İSTANBUL UNIVERSITY CERRAHPAŞA

RESEARCH ARTICLE

Electrica 2020; 20(1): 10-18

The Impact of Increasing Number of Nodes on the Performance of Well-Known Trust and Reputation Models for Wireless Sensor Networks

Gürkan Tuna[1], Resul Daş[2]

[1]Department of Computer Programming, Trakya University, Edirne, Turkey
[2]Department of Software Engineering, Fırat University Technology Faculty, Elazığ, Turkey

Cite this article as: Tuna G, Daş R. The Impact of Increasing Number of Nodes on the Performance of Well-Known Trust and Reputation Models for Wireless Sensor Networks. *Electrica*, 2020; 20(1): 10-18.

ABSTRACT

In recent years, several trust and reputation management models have been proposed to address the security issues of wireless sensor networks. In wireless sensor networks, trust and reputation management systems basically allow sensor nodes to make their own opinion about how trustworthy other nodes are so that a higher number of successful transactions can be obtained and the probability of being defrauded reduced. To assess the performance of trust and reputation management systems a number of performance metrics were proposed. In this study, with the aim of finding out the most suitable trust and reputation model when the number of sensor nodes involved in a wireless sensor network has been increased, the performance of EigenTrust, Linguistic Fuzzy Trust Mechanism, PeerTrust and PowerTrust is evaluated in terms of accuracy rate and path length. The reason for focusing on this is that if a trust and reputation model is able to achieve the same accuracy rate and path length performance without any performance degradation when more sensor nodes are involved in the network, it can be considered as scalable. The results of our simulation studies prove that compared to the other models, Linguistic Fuzzy Trust Mechanism provides higher accuracy and less path length scores and is more suitable for large-scale deployments of wireless sensor networks.

Keywords: Wireless sensor network, node population, eigentrust, linguistic fuzzy trust mechanism, peertrust, powertrust, accuracy, range

Introduction

Wireless sensor networks offer numerous advantages, but because of their distributed architecture, they can be exposed to many security threats [1]. For each type of security threat, there are defense techniques in the literature. However, because the nodes in wireless sensor networks have limited computing capacity and memory, all defense techniques cannot be used in wireless sensor networks. Moreover, although traditional security solutions are able to successfully defend against the attacks of outsiders, their mechanisms generally fail when the attacks are done by compromised sensor nodes or insiders. While some of those attacks happen because of the intentional misbehavior of compromised or selfish nodes, others might be resulted from the unintentional behavior of faulty nodes [2, 3]. In this regard, reputation-based security solutions play a key role in finding out a mechanism to prevent such attacks by node behavior analysis [3].

It is known that one method of minimizing potential security risks when receiving a service is to determine whether the server is reliable [4]. This role is handled by trust and reputation management system. The main difference between trust and reputation management system roles in wireless sensor network is that while a trust management system produces a score that indicates the subjective opinion of the node on the reliability of another node or server, a reputation management system produces the reputation score of a node or server as seen by the entire wireless sensor network. In wireless sensor networks, a trust and reputation management system enables nodes to reliably assess the quality of offered services and the reliability of service providers before deciding to use one or more particular service(s) or interacting with or depending upon a given server. In the literature there are many trust and reputation management models but some of those models are suitable for peer to peer networks, particularly for wireless sensor networks.

Corresponding Author:
Resul Daş

E-mail:
rdas@firat.edu.tr

Received: 12.12.2019

Accepted: 10.01.2020

DOI: 10.5152/electrica.2020.19086

While there are many criteria that affect the performance of wireless sensor networks, it is very important that a wireless network can be extended to meet new needs in the future. Considering the importance of scalability, it is important to make evaluations in terms of different performance metrics. In this context, different approaches have been proposed to ensure scalability in terms of those metrics. In this study we mainly focus on the scalability related performance evaluation of four well-known models, namely EigenTrust [5], Linguistic Fuzzy Trust Mechanism (LFTM) [6], PeerTrust [7] and PowerTrust [8]. We particularly focus on accuracy and path length performance metrics of the compared models. The rest of this paper is as follows. The second section describes EigenTrust, LFTM, PeerTrust and PowerTrust trust and reputation management models. The third section presents the setting of the simulation environment and reports the results, and the fourth section concludes this paper.

EigenTrust, LFTM, PeerTrust, & PowerTrust

EigenTrust is a reputation management system that gathers the local trust values of all peers with minimal message complexity overhead [5]. It relies on asking a peer's acquaintances about their opinions about other peers and the notion of transitive trust. Furthermore, the peer will possibly trust the opinions of those peers who have delivered it authentic messages or files. Because those peers who act honestly about the messages or files they deliver will possibly report their local trust values honestly [5]. Each peer *i* is able to retain the number of satisfactory transactions that it carries out with peer *j, Sat(i, j)* and the number of unsatisfactory transactions that it carries out with peer *j, Unsat(i, j)*. Then, local trust value S_{ij} is calculated using (1).

$$S_{ij} = Sat(i,j) - Unsat(i,j) \tag{1}$$

Before aggregating local trust values, EigenTrust first normalizes them. EigenTrust defines a normalized local trust value, N_{ij}, using (2).

$$N_{ij} = \frac{\max(S_{ij},0)}{\sum_j max(S_{ij},0)} \tag{2}$$

EigenTrust asks for each peer to ask its acquaintances about their opinions about other peers. This way it weighs their opinions placed by the trust peer *i* using (3).

$$T_{ik} = \sum_j N_{ij} N_{jk} \tag{3}$$

where T_{ik} denotes the trust placed in peer *k* by peer *i*, based on asking its acquaintances.

