Journal of Theoretical and Applied Information Technology
31st December 2014. Vol.70 No.3

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

EVALUATED REPUTATION-BASED TRUST 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 Modified Reputation-Based Trust model proposed and optimized for security strength. During evaluation of the model with well-known models two security threats (oscillating and collusion) were applied in order to measure the accuracy, scalability, trustworthiness and energy consumption. As a result, the effects of collusion and oscillating on proposed model are minimized and energy consumption for dynamic networks reduced. Also, simulation results show that MRT has better average accuracy and less average path length than other mechanisms, due to the security and energy aware.

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

1. INTRODUCTION

Due to rapid 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 decade. This is due to the fact 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 network [4], [5]. Currently, most of the trust evaluation structure belongs to a recommendation-

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

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' degree of honesty [6].

This article shows the last enhancement for WSNs by trust and reputation mechanisms found in literature. Modified Reputation-Based Trust (MRT) model for WSN security proposed and evaluated. 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 for trust, reputation and energy models are presented in Section 5. In Section 6, extensive experiments by simulation are conducted to prove the security and power efficiency 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. 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 with which many applications deal with everyday. Trust and reputation arrangement in distributed environments has been lately proposed as a mechanism for minimizing certain risks not fully covered by conventional network security schemes, gaining reasonably 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 10 years. We have surveyed the related work 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. Moreover, Marti et al [17] proposed the use of Watchdog and Path rater. Watchdog promiscuously listens to the transmission of the next node in the path to detect misbehaviors. Path rater keeps the ratings for other nodes and performs route selection by choosing routes that do not contain selfish nodes. However, the Watchdog mechanism needs to maintain the state information on the monitored nodes and the transmitted packets, which undoubtedly increases memory overhead.

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 2004, Xiong and Liu [20] presented one model called PEERTRUST model. This model has two main features. First, it introduces three basic trust parameters and two adaptive factors in computing trustworthiness of peers, namely, the feedback a peer receives from other peers, the total number of transactions a peer performs, the credibility of the

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

feedback sources, transaction context factor, and the community context factor. Second, it defines a general trust metric to combine these parameters. The limitation of this mechanism is that the computation convergence rate in large-scale peer-to-peer (P2P) systems is not provided [21]. The factors used in their trust model must be retrieved with a heavy overhead.

The EIGEN TRUST approach aggregates trust information from peers by having them perform a distributed calculation approaching the eigenvector of the trust matrix over the peers [22]. EIGEN TRUST relies on good choice of some pre-trusted peers, which are supposed to be trusted by all peers in the network. This assumption is a dangerous weakness point in a distributed computing environment. The reason is that pre-trust peers that have been selected may not last forever. When their score becomes unworthy after some transactions, this mechanism system may not work reliably.

Lopez et al. [23] proposed criteria and practices that Trust and Reputation designers should consider for constructing a good trust management system for WSNs. Then, to improve this area of research, a bio-inspired algorithm, called BTRM-WSN was presented. This algorithm aims to provide trust in WSN. In this research, the main focus of evaluation was to evaluate the selection percentage of trustworthy servers achieved with BTRM-WSN. BTRM-WSN remains resilient to a high percentage of malicious servers when this percentage is less than or equal to 80%. Its performance gets worse when there are 90% or more malicious servers in the WSN, and the problem intensifies when the size of the WSN grows [24].

Recently, Marmol, et al. [25] in 2012 applied linguistic fuzzy logic and fuzzy sets to a previous bio-inspired trust and reputation model for WSNs. This enhanced the interpretability of the trust model, making it more human friendly, or human readable, while keeping, and even improving, the accuracy of the underlying trust and reputation model.

Reputation-Base Trust (MRT) model for WSN security proposed. This model concentrated on reduces average path length to minimize energy consumption [26]. The contribution of this model is its ability to increase trustworthiness of network nodes and balance energy at the same time to solve WSNs security challenges. In this paper MRT model evaluated to prove its performance in front of existing trust and reputation models in terms of average accuracy, average path length and energy consumption.

3. GENERIC TRUST AND REPUTATION MODEL

All trust and reputation models have their own characteristics, parameters and properties. However, generality of them possess the same criteria about what steps have to be given in order to complete a whole process in a distributed system making use of a trust and/or reputation model. Those steps are depicted in Figure 1.

