**Indonesian Journal of Electrical Engineering and Informatics (IJEEI)**
Vol. 3, No. 3, September 2015, pp. 150~156
ISSN: 2089-3272


# Modelling of a Trust and Reputation Model in Wireless Networks

**Saurabh Mishra**
Department of Electronics and Communication Engineering
Invertis University, Bareilly, Uttar Pradesh 243123, India
Email: saurabhmishra.er@gmail.com

***Abstract***

*Security is the major challenge for Wireless Sensor Networks (WSNs). The sensor nodes are deployed in non controlled environment, facing the danger of information leakage, adversary attacks and other threats. Trust and Reputation models are solutions for this problem and to identify malicious, selfish and compromised nodes. This paper aims to evaluate varying collusion effect with respect to static (SW), dynamic (DW), static with collusion (SWC), dynamic with collusion (DWC) and oscillating wireless sensor networks to derive the joint resultant of Eigen Trust Model. An attempt has been made for the same by comparing aforementioned networks that are purely dedicated to protect the WSNs from adversary attacks and maintain the security issues. The comparison has been made with respect to accuracy and path length and founded that, collusion for wireless sensor networks seems intractable with the static and dynamic WSNs when varied with specified number of fraudulent nodes in the scenario. Additionally, it consumes more energy and resources in oscillating and collusive environments.*

***Keywords:*** *WSNs, static wireless (SW), dynamic wireless (DW), trust and reputation models (TRMs), malicious nodes.*

## 1. Introduction

Past several years have witnessed a great success of wireless sensor networks (WSNs). As an emerging and promising technology, WSNs have been widely used in a variety of long term and critical applications including event detection, target tracking, monitoring, and localization. In recent years, the basic ideas of trust and reputation have been applied to WSNs to monitor the changing behaviors of nodes in a network. Several trust and reputation monitoring (TRM) systems have been proposed, to integrate the concepts of trust in networks as an additional security measure, and various surveys are conducted on the aforementioned system. However, the existing surveys lack a comprehensive discussion on trust application specific to the WSNs. This survey attempts to provide a thorough understanding of trust and reputation as well as their applications in the context of WSNs. The survey discusses the components required to build a TRM and the trust computation phases explained with a study of various security attacks. The sensor networks are constructed by a large number of nodes with ultra-low power computation and communication units [1]. An adversary can control a sensor node undetectably by physically compromising the node and use the captured nodes to inject faulty or false data into the network system disturbing the normal cooperation among nodes. Authentication and cryptographic mechanisms alone cannot be used to full solve this problem because internal adversarial nodes will have valid cryptographic keys to access the other nodes of the networks. Many existing approaches at most concentrate on cryptography to improve data authentication and integrity but this addresses only a part of the security problem without consideration for high energy consumption. Monitoring behavior of node neighbors using reputation and trust models improves the security of WSNs and maximizes the lifetime for it. However, a few of previous studies take into consideration security threats and energy consumption at the same time. WSNs serve to gather data and to monitor and detect events by providing coverage and message forwarding to base station. However, the inherent characteristics of a sensor network limit its performance and sensor nodes are supposed to be low-cost. An attacker can control a sensor node undetectably by physically exposing the node and an adversary can potentially insert faulty data or misbehavior to deceive the WSNs. Authentication mechanisms and cryptographic methods alone cannot be used to completely solve this problem because internal malicious nodes will have valid cryptographic keys to

*Received January 6, 2015; Revised May 29, 2015; Accepted June 14, 2015*

access the other nodes of the networks. Also conventional security methods cannot be used for WSNs due to power and processing limitations. Recently, a new mechanism has been offered for WSNs security improvement. This mechanism relies on constructing trust systems through analysis of nodes observation about other nodes in the network [2, 3]. A sensor node is always at risk of being compromised by an adversary, who may capture the node's cryptographic keys. Such an attack is also referred as insider attack [5] in which an adversary node would appear to be a legitimate member of the network. Once a sensor node is captured, an adversary may sniff and inject packets with falsified data that may compromise the node's data integrity. Therefore, security and privacy challenges of WSN must be addressed to prevent the system from turning against those for whom the system has to render benefit. Although external security attacks on WSN may be countered by the use of cryptographic techniques, cryptography is not that effective against the internal insider attacks by the malicious node. One approach that has gained global recognition in providing an additional means of security for decision making in WSNs (i.e., to trust a node for communication or not) is the trust and reputation monitoring (TRM) system. TRM deals with the problem of uncertainty in decision making, by keeping the history of a node's previous behavior (repute). A node is trusted and will be forwarded with the packets only if the node holds a good repute; otherwise, the node will be considered untrustworthy. TRM provides a natural choice for security in open systems, the Internet and social networking for being computationally tractable.

