Pervasive Investigations of Trustworthiness over Diverse Orientations of Apportioned Heterogeneous Mobile Networks

Vinod Kumar Verma

***Abstract*—**.Trust and reputation are the prime factors of concern for any apportioned system application nowadays. This paper focuses on the comprehensive evaluation of trustworthiness of apportioned peer to peer networks from a different facet. We developed over model incorporating two orientations namely: stationary and mobile networks. We highlighted the impact of power node augmentation factor along with collusion issue for power trust and reputation model. Moreover, we estimated over designated model over performance based issues like accuracy, pathlength and power consumption. Finally, the outputs converged from our investigation are the indicative to implement analytical exploration over heterogeneous apportioned mobile networks. Experimental setup through simulation proves the validity of our designated model for heterogeneous mobile networks.

***Keywords*—** Augmentation, collusion, networks, power, reputation, trust.

I. Introduction

PEER to peer computing becomes the considerable are of research for scientists and researcher across the globe in recent years. This is actually due to the wider area of applications of peer to peer computing in distributed wireless networks. Real time distributed peer to peer systems requires severe designing constraints like mobility, scalability, robustness, file sharing [1] and digital content delivery [2]. Despite of these critical challenges, the motive to secure peer to peer system is still lagging. There is possibility of attack by vulnerable nodes to damage the security of real time applications. Numerous means have been suggested by researchers in the past to provide secure and reliable applications. Researchers are working for the assurance of adequate services expected through the distributed applications. Trust and reputation models are the probable solutions to overcome the venerable attacks in distributed peer to peer networks. Some of the initiatives in the direction to secure peer to peer system have been already proposed by researchers in the literature. The methods like fuzzy logic [3], Bayesian networks [4], bio-inspired algorithm [5] have been proposed to manage trust and reputation in distributed wireless systems like peer to peer systems [6], ad-hoc networks [7], wireless sensor networks [8] and multi agent based systems [9]. Some of the studies regarding security threats were reflected by researchers in [10-11]. Marmol et al. [12] reported security threats scenarios in trust and reputation models for distributed systems. Verma et al. [13] proposed collusion based realization of trust and reputation models in extreme fraudulent environment over static and dynamic wireless sensor networks. Verma et al. [14] also reported investigations about the impact of malicious servers over trust and reputation models in wireless sensor networks. Recently, authors in [15] highlighted sensors augmentation influence over trust and reputation models realization for dense wireless sensor networks. Nevertheless, we also have observed that many researchers have analyzed different trust and reputation model from different perspectives. But still there is dire need to evaluate and access these models from rigorous assessment point of view, in order to make the application more secure. Here, in this paper we focused on the one of the most robust trust and reputation model namely: power trust. We comprehensively evaluated this model from power node augmentation viewpoint and present our investigations that surely help the peer to peer system designer.

This paper is an enhanced version of a previous paper [18], but in this new version, a deeper investigation on power trust and reputation model over power node augmentation factor for apportioned stationary and mobile networks. Moreover, a new issue 'collusion' has been incorporated in our proposed simulation model for apportioned stationary and mobile peer to peer networks. Additionally, a more detailed experimentation and a new comparative analysis have been added as a part of the new version of this paper. The remaining of this paper is organized in the following sections. Section 2 reported the power trust model description and related work in peer to peer networks. Section 3 presented our detailed simulation design and setup. Section 4 describes the results and validations of our proposed model. Finally, conclusions are made in Section 5 followed by references in Section 6.

II. Power Trust and Reputation Model

This section provides the background and related work on power trust and reputation model with assumptions required for the later sections. This model was proposed by Zhou and

Vinod Kumar Verma is Assistant Professor with Department of Computer Science & Engineering, Sant Longowal Institute of Engineering & Technology (Deemed University, Longowal-148106, Sangrur, Punjab, India. (phone: +91-9417927536;e-mail: vinod5881@gmail.com).

Hwang [16] specifically for more mobile and distributed networks requiring complex constraints like scalability and robustness. Peer to peer feedback mechanism plays a critical role towards the strength determination of reputation system. This model focused to evaluate the feedback received from the peers available in the networks. The reputation is being calculated by assigning the score at the local as well as global level. In order to calculate the trust score at the local level, Bayesian method is used. For the global trust score calculation, distributed ranking mechanism and strategies are used. This model works on the principal of power law which states that the node with fewer feedbacks is common whereas the node with the maximum feedbacks is very rare. So, the node with higher feedbacks is preferred and works as the power node for the entire network. This power node attracts most trustworthiness and reputation in the entire system. The power node can be replaced with other in case it becomes inactive or showing irregular behavior. In order to calculate the reputation score, let there are *k* most reputable nodes in the system which are selected using distributed ranking mechanism and further sorted using hash function. Actually, the power trust model builds trustworthy networks on the top of peer to peer system where ach node knows the reputation score of each other. So, all the nodes in the networks should have local reputation score which further aggregated to make the global trust score in the peer to peer system. A reputation vector *V* is being formed by all the global scores of the nodes using following equation (1).

