Extensive Investigations on Bio-Inspired Trust and Reputation Model over Hops Coefficient Factor in Distributed Wireless Sensor Networks.

Vinod Kumar VERMA,
Department of Computer Science & Engineering,
Sant Longowal Institute of Engineering and Technology (SLIET), Deemed University,
Longowal -148106, District - Sangrur, Punjab, India
vinod5881@gmail.com, http://cs.sliet.ac.in/people/vinodverma/

ABSTRACT

Resource utilization requires a substantial consideration for a trust and reputation model to be deployed within a wireless sensor network (WSN). In the evaluation, our attention is focused on the effect of hops coefficient factor estimation on WSN with bio-inspired trust and reputation model (BTRM). We present the state-of-the-art system level evaluation of accuracy and path length of sensor node operations for their current and average scenarios. Additionally, we emphasized over the energy consumption evaluation for static, dynamic and oscillatory modes of BTRM-WSN model. The performance of the hops coefficient factor for our proposed framework is evaluated via analytic bounds and numerical simulations.

Keywords: Wireless sensor network, BTRM-WSN, accuracy, path length, energy.

1. INTRODUCTION

Wireless sensor networks, with its services, have changed our life in the last few years. In fact, we are using it as a way to access numerous domain services and applications such as defense equipments, ecological and habitat monitoring, industrial process control, home automation, weather forecasting, health care system, traffic control, civilian applications etc. Wireless sensors are small size devices equipped with radio transceivers and low power batteries. Typical features of sensor node include power, storage and low cost computational capability hardware [1-2]. A wireless sensor network is intended to sense, collect, processes and transmit event specific information, in order to accomplish a distributed domain task. Moreover, wireless sensor networks [3-4] are the type of networks, where the resultant is fully based on the sensor nodes cooperation. A wireless sensor network consists of a group of sensors or nodes connected through a linked mechanism to accomplish a distributed sensing task. Wireless sensor networks can be deployed in the conditions which are severe from the physical deployment point of view. Security aspect becomes the contemporary field of research in wireless sensor network and gaining more and more attention from scientists and researchers to proceed further [5]. Usually, wireless sensor networks are deployed in an open informant where the probability of an adversary [6] always remains more than in a closed environment. There are numerous proposals to detect an adversary node in the wireless sensor networks. Traditional means to protect a network include cryptography specific techniques and methodologies. Availability of cryptographic solutions redresses the issues like authentication, authorization, confidentiality and integrity but the requirements of wireless sensor networks are more diverse than the traditional security policies. Complex computations in the cryptography strategies [7] becomes its major drawbacks and made these policies unsuitable to be deployed in wireless sensor network, which constitutes severe power constraints. For the all set of services, trust is advisable and represents a key requirement that should be considered as a mandatory criterion for any application developer. Many efforts have been done so far to address the issue of trust and reputation management in several environments. Thus, for instance, a number of trust and reputation models have been proposed in the literature ranging from peer-to-peer networks [8-10], to wireless sensor networks (WSNs) [11-14], to (mobile) ad hoc networks [15-17], to multi-agent systems [18,19], or even to vehicular-to-vehicular networks [20-22]. Recently, trust and reputation management finds its place in some popular fields such as cloud computing [23-25], identity management and identity federation [26-28], web services [29-31], and the internet of things [32]. Hence, it is remarkable that the wider coverage and acceptance as well as a range of scenarios makes a trust and reputation model very useful and adequate. It is appropriate to mention at this stage that some authors have already applied bio-inspired algorithms in order to perform such trust and reputation management. Some examples are quality of service-based distance vector protocol [33], AntRep [34], time-based dynamic trust model [35] (which make use of ant colony systems [36] and ant colony optimization [37]), which further leads bio-inspired trust and reputation Model for WSN (BTRM-WSN) [38]. Some of the contributors exploited the benefits of fuzzy logic and fuzzy representation which leads to the development of models such as comprehensive reputation-based trust model with fuzzy subsystems [39], A fuzzy reputation agent system [40], or pervasive trust management [41]. An initiative towards linguistic fuzzy logic enhancement of a trust mechanism for distributed networks was proposed by Gomez Marmol et al. [42]. We selected bio-inspired trust and reputation model for investigations in terms of accuracy, path length and energy consumption. This research focuses on the hops coefficient factor based issue, which can be refereed as the coefficient of resource utilization, a trust and reputation model consumes when switching from one hop to another, in order to find the trustworthy nodes. We investigated our findings in extremely critical and rigorous environment.

