International Journal of Informatics and Information System ISSN 2579-7069
Vol. 1, No. 2, December 2018, pp. 90-96

Pre-Trusted Peers Probability Influence on Eigen Trust and Reputation Model Over Peer to Peer Distributed Networks

Vinod Kumar Verma [1,*], Surinder Singh [2]

[1,2] Sant Longowal Institute of Engineering and Technology, Deemed University, India.
[1] vinod5881@gmail.com*; [2] surinder_sodhi@rediffmail.com;
* corresponding author

Abstract

This paper investigates the impact of peer pre-trusted probability on the performance of Eigen's trust and reputation model in distributed wireless networks. Design and develop models for rigorous Eigen Trust assessment and reputation models. In addition, we evaluate our model from performance-based factors namely: accuracy, resource utilization and energy consumption. Finally, the results obtained from our investigation are suggestive of implementation for real-time distributed wireless applications. our proposal.

Keywords: Eigen Model; Peers; Trust; Reputation; Distributed Networks;

1. Introduction

Security in real time application becomes the contemporary area of research nowadays. Numerous means have been suggested by researchers in the past to provide secure and reliable applications.Researchers are working for the assurance of adequate services expected through the distributed applications. Trust and reputation models are the innovative solutions that guarantee security services in distributed peer to peer networks. Some of the efforts in this direction are as follows. Aberer et al. [1] reported a trust and reputation approach based on the P-grid (i.e.decentralized storage method)for peer to peer networks. On the basis of first hand information exchanged frequently and second hand information merged, an approach based on Bayesian learning technique was suggested by Budded [2]. An approach excluding the individual interaction in the system was suggested by the Xiong and Liu [3]which were not suitable for large peer to peer system as computation convergence rate was not provided. In 2001, Sabater et al. [4] proposed multi-agent system for trust and reputations models. Different mechanisms have been proposed earlier for trust and reputation models in peer to peer networks [5] and ad-hoc networks [6]. The incorporation of fuzzy logic concept towards a comprehensive trust and reputation model was proposed by Tajeddine et al. [7]. Boukerche et al. [8] suggested the concept of trust and reputation in the wireless sensor networks. The study and analysis of some of these models were carried out in the WSN domain by Sabater and Sierra [9] and Josang et al. [10].We emphasized in our work towards a rigorous assessment of Eigen trust and reputation model based on pre-trusted peers probability factor for distributed peer to peer networks.

Rest of the paper is organized in the following sections. Section 2 reported the Eigen trust model description and related work in peer to peer networks. Section, 3 presented our detailed simulation design and setup. Section 4 describes the results and validations of our proposed model. Finally, conclusions are made in Section 5 followed by references in Section 6.

2. Eigen Trust Model

This section provides the background and related work on Eigen trust and reputation model with assumptions required for the later sections. Eigentrust model is the most frequently used trust and reputation model in distributed peer to peer networks. This model is based on Eigen trust algorithm. In this algorithm,each peer has a global reputation given by other peers i.e. summation of their local trust values. Kamvar et al. [17] 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 [18-19]. Equation (1) -equation (3) hold in order to compute trust value of the respected peer in the distributed networks.

$$C_{ij} = \frac{max\ (S_{ij}, 0)}{\sum_j max(S_{ij}, 0)} \quad (1)$$

where S_{ij} depicts the difference between satisfactory and unsatisfactory interaction between peers i.e. i, jand described asS_{ij}= sat(i,j)− unsat(i, j).Further, normalized local trust value is calculated which should lies in between 0 and 1.Aggregatedlocal trust values is define as t_{ik}= $\sum_j C_{ij}C_{jk}$where t_{ik}represents the trust that peer i places in peer k based on asking his friends.In the presence of malicious peers, t = $(C^T)^n$ p and generally converge faster than t = $(C^T)^n$e,so we use pas our start vector. Forinactive peers, C_{ij} refined as:

$$C_{ij} = \begin{cases} \frac{max\ (S_{ij}, 0)}{\sum j\ max(S_{ij}).} & if\ \sum j\ max(S_{ij}, 0) \neq 0; \\ otherwise & P_j \end{cases} \quad (2)$$

