IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

A Comparative Study for Trust and Reputation Models for Wireless Sensor Networks

Sura F. Ismail

University of Information Technology and Communications/College of Business Informatics, Baghdad, Iraq

Abstract: Security is one of the important topics in Wireless Sensor Networks (WSNs). Trust and reputation Management System (TRM) is an innovative solution for maintaining a minimum security level between two entities having transactions or interactions within a distributed system. Several trust and reputation monitoring (TRM) models have been proposed. The purpose of this research is to compare between different types of trust and reputation models in terms of accuracy, path length and energy consumption. Finally, the comparative study was simulated by using Trust and Reputation Model Simulator for Wireless Sensor Network.

Keywords: Security Threat, Wireless Sensor Networks, Trust and Reputation Models, Trustworthy Servers, Collusion Threat, Trust and Reputation Model Simulator for Wireless Sensor Network.

I. INTRODUCTION

During the last decade, wireless sensor networks have become very popular. A lot of research and many applications have been developed. Area monitoring, environmental sensing and industrial monitoring are only few examples among the most important applications that WSNs have revolutionized. However, for developing useful and efficient applications, the challenges and obstacles faced in the design of such networks should be properly addressed and solved. One particularly important challenge relates to security issues. Traditional cryptographic approaches are widely used to provide security in WSN. However, because of unattended and insecure deployment, a sensor node may be physically captured by a malicious who may acquire the underlying secret keys, or a subset thereof, to access the critical data and/or other nodes present in the network. Moreover, a node may not properly operate because of insufficient resources or problems in the network link. 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. In this paper a comparative analysis between different trust and reputation models has been illustrated.

The rest of the paper is organized as follows: section 2 illustrated an overview about the trust and reputation models that compared and analyzed in this paper. In section 3 presented and analyzed the simulated models results. Finally, in section 4 conclusions is described.

II. TRUST AND REPUTATION MODELS OVERVIEW

Trust and Reputation management is an innovative solution for maintaining a minimum security level between two entities having transactions or interactions within a distributed system. Trust is a particular level of the subjective probability with which an agent will perform a particular action; while a reputation [**1**] is an expectation about an agent's behavior based on information about it or observations of its past behavior. The use of the words “trust” and “reputation” is commonplace in our daily lives. In WSN transactions, if we define the sensors asking for services as client sensors, and sensors providing services as server sensors, then the client sensors will determine whether to have transactions with a server sensor based on its trustworthiness or reputation. A trust and reputation model is generally composed of five components [**2**], [**3**]: gathering information, scoring and ranking, selecting entities, having transaction, and reward or punishment. Gathering information, the first component of a trust and reputation system, is responsible for collecting behavioral information about other entities, for instance peers, agents, or paths. The information collected might come from different sources [**4**]. It could be first-hand (direct observation or own experience), or second-hand (information provided by peers). Once information about an entity has been properly aggregated and weighed, a reputation score is then computed and given base on certain algorithm. The primary objective of this procedure is to provide the clients a measurable approach to decide which server node is most trustworthy. The next step is that a client selects the most trustworthy or reputable server entity in the community providing certain service and then effectively has an interaction with it. After receiving the service provided, the client will access the result and give a score of satisfaction. Based on the satisfaction obtained, the last step, punishing or rewarding, is carried out. If a server node is unsuccessful in making the client satisfied with the service provider, its reputation

DOI 10.17148/IJARCCE.2017.6324

score will suffer, and the client is less likely to have transaction with it again. The trust and reputation models that described in this paper are Bio-inspired Trust and Reputation Model (BTRM-WSN), Eigen Trust, Peer Trust, Power Trust, LFTM, TRIP.

