Journal of Theoretical and Applied Information Technology
20th October 2013. Vol. 56 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MODIFIED REPUTATION-BASE TRUST (MRT) FOR WSN SECURITY

[1]ABDULLAH SAID ALKALBANI, [2]ABU OSMAN MD. TAP, [3] TEDDY MANTORO

[1]Ph.D. Candidate, Department of Computer Science, KICT, International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia

[2]Professor, Department of Computer Science, KICT, International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia

[3]Professor, Dean of Faculty of Science and Technology, Universitas Siswa Bangsa International (USBI), Jakarta, Indonesia

E-mail: [1]abdullah.said@student.iium.edu.my , [2]abuosman@kict.iium.edu.my, [3] teddy@ieee.org

ABSTRACT

During the last years, Wireless Sensor Networks (WSNs) and its applications have obtained considerable momentum. However, security and power limits of WSNs are still important matters. Many existing approaches at most concentrate on cryptography to improve data authentication and integrity but this addresses only a part of the security problem without consideration for high energy consumption. Monitoring behavior of node neighbors using reputation and trust models improves the security of WSNs and maximizes the lifetime for it. However, a few of previous studies take into consideration security threats and energy consumption at the same time. Under these issues we propose a reputation and trust mechanism optimized for security strength. We apply two security threats (oscillating and collusion) during simulations of the proposed model in order to measure the accuracy, scalability, trustworthiness and energy consumption. As results, effects of collusion and oscillating are minimized and energy consumptions for dynamic networks reduced. Also simulation results show that the proposed model remains resilient to low or high percentages of pernicious servers when the percentage of client sensors are greater than or equal 60%. This result is quite promising; it shows that energy consumption generally is low, especially for dynamic networks.

Keywords: *Wireless Sensor Networks (WSNs), Collusion, Oscillating, Power Consumption, Trust and Reputation Models*

1. INTRODUCTION

Due to fast advances in wireless communications over the last few years, the enhancement of networks of low-cost, low-power, multifunctional sensors has received increasing attention [1]. These sensors have small size and ability to sense, process data, and communicate with each other, usually over Radio Frequency (RF) channels. WSNs are developed to detect events or phenomena, gather and process data, and transmit this data to interested users.

Sensor Networks and related technologies have acquired considerable attention within the last 10 years. This is due to the truth that the technology is maturing and moving out of the purely research driven environment into commercial interests [2]. WSNs serve to gather data and to monitor 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 and 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 [3].

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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

network [4], [5]. Currently, most of the trust evaluation structure belongs to a recommendation-based methodology such that the evaluation results are usually dependent on the accurate measurement of the forwarding behaviors of adjoining nodes and on the recommenders' honesty degree [6].

This article shows the last enhancement for WSNs by trust and reputation mechanisms found in literature. 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 also propositions on our future direction.

2. RELATED WORK

Security is critical issue in a modern network system, although, often, one that the majority of the WSNs literature neglects to support minimizing energy consumption as the sole defining objective. The survey by [7] addresses a number of attacks that prove destructive to many essential WSN routing protocols. The security threats of WSN mainly contain external attacks 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 an immediate effect on internal attacks [7].It has become an important measure to defend against internal attacks and it has received high concern. In recent years, an increasing number of researches have been conducted on the applying of reputation systems to sensor networks [8]. Meanwhile only [9] and [10] have concentrated on the use of reputation systems in WSN.

Trust and reputation are mechanisms which deal with a lot of applications every day. Trust and reputation management in distributed environments has been lately submitted as a mechanism for minimizing certain risks not completely covered by conventional network security mechanisms, obtaining fairly good results [11]. Some researchers do related research on the application of reputation rating technique in security routing protocol [12], and proposed some simulating methods for reputation evaluation models in WSNs.

In this area, some researchers focused on analysis of trust and reputation models. Evaluation of systems that use trust and reputation mechanisms have been accomplished in [13], [14], [15], whereas some others related to simulation tools used for those systems described in [16].

Moreover, some researchers have concentrated 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 [17] 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 [18] 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 [19]. 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 [20] described one approach called PeerTrust model. This model has two major specifications. Firstly, it introduce 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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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 [21]. The factors used in their trust model must be returned with a weighty overhead.