Malicious collectives issue can be addressed by the following equation (3).

$$t^{(k+1)} = (1 - a)\ C^T\ t^{\rightarrow(k)} + ap \quad where\ a < 1. \quad (3)$$

3. Detailed Design and Setup

We implemented our proposed model with Java-based simulator to test trust and reputation models for distributed networks [14].In our designated model, the simulation had the following constraints. We executed our model ten times (i.e.each peer request for service tentimes) over hundred static and dynamic distributed wireless networks. We used Eigen trust model with the following parameters. Pre-trusted probability value varies from0.1 to 0.9 and their weights value is 0.25. Non-damping factor value remains 0.1 with zero trust selection probability value 0.2. The deployment area for our network is 100 m × 100 m.On each network, the percentage of malicious peers is always 70%. Rests of 30% peers are therefore acting as server including 5 % relay peers. There is no delay factor and radio range is 12 m. Table 1 displays the summary of parameters deployed in our model.

Table. 1. Evaluation parameters

Scenario Options	Value
Security Model	Eigen Trust and Reputation
Pre-Trusted Peers Probability	0.1 - 0.9
Pre-Trusted Peers Weights	0.25
Non-Damping Factor	0.1
Zero Trust Selection Probability	0.2
Deployment Area	100 m ×100 m
Network Orientation	Static, Dynamic
Number of Networks	100
Number of Executions	10
Minimum Number of Sensors	50
Maximum Number of Sensors	50
Relay Peers (%)	5
Malicious Peers	70
Radio Range	12
Delay	0 sec

The simulation structure of our model is shown in figure 1.In simulation windows red dots denote malicious peer, blue dots represent relay peers, green dots depict benevolent peers and circle shows radio ranges corresponding to individual peers.