A. *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 [**5**].

B. *Eigen Trust Model:*
It is one of the most commonly used trust and reputation models in the wireless sensor network domain. Kamvar et al. [**6**] 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. Further into this model, the authors define *Sij* as the local trust of peer *i* about peer *j*, in the following Equation (1):

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

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):

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

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

C. *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 [**7**].

D. *Power Trust:*
The main innovation of Power Trust [**8**], a novel reputation model for P2P networks, relies on considering the distribution of peers feedbacks in such environments. Thus, this reputation mechanism is the first one which effectively and accurately takes advantage of that fact. Authors studied the eBay transaction trace over 10,000 users and discovered that feedbacks in those systems followed a power-law distribution, i.e., the node with a few feedbacks is common, whereas the node with a large number of feedbacks is extremely rare. Therefore, Power Trust leverages on those nodes with a higher amount of feedbacks, called power nodes, to aggregate users feedbacks and compute the global reputation scores *vi* ∈ [0; 1] owned by every peer *i*. Furthermore, the set of power nodes is updated dynamically after each round of aggregation as the set of the current *m* most reputable nodes (the ones with highest reputation scores).

E. *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 [**9**].

F. *Trust and Reputation Infrastructure Based Proposal (TRIP) Model:*
This model is based on the environment specific issues like infrastructure, area, density, and so forth, within the specified conditions [**10**]. 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.

SECURITY THREATS

Every node maintains the pheromone traces of its neighbors and it is the only one who can manage, control and modifies them, this fact can lead to some security threats [**11**]. But the security threats can appear if a malicious server colludes with other malicious servers, because a sensor is only able to manage the pheromone

DOI 10.17148/IJARCCE.2017.6324

traces of its neighbors, but it cannot control the pheromone traces that its neighbors have associated with it, and that collusion is only possible if the malicious sensors know each other and also know who the benevolent sensors are, and this assumption is not always feasible in every wireless sensor network. The security threats that assumes here is that malicious sensors can praise their malicious neighbors by assigning them the maximum level of pheromone. Equally they can slander their benevolent neighbors by giving them the minimum value of pheromone.

III. COMPARATIVE AND ANALYSIS THE PERFORMANCE

We simulated three experiments to evaluate and compare the performance of **BTRM-WSN, Eigen Trust, Peer Trust, Power Trust, LFTM, and TRIP models**. The first experiment aims at comparing the six systems in terms of the accuracy in searching for trustworthy sensors, which evaluates the level of security provided, in four different environment; Static WSN, Static with collusion, Dynamic and Dynamic with collision, the second test compares the average path length leading to the trustworthy sensors selected, which evaluates the efficiency, or the easiness in finding trustworthy sensors, of the six systems in the four different environments; and finally, the overall energy saving of applying these six systems in a static and dynamic Wireless Sensor Networks are measured.

3.1 Scenario of WSN Environment

The performance of BTRM-WSN, Eigen Trust, Peer Trust, Power Trust, LFTM, and TRIP models are simulated and compared over four environment scenarios which are:

A. Static WSN: the servers maintaining always the same goodness, does not change their behaviors.

B. Collusion WSN: The security threats that assumes here is that malicious sensors can praise their malicious neighbors by assigning them the maximum level of pheromone. Equally they can slander their benevolent neighbors by giving them the minimum value of pheromone. But the security threats can appear if a malicious server colludes with other malicious servers, because a sensor is only able to manage the pheromone traces of its neighbors, but it cannot control the pheromone traces that its neighbors have associated with it, and that collusion is only possible if the malicious sensors know each other and also know who the benevolent sensors are, and this assumption is not always feasible in every wireless sensor network.

C. Dynamic WSN: This scenario is consist of dynamic Wireless Sensor Networks with nodes continuously entering and leaving the community .The decision scheme of when to switch off and on is as follows: when a server receives and supplies 20 requests it automatically switches off during a certain timeout. On the other hand, if a server does not receive at least 20 requests within a time interval, it also switches off during another timeout.

3.2 TRMSim-WSN

In this paper, we simulated the six models in Trust and Reputation Model Simulator for WSN (TRMSim-WSN) [**12**] which is a Java-based trust and reputation models simulator aiming at providing an easy way to test a trust and reputation model over WSNs and to compare it against other models. We design a WSN template using the Network Parameter settings as shown in Table I. Note that 20% of all nodes in a randomly created WSN are clients which will request default services. The other 70% nodes will act as servers which will be asked to provide services upon request.

TABLE I. EXPERIMENT PARAMETERS.