The EigenTrust approach accumulates trust information from peers. This information gathered through performing distributed calculation approaching the eigenvector of the trust matrix over the peers [22]. 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 [23]. 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 [24].

Linguistic fuzzy logic and fuzzy sets model applied to a previous bio-inspired trust and reputation model for WSNs [25]. 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.

Table 1 compares our MRT model with existing trust and reputation models in terms of average accuracy and average path length. MRT 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 [13], [15]. 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 [13], [15].

4. OPTIMIZED TRUST AND REPUTATION FRAMEWORK

One way to reduce threats in WSNs is evaluate the trustworthiness of peers using community based reputations. An optimal reputation-based trust supporting framework, which includes adaptative trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system. This framework shown in Figure 2.

Two security threats applied during simulation of proposed trust and reputation model in order to measure model accuracy and reliability. The first

Journal of Theoretical and Applied Information Technology
20th October 2013. Vol. 56 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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.

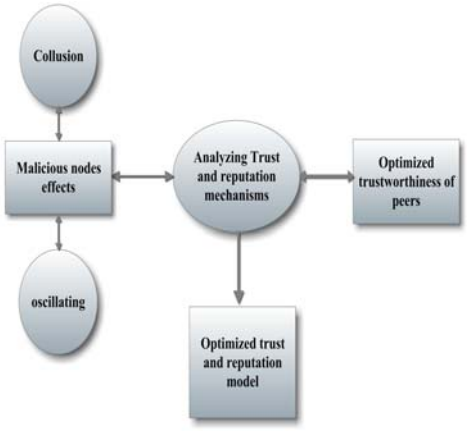

Figure 2: Optimized Trust and Reputation Model

5. TRUST AND REPUTATION MATHEMATICAL MODEL

Trust and Reputation has become a popular topic for constructing online rating systems [26], [27], [28]. This section shows a proposed mathematical model for the trust and reputation process. This model tries to minimize power consumption during the process and improving trustworthiness at the same time.

By considering trust as a factor 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 [29].

5.1 Reputation Model

In this model, beta distribution formula is used to represent node reputation. This formula is simple and more efficient. Reputation of node **y** from the perspective of node **x** represented as following:

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

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

Where **α** and **β** represents magnitude of cooperation and non-cooperation between neighbors and Γ is gamma function [30]. Collaboration may be thought of either in terms of a node's ability to transmit data or perhaps in terms data quality. The node x will assign the value 1 if node y was cooperative and 0 otherwise.

5.2 Trust Model

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 y, Observations α_y as cooperative and β_y as non-cooperative behavior. Trust formula can be written as following:

$$T_{xy} = E[\theta] = E[Beta(\alpha_y + 1, \beta_y + 1)] = \frac{\alpha_y + 1}{\alpha_y + \beta_y + 2} \quad (2)$$

where E is statistical expectation [31].

5.3 Energy Model

This model is used to measure the energy of each sensor node. When node energy is calculated depending on this formula, MRT model consider this as trustworthy factor for sensor nodes. The energy consumed by each node is calculated by:

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

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 [32].

6. SIMULATION AND RESULTS

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

6.1 Simulation Tool

In this research, TRMSim-WSN is used for simulation. 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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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 2.

Table 2: 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

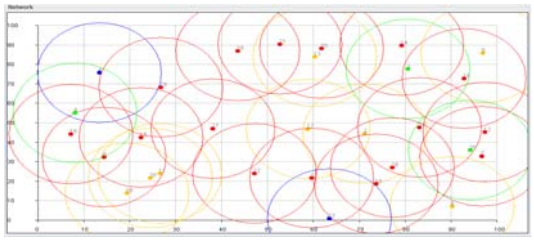

Figure 3: Simulation WSN Distribution for Trust and Reputation Model

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 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, so they both remained 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 2.

The second experiment is over WSNs with collusion, consisting of either static or dynamic networks. 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.

In the last simulation, static and dynamic 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

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 3, 4 and 5. 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.

