Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review and Reputation Based Trust Management towards WLAN (RRTM)

Amruta Pandule, Poonam N. Railkar, Parikshit N. Mahalle
Department of Computer Engineering, STES's Smt. Kashibai Navale College of Engineering, Pune, India

Abstract *— Nowadays wireless networks are becoming more and more admired. These are widely preferred as they are very easy to deploy. They augment the resource sharing and collaboration since these networks are physically decentralized. The anonymous behaviour and open nature of the WLAN put forward an ultimate environment for unauthorized access of resources also can be victim of attacks in the wireless network. WLAN systems may need to face attacks like man-in-middle, replay and Denial of Service (Dos) from malicious nodes in the network. That will cause an essential need of protecting these systems from such external attacks with secured communication between the peer nodes. For this purpose, the trust worthy communication must be established between the nodes. Before setting up the communication it should have trust in advance with the node to which it will communicate. Hence an efficient Trust Management System should be present for launching the trust worthy communication also updating the same based on its performance.*

The proposed system presents an iterative trust score calculation for WLAN based on review and reputation of the node in the network.

Keywords — Trust, Infrastructure Mode, Ad-hoc Network Mode, Reputation, Review, Trust Management System.

I. INTRODUCTION

As WLANs are connectionless, these systems are extremely preferred by the global users as they provide a compatible infrastructure that will diminish the building cost of the network. Any node in a WLAN can contribute to the network maintaining the anonymity. There is 802.11 standard from IEEE and this specifies the WLAN in three types.

- **Infrastructure Mode:** Each WLAN workstation (WS) communicates to any machine through access point (AP).It may be in same WLAN or connected to outside world through AP.
- **Ad Hoc network Mode:** Every node talks to another node directly.
- **Mixed Network Mode:** Every node can work in the above two modes simultaneously.

Contrary 820.11's claims, WLANs have very less security. The open and unobstructed environment of WLAN architecture makes it an ideal environment for unauthorized access to resources and for information sharing also for the attackers to spread malicious content. It has to protect themselves from the attacks by anonymous malicious peers. Node must determine whether other Nodes are authorized to access resources or functionalities. Therefore peers involved must establish trust before transaction happens between them.

So the remedy is,

Don't Trust anybody!!!!!!!!

The trust is defined in various terms in various models [1], [2]. In this we have considered the trust in network as the degree of belief about another node. We can say that trust is a measurable belief and is relative to some transactions. The trust between nodes is directed for e.g. If node A trusts node B but node B may distrust node A. Trust exists and evolves in time. The facts that node A trusted node B in past does not itself guarantee that A will trust B in future. The performance of B and other relevant information may lead A to re-evaluate her trust in B in future.

This paper presents the Trust Management model for Ad-hoc network which will collect the reviews of the node in the network and will periodically monitor its trust values by colleting periodic reviews from the other nodes in the network that already had transaction with it. The actual novelty of the model lies in (a) Review collection, (b) Reputation Calculation, (c) Trust Score Calculation based on review and reputation, (d) Activity tracking for Trust value updation [3].

II. MOTIVATION

The current Trust Management Model is a generic Trust Management Model for peer to peer networks and ad-hoc networks [1]. It mainly considers the reputation of the node and the recommendations as well as basic properties of trust like asymmetry, reflexivity, transitivity.

There is trust based identity management for WLAN with 802.11 which will consider the review and reputation based trust calculation for node before joining the subnet but there is no monitoring of workstations after entering the

network [4]. Evaluation of trust value and trust level is changeless forever. So a malicious node may enter the WLAN by pretending very honest and pure operation on any of the other node in the network. But once it gets entry in network it starts misbehaving and shows deviation in its intended behaviour. This malicious node once entered in network starts attacks on this WLAN. It may cause flooding of the network with traffic (Denial-of-Service attacks), Rogue network by introducing rouge access point, 'Man-in-the-middle' between two nodes, station redirection.

