International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

A Fuzzy Lattice System to Trust Management in Mobile Grid

Grantej Vinod Otari, Vijay Ram Ghorpade, Sachin Harakhchand Dhanani

Abstract : Mobile Grid is a crossbreed technology formed by amalgamation of the two prominent technologies namely mobile technology and grid technology that enable sharing and collaboration of mobile resources cooperatively, transparently, efficiently, reliably and securely. Mobile Grid considers the mobility issues and overcomes the constraints and deficiencies in both the technologies. However, this heterogeneous, dynamic and open mobile grid network is more prone to malicious and selfish nodes inside and outside the network. Hence, a vigorous security mechanism is needed that considers different security threats and pro-vide different levels of security services. Here, we propose one such preventive security service based on Trust Management. The proposed trust management service uses a novel fuzzy lattice approach for trust estimation of the nodes in the network. A node with high trust value is allowed to participate in the network. A malicious node having low trust value is prevented from performing the task. A fuzzy lattice approach can compute incrementally the same intervals in the training data independent of the order of presentation within a short period. Experimental analysis of the fuzzy lattice approach shows that the proposed approach outperforms most of the existing approaches based on fuzzy logic.

Keywords: Mobile Gird, Trust Management, Fuzzy Lattice

I. INTRODUCTION

In order to meet the fluctuating and on-demand resources requirements one of the most promising technology has been in the forefront in the form of Grid Computing. Grid computing allows to share and allocate heterogeneous and distributed resources dynamically. This results in an open and dynamic environment providing computational and storage resources in the form of grid services. The grid service providers need to ensure a secure grid environment to the users of the remote resources for executing their tasks remotely and storing the data on the remote storage resources securely.

With the exponential growth of wireless electronic devices such as smart phones, PDA, laptops etc. along with the high speed internet many recent advents have been done by the researchers and industry to enrich the new comping paradigm of mobile computing. Mobile computing allows collaboration of mobile devices having limited resources such as battery, processor, input/output interfaces and instability in data transfer to solve a common problem. Providing security of such limited and precious resources in mobile devices which are being shared in a highly dynamic, open and heterogeneous environment is a challenging problem.

The Mobile Grid [1] is a crossbreed technology incorporating grid of mobile devices thus addressing mobility issues and providing mobility to the resources and users in a continuous, transparent, secure and effective manner. This allows us to form a self-organized grid system consisting of an underlying ad-hoc network of mobile devices interconnected by wireless network and constructing random and dynamic network topology. Thus the security infrastructure in the mobile grid system should deal with various aspects of security issues both in grid computing and mobile computing.

In the mobile grid network, every node plays the dual role as client and server. Thus mobile grid resources are exposed to distributed and open dynamic environment. However, such mobile grid networks are extremely prone to malicious participants dispersing false contents causing unrecoverable security threat to the system. A viable solution is to develop a trust model which provides a mechanism to establish a trusted relationship between the participating resources and allowing them to share the task and data les securely collaboratively. In the trust model, every peer assesses every other peer in the network after each trans-action. Then a peer selects the trustworthy peer for further transaction based upon its past transaction experiences.

Evaluating trustworthiness of a peer in the mobile grid is a complex problem as trust is a linguistically fuzzy concept. To solve this complex problem of trust calculation fuzzy logic is a good alternative solution. Also it has been observed that all the peers in the network are not always cooperative and may send false feedback to disrupt the reputation of the peers and contribute to the errors in global trust calculation. Thus a robust trust estimation model is needed that detects malicious peers and check the credibility of the recommendations received from such peers. In addition the trust model should also deal with the estimation of trust of the newly joined node in the network.

In this paper, we have designed a novel trust management system based on a fuzzy lattice approach. The proposed model uses multiple attributes of the mobile node to evaluate the direct trust value. These input attributes indicate the capability of the node to perform the specific task based on the currently available resources and its previous performance. The trust model then estimates indirect trust by collecting the recommendations from the neighbors in the network and considering the credibility of the recommenders. Finally, the obtained direct trust value and indirect trust value is aggregated to compute the global trust of a node.