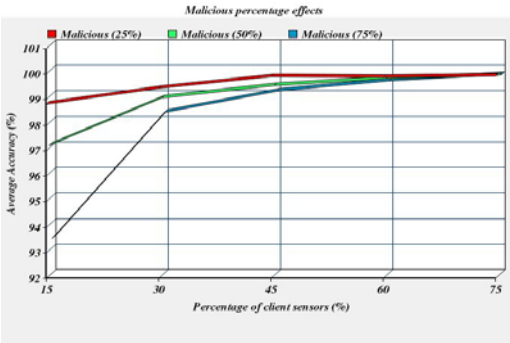

Figure 4: MRT Accuracy and Scalability Evaluation with Different Client Sensors Percentages

It's clear from Figure 4 that the average accuracy for MRT is quite high (more than 90%) with different percentages of malicious nodes. Accuracy reaches its maximum when the client sensors percentage is greater than 60% in every case of malicious percentage.

Malicious percentage variants effect on the average path length presented in Figure 5. The

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

figure shows that the average path length increases in both percentages of client sensors and malicious, but it does not exceed 5.2 in the worst case.

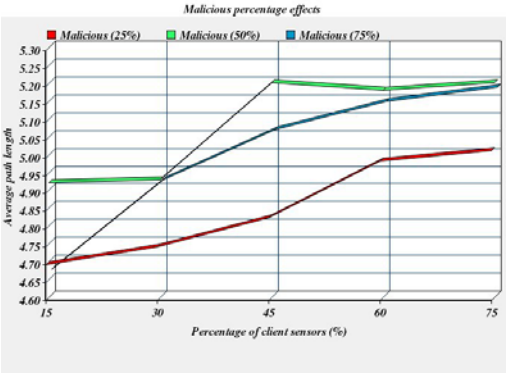

Figure 5: MRT Average Path Length with Different Client Sensors Percentages

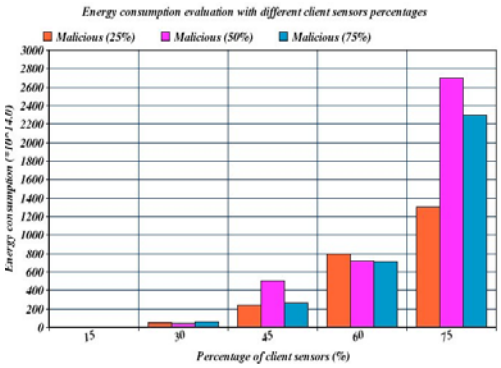

Figure 6: MRT Energy Consumption with Different Client Sensors Percentages

From Figure 6, we can note that energy consumption is generally low. In worst case it will not exceed 2800*10^14.0.

6.3 Experiment 2: WSNs with Collusion Threat

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, first, we carried out a simulation for static networks. We measured trustworthy servers' selection percentage, the average path length of the routes found leading to trustworthy servers and power consumption. Results for this step are presented in Table 6.

For the next step in this experiment, we applied simulations for dynamic WSNs. We carried it out with the same simulation settings that we used for static networks.

In dynamic networks, some nodes switch off for a while. The decision schema of when to go to idle mode and wake-up is as follows: when a server receives and supplies an amount (for example 20) of requests, it directly switches off during a specific timeout. Furthermore, if a server does not receive at least the same amount of requests (for example 20) within interval certain time, it also becomes idle during another timeout. Table 7 shows the results in this step.

The outcomes of the two steps in this experiment are presented in Figure 7, Figure 8 and Figure 9.