There are many other attacks too which can affect the network. So the motivation is to build the Trust Management model which will establish the trust before the communication starts and will track the activities of all the nodes to update their trust values and trust levels periodically so that there will be trusted communication in the network.

III. RELATED WORK

Lot of work has been done in trust-management area. Several trust-management systems have been proposed in recent years for P2P network. Basically the trust management system is classified into three types as Reputation based Trust systems, Policy based Trust systems and Social network based Trust systems.

The Reputation based Trust systems include systems like XRep [5], DMRep [6]. These systems mainly involve trust evaluation based on measuring the reputation of the peer. To compute the trust value of the given peer the witnesses who have interacted with the same peer in past share their experience with that peer and help to compute the trust rating of the given peer. A node's User-based rating is the rating given by its witnesses according to the previous experience with the given peer. Thus Reputation-based trust systems evaluate the trust in the peer and the trust in reliability of the resource.

Social Network based trust systems are based on the social relationship between the peers .The evaluation of the trust is based on the analysis of the social network. It includes the different systems like Marsh [7], NodeRanking [8]. Google's PageRank algorithm [9] can also be considered as a global reputation systems. This algorithm does not require the participation of the users to rank the web pages. Basically, the web page with more back links (links that point to it) is considered to be more important (has higher rank) than the one with fewer back links. Use of the Bayesian Approach is also proposed in [10], [11]. In these systems, a posterior reputation value of a peer is computed combining its a priori reputation values with the new ratings received for the peer. Further, a threshold method is used to determine and update the report reliability of nodes.

The Policy based Trust systems mainly use credentials verification to establish the trust relationship for access control. These systems are based on the notion of delegation, whereby one peer entity gives some of its authority to other peer entity.

A. Evaluation of Related Work

A lot of work has been done on Trust Management System. With this, the previous work is analyzed and according to our context of research the common parameters have been taken for evaluation of the trust. Table1 given below shows the evaluation of state of art. For this purpose, this paper considers these parameters in the proposed architecture which have not been considered in the literature.

In this proposed architecture recommendation of the previous node, transaction history of the node which will include how many successful and failure transactions it had , reputation based on the review from all other nodes and finally its own review which is nothing but the reflexivity property of the trust are combined to calculate the trust value for the particular node. The table 1 shows the evaluation of the related work in the form of parameter consideration.

Table 1: Evaluation of related work

Existing model	Identity Authentication	Recommendation	Transaction History	Reputation	Reflexivity (Self Reviews)	Review
[1]	√	√	ɤ	√	√	ɤ
[12]	√	ɤ	ɤ	ɤ	√	ɤ
[13]	ɤ	√	ɤ	√	ɤ	ɤ
[14]	ɤ	√	√	ɤ	ɤ	√
[15]	ɤ	ɤ	√	√	ɤ	ɤ
[16]	ɤ	√	√	√	ɤ	ɤ

√: Corresponding parameter is considered in given Trust Management Model
ɤ: Corresponding parameter is not considered in given Trust Management Model