Manuscript published on 30 August 2019.
***Correspondence Author(s)
Grantej Vinod Otari, Department of Computer Science & Engineering Shivaji University Kolhapur, India
Dr. Vijay Ram Ghorpade, Department of Computer Science & Engineering Bharati Vidyapeeth's College of Engineering Kolhapur, India
Dr. Sachin Harakhchand Dhanani, Department of Mathematics K.I.T.'s College of Engineering, Kolhapur, India

II. RELATED WORK

There exists a vast and diverse literature for development of trust model. Numerous possible approaches and measures are used for trust calculation. Some approaches use continuous values to measure the trust, while some methods use discrete values. Some models are based on probabilistic approach whereas some others use threshold based approach. However, most of the trust models use fuzzy logic approach. However most of the trust models consider fuzzy logic as most suitable approach. In fuzzy logic approach, the range of possible trust values is signed the adjectives as shown in Figure 1.

In Figure 1 a node which has 1.0 trust is assumed to have 25% very low trust and 75% low trust.

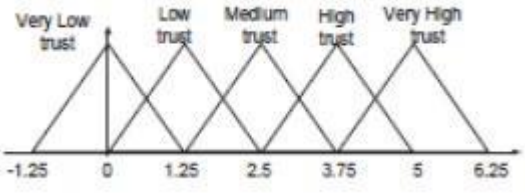

Figure 1. Fuzzy logic based trust

Qiyi Han et al. [2] proposed HFSTrust a hierarchical fuzzy which calculates the local trust metric by retrieving information about past interactions from local logs. Also in this model the information about the experience of the other peers in the network is collected to obtain the recommendation trust metric. Finally, global trust metric is formed by accumulation of local trust and recommendation trust. The trust model proposed for P2P e-commerce transactions FuzzyTrust [3], is based on the fact that trust is imprecise and uncertain. Here local trust value is calculated using fuzzy logic inference rule that can handle imprecise linguistic terms effectively. The proposed system disseminates the reputation information among the peers securely and at high speed using distributed-hash-table(DHT) overlay network. A fuzzy logic based trust model proposed by Chen et al. [4] handles fuzziness, imprecision and uncertainty effectively. It evaluates trust using various factors like capability of peer, QoS of a peer and trustworthiness of the recommender. A multifactor hierarchical fuzzy trust model MHFTrust [5] uses four capability factors, two decision factors and one security factor to evaluate the local trust. The proposed hierarchical model reduces the number of fuzzy rules involved, where the input variables are put into a set of low-dimensional fuzzy logic units instead of a single high-dimensional system. Also the model uses weight and credibility of the recommender to evaluate the global trust. In order to manage Community Of Interest (COI) mobile groups dynamically a dynamic hierarchical trust management protocol COI-HiTrust [6][7] is designed that is accurate and resistant against a malicious node who is inside the group and attacks to harm the system. In order to accomplish a mission a COI is divided into groups based on the type of subtask. Each COI member then evaluates the trust of only the peers in the same group using COI-HiTrust model. Also every Subtask Group Leader (SGL) estimates the trust of other SGLs in the group. An SGL evaluates the trust of all the COI members in its group by aggregating the trust information from all the COI members about each COI member in the same subtask group. Each SGL in the COI group then sends the trust evaluation results for all other SGLs to the commander. The commander aggregates the received results to calculate the final trust of each SGL in the same COI group. A subjective trust management model [8] is based on analytic hierarchy process (AHP) theory AFSTrust [9] which combines qualitative and quantitative factors. The proposed model uses fuzzy logic rule prediction method. Here multiple decision factors are considered along with direct and recommendation trust, incentive function and active degree to reflect the complexity of the trust relationships and overcome the problem of incomplete decision factors unlike traditional methods. The use of AHP theory enables to build weights of decision factors. This makes the model more robust and practicable.