Linguistic Fuzzy Trust Mechanism adapts a bio-inspired trust model similar to the human way of thinking, instead of adapting a trust model that makes use of some reasoning mechanisms and techniques that cannot be understood by humans [6]. It also relies on fuzzy reasoning. LFTM is built upon the enhancement on BTRM-WSN [9]. BTRM-WSN is a bio-inspired algorithm based on the notion of well-known ant colony systems [10, 11], in which pheromone traces denote the probability of discovering the most reputable node through the most trustworthy path. In this way, BTRM-WSN follows the five common steps for trust and reputation management models as given in [12]. When BTRM-WSN is executed, its algorithm first deploys a group of artificial ants over the wireless sensor network so that using the pheromone traces left by those ants the most trustworthy node that provides a certain service can be found. In the second step, when a path going to a node that provides the requested service is found, a score is given to each of those paths using (4).

$$Q(P_i) = \frac{avg_i}{Length(P_i)^F} . \%Ants_i \tag{4}$$

where $Q(P_i)$ denotes the path returned by ant *i*, avg_i denotes the average pheromone of that path, *F* denotes the path length factor, and finally $\%Ants_i$ denotes the percentage of ants that used the same paths as ant *i*.

In the third step, BTRM-WSN selects the path P_i with the highest value of (P_i) as a path that goes to the most trustworthy service provider in the wireless sensor network. In the fourth step, the client requests the service from the selected node explicitly. Then, the client assesses the service it received and measures its satisfaction with that transaction. Finally, if that service satisfied the client, a reinforcement is made. However, if the service provider cheated, a punishment is made [9]. LFTM enhances BTRM-WSN by interpreting some concepts including goodness, client satisfaction, punishment or reward decision, and quality of service at a higher level [6]. Those sophisticated features are realized by the application of fuzzy sets, fuzzy logic, and linguistic labels. LFTM selects the service provider with a perceived goodness, such as medium, high, or very high, to have a transaction with using BTRM-WSN [6]. When the desired attributes of the service and the goodness of the service provider are taken into consideration, the service provider delivers a worse, equal, or better service than the expected. A comparison is made between these desired ones and provided ones using a set of weights for the attributes of the provided service. Then the satisfaction of the client is evaluated and based on it, the punishment level is determined [6].

PeerTrust consists of an adaptive, decentralized trust model. It relies on a transaction-based feedback assessment system and commonly-used trust parameters, namely, feedbacks that a peer obtains from other peers, the total number of transactions that a peer carries out, and the credibility of the feedback sources, and additional factors in measuring trustworthiness of peers, namely, adaptive transaction context factor (ATCF) and adaptive community context factor (ACCF), and provides a general trust metric to integrate all of those parameters [7]. PeerTrust implements its basic trust metrics in two different ways and computes its general trust for peer *e* using (5) [7].

$$G(e) = k \cdot \sum_{i=1}^{T(e)} N(e,i) \cdot C\big(p(e,i)\big) \cdot AT(e,i) + l \cdot AC(e) \tag{5}$$

where *k* represents the normalized weight factors for the collective assessment and *I* denotes the community context factor. *G(e)* represents the total number of transactions carried out by peer *e* with all other peers, *p(e,i)* represents the other peer that participates in peer *e*'s *i*th transaction, *N(e,i)* represents the normalized amount of satisfaction that peer *e* receives from peer *p(e,i)* in its *i*th transaction, *C(e)* represents the credibility of the feedback delivered by peer *e*, *AT(e,i)* represents ATCF for peer *e*'s *i*th transaction, and finally *AC(e)* represents ACCF for peer *e*.

PowerTrust leverages the power-law feedback characteristics. Employing a distributed ranking technique, it automatically picks a set of power nodes, i.e. the most reputable ones. By the use of a look-ahead random walk approach and the power nodes, it offers good accuracy in terms of global reputation and high aggregation speed. Moreover, it is resistant to disturbance by malicious peers and quickly adapts to dynamics in joining and leaving of peers [8]. PowerTrust obtains all of the reputation scores R_j and the normalized local trust scores L_{ji} from those nodes *j* which have had an interaction with node *i* formerly. In this way, it computes the reputation score R_i of node *i* [8]. The weight of power nodes employed by PowerTrust is determined by the greedy factor, *k*. L_{ji} is defined using (6) [8].

$$L_{ij} = \frac{s_{ij}}{\sum_j s_{ij}} \tag{6}$$

where S_{ij} denotes the satisfaction of node *i* regarding the last interaction with node *j*. If *i* is not an ordinary node, the global reputation score of the node, R_i, is obtained using (7). Otherwise it is obtained using (8).