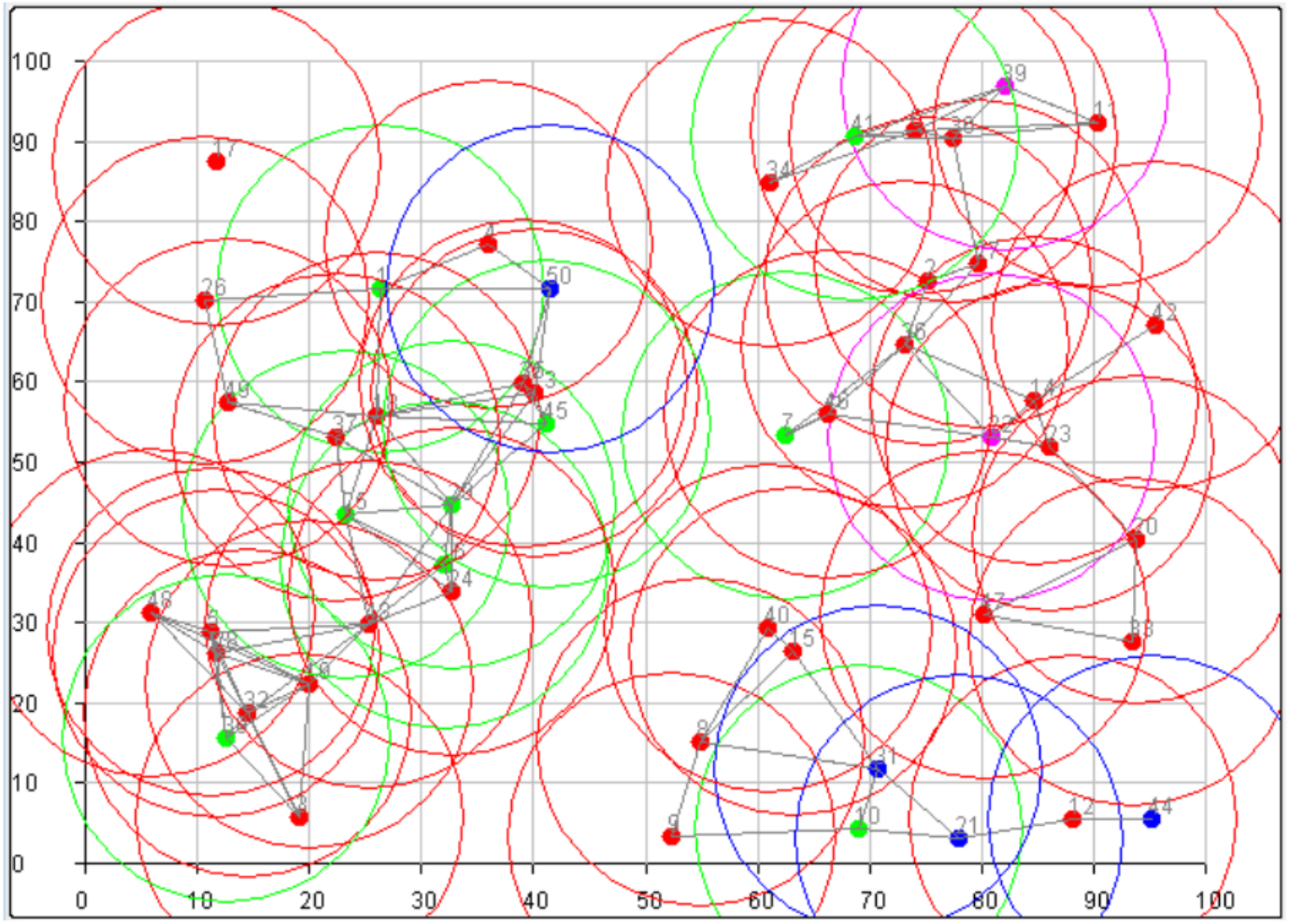

Figure. 1. Simulation Scheme

4. Results and Discussion

We evaluated the performance of Eigen trust model over static and dynamic distributed peer to peer networks. We focused on three factors namely: (i) accuracy, (ii) path length and (iii) energy consumption. An accuracy value may be referred as the fault free services provide by the peers in the networks. Path length value can be defined as the utilizations of resources consumed by the peer in the distributed networks. Energy consumption may be denoted as the power consumed by the peers in our deployed framework. We evaluated accuracy and path length from its current and average value i.e. for the last network and summation of all the deployed distributed peer to peer networks.

4.1. Static Distributed Networks Evaluations

Figure 2 shows the accuracy analysis of static peer to peer distributed networks. We examined the accuracy with respect to the pre-trusted peer probability for its current and average evaluation. We found that the current accuracy value remains maximum at 0.2 pre-trusted peers probability and minimum at 0.8 pre-trusted peers' probability. In case of average accuracy, we noticed that the accuracy value remains maximum at 0.2 pre-trusted peers probability and minimum at 0.9 pre-trusted peers probability. We observed that the current accuracy show the non linear behavior corresponds to average accuracy. This is because of the fact that the current accuracy depicts the value of the last event occurred in the last network whereas average accuracy reflects summations of all the event occurred in all networks. These shows a good agreement with the results reported in reference [15]. We extended the work of reference [15] to pre-trusted peers probability evaluation aspect.