This paper is an enhanced version of a previous paper [51], but in this new version, a deeper investigation on BTRM-WSN model over hops coefficient factor for static, dynamic and oscillatory modes of WSN has been provided. Additionally, a more detailed experimentation and a new comparative analysis have been added as a part of the new version of this paper.

Section 2 presented the BTRM-WSN trust and reputation model in wireless sensor networks. Section 3 highlights our motivation for research work. Section 4, illustrated the problem definition and system model. Section 5 describes the detailed design of our experimental setup. Simulation results and validations are presented and discussed in Section 6. Finally, conclusions are made in Section 7.

2. BTRM-WSN TRUST AND REPUTATION MODEL

This trust model for wireless sensor networks (WSN) is based on the bio-inspired algorithm of ant colony system [36-38][43-44]. In this model, most trustworthy path leads to find the most reputable service provider in a network. WSN launches a set of artificial agents while searching for a most reputable service provider. In order to carry out a decision about next sensor, a probability is given to each arc by the following Eq.(1).

$$pk(r,s) = \begin{cases} \dfrac{[\tau_{rs}]^{\alpha}[\eta_{rs}]^{\beta}}{\sum[\tau_{ru}]^{\alpha}[\eta_{ru}]^{\beta}} & if\ s \in Jk(r); \\ otherwise & 0 \end{cases} \tag{1}$$

where τ_{rs} pheromone value, η_{rs} denotes the heuristic associated with the link joining *r* and *s*, $J_k(r)$ represents the set of neighbors of node *r* not visited yet by ant *k*, and α , β parameters balancing the pheromone and the heuristic. The next Eq.(2) represents modification of the ants pheromone trace.

$$\tau_{s1s2} = (1 - \varphi)\tau_{s1s2} + \varphi\,\Omega \tag{2}$$

where $\Omega = (1+(1 - \varphi)(1- \tau_{s1s2}\ \eta_{s1s2}))\ \tau_{s1s2}$ denotes the convergence value of τ_{s1s2} and φ represents a parameter controlling the amount of pheromone. The best path found by all ants is indicated by Eq.(3).

$$\tau_{rs} = (1-\rho)\tau_{rs} + \rho\left(1 + \tau_{rs}\eta_{rs}Q\left(S_{Global_{Best}}\right)\right)\tau_{rs} \tag{3}$$

where $Q(S_{Global\_Best})$ denotes path quality. The quality of the S_k paths can be measured as the average of all the edges belongs to that path as depicted by Eq.(4).

$$Q(S_k) = \frac{\tau k}{\sqrt{Length(S_k)}}\%A_k \tag{4}$$

where $\%A_k$ denotes the percentage of trustworthy paths. The punishment or rewards of the path leading to the selected peer is given by Eq.(5).

$$\tau_{rs} = (\tau_{rs} - \varphi \times df_{rs})\frac{Sat}{df_{rs}} \tag{5}$$

where Sat reflects the satisfaction value. The distance factor joining the link between sensor *r* and *s* is given by the following Eq.(6).

$$df_{rs} = \sqrt{\frac{df_{rs}}{\mathrm{L}(S_k)(\mathrm{L}(S_k) - d_{rs} + 1}} \tag{6}$$

3. MOTIVATION FOR CURRENT WORK

To effectively exhibits and analyze the performance of a trust and reputation model remains the top priority for the wireless sensor network system. An optimal trust and reputation model can enhance the performance of the overall system, but the wireless sensor network system may not be dependent on the same. A single parameter in trust and reputation modeling strategy may give the best result for one instance, but we have to deploy such an efficient trust and reputation modeling strategies that provide optimal results in data dissemination. The improper assessment strategy may overload the entire network and consume more resources both in terms of energy and computation which result in the entire system performance degradation. There always remains dire influence of the parameters like hops coefficient, sensor augmentation and resource utilization factor in trust and reputation model of the entire operating environment when evaluating a specific wireless sensor network. The goal remains there is to carefully choose and examine the trust and reputation modeling strategies for the identification of parameters responsible for optimal information dissemination without compromising any constraints than expected outcome. Therefore, a typical realization should be required to identify the parameter contribution towards the scope of a particular trust and reputation model strategy for the wireless sensor networks.

