ISSN 1726-5479

SENSORS & TRANSDUCERS

3 vol. 14-2 Special /12

Physical and Chemical Sensors & Wireless Sensor Networks

International Frequency Sensor Association Publishing

IFSA

Sensors & Transducers

Volume 14-2, Special Issue
March 2012

www.sensorsportal.com

ISSN 1726-5479

Sensors & Transducers Journal (ISSN 1726-5479) is a peer review international journal published monthly online by International Frequency Sensor Association (IFSA).
Available in electronic and on CD.

Sensors & Transducers Journal

Contents

Volume 14-2
Special Issue
March 2012

www.sensorsportal.com

ISSN 1726-5479

Research Articles

Authors are encouraged to submit article in MS Word (doc) and Acrobat (pdf) formats by e-mail: editor@sensorsportal.com
Please visit journal's webpage with preparation instructions: http://www.sensorsportal.com/HTML/DIGEST/Submition.htm

International Frequency Sensor Association (IFSA).

The 6th International Conference on Sensor Technologies and Applications

SENSORCOMM 2012

19 - 24 August 2012 - Rome, Italy

Deadline for papers: 5 April 2012

Tracks: Architectures, protocols and algorithms of sensor networks - Energy, management and control of sensor networks - Resource allocation, services, QoS and fault tolerance in sensor networks - Performance, simulation and modelling of sensor networks - Security and monitoring of sensor networks - Sensor circuits and sensor devices - Radio issues in wireless sensor networks - Software, applications and programming of sensor networks - Data allocation and information in sensor networks - Deployments and implementations of sensor networks - Under water sensors and systems - Energy optimization in wireless sensor networks

http://www.iaria.org/conferences2012/SENSORCOMM12.html

The 3rd International Conference on Sensor Device Technologies and Applications

SENSORDEVICES 2012

19 - 24 August 2012 - Rome, Italy

Deadline for papers: 5 April 2012

Tracks: Sensor devices - Ultrasonic and Piezosensors - Photonics - Infrared - Geosensors - Sensor device technologies - Sensors signal conditioning and interfacing circuits - Medical devices and sensors applications - Sensors domain-oriented devices, technologies, and applications - Sensor-based localization and tracking technologies

http://www.iaria.org/conferences2012/SENSORDEVICES12.html

The 5th International Conference on Advances in Circuits, Electronics and Micro-electronics

CENICS 2012

19 - 24 August 2012 - Rome, Italy

Deadline for papers: 5 April 2012

Tracks: Semiconductors and applications - Design, models and languages - Signal processing circuits - Arithmetic computational circuits - Microelectronics - Electronics technologies - Special circuits - Consumer electronics - Application-oriented electronics

http://www.iaria.org/conferences2012/CENICS12.html

Sensors & Transducers Journal, Vol. 14-2, Special Issue, February 2012, pp. 308-320

www.sensorsportal.com

Sensors & Transducers

ISSN 1726-5479

http://www.sensorsportal.com

Secure Packet Transfer in Wireless Sensor Networks

Yenumula B. Reddy
Grambling State University
Grambling, LA 71245, USA
E-mail: ybreddy@gram.edu

Received: 9 December 2011 /Accepted: 20 December 2011 /Published: 12 March 2012

Abstract: Secure data transfer with minimum overhead is essential. Currently, the secure data transfer in sensor networks uses cryptography, authentication, and probability based approaches. Recently, collaborative trust-based packet transfer technique was used in wireless sensor networks. Further, Sporas formula helps to update the node's trust value in a repeated packet transfer. In the proposed research, the trust level of a node is recommended as the average value generated through Sporas formula and repeated trust calculations. If the trust value of a forwarding node is below the threshold (expected value), the node is suspected as malicious and communicates the status to its neighbor nodes. Further, the neighbor nodes calculate their own trust of a suspicious node using their trust value plus trust factor received from their neighbor. The cooperative and collaborative approach helps to eliminate the suspicious node from the communication path. The proposed technique was analyzed, and simulations were provided. *Copyright © 2012 IFSA.*

Keywords: Packet transfer, Wireless sensor networks, Collaborative approach, Protocols, Trust-based approach, Resource.

1. Introduction

Wireless sensor networks (WSN) are composed of a large number of sensors (sensor nodes or nodes) distributed over a designated field. They monitor physical and environmental conditions as desired by the application. The nodes collect the application desired data and communicate to the base-station. The nodes may be deployed in predetermined position and environment or deployed in an unknown environment with no predetermined position. The purpose of the nodes is to collect the data, irrespective of the environment and position. The nodes do not need self organization, if the position, environment, communication path, and purpose are known. Further, in an unknown environment and

irregular positioning of sensors (density of nodes), the network may require the self-organization capability. If the application is sensitive, the security becomes an issue.

The recent developments in electronics and communications, sensors are available in small size and low cost, which can collect and relay the environmental data. Due to their size and capabilities the applications span over the battle field to hazardous and hostile environments. Some of the applications of sensor networks include:

- Control of heating, ventilation, and detect the presence of dangerous materials like biological and chemical environments.
- Design of remote controls to operate motor vehicles, home equipment, toys, building entries, detect enemy movements, shopping malls, and medical facilities (healthy monitoring and surgeries).
- Tracking of shipment, structural monitoring, traffic conditions, plan routs, and status of parking places.

