INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
Tuna et al., Vol. 8, No. 4, pp.114-121

Scalability Evaluation of Trust and Reputation Models for Wireless Sensor Networks

Gürkan Tuna*, Resul Daş**

*Department of Computer Programming, Vocational School of Technical Sciences, Trakya University, Edirne, Turkey
**Department of Software Engineering, Technology Faculty, Fırat University, 23119 Elazığ, Turkey
E-mail: *gurkan.tuna@trakya.edu.tr, rdas@firat.edu.tr*

ORCID ID: 0000-0002-6466-4696, 0000-0002-6113-4649
Research Paper Received: 01.11.2019 Revised: 27.12.2019 Accepted: 29.12.2019

Abstract—A wireless sensor network consists of a group of distributed sensor nodes to monitor physical and / or environmental conditions, such as sound, motion, temperature, pressure or pollutants and to cooperatively deliver their data through the network infrastructure to a main location, generally called sink. Inspite of its several advantages, due to its inherit features, wireless sensor networks are open to many security risks. Although conventional data security solutions are effective for other types of networks, they are not effectively applicable to wireless sensor networks. Therefore, trust and reputation management approaches have been proposed as an alternative. In a wireless sensor network, trust and reputation management enables a node to make their own opinion about how trustworthy or reputable another node is. This way, it reduces the opportunities of being defrauded and augments the probability of a successful transaction. It is known that although in the literature there are many trust and reputation models, stil there is a lack of state-of-the-art models, standart data structures and application programming interfaces, generic testing tools, and security threats analysis. Accordingly, in this study a contribution to the last one is made and the effectiveness of two well-known trust and reputation models proposed for wireless sensor networks, namely PeerTrust and PowerTrust, is evaluated in terms of accuracy, path length, and power consumption.

Keywords—Wireless sensor network, Trust, Reputation, PeerTrust, PowerTrust, Scalability

1. Introduction

A Wireless Sensor Network (WSN) consists of a group of sensor nodes distributed in an area, typically deployed for cooperatively realizing a given task. In the last decade WSNs have been researched extensively. While they were first used for military purposes, later on they have been started to be used for civilian and industrial purposes such as weather monitoring, pollution detection, traffic control, and healthcare monitoring [1]. Although there are many security threats that might affect the proper functioning of WSNs, providing security to them is a challenging issue. WSNs must be secured to keep on-site or cyber attackers from hindering the delivery of sensor data and from forging sensor data [2]. Because WSNs are typically built for remote surveillance purposes and unauthorized changes in the sensed data have the possibility of leading to undesired or unexpected results. Since WSNs are vulnerable to hackers who might go into the networks with the intent of ren-

dering them useless, security solutions are critical for the successful operation of WSNs [2]. Currently, trust and reputation management approaches are preferred in many environments in which there is not enough information about the entities in the system. Basically, trust and reputation systems allow an entity to decide which one of the other entities to have an interaction with, based on the direct trust given by the former, the global reputation given to the latter, or a combination of both [3].

Trust and reputation systems typically follow a five-step process. The steps are gathering information, scoring and ranking, entity selection, transaction, and reward and punish [4]. The gathering information step rely on direct experiences, acquintances' experiences and pre-trusted entities. An additional step called checking integrity, which relies on raters' reliability, provides information to the gathering information step. The gathering information step creates recommendations and provides data to the transaction history. The scoring and ranking step receives the recommendations and the transaction history [5]. As well as the recommendations provided by the gathering information step, it can also rely on anonymous recommendations though they might be quite subjective. Although the transaction history is a good indicator, assigning higher weight to more recent transactions may be useful. The scoring and ranking step relies on various mechanisms such as analytic processes, bayesian, fuzzy logic [6] and bio-inspired approaches [7], and provides reputation and trust information to the entity selection step. Then, entity selected by the entity selection performs a transaction. Regarding the scores, different trust and/or reputation scores can be given to different services [8] and the scores can take into account bandwidth, energy consumption, and scalability for optimal performance. Finally, depending on the transaction a service is received, which provides data to the reward and punish step. Trust and reputation systems should avoid abuse of a high achieved reputation. Although opportunity to participate should be given to benevolent newcomers, it is desired that benevolent nodes have more opportunities than the newcomers. Finally, redemption of past malicious entities should be considered. As a result of the increasing interest on machine-machine and human-machine interactions, a multidimensional framework has been proposed in [9] to classify and compare computational trust and reputation models. In addition, since in recent years computational trust and reputation models have attracted the attention of researchers, surveys on this area have been provided in [10,11]. Although there are many trust and reputation models and several metrics used to evaluate the performance of trust and repuation models [11], this paper presents two well-known trust and reputation models, namely PeerTrust and PowerTrust, and evaluates them in terms of three commonly used metrics, accuracy, path length and power consumption, respectively, to decide their scalability. The rest of this paper is structured as follows. The second section introduces PeerTrust and PowerTrust trust and reputation models. The third section presents the simulation settings and analyzes the results obtained, and finally the fourth section concludes the paper.