4. PROBLEM DEFINITION AND SYSTEM MODEL

In our analysis, we consider hundred networks composed of fifty sensor nodes each for hundred scenarios in a two dimensional fields. Sensor nodes in a cluster with a specific radio range transmit the data to the cluster head and then the base station within the entire network. Network deployment focuses on hops coefficient and path length factor in the specified conditions. Although any trust and reputation sensor node strategy can be used in our model, we utilized BTRM-WSN trust and reputation model for our proposed framework. Accordingly, for static, dynamic and oscillatory wireless sensor networks with trust and reputation model strategy mentioned above, we are concerned in finding the following two problems. (i) What is the influence of hops coefficient factor over fixed coverage area on static, dynamic communication mode of wireless sensor networks, (ii) How the BTRM-WSN trust and reputation model affect the parameters like accuracy, resource utilization and energy consumption in the said WSN system.

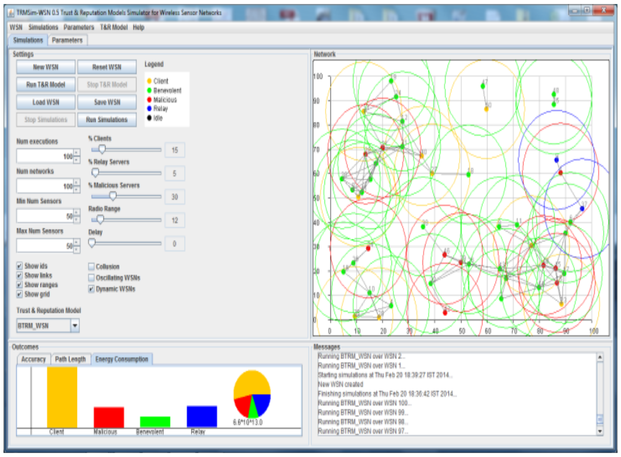
5. DETAILED SETUP

We focused on three parametric aspects namely: accuracy, path length and energy consumption for information dissemination in wireless sensor networks. For this, we have developed the unmitigated scenario pinpointing two main targets. Firstly, we are interested to find the value of three above mentioned parameters for stationary wireless sensor networks. We want to know the summation of all the node operations with sensor augmentation and resource utilization factor parameter. Lesser path length of node operation always given due attention as it consumes fewer resources and exhibits more efficiency. Secondly, we want to make an estimation of the sensor value variation effects on communication performance in correlation with two trust and reputation models. Finally, we made the comprehensive evaluation of energy consumption with static wireless sensor network in our proposed framework. We designed a wireless sensor network template using the following parameters as shown in Table 1.

Table 1 Scenario Parameters

Scenario Options	*Value*
% Client	*15*
% Relay Sever	*5*
% Fraudulent Server	*30*
Radio Range	*12*
Delay	*0*
Number Execution	*100*
Number of Network	*100*
WSN Area	*100 m × 100 m*
Minimum Number of Sensors	*50*
Maximum Number of Sensors	*50*
Hops Coefficient Factor	*0.1 - 1.0*
Node Orientation	*Static , Dynamic, Oscillatory*

15% of all nodes in a randomly created WSN acted as clients and the rest of 85% nodes acted as servers. 5% of the nodes acted as relay servers not offered any services and acted as relay nodes. The radio range of the nodes set at 12 hops to its neighbors. We consider a scenario where the percentage of malicious servers remained 30% which specify the indispensable condition for our WSN framework evaluation. We set the minimum and maximum number of sensors 50 that creates a WSN. Sensor nodes belonging to our developed networks spread over the area of 100 m × 100 m. A total of hundred networks were examined hundred times and the final result reflects the average value of all the networks. The process of searching trustworthy server was conducted hundred times for each network. Table 1 displays the summary of parameters deployed in our model. Figure 1 shows the setup of our simulation. In the simulation window, yellow dots denotes client nodes, green dots represent the benevolent nodes, red dots show malicious node, blue dots depicts relay nodes and black dots exhibit idle nodes respectively.


TRMSim-WSN 0.5 Trust & Reputation Models Simulator for Wireless Sensor Networks
WSN Simulations Parameters T&R Model Help
Simulations Parameters
Settings
New WSN
Reset WSN
Run T&R Model
Stop T&R Model
Load WSN
Save WSN
Stop Simulations
Run Simulations
Legend
Client
Benevolent
Malicious
Relay
Idle
Network
Outcomes
Accuracy Path Length Energy Consumption
Client Malicious Benevolent Relay
6.6*10*13.0

Num executions: 100
Num networks: 100
Min Num Sensors: 50
Max Num Sensors: 50
% Clients: 15
% Relay Servers: 5
% Malicious Servers: 30
Radio Range: 12
Delay: 0
☑ Show ids
☑ Show links
☑ Show ranges
☑ Show grid
□ Collusion
□ Oscillating WSNs
☑ Dynamic WSNs
Trust & Reputation Model: BTRM_WSN