The sensors became part of life due to their applications in daily life. Since the applications are unlimited, study of the sensor design and security became extremely important.

Massive deployment of sensors in hostile areas including forests, biological and chemical fields is very common and requires secure communication. Further, the network face challenges due to limited power supply, storage, computational constraints. Replacement of failing sensors or adding sensors to cover the black holes is very common in such dangerous places. Since they are organized in an open environment, injecting of bad nodes to corrupt the transmission is possible. Therefore, a secure transmission model is required to avoid the transmission through corrupted node. Further, design of secure communication model between sensor nodes is very difficult. The traditional protocols use exchange and distribute the keys through cryptographic tools for trust evidence. The resource limitations in sensor networks obstruct the use of traditional tools including cryptographic models and protocols for secure communications.

In sensor networks, the topology changes dynamically due to failure of sensors nodes. Recent research shows that algorithms were developed to address the energy aware routing, optimal deployment of sensors, localization, data aggregation and fusion. The algorithms meet the problems including communication failures and topology changes. Further, sensing data and reporting data with limited communication distance requires cooperation of nodes to complete the task. The cooperation happens between the nodes only if they trust their neighbor to transfer the data. Therefore, a trust management system that uses limited recourses is required to detect the node (s) with undesired behavior.

The trust depends upon the predictable behavior of other nodes in the network and builds upon continuous positive behavior. Further, trust depends upon the degree of belief based upon the experience. Trust is subjective, non-transferable, time dependent, contextual, and unidirectional. Due to the simplicity and effectiveness of the trust and reputation based models researchers' attention is diverted towards these models.

The trust starts with sensing the behavior of the neighbor node. The misbehavior is dropping the packets continuously or randomly. The packet dropping may be due to malicious attacks (influence of bad nodes or intruders) on the node or communication defects. The trust can be measured through repeated positive behavior of the node. Reputation is a tool to detect the good (or bad) behavior of the neighboring node [44- 8]. The node could be assigned a reputation value to detect the behavior and keep track of the next node (forward path) in the path. To prove the successive node in the path is trustworthy, the current node should maintain a table. The table must contain the number of packets received and transmitted from the successive node. Further, it matches the table by overhearing from the next node, which transmits the packets to its neighbor. All nodes in the path will follow this process. The table includes the number of transmitted packets and will be initialized to zero after a set time. The

method is simple with minimum resource utilization and easy to maintain. The design of such simple and low cost secure model is very important and an open research area.

Routing the packets in wireless sensor networks (WSN) is done by routing protocols. The routing procedure uses encryption, digital signature, and authentication. Further encryption and authentication limits the performance of nodes in WSNs. Encryption and authentication cannot prevent the malicious or misbehavior of the sensor nodes. After reviewing relevant sensor network models, we found that the trust-based model is a better model than the existing models. Since trust cannot be generated automatically, we use the verification of repeated data transfer in the successive node. The trust model detects the sinkholes, selective packet dropping, and malfunction of the node.

Once the trust is established, it cannot be taken for granted for the rest of the sensor lifetime without repeated reevaluation. The trust relationship changes continuously due to sensor failures and malfunctions. To keep track of the uncertainties, the trust relationships among the neighboring nodes are very important. The Sporas reputation function helps to maintain the trust level of a node by minimizing the single user as well as a new user influence. The process further helps to avoid the Sybil attacks [17].

The remaining part of the paper discusses the recent developments, collaborative reputation activity, simulations using Sporas formula, reputation-based trust formulation, trust cluster approach and conclusion of results.

2. Recent Developments

The security issues were studied by many researchers [1-2, 5-12, 17-27]. The security issues using cryptographic, stochastic, and authentication were studies by [28-35] to transfer the data on WSN. These models require more memory, energy, and computations. New techniques are required to optimize the resource usage and transfer the data securely. Further, a secure routing protocol that addresses the limitations of sensor nodes and safe transfer of data on a communication path between the nodes is required. The process must detect and eliminate the malicious nodes from the communication path. Trust-based approach was one of the models to detect and eliminate the malicious node. Trust-based approach maintains a table at each node to record the history and behavior of a node. The trust-based approach seems less expensive and easy to use.

For example, if a user is given the work repeatedly and the user completes to the level of satisfaction, we say the user will be trusted. The same concept is used in credit cards, bank loans, and at work places. Sensor networks are not different when we consider the trust. The Fig. 1 shows the scenario of a senor network. The nodes A, B, C are transferring the data to their successive node D, where D transfers to its next successive node E. The level of trust of a node D depends upon the percentage of packets successfully transferred to its next successive node E. The trust of node D depends upon the behavior of node D at a given time. The trust evaluation of node D also monitored through the neighboring nodes (node B and node C within communication distance) of A.