$$V = \{v_1, v_2, v_3 \dots \dots \dots \dots . v_n\} \quad (1)$$

We consider a trust matrix $TM = (tm_{ij})$ where $tm_{ij} \epsilon [0,1]$ is the normalized local trust value defined by equation (2).

$$tm_{ij} = fb_{ij} / \sum fb_{ij} \quad (2)$$

where $\sum tm_i = 1$ and fb_{ij} represents most recent feedback that node *i* gives node *j*. Further, assuming initial reputation vector set V_0 and successive reputation vectors score are iteratively calculated using equation (3).

$$V_{t+1} = TM^T \times V_t \quad (3)$$

where $v_i = 1/n$ and while $\left| V_{(t)} - V_{(t-1)} \right| > \epsilon$.

The global reputation vector will converge to Eigenvector after *p* successful iterations. Lastly, this global score is being updated by the power nodes to entire peer to peer system.

III. Detailed Setup

We implemented our proposed model with Java-based simulator to explore power trust and reputation model for apportioned peer to peer networks [17]. Table 1 displays the summary of parameters deployed in our model. In our designated model, the simulation had the following constraints. We executed our model over hundred apportioned stationary and mobile peer to peer networks. We used power trust model with the following parameters. Power node augmentation value varies from 0.01 to 0.1 and their weights value is 0.25. Non-damping factor value remains 0.1 with zero trust selection probability value 0.2. The deployment area for our network is 100 m × 100 m.

Table 1. Scenario Parameters

Scenario Options	**Value**
Deployment Area	100 m ×100 m
Network Orientation	Stationary, Mobile
Number of Networks	100
Number of Executions	10
Minimum Number of Sensors	50
Maximum Number of Sensors	50
Relay Peers (%)	5
Malicious Peers	70
Radio Range	12
Delay	0 sec
Clients (%)	15
Security Model	Power Trust & Reputation
Power Node Augmentation	0.01 - 0.10
Power Node Weights	0.15
Small error Threshold	0.0001
Trust Affecting Factor	Collusion

On each network, the percentage of malicious peers is always 70%. Rests of 30% peers are therefore acting as servers including 5 % relay peers. There is no delay factor and radio range is 12 m. The simulation structure of our model is shown in figure 1. In simulation windows yellow dots denote client peers, green dots depict benevolent peers, red dots reflect malicious peers, blue dots represent relay peers, black dots represents idle peers, pink dots exhibits power peers and circle shows radio ranges corresponding to individual peers.

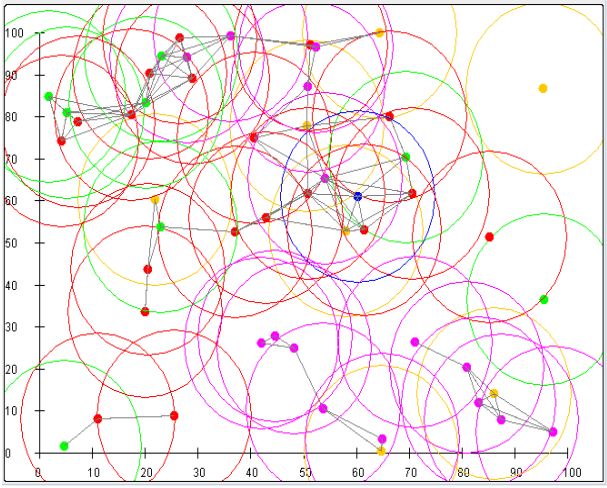

Fig. 1. Simulation Snapshot

IV. Results and Discussion

We investigated the performance of power trust and reputation model over apportioned stationary and mobile peer to peer networks. Moreover, we evaluated stationary and mobile networks over the collusion issue. Collusion may be defined as the probability of giving false rating to the trustworthy node. We focused on three factors namely: (i) accuracy, (ii) pathlength and (iii) energy consumption. An accuracy value may be referred as the fault free services provide by the peers in the networks. Pathlength value can be

defined as the utilizations of resources consumed by the peer in the apportioned networks. Energy consumption may be denoted as the power consumed by the peers in our deployed framework. We evaluated accuracy and pathlength from its current and average value *i.e.* for the last network and summation of all the deployed apportioned peer to peer networks.