A trust model based on the concept of how humans trust each other is proposed by Pedro B. Velloso et al.[10] and Lei Chen et al. [11] and is applied for ad hoc networks. Here the node is assumed to interact only with its neighbors, thereby requiring to store trust value of only its neighbors or nodes within the radio range. The evaluation of trust is based on individuals past experiences and the recommendations received from other nodes in the network. The key concept used in the model is relation-ship maturity as in case of human relations trust goes on increasing with time. The relationship maturity concept associates time factor to measure the weight of the recommender. Since each node is required to store trust information of only its neighbors, the proposed model is highly scalable and requires less communication and energy for disseminating trust information. A new trust management framework (TMF) for mobile ad-hoc networks based on Grey theory and Fuzzy sets is proposed by JiGuo et al. [12][13] that evaluates the nodes trust value using the past observations of the neighbor nodes and uses multiple input parameters such as packet loss, delay, signal strength, throughput, data rate etc. The model considers the weights of neighbor nodes and relation factors to calculate the total trust value of a node. For this the model uses weight vector groups for input parameters. TMF detects selfish or malicious behaviour of a node along with the particular parameter which contributes the attack made by the selfish attacker.

M-trust proposed by BasitQureshi et al., [14][15][16] is a trust rating aggregation algorithm for mobile P2P network that uses trust ratings based on direct and witness interactions. The algorithm computes the confidence [0; 1] of a node based on the number of positive and negative interactions with it. If the con defence value of the node is less than the threshold the node is less trustworthy and vice versa. Each node then aggregates the trust value from the peers and prepares the list of trust values t_list. After the aggregation process is completed the algorithm uses trust con defence to implement the weighted average function for witness recommendations. Zhexiong Wei et al.[17] proposed a trust management scheme for MANETs using the concept of uncertain reasoning from artificial intelligence system.The proposed model estimates the total trust using two phases: direct trust estimation and indirect trust estimation. Direct trust is evaluated using the direct observations done by the observer node and uses Baysian inference model which is a kind of uncertain reasoning. Indirect trust is estimated using the second hand information given by the neighbor nodes of an observer node and uses Dumpster-Shafter theory, which is also a type of uncertain reasoning.

III. FUZZY LATTICE TRUST MODEL

3.1. Attributes for Trust Evaluation

Trust is a non-concrete idea, which joins many convoluted elements or attributes. For the development of collaborative and secure point to point sharing environment, it is necessary that the resource provider node provides resources to the requester node for performing its job or a task in a secure manner. Hence a trusted relationship is required between the resource provider and resource requester. The attributes used for evaluating the trust of a node in a mobile grid network are shown in Table 1.

Table 1. Attributes for Trust Estimation

Attributes	Description
CPU	Mobile node Processor available
Battery	Mobile Battery available
Storage	Mobile Storage space available
Bandwidth	Bandwidth available for uploading and downloading data
Operating System	Type of OS(iOS, Android etc.) in case task requires OS compatability
Job Success rate	Number of successfully completed jobs
Online Time rate	Rate at which node is available in the network
Task completion time	Average time taken to complete a task

3.2. Fuzzy Lattice Approach

Fuzzy logic used in the Trust model involves a rule-based system. Fuzzy rules describe the nature of the inference system that uses semantic terms associated with the input and output variables. The rule reforms the expert knowledge in form collection of IF X THEN Y rules. If the constraints between the objects used for classification are loose, the rule based fuzzy systems are inefficient. The rule based fuzzy system allows to add multi-sequential data only ate the cost of increased computational time. The rule based fuzzy systems are based on knowledge of the experts. Insufficient knowledge about the classification target does not allow the system to apply the explicit rule definition. Also with the increase in the number of input variables, the chances of trying each possible combination of inputs decrease.

On the other hand, a fuzzy lattice approach can compute incrementally the same intervals in the training data independent of the order of presentation and within a short span of time. Moreover, this approach can justify its answer by extracting rules in the data. Hence it can be useful for data mining and rule extraction involving disparate types of data. Further work on this approach may include the study of techniques both in order to improve performance and to reduce the number of rules.

3.3. Direct Trust calculation

Each peer maintains a record of trust factors whenever it interacts with all other peers in the network. The proposed model uses fuzzy lattice approach to analyse the trust factors. The trust management system uses agglomerative approach as shown in Figure 2.