Messages

```
Running BTRM_WSN over WSN 2...
Running BTRM_WSN over WSN 1...
Starting simulations at Thu Feb 20 18:39:27 IST 2014...
New WSN created
Finishing simulations at Thu Feb 20 18:36:42 IST 2014...
Running BTRM_WSN over WSN 100...
Running BTRM_WSN over WSN 99...
Running BTRM_WSN over WSN 98...
Running BTRM_WSN over WSN 97...
```

Figure 1 Simulation Scenario

6. ANALYTICAL RESULTS AND VALIDATIONS

This section enables us to implement and evaluate trust and reputation models for different wireless sensor network modes. We used Java based event driven TRMSim-WSN simulator [45] version 0.5 for wireless sensor network allowing the researchers to simulate and represent random network distributions and provides statistics of different data dissemination policies including the provision to test the different trust and reputation model strategies. Numerous decisions like static or dynamic or oscillating networks, a combination of dynamic and oscillatory networks, the percentage of fraudulent nodes, the percentage of nodes acting as clients or servers, etc. can be implemented as well as tested over it. The proposed model is tested on BTRM-WSN trust and reputation models with extreme conditions. We reported a comprehensive analysis based on hops coefficient factor and resource utilization factor over static, dynamic and oscillatory wireless sensor networks. Static WSN can be referred as the type of networks where the sensors positions remain predefined and fixed. Dynamic WSN are the type of WSN where the sensors swaps into the idle state for a while if they do not receive any request within certain amount of time. In case of oscillatory WSN, each malicious sensor becomes benevolent after certain executions. We gathered data for three metrics namely accuracy, path length and energy consumption. The outcome of the simulations will be subject to the following subsections.

6.1 Accuracy Investigations

The term accuracy in the trust and reputation models may be defined as the selection percentage of trustworthy nodes. We calculated the accuracy from two viewpoints namely: Current and average. Initially, we calculated current accuracy corresponds to static, dynamic and oscillatory WSN mode as shown in figure 2. Static WSN mode exhibits less zigzag behavior than dynamic and oscillatory WSN modes. In case of static WSN mode the current accuracy remained more stable as compared to other WSN modes. The reason behind the same is complex computation for accuracy calculation in dynamic and oscillatory WSN mode. Next, we calculated average accuracy which depicts approximately similar behavior as we noticed in case of current accuracy. At the beginning and at the ending instance, average accuracy outperforms current accuracy as shown in figure 3. This is because of the fact that current accuracy reflects the resultant of one event whereas the average accuracy depicts the summation of all the events. One common observation we noticed that the accuracy reflect incremental behavior as we increase the hops coefficient values in BTRM-WSN trust and reputation model.

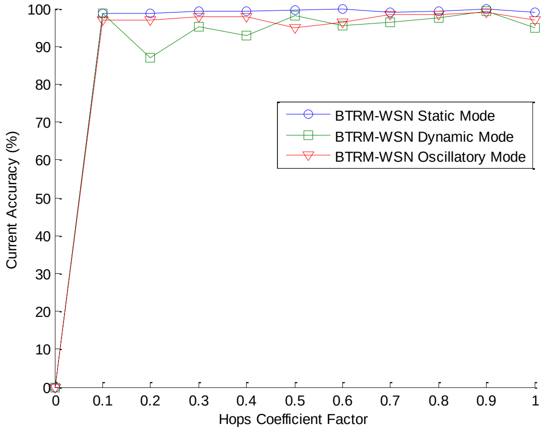


Figure 2 - Current accuracy versus hop coefficient factor in BTRM-WSN model

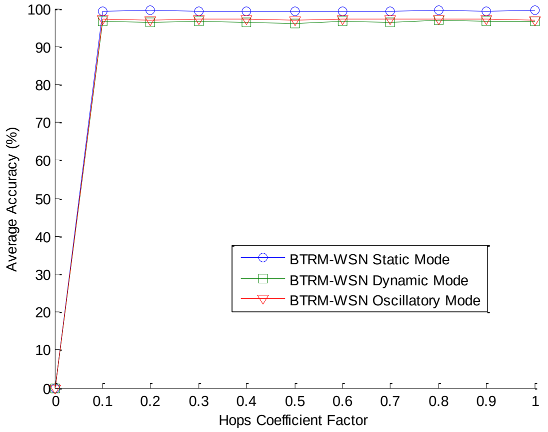


Figure 3 - Average accuracy versus hop coefficient factor in BTRM-WSN Model

This shows a good agreement with the results reported in reference [46]. An initiative towards the description of energy consumption analysis for different trust and reputation models was proposed in reference [46]. We enhanced this evaluation towards a bit intricate assessment by incorporating hops coefficient factor, resource utilization and energy evaluation aspect in our scenario.