Network	NumExecutions	100	%Clients	20%
	NumNetworks	100	%Relay	5%
	MinNumSensors	{50,100,150, 200}	%Malicious	70%
	MaxNumSensors	{50,100,150, 200}	Radio range	{10,8,6,4}

3.3 Accuracy

Here we use the concept “accuracy” to evaluate the reliability and level of security provided by the trust and reputation system over static, static with collusion-threat, dynamic and dynamic with collusion-threat. The accuracy of a trust and reputation system is represented by the percentage that the number of times when it successful selects trustworthy sensors (the former situation) out of the total number of transactions.

Fig. 1 shows the accuracy of BTRM-WSN, Eigen Trust, Peer Trust, Power Trust, LFTM and TRIP systems with various numbers of sensor nodes and over static WSN. We conclude that LFTM system can approximately provide the highest accuracy and thus the highest level of reliability and security, while TRIP provides the lowest value. Also it is observed that Peer Trust model is the most oscillated and unstable in accuracy.

The selection percentage of trustworthy servers of the six systems over static WSN with collusion-threat is shown in Fig. 2. It can be checked that Eigen Trust model provide the highest accuracy and LFTM came in the second stage, while Peer Trust provides the lowest value. Also here, Power Trust model provides the most oscillated and unstable result in accuracy.

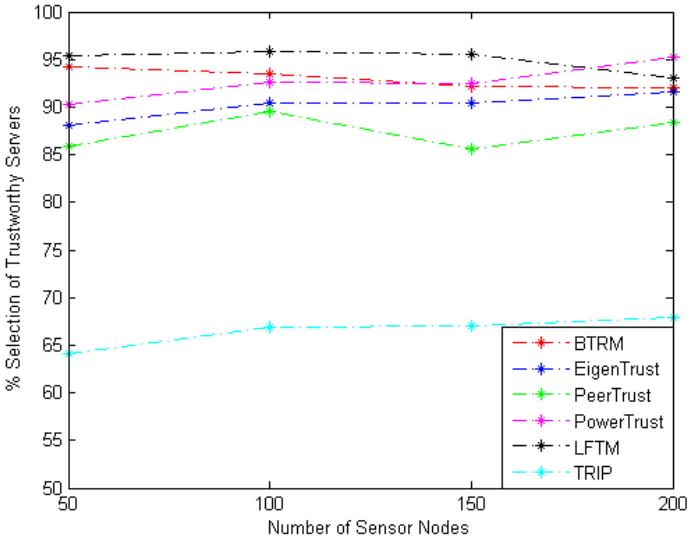

Fig. 1. Selection percentage of trustworthy servers over static WSNs.

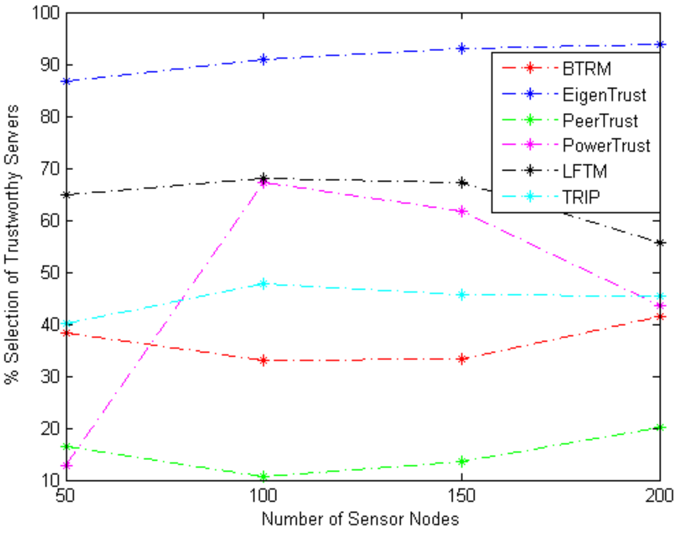

Fig. 2. Selection percentage of trustworthy servers over static WSNs with collusion- based.

Fig. 3 described the accuracy with various numbers of sensor nodes over dynamic WSN. It can be observed that approximately all models show unstable behavior. LFTM model shows the highest value when the numbers of sensor nodes are 50,100 or 150; but when the number of sensor nodes become 200 the accuracy drop down and become after Eigen Trust, Power Trust, BTRM and Peer Trust while TRIP give the lowest value.