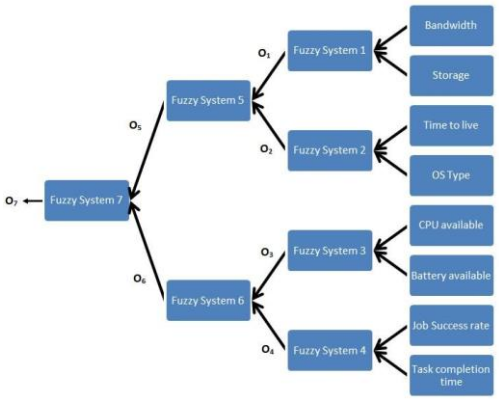

Figure 2. Agglomerative trust management system

In the above fuzzy system, the attributes shown in Table 1 are used as input fuzzy variables. The output fuzzy set indicates the trust satisfaction at five levels (Very high trust, High trust, Medium trust, Low trust and Very low trust). The fuzzy system uses the input trapezoidal membership function (X) for trust satisfaction. The function (x) denote the output trapezoidal membership function.

The output fuzzy variable denoting the direct trust metric is obtained by the system by integrating the eight trust attributes. Also the system has six intermediary fuzzy variables (O1 to O6) and one output fuzzy (O7) variable.Pairwise peers are related, and the optimal path is selected.

3.3.1. Fuzzy lattice approach for trust computation

In the above agglomerative trust management system, the fuzzy system at each level uses the rule base shown below for processing the respective input fuzzy variables.

Fuzzy System 1:

$$O_1 = \bigvee_{k=1}^{5} \{ \max \{ \min \{ 1 - \mu_k^{n1}(X_1), 1 - \mu_k^{n1}(X_2) \}, \min \{ 1 - \mu_k^{n2}(X_1), 1 - \mu_k^{n2}(X_2) \}, ß'_k(x) \} \}$$

where $ß'_k(x) = \min \{ ß'_k(x_1), ß'_k(x_2) \}$. (1)

Fuzzy System 2:

$$O_2 = \bigvee_{k=1}^{5} \{ \max \{ \min \{ 1 - \mu_k^{n3}(X_3), 1 - \mu_k^{n3}(X_4) \}, \min \{ 1 - \mu_k^{n4}(X_3), 1 - \mu_k^{n4}(X_4) \}, ß''_k(x) \} \}$$

where $ß''_k(x) = \min \{ ß''_k(x_3), ß''_k(x_4) \}$. (2)

Fuzzy System 3:

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$O_3 = \bigvee_{k=1}^{5} \{ \max \{ \min \{ 1 - \mu_k^{n5}(X_5), 1 - \mu_k^{n5}(x_6) \},$

$\min \{ 1 - \mu_k^{n6}(x_5), 1 - \mu_k^{n6}(X_6) \}, ß'''_k(x) \} \}$

where $ß'''_k(x) = \min \{ ß''_k(x_5), ß''_k(x_6) \}$. (3)

Fuzzy System 4:

$O_4 = \bigvee_{k=1}^{5} \{ \max \{ 1 - O_1, 1 - O_2, ß^{IV}_k(x) \} \}$

where $ß^{IV}_k(x) = \min \{ ß^{IV}_k(x_7), ß^{IV}_k(x_8) \}$ (4)

Fuzzy System 5:

$O_5 = \bigvee_{k=1}^{5} \{ \max \{ 1 - O_3, \min \{ 1 - \mu_k^{n7}(x_9), 1 - \mu_k^{n7}(x_{10}) \}, ß^{V}_k(x) \} \}$

where $ß^{V}_k(x) = \min \{ O_3, ß^{IV}_k(x_{10}) \}$ (5)

Fuzzy System 6:

$O_6 = \bigvee_{k=1}^{5} \{ \max \{ 1 - O_4, 1 - O_5, ß^{VI}_k(x) \} \}$

Where $ß^{VI}_k(x) = \bigvee_{i=1}^{5} \bigvee_{j=1}^{5} \{ ß^{IV}_i(x) . ß^{V}_j(x) \}$ (6)

