks and sensors is different due to nature of applications. Some of the major differences between wireless sensor networks and wireless networks (ad-hoc networks) are given in Table I.

Table 1: Major differences between wireless sensor networks and ad-hoc networks

Wireless sensor networks	**Ad-hoc networks**
The wireless sensor nodes are densely deployed.	Deploying the nodes in Ad-hoc are depends upon specific policy.
Sensor nodes are bound to (prone to) fail.	It is not the same case in ad-hoc networks.
Topology changes frequently, since positions of nodes are not predetermined and nodes may fail at any time.	Positions and policies are predetermined.
Limited memory, computational capability, and transmission power.	Capabilities are different in ad-hoc networks.
Global identification of a specific node may not exist.	Each node is connected and identified.
Sensor networks require special protocols to work with its design specifications.	Traditional protocols use exchange and distribute the keys through cryptographic tools for trust evidence.

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 the ratio (R=Pt/Pr) of packets transmitted (Pt) to receive (Pr). The minimum acceptable number is called threshold $(R \geq T)$. The threshold is used to rate the node. One of the

methods to update the node ratings is using the E-commerce formula called Sporas formula [7] or Molina's fuzzy reputation model [5] or proposed agent-based model. The proposed agent-based model reduces the overheads on sensor nodes and helps to improve the life sensor nodes in terms of battery power, computational, and management of node data.

Dynamic topology is one of the property in massive deployment of sensors is a dense unknown field. Failure of sensors is common in such situations. The recent research [29, 36, 40] shows that the new algorithms for optimal deployment of sensors, localization, energy efficient, energy aware routing, data aggregation, and fusion. The algorithms meet the problems of transmission failure, automatic adjustment in topology. Further, task completion that includes sensing data, reporting data, and detecting malicious node requires cooperation of neighbor nodes. The cooperation between the needs trust of neighboring nodes. The research builds on trust of neighboring nodes and rating the successive node that transmits the data. Therefore, a trust management system that uses the limited resources is a requirement. The new trust based system must detect the malicious node with minimal resource usage.

The sensing the misbehavior of a node starts with dropping of packets purposefully (effect of an intruder) or randomly. The trust is based on repeated positive behavior of a node. The reputation is a tool to detect the behavior of a node [50-53]. In agent based systems, all node tables are maintained at the agent. The agent further maintains the neighboring nodes. Therefore, the agent based system helps to detect the malicious node with minimal effort. Since the current encryption or stochastic models cannot detect the malicious node, the trust based system is more suitable. Further, trust of a node cannot be generated automatically. It requires an appropriate procedure to generate trust and further actions of detecting malicious node.
Figure 1 show the wireless sensor network with nodes, connected to neighbor nodes, and an agent to collect and process trust information. The agent's responsibility is to collect the node ratings and update the trust of each node within communication distance of successive node in the path. The agent further provides the level of trust, detects the malicious node, and recommends alternative path if the trust of a node in the communication path 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.

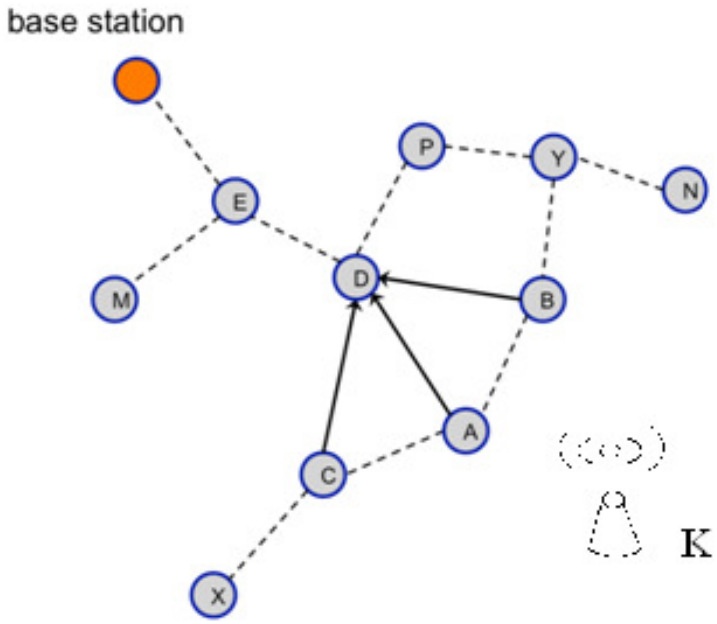


Figure 1: Wireless sensor network communication topology.