Trust values are derived in [2] by evaluating risk and reputation. In [3] the authors developed an algorithm to calculate trust using the complaints of another agent. Reputation-based framework using Bayesian formulation was developed by Generiwal et al. [4]. The proposed system uses community trustworthy behavior of the sensor nodes. The trust calculation in WSN using a bio-inspired algorithm (BTRM-WSN) based on ant colony systems were presented in [5]. The system uses similarity of how the ants' deposited pheromone helps to trace the path and quality of path by trusting the deposited pheromone.

Momani et Al. [6], explained the difference between trust, security, and reputation. Further, authors introduced the WSN security issues and innovative approaches to solve these problems. The authors concluded that the future research follows the innovative approach to model trust-based approach in WSN.

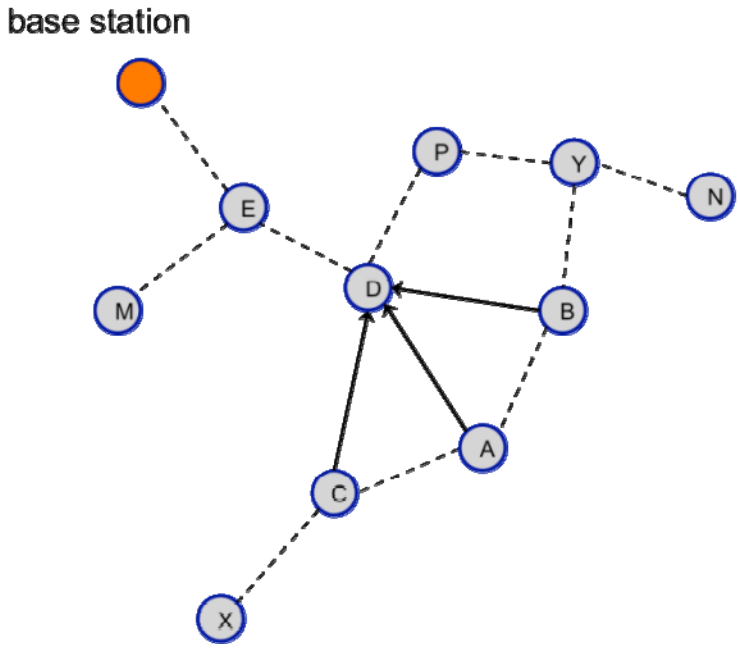

Fig. 1. Wireless sensor network communication topology.

Task-based trust management, event-based trust management and an agent-based trust management was studied in [7-11]. In [7], a general approach for task-based trust management is used similar to economics to detect the malicious node. The event-based approach [8] uses several trust ratings to enforce the security in WSN. The agent-based trust models in [8-11] 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.

Zhang et al. [12] 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 [13] uses the Bayesian probabilistic approach. The current model calculates the trust factor by using the current trust factor plus the second hand information received from its neighboring nodes. The comparison of trust algorithms, trust in grid computing, and event-based distributed trust models are studied in [36-41].

The collaborative approaches in uncertainty environment, filtering false data, and mobile ad-hoc networks were discussed in [40-43]. Further, the collaborative approach to the electronic market was discussed in [15]. The collaborative approach for secure trust-based system was discussed in [48]. These models are used to better selection of a product, to identify and filter the false data, and identifying a trusted node to transfer the data on a communication path. The collaborative approach is historically used to select an item. Recently the collaborative approach was used in the electronic market, but the purpose is the selection of a good product.

3. Collaborative Reputation Activity

Reputation builds the trust in a specific domain. Reputation-based trust was discussed in [14] and defined as the amount of trust influenced by a person or node in a specific domain. Like with human relationships, reputation values associated with a node may change over a time. Therefore, it is advised to update the node ratings using current ratings. This procedure helps to calculate better trust factor. The reason for changing the trust rates overtime is that the node may get corrupt due to malicious activity.

Assume that each node entering in the sensor network has a minimum reputation value, i.e., initially every node transfers packets correctly. The node value will be updated after a set time period. A threshold value (trust value) will be set to decide either the node will continue in the communication path or discord at the end of each set period. In a sensor network, a new node can join the existing set of sensors or a malicious sensor will be discarded from communicating path (Similar to an electronic market, a new user may join in the group or untrusted member may discontinue). The reputation value of a current node should not fall below the newly joined node. A node can rate the neighboring node more than once, but the current rating will be taken. A higher rated node will have smaller change after each rating (unless the node is corrupted).

The sample rating of a neighboring node is done depending upon the trust. Trust of each node depends upon the opinion of other nodes, particularly neighboring nodes. Trust of a node is continuous updating through rating. The current reputation of a node (trust level) is updated using the following Sporas formula [15].

$$R_i = R_{i-1} + \frac{1}{\theta}.\phi(R_{i-1}).(W_i - E_i) \tag{1}$$

$$\phi(R_{i-1}) = 1 - \frac{1}{1 + e^{-(R_{i-1} - D)/\sigma}} \quad \textit{and} \quad E_i = \frac{R_{i-1}}{D}, \tag{2}$$

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;

W_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 is compromised, the rating will be smaller and $(W_i - E_i)$ become negative. Further, the current reputation slowly crosses below threshold and node declared as malicious.