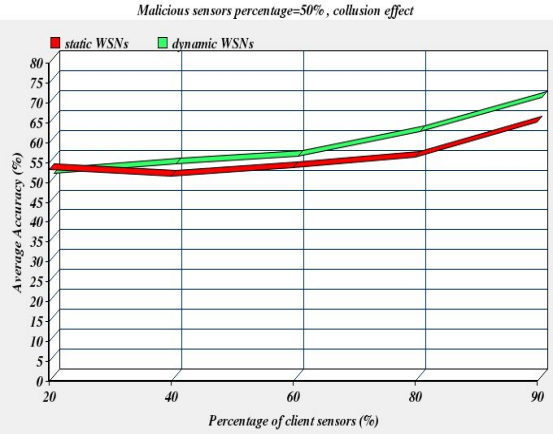

Figure 7: MRT Accuracy and Scalability Evaluation with Collusion

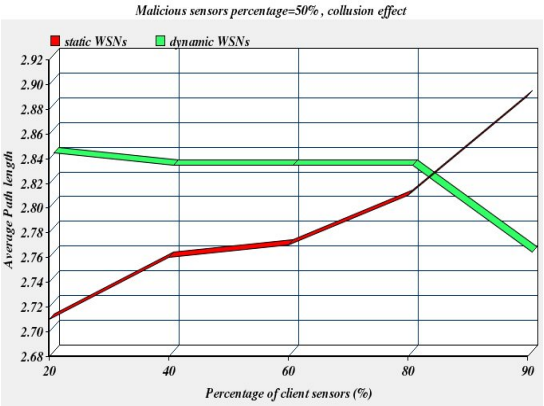

Figure 8: MRT Average Path Length with Collusion

Journal of Theoretical and Applied Information Technology
20th October 2013. Vol. 56 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

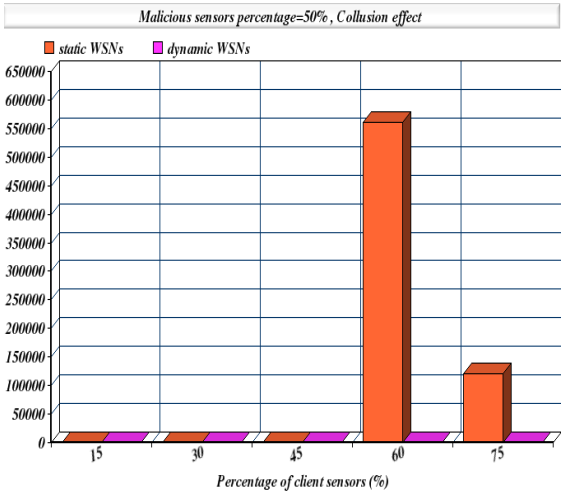

Figure 9: MRT Energy Consumption with Collusion (Dynamic WSNs)

From the simulation results, we can conclude that the average accuracy and scalability increases with increasing client nodes percentage. The average path length decreases in parallel with the client's percentage for dynamic networks due to minimization of energy consumption whereas it increases for static networks. We can notice that the energy consumption for dynamic networks is very low because of its nature.

6.4 Experiment 3: WSNs with Oscillating Threat

Simulation results in this test, consisting of a wireless network whose server nodes change their quality over time, are presented in Table 8 and 9. Results presented in Figure 10 show that the average accuracy of the model gets worse as the malicious nodes percentage approaches 50 % and the client sensors percentage do not reach 80%.