2. 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, 48-52], event-based trust management [2], and agent-based trust management [7-9]. Repeated games help to detect the trustworthiness of a node in the path [1].

Ganeriwal et al. [4] discussed the reputation-based framework for high integrity sensor networks. The model 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. Dragovic et al [45] discussed the event-based trust management. They described the methodology for storage and retrieval based on reputation information can improve the scalability while exploiting the asynchrony.

Trust management in wireless sensor networks and pervasive computing using Bayesian estimation was studied in [11,42]. In [42], the authors proposed a framework that evolves trust based on Bayesian formulation. Even it is expensive, it helps to resist the Sybil attacks. The

Momani and Challa [11] proposal concludes that relationship between the nodes helps to purge the bad nodes. Filtering the false data in sensor networks was discussed in [40]. Further, the security models in sensor networks and trust based security was discussed in [22-39]. The security aspects discussed in [22-39] proposes many intrusion attacks non wireless networks and wireless sensor networks. The neural network approach to detect the local trust value in P2P environment was discussed in [41]. Further, managing trust in P2P environment was studied in [14, 15]. Trust in an uncertain environment was studied in [6, 46]. The authors in [6] studied the trust of fuzzy reputation systems and uncertain environment in [46] to secure the nodes in the communication path.

The survey of trust and security models was studied in [16, 27, 30]. Wireless sensor network security issues and innovative approaches to solve these problems are studied in [16]. The authors concluded that the future research follows the innovative approach to model trust based approach in wireless sensor networks. The security using trust with task-based and data aggregation, filtering false data, beta reputation, and trust as a computational concept were studied in [13, 17-21]. Trust management in grid computing was studied in [43]. The event based trust management and collaborative trust management was studied in [44-45]. Recently, event-based and agent-based trust management systems are gaining more attention in the research world.

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. Recently, the E-commerce models for trust management and intrusion detection have more attention in sensor network research.

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 wireless sensor networks. Bio-inspired techniques based on ant colony system are another attraction in trust based systems. In ant colony based trust systems, we can detect most worthy path 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 wireless sensor networks. 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.

3. TRUST AND REPUTATION

The reputation-based models use the trust model based on the ratio that the rate of a number of packets received to the number of packets transmitted [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 voted 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 communication (data transfer) path. These calculations show that the 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 ω. The maximum value of remembrance is 1 and the minimum value is 0. Hence ω may be chosen between 0 and 1 ($0 \le \omega \le 1$). Using the Molina's formula, the current reputation of a node is calculated as [5]:

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

In equation (1), if $\omega = 0$ then the current reputation is same as current rating ($R_i = C_i$). Further, if the node does not remember the previous reputation ($\omega = 0$), then current rating is same as the reputation value. It shows that a new node entering into network does not have previous value and the new node is treated as old node with $\omega = 0$. If the learning rate equals 1 ($\omega = 1$), means the node has maximum learning level and the new reputation value of a node is calculates as the average of previous reputation with remembrance weight and current rating. The maximum value of ω provides the excellent reputation and more trustworthy. Therefore, the equation (1) becomes

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

The equation (2) shows that a new node is added with the best possible rating, the next rating may not be same and depends upon the new ratings. The rating of a node must be established by each node sending the packets. The conclusion is that the reputation must be established and it should not be taken randomly some value. Figure 2a shows that the node ratings depend upon the learning factor. If the learning factor is greater than zero, the node ratings always increase and proportional with the iterations. In Figure 2b, we have fixed the value of ω and the node current ratings and previous ratings were initialized. The learning variable does not influence the node ratings. The reason is that each time separate learning factor is used. The learning factor may increase or decrease, but never be same in sensor nodes. If the learning factor is initialized each time, there are no updates to node ratings. Therefore, the variation for higher value of learning is marginal or no change in value.