2. PeerTrust and PowerTrust

PeerTrust is a reputation-based trust model designed for peer-to-peer networks [12]. In the model, two different strategies are employed to implement the basic trust metrics of PeerTrust [3]. The general trust metric of PeerTrust for peer e, $GT(e)$, is defined using Eq. 1.

$$GT(e) = k.\sum_{i=1}^{T(e)} NS(e,i).CF(p(e.i)).TCF(e,i) + CCF(e) \quad (1)$$

where k and l represent the normalized weight factors for the feedback-based reputation evaluation and the community context factor (CCF) for different situations. $GT(e)$ represents the total number of transactions realized by peer e with all other peers, p(e,i) represents the other participating peer in peer e's ith transaction, $NS(e,i)$ represents the normalized amount of satisfaction which peer e receives from peer $p(e,i)$ in its ith transaction, CF(f) represents the credibility of the feedback delivered by peer f, $TCF(e,i)$ represents the adaptive transaction context factor for peer e's ith transaction, and finally $CCF(e)$ is the adaptive CCF for peer e.

In PeerTrust, two different metrics are provided for the credibility. The first metric proposed by the authors is Trust Value Metric (TVM) which is proportional to the general trust metric directly [3]. Therefore, if a peer provides a more trustworthy service, it becomes more credible for providing recommendations. The second metric proposed by the authors is Peer Similarity Metric (PSM) which is based on using the similarity between the feedbacks delivered by two different nodes so that dishonest recommendations can be eliminated successfully [3]. Because benevolent peers normally provides similar feedbacks to similar services and same service providers. PeerTrust uses two different strategies to implement TVM and PSM [12]. While Dynamic Trust Computation (DTC) uses fresh trust data gathered at run-time in the computation of the trust value, Approximate Trust Computation (ATC) uses a cache in order to accelerate the trust computation [3]. The computed trust values are used either to select the node with the highest trust value or to assist a node with determining whether to interact with another peer or not. For any peer, threshold trust value is the lowest value to trust.

PowerTrust is another reputation model for peer-to-peer networks. It relies on power nodes, nodes with more feedbacks, to aggregate the feedbacks of users and compute the global reputation scores of every peer [13]. Moreover, whenever a round of aggregation is completed, it updates the set of power nodes as the set of nodes with the highest reputation scores dynamically [3]. PowerTrust gathers all of the reputation scores v_j and the normalized local trust scores r_{j_i} from those nodes j who have previously interacted with node i so that the reputation score v_i of a node i can be calculated. r_{j_i} is defined using Equation 2.

$$r_{i_j} = \frac{S_{i_j}}{\sum_j S_{i_j}} \tag{2}$$

where s_{i_j} is the satisfaction of node i about the last interaction with node j. The aggregation needed to compute v_i is obtained using Equation 3.

$$v_i = (1-k).\sum_j (v_j X r_{i_j}) + k/m \tag{3}$$

The weight of power nodes is determined by the greedy factor, k. If i is an ordinary node, its global reputation score is computed using Equation 4.

$$v_i = (1-k).\sum_j (v_j X r_{i_j}) + k/m \tag{4}$$

In PowerTrust, each node is assigned a global reputation score aggregated from local trust scores weighted by the global reputations of all of the other nodes with a previous interaction with the former [3]. In addition, each power node receives an extra reinforcement. As well as achieving quick aggregation and high accuracy, PowerTrust is robust to resist malicious peers and suitable for supporting large-scale peer-to-peer applications [13]. Because of the replaceable set of power nodes, it is specifically reliable in case of dynamic behavior of peers.

