Indian Journal of Science and Technology, Vol 9(37), DOI: 10.17485/ijst/2016/v9i37/92135, October 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Improved Modified Reputation-Base Trust for Wireless Sensor Networks Security

Abdullah Said Alkalbani[1]* , Teddy Mantoro[2] and Abu Osman Md Tap[3]

[1]Electrical and Computer Engineering Department, College of Engineering, University of Buraimi, Sultanate of Oman, Al-Buraimi; abdullah.s@uob.edu.om
[2]Faculty of Science and Technology, Universitas Siswa Bangsa International (USBI), Jakarta, Indonesia; teddy@ieee.org
[3]Department of Computer Science, KICT, International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia; kict.iium.edu.my

Abstract

Background/Objectives: Trust, reputation and power resources limits of WSNs are active matters. In this paper Modified Reputation Based-Trust Mechanism (MRT) enhanced to minimize power consumption and increase privacy at the same time. **Methods/Statistical analysis:** Two security testing threats considered during simulation of proposed trust and reputation model in order to evaluate model efficiency and trustworthy. The first testing threat has to do with the oscillating behavior of the pernicious nodes offering the required service. The another threat applied contains of the possibility for the malicious nodes to sort a collusion through themselves. **Findings:** Simulation results prove limited energy consumption and enhancement is security better than previous studies. **Application/Improvements:** Proposed mechanism has security strengths against malicious nodes with oscillating and collusion effects. Results prove that its remains malleable to high percentages of malicious servers when the percentage of client sensors are greater than 60%.

Keywords: Collusion, Modified Reputation-Base Trust, Oscillating, Power Consumption, Trust and Reputation Modls, Wireless Sensor Networks (WSNs)

1. Introduction

Security and trust challenges in WSNs have been widely investigated by many studies and remain an active area for research and development[1].

The size of network sensors is small and its ability to gather information, process data, and communicate with other sensors, Radio Frequency (RF) channels. WSNs are developed to detect events or phenomena, gather and process data, and transmit this data to base station.

Sensor Networks and related technologies have become very active the last decade. This is due to the truth that the technology is maturing and moving out of the purely research driven environment into commercial interests[2,3]. WSNs used to collect data and to track and detect events by providing coverage and message forwarding to base station. However, the inherent characteristics of a sensor network limit its performance and sensor nodes are supposed to be low-cost. An attacker can control a sensor node undetectably by physically exposing the node, an adversary can potentially insert faulty data or misbehavior to deceive the WSNs. Authentication mechanisms and cryptographic methods alone cannot be used to completely solve this problem because internal malicious nodes will have valid cryptographic keys to access the other nodes of the networks. Also conventional security methods cannot be used for WSNs due to power and processing limitations. In addition to the node malicious raids, the nodes are also vulnerable to system faults for low-cost hardware of these nodes[4].

Recently, a new mechanism has been offered for WSNs security improvement. This mechanism relies on constructing trust systems through analysis of nodes observation about other nodes in the network[5,6]. Currently, most of the trust evaluation structure belongs to a recommendation-based methodology such that the

* Author for correspondence

evaluation results are usually dependent on the accurate measurement of the forwarding behaviors of adjoining nodes and on the recommenders' honesty degree[7].

This article shows the last enhancement for WSNs by improving MRT mechanism found in literature[8]. Research on the trust and reputation model is proposed for optimization in terms of security and scalability. This model is evaluated through applying security threats such as collusion and oscillating of malicious nodes in WSNs.

The remainder of the paper is structured as follows: In Section 2, the related work in this area is given. Section 3 describes the steps of generic trust and reputation model. Section 4 shows our research framework. Mathematical models are presented in Section 5. In Section 6, extensive experiments by simulation are conducted to prove the accuracy and security of the proposed model. The results discussion is given in Section 7 and the last section; conclusion, as well as the challenges encountered and propositions on our future direction.

2. Related Work

Networks and data protection is very important issue for modern systems. The main challenges for security issue in WSNs are balancing between security and power consumption. There are many solutions for security in traditional networks which not suitable for wireless networks due to high calculations needed and limits of resources available.