## 2. Background of Trust and Reputation Models

This section reports surveys of five trust and reputation models briefly with the work on wireless sensor networks.

**Eigen Trust Model:** It is one of the most commonly used trust and reputation models in the wireless sensor network domain. Kamvar et al. [4] evaluated this model on the basis of the peer's history of contributions by assigning a unique global trust value in the peer-to-peer file system for each peer [5, 6]. Further into this model, the authors define $Sij$ as the local trust of peer $i$ about peer $j$, in the following Equation (1):

$$Sij = \text{sat}(i, j) - \text{unsat}(i, j) \quad (1)$$

Equation (1) shows the difference between satisfactory and unsatisfactory interaction between peers: $(i, j)$. Further, the authors define normalized local trust value in Equation (2):

$$Cij = \max(Sij, 0)/\Sigma j \max(Sij, 0) \quad (2)$$

The above equation ensures that all the value lies in between 0 and 1.

**Peer Trust Model:** In this model many aspects related to the trust and reputation management such as the feedback a peer receives from other peers, the total number of transactions of a peer, the credibility of the recommendations given by a peer, the transaction context factor and the community context factor are combined.

**Bio-inspired Trust and Reputation Model (BTRM-WSN):** This model for wireless sensor networks is based on the bio-inspired algorithm of ant colony system. In this model, most trustworthy path leads to finding the most reputable service provider in a network.WSN launches a set of artificial agents while searching for a most reputable service provider.

**LFTM Model:** This linguistic fuzzy trust model uses the concept of fuzzy reasoning. On one hand, it uses the representation power of linguistically labeled as fuzzy sets for the satisfaction of a client or the goodness of a server. On the other hand, it remains affected by the inference power of fuzzy logic, as in the imprecise dependencies between the originally requested service and the actual received one, or the punishment to apply in case of fraud. The expected result will be an easily interpretable system with adequate performance. In this model, a set of linguistic labels describing several levels of a variable or concept could be associated with a fuzzy set. The resultant set constitutes linguistic labels such as VERY LOW, LOW, MEDIUM, HIGH and VERY HIGH. These defined fuzzy sets associated with such labels specify the level of client satisfaction.

## 3. Modified Trust and Reputation Models

To choose accurate trust and reputation models remains the top priority for the performance assessment of wireless sensor networks. Optimal trust and reputation models enhance the performance of the overall system about information dissemination, but the wireless sensor network system may not be dependent on the same. A simple trust and reputation modeling strategy may give the best result for a single instance but we have to deploy such efficient trust and reputation modeling strategies that provide optimal results in data dissemination. The improper modeling strategy may overload the entire network and consume more resources both in terms of energy and computation which result in the entire system performance degradation [14]. There always remains dire influence of trust and reputation strategy on the entire operating environment when evaluating a specific wireless sensor network. The goal which remains there are to carefully choose and examine the trust and reputation modeling strategies for information dissemination and present an optimal result without compromising any constraints than the expected outcome. Therefore, a typical realization should be required to access the scope of a particular trust and reputation model strategy for the wireless sensor networks. In our analysis, we consider ten networks composed of two hundred sensor nodes, each for twenty scenarios in two-dimensional fields. Sensor nodes in a cluster with a specific radio range transmit the data to the cluster head and then to the base station within the entire network. Network deployment focuses on collusion and oscillating conditions.

Although any trust and reputation sensor node strategy can be used in our model, we used Eigen trust model with static, dynamic and oscillating wireless sensor network for our proposed framework. Static wireless sensor network can be referred to as a mode of communication where the position of all the nodes remains stationary, whereas in case of dynamic wireless sensor network, the nodes can change their positions in an accord manner. Accordingly, for a given network with static and dynamic wireless sensor network and trust and reputation models node strategy described above, we are interested in finding the following two problems: (i) what is the influence of variation of collusion on static and dynamic communication node operations in the wireless sensor networks and (ii) how the varying collusive environment affects the accuracy and path length for different modes of Eigen trust and reputation model in wireless sensor network.