Finally, the selection percentage of trustworthy servers over dynamic WSN with collusion-threat is illustrated in Fig. 4. It can be conclude that the behavior of accuracy value of all models are the same as static WSN with collusion – threat that shown in Figure 2 but with a light increasing, for example, TRIP gives the lowest value in both scenarios, but the range of value giving by this model in static WSN with collusion is between 10 and 20 while in dynamic WSN with collusion, the accuracy value is between 15 and 27.

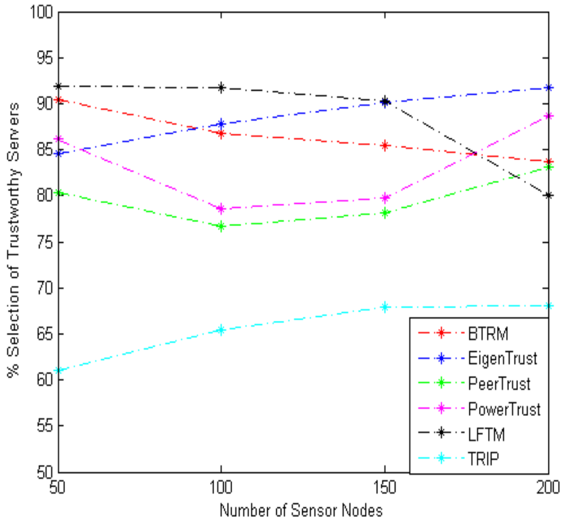

Fig. 3. Selection percentage of trustworthy servers over dynamic WSNs.

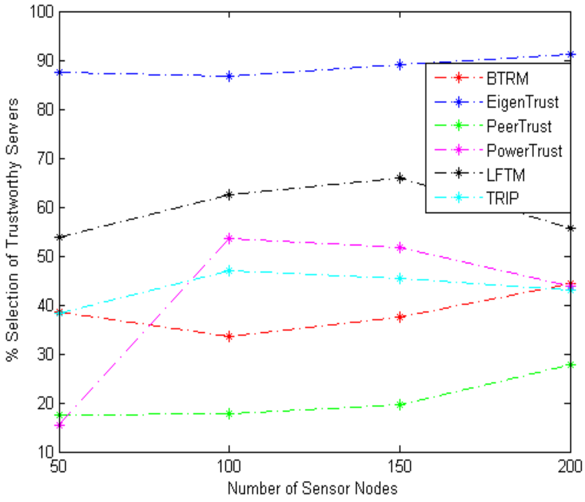

Fig. 4. Selection percentage of trustworthy servers over dynamic WSNs with collusion-based.

3.4 Path Length

Path length is the average hops leading to the most trustworthy sensors which are selected by the client in a WSN applying a certain type of trust and reputation system. It is assumed that less average path length indicates a better performance in efficiency and easiness in searching for trustworthy sensors of a trust and reputation system. This is because: 1) less number of intermediaries means higher security level and less energy consumption; and 2) shorter path length implies that it is easier to find trustworthy nodes and thus, server nodes will response quicker to client nodes.

DOI 10.17148/IJARCCE.2017.6324

Fig. 5 and Fig. 6 will compare the BTRM-WSN, Eigen Trust, Peer Trust, Power Trust, LFTM and TRIP in terms of average path length leading to trustworthy sensors with various number of sensor nodes over Static WSN and Static WSN with collusion-based. TRIP has the best performance, and Eigen Trust has the worst performance in terms of shorting average path length. Since, in TRIP by increasing the number of sensor nodes, the average path length remains one. Eigen Trust, Power Trust and Peer Trust are unstable and lengthiest in average path length that BTRM, LFTM and TRIP models.

The average path length leading to trustworthy sensors over dynamic WSN and dynamic WSN with collusion-based are show in Fig. 7 and Fig. 8. It can be conducted that all six models over Dynamic WSN give the same behavior as in Static WSN. It can be observed that the average path length over Dynamic WSN with collusion-based also give the same reaction by varying number of sensor nodes over Static WSN with collusion-based.