$$R_i = (1-k)\cdot\sum_j(R_j \times L_{ji}) + k/m \tag{7}$$

$$R_i = (1-k)\cdot\sum_j(R_j \times L_{ji}) \tag{8}$$

Except for the common properties of all trust and reputation management models, as abovementioned the methodology of behind the compared models, EigenTrust, LFTM, PeerTrust and PowerTrust, is quite different. Although this makes it difficult to make a quantitative evaluation between them, there are some tools that allow researchers to compare the performance of trust and reputation management models. Path length, accuracy, and power consumption are the leading metrics used in most comparison studies. Similarly in this study accuracy and path length performance of EigenTrust, LFTM, PeerTrust and PowerTrust are compared. For a trust and reputation management model, accuracy is an indicator of the success of the model and shows the percentage that the number of times when the model successfully selects trustworthy nodes considering the total number of transactions. Path length can be described as the average number of hops that leads to the most trustworthy nodes selected by the client. Less path length is desirable since it is an indicator of better performance in terms of response time, energy efficiency, and smoothness in searching for trustworthy nodes.

Performance Evaluation

In reality, there is no standard model that allows a fair comparison between reputation-based trust systems that compete to provide higher resilience to attacks or higher level of security [11]. The main reason of this is that most reputation-based trust systems do not consist of all reputation components and this makes the comparison difficult or practically not applicable [13]. However, considering the role of scalability in wireless sensor networks, in this study we particularly focus on the evaluation of accuracy and path length performance metrics.

Performance evaluation of EigenTrust, LFTM, PeerTrust and PowerTrust was carried out by using the simulator proposed in [14]. The distribution of sensor nodes in the environment for 50 nodes is given in Figure 1 and parameters preferred in the simulation environment are given in Table 1. The positions of sensor nodes for each scenario (total number of sensor nodes: 50, 100, and 150) were the same for all the trust models and sensor nodes did not have the capability of movement. Oscillating server behavior was not allowed; hence, malicious servers did not become malicious or conversely after a number of iterations. In the simulation studies, malicious servers were not allowed to form collusions among them.

Table 1. Parameters preferred in the simulation environment

Parameter	Value
Number of repetitions	50
Number of wireless sensor networks	50
Number of sensor nodes in each wireless sensor network	50, 100, 150
Percentage of clients	15
Percentage of relay servers	5
Percentage of malicious servers	70
Delay (second)	0
Radio range (m)	12

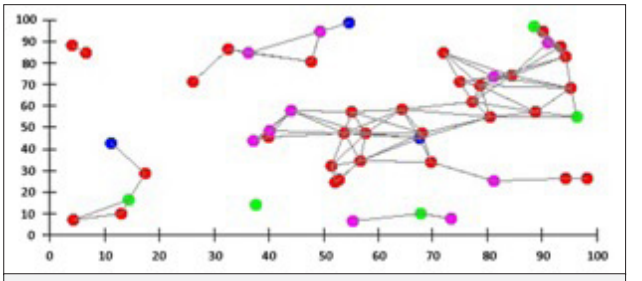

Figure 1. Simulation scenario for 50 nodes. Please note that green dots represent benovelent nodes, red dots represent malicious nodes, blue nodes represent relay nodes, and pink dots represent clients, respectively

As can be seen from Figures 2-4, increasing the number of sensor nodes in the environment did not have significant negative impact on the accuracy, i.e. the success rate when selecting a trustworthy or benevolent server, and path length performance metrics of EigenTrust. It can be concluded that EigenTrust is scalable and can be implemented in large-scale deployments of wireless sensor networks.

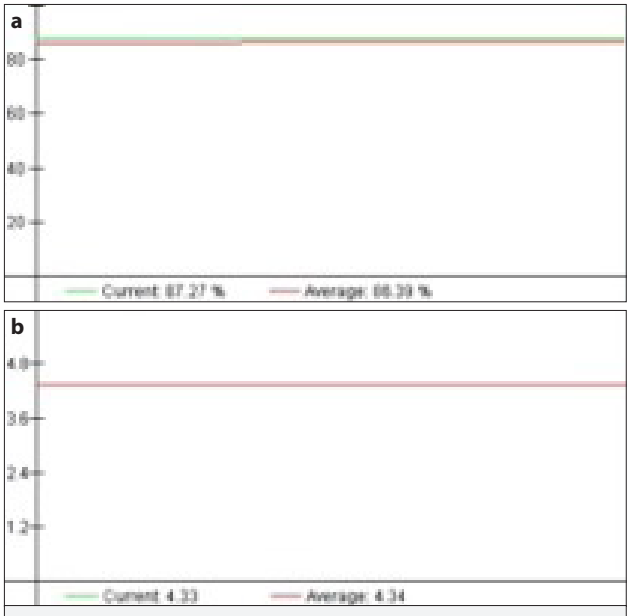

Figure 2. a, b. Results obtained using EigenTrust (Number of wireless sensor networks: 50, Number of nodes: 50). Accuracy (%) (a), path length (m) (b)