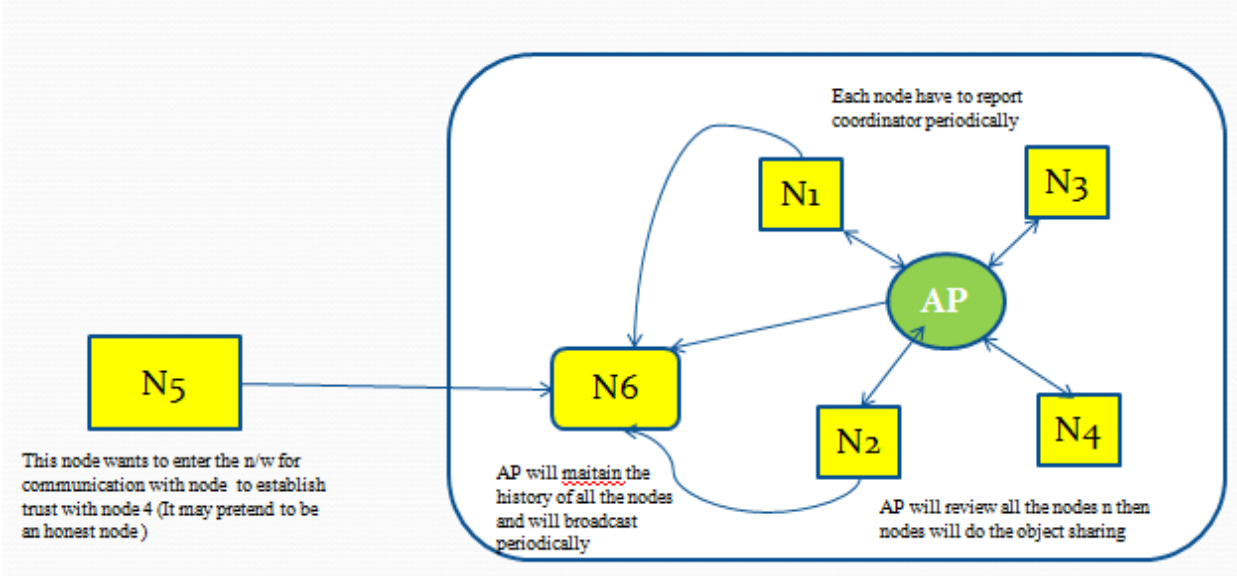
IV. PROPOSED SYSTEM

As there is no wiring to define membership, this open air nature of WLAN makes it prone to more security threats. Therefore it is necessary to secure WLAN through Trust Management which will consider the reputation and its review from the other node who already had transaction with this node. Thus the Trust Management which will collect the review of the node and compute the reputation based on its transaction history and all other parameters like its self review. And this computed Trust value need to be updated periodically as the node may pretend just to get the entry in the network and then may start misbehaving. So the Trust management model which will establish the trust before communication starts and will monitor the calculated trust periodically need to be developed.

A. Proposed Architecture

In this section we will briefly describe how the review and reputation based trust score is calculated for WLAN. Here we assume that the whole model will work in following steps (a) Network Scanning and Object Sharing (b) Review collection (c) Reputation Calculation, (d) Trust Score Calculation based on review and reputation, (e) Activity tracking for Trust value updation

Let's consider a WLAN with different workstations connected to an Access Point (AP) depicted by Fig 1. Each node communicates with AP directly. Node will scan the network for object sharing in the network. Node can transmit the object in network and this transmission of object will add to the contribution of the node in the network. Node can share the same object with the other nodes in the network after observing their trust values. Then trusted node who has received the shared data successfully will give the feedback for the transaction happened. If node has completed the intended task its trust value increases. Reputation of the node will be considered transactions in the network. Successful transaction will add the trust score value whereas failed transaction will affect the trust of the node in the network. Feedback from the node will also contribute for the trust value updation. Now the three steps of the architecture come into picture for monitoring of the trust once it has started the transaction in network.



i

Fig 1. WLAN Network

Initially the new node is allowed to enter in the network with lowest trust level value and once it is entered in the network its behavior is monitored periodically so to update its trust value based on its review from the other nodes.

Fig. 1 Shows proposed architecture of the RRTM system. The detailed flow for establishment of trustworthy communication is shown in Fig. 2 and it is mainly in three phases and details of the each phase are as follows:

- Initialization Phase: In this phase one of the node requests for the communication with the other node in the network and then the review is collected for the node and trust score is calculated for the node.
- Actual Transaction Phase: In this phase actual communication takes place between the nodes. That communication may be transmit and receive of data in the network. In this phase the participation score of the node is updated.
- Feed Back Phase: When actual transaction takes place between two nodes then rating is assigned to this transaction. Thus host node receives the rating for the transaction taken place.