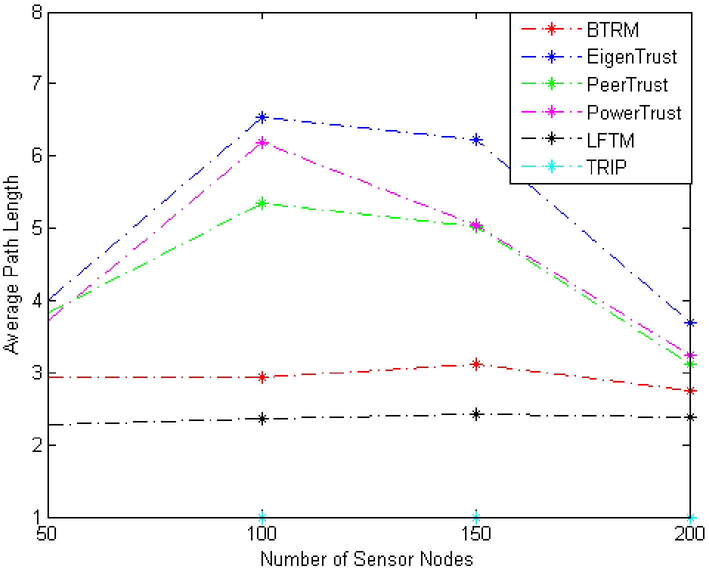

Fig. 5. Average path length leading to trustworthy servers over static WSNs.

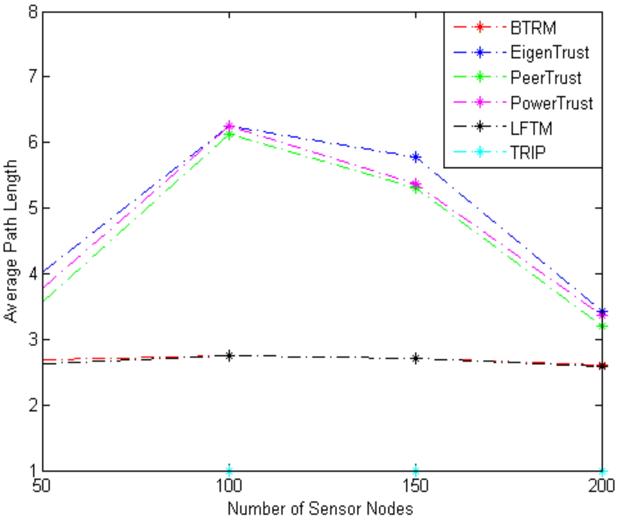

Fig. 6: Average path length leading to trustworthy servers over static WSNs with collusion-based.

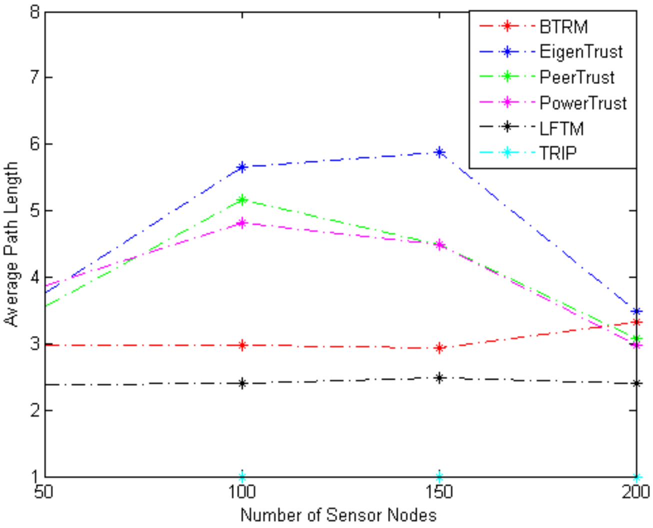

Fig. 7. Average path length leading to trustworthy servers over dynamic WSNs.