The research by[9] defines some attacks that show destructive to many essential WSN routing protocols. The security threats of WSN mainly contain both external and internal attacks. External attacks can be avoided by conventional encryption mechanism but it is not effective against internal attacks. As an important measure, reputation evaluation technique has direct effect on internal attacks[10]. It has become an important factor to defend against internal attacks and it has received high concern. In last decade, researches have been conducted on the applying of reputation systems to sensor networks[9]. Meanwhile only[11,12] have concentrated on the use of reputation systems in WSN.

Nowadays, there are many applications use trust and reputation mechanisms for minimizing certain risks not completely covered by conventional network security mechanisms, providing good protection[13]. Some researchers do related research on the application of reputation rating technique in security routing protocol[14], and proposed some simulating methods for reputation evaluation models in WSNs. Analyzing and evaluation of trust and reputation methods conducted by many researchers such as work in[15–18], whereas simulation tools used for evaluation presented in[18].

Moreover, some researchers have directed their effort in developing new trust and reputation models in the last decade. We have surveyed the related literature and have realized that most of those developers focused on describing their approaches. Many experiments presented and analyzed by researchers in order to prove the reliability of their proposals under certain conditions or circumstances. In[19] the use of Watchdog and Pathrater has suggested. Watchdog listens to the data transmission of the next node in the path to detect naughtiness. Pathrater keeps the ratings for other nodes and performs route selection by choosing routes that do not contain selfish nodes. However, the Watchdog mechanism needs high memory overhead to maintain the state information on the monitored nodes and the transmitted packets.

Researchers' in[20] submitted a trust model to identify the trustworthiness of sensor nodes and to filter out the data transmitted by malicious nodes. In this model, researchers assume that every sensor node has knowledge of its own location coordinates, nodes are densely deployed and time is coincided. They evaluated trust in a conventional way, weighting the trust factors and there is no update of trust.

Architecture based on reputation to create a network of autonomous sensors capable of detecting most kind of attacks and network failures using an anomaly detection system together with specification-based detection system have proposed in [21]. All this was created from the premise of designing a system that suit the characteristics of sensor networks and maintains the protocol as lightweight as possible to guarantee the autonomy of the nodes.

In addition, researchers' in[22] described one approach called PeerTrust model. This model has two major specifications. Firstly, it introduces two adaptive factors and three basic trust factors in evaluating trustfulness of peers, called, feedback a peer receives from other peers, the total number of transactions a peer performs, the trustiness of the feedback sources, transaction context parameter, and the community context parameter. Second, it determines a general trust metric to combine these parameters. The restriction in this mechanism is that

the calculation convergence rate in large-scale systems is not provided[23]. The factors used in their trust model must be returned with a weighty overhead.

Researchers' in[24] provided EigenTrust approach, which support peers trust information. This information gathered through performing distributed calculation approaching the eigenvector of the trust matrix over the peers. EigenTrust counts non-on a good selection of some pre-trusted peers, which are assumed to be trusted by all peers in the network. This assumption is a dangerous weakness a distributed computing environment has. The reason is that pre-trusted peers that have been selected may not last forever. When they become unworthy after some transactions, this mechanism may not work reliably

To enhance this area of research a bio-inspired algorithm, called BTRM-WSN is presented. The objective of this algorithm is to provide trust in WSN. It is precisely an ant colony system application for assisting a node finding the most reliable node offering a particular service, and to reach such sensor through the most reputable transmission route[25]. In this research, the main focus of evaluation was to evaluate the selection percentage of trustworthy servers achieved with BTRM-WSN. BTRM-WSN stays flexible to a high percentage of malicious servers when this percentage is less than or equal to 80%. Its efficiency gets worse when malicious servers reach 90% or more in the WSN, and the when the size of the WSN grows the problem increase[26].

Linguistic fuzzy logic and fuzzy sets model applied to a previous bio-inspired trust and reputation model for WSNs[27]. This enhanced the interpretability of the trust model, making it more human readable, while keeping and even improving, the accuracy of the trust and reputation model. IMRT experiments and simulation results described with details in Section 6.

3. General Trust and Reputation Model

Trust and Reputation models have their own characteristics, parameters and properties. However, most of them have the same criteria about what procedure have to be followed in order to supplement a whole process in a distributed system making use of a trust and reputation model. Steps for this procedure are drawn in Figure 1.

Figure 1. Generic trust and reputation model steps.