Figure 1: Generic Trust and Reputation Model Steps

In the first stage, behavioral information about the members of the monitored environment is collected. Then, that information is used to provide a score that will determine the reputation and/or trust worthiness of every node in the system. After that, the most trustworthy and/or reputable entity is generally selected and a transaction is performed with it, evaluating next, the satisfaction of the requester with the received service. According to that satisfaction, a last step of discard or accept is applied, modifying the previous given score to the selected party [13], [15].

4. MODIFIED REPUTATION-BASED TRUST EVALUATION MODEL

To prove the performance of the MRT model, it is evaluated and compared with EIGEN TRUST [5], PEERTRUST [20], POWERTRUST [21], and BTRM-WSN [24]. The comparison factors are average accuracy, average path length (number of hops) from source to destination, and energy consumption. One way to minimize threats in WSNs is to use community-based reputations to help estimate the trustworthiness of peers. A reputation-based trust supporting framework, which includes a coherent adaptive trust model for quantifying and comparing the trustworthiness of

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

peers is based on a transaction-based feedback system. In order to measure the accuracy of a proposed simulated trust and reputation model, we have to apply two security threats during simulations.

As shown in Figure 2, the first one has to do with the oscillating behavior of the malicious nodes offering the requested service. If this option is selected during simulation, after every 20 executions (i.e. transactions or interactions), each malicious server becomes benevolent. Then, the same percentage of previous malicious servers is randomly chosen to be malicious (note that with a scheme like this, a malicious server could remain malicious after 20 executions).

Another security threat introduced consists of the possibility for the malicious servers to form collusion among themselves, which implies that every malicious sensor will give the maximum rating for every other malicious sensor, and the minimum rating for every benevolent one.

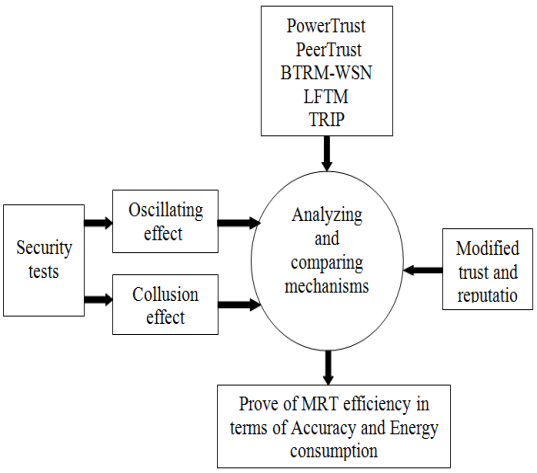

Figure 2: MRT Evaluation Model

5. TRUST AND REPUTATION MATHEMATICAL MODEL

This section describes the proposed mathematical models for energy, trust and reputation models. Energy model represents energy measurement for each sensor and energy for the whole network. Then, it shows a proposed mathematical model for the trust and reputation process. This model tries to minimize power consumption during the process and improve trustworthiness at the same time.

5.1 Reputation Model

In this model, [27] define the reputation of node y from the perspective of node x represented as follows:

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

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

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

5.2 Trust Model

In order to know the expected action of a cooperative node, we present trust in the mathematical model, estimating θ as the future behavior of node y, and observation of αy as cooperative and βy as non-cooperative behavior. [28] give a trust formula as follows:

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

where E is statistical expectation .

5.3 Energy Model

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

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

where E_{ele} is the receiver of electronics energy and assumed equal to 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 [29]. Moreover, the total energy consumed for the network is

Journal of Theoretical and Applied Information Technology
31st December 2014. Vol.70 No.3

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

$$E_{total} = \sum_{i=1}^{n} E_i \quad (4)$$

where E_i is the node total energy.

6. SIMULATION AND RESULTS

In this section simulation results for evaluation of proposed reputation model presented and comparison with well-known models 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 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

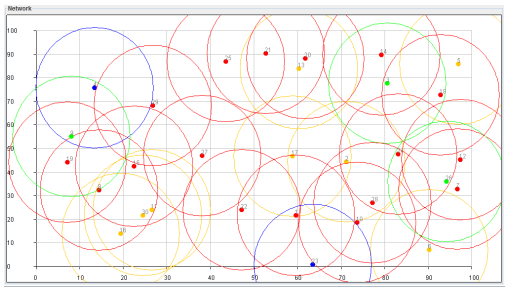

Figure 3: Simulation WSN Distribution for Trust and Reputation Model

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, security and privacy are evaluated by applying security threats to measure, such as collusion and oscillating of malicious nodes through three cases. First, the models are simulated without applying any threats. Second, the models' resilience against collusion threats is tested. Third, the models' strength towards oscillating threats is tested. The more secure the model the more resilient it will be to all these threats, following the configuration described in Table 1.