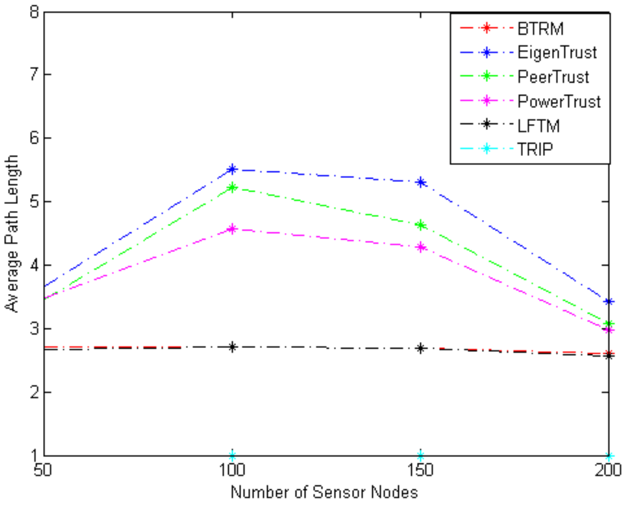

Fig. 8. Average path length leading to trustworthy servers over dynamic WSNs with collusion-based.

3.5 Energy Consumption

Energy consumption of the network is the overall energy consumed in: 1) client nodes sending request messages; 2) server nodes sending response services; 3) energy consumed by malicious nodes which provide bad services; 4) relay nodes which do not provide services; and 5) the energy to execute the trustworthy sensor searching process of a certain trust and reputation system. How to effectively reduce energy consumption is a major issue in WSN researches. Figs 9, 10, 11,12,13 and 14 will compare the energy consumption of BTRM-WSN, Eigen Trust, Peer Trust, Power Trust, LFTM and TRIP, respectively over Static and Dynamic WSN and by various number of sensor nodes. It illustrated how the dynamics behavior will decrease the energy consumption in each model. Also, it can be conducted that Eigen Trust is the most energy consumption model in both static and dynamic environments, while TRIP is the least energy consumption

DOI 10.17148/IJARCCE.2017.6324

model and the consumption will remain the same in both environments.

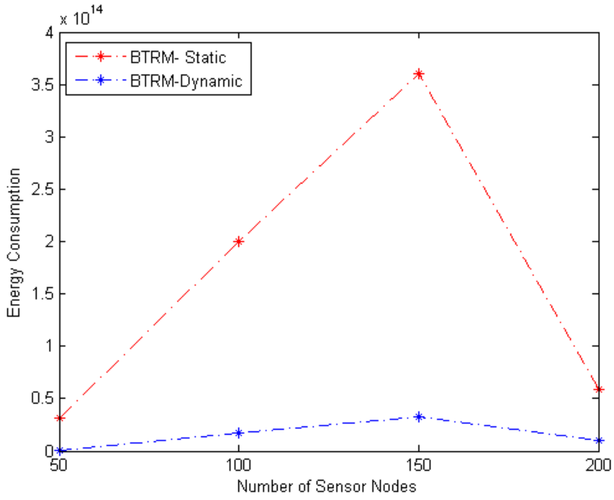

Fig. 9. BTRM overall network energy consumption over static and dynamic WSNs.

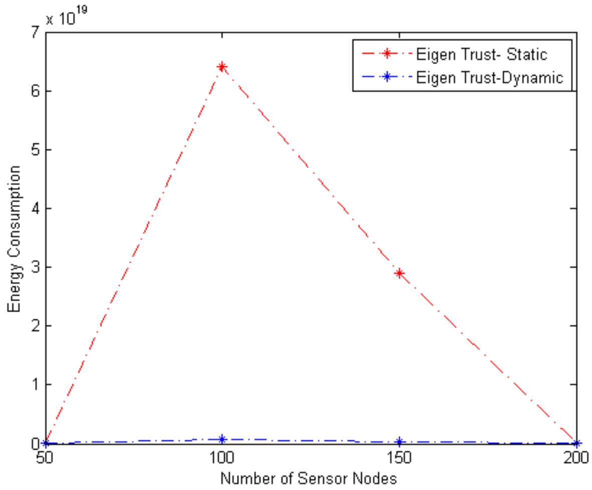

Fig. 10. Eigen Trust overall network energy consumption over static and dynamic WSNs.

