Research Article

Collusion Based Realization of Trust and Reputation Models in Extreme Fraudulent Environment over Static and Dynamic Wireless Sensor Networks

Vinod Kumar Verma, 1 Surinder Singh, 2 and N. P. Pathak 3

1 Department of Computer Science & Engineering, Sant Longowal Institute of Engineering & Technology, Longowal 148106, India
2 Department of Electronics & Communication Engineering, Sant Longowal Institute of Engineering & Technology, Longowal 148106, India
3 Department of Electronics & Communication Engineering, IIT, Roorkee 247667, India

Correspondence should be addressed to Surinder Singh; surinder_sodhi@rediffmail.com

Received 11 November 2013; Accepted 26 March 2014; Published 26 May 2014

Abstract

We derive a new representation for the collusive sensor nodes when the underlying fraudulent correlated environment has strong influence on wireless sensor networks performance. We have evaluated collusion effect with respect to static (SW) and dynamic (DW) wireless sensor networks to derive the joint resultant. Moreover accuracy, path length, and energy consumption of sensor node operations are also evaluated. Additionally, we emphasized over the satisfaction evaluation for linguistic fuzzy trust and reputation (LFTM) models in the deployed WSN framework. Finally, simulation analysis has been carried out to prove the validity of our proposal. However, collusion for wireless sensor networks seems intractable with the static and dynamic WSNs when varied with specified number of fraudulent nodes in the scenario.

1. Introduction

Rapid development in the area of communications through wireless sensor networks (WSN) attracted more attention of scientists and researchers over the last few years [1]. Wireless sensors are small-sized devices equipped with radio transceivers and low power batteries. Typical features of sensor node include power, storage, and low cost computational capability hardware [2, 3]. A wireless sensor network is designed to sense, collect, process, and transmit event specific information in order to accomplish a distributed domain task. Moreover wireless sensor networks [4, 5] are the type of networks where the resultant is fully based on the sensor nodes cooperation. The potential of wireless sensor networks can be equally deployed in the wider area of applications such as defense equipment, ecological and habitat monitoring, industrial process control, home automation, weather forecasting, health care system, traffic control, and civilian applications. Usually wireless sensor networks are deployed in an open informant where the probability of an adversary [6] always remains more than in a closed environment. These malicious nodes may spread wrong information on the entire network which results in overall system performance degradation. Therefore, it is quite mandatory to identify the collusive nodes and punish them in an accord manner. There are numerous proposals to detect an adversary node in the wireless sensor networks. Traditional means to protect a network include cryptography specific techniques and methodologies. Complex computations in the cryptography strategies [7] become its major drawbacks and made these policies unsuitable to be deployed in wireless sensor network which constitutes severe power constraints. Some lightweight cryptographic mechanisms are available in the literature, but they are not serving the goal in entirety. Therefore, there remains a dire need to probe for wireless sensor network reliability aspect and search some complementary means to incorporate more faith in the overall scenario. Trust and reputation models are the solution for the given problem to adhere to reliability in the wireless sensor networks. This is the reason why research on trust and reputation models has
gained considerable momentum in the last few years. Many trust and reputation models have been proposed in the past. Some of them were centered around secure routing, data aggregation, cluster head selection, and synchronized trust management [8–10] but still there is need to address various issues like collusion, scalability, mobility, and computability in the wireless sensor networks. At present, most of the trust evaluation frameworks belong to an algorithm based methodology, over which entire behavior of nodes depends on accuracy, resource usability, and energy consumption. It is therefore necessary to concentrate on these issues in parallel with their performance and some real time aspects like collusion and fraudulent environment. Collusion can be referred to as a specific level of probability with which every malicious server will assign maximum rating to other malicious servers and minimum rating to the benevolent server. As a result, the most obedient node will become unable to contribute its services to the WSN system for most of the times, which further severely affect the overall system performance. Presence of malicious servers in the wireless sensor networks is the major and real root cause behind the collusion parameter. Therefore the specific issue like collusion must be addressed to enhance the capability of the entire WSN framework. So, we selected five popular trust and reputation models for their comparison and evaluation in terms of accuracy, path length, satisfaction, and energy consumption. This research focuses on the collusion issue and presented our analysis in the extreme fraudulent environment.