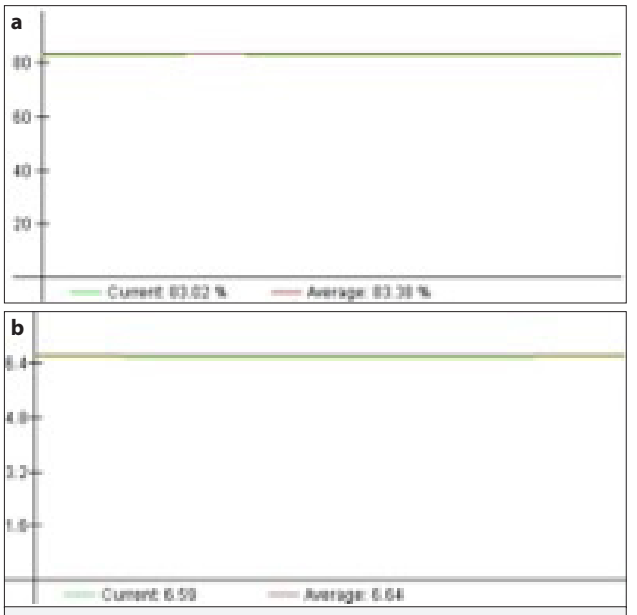

Figure 3. a, b. Results obtained using EigenTrust (Number of wireless sensor networks: 50, Number of nodes: 100). Accuracy (%) (a), path length (m) (b)

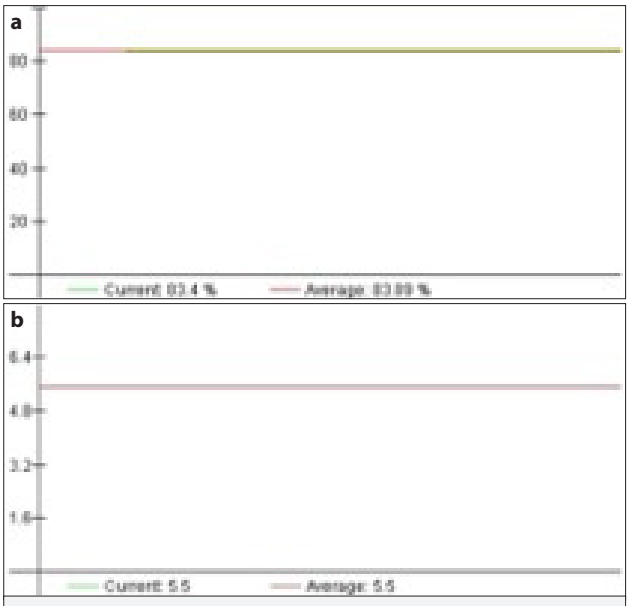

Figure 4. a, b. Results obtained using EigenTrust (Number of wireless sensor networks: 50, Number of nodes: 150). Accuracy (%) (a), path length (m) (b)

As can be seen from Figures 5-7, increasing the number of sensor nodes in the environment did not have negative impact on the accuracy and path length performance metrics of LFTM. However, when there are more sensor nodes in the environment, LFTM provided higher accuracy and almost the same path length. It can be concluded that LFTM is highly scalable and can be implemented in large-scale deployments of wireless sensor networks.

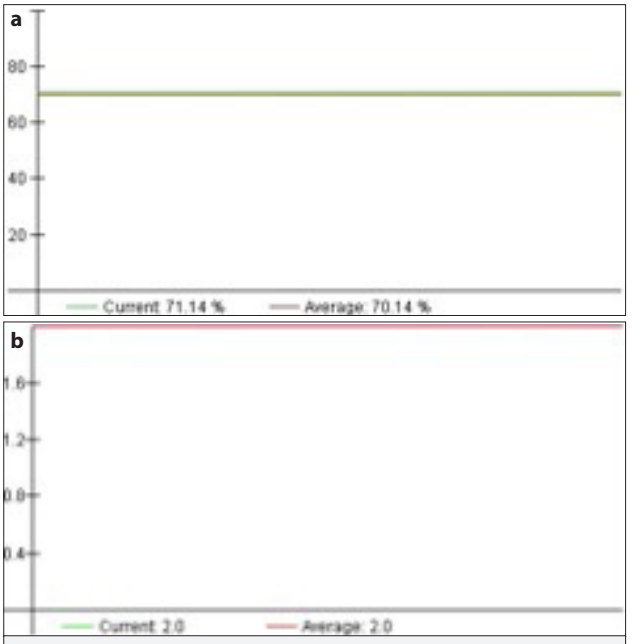

Figure 5. a, b. Results obtained using LFTM (Number of wireless sensor networks: 50, Number of nodes: 50). Accuracy (%) (a), path length (m) (b)