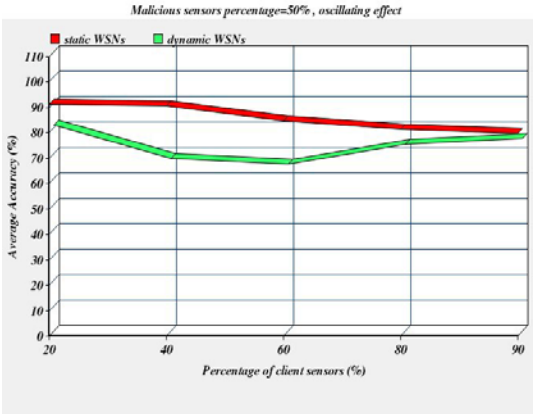

Figure 10: MRT Accuracy and Scalability Evaluation with Oscillating

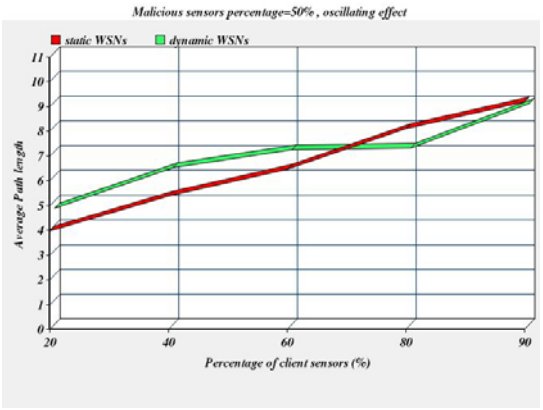

Figure 11: MRT Average Path Length with Oscillating

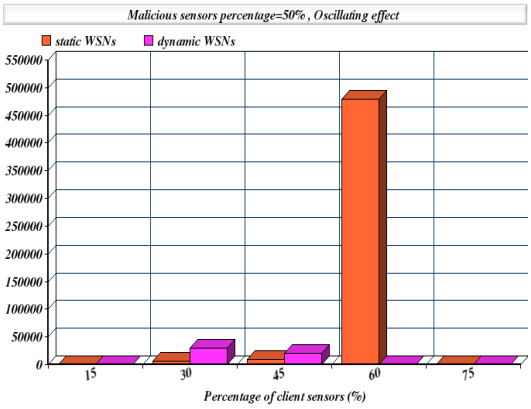

Figure 12: MRT Energy Consumption with Oscillating

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%.

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 DISCUSSION

From the results of the simulation, we can summarize the contribution of this research in the following points:

- Experiment results have shown that proposed model remains flexible to low or high percentages of malicious servers when the percentage of client sensors greater than or equal 60%. We can improve the accuracy of the network through increasing the number of client sensors.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Simulation results show the average path length leading to trustworthy servers. It's clear that the average path length is low and does not override 5.2.
- Proposed model is resilient to collusion effects. Accuracy and scalability remains high for static WSNs and increase with increasing number of client sensors.
- Collusion effects are high on an average path length for static WSNs whereas dynamic networks have a minimum average path length when client sensors increase.
- In general, MRT 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.
- In both static and dynamic networks, the results show that energy consumption is generally low.

8. CONCLUSIONS AND FUTURE WORK

The tasks of WSNs are functionally influenced by the greedy and malicious network sensors. Evaluation the trust and reputation of nodes have proven to be an effective solution to enhance WSNs security. However, optimizing trust and reputation in WSNs in an effective, precise and strong way has not been entirely resolved yet. In this work, an optimized model is proposed to improve WSNs security. This model is evaluated through applying security threats such as collusion and oscillating of malicious nodes in WSNs. Simulation results show that proposed model 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%. So, in small or large WSNs, our model would function properly regardless malicious servers have high percentage. Thus, we can say that general performance of MRT 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.

REFRENCES:

[1] T. V. U. Kiran Kumar and B. Karthik, "Improving Network Life Time Using Static Cluster Routing for Wireless Sensor Networks ", *Indian Journal of Science and Technology*, Vol. 6, 2013, pp.4642-4647.

[2] A. Alkalbani, T. Mantoro, and A.O. Md Tap, "Improving the Lifetime of Wireless Sensor Networks Based on Routing Power Factors", Fourth International Conference on Networked Digital Technologies (NDT2012) , IEEE UAE Conference , Dubai, (UAE), 2012, pp.565-576.

[3] H. Chen, H. Wu, X. Zhou, and C. Gao, "Reputation-based Trust in Wireless Sensor Networks", International Conference on Multimedia and Ubiquitous Engineering (MUE'07), Seoul, (Korea), 2007, pp. 603-607.

[4] A. Josang, , R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision", Decision Support Systems, Vol. 43 No. 2, 2007, pp. 618-44.

[5] J. Sabater, and C. Sierra, "Review on Computational Trust and Reputation Models", *Artificial Intelligence Review*, Vol. 24, No. 1, 2005, pp. 33-60.

[6] J. Wang, Y. Liu, and Y. Jiao, "Building A Trusted Route In A Mobile Ad Hoc Network Considering Communication Reliability and Path Length", *Journal of Network and Computer Applications*, Volume 34, Issue 4, 2011, pp. 1138–1149.

[7] C. Karlof, and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*, 2003, pp.113-27.

[8] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks", *Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks*, 2007.

[9] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed Reputation Based Beacon Trust System, Independable, Autonomic and Secure Computing", *2nd IEEE International Symposium on IEEE*, 2006. pp. 277–283.

[10] S. Ganeriwal, , L.K. Baizano, , M.B. Srivastava, "Reputation based Framework for High Integrity Sensor Networks", *ACM Transactions on Sensor Networks (TOSN)*, May 2008, Vol 4, Issue 3, pp. 15:1-15:37

[11] S.P. Marsh, "Formalizing Trust as a Computational Concept", *PhD thesis*, Department of Computing Science and Mathematics, University of Stirling, Stirling, 1994.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[12] L. Mui, "Computational Models of Trust and Reputation: Agents, Evolutionary Games, And Social Networks", *PhD thesis*, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, (USA), 2002.