Section 2 reported surveys of five trust and reputation models with prior work on wireless sensor networks. Section 3 highlights our motivation for research work. Section 4 presented the problem definition and system model. Section 5 describes the detailed design of our experimental setup. Simulation results and validations are presented and discussed in Section 6. Finally, conclusions are made in Section 7.

2. Trust and Reputation Models with Related Prior Work

This section provides the background and related work on trust and reputation models in wireless sensor network with assumptions required for the designed frameworks for the later sections.

2.1. Eigen Trust Model. It is one of the most commonly used trust and reputation models in the wireless sensor network domain. Kamvar et al. [11] 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 [12, 13]. Further into this model, the authors define $S_{ij}$ as the local trust of peer $i$ about peer $j$, in the following manner: $S_{ij} = \text{sat}(i, j) - \text{unsat}(i, j)$. It shows the difference between satisfactory and unsatisfactory interaction between peers: $(i, j)$. Further, the authors define normalized local trust value,

$$C_{ij} = \frac{\max(S_{ij}, 0)}{\sum_j \max(S_{ij}, 0)}.$$  

(1)

It ensures that all the value lies in between 0 and 1. The authors also introduced aggregated local trust value which is defined as $t_{jk} = \sum_i C_{ij} C_{jk}$, where $t_k$ represents the trust that peer $i$ places in peer $k$ based on friends information. This model also incorporates three practical issues like a priori notion of trust, inactive peers, and malicious collectives. First of all, in the presence of malicious peers, $t = (C^T)^n p$ will generally converge faster than $t = (C^T)^n e$, so we use $p$ as our start vector. In the case of inactive peers, $C_{ij}$ refined as

$$C_{ij} = \begin{cases} \frac{\max(S_{ij}, 0)}{\sum_j \max(S_{ij}, 0)} & \text{if } \max(S_{ij}, 0) \neq 0; \\ P_j & \text{otherwise} \end{cases}$$  

(2)

The malicious collectives issue was addressed by the following equation in this model:

$$t^{(k+1)} = (1 - a)C^T t^{(k)} + ap \quad \text{where } a < 1.$$  

(3)

2.2. Peer Trust Model. Xiong and Liu [14] in this model combine 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. The trust value of peer $u$, $T(u)$ is represented by the following expression:

$$T(u) = \alpha \sum_{i=1}^{I(u)} S(u, i) C R(p(u, i) TF(u, i) + \beta CF(u)),$$  

(4)

where $I(u)$ represents total number of transactions performed by peer $u$ with all other peers, $p(u, i)$ represents other participating peer in peer $u$’s $i$th transaction, $S(u, i)$ represents normalized amount of satisfaction peer $u$ receives from $p(u, i)$ in its $i$th transaction, $CR(v)$ represents credibility of the feedback submitted by $v$, $TF(u, i)$ represents adaptive transaction context factor for peer $u$’s $i$th transaction, and $CF(u)$ represents adaptive community context factor for peer $u$. On the other hand, the credibility of $v$ from $w$’s point of view is computed as

$$Cr(p(u, i), w) = \frac{\text{Sim}(p(u, i), w)}{\sum_{j=1}^{I(u)} \text{Sim}(p(u, j), w)},$$  

(5)

where

$$\text{Sim}(v, w) = 1 - \left( \sum_{x \in IJS(v, w)} \left( \frac{\sum_{j=1}^{I(x, v)} \text{Sim}(x, i)}{I(x, v)} - \frac{\sum_{j=1}^{I(x, w)} \text{Sim}(x, i)}{I(x, w)} \right)^2 \right)^{1/2}.$$  

(6)
\( I(u, v) \) represents the total number of transactions performed by peer \( u \) with peer \( v \), \( IS(v) \) represents a set of peers that have interacted with peer \( v \), and \( IJS(v, w) \) denotes a common set of peers which interacted with peers \( v \) and \( w \) for \( IS(v) \cap IS(w) \) computation. The stimulation for the community incentive or rewards is done through the context factor, with the following expression: \( CF(u) = F(u)/I(u) \), where \( F(u) \) represents the total number of feedback peer \( u \) gives to others.