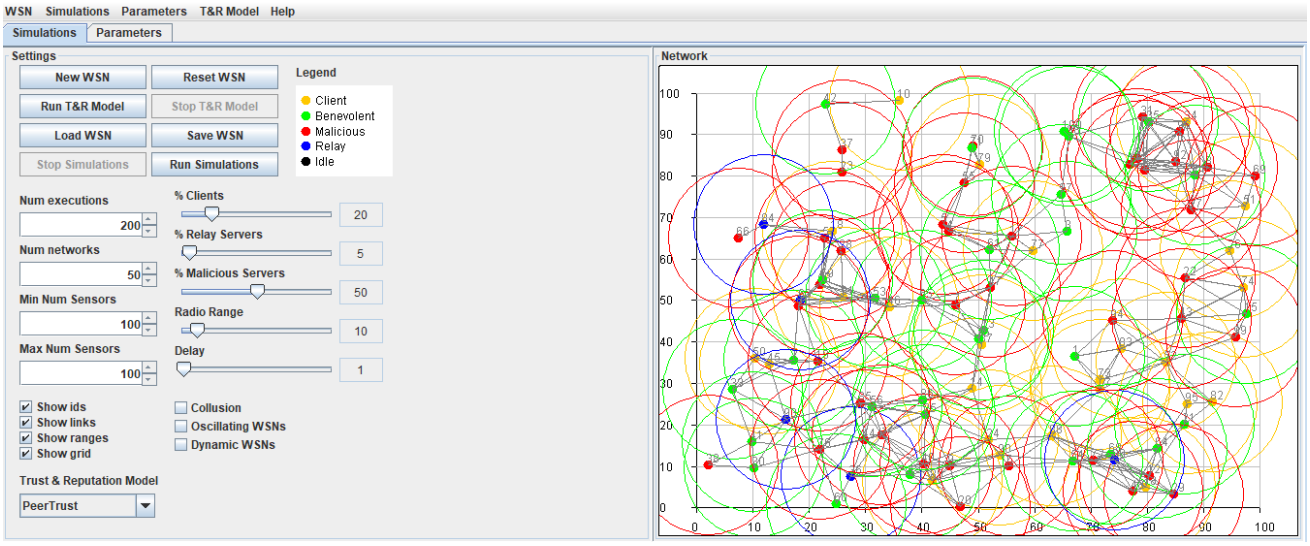
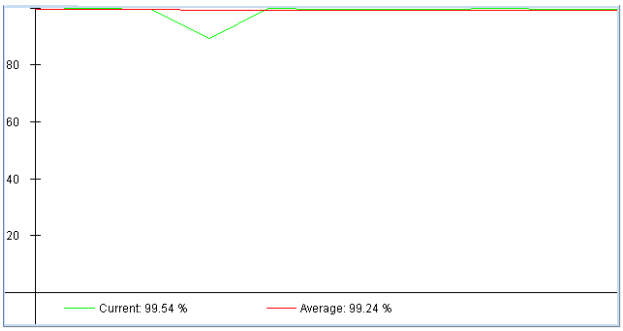


Fig. 1: Simulation environment.

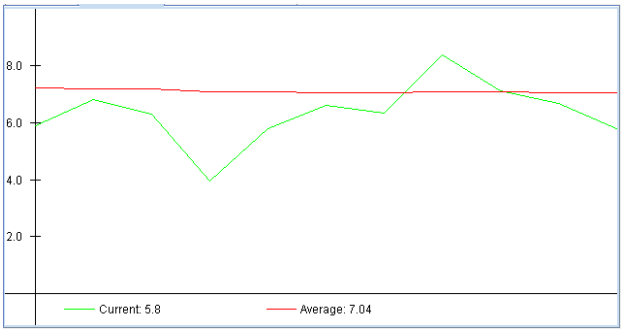
3. Performance Evaluation

Performance evaluation of PeerTrust and PowerTrust was performed by using the simulator [14] shown in Fig. 1. As shown Table 1, node positions for each scenario (total number of sensors: 100, 200 and 400) were the same for PeerTrust and PowerTrust. In the simulation study, oscillating server behavior option was not selected; therefore, malicious servers did not become benevolent or conversely after a predetermined number of iterations. Similarly, collusion option was not selected; therefore, malicious servers did not form collusions among themselves. As a rule of thumb, malicious servers assign their minimum rating for benevolent servers and their maximum rating for other malicious servers [14].