[13] Y. Sun, and Y. Yang, "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, pp. 1266-1273.

[14] S.K. Lam, and J. Riedl, "Shilling Recommender Systems for Fun and Profit", *Proceedings of the 13th International Conference on World Wide Web*(*WWW '04*), 2004, pp.393-402.

[15] S. Marti, and H. Garcia-Molina, "Taxonomy of Trust: Categorizing P2P Reputation Systems", *Computer Networks*, Vol. 50, No. 4, 2006, pp. 472–484.

[16] S. Moloney, "Simulation of a Distributed Recommendation System for Pervasive Networks", *SAC05: Symposium on Applied Computing*, 2005, pp. 1577-81.

[17] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", *International conference on mobile computing and networking (MOBICOM'00)*, 2000, pp. 255–65.

[18] J. Hur, Y. Lee, H. Yoon, D. Choi, and S. Jin, "Trust Evaluation Model for Wireless Sensor Networks", The 7th International Conference on Advanced Communication Technology (ICACT '05). Gangwon-Do, (Korea), 2005, pp. 491-496.

[19] K. Gerrigagoitia, R. Uribeetxeberria, U. Zurutuza, and I. Arenaza, "Reputation-based Intrusion Detection System for Wireless Sensor Networks", *Complexity in Engineering (COMPENG)*, 2012, pp.1-5.

[20] 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, 2004, pp. 843-85.

[21] 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, 2007, pp. 460-473.

[22] S. Kamvar, , M. Schlosser, and H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks", *Proceedings of the 12th international conference on World Wide Web (WWW03)*, 2003, pp. 640-651.

[23] M. Dorigo, L.M. Gambardella, M. Birattari, A. Martinoli, R. Poli, and T. Stutzle, "Ant Colony Optimization and Swarm Intelligence", *5th International Workshop, ANTS*, Springer, Berlin, (Germany), 2006, pp. 224-234.

[24] F. Marmol, and G. Perez, "Providing Trust in Wireless Sensor Networks using a Bio-inspired Technique", *Telecommunication Systems Journal*, Vol. 46, No. 2, 2011, pp. 163-180.

[25] F. Marmol, , J. Marin-Blazquez, and G. Perez, "LFTM: Linguistic Fuzzy Trust Mechanism for distributed networks", *Concurrency and Computation: Practice & Experience*, Vol. 24, Issue 17, 2012, pp. 2007–2027.

[26] G. Zacharia, P. Maes, "Collaborative Reputation Mechanisms in Electronic Marketplaces", *In proceedings of the 32nd Hawaii International Conference on System Sciences*, Vol. 8, (USA), 1999.

[27] B. Yu, M. P. Singh, "Towards a Probabilistic Model of Distributed Reputation Management", *4th Workshop on Deception, Fraud and Trust in Agent Societies*, Montreal, (Canada), 2001.

[28] L. Mui, M. Mohtashemi, A. Halberstadt, "A Computational Model of Trust and Reputation", *35th Hawaii International Conference on System Science (HICSS)*. 2002.

[29] J. Lopez, R. Roman , I. Agudo , C. Fernandez-Gago, "Trust Management Systems for Wireless Sensor Networks: best practices", *Computer Communications*, Vol 33, Issue 9, 2010, pp. 1086–1093.

[30] A.Gelman, J. B.Carlin, H. S.Stern, and D. B. Rubin, "Bayesian Data Analysis", Chapman and Hall, Second Edition, 2003.

[31] S. Ganeriwal and M. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks". *In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04)*, Washington, DC, (USA), 2004, pp. 66-77.

[32] K. Nagarathna, Y. B. Kiran, J D. Mallapur, S. Hiremath, "Trust Based Secured Routing in Wireless Multimedia Sensor Networks", *Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN'12)*, 2012, pp. 53-58.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Comparison between Proposed and Existing Trust and Reputation Models (Malicious Nodes Percentage ≈ 60%).