In the first stage, behavioral information about the objects of the monitored environment is gathered. Then, that information is used to supply a score that will determine the reputation and trust eligibility of every node in the network. After that, the most reliable and reputable entity is generally elected and a process is performed with it, evaluating next, the satisfaction of the requester with the offered service. According to that satisfaction, a final step of discard or accept is applied, updating the previous given rate to the selected party[15,17].

4. Optimized Trust and Reputation Framework

Evaluation of trustworthiness of peers using based reputations is the best way to decrease threats in WSN. An improved reputation-based trust supporting framework, which contains adaptative trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system. This framework shown in Figure 2.

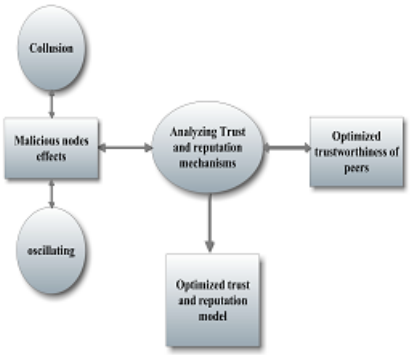

Figure 2. Optimized trust and reputation model.

During simulation of this model two security threats to evaluate accuracy and reliability. The first security threat has to do with the oscillating behavior of the pernicious nodes offering the required service. If this selection is choosed during simulation, after every 20 executions (transactions or interactions), each malicious server be good. Then the same percentage of previous malicious servers are randomly selected to be malicious (note that with a plan like this a malicious server could remain malicious after 20 executions). The another security threat inserted contains of the possibility for the malicious servers to sort a collusion through themselves. This means that every malicious sensor will give the maximum rating for every other malicious sensor, and the minimum rating for every good one.

5. Mathematical Model

Trust and Reputation has become a popular topic for constructing online rating systems[28–30]. This section shows a mathematical model for the trust and reputation process.

By considering trust as a base to take into account on the relationship between two sensors, it is possible to interact with the inherent uncertainty of the cooperation process. Trust systems are classified into trust based on the identity of a node or based on the actions of a node[31].

5.1 Reputation and Trust Mathematical Models

In this model, node reputation represented by beta distribution equation. This equation is simple and efficient. Reputation of node b from the perspective of node a represented as following:

$$R_b = Beta(\alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} Z^{\alpha-1} (1-Z)^{\beta-1}$$

$$0 \le Z \le 1, \alpha \ge 0, \beta \ge 0$$

Where **α** and **β** represents magnitude of cooperation and non-cooperation between neighbors and Γ is gamma function[32]. Collaboration may be thought of either in terms of a node's ability to transmit data or perhaps in terms data quality. The node a will assign the value 1 if node b was cooperative and 0 otherwise.

To know the expectation of next action of node being cooperative, we present trust in mathematical model, we estimate θ as the future behavior of node b, Observations α_y as cooperative and β_b as non-cooperative behavior. Trust formula can be written as following:

$$T_b = E[\theta] = E[Beta(\alpha_b + 1, \beta_b + 1)] = \frac{\alpha_b + 1}{\alpha_b + \beta_b + 2} \quad (2)$$

Where, E is statistical expectation[33].

5.2 Energy Mathematical Model

Sensor energy considered as trustworthy factor in IMRT. For each sensor in the network, the energy consumption measured by the following formula:

$$E_{con} = E_{ele} * K + E_{amp} * K * L^2 \quad (3)$$

where E_{ele} is receiver electronics energy and assumed equal 50, E_{amp} is transmission energy of Radio Frequency (RF) signal generation and it is considered equal to 100, K is the number of bytes (packet size capacity of each node), L is the radio range of each node, which is 12 in our experiments. Initial energy for each node is initialized randomly. At any time, the remaining energy in each node can be calculated through the difference between initial energy and consumed energy[34].

6. Simulation and Results

In this section simulation results for proposed reputation model presented and demonstrated.

6.1 Implementation and Simulation Tool

This paper used TRMSim-WSN for implement and simulate IMRT model. All the experiments carried out consisted of 100 WSNs whose nodes were randomly distributed over an area of 100 square units. Of the nodes, requesting 100 times a certain service and applying a specific trust and/or reputation. Number of sensors used in the simulation is 50 and simulated for 100 executions. Another assumption in this simulation, every node only knows its neighbors within its RF range. Simulation parameters and default values used in the experiments are summarized in Table 1.