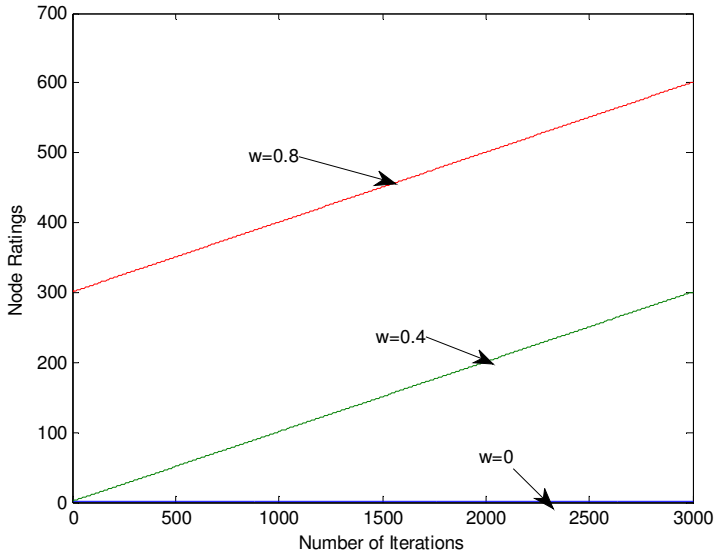


Figure 2a: Ratings of the node with iterations

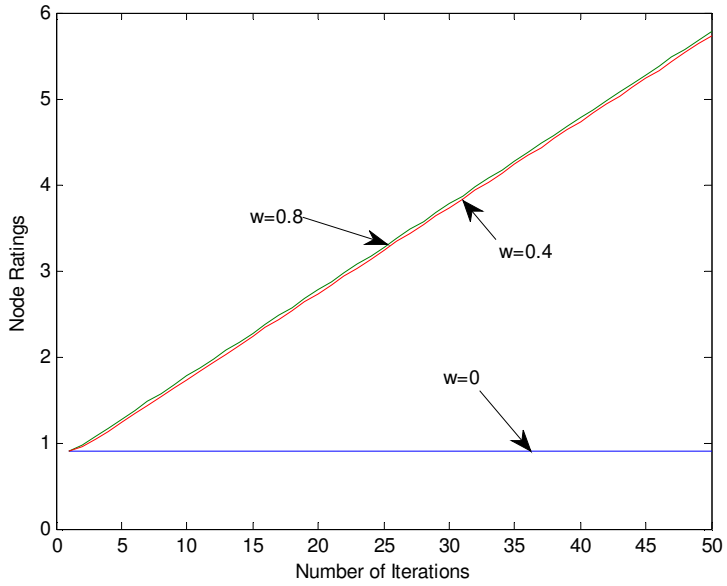


Figure 2b: Ratings of the node with iterations

In sensor networks, the trust of a node depends upon the reputation. The reputation achieved through voting by the nodes transferring the packets through that node. In E-commerce, the voting updates on a product or node (in the present case) are obtained using Sporas formula. The current ratings are obtained using the following Sporas formula [7].

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

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

where:

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

ϕ - helps to slow down the incremental change

C_i - represents the rating given by the node i

D - range or maximum reputation value

σ - the acceleration factor to keep the ϕ above certain value (> threshold).

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.

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

Assume the remembrance weight ω=1 or ω =0 the equation (5) simplifies

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

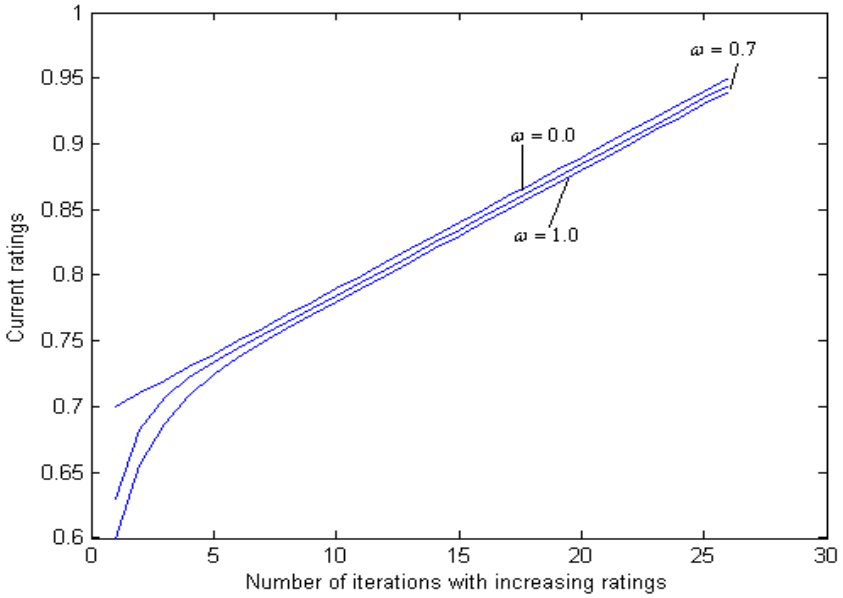
The equation (6) shows that if the remembrance ω = 1 or ω = 0 the ratings given by a node i (ith node) is equal to reputation of the node. That is, a long term excellent reputation node and recent added good node assumes to be trustworthy.

