Asia Pacific Journal of Contemporary Education and Communication Technology
ISBN (eBook): 978 0 9943656 8 2 | ISSN : 2205-6181
Year: 2018 , Volume: 4, Issue: 1

INFORMATION BASED MUTABLE TRUST COMMUNICATION SCHEME FOR HETEROGENEOUS WIRELESS NETWORKS

Vinod Kumar Verma
Sant Longowal Institute of Engineering and Technology, Longowal, India
Email: vinod5881@gmail.com

Abstract

Accuracy is the prime concern for any real time distributed system application which varies from simple home applications to complex military surveillance systems. The concept of trust and reputation was the dream for the conventional distributed applications some years ago. This paper addressed the past research effort in the direction of infrastructure based routing protocol. Moreover, the focus is on the evaluations of accuracy over the trust, hops and non trust based factors. We designed and implemented a model for the comprehensive investigations over the trust issue. Infrastructure has also been given greater importance in the deployed model. The outcomes obtained from these investigations can help the real time distribution applications direly. The proposed scenario has been validated through simulation means.

Keywords: Region, Energy, Mobile, Distributed Networks.

1.Introduction

Trust is a major area of concern for all the distributed system applications used on the daily basis. This becomes more contemporary in the field of homogeneous wireless sensor networks which are serving as the backbone for the majority of distributed system applications. In order to incorporate more trustworthiness in real time application, there always remains a need to work in this direction. An infrastructure based routing protocol has been assessed from a deeper horizon. A trust based routing protocol for the nodes in the networks have been proposed in this paper. The goal is to investigate and enhance the existing work in the field of trust and reputation models. We focused on the self trustworthiness, other recommended trustworthiness and query for hops for the heterogeneous wireless network. The structure of this paper covers the following sections. Section 2 presented the related work in trust based heterogeneous wireless networks. Section 3 illustrated the variable trust based infrastructure scheme. Section 4 describes the through setup. Section 5 reported the results and discussion of the designated model. Finally, conclusions are drawn in Section 6.

2. Related Work in Trust Based Heterogeneous Wireless Networks

A number of efforts have been reported so far in the context of trustworthiness evaluation for heterogeneous wireless networks. The major research works presented in this direction are as follows. Boukerche, et al., (2007) highlighted a security based strategy in 2007 for the trustworthiness in ad hoc and sensor networks. Raya, et al., (2008) proposed an approach for the data centric trust computation for the ad hoc networks. Ma´rmol, et al., (2010) suggested probable

security threat conditions for the distributed system using trust and reputation models. Ma´rmol & rez, (2009) developed a trout and reputation model simulator for the wireless sensor networks. The approach of linguistic based fuzzy system for the trout computation has been suggested by the Ma´rmol, et al., (2010) for the emerging applications. An infrastructure based scheme for the trout computation for vehicular ad hoc networks was presented by authors in reference. Lung & Zhou, (2010) reported an energy-efficient and flexible approach with hierarchical agglomerative clustering in wireless sensor networks. The performance of ad hoc on demand distance routing protocol for wireless sensor networks was investigated in reference. Verma, et al., (2014) signifies the role of battery model and routing protocols for the evaluation of heterogeneous wireless networks. Authors in reference 10carried out a comprehensive event based estimation of sensor node distribution strategies using classical flooding routing protocol in wireless sensor networks. An initiative based on the bio-inspired trust and reputation model investigations hops coefficient factor for wireless sensor networks was proposed in(Verma, 2012). Sensors augmentation influence over trust and reputation models realization for dense wireless sensor networks was suggested in. Verma, et al., (2014) made a comparative evaluation of trust and reputation models over static, dynamic and oscillating wireless sensor networks. Verma & Singh, (2015) investigated pre-trusted peers probability influence on Eigen trust and reputation model over peer to peer distributed networks. Verma & Singh, (2015) made simulative explorations of power trust and reputation model over power node augmentation factor in distributed peer to peer networks. Verma, (2016) proposed pervasive investigations of trustworthiness over diverse orientations of apportioned heterogeneous mobile networks. After reviewing theses efforts from the researchers, we observe that there is need to evaluate the existing work in the direction of trust and reputation models for day to day distributed sensing applications. The proposed methodology has been presented in the next section.