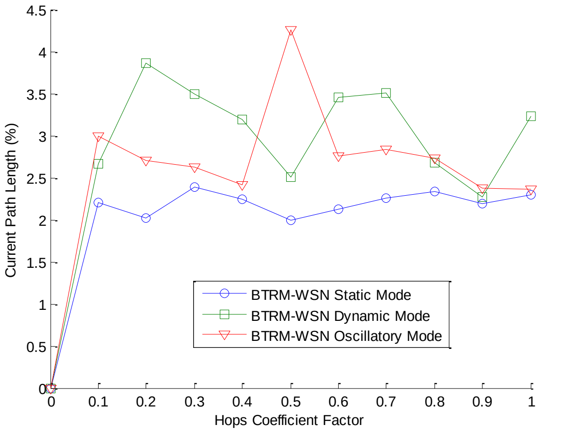


Figure 4 - Current path length versus hop coefficient factor in BTRM-WSN Model

Further, we observed average path length which shows steady behavior than the current path length as reported in figure 5. One common thing we analyzed that the dynamic and oscillatory modes of WSN consumes more resources than the static WSN in both types of path length values.

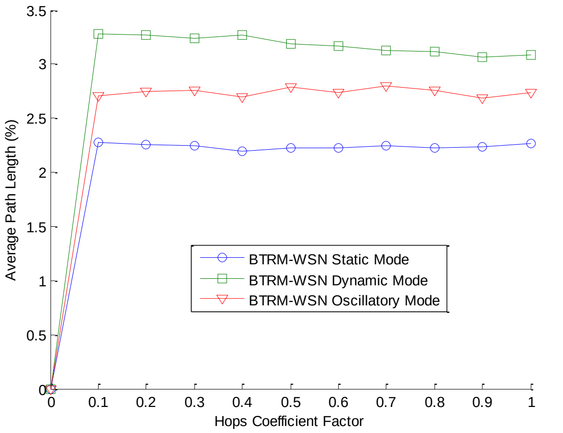


Figure 5 - Average path length versus hop coefficient factor in BTRM-WSN Model

We also observed that the static WSN mode is more prone towards resource utilization than dynamic and oscillatory WSN modes. We proposed a more robust framework subsuming different WSN nodes versus hops coefficient and resource utilization on a single platform. Verma et al. [47] presented scalability impact on the wireless sensor network. We extended this scalability concept to a further extent by adhering the hops coefficient towards the evaluation of BTRM-WSN trust and reputation model which make our proposal more robust. Moreover, Xiong et al. [48] reported peer to peer trust and reputation based model for structured peer to peer networks, including strategies for its implementation and evaluation in decentralized environmental conditions. Especially for unstructured peer to peer networks based on parameters was suggested by Chen et al. [49]. We enhanced the contribution to a certain extent by hops coefficient, path length and energy consumption parameters for wireless sensor network evaluation making our investigation more rigorous and real time.

6.4 Energy Concerns

Lastly, we focused on the average energy consumption for BTRM-WSN trust and reputations model. A comparative analysis from the energy consumption aspect is shown in figure 6.

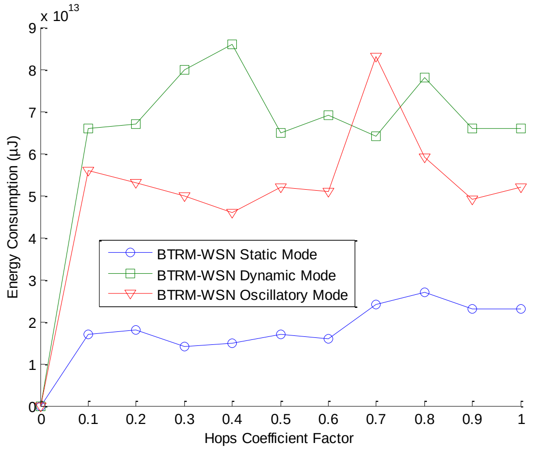


Figure 6 - Energy consumption versus hop coefficient factor in BTRM-WSN Model

We observed that the energy consumption increases with the increase in the hops coefficient factor in a zigzag manner. In case of static WSN, energy consumption exhibits gradual incremental behavior and remains maximum for the hops coefficient value 0.8 and minimum for 0.1. For the dynamic WSN mode, energy consumption remains highest at the hops coefficient value 0.4 and lowest for 0.1.For the oscillatory mode of WSN, energy consumption remains at the peak with hops coefficient factor value 0.7 and lowest at 0.4. Marmot. et al. [50] reported a comparative analysis of the energy consumption with respect to sensors specific aspects. In our proposal, we extended this concept towards a more robust evaluation with the static and dynamic WSN mode.