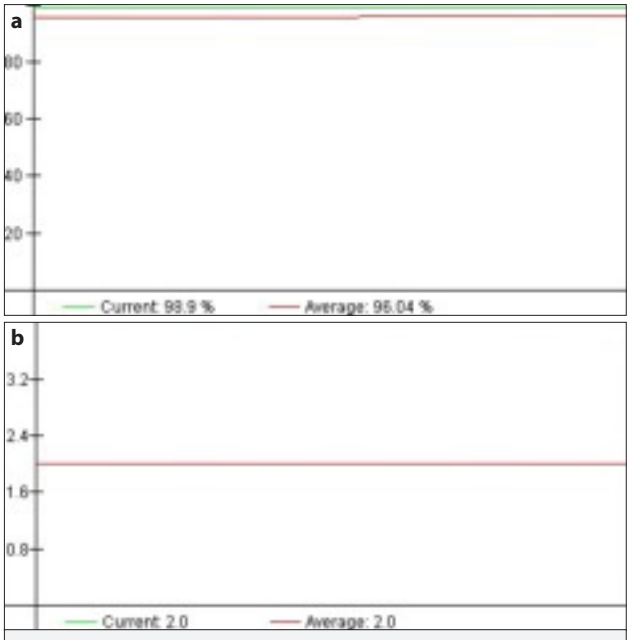

Figure 6. a, b. Results obtained using LFTM (Number of wireless sensor networks: 50, Number of nodes: 100). Accuracy (%) (a), path length (m) (b)

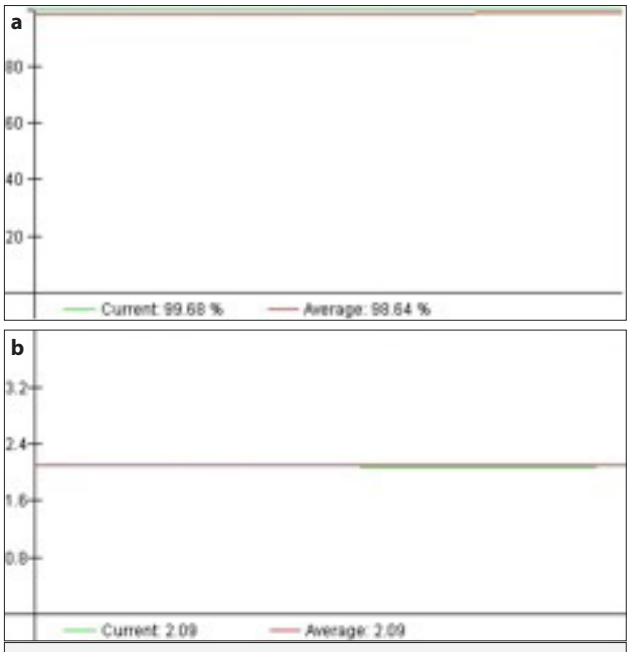

Figure 7. a, b. Results obtained using LFTM (Number of wireless sensor networks: 50, Number of nodes: 150). Accuracy (%) (a), path length (m) (b)

Similarly, as can be seen from Figures 8-10, increasing the number of sensor nodes in the environment did not have negative impact on the accuracy and path length performance metrics of PeerTrust. It can be concluded that PeerTrust is scalable and can be implemented in large-scale deployments of wireless sensor networks, too.

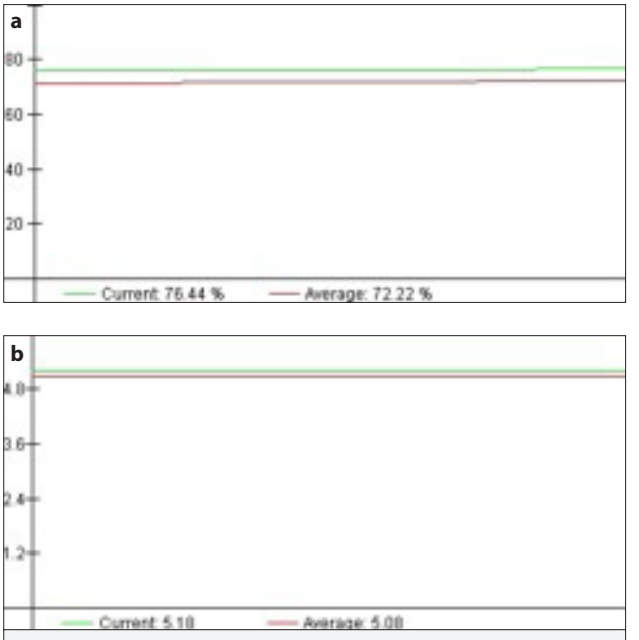

Figure 8. a, b. Results obtained using PeerTrust (Number of wireless sensor networks: 50, Number of nodes: 50). Accuracy (%) (a), path length (m) (b)