In the Fig. 1, the opinion poll on node D will be done by nodes A, B, C, and P, because these nodes communicates the packets through D to the base station. The node E cannot poll on D, since it receives the packets from D. Assume that there is a node Z between E and base station. If the node Z becomes malicious, then the node E may need to transfer the data through node D or another alternate node to reach the base station. In the opinion poll, the node A may poll 70 % and node B may poll 80 %. Sporas formula updates the rating (helps to build the trust) on node D using the rates polled by the connected nodes.

The change in node ratings and current status of a particular node (node D) is calculated using the Sporas formula. In the present case, the status of node D is calculated using the ratings of the neighboring nodes C, A, B, and P. The ratings calculation will be taken once in each window time. Multiple ratings by a particular node will be taken once (the latest poll). The fake ratings will be eliminated by using the maximum rating value allowed by a specific node at a given time (window). If the ratings on node D go down suddenly, means that there is a problem in communication (battery down or node breakdown). In such cases, the sudden high rate change happens with all nodes rating that poll to the node D (in the current case). The sudden rate change in only one node determines the problem in that particular node. The ratings node D recorded at A in a window time is shown in Fig. 2. The curve slowly increases and stabilizes after 30 times. The variation of ratings after 30 will be minor. Further, any major changes in ratings are identified the node A communicates the collaborative nodes (neighboring nodes) before a final decision about node D (good or malicious). After the analysis of collaborative data, if the node D is confirmed as dependable, the node A further analyzes its problem (with communication distance or energy level).

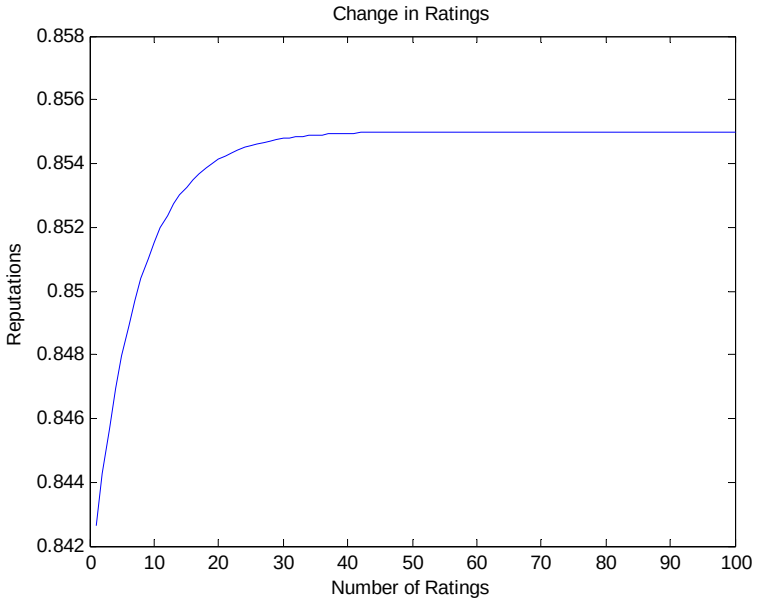

Fig. 2. The rating of node D recorded at node A.

The ratings of node D at node A may slowly drop and stabilize above threshold as shown in Fig. 3. If the ratings do not stabilize, then we need to see the ratings at collaborative nodes.

Fig. 4 shows the ratings of node A are dropping, while the ratings of other nodes stabilizes. The results show that the node A has a problem and needs to analyze its resources (communication path, energy, and other related parameters).

Further, in Fig. 5 the ratings of all nodes communicating through node D dropped below the threshold value 0.85. Each node analyzes the node D and communicates with its collaborative nodes. If the collaborative nodes have the same problem, the node D will be declared as malicious and eliminated from communication path with the help of base-station. The base-station will then provide the alternate path.

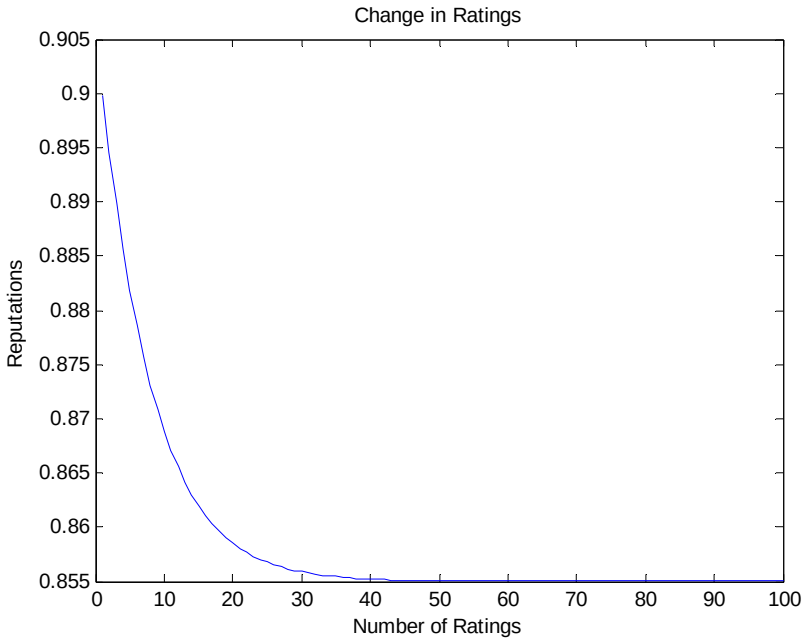

Fig. 3. The rating of node D recorded at node A (while dropping).