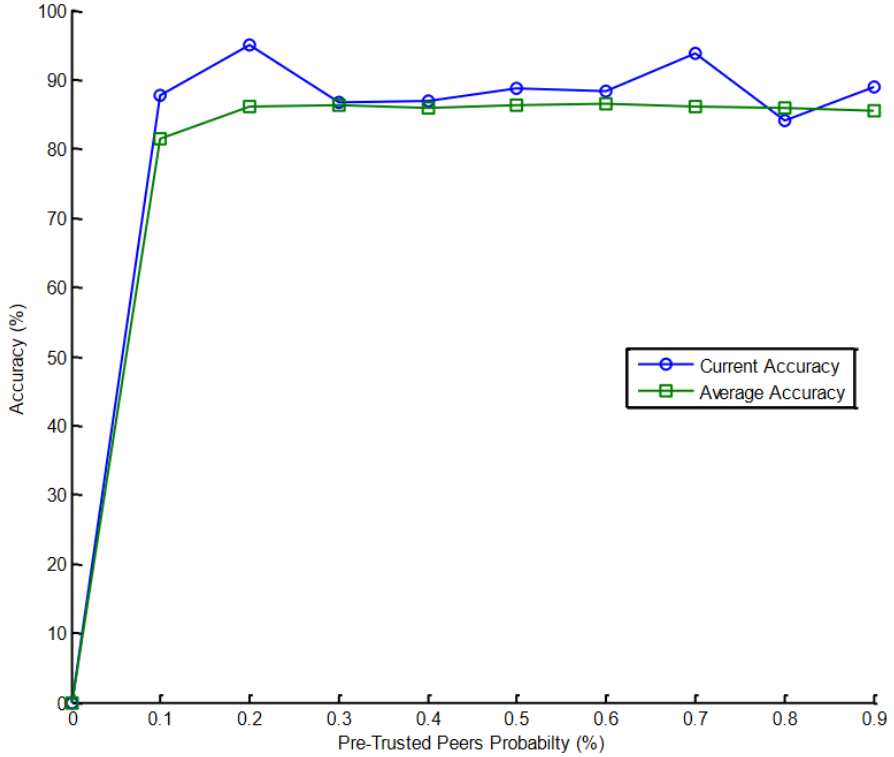

Figure. 2. Accuracy analysis for static peer to peer distributed networks

Next, we calculated path length on the consistent pattern of accuracy for our proposed model. According to figure 3, the path length is showing an increasing trend up to 0.3 the pre-trusted peer probability afterwards it decreased. We observed that the path length value remained maximum with 0.3 pre-trusted peer probability and minimum with 0.7 pre-trusted peers probability. We noticed that the average path length value show more linear behavior in contrast with the current path length.