V. IMPLEMENTATION DETAILS

Proposed RRTM is implemented in Java 1.6 and using the Socket programming for the communication between the nodes.

Following parameters are considered for the calculation of the reputation and review of the node in the network,

1. Transmit Receive Ratio in the network
2. Experience of the node in the network
3. Feedback of the node in the network from other nodes

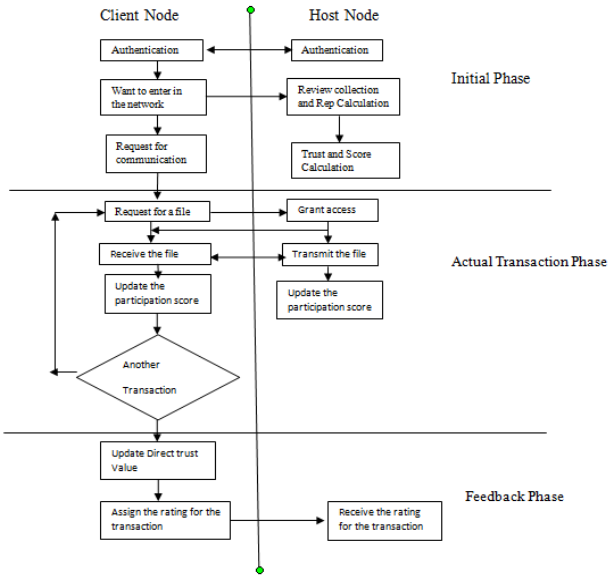


Fig 2. Establishment of trustworthy Communication

The detailed calculation of the above parameters is as follows…

1. Transmit Receive Ratio in the network:

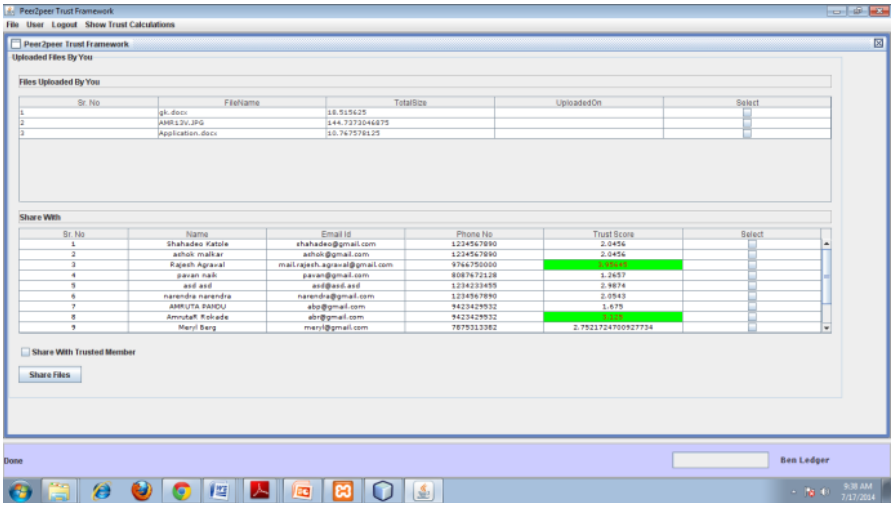


Fig 3. Object Sharing in the network

This parameter will consider the transactions which had taken place in the network. Fig. 3 shows the object sharing in the network. This will include three different factors as follows:

I.) The ratio of the total files transmitted by the node in the network to the total no of files transmitted on the network. It will be as

$$F_1=T_i/T_t \quad \text{where F1 belongs to [-1 to +1]} \qquad (1)$$

Where T_i = Total files transmitted by the node in the network

T_t= Total files transmitted on the network

II.) The ratio of the total files received by the node in the network to the total no of files received on the network. It will be as follows:

$$F2= R_i/R_t \quad \text{where } F_1 \text{ belongs to [-1 to +1]} \qquad (2)$$

Where R_i= Total files received by the node in the network

R_t = Total no of files received by all the users in the network

2. Experience of the Node in the network:

This parameter includes the experience of the node in the network which will include whether the transaction taken place is successful or not.