### 3.1. Simulation for Related Research

Although there is much research work conducted in application of trust and reputation in various network domains, the task is still in evolutionary phases in the case of WSNs, where node security is the biggest challenge because of low resources of node. Every proposed TRM has some limitations and covers only a subset of various issues and challenges in providing complete security to a WSN. Some of the issues for future research can be considered in the field of TRMs, which are discussed in the subsequent paragraphs.

In a few TRMs, to survive in the network, a node must continuously contribute to the network traffic. Nodes in the low activity areas of a network may suffer because of their gradual decrease in reputation. Therefore, a mechanism must be devised to keep the repute above a threshold in such low activity areas.

In most of the trust models, a node calculates the direct trust through promiscuous learning mode. However, when directional antennas are used, the technique becomes difficult to implement. Similarly, noise may be another factor that can cause hindrances to watchdog mechanisms [14].

Most of the TRMs that we discussed in this survey use a flooding approach for trust information dissemination, and this may lead to high traffic over the network. With the addition of more nodes in the network, the performance may further degrade. Therefore, an optimal trust and reputation modeling strategy may give the best result for a single instance but we have to deploy such efficient trust and reputation modeling strategies that provide optimal results in data dissemination. The improper modeling strategy may overload the entire network and consume more resources both in terms of energy and computation which result in the entire system performance degradation.

We focused on two parametric aspects, namely: accuracy and path length for information dissemination in wireless sensor networks. For this, we have developed the unmitigated scenario pinpointing two main targets. Firstly, we are interested in finding the value

of two above-mentioned parameters for static and dynamic wireless sensor network with and without collusion aspect. We want to know the summation of all the node operations with respect to collusion parameter. Lesser path length of node operation always gives due attention as it consumes fewer resources and exhibits more efficiency. Secondly, we want to make an estimation of the mobility effects on communication performance in correlation with the collusion for Eigen trust and reputation model. We designed a wireless sensor network template using the following parameters: 20% of all nodes in a randomly created WSN acted as clients where and the rest 80%of nodes acted as servers. Client nodes refer to the percentage of nodes which want to have or ask for services in a WSN. 5% of the nodes acted as relay servers which do not offer any services and act as relay nodes. The radio range of the nodes set at 10 hops to its neighbors. We consider a scenario where the percentage of fraudulent servers varied from 10% to 100% which specifies the indispensable condition for our WSN framework evaluation. Fraudulent servers depict the percentage of adversaries in a wireless sensor network. We set the minimum and maximum numbers of nodes that can create a WSN equal to 200.

Sensor nodes belonging to our developed networks spread over the area of 100m × 100 m. A total of ten networks were examined and the final results reflect the average value of all the networks. The process of searching trustworthy server was carried out ten times for each network.

### 3.2. Simulation Results

This section enables us to implement and evaluate Eigen trust and reputation model for different wireless sensor network modes. We used Java based event driven TRMSim-WSN simulator [9] version 0.5 for wireless sensor network allowing the researchers to simulate and represent random network distributions and provides statistics of different data dissemination policies including the provision to test the different trust and reputation models' strategies. Many decisions, like static or dynamic or oscillating networks, a combination of dynamic and oscillatory networks, the percentage of fraudulent nodes, the percentage of nodes acting as clients or servers, and so forth, can be implemented and tested over it. The proposed model is tested on five different modes with varying fraudulent conditions. We reported a comprehensive analysis based on collusion with static and dynamic wireless sensor networks.

We collected data for two metrics, namely, accuracy and path length. We investigated the comparative analysis of different modes with oscillating, static WSN and dynamic in contrast with and without collusion parameter. Static node refers to the type of nodes whose position remains fixed and whereas the dynamic node can be mobile in the network. We considered five WSN modes, namely, (i) Static WSN (SW) (ii) Static WSN with collusion (SWC) (iii) Dynamic WSN (DW) (iv) Dynamic WSN with collusion (DWC) (v) Oscillating WSN.