7. CONCLUSIONS

This paper concluded the influence of hops coefficient factor on the BTRM-WSN trust and reputation models in wireless sensor networks. We have observed the effect of hops coefficient factor for static, dynamic and oscillatory modes of WSN. It is evident from the simulation that there is a strong relationship in between hops coefficient factor and resource utilization on the WSN modes of trust and reputation model evaluation. We evaluated a wireless sensor network framework with reference to three performance metrics namely: accuracy, path length and energy consumption viewpoint. We estimated accuracy and path length in terms of overall percentage of the functionality whereas energy consumption in terms of millijoule specifically for sensor node operations. We stressed on three major directions. Firstly, we evaluated accuracy, path length and energy consumption for BTRM-WSN trust and reputation model. Secondly, we investigated the entire framework for hops coefficient factor evaluation on above stated trust and reputation model and lastly the same model is deployed for the overall evaluation of a static, dynamic and oscillatory wireless sensor networks. We observed that with the increment of the hops coefficient factor value reflects their strong affection and correlation in static and dynamic WSN modes. We can predict with our investigations that more hops coefficient value better will be the probability of accuracy, optimal resource utilization and more energy consumption by the wireless sensor network system. Further, we also estimated that static WSN can have more probably of accuracy, optimal path length and lesser energy consumption than the dynamic and oscillatory WSN mode. In the future, we would like to work towards additions on newer trust and reputation models for the wireless sensor network domain.

8. REFERENCES

[1] A. Alkalbani, T. Mantoro, and A. O. Md Tap, "**Improving the Lifetime of Wireless Sensor Networks Based on Routing Power Factors**", NDT , IEEE UAE Conference , Dubai, UAE, April 2012.

[2] 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), 0-7695-2777-9/07.2007.

[3] Chee-Yee Chong, Srikanta P. Kumar **"Sensor Networks: Evolution, Opportunities and Challenges**" proceeding of the IEEE. Vol. 91, No. 8, pp.1247-56 August 2003.

[4] IF Akyildiz, W Su, Y Sankarasubramaniam, E Cayirci**, A survey on sensor networks.** IEEE Commun Mag. 40(8), 102–114 (2002). doi:10.1109/ MCOM.2002.1024422.

[5] Jim Esch, "**A Survey of Trust and Reputation Management Systems in Wireless Communications**" Proceedings of the IEEE | Vol. 98, No. 10, October 2010, Digital Object Identifier: 10.1109/JPROC.2010.2060252.

[6] J. Hurt, Y. Lee, H. Yoont, D. Choi, and S. Jin, "**Trust evaluation model for wireless sensor networks**," in Proceedings of the 7th International Conference on Advanced Communication Technology (ICACT '05), pp. 491–496, Phoenix Park, Republic of Korea, February 2005.

[7] Q. Jing, L. Y. Tang, and Z. Chen, "**Trust management in wireless sensor networks**," Journal of Software, vol. 19, no. 7, pp. 1716–1730, 2008.

[8] Kamvar S, Schlosser M, Garcia-Molina H. "**The Eigen Trust algorithm for reputation management in P2P networks**". Proceedings of the International World Wide Web Conference (WWW), Budapest, Hungary, 2003.

[9] Xiong L, Liu L. "**PeerTrust: supporting reputation-based trust in peer-to-peer communities**". IEEE Transactions on Knowledge and Data Engineering 2004; 16(7):843–857.

[10] Zhou R, Hwang K. "**PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing**". Transactions on Parallel and Distributed Systems 2007; 18(4):460–473.

[11] Boukerche A, Xu L, El-Khatib K. "**Trust-based security for wireless ad hoc and sensor networks**". Computer Communications 2007; 30(11–12):2413 –2427.

[12] Dhurandher SK, Misra S, Obaidat MS, Gupta N."**An ant colony optimization approach for reputation and quality of service based security in wireless sensor networks**". Security and Communication Networks 2009; 2(2):215-224.

[13] Kim TK, Seo HS. "**A trust model using fuzzy logic in wireless sensor network**". Proceedings of World Academy of Science, Engineering and Technology, vol. 32, 2008; 69–72.

[14] Zhang Z, Ho PH, Nat-Abdesselam F. "**RADAR: A reputation-driven anomaly detection system for wireless mesh networks**". Wireless Networks 2010; 16:2221–2236.