In the second experiment, average length (number of hops) of all paths of every simulated network measured and evaluated. All the three cases applied in the first experiment used.

In the last simulation, energy consumption for models is evaluated under effects of collusion and oscillating threats with comparison to other models.

6.2 Comparison with Well-Known Trust and Reputation Models

This section shows comparison results between proposed model and well-known models. Security and privacy are evaluated by applying security threats to measure, such as collusion and oscillating of malicious nodes. Initially, the models are simulated without applying any threats. Then, the models' resilience against collusion and oscillating threats is tested. In these tests, trust and reputation models should quickly respond against behavioral changes, and adapt to prevent selecting a malicious node as the most trustworthy one. The more secure the model the more resilient it will be to all these threats.

6.2.1 Average accuracy

The average accuracy factor is the important factor that indicates the security level. . High average accuracy means that the model is secure. The results displayed in Table 2 and graphically represented in Figure 4, Figure 5, and Figure 6 prove that MRT is generally more secure than other methods.

Journal of Theoretical and Applied Information Technology
31st December 2014. Vol.70 No.3

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

Table 2: Comparison between MRT and well-known trust and reputation models (Malicious Nodes Percentage ≈ 60%)

	WSN without collusion/ oscillating	collusion	oscillating
EIGEN TRUST	44%	85%	85%
PEER TRUST	59%	15%	80%
POWER RUST	78%	87%	90%
BTRM-WSN	60%	39%	90%
MRT	80%	69 %	91%

Figure 4 shows that MRT model is more secure than other models for WSNs without collision or oscillating effects due to its highest average accuracy. In WSN with collusion effect, MRT is more secure than PEER TRUST and BTRM-WSN trust models but less secure than other models as shown in Figure 5. MRT average accuracy for WSN with Oscillating Threat is better than other methods as shown in Figure 6.

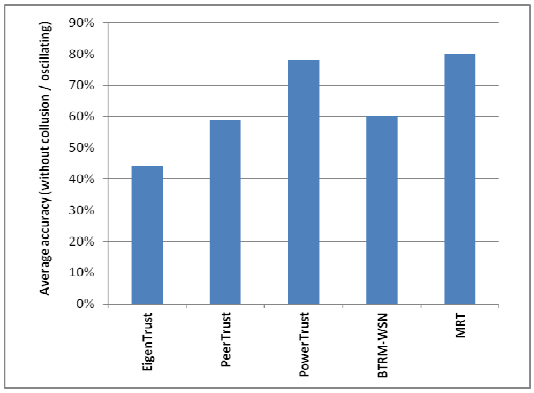

Figure 4: Comparison between MRT model and existing trust and reputation models in terms of average accuracy without collusion / oscillating

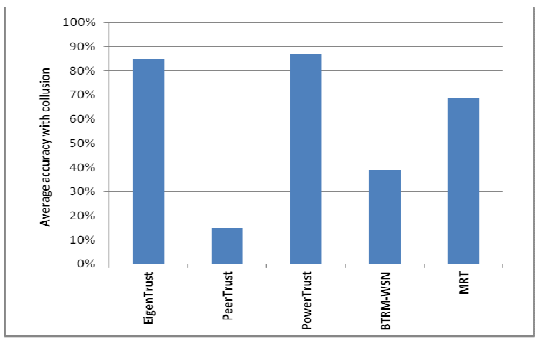

Figure 5: Comparison between MRT model and existing trust and reputation models in terms of average accuracy with collusion

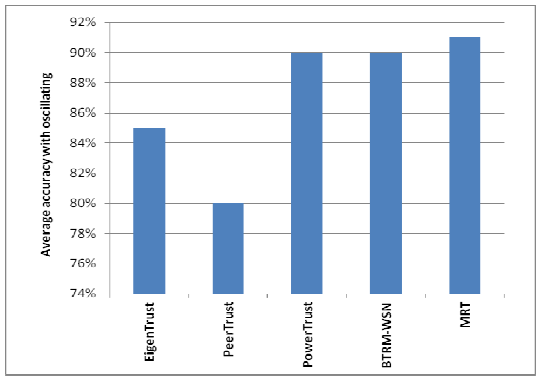

Figure 6: Comparison between MRT model and existing trust and reputation models in terms of average accuracy with oscillating

In summarizing the results, it can be seen that MRT is resilient to Oscillating effects and its accuracy and scalability remain high while results are optimal to WSN with or without collusion or oscillating threats.