***Accuracy:*** The term accuracy in the trust and reputation systems may be defined as the selected percentage of trustworthy nodes. We calculated accuracy parameter in terms of their current and average values. Current accuracy denotes the trustworthiness value calculated for the last node, whereas average accuracy presents the value of all nodes available in the mentioned framework. We calculated current and average accuracy corresponds to different WSN modes for Eigen Trust model. According to Figure 1, for 10% of fraudulent environment, the value of current accuracy is highest in case of static WSN as compared to the rest of the WSN modes and lowest in case of dynamic WSN because of the fact that static nodes are less prone to failure than the dynamic as well as the combination of static and dynamic WSN with collusion aspect. The value of current accuracy remains highest in case of DWC mode as compared to the rest of the WSN modes for 20%, 30%, 40% and 70% of fraudulent environment and lowest in case of dynamic, static and static with collusion WSN for the same environment. For maximum collusive network this value is lowest in case of static WSN and highest for SWC mode.

Next, we considered the second evaluation for average accuracy with the same WSN framework. According to Figure 2, again average accuracy shows that the value of average accuracy remains highest for 10%, 30% and 40% fraudulent environment in case of dynamic WSN than the rest of the WSN modes. For static WSN (SW), this value remains lowest, when malicious server strength is 20%, 30% and 50%. In case of static with collusion (SWC) WSN it is highest in extreme fraudulent environment and lowest when malicious nodes percentage is 40%. The value is highest in case of dynamic WSN with collusion (DWC) mode for 50%, 60% and 70% collusive environment in the Eigen trust model. The oscillating mode outperforms the

rest of the modes in average accuracy values. In this mode average accuracy is highest at 80% and lowest at 60% and 70%.

***Path Length:*** The next parameter of our concern is path length which can be defined as the number of resources a particular network utilizes with a particular trust and reputation model. In the consistent pattern of accuracy evaluation types, we evaluated the current and average path length on the similar pattern of accuracy for all the WSN modes. Current path length depicts the resource utilization value calculated for the last node, whereas average path length exhibits the value of all nodes present in the scenario. Figure 3 and 4 represent the value of current and average path length which remains quiet in case of dynamic (DW) WSN and dynamic with collusion (DWC) WSN for both the current and average case viewpoints than other modes. Among the rest of the modes, oscillating and static (SW) mode consumes lesser path length than the rest of the modes in the case of 30% and 80% fraudulent environment for current accuracy, whereas the SWC mode for average accuracy utilizes the minimum path length for 70% fraudulent servers. We also observed that oscillating mode utilizes the maximum path length for 40% to 60% strength of malicious servers.

We proposed a more robust framework subsuming different WSN versus collusion scalability on a single platform.

We enhanced the contribution to a certain extent by incorporating collusion and oscillation parameters for wireless sensor network evaluation making our investigation more robust and real time.

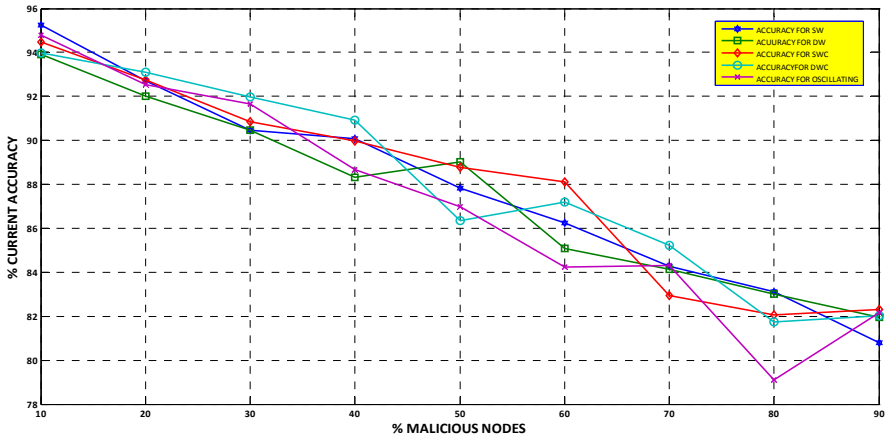


Figure 1. Current accuracy of different WSN modes with varying fraudulent WSN for Eigen trust and reputation model