[15] Omar M, Challal Y, Bouabdallah A. "**Reliable and fully distributed trust model for mobile ad hoc networks**". Computers and Security 2009; 28(3–4):199 –214.

[16] Buchegger S, Le Boudec JY. "**A robust reputation system for P2P and mobile ad-hoc networks**". Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems, Cambridge MA, USA, 2004.

[17] Almenárez F, Marín A, Campo C, García C. "**PTM: a pervasive trust management model for dynamic open environments**". Privacy and Trust, First Workshop on Pervasive Security and Trust, Boston, USA, 2004.

[18] Sabater J, Sierra C. "**REGRET: reputation in gregarious societies**". In Proceedings of the Fifth International Conference on Autonomous Agents, Müller JP, Andre E, Sen S, Frasson C (eds). ACM Press: Montreal, Canada, 2001;194–195.

[19] Songsiri S. M. "**Trust: a reputation-based trust model for a mobile agent system**". In Autonomic and Trusted Computing, no.4158 in LNCS Third International Conference, ATC 2006. Springer: Wuhan, China, 2006; 374–385.

[20] Breuer J, Held A, Leinmller T, Delgrossi L." **Trust issues for vehicular ad hoc networks** ". 67th IEEE Vehicular Technology Conference (VTC2008-Spring), Singapore, 2008.

[21] Raya M, Papadimitratos P, Gligor V, Hubaux JP. " **On data-centric trust establishment in ephemeral ad hoc networks** ". Proceedings of IEEE INFOCOM, Phoenix, AZ, USA, 2008.

[22] Lo NW, Tsai HC." **A reputation system for traffic safety event on vehicular ad hoc networks** ". EURASIP Journal on Wireless Communications and Networking 2009; 2009:1–10.

[23] Takabi H, Joshi JBD, Ahn GJ. "**Security and privacy challenges in cloud computing environments**". IEEE Security and Privacy 2010; 8:24–31. DOI: 10.1109/MSP.2010.186.

[24] Wang S, Zhang L, Wang S, Qiu X. "**A cloud-based trust model for evaluating quality of Web services**". Journal of Computer Science and Technology 2010; 25(6):1130-1142. DOI: 10.1007/s11390-010-9394-1.

[25] Hwang K, Kulkarni S, Hu Y."**Cloud security with virtualized defense and reputation-based trust management**". Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 2009;717–722, DOI: 10.1109/DASC.2009.149.

[26] Gómez Mármol F, Girao J, Martínez Pérez G. " **TRIMS, a privacy-aware trust and reputation model for identity management systems** ". Elsevier Computer Networks Journal 2010; 54(16):2899–2912. DOI: 10.1016/j.comnet.2010.07.020.

[27] Mohan A, Blough DM. " **Attribute Trust - a framework for evaluating trust in aggregated attributes via a reputation system** ". In Proceedings of the 2008 Sixth Annual Conference on Privacy, Security and Trust, 2008; 201–212. DOI: 10.1109/PST.2008.28.

[28] Windley PJ, Daley D, Cutler B, Tew K. " **Using reputation to augment explicit authorization** ". In Proceedings of the 2007 ACM workshop on Digital identity management, DIM '07, 2007; 72–81.

[29] Conner W, Iyengar A, Mikalsen T, Rouvellou I, Nahrstedt K." **A trust management framework for service-oriented environments** ". Proceedings of the 18th International Conference on World Wide Web, WWW '09, 2009; 891–900, DOI: 10.1145/1526709.1526829.

[30] Malik Z, Bouguettaya A. " **RATEWeb: Reputation Assessment for Trust Establishment among Web services** ". The VLDB Journal 2009; 18(4):885–911. DOI: 10.1007/s00778-009-0138-1.

[31] Bianculli D, Jurca R, BinderW, Ghezzi C, Faltings B. "**Automated dynamic maintenance of composite services based on service reputation**". Proceedings of the 5th International Conference on Service-Oriented Computing, ICSOC '07, 2007; 449–455. DOI: 10.1007/978-3-540-74974-5_42.

[32] Sachin B, Parikshit M, Antonietta S, Neeli P, Ramjee P. " **Proposed security model and threat taxonomy for the Internet of Things (IoT)** ". In Recent Trends in Network Security and Applications, Third International Conference, CNSA 2010, Communications in Computer and Information Science vol. 89, Natarajan M, Selma B, Nabendu C, Dhinaharan N (eds): Chennai, India, 2010; 420–429.