Table 1. Simulation and network parameters

Parameter	Value
Number of executions	100
Number of networks	100
Minimum number of sensors	50
Maximum number of sensors	50
Clients (%)	Variable
Malicious nodes (%)	Variable
Plane (units)	100
delay between simulated networks	0
Radio range	12
Security threats used	Collusion and oscillating

Since one of the essential constrains that effects on WSNs is battery limits and high-energy consumption during transmission and reception, a dynamic WSN is simulated in our experiments. In these networks, power consumption reduced by a method that let some sensors goes into an idle state for a while if they do not receive any request from its neighbors within a specific period of time. A sensor during idle state does not receive nor transmit any data. After a certain timeout they wake up again.

In the first experiment, static, neither the topology of the networks, nor the goodness of the sensors changed during simulation, both of them remains unalterable. In this state, we evaluated the proposed model with three different percentage values used for malicious sensors (25%, 50%, and 75% respectively), following the configuration described in Table 1.

The second experiment covers static WSNs with collusion effect. In this experiment the pernicious nodes connived in order to unfairly compliment themselves and, in addition, minimize the reputation of good sensors. This is also a quite generic script which can be found in these kind of systems, where the more reputable or reliable you are, the more probabilities you have to be elected as a service provider.

Finally, static WSNs were tested over oscillating. In this type on WSNs servers change their behavior during all WSN lifetime. Alternatively, a redistribution of malicious sensors occurs, that is, one sensor can remain with its current liberality or, on the inversion and it can change its liberality and become the opposite. In all cases, malicious nodes percentage remains fixed after this behavioral oscillation. It is important to test the elasticity of trust and reputation model against this type of threats, since it is not realistic to assume there will be no change for sensor's behavior during its whole lifetime.

6.2. Experiment 1: Malicious Percentage Effects with Different Percentage Values of Client Sensors (Static Network)

In this experiment, three different values are used for malicious sensors with percentage 25%, 50%, and 75% respectively. The simulation results are the average outcomes for a whole simulation as shown in Table 2, 3 and 4. Three important values can be noticed here: The mechanism accuracy, the average length (number of hops) of all the paths in every simulated network found by every client, and the mechanism energy consumption.

Table 2. IMRT accuracy evaluation with different client sensors and malicious sensors percentages (Static WSNs)

Percentage of client sensors	Malicious sensors (25%)	Malicious sensors (50%)	Malicious sensors (75%)
15%	99.78	97.37	99.83
30%	99.33	97.07	96.29
45%	99.28	99.64	99.24
60%	99.86	99.67	98.21
75%	99.84	99.75	98.97

Table 3. IMRT average path length with different client sensors and malicious sensors percentages (Static WSNs)

Percentage of client sensors	Malicious sensors (25%)	Malicious sensors (50%)	Malicious sensors (75%)
15%	2.48	2.34	2.72
30%	2.38	3.1	5.06
45%	3.04	2.67	3.29
60%	3.51	3.75	5.87
75%	7.85	4.53	7.4

Table 4. IMRT energy consumption evaluation with different client sensors and malicious sensors percentages (Static WSNs)

	Energy consumption		
Percentage of client sensors	Malicious sensors (25%)	Malicious sensors (50%)	Malicious sensors (75%)
15%	3.7*10^14.0	2.1*10^14.0	3.7*10^14.0
30%	2.5*10^15.0	1.5*10^15.0	6.7*10^15.0
45%	1.5*10^16.0	3.3*10^16.0	5.0*10^16.0
60%	4.9*10^16.0	1.2*10^16.0	6.8*10^16.0
75%	5.1*10^17.0	6.5*10^17.0	1.6*10^17.0

It's clear from Figure 4 that the average accuracy for IMRT is quite high (more than 95%) with different percentages of malicious nodes. Accuracy reaches its maximum when the client sensors percentage is 60% and malicious sensors percentage is 25%.

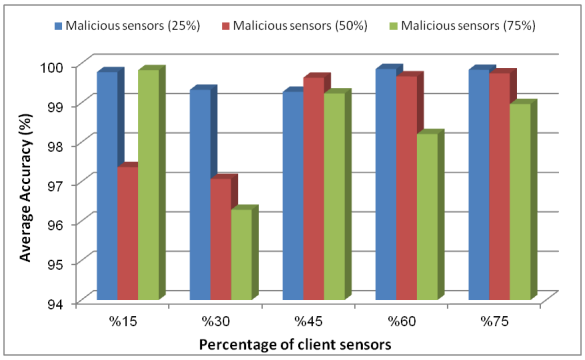

Figure 4. BIMRT accuracy and scalability evaluation with different client sensors percentages (Static WSNs).