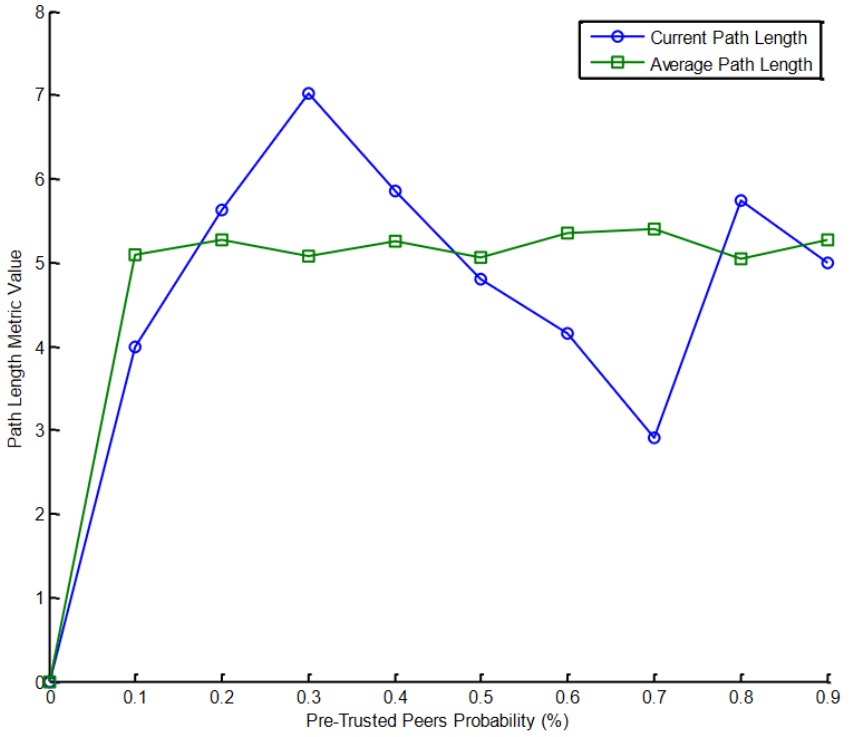

Figure. 3. Path Length analysis for static peer to peer distributed networks

4.2. Identify the Headings

Further, we evaluated our model on the dynamic distributed networks on the consistent pattern of static distributed networks. We evaluated accuracy and path length value for dynamic distributed networks. As per figure 4, current accuracy value remains maximum at 0.2 pre-trusted peers probability and minimum at 0.4 pre-trusted peers probability. Average accuracy shows its maximum value at 0.9 pre-trusted peers probability and minimum value at 0.1 pre-trusted peers probability. We observed that the average accuracy depicts linear incremental trend and current accuracy shows non linear behavior with respect to pre-trusted peers probability. Next, we evaluated path length value for the dynamic distrusted networks as shown in figure 5. We observed that the current path length remain maximum at 0.5 pre-trusted peers probability and minimum at 0.8 pre-trusted peers probability.We found that the average path length shows a linear decline in behavior and its value remains maximum at 0.1 pre-trusted peers probability and minimum at 0.9 pre- trusted peers probability.

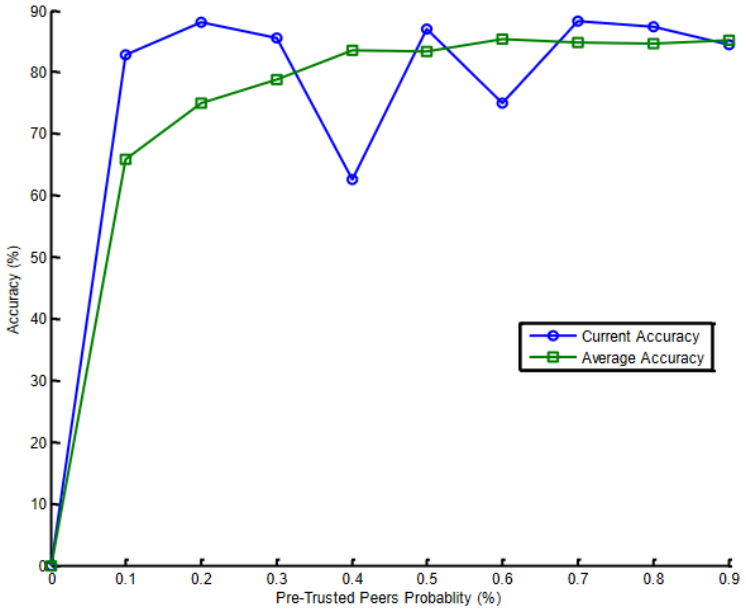

Figure. 4. Accuracy analysis for dynamic peer to peer distributed networks

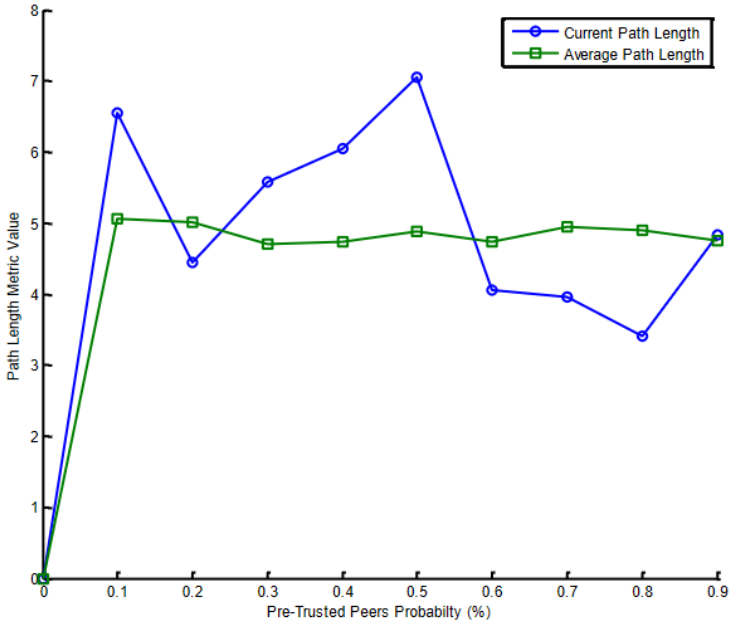

Figure. 5. Path Length analysis for dynamic peer to peer distributed networks

4.3. Energy Analysis for Static and Dynamic Distributed Networks

Lastly, we calculated the energy consumed by static and dynamic distributed networks. In case of static distributed networks, we observed that the energy consumption show non linear behavior. We found that energy consumption remained maximum at 0.7 pre-trusted peers probability and minimum at 0.8 pre-trusted peers probability correspond to static distributed networks.In case of dynamic distributed networks, we noticed that the energy consumption shows linear elliptical behavior. We observed that energy consumption remained maximum at 0.7 pre-trusted peers probability and minimum at 0.9 pre-trusted peers probability correspond to dynamic distributed networks.