3. Infrastructure Based Mutable Trust Scheme

We proposed and evaluated an infrastructure based routing protocol for distributed heterogeneous networks. In this protocol, the trust value has been assigned to all the nodes within the networks. Then, the score of the all the node from each other also computed. The score of individual node after the exchange of their services with other nodes have calculated. Further, trust levels have been assigned to each node in the self context, as well as from the others recommendation context. Three levels have been assigned to the trust domain namely: mean, standard deviation and tolerances. A trust fuzzy set has been created according to the mean, standard deviation and tolerances for the further service exchange. A node can be trustworthy if it fulfils a particular trust level otherwise it has to be rejected. There is also another level of trust in-between acceptance and rejection *i.e.* intermediate level. This level depicts the node services can be accepted but should not be forwarded to other nodes in the networks. The number of the other parameters like area, number of nodes, number of networks, relay nodes, radio range, malicious nodes, number of hops etc. has been considered on the consisted pattern of reference.

4. Detailed Setup

We used a Java based simulator TRM-WSN over the Windows platform for the deployment of the proposed model. The simulation setup of the designated model is shown in figure 4.1. The proposed model had the following constraints. The direct trust weight probability is set as 0.3 which further varied from 0.1 to 1.0 in further investigations. The indirect trust from others recommendation is set as 0.4 which also evaluated from 0.1 to 1.0 in the designated model. The relay server weight is kept as 0.3. The mean and standard deviation of the not trust level is set as 0.0 and 0.2 respectively. The simulation had the following structure. Number of networks used for evaluation remained 100 over an area of 100 m × 100 m. Minimum and maximum sensors

used were 50. The value of relay server and malicious servers remained at five and seventy percentage respectively. Trust fuzzy set mean and standard deviation were 0 and 0.2. Mean tolerance and standard deviation tolerance were 0.5 and 0.15. The value for query recommender hops varied from 1 to 10. Table 1 exhibits the parameters summarization for the deployed scheme.

Table 1: Simulation parameters

Parameters	**Value**
Number of networks	100
Minimum sensors	50
Maximum sensors	50
Relay servers (%)	5
Malicious servers	70
Radio range	12
Delay	0
Self node trust probability (%)	0 - 100
Others nodes recommended trust probability (%)	0 - 100
Area	100 m × 100 m
Trust fuzzy mean	0.0
Trust fuzzy standard deviation	0.2
Mean tolerance	0.5
Standard deviation tolerance	0.15
Query recommender hops	1 - 10
Node orientation	Heterogeneous
Number of execution	10

The simulation snapshot is shown in figure 4.1. In the snapshot, different circle shows the type of nodes in the network by the color coding where green circle shows the benevolent nodes, red circles depicts the malicious nodes and pink circle denotes the relay server units.

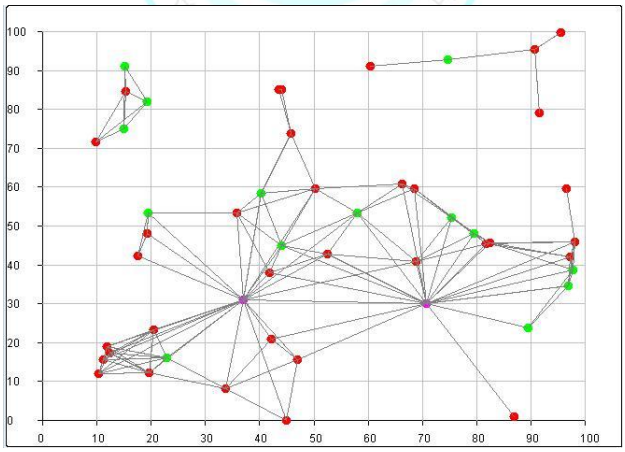

Figure 4.1: Simulation Snapshot

5. Results and Discussion

In this section, the investigations over infrastructure based protocols have been presented in heterogeneous sensor networks. The focus remained over the accuracy based explorations for the direct and indirect trust probability. Additionally, the stress has been given on the number of hops for the query recommendation by nodes in the networks. Figure 4.2 shows the accuracy

influence over the direct trust probability. The value of the direct trust probability has been varied from 0 to 1. We computed two accuracies namely current and average.