Malicious percentage variants effect on the average path length presented in Figure 5. The figure shows that the average path length increases in both percentages of client sensors and malicious, but it does not exceed 8 hops in the worst case.

From Figure 6, we can note that energy consumption is generally low for different client sensors percentages. In worst case it will not exceed 700*10^15.0 mj. This indicates that network can still alive for more time.

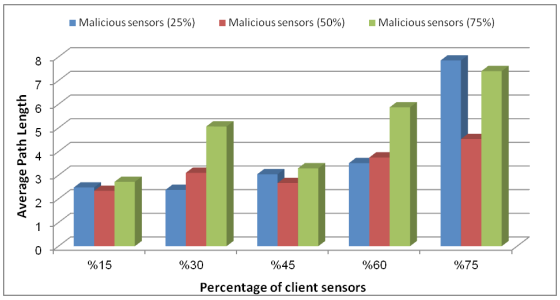

Figure 5. IMRT average path length with different client sensors percentages (Static WSNs).

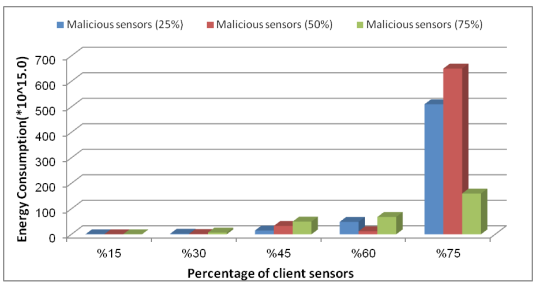

Figure 6. IMRT energy consumption with different client sensors percentages (Static WSNs).

6.3. Experiment 2: WSNs with Collusion Threat (Static Network)

Functional trust and reputation models should fast respond versus behavioral changes such as collusions and oscillations, and adapts to prevent electing a malicious node as the most reliable one.

In this experiment, we carried out a simulation for collusion threat effect on static networks. The percentage of malicious sensors is fixed for all tests as 50%. We measured trustworthy servers' selection percentage, the average path length of the routes found leading to trustworthy servers and power consumption.

Results for this experiment are presented in Table 5, 6 and 7. The graphical representations for these results are shown in Figure 7, Figure 8 and Figure 9.

From Figure 7, we can note average accuracy is high for different client sensors percentages. This presents the security strength of IMRT.

As shown in Figure 8, average path length is not exceeding 3 hops for 60% client sensors or less. It's not reaching 6 hops for high client sensors percentages.

From IMRT Energy Consumption simulation results shown in Figure 9, we can conclude that the energy consumption generally low especially for networks with client sensors percentages 60% or less.

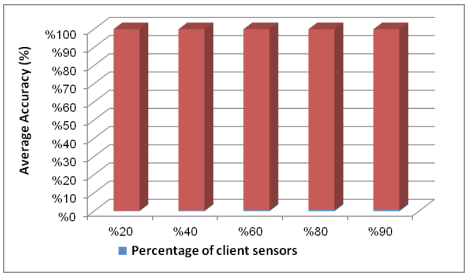

Figure 7. IMRT accuracy and scalability evaluation with different client sensors percentages with collusion (Static WSNs).

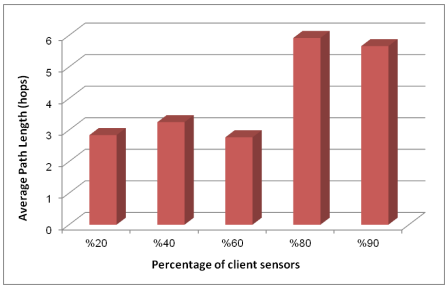

Figure 8. IMRT average path length with different client sensors percentages with collusion (Static WSNs.

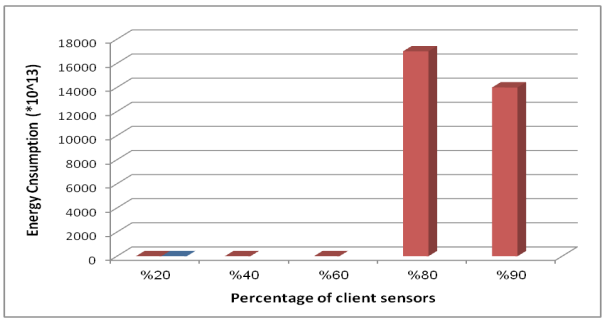

Figure 9. IMRT energy consumption evaluation with different client sensors percentages with collusion (Static WSNs.