	Average accuracy			Average path length		
Model	Dynamic network	collusion	oscillating	Dynamic network	collusion	oscillating
EigeTrust (Kamvar, *et al*., 2003)	44%	85%	85%	7.5	7.4	6.4
PeerTrust (Xiong and Liu, 2004)	59%	15%	80%	7	6.8	6.5
PowerTrust (Zhou and Hwang, 2007)	78%	87%	90%	6.5	7	7
BTRM-WSN (Marmol and Perez, 2011)	60%	39%	90%	5.8	2.9	4.5
MRT	80%	69 %	91%	4.67	2.71	3.96

Table 3: MRT Accuracy, Scalability and Average Path Length Evaluation With Different Client Sensors Percentages (Malicious Sensors Percentage=25%).

Percentage of client sensors	Average Accuracy (%)	Average Path length (hops)	Energy consumption
15%	98.80	4.7	3.3*10^14.0
30%	99.44	4.75	5.0*10^15.0
45%	99.88	4.83	2.4*10^16.0
60%	99.86	4.99	8.0*10^16.0
75%	99.91	5.02	1.3*10^17.0

Table 4: MRT Accuracy, Scalability and Average Path Length Evaluation with Different Client Sensors Percentages (Malicious Sensors Percentage=50%).

Percentage of client sensors	Average Accuracy (%)	Average Path length (hops)	Energy consumption
15%	97.09	4.92	4.4*10^14.0
30%	98.94	4.93	4.2*10^15.0
45%	99.44	5.2	5.1*10^16.0
60%	99.69	5.18	7.2*10^16.0
75%	99.83	5.2	2.7*10^17.0

Table 5: MRT Accuracy, Scalability and Average Path Length Evaluation with Different Client Sensors Percentages (Malicious Sensors Percentage=75%).

Percentage of client sensors	Average Accuracy (%)	Average Path length (hops)	Energy consumption
15%	93.33	4.67	3.3*10^14.0
30%	98.27	4.92	5.7*10^15.0
45%	99.1	5.06	2.7*10^16.0
60%	99.5	5.14	7.1*10^16.0
75%	99.76	5.18	2.3*10^17.0

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 6: MRT Accuracy, Scalability and Average Path Length Evaluation with Different Client Sensors Percentages (Malicious Sensors Percentage=50% , Collusion Effect (Static WSNs)).

Percentage of client sensors	Average Accuracy (%)	Average Path length (hops)	Energy consumption
20%	53.13	2.71	2.1*10^13.0
40%	51.46	2.76	7.6*10^13.0
60%	53.65	2.77	5.2*10^13.0
80%	56.15	2.81	5.6*10^17.0
90%	65.16%	2.89	1.2*10^17.0

Table 7: MRT Accuracy, Scalability and Average Path Length Evaluation with Different Client Sensors Percentages (Malicious Sensors Percentage=50% , Collusion Effect (Dynamic WSNS)).

Percentage of client sensors	Average Accuracy (%)	Average Path length (hops)	Energy consumption
20%	50.67	2.84	4.6*10^12.0
40%	53.15	2.83	1.4*10^13.0
60%	55.51	2.83	1.5*10^13.0
80%	61.16	2.83	8.5*10^11.0
90%	69.92	2.76	3.4*10^11.0

Table 8: MRT Accuracy, Scalability and Average Path Length Evaluation with Different Client Sensors Percentages (Malicious Sensors Percentage=50% , Oscillating Effect (Static WSNs)).

Percentage of client sensors	Average Accuracy (%)	Average Path length (hops)	Energy consumption
20%	91.21	3.96	3.4*10^14.0
40%	90.62	5.38	5.9*10^15.0
60%	84.43	6.44	9.4*10^15.0
80%	81.15	8.11	4.8*10^17.0
90%	79.53	9.19	4.4*10^14.0

Table 9: MRT Accuracy, Scalability And Average Path Length Evaluation With Different Client Sensors Percentages (Malicious Sensors Percentage=50% , Oscillating Effect (Dynamic WSNs)).

Percentage of client sensors	Average Accuracy (%)	Average Path length (hops)	Energy consumption
20%	80.83	4.67	7.6*10^13.0
40%	67.8	6.32	3.0*10^16.0
60%	65.51	7.04	2.1*10^16.0
80%	73.38	7.11	3.9*10^13.0
90%	75.71	8.9	5.2*10^12.0