6.2.2 Average path length

This factor indicates network efficiency and availability. Shorter average path length indicates that energy consumption is low and the network throughput is high due to increase in network lifetime. Results of this comparison are provided in Table 3.

Table 3: Comparison between MRT model and existing trust and reputation models in terms of average path length (Malicious Nodes Percentage ≈ 60%

	WSN without collusion/ oscillating	collusion	oscillating
EIGEN TRUST	7.5	7.4	6.4
PEER TRUST	7	6.8	6.5
POWER TRUST	6.5	7	7
BTRM-WSN	5.8	2.9	4.5
MRT	4.67	2.71	3.96

Results in Figure 7 show that MRT has an average length less than other mechanisms during simulation for WSN without applying oscillating and collusion threats. Figure 8 and Figure 9 prove the quality of the MRT model and that it is energy aware rather compared to other models during effects of oscillating and collusion threats.

To summarize these results, MRT has less average path length than other models during WSN simulation with or without threat tests which means

Journal of Theoretical and Applied Information Technology
31st December 2014. Vol.70 No.3

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

that it performs packet transfer from source to destination with less energy consumption.

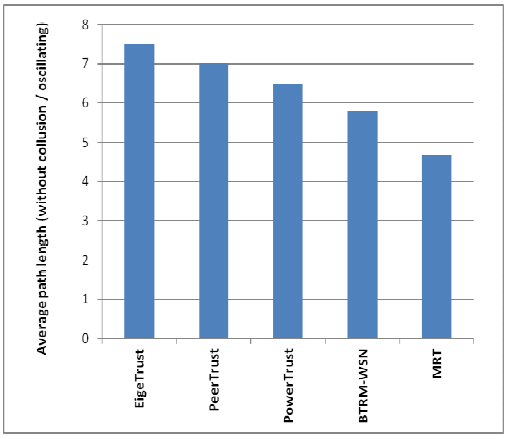

Figure 7: Comparison between MRT model and existing trust and reputation models in terms of average path length without collusion / oscillating

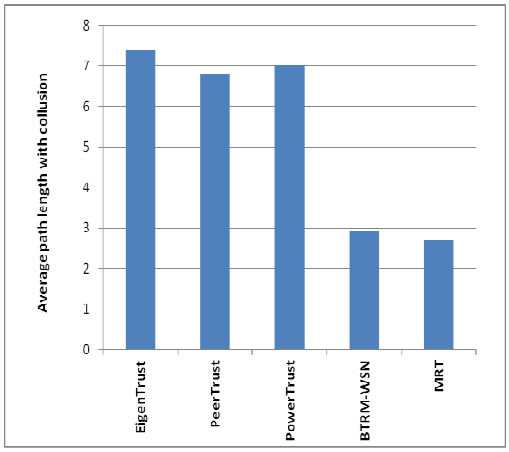

Figure 8: Comparison between MRT model and existing trust and reputation models in terms of average path length with collusion

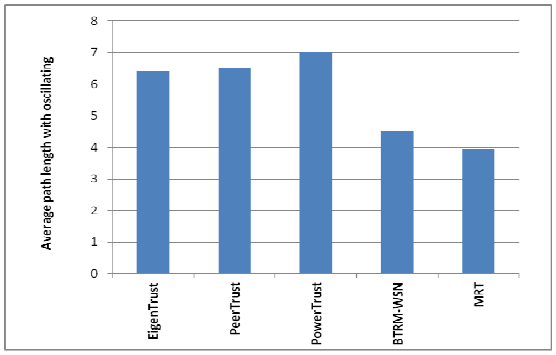

Figure 9: Comparison between MRT model and existing trust and reputation models in terms of average path length with oscillating

6.2.3 Energy consumption

Energy consumption is the main indicator of network lifetime. High energy consumption causes a network to die in a short time. Table 4 shows the energy consumption values for MRT and other well-known models under collusion and oscillating effects.