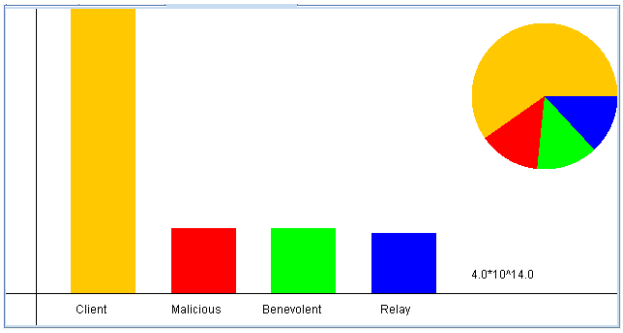
As can be seen from Figures 2-4, increasing the number of sensor nodes in the environment do not have any negative impact on the accuracy and path length performance metrics of PeerTrust. As expected, only the power consumption increases in parallel with the increase in the number of sensor nodes.



(a) accuracy (%)



(b) path length (m)

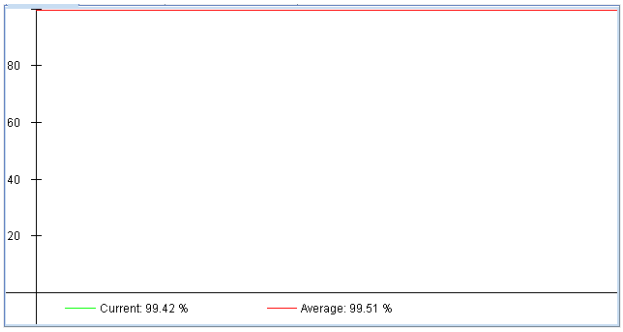


(c) power consumption (j)

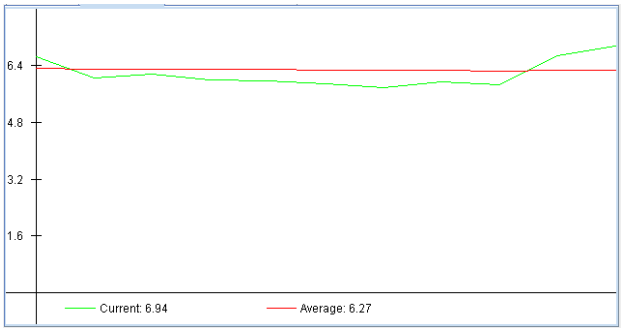
Fig. 2: Results obtained using PeerTrust (number of sensors: 100).

TABLE 1: Simulation parameters

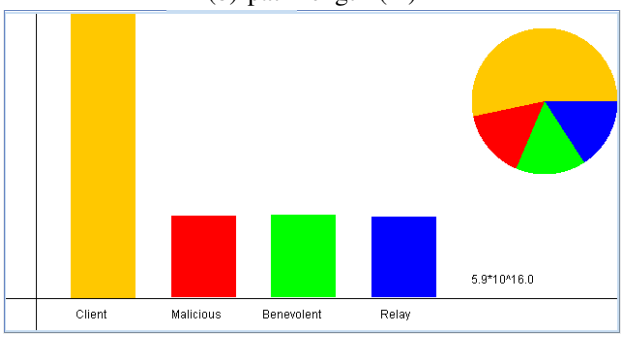
Paramater	Value
Number of executions	200
Number of networks	50
Number of sensors	100, 200, 400
Percentage of clients	20
Percentage of relay servers	5
Percentage of malicious servers	50
Delay (sec)	1



(a) accuracy (%)

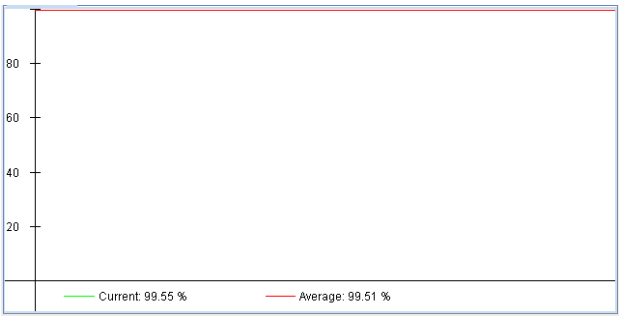


(b) path length (m)