2.3. Bioinspired Trust and Reputation Model (BTRM-WSN). This model for wireless sensor networks is based on the bioinspired algorithm of ant colony system [15–19]. 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. In order to carry out a decision about next sensor, a probability is given to each arc by the following expression:

\[
p_{k}(r,s) = \frac{[\tau_{r,s}]^{\alpha}[\eta_{r,s}]^{\beta}}{\sum_{l \in J_{k}(r)}[\tau_{r,l}]^{\alpha}[\eta_{r,l}]^{\beta}} \quad \text{if } s \in J_{k}(r); \\
0 \quad \text{otherwise}
\]

The following equation represents modification of the ants [20] pheromone trace:

\[
\tau_{r,s} = (1 - \varphi)\tau_{r,s} + \varphi\Omega,
\]
where \( \Omega = (1 + (1 - \varphi)(1 - \tau_{r,s}^{2}\eta_{r,s}^{2}))\tau_{r,s} \) denotes the convergence value of \( \tau_{r,s} \) and \( \varphi \) represents a parameter controlling the amount of pheromone. The best path found by all ants is given by

\[
\tau_{s} = (1 - \rho)\tau_{r,s} + \rho \left( 1 + \tau_{r,s}Q \left( S_{\text{Globaladj}} \right) \right)\tau_{r,s},
\]
where \( Q(S_{\text{Globaladj}}) \) denotes path quality. The quality of the \( S_{k} \) paths can be measured as the average of all the edges belonging to that path

\[
Q(S_{k}) = \frac{\tau_{k}}{\text{Length}(S_{k})}\%A_{k},
\]
where \( \%A_{k} \) denotes the percentage of trustworthy paths. The punishment or rewards of the path leading to the selected peer are given by

\[
\tau_{rs} = (\tau_{rs} - \varphi \times df_{rs}) \frac{\text{Sat}}{df_{rs}}.
\]

The distance factor joining the link between sensor \( r \) and \( s \) is given by the following equation:

\[
df_{rs} = \sqrt{\frac{df_{rs}}{L(S_{r})L(S_{s}) - d_{rs} + 1}}.
\]

2.4. LFTM Model. This linguistic fuzzy trust model [21] 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.

2.5. Trust and Reputation Infrastructure Based Proposal (TRIP) Models. This model is based on the environment specific issues like infrastructure, area, density, and so forth, within the specified conditions [22]. Every time a node receives a signal from the other node, it assesses the reputation of the node in order to reject or drop the message based on the trustworthiness of that node. Each message depicts its actual level of importance or risk. Even the harmful message will not affect the system because of the fact that each message constitutes its trust level. The higher the trust level, the better the probability for its selection. Additionally, a reputation score calculation for each message is based on three different aspects, namely, (i) information directly from the targets, (ii) information from neighbor nodes, and (iii) information from the central unit. Informational database from all the three sources can be stored in the central unit. Finally, taking into consideration the entire information the best and appropriate decision can be easily taken.

3. Motivation for Current Work

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. 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 is 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.
4. Problem Definition and System Model

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 fraudulent conditions. Although any trust and reputation sensor node strategy can be used in our model, we used LFTM, BTRM, and peer trust model with static and dynamic 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 collusion on static and dynamic communication node operations in the wireless sensor networks and (ii) how collusion affects the accuracy, path length, and energy consumption for different trust and reputation models in wireless sensor network.

5. Detailed Setup

We focused on three parametric aspects, namely: accuracy, path length, and energy consumption 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 three above-mentioned parameters for static 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 different trust and reputation models. Finally, we made the comprehensive evaluation of energy consumption with static and dynamic wireless sensor networks in our proposed framework. 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 refers 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 remained 70% 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 100 m × 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. Table 1 shows the summary of parameters deployed in our model.

Figure 1 shows the setup of the simulation. In the simulation window, yellow dots denote client nodes, green dots represent the benevolent nodes, red dots denote malicious node, blue dots represent relay nodes, and black dot denotes idle nodes respectively.