A. Stationary Peer to Peer Networks Evaluations

Figure 2 shows the accuracy analysis of apportioned stationary peer to peer networks. We examined the accuracy with respect to power node augmentation for its current and average evaluation. We found that the current accuracy value shows non linear behavior and remained minimum at 0.05 and maximum at 0.1 power node augmentations. In case of average accuracy, we noticed that the accuracy value depicts some steady behaviour as compare to current accuracy. Its value remains maximum at 0.1 and minimum at 0.03 power node augmentation values respectively. We observed that the current accuracy show the non linear behaviour corresponds to average accuracy. This is because of the fact that the current accuracy depicts the value of the last event occurred in the last network whereas average accuracy reflects summations of all power node augmentation values in all networks. This shows a good agreement with the results reported in [13]. We extended the work of [13] to power node augmentation evaluation aspect.

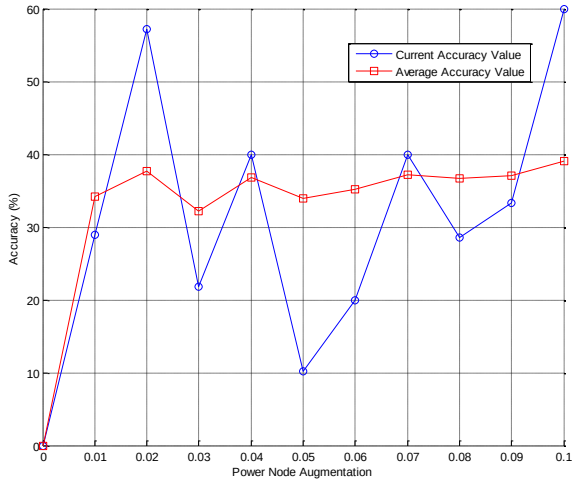

Fig. 2. Accuracy versus power node augmentation analysis for stationary peer to peer networks

Next, we calculated pathlength on the consistent pattern of accuracy for our proposed model. According to figure 3, pathlength is showing decrement for both the pathlength values namely: current and average. Current pathlength value remains maximum for 0.01 power node augmentation value and minimum for 0.07 power node augmentation value. In case of average pathlength, its value remained maximum at 0.01 power node augmentation value and minimum at 0.04 power node augmentation value. We observed that the pathlength shows non linear decline in behavior for current value and some steady behavior for its average value. We noticed that the average pathlength value show more linear behaviour in contrast with the current pathlength.

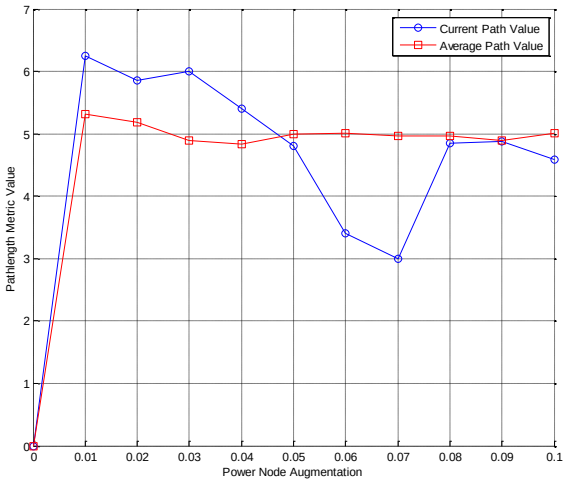

Fig. 3. Pathlength versus power node augmentation analysis for stationary peer to peer networks

B. Collusion Based Stationary Networks Evaluations

Figure 4 depicts the evaluation of accuracy over the collusion issue for apportioned stationary peer to peer networks. On the consistent pattern of our earlier analysis for stationary networks, we examined the accuracy for its current and average values.

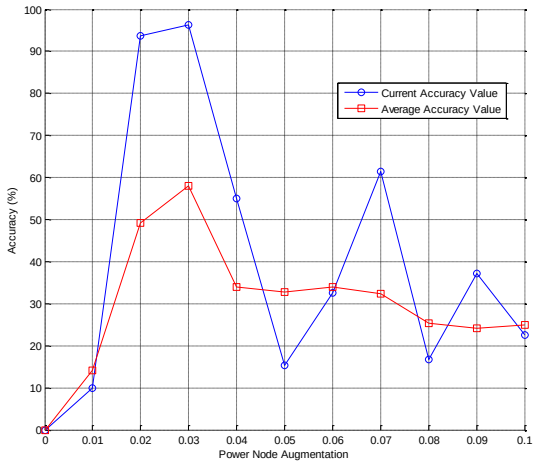

Fig. 4. Collusion based analysis for accuracy and power node augmentation factor over stationary peer to peer networks

We noticed that that the current accuracy value shows non linear behavior and remained maximum at 0.03 and minimum at 0.01 power node augmentations. In case of average accuracy, we found that the accuracy value shows some steady behaviour than the current accuracy. Its value remains maximum at 0.07 and minimum at 0.01 power node augmentation values respectively. We observed that the current accuracy shows non linear behaviour with respect to

average accuracy due to fact that current accuracy remained the resultant of last accuracy value and average accuracy describe the summation of all the networks accuracies. This shows a good agreement with the results reported in [14]. We extended the work of [14] to power node augmentation evaluation aspect. Further, we computed pathlength over the collusion issue on the consistent pattern of accuracy for our proposed model. According to figure 5, pathlength is showing non linear behavior for its current and average values.