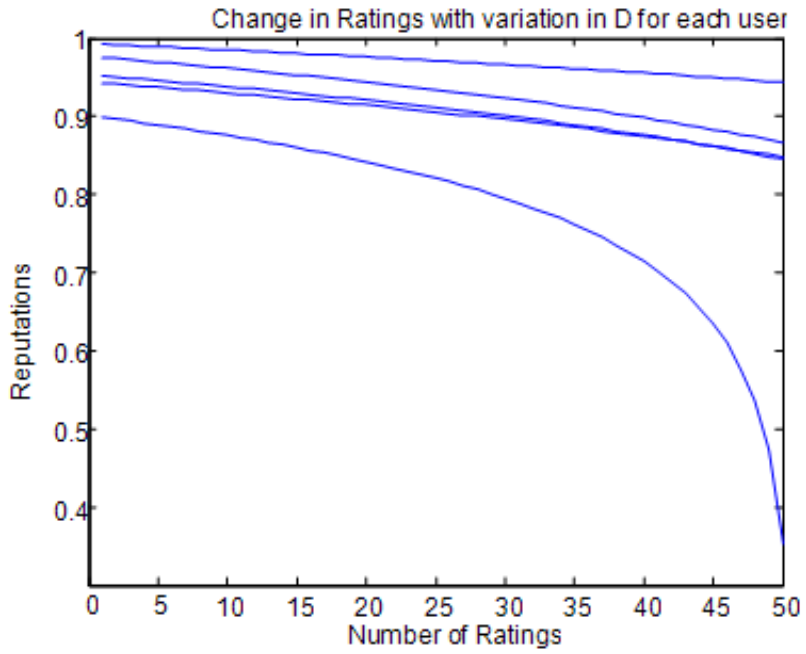

Fig. 4. The rating of node D recorded at node A is dropping but ratings of other nodes stabilizes.

The calculations seem tedious and may not seem better than encryption. Further, encryption is still an expensive process. Further, the computations will be more energy efficient by using agent based systems (future research). In agent based systems, the table maintenance and computations are managed by the agent. In agent based systems, each cluster of nodes will have one agent to manage the computations and eliminate the overheads of the nodes. The process will save energy and improves the life time of node.

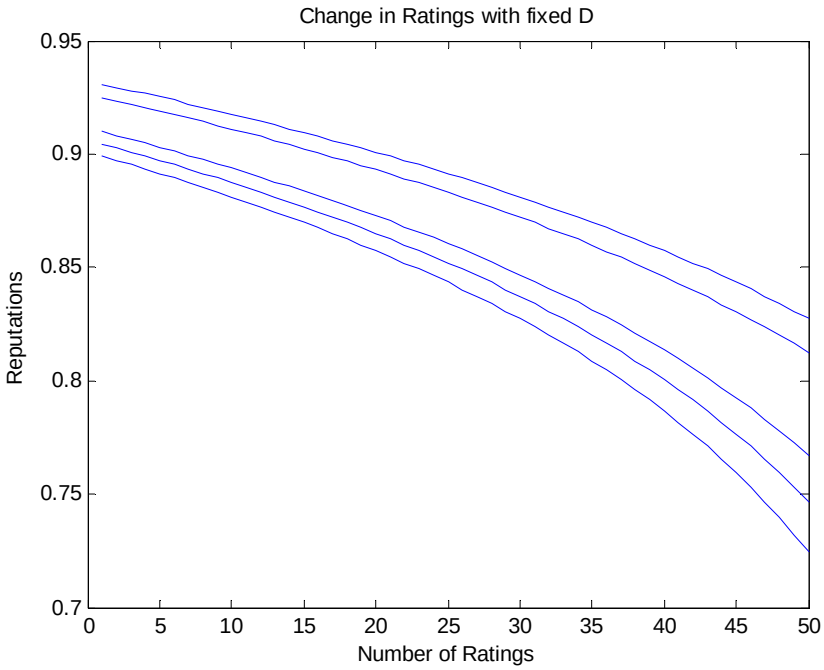

Fig. 5. The rating of node D recorded at nodes A, C, B, Y, and P are is dropping.

The simulations were presented using the random values assigned to the variables in the Sporas formula. The random values selected for the parameters in Sporas formula are given below. The number of ratings may set above 50 for better results. The θ value can be less than 10. It is proffered to set more than 10. The programs were written in MATLAB 2011b.