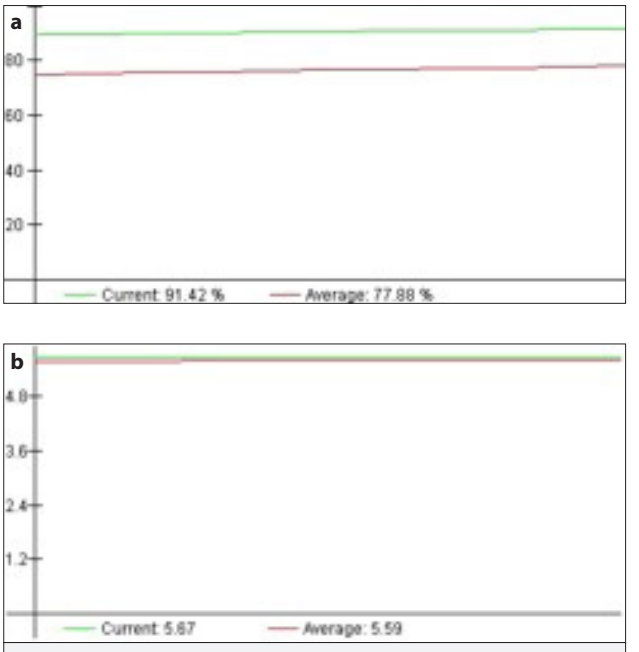

Figure 9. a, b. Results obtained using PeerTrust (Number of wireless sensor networks: 50, Number of nodes: 100). Accuracy (%) (a), path length (m) (b)

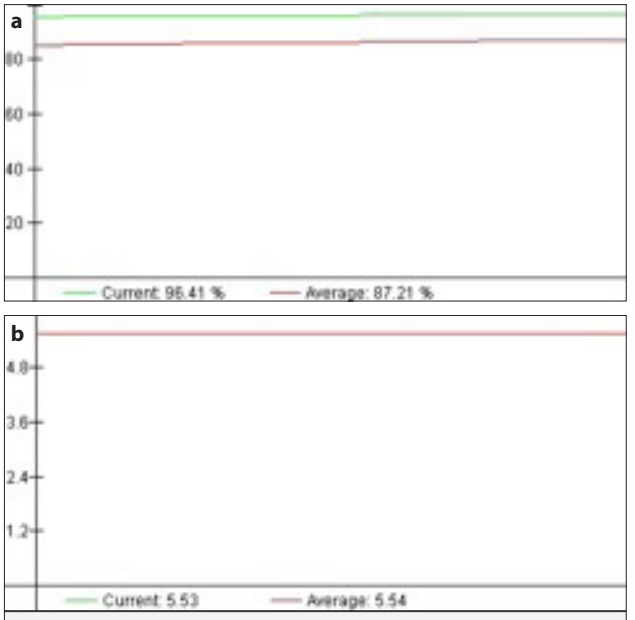

Figure 10. a, b. Results obtained using PeerTrust (Number of wireless sensor networks: 50, Number of nodes: 150). Accuracy (%) (a), path length (m) (b)

However, as can be seen from Figures 11-13, although increasing the number of sensor nodes in the environment did not have negative impact on the accuracy of PowerTrust, it resulted in worse path length performance. It can be concluded that in terms of accuracy, PeerTrust is scalable and can be implemented in large-scale deployments of wireless sensor networks, too.

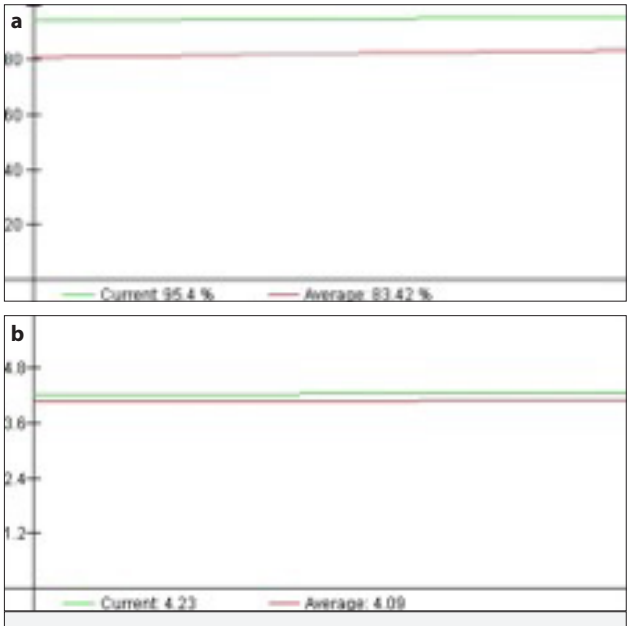

Figure 11. a, b. Results obtained using PowerTrust (Number of wireless sensor networks: 50, Number of nodes: 50). Accuracy (%) (a), path length (m) (b)

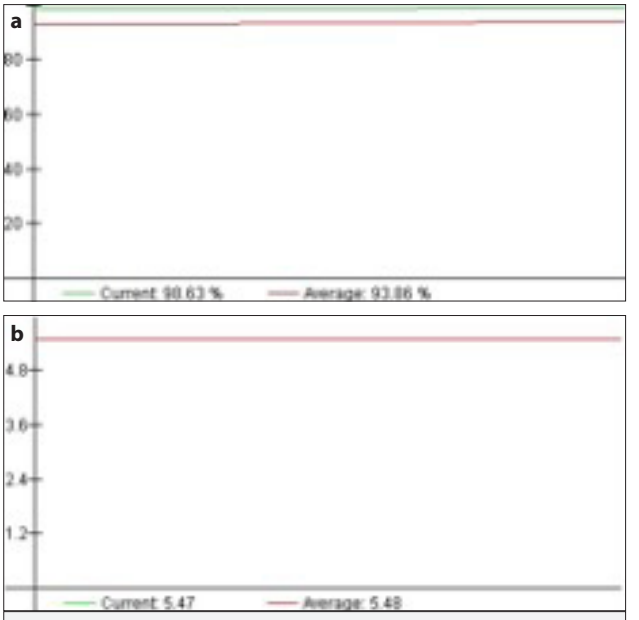

Figure 12. a, b. Results obtained using PowerTrust (Number of wireless sensor networks: 50, Number of nodes: 100). Accuracy (%) (a), path length (m) (b)