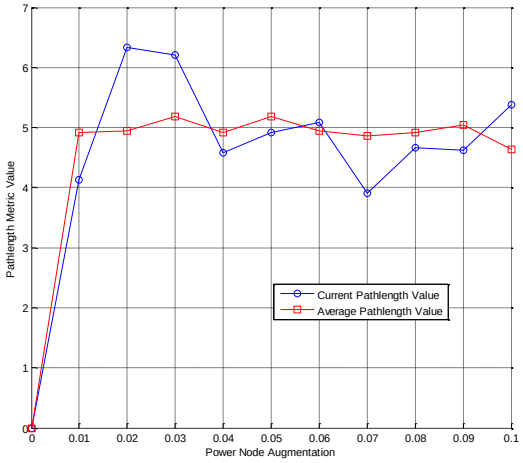

Fig. 5. Collusion based analysis for pathlength and power node augmentation factor over stationary peer to peer networks

Current pathlength value remained maximum for 0.02 power node augmentation value and minimum for 0.07 power node augmentation value. For average pathlength, its value remained maximum at 0.05 power node augmentation value and minimum at 0.1 power node augmentation value. We found that the pathlength shows some steady behavior for its average value and non linear decline in behavior for its current value. We observed that the average pathlength value show more linear behaviour in contrast with the current pathlength.

C. Mobile Peer to Peer Networks Evaluations

Next, we evaluated our model on the mobile peer to peer networks on the consistent pattern of stationary peer to peer networks. We evaluated accuracy and pathlength value for apportioned mobile networks. As per figure 6, current accuracy value remains maximum at 0.04 power node augmentation value and minimum at 0.03 power node augmentation value. Average accuracy shows its maximum value at 0.02 power node augmentation value and minimum value at 0.03 power node augmentation value. We observed that the average accuracy depict linear decline trend and current accuracy shows non linear behaviour with respect power node augmentation value.

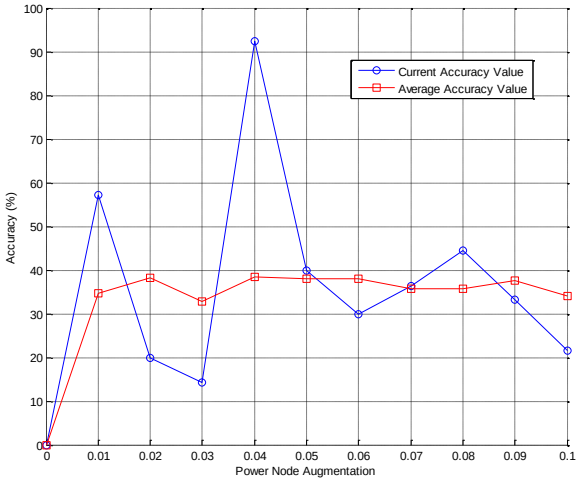

Fig. 6. Accuracy versus power node augmentation analysis for mobile peer to peer networks

Further, we evaluated pathlength value for the mobile peer to peer networks as shown in figure 7.

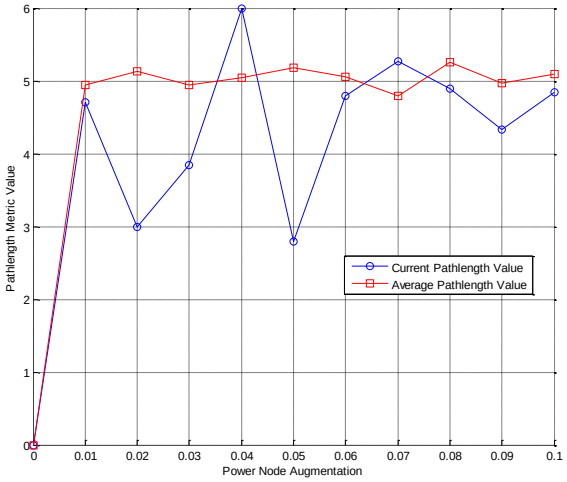

Fig. 7. Pathlength versus power node augmentation analysis for mobile peer to peer networks

We observed that the current pathlength remain maximum at 0.04 power node augmentation value and minimum at 0.02 power node augmentation value. We found that the average pathlength shows a non-linear increment in behaviour and its value remain maximum at 0.08 power node augmentation value and minimum at 0.07 power node augmentation values. We found that average pathlength reflects more steady behaviour as compared to current pathlength value.