θ>10; $0.5<W_i<1$;

0.6<D<0.99 $0<\sigma<0.5$;

$0.5<R_{i-1}<1$;

4. Reputation-based Trust Formulation

The Sporas formula updates the node reputation to current status. The reputation status value of each node is stored by its neighboring nodes. Therefore, each node maintains a table and stores the reputation status of its neighboring node or nodes. If any node gets malicious, then the connected nodes change the reputation value in their table. If the value of a node drops below the threshold, then the node will be declared as malicious. The declared malicious node will be disconnected from the network.

The reputation of a node is calculated average of two methods. First, reputation value is calculated through Sporas formula using equation (1) basing on opinion poll. Second, reputation of a neighboring node is calculated using the ratio of the number of packets sent to the node (S_m) to the number of packets forwarded (F_n) by the node as shown in equation (3).

$$R_{nm} = \frac{F_n}{S_m} \tag{3}$$

The ratio $F_n / S_m \leq 1$ and $n/m \leq 1$ must be true all time. Unlike in Sporas formula, whenever a node is added to the network, it is given a reputation value equals to 1, means the reputation value is 100%. The reputation R must be calculated in fixed intervals (window times). After few intervals, the average reputation value will be generated (includes the initial value). The average reputation value R_{av} should not fall below the threshold T. Therefore, it follows that $R_{av} > T$, otherwise the node is treated as malicious. Consider an arbitrary variable x that has a maximum value 1 and minimum 0. The current reputation value of a node is calculated as:

$$R_r = ((1-x).R_p + x.R_c) \leq 1, \tag{4}$$

where R_r is the calculated reputation calculated, R_p is the previous reputation value, and R_c is the current reputation value. The value of x can be above 0.5 and close to the threshold value (0.9). The new updates must be small enough to be comparable with Sporas formula. The equation (4) will be compared to the equation (1), where the reputation in both cases provides the current trust status of the node. The average of these two values will provide best possible trust value R. Therefore,

$$R = (R_i + R_r)/2 \leq 1 \tag{5}$$

If the node A observes that the node D is suspicious, Fig. 1, then it broadcasts to its neighbor nodes C and B. The node C and node B calculates the trust value of node D using the broadcasted value and determines the node A's claim of suspiciousness. The node B calculates the trust of node D as below:

$$T_{ND} = R.R_{BA} + (1 - R_{BA}).R_{BD}, \tag{6}$$

where
T_{ND} is the new trust value of D at B;
R is the trust value received from A;
R_{BA} is the trust value of B on A;
R_{BD} is the trust value of B on D.

If A broadcasts that D is suspicious, B should not believe immediately. It should use the trust on A and trust on D and calculate the combined trust. If the calculated value is below the threshold then B believes that D is suspicious otherwise it broadcasts that D is not suspicious. Similarly the node C calculates its own trust on D.

For example, let us assume the following to calculate T_{ND}
R = 0.8 (the trust value received from A);
R_{BA} = 0.85 (the trust value of B on A);
R_{BD} = 0.95 (the trust value of B on D).

T_{ND} = 0.8 * 0.85 + (1 – 0.85) * 0.95
= 0.68 + 0.1425
= 0.8225

The calculated value of the trust of node D at node B (T_{ND}) depends upon the trust value supplied by node A and the level of trust that B has on A. But still it is above the value that A supplied. That is node D can be trusted and further analysis is required before we declare the node D is malicious.

5. Discussion of Results

We assume that the current trust value of node D is known by nodes A, B, and C. Suppose the current trust values of node D at nodes A, B, and C are 0.8, 0.85, and 0.92 respectively. Let x=0.8, and let R_r, R, and T_{ND} be given by equations (5) and (6). The value of R_r, R, and T_{ND} with respect to node C and node B decides that either node D will be trusted or not.

It is a known fact that sensors have limited resources including battery, computational, and communication resources. Therefore, it is suggested to use either Sporas formula or reputation-based trust model. It is further suggested using average of both formulas depending upon the sensitivity of the problem. If the data sensitivity is low and data need to be transferred securely then use either one of the formulas.

The new approach "No-Regret Learning Approach for Trust-based packet Transfer in Wireless Sensor Networks" was suggested in [47] using the agent based learning system. The agent based learning system helps to save the energy of the sensor nodes, since the load will be taken by the agent (created for each cluster).

6. Trust Based Cluster Approach

Clusters are very useful in the trust based collaborative approach. The nodes within communication distance forms a cluster, and conduct collaborative activity in calculating the trust of any successive node. For example, if n_j is a neighbor of node n_i then we represent the neighbors $(n_i, n_j) = true$. Suppose, if n_i has more than one neighbor then we write

$$(n_i, n_j)_{\hat{\lambda} j} = true. \tag{7}$$

$\hat{\lambda} j$ are the j nodes which are within the communication distance of node i. That is, i has the collaborative relation to the $\hat{\lambda} j$ nodes. Similarly, we form the neighboring nodes to each node in the network. Suppose $\zeta_{i,j}$ is the trust factor of each of j node close i^{th} node, then most dependable node in the neighborhood of a node i is the highest reputation value calculated through equation (5).