Further, in equation (1), if the remembrance ω=1, then current reputation is average of previous reputation and current ratings. Figure 3a shows the relation between reputation of a node and current reputation. In normal conditions, the current reputation is proportional to previous reputation.

Figure 3b 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 3c and Figure 3d 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 wireless sensor networks is temporary. The continuous update of ratings is required in the wireless sensor networks.



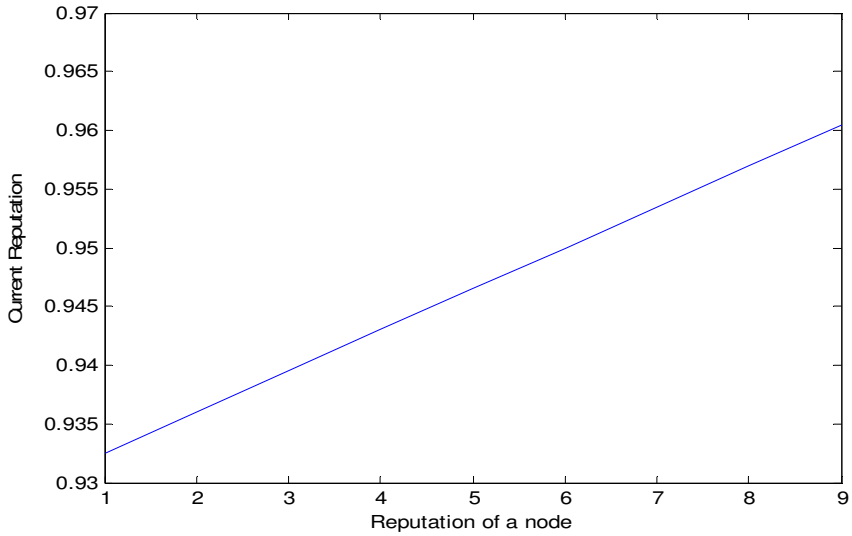


Figure 3a: Relation between the reputation of a node and current reputation

Figure 3b: Relation between the reputation of a node and current reputation

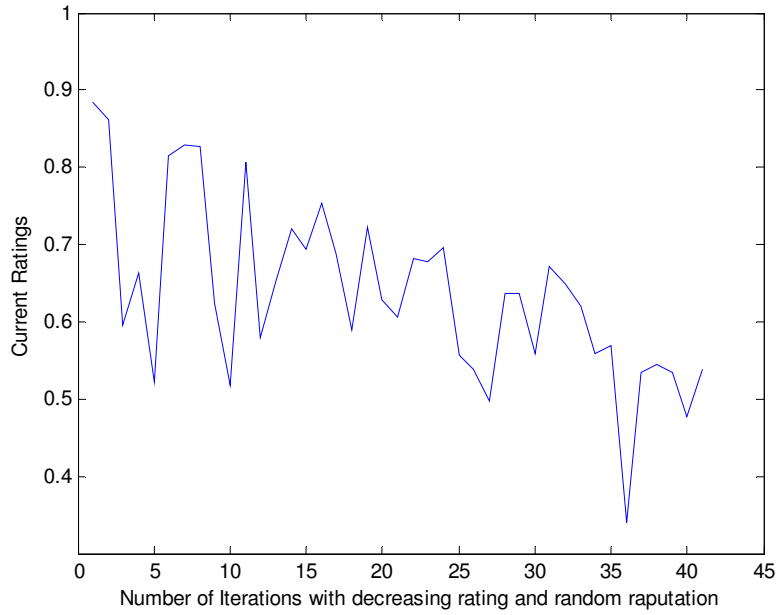


Figure 3c: Relation between the reputation of a node and current reputation

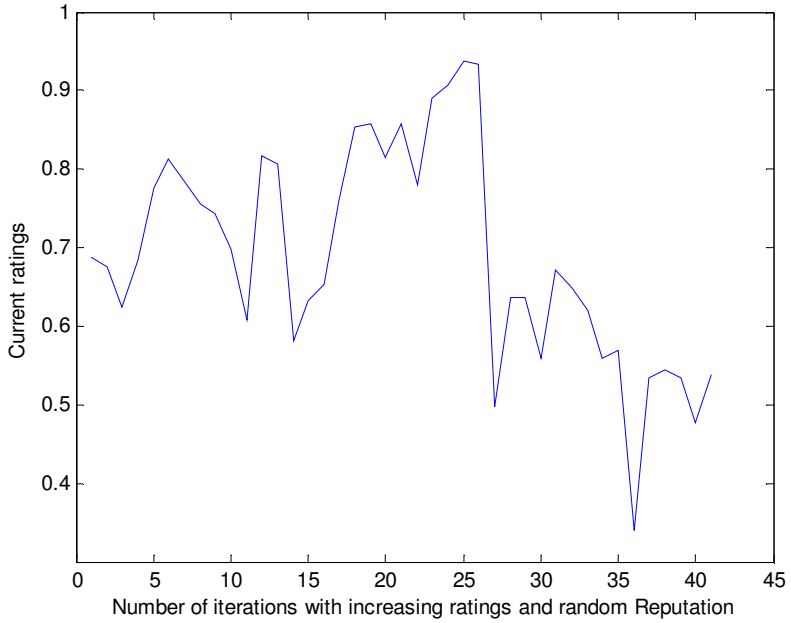


Figure3d: Relation between the reputation of a node and current reputation

4. 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 nodes that are within communicating distance and calculates the trust of a node in the transmitting path. The current trust value of a common packet transmission node decides the status of that node (malicious or not). Therefore, the trust depends upon the direct observations of a node plus the indirect observations received from its neighbor nodes. Further, 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 with appropriate multiplication factor. 