Fuzzy System 7:

$$DT = O7 = \frac{\sum_{i=1}^{n} \sum_{i=1}^{k} \sum_{j=1}^{k} \beta_i^j(X_j) \cdot O_5 \cdot O_6}{\sum_{i=1}^{k} \sum_{j=1}^{k} O_5 \cdot O_6}$$

(7)

3.4. Recommendation Trust calculation

Resources in mobile grid network are limited in nature due to which in order to save the energy or any other selfish reason nodes may be reluctant to cooperate in the network. Also, the communication between the participating nodes is for short duration.

We propose a general recommendation based trust framework for evaluating the indirect trust value of non-neighboring nodes based on the approach used by social networks like Facebook, twitter etc. and the principle of psychology. The nodes in the network decide whom to trust based on the recommendation received from the common friend in the network.

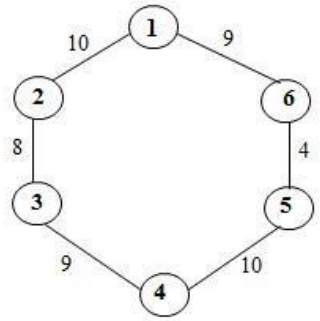

Figure 3. Recommendation Trust Estimation

Consider the scenario in Figure 3. Node 1 wishes to evaluate the trust value of a non-neighboring node 4. Nodes 3 and 5 which are direct neighbors of node 4 evaluate the direct trust values $DT_{3,4}$ and $DT_{5,4}$ respectively. These values are then forwarded by nodes 3 and 5 to nodes 2 and 6 respectively in the form of recommendations. Nodes 2 and 6 evaluate their own recommendation trust values $RT_{2,4}$ and $RT_{6,4}$ respectively using equation 1. Nodes 2 and 6 now forward the calculated values to node 1 which then computes its own recommendation trust for node 4.

$$RT_{i,j} = \frac{\sum_{k=1}^{n} DT_{i,k} * RT_{k,j}}{\sum_{k=1}^{n} DT_{i,k}} \quad (8)$$

When the trusted relationship is established between the trustor and the trustee using the recommendations received from the recommender nodes, the trust value between the trustor and the trustee should not exceed the trust value between recommender and the trustee.

3.5. Global Trust calculation

Finally, global trust value GT is evaluated by aggregation of direct trust DT and recommendation trust RT using the following equation.

$$GT = \omega * DT + (1 - \omega) * RT \quad (9)$$

Where ω is a weighting factor ranging between 0 and 1.

IV. EXPERIMENTATION AND RESULTS

This section summarizes the experimentation's done and the results observed. We have created a scenario of mobile grid system using pervasively available android smartphones connected with Wi-Fi. To assign the tasks to the mobile nodes in the grid we have considered the application of mobile healthcare (m-Healthcare) [18] . Mobile Healthcare application requires sharing of resources and data by the hospitals and patients thereby comprising of interaction between different smartphones and technologies, PDAs, digital medical equipment's and physiological sensors to measure patients signal. This helps the hospitals and doctors to monitor the status of the remote patient and provide the medical facility in case of emergency as well as to send reminders to patients about necessary medication or examinations. We have used the ECG data of up to 500 patients for processing. ECG data contains the cardiological signals that show the electrical activity. From the ECG data we can measure the heart rate of a patient and analyse if the patient requires immediate.

The node which needs to submit the task of processing the ECG data searches for the other nodes in the grid to perform the parallel task. It then evaluates the trust index of all the nodes in the grid based on the initial attribute values and selects the most trusted nodes based on task requirements. Once the task is successfully complete the node then recalculates the trust index of all the nodes in the grid and considers the most trustworthy nodes for the further task.

To analyse the performance of our proposed system we considered five different scenarios of mobile grid network consisting of 10, 20, 30, 40 and 50 mobile nodes respectively consisting of smartphones of different make like Samsung Galaxy On7 Pro, XiaomiRedmi Note-11,Motorola G3 etc. with heterogeneous hardware and software resources. We compared the proposed Fuzzy lattice-based trust management system with the existing Hierarchical Fuzzy logic based trust system and analysed the performance of both the systems based on execution time, battery consumed and CPU utilization.