It is always necessary to keep track of the most trusted nodes within the communication distance and most inferior nodes within the communication distance. The inferior nodes will be eliminated to calculate the trust factor and if the trust factor of any inferior node is below the threshold, then all neighbors must discord the suspected node from the network. The inferior node is denoted as

$$\varsigma_{\inf} = (n_i, n_j)_{\lambda_j < threshold} \tag{8}$$

Therefore, the node i must depend upon the trusted neighbor nodes for the future path selection.

Trust based cluster approach is new and infantry state. More work is needed in this direction for sensitive data collection. The data collection in sensitive areas requires identifying the trusted neighbors. Information cannot be transferred to any neighbor, unless the neighboring node is trusted. Calculation of the trusted neighbors, identifying the malicious nodes, and transfer the data safly using various application is left for future research.

7. Conclusions

Sensors are organized in an open environment and injecting of bad nodes to corrupt the transmission is possible. Therefore, a secure transmission model is required to avoid the transmission through corrupted node. The traditional protocols use exchange and distribute the keys for trust evidence. The resource limitations in sensor networks obstruct the use of traditional tools including cryptographic models and intrusion detection packages for secure communications. Encryption, intrusion detection models, and authentication techniques limits the performance of nodes in WSNs. Encryption and authentication cannot prevent the malicious or misbehavior of the sensor nodes. After reviewing relevant sensor network models, we believed that proposed collaborative trust-based model will overcome the shortcomings in the current models.

In the proposed collaborative model, each node is updated through ratings. The ratings are provided by the nodes forwarded the packets. The update of node ratings is done through Sporas formula. If the node rate is below the threshold, the previous node uses the cooperative effort through their neighbor nodes. By using the cooperative and collaborative effort, we eliminate the suspicious node from the communication path. Preliminary results are presented using the rating of a node updated through Sporas formula.

The future work includes the agent-based trust model. Each cluster has an agent and agent relieves the computations of the nodes. All decisions will be taken at the agent.

Acknowledgement

The research work was supported by the ONR with award No. N00014-08-1-0856. The author wishes to express appreciation to Dr. Connie Walton, Grambling State University and Dr. S. S. Iyengar, LSU Baton Rouge for their continuous support. The Author wishes to thank to Dr. Selmic, Louisiana Tech University for the discussions.

References

[1]. E. Kotsovinos, and A. Williams, BambooTrust: Practical Scalable Trust Management for Global Public Computing, in *Proceedings of the ACM Symposium on Applied Computing, Dijon*, France 2006.

[2]. Z. Liang, and W. Shi, PET: A Personalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing, in *Proceedings of the 38th Hawaii Int. Conf. on Systems Sciences*, 2005, pp. 201-210.

[3]. A. Aberer, and Z. Despotovic, Managing trust in a Peer-2-Peer information system, in *Proceedings of the 10th International Conference on Information and Knowledge Management*, 2001, pp. 310-317.

[4]. S. Generowal, and M. Srivastava, Reputation-based Framework for high Integrity Sensor Networks, in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2004, pp. 1-36.

[5]. F. Marmol, and M. Perez, Providing Trust in Wireless Sensor Networks using a Bio-Inspired Technique, in *Proceedings of the Networking and Electronic Commerce Research Conference (NAEC' 08*), 2008, pp. 1-16.

[6]. 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.

[7]. H. Chen, Task-based Trust Management for Wireless Sensor Networks, *International Journal of Security and its applications*, Vol. 3, 2009.

[8]. H. Chen, H. Wu, J. Hu and C. Gao, Event-based Trust Framework Model in Wireless Sensor Networks, in *Proceedings of the IEEE International Conference on Networking, Agriculture, and Storage*, 2008, pp. 359-364.

[9]. H. Chen, H. Wu, J. Hu and C. Gao, Agent-Based Trust Management Model for Wireless Sensor Networks, in *Proceedings of the International Conference on Multimedia and Ubiquitous Engineering*, 2008, pp. 150-154.

[10]. A. Boukerche and L. Xu, An agent-based trust and reputation management scheme for wireless sensor networks, in *Proceedings of the Global Telecommunications Conference (GLOBECOM '05)*, 28 November-2 December 2005, pp. 1857-1861.

[11]. H. Chen, H. Wu, J. Hu and C. Gao, Agent-based Trust Model in Wireless Sensor Networks, in *Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, 2007, pp. 119-124.

[12]. W. Zhang, S. K. Das, and Y. Liu, A Trust Based Framework for Secure Data Aggregation in Wireless Sensor Networks, in *Proceedings of the 3rd Annual IEEE Communications on Sensor and Ad Hoc Communications and Networks (SECON '06)*, 2006, pp. 60-69.

[13]. M. Momani, and S. Challa, Probabilistic Modelling and Recursive Bayesian Estimation of Trust in Wireless Sensor Networks, A*d Hoc Networks*, 2007, pp. 381-403.

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

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

[16]. A. Josang and R. Ismail, The Beta Reputation System, in *Proceedings of the 15th Bled Electronic Commerce Conference*, 2002, pp. 1-14.