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 β and γ are based on the trust of node A with respect to nodes C and B. Figure 4a shows that the higher value of alpha lower the confidence of a node that was put in trust test. If the value of β and γ 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 4b 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 4a and 4b), 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 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 of each node on its neighbor nodes. The level of belief is the multiplication factors α, β and γ with appropriate trust values. Further, the agent-based system eliminates the computations required at each node and saves the energy of nodes. Therefore, the energy savings increase the life of a sensor node.

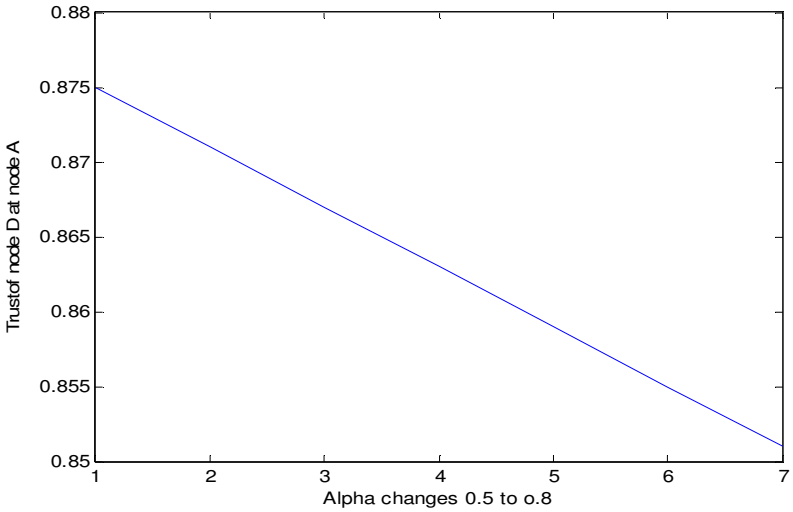


Figure 4a: Trust of node D at A with collaborative effort

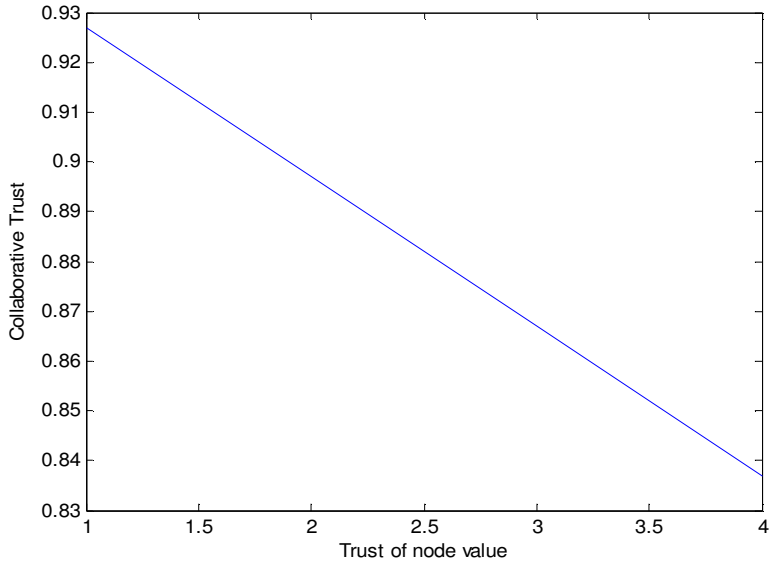


Figure 4b: Trust of node D at A with collaborative effort

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}) :

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

(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}) :

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

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.