TABLE 4: Comparison between MRT model and existing trust and reputation models in terms of energy consumption (mj)

	collusion	oscillating
PEER TRUST	3.7*10^15.0	5.6*10^15.0
POWER TRUST	3.7*10^15.0	1.2*10^17.0
BTRM-WSN	5.8*10^15.0	5.3*10^17.0
MRT	1.5*10^13.0	2.1*10^16.0

From Figure 10 it can be noted that energy consumption is very much lower than other models during collusion effects. In the networks under oscillating effects MRT shows a decrease in energy consumption compared to PowerTrust and BTRM-WSN as show in Figure 11.

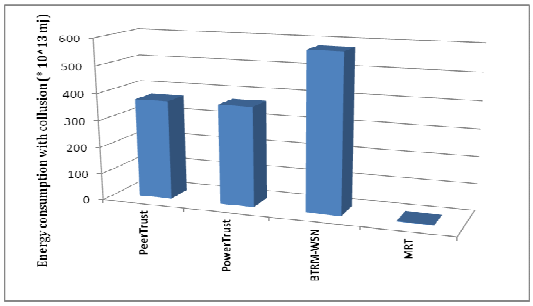

Figure 10: Comparison between MRT model and existing trust and reputation models in terms of energy consumption with collusion

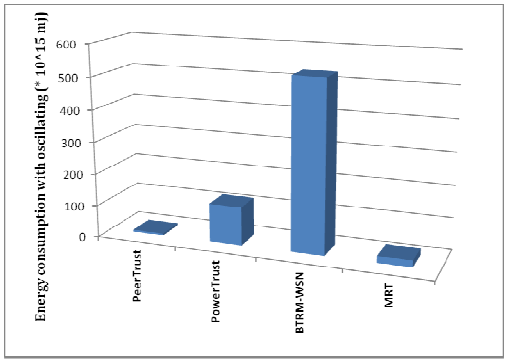

Figure 11: Comparison between MRT model and existing trust and reputation models in terms of energy consumption with oscillating

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

7. RESULTS DISCUSSION

Simulation outcomes for the MRT model show its performance and reliability for WSN security. Results indicate that MRT rather than other well-known models shows flexibility in strength and accuracy toward malicious nodes. Energy consumption by using MRT is lower than using other models. Accordingly, it can be summarized that the contribution of this research is as follows:

- The MRT model is resilient to collusion effects. Accuracy and scalability remain high for static WSNs and increase with increasing number of client sensors.
- Comparing well-known trust and reputation models such as EIGEN TRUST, PEER TRUST, PowerTrust, and BTRM-WSN with MRT shows that MRT has better average accuracy and less average path length than other mechanisms, due to the security and energy aware.

8. CONCLUSIONS AND FUTURE WORK

In WSNs security direction, this paper considered some popular trust and reputation models for WSNs. MRT model was proposed to improve WSNs security. This model was evaluated by applying security threats such as collusion and oscillating of malicious nodes in WSNs. Simulation results showed that the proposed model has security strengths against malicious nodes with oscillating and collusion effects. Results prove that it remains malleable to high percentages of malicious servers when the percentages of client sensors are greater than 60%. So, in small or large WSNs, the proposed study model would function properly regardless of malicious servers having high percentage. Thus, it can be said that general performance of MRT is high and energy consumption is low.

As future work, we need to conduct further research to conduct more experiments on the MRT model using different network sizes and variable number of executions. In addition, balancing the authentication, energy consumption with trust and reputation according to the scheme proposed in this study could be further investigated.

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.

[12] L. Mui, "Computational Models of Trust and Reputation: Agents, Evolutionary Games, And Social Networks", *PhD thesis*, Department of

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

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] J. Lopez, R. Roman, I. Agudo, & C. Fernandez-Gago, C. (2010). Trust management systems for wireless sensor networks: best practices, Computer Communications, vol. 33, no. 9, pp. 1086–1093..

[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] A. Alkalbani, A.O. Md Tap and T. Mantoro, "Modified Reputation-Base Trust (MRT) for WSN", *Journal of Theoretical and Applied Information Technology(JATIT)*, Vol. 56 No.2, pp.417-427 ..

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

[28] 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.

[29] 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.