6. Analytical Results and Validations

This section enables us to implement and evaluate trust and reputation models for different wireless sensor network modes. We used Java based event driven TRMSim-WSN simulator [23] 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 trust and reputation models with extreme fraudulent conditions. We reported a comprehensive analysis based on collusion with static and dynamic wireless sensor networks. We collected data for four metrics, namely, accuracy, path length, satisfaction, and energy consumption. We investigated the comparative analysis of trust and reputation models.
with 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 four WSN modes, namely, (i) static WSN (SW), (ii) static WSN with collusion (SWC), (iii) dynamic WSN (DW), and (iv) dynamic WSN with collusion (DWC). We denote Eigen trust model with value 1, peer trust model with 2, BTRM-WSN model with value 3, LFTM with value 4, and TRIP model with value 5. The outcome of the simulations will be subject to the following subsections.

6.1. 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. Initially, we calculated average accuracy correspond to different trust and reputation models as reported in Figure 2. The value of current accuracy remains highest in case of static WSN as compared to the rest of the WSN modes 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.

Next, we considered the second evaluation for average accuracy with the same WSN framework. According to Figure 3, again average accuracy shows the similar behavior with the current accuracy in Figure 2 above as the value of average accuracy remains highest in case of static WSN than the rest of the WSN modes. For static WSN (SW) and dynamic WSN (DW) modes, the value of current and average accuracy remains highest in LFTM model than other models in most fraudulent conditions, whereas TRIP model depicts the minimum value. In case of static WSN with collusion (SWC) and dynamic WSN with collusion (DWC) mode, the Eigen trust model outperforms the rest of the models in current and average accuracy values, whereas peer trust model shows minimum accuracy value. We have also presented the scalability impact on the wireless sensor network [24]. We enhanced this evaluation towards a bit of an intricate assessment by incorporating collusion, malicious servers, resource utilization, satisfaction, and energy evaluation aspect on a single platform. One common point we have noticed is that there is severe effect of collusion and mobility of nodes on the accuracy of WSN system, as the accuracy declines to a bit of an intricate level when a node changes its state from static to dynamic.

6.2. 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. Figures 4 and 5 represent the value of current and average path length which remains quiet in case of TRIP model for both the current and average case viewpoints than other models. This is due to the fact that the TRIP model constitutes the fixed infrastructure for its functionality resulting in lesser path length as compared to other models. Among the rest of the models, LFTM model consumes lesser path length than the rest of the models in the case of SW mode and DW mode, whereas the SWC and DWC modes of BTRM utilize the minimum path length.

We also observed that BTRM utilizes the maximum path length of all the SW, SWC, DW, and DWC WSN modes. This shows the excellent agreement with the results reported
in reference [25]. An initiative towards the description of energy consumption analysis for different trust and reputation models was proposed in reference [25]. We enhanced this evolution towards a bit of a complex assessment by incorporating collusion, satisfaction, and energy evaluation aspect in our scenario. Moreover in the later energy consumption subsection we proposed a mathematical equation for overall energy consumption which adds more robustness in our evaluation.

We proposed a more robust framework subsuming different WSN versus collusion scalability on a single platform. Xiong and Liu [14] reported peer-to-peer trust and reputation based model for structured peer-to-peer networks including strategies for their implementation and evaluation in decentralized environmental conditions. Also, Xiong and Liu [14] emphasized over trust metric in order to assess trustworthiness, feedback, and credibility of peer-to-peer networks. Specifically, unstructured peer-to-peer networks based on parameters were proposed by Chen et al. [26]. We enhanced the contribution to a certain extent by incorporating collusion, satisfaction, and energy consumption parameters for wireless sensor network evaluation making our investigation more robust and real time.

6.3. Satisfaction. Additionally, we calculated the satisfaction level of different WSN modes for LFTM model as shown in Figure 6. In the context of trust and reputation models, satisfaction can be defined as a particular level of subjectivity up to a specific degree in which the system can behave as per desired goal for mentioned probability. The observation shows that in the static mode satisfaction level is very high as compared to the rest of WSN modes, whereas incorporation of collusion to SW and DW modes decreases its value.