D. Collusion Based Mobile Networks Evaluations

In this subsection, we evaluated our model over collusion issue for mobile peer to peer networks on the consistent evaluation pattern of subsection 4.3. We calculated accuracy and pathlength value over the collusion factor for apportioned networks. As per figure 8, current accuracy value remains maximum at 0.05 power node augmentation value and minimum at 0.1 power node augmentation value.

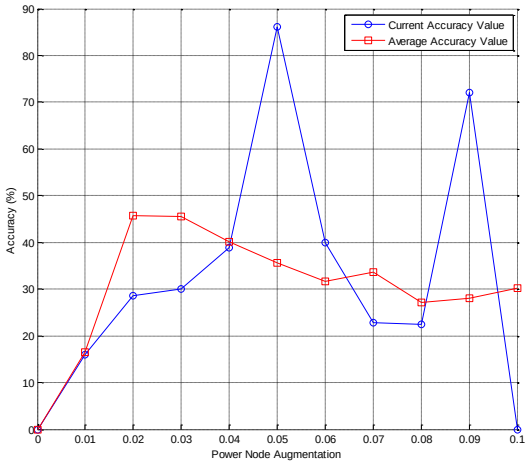

Fig. 8. Collusion based analysis for accuracy and power node augmentation factor over mobile peer to peer networks

Average accuracy shows its maximum value at 0.02 power node augmentation value and minimum value at 0.01 power node augmentation value. We observed that the average accuracy depict linear decline in behaviour with respect to current accuracy for power node augmentation value. Next, we calculated pathlength value for the collusive mobile networks as shown in figure 9. We observed that the current pathlength remain maximum at 0.07 power node augmentation value and minimum at 0.04 power node augmentation value. We noticed that the average pathlength shows a non-linear increment in behaviour and its value remain maximum at 0.09 power node augmentation value and minimum at 0.10 power node augmentation values. We found that average pathlength reflects more steady behaviour than current pathlength value.

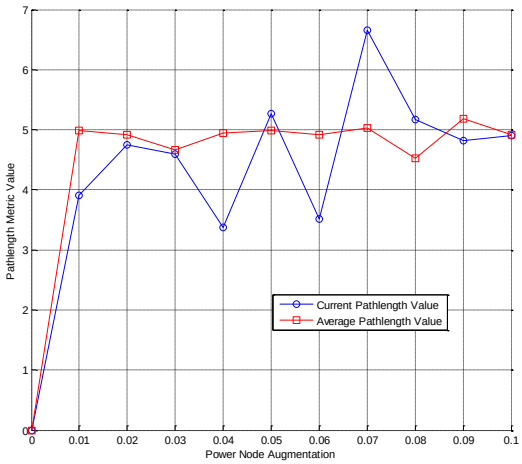

Fig. 9. Collusion based analysis for pathlength and power node augmentation factor over mobile peer to peer networks

E. Energy Consumption Analysis for Stationary and Mobile Networks along with Collusion

Further, we calculated the energy consumed by stationary and mobile peer to peer networks as shown in figure 10. In case of stationary peer to peer networks, we observed that the energy consumption shows non linear behaviour.

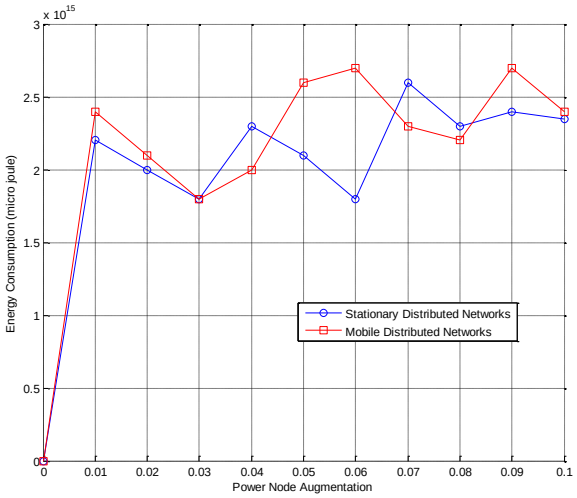

Fig. 10. Energy consumption analysis for stationary and mobile peer to peer networks.