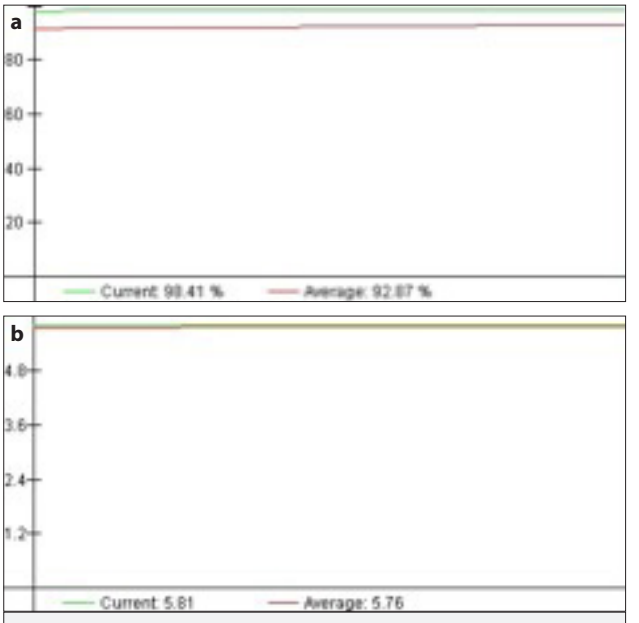

Figure 13. a, b. Results obtained using PowerTrust (Number of wireless sensor networks: 50, Number of nodes: 150). Accuracy (%) (a), path length (m) (b)

When all the results are taken into consideration, LFTM obtained higher accuracy and less path length scores compared to EigenTrust, PeerTrust and PowerTrust. Although the simulation studies in this study were limited, each simulation study was repeated 50 times to obtain average values of accuracy and path length. LFTM seems to be more suitable for large-scale deployments of wireless sensor networks. However, it should be taken into consideration that the performance of all

reputation models depends on the application scenarios and most prioritized performance metrics. Moreover, in open network environments such as wireless sensor networks, the trust between sensor nodes can dynamically vary with behavior and time and the trust value computed by the applied model can change depending on the communication behavior between the nodes, too [15]. Hence, in every trust and reputation model defining trust relationships while improving the efficiency of the model becomes a major issue [15]. In this regard, a multi-model trust and reputation system that allows switching to the most appropriate trust model might be quite useful [4].

While the results given in this paper can be useful for researchers and practitioners, in addition to accuracy and path length, other metrics such as radio range, hop count, packet loss and energy consumption should also be considered in order to enhance accuracy of a computed trust value. In addition, most reputation-based trust management systems are questionable in practice, because the predefined threshold may significantly deviate from the practical situation [16]. Another limitation of most reputation-based trust management systems is that they compute trust values based on interactions among sensor nodes. On the other hand, they generally do not consider how to preserve privacy in the computation of the trust values [16]. Finally, most of them rely on entity-centric mechanisms and evaluate trustworthiness based on the past behavior of nodes and the recommendations from neighbor nodes; they do not take how to efficiently predict future trust values into account [16]. Considering the shortcomings of the existing trust and reputation management systems, exponential distribution was proposed to enhance the accuracy of trust assessment [17]. Compared to the existing trust and reputation management models that rely on the beta distribution, the exponential distribution approach is based on the time interval of independent random events and only employs the time interval between successive neighbor cooperation to compute trust values without taking the other states into consideration. This way, it prolongs the network lifetime significantly. Although the models evaluated in this study provide satisfactory accuracy and path length performance for wireless sensor networks, energy consumption is an important factor for the lifetime of sensor nodes. Therefore, novel schemes that can reduce energy consumption significantly are needed [18, 19].

Conclusion

The decentralized nature of wireless sensor networks makes them exposed to a number of security attacks from malicious servers. Trust and reputation management models proposed for wireless sensor networks help nodes to decide how trustworthy or reputable another node is before realizing a transaction. Each trust and reputation management model has some distinct advantages and disadvantages; therefore, it can provide high accuracy in some scenarios or vice versa. Scalability is an important factor for the long-term reliable operation of wireless sensor networks and an indicator of whether a wireless sensor network can provide the same service at the same performance when it involves more nodes. In this paper a number of simulation studies were performed in order to find out which one of EigenTrust, LFTM, PeerTrust and PowerTrust is more scalable and suitable for large-scale deployments of wireless sensor networks. As given in the paper, LFTM obtained slightly better accuracy compared to the other models but much better range performance in the simulation studies realized in this study. However, since there is a slight difference in the results of the compared models, if a different node distribution is applied, the results might change. Future work of this study consists of field tests using a set of real sensor nodes.