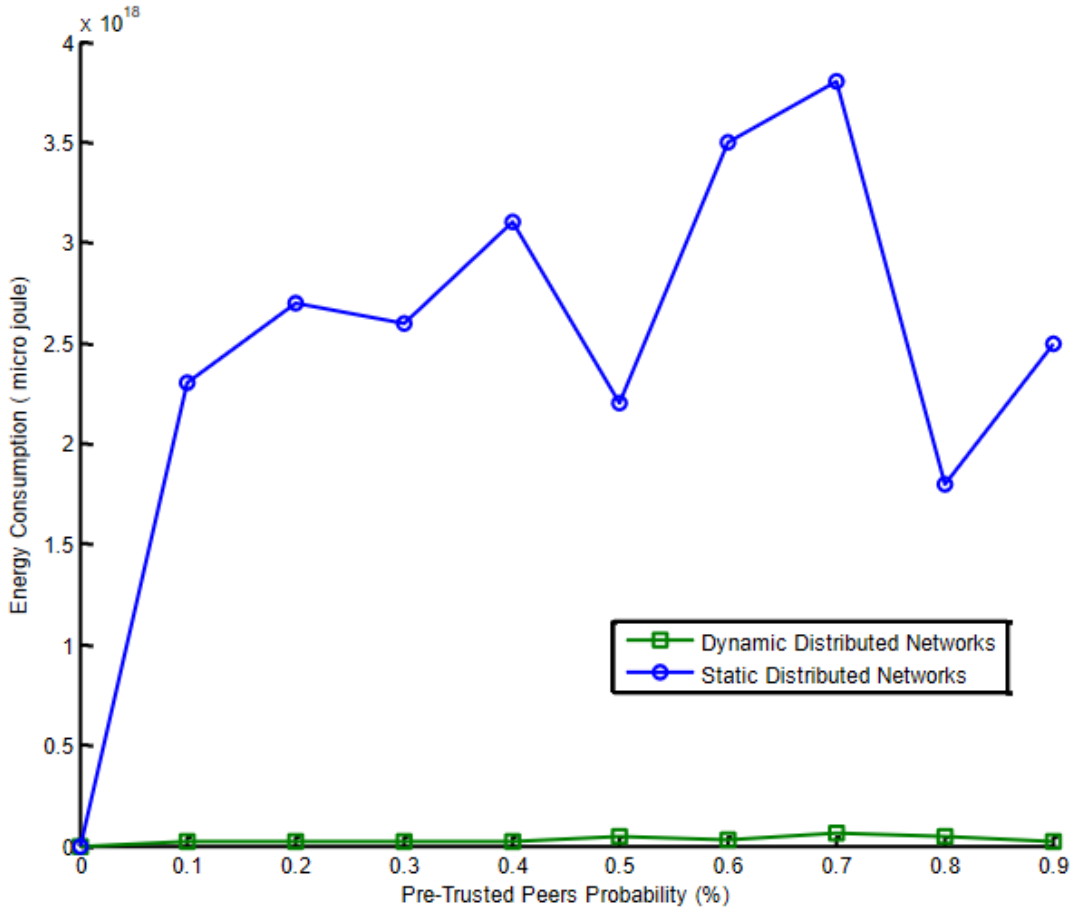

Figure. 6. Energy consumption analysis for static and dynamic distributed networks

Abrams et al. [16] presented anon-manipulable trust system based on Eigenrustand reputation model. We extended the work of reference [16] for rigorous evaluation of eigen trust and reputation model. Verma et al. [17] made a comprehensive evaluation of static and dynamic routing protocols for distributed networks. We incorporated this work towards Eigen trust and reputation model over static and dynamic distributed networks.