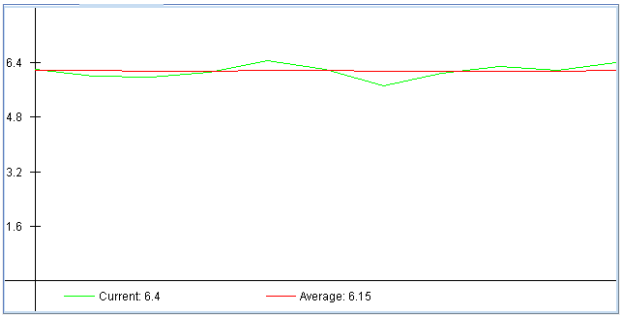


(c) power consumption (j)

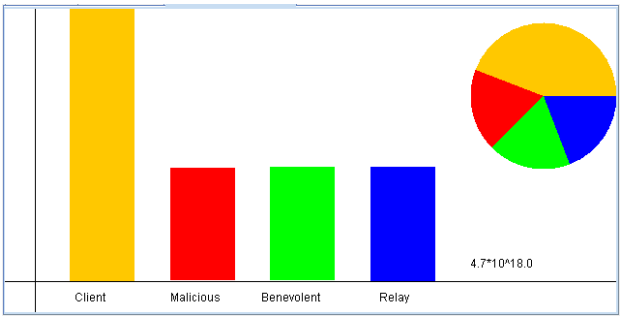
Fig. 3: Results obtained using PeerTrust (number of sensors: 200).



(a) accuracy (%)



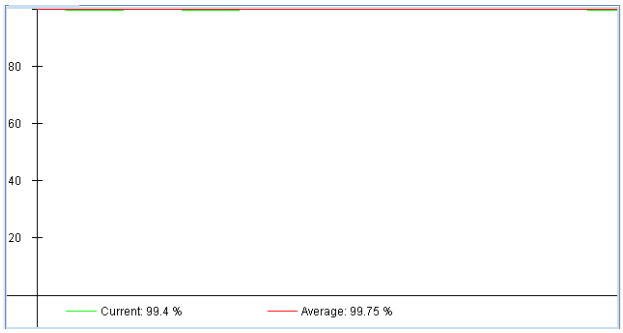
(b) path length (m)



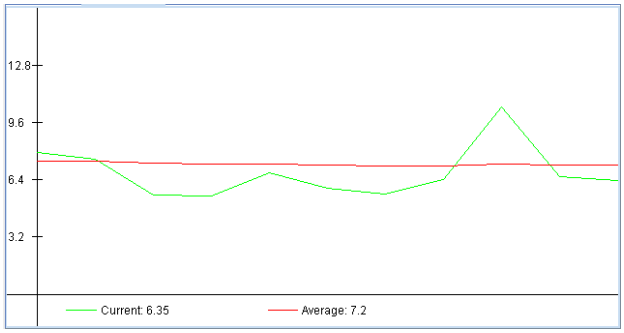
(c) power consumption (j)

Fig. 4: Results obtained using PeerTrust (number of sensors: 400).

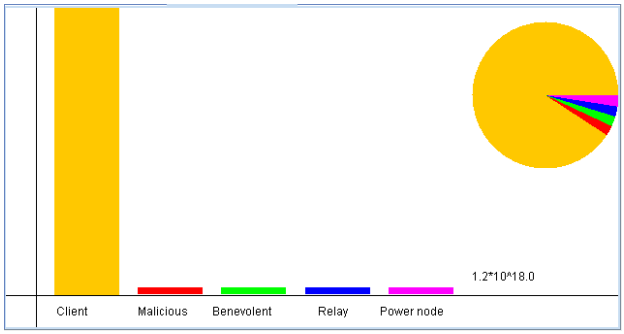
Similar to PeerTrust, as can be seen from Figures 5-7 that increasing the number of sensor nodes in the environment do not have any negative impact on the accuracy and path length performance metrics of PowerTrust. As expected, only the power consumption increases due to the increase in the number of sensor nodes. When all the results are taken into consideration, it can be seen that at the expense of higher power consumption, PowerTrust obtain slightly higher accuracy and less path length scores compared to PeerTrust. Although this study makes



(a) accuracy (%)

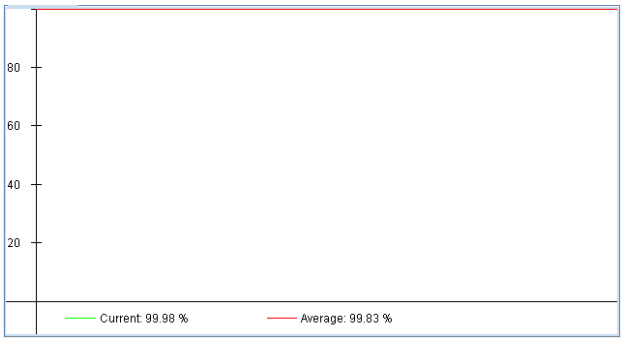


(b) path length (m)