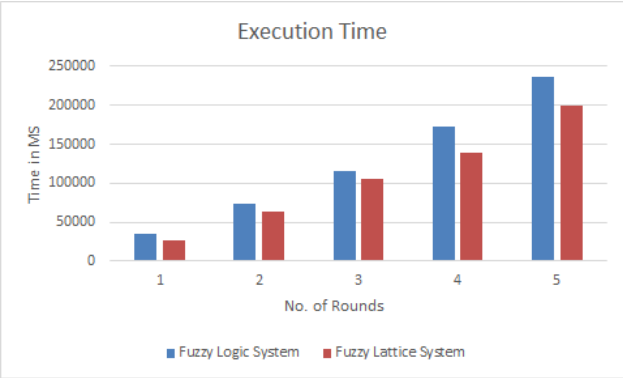

Figure 4. Execution Time

As shown in Figure 4. the time taken for execution of the Fuzzy hierarchical system is more for each dataset as compared to the trust management system based on fuzzy lattice as the number of comparisons required in rule-based fuzzy logic system is reduced in the proposed fuzzy lattice-based system. Also, the amount of battery consumed and CPU utilization also varies and is more in case of hierarchical fuzzy system and less in case of fuzzy lattice-based system as shown in Figure 5 and Figure 6 respectively.

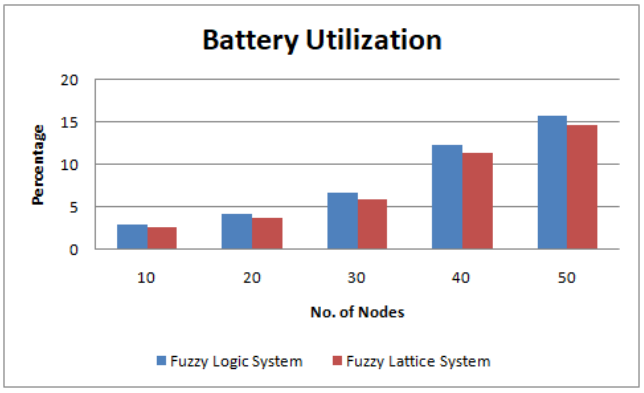

Figure 5. Battery Utilization

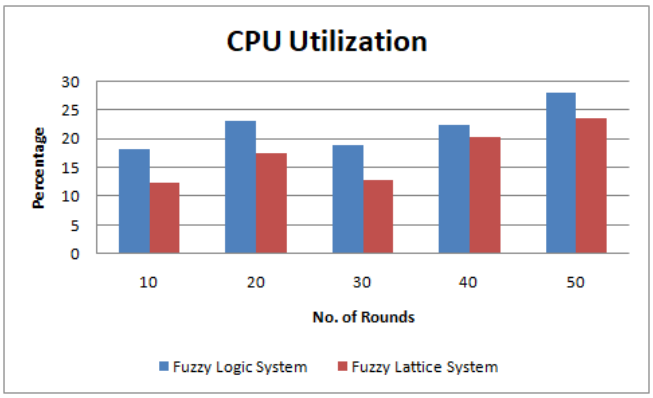

Figure 6. CPU Utilization

V. CONCLUSION

In this paper a trust management model is proposed based on a novel approach of fuzzy lattice to improve the efficiency and security of mobile grid systems. The reputation-based trust model evaluates the indirect trust of non-neighboring nodes using social network theory and is based on psychology and common sense. The fuzzy lattice trust model is an efficient alternative solution to the existing fuzzy logic based models. Comparative results prove that fuzzy lattice based trust model gives improved results than fuzzy logic based models at high speed and consuming less resources. In the future, the features of machine learning can be incorporated into our algorithm to make them more efficient, accurate and intelligent. This would eliminate not only false feedback but also get rid of the widespread spamming happening in the mobile grid network.