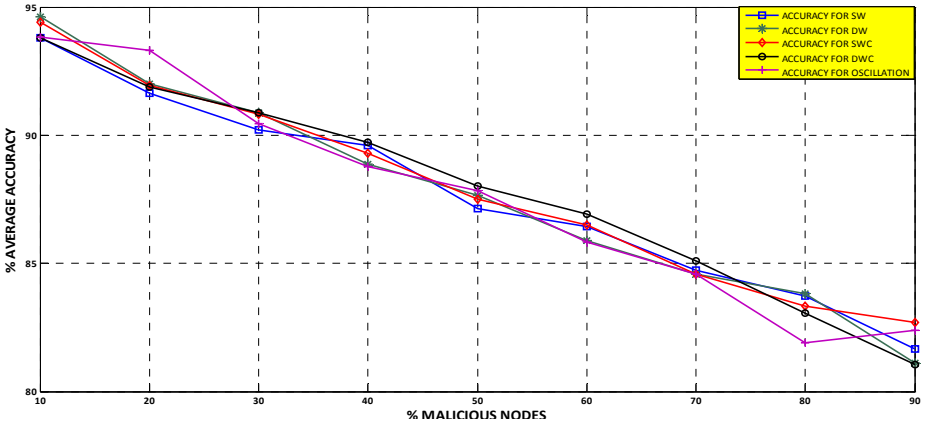


Figure 2. Average accuracy of different WSN modes with varying fraudulent WSN for Eigen trust and reputation model