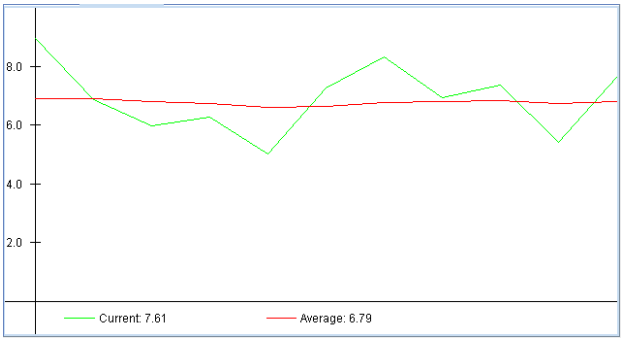


(c) power consumption (j)

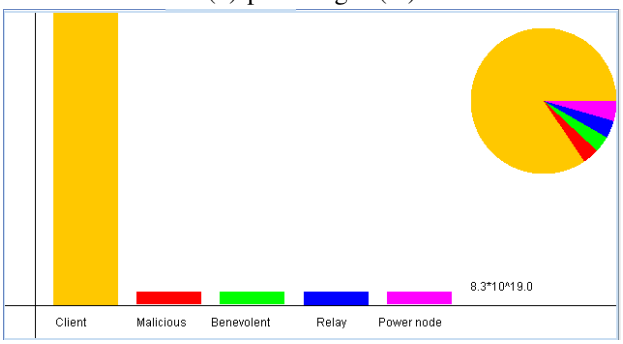
Fig. 5: Results obtained using PowerTrust (number of sensors: 100).



(a) accuracy (%)



(b) path length (m)



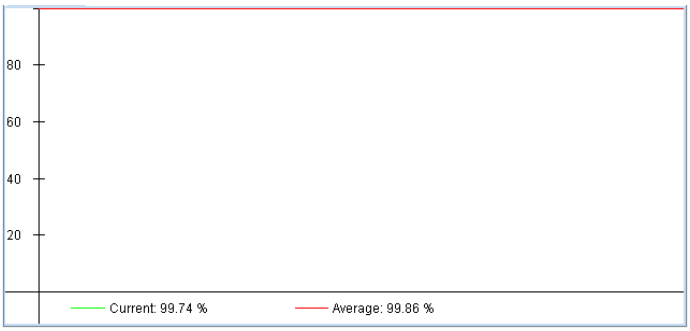
(c) power consumption (j)

Fig. 6: Results obtained using PowerTrust (number of sensors: 200).

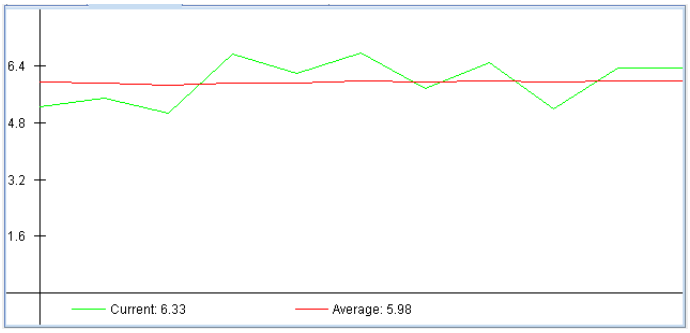
a comparison between PeerTrust and PowerTrust, the performance of reputation models depend on the application scenario and current system conditions as well as the expected performance metrics. Therefore, a smart multi-reputation engine based system that can dynamically select the most appropriate one of the provided reputation engines might be quite useful. However, this requires a seamless transition process between the previous reputation computation engine and the new one in order to prevent a sudden change in the computed reputation score. Also, for a certain period, both reputation values should be taken into consideration.