5. Conclusion

This paper made a comprehensive evaluation of Eigen trust and reputation model over static and dynamic distributed networks. We focused on pre-trusted peers probability aspect through out our evaluation.We found that leverage accuracy depicts linear behavior as compare to current accuracy in both the static and dynamic distributed networks. accuracy in terms of average and current value. Path length shows more linear behavior in the average path length case than that of current path length case. We noticed that path length reflect incremental behavior in static distributed networks and declines in behavior for dynamic distributed networks. We observed that the energy consumption remains higher in static distributed networks than the dynamic distributed networks for Eigen trust model evaluation. This makes Eigen trust and reputation model more suitable for dynamic distributed networks. In future, we will work for further enhancement of Eigen trust and reputation model for distributed networks.

References

[1] LA. Adamic, “Zipf,” Power-Laws and Pareto — A Ranking Tutorial, ”http://www.hpl.hp.com/research/idl/papers/ranking/ranking.html, HP Labs, Calif., 2002.

[2] S. Buchegger and J.-Y.L. Boudec.A Robust Reputation Systemfor P2P and Mobile Ad-hoc Networks.Proc. Second Workshop Economics of P2P Systems, 2004.

[3] L. Xiong and L. Liu. Peer Trust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. IEEE Trans. Knowledge and Data Eng., Vol. 16, no. 7, pp. 843-857,2004.

[4] Sabater, J., Sierra, C. REGRET: reputation in gregarious societies. In AGENTS '01. Proceedings of the Fifth International Conference on Autonomous Agents, New York, NY, USA, ACM Press, 194-195, 2001.

[5] Almena´rez F, Marı´n A, Campo C, Garcı´a C.PTM: a pervasive trust management model for dynamic open environments.in Privacy and trust. First workshop on pervasive security and trust, Boston, USA, 2004.

[6] Moloney M, Weber S. A context-aware trust-based security system for ad hoc networks.in workshop of the 1st international conference on security and privacy for emerging areas in communication networks, Athens, Greece; pp. 153–60,2005.

[7] Tajeddine A, Kayssi A, Chehab A, Artail H. PATROL-F, A comprehensive reputation-based trust model with fuzzy subsystems.Autonomic and trusted computing, Third international conference, ATC. LNCS, vol. 4158. Wuhan, China: Springer; pp. 205–17,2006.

[8] Boukerche A, Xu L, El-Khatib K. Trust-based security for wireless ad hoc and sensor networks. Computer Communications. 30 (11–12): 2413–27,2007.

[9] Sabater J, Sierra C. Review on computational trust and reputation models. Artificial Intelligence Review. 24 (1): pp. 33–60, 2005.

[10] Josang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision, Decision Support Systems, 43 (2): 618–44,2007.

[11] Kamvar S, Schlosser M, Garcia-Molina H. The Eigen Trust algorithm for reputation management in P2P networks. Budapest, Hungary. 2003

[12] Advogato's Trust Metric (White Paper), 2002.

[13] J. Douceur. The Sybil Attack.InFirst IPTPS, March Proceeding IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems Pages 251-260, 2002.

[14] Félix Gómez Mármol, Gregorio Martínez Pérez, TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. IEEE International Conference on Communications (IEEE ICC 2009), Communication and Information Systems Security Symposium, Dresden, Germany. 2009.

[15] Vinod Kumar Verma, Surinder Singh, and N.P. Pathak, Collusion Based Realization of Trust and Reputation Models in Extreme Fraudulent Environment over Static And Dynamic Wireless Sensor Networks.International Journal of Distributed Sensor Networks, Volume 2014, Article ID 672968.2014.

[16] Zoe Abrams and Robert McGrew and Serge Plotkin. A Non-Manipulable Trust System Based on EigenTrust, ACM SIGecom Exchanges, Vol. 5, No. 4, July 2005, Pages 21–30.

[17] Vinod Kumar Verma, Surinder Singh, and N.P. Pathak. Optimized Battery Models Estimation for Static, Distance Vector and On-Demand Based Routing Protocols over 802.11 Enabled Wireless Sensor Networks. Wireless Personal Communications: An International Journal, Springer Science + Business Media New York 2014.