6.4. Energy Concerns. One of the major issues, when dealing with the wireless sensor network, is energy consumption. So, lastly we emphasized on the average energy consumption by SW, SWC, DW, and DWC modes of five trust and reputation models in wireless sensor networks. The power requirement of a sensor node can be analyzed as a function of distance as per the references [27, 28]. For most of the models, energy consumption $E$ by a message at a distance $d$ is given by [16, 29]

$$E (d) = d^\alpha + C,$$

(13)

where $\alpha$ represents attenuation factor and $C$ is constant used for radio signal and dimensionless.
Table 2: Energy consumption for trust and reputation models with WSN modes.

| WSN modes                        | Eigen trust (ml) | Peer trust (ml) | BTRM (ml) | LFTM (ml) | TRIP (ml) |
|----------------------------------|------------------|----------------|-----------|-----------|-----------|
| Static WSN (SW)                  | $8.2 \times 10^4$ | $8.7 \times 10^6$ | $4 \times 10^7$ | $2.5 \times 10^7$ | $4 \times 10^9$ |
| Static WSN with collision (SWC)  | $6.4 \times 10^4$ | $1.0 \times 10^7$ | $8 \times 10^7$ | $1.4 \times 10^8$ | $4 \times 10^9$ |
| Dynamic WSN (DW)                 | $5.1 \times 10^4$ | $3.2 \times 10^6$ | $1.1 \times 10^7$ | $1.2 \times 10^7$ | $4 \times 10^9$ |
| Dynamic WSN with collision (DWC) | $8.6 \times 10^4$ | $2.2 \times 10^6$ | $6.8 \times 10^7$ | $7.6 \times 10^7$ | $4 \times 10^9$ |

Table 2 compares the five trust and reputation models from the energy consumption aspect as shown below. Reference [30] reported a comparative analysis of the energy consumption with respect to sensors value increment.

In our proposal, we extended this concept towards the different WSN modes and simultaneously clubbing these modes with different trust and reputation models. We observed that the Eigen trust model consumes maximum power in all the SW, SWC, DW, and DWC modes, whereas TRIP model reported minimum energy consumption. We observed that more complexity involvement in the Eigen trust model is the reason for utmost energy consumption and in case of TRIP model energy consumption being the minimum because of the simpler computation involved in trust value computation. We also extended the mathematical relation as reported in references [27, 28] for the energy consumption for trust and reputation models in our framework

$$E_o = E_c + E_s + E_F + E_R + E_{sim},$$

(14)

where $E_o$ represents overall energy consumption, $E_c$ denotes client nodes energy consumption, $E_s$ depicts server nodes energy consumption, $E_F$ shows energy consumption for fraudulent node, $E_R$ denotes relay node energy consumption, and $E_{sim}$ denotes energy consumption used by the simulator.

Overall, we investigated the entire framework twenty times for different WSN modes and corresponding five trust and reputation models. One common thing we observed that is more complexity in any trust and reputation model attracts more resources utilization and power consumption. We added a variety of evaluation strategies based on accuracy, path length, satisfaction, and power consumption for sensor node operations in our proposed framework which make over a scenario more robust as compared to the approach reported by Pan et al. [31]. A new trust and reputation model by adding additional constraints to BTRM-WSN adopting an interactive multiple ant colony algorithm was also suggested in reference [31]. We extended the concept by adding more robust constraints like static, dynamic, collusive, and a combination of all these aspects on a single platform for the trust and reputation models investigations in wireless sensor networks. Qureshi et al. [20] presented FIRE trust and reputation model extension to detect and prevent direct interaction and validate interaction collusion attacks in wireless networks. We enhanced this concept of reference [20] for wireless sensor networks with collusion and satisfaction aspect evaluation with five trust and reputation models over wireless sensor networks. Our analysis shows that there remains always significant impact of collusion over static and dynamic mode of WSN, resulting in the performance degradation of the overall system.