[17]. J. Newsome, E. Shi, D. Song and A. Perrig, The Sybil Attack in Sensor Networks: Analysis & Defenses, in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, IPSN 2004*, pp. 259-268.

[18]. H. Chan and A. Perrig, Security and Privacy in Sensor Networks, *IEEE Computer Journal*, Vol. 36, 2003, pp. 103-105.

[19]. T. Zia and A. Zomaya, Security Issues in Wireless Sensor Networks, in *Proceedings of the International Conference on Systems and Networks Communication (ICSNC '06)*, Tahiti, French Polynesia 2006.

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

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

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

[23]. F. Stajano and R. Anderson, The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, in *Proceedings of the 8th International Workshop on Security Protocols, Lecture Notes in Computer Science*, Berlin, Germany, 1999.

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

[25]. 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.

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

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

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

[29]. S. Zhu, S. Setia and S. Ja, Sensor Networks, in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, Washington D. C., USA, 2003.

[30]. C. Karlof and D. Wagner, Secure Routing in Sensor Networks: Attacks and Countermeasures, in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, 2003.

[31]. 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.

[32]. 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, 2006, pp. 247-260.

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

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

[35]. 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*, 2005, Vol. 23.

[36]. H. Baohua, H. Heping and L. Zhengding, Identifying Local Trust Value with Neural Network in P2P Environment, in *Proceedings of the 1st IEEE and IFIP International Conference in Central Asia on Internet*, Bishkek, Kyrgyz Republic, 2005.

[37]. D. Quercia, S. Hailes and L. Capra, B-trust: Bayesian Trust Framework for Pervasive Computing, in *Proceedings of the 4th International Conference on Trust Management (Trust '06)*, Pisa, Italy, 2006.

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

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

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

[41]. 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, 2003, pp. 52-61.

[42]. P. Michiardi, and R. Molva, CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad-hoc Networks, in *Proceedings of the 6th Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security Portoroz, IFIP TC6/TC11*, Slovenia, 2002.

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

[44]. Y. B. Reddy and Selmic, R., Secure Packet Transfer in Wireless Sensor Networks – A Trust-based Approach, *International Journal on Advances in Security*, Vol. 4, No. 3-4, 2011.

[45]. Y. B. Reddy and Rastko Selmic, Secure Packet Transfer in Wireless Sensor Networks – A Trust-based Approach, in *Proceedings of the IARIA Conference(ICN '2011)*, St. Maarten, January 23-28, 2011.

[46]. 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.

[47]. Y. B. Reddy and Rastko Selmic, No-Regret Learning Approach for Trust-based packet Transfer in Wireless Sensor Networks, in *Proceedings of the SENSORCOMM' 11*, August 2011.

[48]. Y. B. Reddy, Kafle, S, and Selmic, R., Cooperative and Collaborative Approach for Secure Packet Transfer in Wireless Sensor Networks, in *Proceedings of the SENSORCOMM '11*, August, 2011.

Sensors & Transducers Journal

Guide for Contributors

Aims and Scope

Sensors & Transducers Journal (ISSN 1726-5479) provides an advanced forum for the science and technology of physical, chemical sensors and biosensors. It publishes state-of-the-art reviews, regular research and application specific papers, short notes, letters to Editor and sensors related books reviews as well as academic, practical and commercial information of interest to its readership. Because of it is a peer reviewed international journal, papers rapidly published in *Sensors & Transducers Journal* will receive a very high publicity. The journal is published monthly as twelve issues per year by International Frequency Sensor Association (IFSA). In additional, some special sponsored and conference issues published annually. *Sensors & Transducers Journal* is indexed and abstracted very quickly by Chemical Abstracts, IndexCopernicus Journals Master List, Open J-Gate, Google Scholar, etc. Since 2011 the journal is covered and indexed (including a Scopus, Embase, Engineering Village and Reaxys) in Elsevier products.

Topics Covered

Contributions are invited on all aspects of research, development and application of the science and technology of sensors, transducers and sensor instrumentations. Topics include, but are not restricted to:

- Physical, chemical and biosensors;
- Digital, frequency, period, duty-cycle, time interval, PWM, pulse number output sensors and transducers;
- Theory, principles, effects, design, standardization and modeling;
- Smart sensors and systems;
- Sensor instrumentation;
- Virtual instruments;
- Sensors interfaces, buses and networks;
- Signal processing;
- Frequency (period, duty-cycle)-to-digital converters, ADC;
- Technologies and materials;
- Nanosensors;
- Microsystems;
- Applications.

Submission of papers

Articles should be written in English. Authors are invited to submit by e-mail editor@sensorsportal.com 8-14 pages article (including abstract, illustrations (color or grayscale), photos and references) in both: MS Word (doc) and Acrobat (pdf) formats. Detailed preparation instructions, paper example and template of manuscript are available from the journal's webpage: http://www.sensorsportal.com/HTML/DIGEST/Submition.htm Authors must follow the instructions strictly when submitting their manuscripts.

Advertising Information

Advertising orders and enquires may be sent to sales@sensorsportal.com Please download also our media kit: http://www.sensorsportal.com/DOWNLOADS/Media_Kit_2012.pdf