REFERENCES

1. David G. Rosado, Eduardo Fernandez-Medina, Javier Lopez, Mario Piat-tini ,'Systematic design of secure Mobile Grid systems', Journal of Network and Computer Applications, (2011).
2. Qiyi Han1, HongWen, Gang Feng, BinWu, Mengyin Ren, 'Self-nominating trust model based on agglomerative fuzzy systems for peer-to-peer networks', Springer Peer-to-Peer Networking and Applications, Volume 9, Issue 6, (2016), pp 020-1030.
3. Song SS, Hwang K, Zhou RF, Kwok YK, 'Trusted P2P transactions with fuzzy reputation aggregation', IEEE InternetComput., 9(6),(2005), pp24-34.
4. Chen HW, Ye ZW (2008), 'Research of P2P trust based on fuzzy decision-making', In: Proceedings of 12th International Conferenceon Computer Supported Cooperative Work in Design, (2008), pp 793-796.
5. Lin HQ, Li ZT, Huang QF, 'Multifactor hierarchical fuzzy trust evaluation on peer-to-peer networks', Peer-to-Peer Networking and Applications, (2011), pp:376-390.
6. Ing-Ray Chen and JiaGuo, 'Dynamic Hierarchical Trust Management of MobileGroups and Its Application to Misbehaving NodeDetection', IEEE International Conference on Advanced Information Networking and Ap-plications (AINA), (2014).
7. Ing-Ray Chen, JiaGuo (2015), 'Hierarchical trust management of community of interest groups in mobile ad hoc networks' , Ad Hoc Networks, Volume 33, (2015), pp 154-167.
8. Bedi Punam, N.A. Aakanksha, and Richa Sharma, 'Trust and context view-based knowledge sharing in MANets', International Journal of Trust Management in Computing and Communications, Vol.1 No.1, (2013), pp.85 – 103.

9. Hui Xia, Zhiping Jia, Lei Ju, Xin Li, Youqin Zhu, 'A Subjective Trust Management Model with Multiple Decision Factors for MANET based on AHP and Fuzzy Logic Rules', IEEE/ACM International Conference on Green Computing and Communications, (2011).
10. Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Car-los M. B. Duarte, and Guy Pujolle, 'Trust Management in Mobile AdHoc NetworksUsing a Scalable Maturity-Based Model' , IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 7, NO.3, (2010).
11. Lei Chen, JiahuangJi, Zihong Zhang, Wireless Network Security, Springer Nature America, Inc., (2013).
12. JiGuo , Alan Marshall, Bosheng Zhou, 'A New Trust Management Frame-work for Detecting Malicious and Selfish Behaviour for Mobile Ad hoc Networks', International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, (2011).
13. JiGuo (2011), 'A New Trust Management Framework for Detecting Malicious and Selfish Behaviour for Mobile Ad Hoc Networks' , IEEE 10th International Conference on Trust Security and Privacy in Computing and Communications, (2011).
14. BasitQureshi, Geyong Min, DemetresKouvatsos, 'M-Trust: A Trust Management Scheme for Mobile P2P Networks',IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, (2010), pp 476-483.
15. Qureshi, Basit I.(Kouvatsos, Demetres and Min, Geyong), 'Trust Management for P2P application in Delay Tolerant Mobile Ad-hoc Networks. An Investigation into the development of a Trust Management Framework for Peer to Peer File Sharing Applications in Delay Tolerant Disconnected Mobile Ad-hoc Networks', Ph. D. thesis, University of Bradford, (2011).
16. BasitQureshi, Geyong Min, DemetresKouvatsos, 'A distributed reputation and trust management scheme for mobile peer-to-peer networks', Computer Communications, Volume 35, Issue 5, (2012), pp 608-618.
17. Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, 'Security Enhancements for Mobile Ad HocNetworks with Trust Management Using UncertainReasoning', IEEE Transactions on Vehicular Technology, Volume: 63, Issue: 9, (2014).
18. Azzedine Boukerche, and Yonglin Ren, 'A Secure Mobile Healthcare System usingTrust-Based Multicast Scheme', IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 27, NO. 4, (2009).