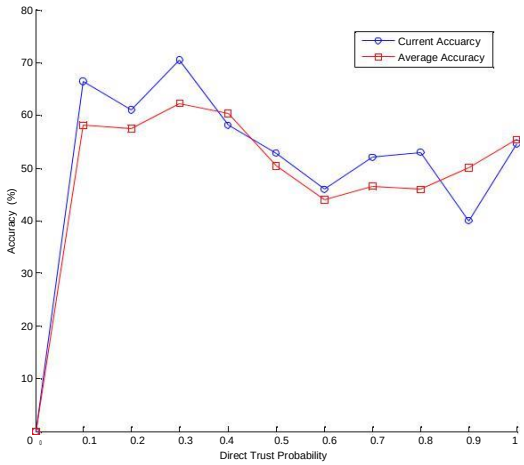

Figure 4.2: Accuracy over direct trust probability analysis

Current accuracy reflects the outcome of the last network and average accuracy shows the resultants of all the networks. We observed that the both the accuracies show decremental behaviour with respect to direct trust probability. In case of current accuracy, the accuracy vale remains maximum at 0.3 probability value and minimum at 0.9 probability value. For the average case, the accuracy value shows peak level at 0.3 and least level at 0.6 highest at probability value. Next, we examined the accuracy value over the indirect trust probability factor as depicited in figure 4.3. The investigation shows the steep decremental behaviour of the accuracies over the indirect trust probability values.

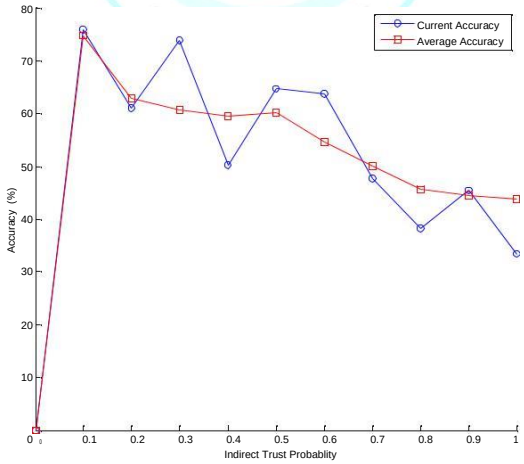

Figure 4.3: Accuracy over indirect direct trust probability analysis

The Average accuracy shows linear decemental behaviour as compared to current accuracy. This has been shown in figure 4.4.

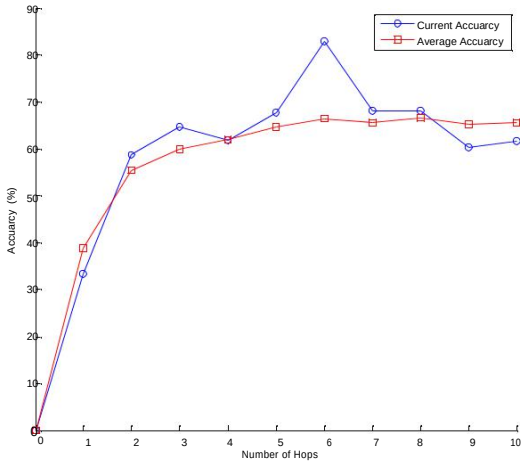

Figure 4.4: Accuracy over number of hops analysis

Both types of accuracies show a maximum value at 0.1 and minimum at 1.0. Further, we calculated the accuracy over the number of factors over the query recommended by the nodes. We analysed that both the types of accuracies shows the linear incremental behavior. The value of current accuracy occupies its maximum level at the six hop values and minimum level at one hope value. In case of average accuracy, the value remains highest at eight hope value and minimum at one hope value. The comprehensive investigations of the accuracy over the direct trust probability, indirect trust probability and number of query hops recommended is shown in figure 4.5.

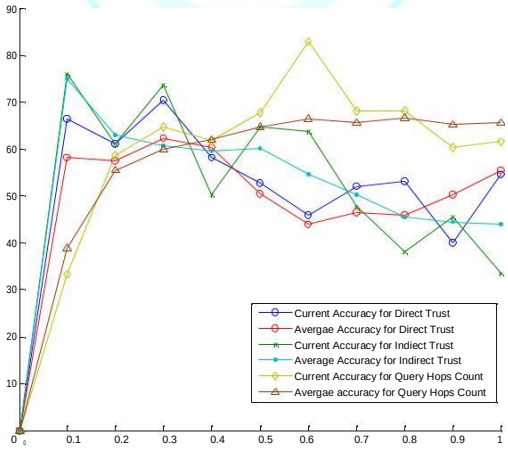

Figure 4.5: Comprehensive accuracy analysis

Conclusion

This research work remained focused over the comprehensive explorations of accuracy parameter for the heterogeneous networks. We implemented an infrastructure based routing protocol for the trustworthiness evaluation over the deployed scenario. The focused parameters of the investigations remained direct trust probability, indirect trust probability and number of query hops recommended. The conclusion reveals that accuracy is affected by the direct and indirect trust probability value in the infrastructure based routing protocol. We observed that direct trust probability shows the decline in behavior for accuracy after a certain value, indirect trust probability value depicts liner decremented behavior and number of hops value shows incremental behaviour for the accuracy parameter. The future work will focus towards development of a newer simulator for heterogeneous wireless networks.