Table 6. IMRT average path length with different client sensors percentages with collusion (Static WSNs)

Percentage of client sensors	Average Path length (hops)
20%	2.84
40%	3.25
60%	2.77
80%	5.92
90%	5.66

Table 7. IMRT accuracy and scalability evaluation with different client sensors percentages with oscillating (Static WSNs)

Percentage of client sensors	Average Accuracy (%)
20%	85.29
40%	84.9
60%	84.5
80%	79.78
90%	78.2

6.4. Experiment 3: WSNs with Oscillating Threat (Static Network)

Final experiment used to test WSNs over oscillating WSNs. In this test WSNs behavior changes in the servers along time. From time to time, a redistribution of malicious sensors occurs, that is, one sensor can remain with its current benevolence or it can swap its benevolence and become the opposite, malicious. In any case, the percentage of malicious nodes remains constant after this behavioral oscillation. It is important to test the resilience of trust and reputation model against these types of threats, since it is not realistic to suppose that a sensor's behavior will never change in its whole lifetime. Simulation results in this test are listed in Table 8, 9 and 10 whereas graphical representation shown in Figures 9,10 and 11.

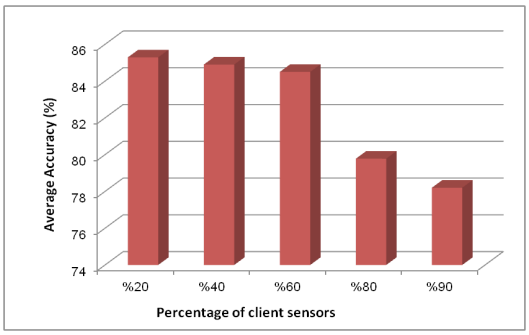

Figure 10. IMRT accuracy and scalability evaluation with different client sensors percentages with oscillating (Static WSNs.

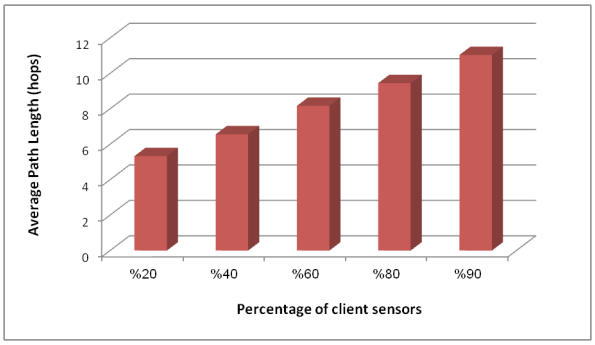

Figure 11. IMRT average path length with different client sensors percentages with oscillating (Static WSNs).

Table 8. IMRT energy consumption evaluation with different client sensors percentages with collusion (Static WSNs)

Percentage of client sensors	Energy consumption
20%	1.3*10^13.0
40%	8.9*10^13.0
60%	5.2*10^13.0
80%	1.7*10^17.0
90%	1.4*10^17.0

Table 9. IMRT average path length with different client sensors percentages with oscillating (Static WSNs)

Percentage of client sensors	Average Path length (hops)
20%	5.33
40%	6.56
60%	8.17
80%	9.45
90%	11.04

Table 10. IMRT energy consumption evaluation with different client sensors percentages with oscillating (Static WSNs)

Percentage of client sensors	Energy consumption
20%	5.2*10^15.0
40%	1.9*10^16.0
60%	3.2*10^16.0
80%	1.3*10^16.0
90%	1.0*10^16.0

Results presented in Figure 9 show that the average accuracy of the model gets worse as the client sensors percentage reach 90%.

From Figure 12, we can contribute that for dynamic networks under oscillating effect, energy consumption is very low due to the switch off nodes criteria when the node becomes idle. Energy consumption reaches the maximum value when the percentage of client sensors is 30%.