We found that energy consumption remained maximum at 0.07 power node augmentation value and minimum at 0.03 power node augmentation value correspond to stationary peer to peer networks. In case of mobile peer to peer networks, we noticed that the energy consumption also exhibits non-linear behaviour. We observed that energy consumption remained maximum at 0.09 power node augmentation value and minimum at 0.03 power node augmentation value correspond to mobile peer to peer networks.

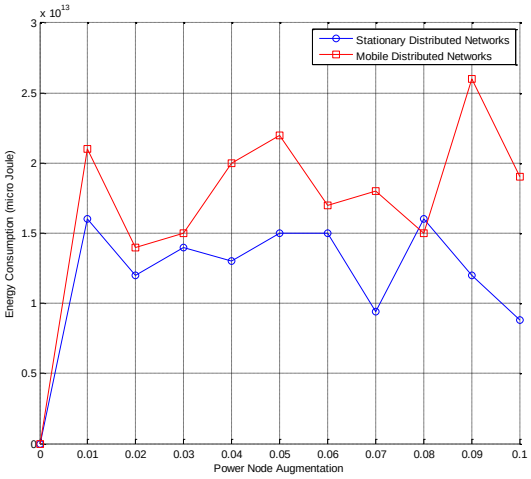

Fig. 11. Collusion based energy consumption analysis for stationary and mobile peer to peer networks

Lastly, we evaluetd the energy consumed over the collusion issue by stationary and mobile peer to peer networks as depicted by figure 11. For stationary peer to peer networks, we observed that the energy consumption shows non linear behaviour. We found that energy consumption remained maximum at 0.08 power node augmentation value and minimum at 0.1 power node augmentation value correspond to stationary peer to peer networks. In case of mobile peer to peer networks, we noticed that the energy consumption also exhibits non-linear behaviour. We observed that energy consumption

remained maximum at 0.09 power node augmentation value and minimum at 0.02 power node augmentation value correspond to mobile peer to peer networks. Zhou et al. [16] presented a power trust and reputation model for a robust and scalable reputation system towards trusted peer-to-peer computing. We extended the work of [16] for rigorous evaluation of power trust and reputation model. Verma et al. [14] made a comprehensive evaluation of trust and reputation models over malicious server based aspect for apportioned wireless sensor networks. We incorporated this work towards power trust and reputation model over stationary and mobile peer to peer networks.

F. Comprehensive Investigations

In this subsection, table 2 - table 5 represents overall experimetal summarization for apportioned stationary, mobile and collusive peer to peer networks. In all the tables, *CV* denotes current value and *AV* shows average value for accuracy and pathlength parameters respectively. Table 2 represents investigational analysis of stationary peer to peer networks. Energy consumption remained maximum at power node augmentation value 0.07 and minimum at 0.03 and 0.06 repectively.

Table 2. Stationary Peer to Peer Networks

Power Node Augmentation	**Accuracy %**		**Pathlength**		**Energy Consumption**
	CV	*AV*	*CV*	*AV*	
0.01	28.9	34.2	6.25	5.31	2.2×10^{15} μJ
0.02	57.1	37.6	5.85	5.18	2.0×10^{15} μJ
0.03	21.8	32.2	6.00	4.89	1.8×10^{15} μJ
0.04	40.0	36.8	5.40	4.84	2.3×10^{15} μJ
0.05	10.2	34.0	4.80	5.00	2.1×10^{15} μJ
0.06	20.0	35.2	3.40	5.01	1.8×10^{15} μJ
0.07	40.0	37.1	3.00	4.96	2.6×10^{15} μJ
0.08	28.5	36.6	4.85	2.30	2.3×10^{15} μJ
0.09	33.3	37.1	4.97	3.40	2.4×10^{15} μJ
0.10	60.0	39.0	2.30	2.40	2.41×10^{15} μJ

Table 3 depicts the evaluation analysis of mobile peer to peer networks. We observed that energy consumption remained maximum at power node augmentaion value 0.06 and 0.09 respectively and minimum at 0.03 power node augmentation value.

Table 3. Mobile Peer to Peer Networks

Power Node Augmentation	**Accuracy %**		**Pathlength**		**Energy Consumption**
	CV	AV	CV	AV	
0.01	57.1	34.7	4.71	4.94	2.4×10^{15} μJ
0.02	20.0	38.3	3.00	5.13	2.1×10^{15} μJ
0.03	14.2	32.8	3.85	4.95	1.8×10^{15} μJ
0.04	92.4	38.5	6.00	5.04	2.0×10^{15} μJ
0.05	40.0	38.1	2.80	5.18	2.6×10^{15} μJ
0.06	30.0	37.9	4.80	5.06	2.7×10^{15} μJ
0.07	36.3	35.6	5.27	4.79	2.3×10^{15} μJ
0.08	44.4	35.8	4.89	5.26	2.2×10^{15} μJ
0.09	33.3	37.5	4.33	4.97	2.7×10^{15} μJ
0.10	21.0	33.9	4.85	5.09	2.4×10^{15} μJ