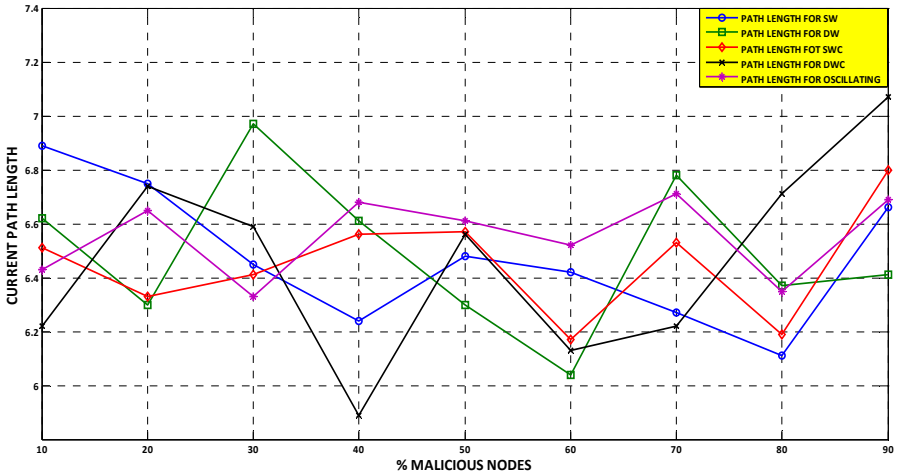


Figure 3. Current path length of different WSN modes with Eigen trust mode

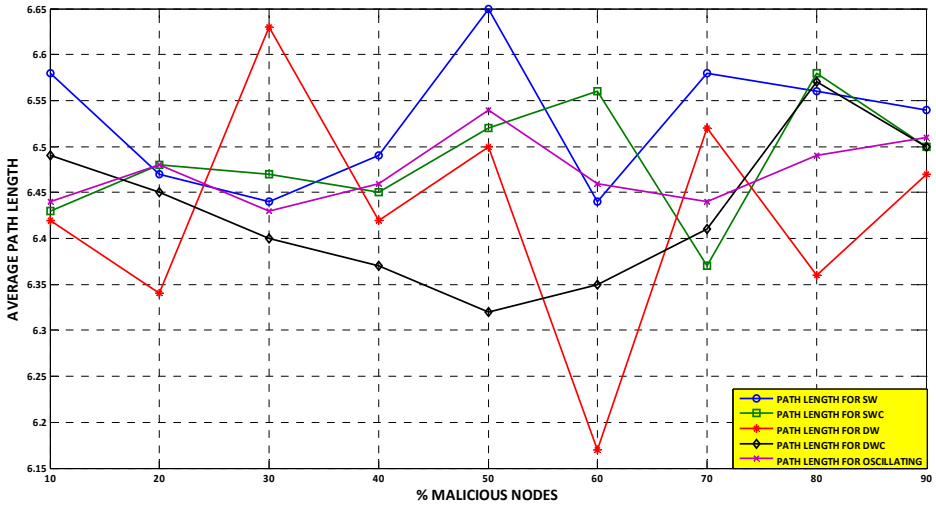


Figure 4. Average path length of different WSN modes with Eigen trust model

## 4. Conclusion

Trust is an important tool for self-configuring and autonomous systems, such as WSNs, to make effective decisions in detecting a misbehaving node. The task of establishing trust and reputation becomes more challenging when the nodes are mobile. This paper concluded the impact of varying collusion on different trust and reputation modes in wireless sensor networks. We have observed the effect of collusion for static, dynamic, collusive and oscillating sensor nodes in a WSN framework. It is evident from the simulation that there is a strong relationship between collusion and WSN modes in trust and reputation model evaluation. We evaluated a wireless sensor network framework for varying collusion aspect with reference to two performance metrics, namely: accuracy and path length viewpoint. We estimated accuracy and path length in terms of overall percentage of the functionality for sensor node operations. The performance of the WSN system changes along with the different WSN modes and strength of collusion present in the scenario. We mainly concentrated toward the comparative evaluation of static, dynamic, oscillating and collusive WSN modes deployed in our designed model. Our research work presented a comprehensive investigation over collusion parameters with Eigen trust and reputation model. We stressed on two major directions. Firstly, we evaluated accuracy and path length for collusive and non collusive modes of wireless sensor networks. Secondly,

we investigated the entire framework for comparative evaluation of above-discussed modes. We observed that with the collusion adoption in the WSN modes, the result becomes much steeper that is, performance degradation. In case of static nodes, the collusion affects less to WSN when it is incorporated in dynamic mode. Also, node operations remain more in case of collusion than without it. From this investigation, we can predict that the lesser the collusive nodes the more the probability of accuracy, the better resource utilization of the entire WSN will be exhibited by the wireless sensor network system.

In the future, we would like to develop further trust and reputation models in our evaluation as well as work towards additions on newer distribution strategies for the wireless sensor network domain.

## References

[1] S Farahani. Zig Bee Wireless Networks and Transceivers. Oxford, UK: Elsevier. 2008.
[2] A Alkalbani, T Mantoro, AO Md Tap. *Improving the lifetime of wireless sensor networks based on routing power factors.* In Networked Digital Technologies of Communications in Computer and Information Science. Springer, Berlin, Germany. 2012; 293: 565-576.
[3] H Chen, H Wu, X Zhou, C Gao. *Reputation-based trust in wireless sensor networks.* In Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE'07). Seoul, Republic of Korea. 2007: 603–607.
[4] M Dorigo, L Gambardella, M Birattari, A Martinoli, R Poli, T St¨utzle. Ant Colony Optimization and Swarm Intelligence. *Computer Science*. Springer, Berlin, Germany. 2006; 4150.
[5] O Cord´on, F Herrera, T. St¨utzle. A review on the ant colony optimization meta heuristic: basis, models and new trends. *Mathware & Soft Computing.* 2002; 9(2-3): 141-175.
[6] M Dorigo, T St¨utzle. Ant Colony Optimization. Bradford Book. 2004.
[7] FG M´armol, GM P´erez. Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication Systems.* 2011; 46(2): 163-180.
[8] FG M´armol, GM P´erez. TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications.* 2012; 35(3): 934-941.
[9] FG M´armol, GM P´erez. *TRMSim-WSN, trust and reputation models simulator for wireless sensor networks.* In Proceedings of the IEEE International Conference on Communications (ICC '2009). Dresden, Germany. 2009: 1-5.
[10] VK Verma, S Singh, NP Pathak. Analysis of scalability for AODV routing protocol in wireless sensor networks. *Optik—International Journal for Light and Electron Optics.* 2014; 125(2): 748-750.
[11] AS Alkalbani, AO Md Tap, T Mantoro. *Energy consumption evaluation in trust and reputation models for wireless sensor networks.* In Proceedings of the 5th International Conference on Information and Communication Technology for the Muslim World. Rabat, Morocco. 2013: 1-6.
[12] S Chen, Y Zhang, G Yang. Parameter-estimation based Trust model for unstructured peer-to-peer networks. *IET Communications.* 2011; 5(7): 922–928.
[13] Y Pan, Y Yu, L Yan. An improved trust model based on interactive ant algorithms and its applications in wireless sensor networks. *International Journal of Distributed Sensor Networks.* 2013; 2013: 9.
[14] OP Sahu, Tarun Dubey. A Fault Tolerant Topology for Reliable Data Forwarding in Localized Wireless Sensor Network. *Journal of Instrument Society of India.* 2011; 41(4): 245-247.