7. Conclusions

This paper concluded the impact of collusion on different trust and reputation models in wireless sensor networks. We have observed the effect of collusion for static, dynamic, and collusive 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 collusion aspect with reference to four performance metrics, namely: accuracy, path length, satisfaction, and energy consumption viewpoint. We estimated accuracy and path length in terms of overall percentage of the functionality, whereas energy consumption in terms of millijoule specifically for sensor node operations. The performance of the WSN system changes along with the different WSN modes and collusion present in the scenario. We mainly concentrated toward the comparative evaluation of static, dynamic, and collusive WSN modes deployed in our designed model. Our research work presented a comprehensive investigation over collusion parameters with five trust and reputation models. We stressed on three major directions. Firstly, we evaluated accuracy, path length, satisfaction, and energy consumption for collusive and non-collusive modes of wireless sensor networks. Secondly, we investigated the entire framework for comparative evaluation of above-discussed trust and reputation models, and lastly the same model is deployed for the mathematical derivation of the energy equation of a wireless sensor network. 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, the adequate satisfaction level, and the lesser the energy consumption 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. Finally, this work allows us to analytically formulate investigative strategies under specified
scenarios and therefore provides insight for directing the designated model for wireless sensor network evolution.

**Conflict of Interests**

The authors declare that they have no conflict of interests regarding the publication of this paper.

**Acknowledgments**

The authors would like to thank the Department of Information and Communication Engineering, University of Murcia (Spain) [23], for TRMSim-WSN simulator for wireless sensor network which greatly supports them for their research work. Authors are also thankful to NetSim simulator developers. Additionally, they would like to thank the Department of Electronics and Communication engineering, Sant Longowal Institute of Engineering & Technology, Longowal, India, for providing them with Wireless SignalPro software which helps them in the final result preparation. Last but not least, the authors would like to thank the reviewers for their valuable suggestions which bring the paper in present form.

**References**

[1] S. Farahani, *ZigBee Wireless Networks and Transceivers*, Elsevier, Oxford, UK, 2008.

[2] A. Alkalbani, T. Mantoro, and A. O. Md. Tap, “Improving the lifetime of wireless sensor networks based on routing power factors,” in *Networked Digital Technologies*, vol. 293 of *Communications in Computer and Information Science*, pp. 565–576, Springer, Berlin, Germany, 2012.

[3] H. Chen, H. Wu, X. Zhou, and C. Gao, “ Reputation-based trust in wireless sensor networks,” in *Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE ’07)*, pp. 603–607, Seoul, Republic of Korea, April 2007.

[4] C.-Y. Chong and S. P. Kumar, “Sensor networks: evolution, opportunities, and challenges,” *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[6] J. Hurt, Y. Lee, H. Yoont, D. Choi, and S. Jin, “Trust evaluation model for wireless sensor networks,” in *Proceedings of the 7th International Conference on Advanced Communication Technology (ICACT ’05)*, pp. 491–496, Phoenix Park, Republic of Korea, February 2005.

[7] Q. Jing, L.-Y. Tang, and Z. Chen, “Trust management in wireless sensor networks,” *Journal of Software*, vol. 19, no. 7, pp. 1716–1730, 2008.

[8] J. Hur, Y. Lee, S. Hong, and H. Yoon, “Trust-based secure aggregation wireless sensor networks,” in *Proceedings of the 3rd International Conference on Computing, Communications and Control Technologies*, vol. 3, pp. 1–6, 2005.

[9] G. V. Crosby, N. Pissinou, and J. Gadze, “A framework for trust-based cluster head election in wireless sensor networks,” in *Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS ’06)*, pp. 13–22, Columbia, Md, USA, April 2006.

[10] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, “Information theoretic framework of trust modeling and evaluation for ad hoc networks,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 305–317, 2006.

[11] S. Kamvar, M. Schlosser, and H. Garcia-Molina, “The Eigen trust algorithm for reputation management in P2P networks,” in *Proceedings of the 12th International World Wide Web Conference (WWW ’03)*, Budapest, Hungary, May 2003.

[12] “Advogato’s trust metric (white paper),” 2000, http://www.advogato.org/trust-metric.html.