Table 4 and table 5 shows collusion based investigations for apportioned stationary and mobile peer to peer networks. We noticed that energy consumption remained higher when incresing the power augmentation factor. Even more in presence of collusion as reflected by table 5. Its value remained maximum at two values 0.07 and 0.1 respectively than the stationary networks without collusion as shown in table 3 and table 5 respectively. As far as apportioned mobile networks are concened, the consequece remained on the similar pattern. In case of apportined mobile networks, we obseved more enrgy consumption for all the power node augmentation values. This depicts that collusion prevail over more for apporioned mobile peer to peer networks than the stationary peer to peer networks. The collusion presence in both the type of newtorks shows progressive energy consumption as can be obseved from our investigations.

Table 4. Collusive Stationary Networks Evaluation

Power Node Augmentation	**Accuracy %**		**Pathlength**		**Energy Consumption**
	CV	AV	CV	AV	
0.01	10.0	14.1	4.13	4.92	1.6×10^{15} μJ
0.02	93.7	49.1	6.33	4.94	1.2×10^{15} μJ
0.03	96.2	58.0	6.21	5.19	1.4×10^{15} μJ
0.04	55.0	33.9	4.58	4.92	1.3×10^{15} μJ
0.05	15.3	32.8	4.92	5.19	1.5×10^{15} μJ
0.06	32.5	34.0	5.09	4.95	1.5×10^{15} μJ
0.07	61.4	32.4	3.91	4.86	9.4×10^{12} μJ
0.08	16.6	25.3	4.66	4.92	1.6×10^{15} μJ
0.09	37.1	24.0	4.62	5.05	1.2×10^{15} μJ
0.10	22.5	25.0	5.38	4.63	8.8×10^{12} μJ

Table 5. Collusive Mobile Networks Evaluation

Power Node Augmentation	**Accuracy %**		**Pathlength**		**Energy Consumption**
	CV	*AV*	*CV*	*AV*	
0.01	16.0	16.4	3.90	4.98	2.1×10^{13} μJ
0.02	28.5	45.7	4.75	4.91	1.4×10^{13} μJ
0.03	30.0	45.5	4.59	4.67	1.5×10^{13} μJ
0.04	38.8	40.0	3.37	4.95	2.0×10^{13} μJ
0.05	86.7	35.6	5.27	4.98	2.2×10^{13} μJ
0.06	40.0	31.7	3.52	4.91	1.7×10^{13} μJ
0.07	22.8	38.5	6.65	5.03	1.8×10^{13} μJ
0.08	22.5	27.0	5.17	4.53	1.5×10^{13} μJ
0.09	72.0	28.1	4.82	5.19	2.9×10^{13} μJ
0.10	0.0	30.3	4.90	4.92	1.9×10^{13} μJ

One common thing, we have observed that collusion affects the performance of apportioned mobile networks based on accuracy, resource utilization and energy consumption viewpoints. In presence of collusive networks, the value of accuracy remained low, and more resource utilization as observed from our evaluation. As far as energy consumption is concerned, collusion also consumes high energy in our designated scenario.

V. Conclusions

This paper made an inclusive exploration of power trust and reputation model over apportioned stationary and mobile networks. We focused on power node augmentation aspect throughout our investigations. Additionally, we added collusion based investigations in our proposed model. We found that average accuracy depicts steady behavior as compare to current accuracy in both the stationary and mobile peer to peer networks. In presence of collusion, current accuracy reflects highly non linear decrement in behaviour than the average accuracy. As far as the pathlength factor is concerned, it works on the consistent pattern of accuracy in terms of its average and current value. Pathlength shows more linear behaviour in the average pathlength case than that of current pathlength case. We noticed that pathlength reflect incremental behaviour in mobile peer to peer networks and

declines in behaviour for stationary peer to peer networks. Also in presence of collusion, current pathlength shows significant decline in behaviour as compared to average pathlength. This reflects that collusion prevents the use of our proposed model resources up to optimal extent. This remained true in case of accuracy domain too. We observed that the energy consumption remain higher in apportioned mobile peer to peer networks than the stationary peer to peer networks for power trust and reputation model evaluation. In domain of energy consumption, collusion affects overall system severely for both the stationary and mobile networks. The investigations shows better results for power trust and reputation model over mobile networks than stationary networks which also remained true in presence of collusion too. This makes power trust and reputation model more robust for mobile peer to peer networks. Overall, we observed that presence of collusion added more uncertainty in the apportioned networks system which results in severe performance degradation. In future, we will work for the incorporation and enhancement of trust and reputation models in apportioned wireless networks applications.