[33] Dhurandher SK, Misra S, Obaidat MS, Gupta N." **An ant colony optimization approach for reputation and quality-of service-based security in wireless sensor networks**". Security and Communication Networks 2009; 2(2):215-224.

[34] Wang W, Zeng G, Yuan L." **Ant-based reputation evidence distribution in P2P networks** ". In GCC, Fifth International Conference on Grid and Cooperative Computing. IEEE Computer Society: Changsha, Hunan, China, 2006; 129–132.

[35] Zhuo T, Zhengding L, Kai L. " **Time-based dynamic trust model using ant colony algorithm** ". Wuhan University Journal of Natural Sciences 2006; 11(6):1462–1466.

[36] Dorigo M, Stützle T."**Ant Colony Optimization"**. Bradford Book: Cambridge, MA, 2004.

[37] Cordón O, Herrera F, Stützle T." **A review on the ant colony optimization metaheuristic: basis, models and new trends** ". Mathware and Soft Computing 2002; 9(2–3):141–175.

[38] Gómez Mármol F, Martínez Pérez G." **Providing trust in wireless sensor networks using a bio-inspired technique** ".Telecommunication Systems Journal 2011; 46(2):163–180.

[39] Tajeddine A, Kayssi A, Chehab A, Artail H. **" PATROL-F- a comprehensive reputation-based trust model with fuzzy subsystems** ". In Autonomic and Trusted Computing, no.4158 in LNCS Third International Conference, ATC 2006. Springer: Wuhan, China, 2006; 205–217.

[40] Carbó J, Molina JM, Dávila J." **Trust management through fuzzy reputation** ". International Journal of Cooperative Information Systems Mar 2003; 12:135–155.

[41] Almenárez F, Marín A, Campo C, García C. " **PTM: a pervasive trust management model for dynamic open environments Privacy and Trust** ", First Workshop on Pervasive Security and Trust, Boston, USA, 2004.

[42] GómezMármol F, Gómez Marín-Blázquez J,Martínez Pérez G. " **Linguistic fuzzy logic enhancement of a trust mechanism for distributed networks** '. Proceedings of the Third IEEE International Symposium on Trust, Security and Privacy for Emerging Applications (TSP-10), Bradford, UK, 2010; 838–845. DOI: 10.1109 /CIT.2010. 158.

[43] Dorigo, M., & Gambardella, L. "**Ant colony system: a cooperative learning approach in the traveling salesman problem**". IEEE Transaction on Evolutionary Computing, 1(1), 53–66.1997.

[44] Dorigo, M., Gambardella, L., Birattari,M., Martinoli, A., Poli, R.,& Stützle, T. " **Ant colony optimization and swarm intelligence** " in LNCS 2006, Vol. 4150. 5th international workshop, ANTS 2006. Brussels: Springer, 2006.

[45] Félix Gómez Mármol, Gregorio Martínez Pérez, "**TRMSim-WSN, Trust and Reputation Models Simulator for Wireless Sensor Networks**", IEEE International Conference on Communications (IEEE ICC 2009), Communication and Information Systems Security Symposium, Dresden, Germany, 14-18 June 2009.

[46] A. S. Alkalbani, A.O. Md. Tap, T. Mantoro "**Energy Consumption Evaluation in Trust and Reputation models for Wireless Sensor Networks**", 5th International Conference on Information and Communication Technology for the Muslim World, 2013.

[47] Vinod Kumar Verma, Surinder Singh, N.P Pathak., "**Analysis of scalability for AODV routing protocol in wireless sensor networks**", Optik-International Journal of Light and Electron Optics .Sciencedirect, (2013), http://dx.doi.org/10.1.016/j.ijleo.2013.07.041.

[48] L. Xiong and L. Liu, "**PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities**," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 843-857, 2004.

[49] S. Chen Y. Zhang G. Yang ,"**Parameter-estimation based trust model for unstructured peer-to-peer network's**" IET Communication, 2011, Vol. 5, Issue 7, pp. 922–928 & The Institution of Engineering and Technology 2011, www.ietdl.org doi: 10.1049/iet-com.2010.0619

[50] Go´mez Ma´rmol F, Martı´nez Perez, G. "**Providing trust in wireless sensor networks using a bio-inspired technique**". In Proceedings of the networking and electronic commerce research conference, NAEC'08. Lake Garda, Italy; Sep 2008.

[51] Vinod Kumar Verma, "**Bio-inspired trust and reputation model investigations over hops coefficient factor in static and dynamic wireless sensor networks**", in proceeding of 7th international multi-conference on engineering and technological innovation (IMETI-2014), Orlando, Florida, USA.