[13] J. Douceur, “The Sybil attack,” in *Proceedings of the First International Workshop on Peer-to-Peer Systems (IPTPS ’02)*, Cambridge, Mass, USA, March 2002.

[14] L. Xiong and L. Liu, “PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 7, pp. 843–857, 2004.

[15] M. Dorigo and L. M. Gambardella, “Ant colony system: a cooperative learning approach to the traveling salesman problem,” *IEEE Transactions on Evolutionary Computation*, vol. 1, no. 1, pp. 53–66, 1997.

[16] M. Dorigo, L. Gambardella, M. Birattari, A. Martinoli, R. Poli, and T. Stützle, *Ant Colony Optimization and Swarm Intelligence*, vol. 450 of *Lecture Notes in Computer Science*, Springer, Berlin, Germany, 2006.

[17] O. Cordón, F. Herrera, and T. Stützle, “A review on the ant colony optimization meta heuristic: basis, models and new trends,” *Mathware & Soft Computing*, vol. 9, no. 2–3, pp. 141–175, 2002.

[18] M. Dorigo and T. Stützle, *Ant Colony Optimization*, Bradford Book, 2004.

[19] F. G. Mármol and G. M. Pérez, “Providing trust in wireless sensor networks using a bio-inspired technique,” *Telecommunications Systems*, vol. 46, no. 2, pp. 163–180, 2011.

[20] B. Qureshi, G. Min, and D. Kouvatso, “Collusion detection and prevention with FIRE+ trust and reputation model,” in *Proceedings of the 10th IEEE International Conference on Computer and Information Technology (CIT ’10)*, pp. 2548–2555, July 2010.

[21] F. G. Marmol, J. G. Marin-Blazquez, and G. M. Perez, “Linguistic fuzzy logic enhancement of a trust mechanism for distributed networks,” in *Proceedings of the 10th IEEE International Conference on Computer and Information Technology*, pp. 838–845, Washington, DC, USA, July 2010.

[22] F. G. Mármol and G. M. Pérez, “TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks,” *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012.

[23] F. G. Mármol and G. M. Pérez, “TRMSim-WSN, trust and reputation models simulator for wireless sensor networks,” in *Proceedings of the IEEE International Conference on Communications (ICC ’09)*, pp. 1–5, Dresden, Germany, June 2009.

[24] V. K. Verma, S. Singh, and N. P. Pathak, “Analysis of scalability for AODV routing protocol in wireless sensor networks,” *Optik—International Journal for Light and Electron Optics*, vol. 125, no. 2, pp. 748–750, 2014.

[25] A. S. Alkalbani, A. O. Md. Tap, and 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*, pp. 1–6, Rabat, Morocco, March 2013.
[26] S. Chen, Y. Zhang, and G. Yang, “Parameter-estimation based trust model for unstructured peer-to-peer networks,” *IET Communications*, vol. 5, no. 7, pp. 922–928, 2011.

[27] L. Li and J. Y. Halpern, “Minimum-energy mobile wireless networks revisited,” in *Proceedings of the IEEE International Conference on Communications (ICC ’01)*, vol. 1, pp. 278–283, Helsinki, Finland, June 2001.

[28] J. A. Sánchez and P. M. Ruiz, “Improving delivery ratio and power efficiency in unicast geographic routing with a realistic physical layer for wireless sensor networks,” in *Proceedings of the 9th EUROMICRO Conference on Digital System Design: Architectures, Methods and Tools (DSD ’06)*, pp. 591–597, Dubrovnik, Croatia, September 2006.

[29] F. Li and Y. Wang, “Routing in vehicular ad hoc networks: a survey,” *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, 2007.

[30] F. G. Már mol and G. M. Pérez, “Providing trust in wireless sensor networks using a bio-inspired technique,” in *Proceedings of the Networking and Electronic Commerce Research Conference (NAEC ’08)*, Lake Garda, Italy, September 2008.

[31] Y. Pan, Y. Yu, and L. Yan, “An improved trust model based on interactive ant algorithms and its applications in wireless sensor networks,” *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 764064, 9 pages, 2013.