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

Figure 5a shows the slow decrease of trust calculated through equations (9) to (11). The confidence factor helps to confirm the successive node status. The Figure 5a is drawn with higher reputation of neighbor nodes and trust of node A on node D is decreasing. Figure 5b 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.

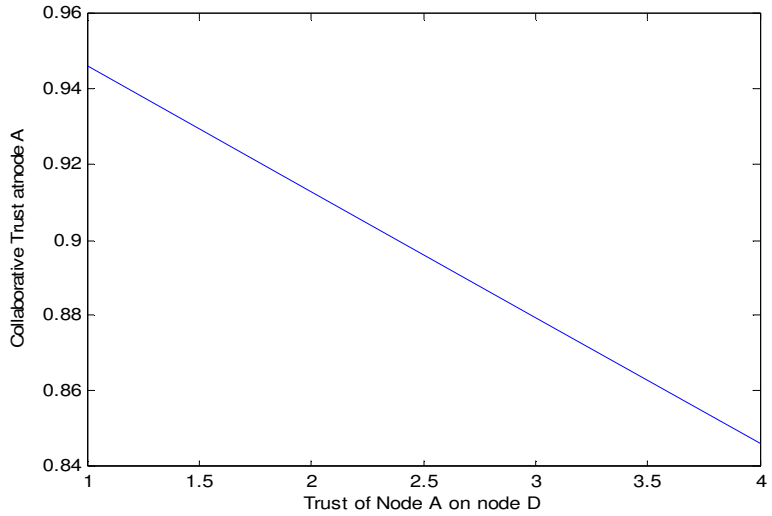


Figure 5a: Trust of node D at A with collaborative effort for Case 2.

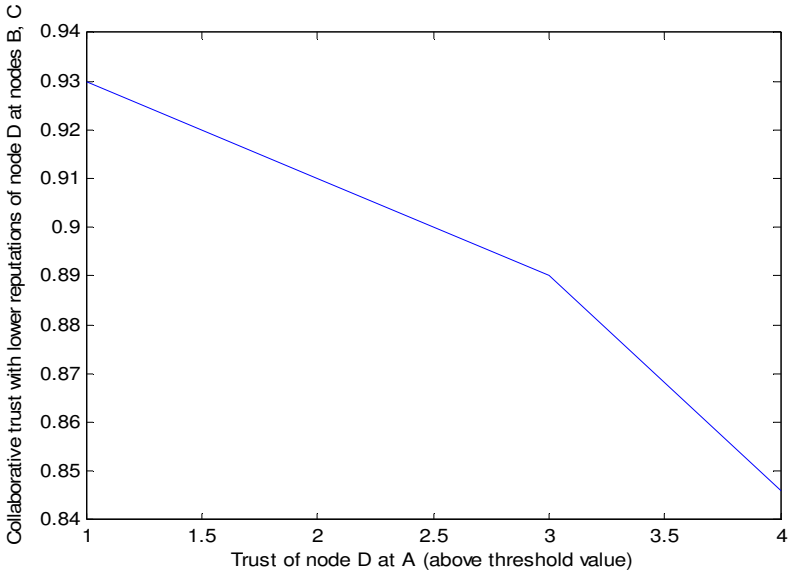


Figure 5b: Trust of node D at A with collaborative effort with lower confidence at nodes B and C (for Case 2).

5. CONCLUSIONS

Trust-based packet transfer in sensor networks has been taken significant importance in recent years. The secure transfer of information with low cost is still a debatable problem in wireless sensor networks. In this paper, we first presented the fuzzy rating models to find the note ratings. Later we used Sporas formula to update the 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 triggers the node whenever a specific event happens (increase in sound, light, humidity, sound, or any similar event) to collect and communicate the data to base station. Further, 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] H. Chen, H. Wu, J. Hu, and C. Gao., "Event-based Trust Framework Model in Wireless Sensor Networks", International Conference on Networking, Architecture, and Storage, 2008, pp. 359-364.

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

[4] S. Ganeriwal, and M. B. Srivastava., "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] J. Carbo, J. M. Molina, and J. Davila., "Trust Management through Fuzzy Reputation", International Journal of Cooperative Information Systems", Vol. 12, Issue 1, 2003, pp. 135-155.

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

[8] H. Chen, H. Wu, J. Hu, and C. Gao., "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] A. Boukerche, and X. Li., "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] F. G. Momani, and G. M. Perez., "Providing Trust in Wireless Sensor Networks using a Bio-Inspired Technique", NAEC 2008, pp. 1-16.