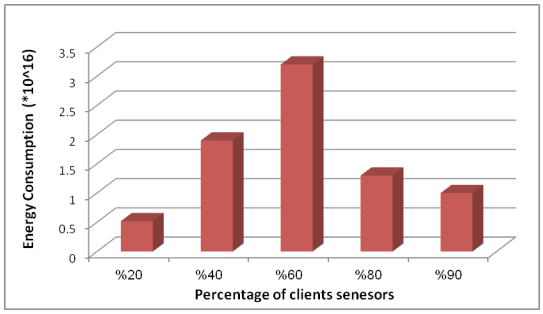

Figure 12. IMRT energy consumption evaluation with different client sensors percentages with oscillating (Static WSNs).

In static networks, the results show that energy consumption is generally low and it increases when the client sensors increase. It reaches the highest value when the percentage of clients is around 60% and after that, it falls down.

7. Results and Discussion

Analysis and simulation results show specifications of proposed model; we can summarize the contribution of this paper as follows:

- Simulation results have shown that IMRT model remains stable to high or low number of malicious servers when the percentage of client sensors greater than or equal 60%. The network accuracy can be improved by adding more client sensors.
- Simulation shows the average path length is low and does not override 5.2.
- IMRT approach remains string to collusion effects. Accuracy and scalability remains high for static WSNs and increase with increasing number of client sensors.
- Dynamic WSNs have minimum average path length when the number of client nodes increase, However, the collusion impacts are high on an average path length for static WSNs.
- Generally, IMRT slightly outperforms PowerTrust by about 2% in accuracy for dynamic networks, and 1%-11% greater than the optimal performance of the other models under oscillating effect. Average path length is lower than other mechanisms in all cases.
- Proposed model shows generally low power consumption for both static and dynamic WSNs.

8. Conclusions and Future Work

Malicious sensors have high impacts on WSNs. Enhancing WSNs security can be effective by evaluation the trust and reputation of nodes. However, enhancing trust and reputation in WSNs in an effective, precise and strong way has not been entirely resolved yet. In this work, Modified Trust and Reputation Model enhanced to increase WSNs security. This modified model is tested through simulation that deploy security threats such as collusion and oscillating of malicious nodes in WSNs. Simulation results show that enhanced model has security strong points towards malicious nodes with oscillating and collusion effects. Results prove that its remains strong to highest number of malicious servers when the number of client sensors is high. Therefore, in small or large WSNs, our model would function properly regardless

malicious servers have high percentage. Thus, we can say that overall performance of IMRT is high and energy consumption is low.

As future work, we need to apply experiments for the model using different network sizes and variable number of executions. Also, the balancing between the security and trust and reputation as per our scheme needs further investigation.