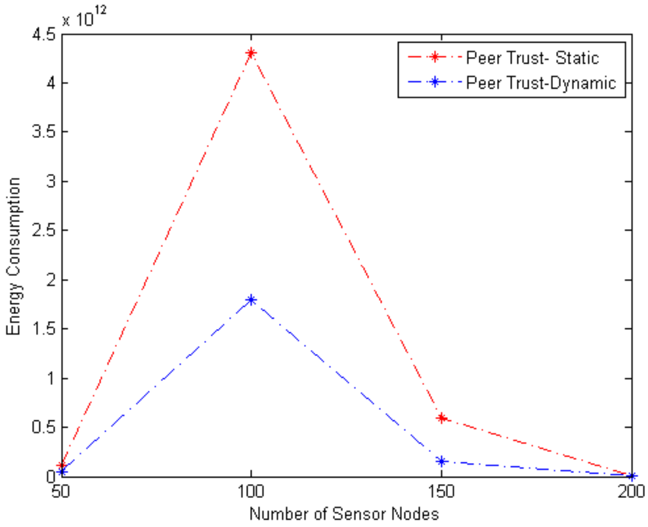

Fig. 11. Peer Trust overall network energy consumption over static and dynamic WSNs.

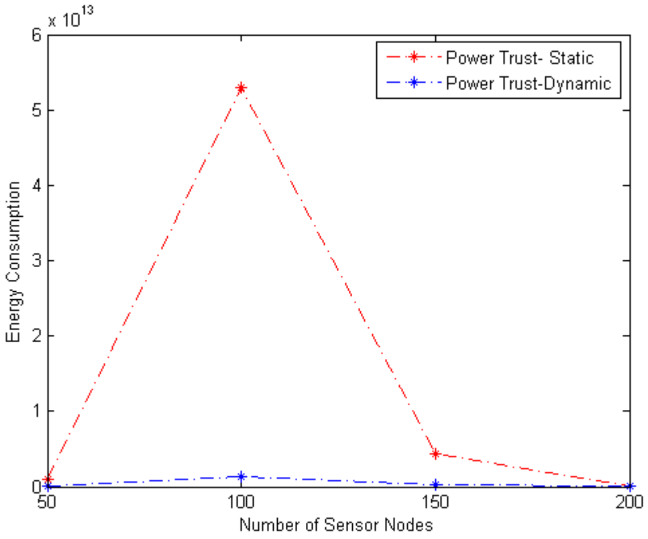

Fig. 12. Power Trust overall network energy consumption over static and dynamic WSNs.

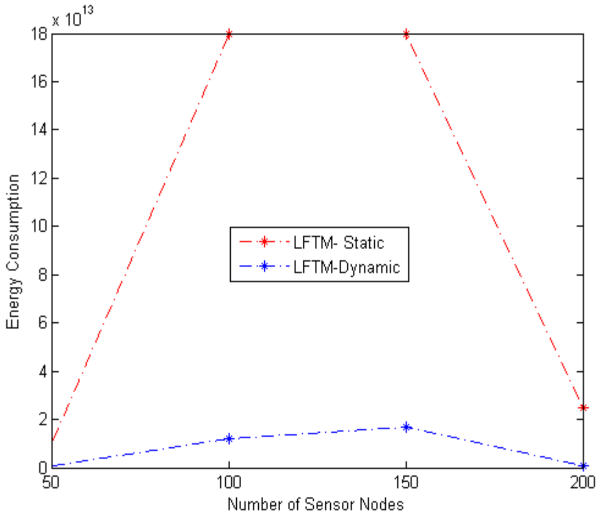

Fig. 13. LFTM overall network energy consumption over static and dynamic WSNs.