REFERENCES

[1] M. Ripeanu, I. Foster, and A. Iamnitchi, "Mapping the Gnutella Network: Properties of Large-Scale P2P Systems and Implications for System Design," IEEE Internet Computing, vol. 6, no. 1, 2002.

[2] S. Saroiu, K.P. Gummadi, R.J. Dunn, S.D. Gribble, and H.M. Levy, "An Analysis of Internet Content Delivery Systems," Proc. Fifth Symp. Operating Systems Design and Implementation, Dec. 2002.

[3] Tajeddine A, Kayssi A, Chehab A, Artail H. PATROL-F –a comprehensive reputation-based trust model with fuzzy subsystems. In: Autonomic and trusted computing, Third international conference, ATC. LNCS, vol. 4158. Wuhan,China: Springer; 2006. p. 205–17.

[4] Wang Y, Cahill V, Gray E, Harris C, Liao L. Bayesian network based trust management. In: Autonomic and trusted computing, Third international conference, ATC. LNCS, vol. 4158. Wuhan, China: Springer; 2006. p. 246–57.

[5] Go´mez Ma´rmol F, Martı´nez Pe´ rez, 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.

[6] Almena´ rez F, Marı´n A, Campo C, Garcı´a C. PTM: a pervasive trust management model for dynamic open environments. In: Privacy and trust. First workshop on pervasive security and trust, Boston, USA; Aug 2004.

[7] Moloney M, Weber S, A context-aware trust-based security system for ad hoc networks. In: Workshop of the 1st international conference on security and privacy for emerging areas in communication networks, Athens, Greece; Sep 2005.

[8] Boukerche A, Xu L, El-Khatib K. Trust-based security for wireless ad hoc and sensor networks. Computer Communications 2007;30(11–12):2413–27.

[9] Sabater J, Sierra C. REGRET: reputation in gregarious societies. In: Mu¨ ller JP, Andre E, Sen S, Frasson C, editors. Proceedings of the fifth international conference on autonomous agents. Montreal, Canada: ACM Press; 2001. p. 194–5.

[10] Josang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision. Decision Support Systems 2007; 43(2):618–44.

[11] Sabater J, Sierra C. Review on computational trust and reputation models. Artificial Intelligence Review 2005; 24(1):33–60.

[12] Fe´lix Go´mez Ma´rmol*, Gregorio Martı´nez Pe´rez. Security threats scenarios in trust and reputation models for distributed systems. Computers & security 28:545 – 556. 2009.

[13] Vinod Kumar Verma, Surinder Singh, and N.P. Pathak, Collusion Based Realization of Trust and Reputation Models in Extreme Fraudulent Environment over Static and Dynamic Wireless Sensor Networks. International Journal of Distributed Sensor Networks, Volume 2014, Article ID 672968. 2014.

[14] Vinod Kumar Verma, Surinder Singh and N.P. Pathak. Impact of Malicious Servers over Trust and Reputation Models in Wireless Sensor Networks, International Journal of Electronics, Taylor & Francis Publications. 2015. pp. 1-13.

[15] Singh, S.; Verma, Vinod Kumar ; Pathak, N.P. " Sensors Augmentation Influence over Trust and Reputation Models Realization for Dense Wireless Sensor Networks" Sensors Journal, IEEE, Year:2015,Volume:15, Issue: 11,Pages: 6248-6254,DOI: 10.1109 /JSEN .2015.2448642.

[16] Zhou R, Hwang K. PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing. Transactions on Parallel and Distributed Systems 2007.

[17] 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. 2009.

[18] Vinod Kumar Verma. Simulative Exploration of Power Trust and Reputation Model over Power Node Augmentation Factor in Distributed Peer to Peer Networks, WSEAS 18 th International Conference on Automatic Control, Modelling & Simulation (ACMOS '16) Venice, Italy. 29-31 January 2016.

Vinod Kumar Verma born in Kalka (Haryana), India. Dr. Verma holds Ph.D. degree in Computer Science and Engineering, M.S degree in Software Systems and B.Tech. degree in Computer Engineering. He is currently working as Assistant Professor in the Department of Computer Science and Engineering at Sant Longowal Institute of Engineering and Technology, Longowal. Deemed University, Punjab, India. Dr. Verma has published many research papers in International Journals of IEEE, Springer, Elsevier ScienceDirect, Taylor and Francis. Dr. Verma is serving as Editorial Board Member / Reviewer of Many International Journals. His fields of interests are wireless sensor networks, trust and reputation systems, distributed computing, cryptography and software systems.