Peer-review: Externally peer-reviewed.

Conflict of Interest: The authors has no conflicts of interest to declare.

Financial Disclosure: The authors declared that the study has received no financial support.

References

1. J. Grover, S. Sharma, "Security issues in Wireless Sensor Network - A review", Proceedings of the 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2016. [CrossRef]
2. S. Li, Y. Li, "Distributed Range-Free Localization of Wireless Sensor Networks via Nonlinear Dynamics", in Wireless Sensor Networks - Technology and Protocols, Eds. Mohammad A. Matin, Intech Open, 2012.
3. S. Ganeriwal, M. Srivastava, "Reputation-based framework for high integrity sensor networks", Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, pp. 66-77, 2004. [CrossRef]
4. F. G. Marmol, G. M. Perez, "Trust and reputation models comparison", Internet Research, vol. 21, no. 2, pp. 138-153, 2011. [CrossRef]
5. S. Kamvar, M. Schlosser, H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks", WWW03: Proceedings of the 12th international conference on World Wide Web, pp. 640-651, 2003. [CrossRef]
6. F. G. Marmol, J. G. Marin-Blazquez, G. M. Perez, "LFTM, Linguistic Fuzzy Trust Mechanism for Distributed Networks", Concurrency and Computation: Practice & Experience, 2012.
7. L. Xiong, 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. [CrossRef]
8. R. Zhou, 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. [CrossRef]
9. F. G. Marmol, 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. [CrossRef]
10. M. Dorigo, T. Stützle. Ant Colony Optimization. Bradford Book: Cambridge, MA, 2004. [CrossRef]
11. M. Dorigo, V. Maniezzo, A. Colorni, "Ant System: Optimization by a colony of cooperating agents", IEEE Transactions on Systems, Man, and Cybernetics-Part B, vol. 26, no. 1, pp. 29-41, 1996. [CrossRef]
12. S. Marti, H. Garcia-Molina, "Taxonomy of trust: categorizing P2P reputation systems", Computer Networks, vol. 50, no. 4, pp. 472-484, 2006. [CrossRef]

13. H. Alzaid, M. Alfaraj, S. Ries, A. Jøsang, M. Albabtain, A. Abuhaimed, "Reputation-Based Trust Systems for Wireless Sensor Networks: A Comprehensive Review", 7th Trust Management (TM), Jun 2013, Malaga, Spain. pp. 66-82. [CrossRef]
14. F. G. Marmol, 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. [CrossRef]
15. X. Yin, S. Li, S., "Trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks", EURASIP Journal on Wireless Communications and Networking, vol. 2019, pp. 198, 2019. [CrossRef]
16. G. Han, J. Jiang, L. Shu, J. Niu, H.-C. Chao, "Management and applications of trust in Wireless Sensor Networks: A survey", Journal of Computer and System Sciences, vol. 80, no. 3, pp. 602-617, 2014. [CrossRef]
17. J. Zhao, J. Huang, & N. Xiong, "An Effective Exponential-Based Trust and Reputation Evaluation System in Wireless Sensor Networks", IEEE Access, vol. 7, pp. 33859-33869, 2019. [CrossRef]
18. Z. Chen, L. Tian, & C. Lin, "Trust Model of Wireless Sensor Networks and Its Application in Data Fusion", Sensors (Basel), vol. 17, no. 3, pp. 703, 2017. [CrossRef]
19. D.D.S. Braga, M. Niemann, B. Hellingrath, F.B.D.L. Neto, "Survey on Computational Trust and Reputation Models", ACM Computing Surveys, vol. 51, no. 5, pp. 101, 2019. [CrossRef]

Gurkan Tuna is currently an Professor at the Department of Computer Programming of Trakya University, Turkey. He has authored several papers in international conference proceedings and refereed journals, and has been actively serving as an Associate Editor for IEEE Access and Australian Journal of Electrical and Electronics Engineering journals. His current research interests include smart cities, smart grid, wireless sensor networks, underwater networks and M2M communications.

Resul Daş has been working as Associate Professor in the Department of Software Engineering at the University of Firat, where he has been a faculty member since 2011. From 2000 to 2011 he served as both instructor and network administrator at the Department of Informatics at the Firat University. He is the instructor and the coordinator of Cisco Networking Academy Program since 2002 at this university. He graduated B.S. and M.S. degrees from the Department of Computer Science at the Fırat University in 1999 and 2002 respectively. Then he completed his Ph.D. degree at the Department of Electrical-Electronics Engineering at the same university in 2008. He also worked between September 2017 and June 2018 as a visiting professor at the Department of Computing Science at the University of Alberta, Edmonton, Canada. He has authored more than seventy papers in international conference proceedings and refereed journals and has been actively serving as a reviewer for international journals and conferences. And also he has been serving as Associate Editor for Journal of IEEE Access and Turkish Journal Electrical Engineering and Computer Science. His current research areas include computer networks and network security, cyber-security, software design and architecture, IoT/M2M applications, knowledge discovery, and multi-sensor data fusion.