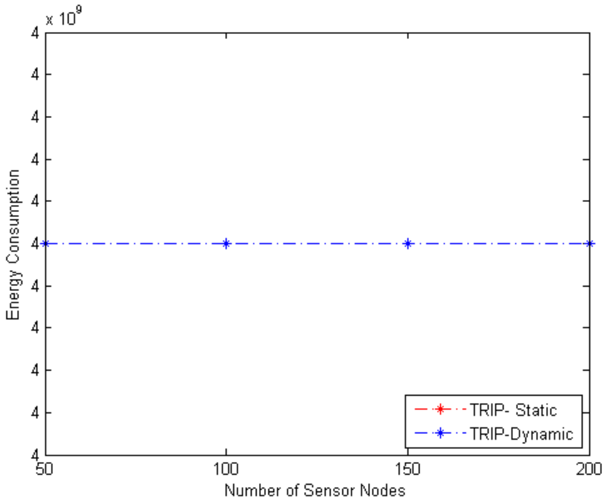

Fig 14. TRIP overall network energy consumption over static and dynamic WSNs.

DOI 10.17148/IJARCCE.2017.6324

IV. 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 illustrated a survey about different trust and reputation models; BTRM-WSN, Eigen-Trust, Peer-Trust, Power-Trust, LFTM, and TRIP. Over static and dynamic WSNs with and without collusion threat. This paper concluded that the accuracy of each model will decrease with collusion threat in both static and dynamic environments. While average path length gives the conclusion that the six models over dynamic WSN give the same behavior as in static WSN with and without collusion threat. TRIP has the best performance, and Eigen Trust has the worst performance in terms of shorting average path length. Also the energy consumed in each models over static and dynamic WSNs will illustrate. It observed how the dynamics behavior will decrease the energy consumption in each model.

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.

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their detailed comments on earlier versions of this paper.

REFERENCES

[1] Abdul-Rahman, A. and S. Hailes. "Supporting Trust in Virtual Communities." System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on . London, UK: IEEE, 2000. 9.

[2] Marti, S. and H. Garcia-Molina. "Taxonomy of Trust: Categorizing P2P Reputation Systems." Computer Networks 50.4 (2006): 472-484.

[3] Mármol, F. G. and G. M. Pérez. "Towards Pre-Standardization of Trust and Reputation Models for Distributed and Heterogeneous Systems." Computer Standards' Interfaces 32.4 (2010): 185-196.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[4] Srinivasan, A., et al. "Reputation and Trust-based Systems for Ad Hoc and Sensor Networks." On Trust Establishment in Mobile Ad-Hoc Networks. Ed. A. Boukerche. Wiley & Sons, 2007.

[5] Mármol, F. G. and G. M. Pérez. "Providing Trust in Wireless Sensor Networks Using a Bio-Inspired Technique." Telecommunication Systems 46.2 (2011): 163-180.

[6] Kamvar, S., Schlosser, M. and Garcia-Molina, H. (2003), "The EigenTrust algorithm for reputation management in P2P networks", WWW03: Proceedings of the 12th international conference on World Wide Web, pp. 640-51.

[7] Xiong, L. and L. Liu. "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities." Knowledge and Data Engineering, IEEE Transactions on 16.7 (2004): 843-857.

[8] Zhou, R. and Hwang, K. (2007), "PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing", IEEE Transactions on Parallel and Distributed Systems, Vol. 18 No. 4, pp. 460-73.

[9] Mármol, F. G, Marín-Blázquez, J. G, and Pérez, G. M, 2011, *Linguistic Fuzzy Logic Enhancement of A Trust Mechanism for Distributed Networks*, Proceedings of the Third IEEE International Symposium on Trust, Security and Privacy for Emerging Applications, PP. 838-845, Bradford, UK.

[10] Mármol F. G., Pérez G. M.TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networksJournal of Network and Computer Applications, 2011.

[11] GómezMármol F, Martínez Pérez G,"Security threats scenarios in trust and reputation models for distributed systems", Elsevier Computers & Security, 28(7):545–556, 2009.

[12] Gómez Mármol F, Martinez Pérez G. 2009. TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks. Proceedings of the IEEE International Conference on Communications, Communication and Information Systems Security Symposium. DOI:10.1109/ICC.5199545,Dresden, Germany.

BIOGRAPHY

Sura Fawzi Ismail is an assistant lecturer at University of Information Technology and Communications. She received the BS Degree in Computer Engineering from the University of Baghdad, Iraq, in 2011, and the MS Degree in Computer engineering from the University of Baghdad, Iraq, in 2014. Her major research interests include energy conservation, clustering, mobility and network security in wireless sensor networks.