References

i. Boukerche, A., Xu, L. & El-Khatib, K., 2007. Trust-based security for wireless ad hoc and sensor networks.. *Computer Communications,* 3(11-12), pp. 2417-2417.

ii. Lung, C. & Zhou, C., 2010. Using hierarchical agglomerative clustering in wireless sensor networks An energy-efficient and flexible approach.. *Ad Hoc Networks,* 8(3), pp. 328-344.

iii. Ma´rmol, F. G., Marı´n-Bla´zquez, J. G. & Pe´rez, G. M., 2010. *Linguistic fuzzy logic enhancement of a trust mechanism for distributed networks. In: Proceedings of the third IEEE international symposium on trust, security and privacy for emerging applications (TSP-10).* Bradford, UK, International symposium on trust, security and privacy for emerging applications (TSP-10).

iv. Ma´rmol, F. G. & rez, G. M. P., 2009. Security threats scenarios in trust and reputation models for distributed systems.. *Elsevier Computers & Security ,* 28(7), pp. 545--556.

v. Ma´rmol, F. G. & rez, G. M. P., 2009. *TRMSim-WSN trust and reputation models simulator for wireless sensor networks. In: Proceedings of the IEEE international conference on communications (IEEE ICC 2009).* Dresden, Communication and information systems security symposium.

vi. Mármol, F. G. & Pérez, G. M., 2012. TRIP, a Trust and Reputation Infrastructurebased Proposal for Vehicular Ad-hoc Networks". *Journal of Network and Computer Applications,* 33(3), pp. 934-941.

vii. Raya, M., Papadimitratos, P., Gligor, V. & Hubaux, J., 2008. *On data-centric trust establishment in ephemeral ad hoc networks.* Phoenix, AZ, Proceedings of IEEE Infocom.

viii. Singh, S., Verma, Kumar, V. & Pathak, N., 2015. Sensors Augmentation Influence Over trust and reputation models for realization for dense wireless sensor networks. *Sensors Journal, IEEE,* 15(11), pp. 6248-6254.

ix. Verma, V. K., 2012. *Performance Assessment of AODV Routing Protocol over Temperature Constraints in Wireless Sensor Network. Published in proceeding of 11th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communication (EHAC '12).* Cambridge, UK, s.n.

x. Verma, V. K., 2014. *Bio-Inspired trust and Reputation Model Investigations Hops Coefficient Factor In Wireless Sensor networks, Published in 7th International Conference on engineering and Technological Innovations IMETI- CITSA.* Orlando, Florida, IMETI-CITSA.

xi. Verma, V. K., 2016. Pervasive Investigations of Trustworthiness over Diverse Orientations of Apportioned Heterogeneous Mobile Networks.. *International Journal of Mathematics and computers in simulation,* Volume 10, pp. 281-287.

xii. Verma, V. K., 2016. *Simulative Exploration of Power Trust and Reputation Model over Power Node Augmentation Factor in Distributed Peer to Peer Networks..* Venice, Italy, International Conference on Automatic Control, Modelling & Simulation (ACMOS '16).

xiii. Verma, V. K., Singh, S. & Pathak., N., 2015. Towards comparative evaluation of trust and reputation models over static, dynamic and oscillating wireless sensor networks.. *The Journal of Mobile Communication, Computation and Information.*

xiv. Verma, V. K., Singh, S. & Pathak, N., 2014. Comprehensive Event Based Estimation of Sensor Node Distribution Strategies using Classical Flooding Routing Protocol in Wireless Sensor Networks. *The Journal of Mobile Communication, Computation and Information. ,* Volume 20, pp. 2347-2357.

xv. Verma, V. K., Singh, S. & Pathak, N., 2014. Optimized Battery Models Estimation for Static, Distance Vector and On-Demand Based Routing Protocols over 802.11 Enabled Wireless Sensor Networks, Published in Wireless Personal Communications:. *Springer Science + Business Media New York .*