9. References

1. Yanli Y, Keqiu L, Zhou W, Li P. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. Journal of Network and Computer Applications. 2012; 35:867–80.
2. Alkalbani A, Mantoro T, Tap AOM. Improving the lifetime of wireless sensor networks based on routing power factors. 4th International Conference on Networked Digital Technologies (NDT2012); Dubai, (UAE). 2012. p. 565–76.
3. Mantoro T. Metrics evaluation for context-aware computing. Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia, ACM; 2009. p. 574–8.
4. Chen H, Wu H., Zhou X, Gao C. Reputation-based trust in wireless sensor networks. International Conference on Multimedia and Ubiquitous Engineering (MUE'07); Seoul, Korea. 2007. p. 603–7.
5. Josang A, Ismail R, and Boyd C. A survey of trust and reputation systems for online service provision. Decision Support Systems. 2007; 43(2):618–44.
6. Sabater J, Sierra C. Review on computational trust and reputation models. Artificial Intelligence Review. 2005; 24(1):33–60.
7. Wang J, Liu Y, Jiao Y. Building a trusted route in a mobile ad hoc network considering communication reliability and path length. Journal of Network and Computer Applications. 2011; 34(4):1138–49.
8. Alkalbani A, Tap AOM, Mantoro T. Modified Reputation-Base Trust (MRT) for WSN Security. Journal of Theoretical and Applied Information Technology. 2012; 56(2):417–27.
9. Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures. Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications; 2003. p. 293–325b.
10. Srinivasan A, Teitelbaum J, Liang H, Wu J, Cardei M. Reputation and trust-based systems for ad hoc and sensor networks. Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks; 2007.
11. Srinivasan A, Teitelbaum J, Wu J. DRBTS: Distributed Reputation Based Beacon Trust System. 2nd IEEE International Symposium on Independable, Autonomic and Secure Computing; 2006. p. 277–83.
12. Ganeriwal S, Baizano LK, Srivastava MB, Reputation based framework for high integrity sensor networks. ACM Transactions on Sensor Networks (TOSN). May 2008; 4(3):1–37.
13. Marsh SP. Formalizing trust as a computational concept [PhD thesis]. Stirling: Department of Computing Science and Mathematics, University of Stirling; 1994.
14. Mui L. Computational models of trust and reputation: Agents, evolutionary games, and social networks [PhD thesis]. Cambridge, USA: Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology; 2002.
15. Sun Y, Yang Y, Trust establishment in distributed networks: Analysis and modeling. Proceedings of the IEEE International Conference on Communications (IEEE ICC), Communication and Information Systems Security Symposium; Glasgow, Scotland. 2007 p. 1266–73.
16. Lam SK, Riedl J. Shilling recommender systems for fun and profit. Proceedings of the 13th International Conference on World Wide Web (WWW '04); 2004. p. 393–402.
17. Marti S, Garcia-Molina H. Taxonomy of trust: Categorizing P2P reputation systems. Computer Networks. 2006; 50(4):472–84.
18. Moloney S. Simulation of a distributed recommendation system for pervasive networks. SAC05: Symposium on Applied Computing; 2005. p. 1577–81.
19. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. International Conference on Mobile Computing And Networking (MOBICOM'00); 2000. p. 255–65.
20. Hur J, Lee Y, Yoon H, Choi D, Jin S. Trust evaluation model for wireless sensor networks. The 7th International Conference on Advanced Communication Technology (ICACT '05); Gangwon-Do, Korea. 2005. p. 491–6.
21. Gerrigagoitia K, Uribeetxeberria R, Zurutuza U, Arenaza I. Reputation-based intrusion detection system for wireless sensor networks. Complexity in Engineering (COMPENG); 2012. p. 1–5.
22. Xiong L, Liu L. PeerTrust: Supporting reputation-based trust in peer-to-peer communities. IEEE Transactions on Knowledge and Data Engineering. 2004; 16(7):843–85.
23. Zhou R, Hwang K. PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing. IEEE Transactions on Parallel and Distributed Systems. 2007; 18(4):460–73.
24. Kamvar S, Schlosser M, Garcia-Molina H. The eigentrust algorithm for reputation management in P2P networks. Proceedings of the 12th international conference on World Wide Web (WWW03); 2003. p. 640–51.
25. Dorigo M, Gambardella LM, Birattari M, Martinoli A, Poli R, Stutzle T. Ant colony optimization and swarm intelligence. 5th International Workshop, ANTS; Springer, Berlin, Germany. 2006. p. 224–34.
26. Marmol F, Perez G. Providing trust in wireless sensor networks using a bio-inspired technique. Telecommunication Systems Journal. 2011; 46(2):163–80.

27. Marmol F, Marin-Blazquez J, Perez G. LFTM: Linguistic Fuzzy Trust Mechanism for distributed networks. Concurrency and Computation: Practice and Experience. 2012; 24(17):2007–27.
28. Zacharia G, Maes P. Collaborative reputation mechanisms in electronic marketplaces. Proceedings of the 32nd Hawaii International Conference on System Sciences; USA. 1999. p. 8.
29. Yu B, Singh MP. Towards a probabilistic model of distributed reputation management. 4th Workshop on Deception, Fraud and Trust in Agent Societies; Montreal, Canada. 2001.
30. Mui L, Mohtashemi M, Halberstadt A. A computational model of trust and reputation. 35th Hawaii International Conference on System Science (HICSS); 2002.
31. Lopez J, Roman R, Agudo I, Fernandez-Gago C. Trust management systems for wireless sensor networks: best practices. Computer Communications. 2010; 33(9):1086–93.
32. Gelman A, Carlin JB, Stern HS, Rubin DB. Bayesian data analysis. 2nd ed. Chapman and Hall; 2003.
33. Ganeriwal S, Srivastava M. Reputation-based framework for high integrity sensor networks. Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04); Washington, DC, USA. 2004. p. 66–77.
34. Nagarathna K, Kiran YB, Mallapur JD, Hiremath S. Trust based secured routing in wireless multimedia sensor networks. 4th International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN'12); 2012. p. 53–8