[11] Mohammad Momani and Subhash Challa (2010). Probabilistic Modelling and Recursive Bayesian Estimation of Trust in Wireless Sensor Networks, Bayesian Network, Ahmed Rebai (Ed.), ISBN: 978-953-307-124-4, InTech, Available from: http://www.intechopen.com/articles/show/title/probabilistic-modelling-and-recursive-bayesian-estimation-of-trust-in-wireless-sensor-networks.

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

[13] E. Kotsovinos, and A. Williams., "BambooTrust: Practical Scalable Trust Management for Global Public Computing", 2006 ACM Symposium on Applied Computing, Dijon, France 2006.

[14] Z. Liang, and W. Shi., "PET: A Personalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing", 38 Hawaii Int. conf. on Systems Sciences, 2005, pp. 201-210.

[15] A. Aberer, and Z. Despotovic., "Managing trust in a Peer-2-Peer information system", 10th International Conference on Information and Knowledge management, 2001, pp. 310-317.

[16] M. Momani, and S. Challa., "Survey of Trust Models in different Network Domains", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), Vol.1, No.3, September 2010, pp. 1-19.

[17] H. Chen., "Task-based Trust Management for Wireless Sensor Networks", International Journal of Security and its applications, vol 3, 2009, 28 Nov.-2 Dec. 2005, pp.1857-1861.

[18] W. Zhang, S. K. Das, and Y. Liu., "A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks", 3rd annual IEEE communications on sensor and ad hoc communications and networks (SECON 06), 2006, pp. 60-69.

[19] W. Zhang, and G. Cao., "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach", The 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05), Miami, USA, 2005.

[20] S. P. Marsh, "Formalising Trust as a Computational Concept", PhD Thesis, University of Stirling, 1994.

[21] A. Josang and R. Ismail., "The Beta Reputation System", 15th Bled Electronic Commerce Conference, 2002, pp. 1-14.

[22] J. Newsome, E. Shi, D. Song and A. Perrig., "The Sybil Attack in Sensor Networks: Analysis & Defenses", Third International Symposium on Information Processing in Sensor Networks, 2004. IPSN 2004. Pp. 259-268, ISBN: 1-58113-846-6.

[23] H. Chan and A. Perrig., "Security and Privacy in Sensor Networks", IEEE Computer Journal, vol. 36, pp. 103-105, 2003.

[24] T. Zia and A. Zomaya., "Security Issues in Wireless Sensor Networks", International conference on Systems and Networks Communication (ICSNC '06), , Tahiti, French Polynesia 2006.

[25] L. Zhou and Z. J. Haas., "Securing Ad-hoc Networks", IEEE Network Magazine, 1999.

[26] B. Przydatek, D. Song and A. Perrig., "SIA: Secure Information Aggregation in Sensor Networks", 1st International Conference on Embedded Networked Sensor Systems Los Angeles, California, USA 2003.

[27] Y. Wang, G. Attebury and B. Ramamurthy., "A Survey of Security Issues in Wireless Sensor Networks", IEEE Communications Surveys and Tutorials, vol. 8, pp. 2-23, 2006.

[28] F. Stajano and R. Anderson., "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", 8th International Workshop on Security Protocols, Lecture Notes in Computer Science, Springler-Verlag, Berlin, Germany, 1999.

[29] A. Perrig, J. Stankovic and D. Wagner., "Security in Wireless Sensor Networks, Communications of the ACM", vol. 47, pp. 53-57, 2004.

[30] J. P. Walters, Liang, Z. W. Shi and V. Chaudhary., "Wireless Sensor Network Security: A Survey, Security in Distributed, Grid, and Pervasive Computing", Y. Xiao, Ed.: Auerbach Publications, CRC Press, 2006.

[31] D. Zhou., "Security Issues in Ad-hoc Networks", The Handbook of Ad-hoc Wireless Networks Boca Raton, FL, USA: CRC Press, Inc. , 2003, pp. 569 - 582.

[32] P. Papadimitratos and Z. J. Haas., "Securing Mobile Ad-hoc Networks", The Handbook of Adhoc Wireless Networks: CRC Press LLC, 2003.

[33] C. Karlof, N. Sastry, and D. Wagner., "TinySec: A Link Layer Security Architecture for Wireless Sensor Network", Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 2004.

[34] S. Zhu, S. Setia and S. Ja., "Sensor Networks", 10th ACM Conference on Computer and Communications Security, Washington D.C., USA, 2003.