4. Conclusion

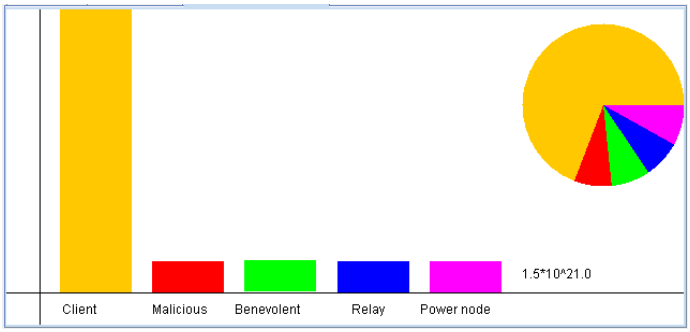
The decentralization of wireless sensor networks comes at the cost of data security. The distributed



(a) accuracy (%)



(b) path length (m)



(c) power consumption (j)

Fig. 7: Results obtained using PowerTrust (number of sensors: 400).

nature of wireless sensor networks makes them be vulnerable to attacks from malicious agents. Trust and reputation management models are effective tools to combat some of the potential security threats targeted at wireless sensor networks. Basically, trust and reputation management models help their users to decide how trustworthy the other party is before making a transaction. Different trust and reputation models were proposed to mitigate the adverse behavior of unreliable or malicious nodes in wireless sensor networks. However, our understanding of how to incorporate an effective trust and reputation system into these networks is still limited. Therefore, the specific features of the wireless sensor networks in which a trust and reputation system model is to be set up, in addition to the potential security threats that can reduce its accuracy should be studied and analyzed in order to decide which trust and reputation model suits better. Accordingly, in this study, the effectiveness of PeerTrust and PowerTrust is evaluated in terms of the effect of network size on accuracy, path length and power consumption in order to find out the most scalable trust and reputation model. As given in the paper, PowerTrust obtained slightly better results compared to PeerTrust in the scenarios held in this study. However, since there is a slight difference in the results of the two models, there is a possibility that if a different node distribution is applied, the results might change slightly on behalf of both models.

References

[1] I. F Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, vol. 38, no. 4, pp. 393-422, 2002.

[2] J. Grover and S. Sharma, "Security issues in Wireless Sensor Network - A review", in Proceedings of the 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 7-9 Sept. 2016.

[3] F. G. Marmol, and G. M. Perez, "Trust and reputation models comparison", Internet Research, vol. 21, no. 2, pp.138-153, 2011.

[4] R. Roman, C. Fernandez-Gago, J. Lopez, and H. H. Chen, "Trust and Reputation Systems for Wireless Sensor Networks", in Security and Privacy in Mobile and Wireless Networking, Eds. S. Gritzalis, T. Karygiannis, and C. Skianis, pp. 105-126, Troubador Publishing Ltd, 2009.

[5] F. G. Marmol and G. M. Perez, “Security threats scenarios in trust and reputation models for distributed systems”, Computer & Security, vol. 28, pp. 545-556, 2009.

[6] F. G. Marmol, J. G. Marin-Blazquez, and G. M. Perez, “LFTM,

Linguistic Fuzzy Trust Mechanism for distributed Networks", Concurrency and Computation: Practice & Experience, 2012.

[7] F. G. Marmol and G. M. Perez, "Providing Trust in Wireless Sensor Networks using a Bio-inspired Technique", Telecommunication Systems Journal, vol. 46, no. 2, pp. 163-180, 2011.

[8] G. Tuna, S. M. Potirakis, and G. Koulouras, "Implementing a Trust and Reputation Model for Robotic Sensor Networks", Elektronika Ir Elektrotechnika, vol. 19, no. 10, pp. 3-8, 2013.

[9] Z. Noorian and M. Ulieru, "The state of the art in trust and reputation systems: a framework for comparison", Journal of Theoretical and Applied Electronic Commerce Research, vol. 5, no. 2, pp. 97-117, 2010.

[10] J. Sabater-Mir and C. Sierra, "Review on Computational Trust and Reputation Models", Artificial Intelligence Review, vol. 24, no. 1, pp. 33-60, 2005.

[11] D. D. S. Braga, M. Niemann, B. Hellingrath, and F. B. D. L. Neto, "Survey on Computational Trust and Reputation Models", ACM Computing Surveys, vol. 51, no. 5, article no. 101, 2019.

[12] L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-Based Trust in Peer-to-Peer Communities", IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, pp. 843-857, 2004.

[13] R. Zhou and K. Hwang, "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. 460-473, 2007.

[14] F. G. Marmol and G. M. Perez, "TRMSim-WSN, trust and reputation models simulator for wireless sensor networks", in Proceedings of the IEEE International Conference on Communications, Dresden, Germany, 2009.