[35] C. Karlof and D. Wagner., "ecure Routing in Sensor Networks: Attacks and Countermeasures", First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[36] M. Bohge and W. Trappe., "An Authentication Framework for Hierarchical Ad-hoc Sensor Networks", ACM Workshop Wireless security (WiSe '03), San Diego, CA, USA, 2003.

[37] Y. Zhang, W. Liu, W. Lou and Y. Fang., "Location-based Compromise Tolerant Security Mechanisms for Wireless Sensor Networks", IEEE Journal on Selected Areas in Communications, vol. 24, pp. 247-260, 2006.

[38] W. Zhang and G. Cao., "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach", 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05), Miami, USA, 2005

[39] A. Perrig, R. Zewczyk, V. Wen, D. Culler and D. Tygar., "SPINS: Security Protocols for Sensor Networks, Wireless Networks", vol. 8, pp. 521-534, 2002.

[40] F. Ye, H. Luoa, S. Lu and L. Zhang., "Statistical En-route Filtering of Injected False Data in Sensor Networks", Selected Areas in Communications of the ACM, vol. 23, 2005.

[41] H. Baohua, H. Heping and L. Zhengding., "Identifying Local Trust Value with Neural Network in P2P Environment", First IEEE and IFIP International Conference in Central Asia on Internet, Bishkek, Kyrgyz Republic, 2005.

[42] D. Quercia, S. Hailes and L. Capra., "B-trust: Bayesian Trust Framework for Pervasive Computing", Trust 2006 - 4th International Conference on Trust Management, Pisa, Italy, 2006.

[43] F. Azzedin, andM. Maheswaran., "Evolving and Managing Trust in Grid Computing Systems", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE '02), 2002.

[44] B. Dragovic, E. Kotsovinos, S. Hand, and P. R. Pietzuch., "XenoTrust: Event-Based Distributed Trust Management", 14th International Workshop on Database and Expert Systems Applications Prague, Czech Republic, 2003.

[45] B. Shand, N. Dimmock, and J. Bacon., "Trust for Ubiquitous, Transparent Collaboration", Wireless Networks, vol. 10, pp. 711-721, 2003.

[46] V. Cahill, E. Gray, J. M. Seigneur, C. D. Jensen, Y. Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. W. Wagealla, S. Terzis, P. Nixon, G. D. Marzo Serugendo, C. M. Bryce, K. Carbone, and M. Nielson., "Using Trust for Secure Collaboration in Uncertain Environments", IEEE Pervasive Computing, vol. 2, pp. 52-61, 2003.

[47] P. Michiardi, and R. Molva., "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad-hoc Networks", The IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security Portoroz, Slovenia, 2002.

[48] Y. B. Reddy and Rastko Selmic., "Secure Packet Transfer in Wireless Sensor Networks – A Trust-based Approach", International Journal on Advances in Security, vol 4, no 3&4, 2011.

[49] Y. B. Reddy., "Spectrum selection Through Resource Management in Cognitive Environment", International Journal on Advances in Systems and Measurements, vol 4, no 1&2, year 2011

[50] 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

[51] Y. B. Reddy, Kafle, S, and Selmic, R., Cooperative and Collaborative Approach for Secure Packet Transfer in Wireless Sensor Networks, SENSORCOMM 2011, August, 2011.

[52] Y. B. Reddy and Rastko Selmic., No-Regret Learning Approach for Trust-based packet Transfer in Wireless Sensor Networks, SENSORCOMM 2011, August 2011.

Author,

Yenumula B. Reddy, Ph. D. from IIT Delhi, India, Professor of Computer Science, Grambling State University. His research contributions span a number of areas including wireless communications, intrusion detection, data mining, neural networks, intelligent systems, and genetic algorithms. He published more than 100 papers in Journal/Conference proceedings (IEEE/IARIA/IFIP/IASTED) and more than 100 student project presentations in conferences. He is one of the Editor of SENSORCOMM 2011, associate editor of proceedings of ITNG 2009, ITNG 2010, ITNG 2011, and book "Soft Computing Ap plications in Industry. He is editorial board member of Journal BITM Transactions on EECC, Science Academy Transactions on Computer and Communications Networks (SATCCN), and International Journal of Engineering and Industries (IJEI). He is review Committee member of journals IEEE-TVC, IEEE-TVT, and Journal of Communications, and program Committee member of many conferences. He was selected by Louisiana Board for International faculty exchange Program 2010 to conduct "High Performance Computing" course at Pole University, Paris. He was chair of 'International Symposium on Networking and Wireless communications' in connection with ITNG 2008, 2009, 2010, and 2011. He was award winner of best track/Symposium in ITNG 2008-2011. He has successful funding record from the federal and state grants.