Here the Experience is considered as the ratio of total no of successful transactions to the total no of transactions in the network.

$$F3= TR_s/TR_t \quad \text{where F3 belongs to [-1 to +1]} \qquad (3)$$

Where TR_s= Total no of successful transactions in the network.

TR_t=Total no of transactions in the network

3. Feedback of the node in the network from other nodes:

This parameter is calculated based on the feedback given by the other user who already had the transaction with it. Fig. 4 shows the feedback process for the object shared.

Node can give the feedback for the particular object more than once and accordingly the latest feedback score will be considered for the trust score calculation.

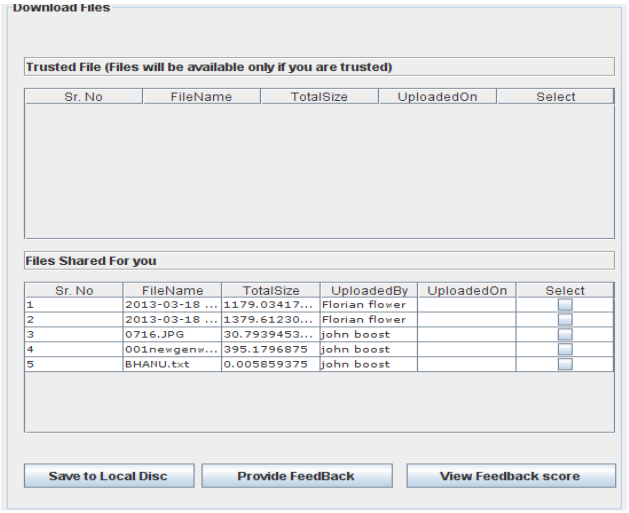


Fig. 4 Feedback for the transactions happened.

$$F5=F*(U_f/T_f) \quad (5)$$

Where F = this is individual node's feedback score

U_f= this is the no of feedbacks given by the node

U_t = this is no of feedback given by all the nodes

Thus the trust is considered as the uncertain prediction of node in the network dependent on the above parameters. Here all the above parameters are represented in the linguistic values. With reference to Mamdani scheme, each rule is represented by an If-Then relationship. Mamdani type if-then rule is written as follows:

If X_1 is A_{1r} and……X_n is A_{nr}

Then Y is B_r

Where Air denotes the linguistic labels of the ith input variable associated with r^{th} rule (i= 1,....., n) and Br is linguistic label of output variable.

So the linguistic labels for the above parameters are represented in the table below:

Table 2: Linguistic Labels of the parameters

L(TR)	L(EXP)	L(RV)	Trust Level
Low	Bad	Bad	Below 0 to -1
Medium	Average	Average	It will be 0
High	Good	Good	Above 0 to +1

Therefore the final trust value for the node by combing these parameters will be will be

$$T = \frac{\sum_{i=0}^{n}(F1 + F2 + F3 + F5)}{n} \quad (A)$$

Where T belongs to will be from 0 to infinity.

n = total no of the nodes who have given the feedback and have experience in the network.

This trust value will start from 0 to ∞ values from so if the value is in between 0 to 1.5 then the trust level is the lowest, if it is in between 1.5 to 3 then the trust level is average and if it is above 3 then the trust level of the node will be highest i.e. it can be trusted blindly for communication in the network.

Thus the access right for the communication between the two nodes in the network is assigned on the basis of the trust level. This trust level is mapped with the access permissions in the communication between the two nodes.

Following mapping is used between trust level L and access Permission AP:

L = {Lowest, Average, Highest}

And AP = {(RECEIVE), (RECEIVE, SEND), (RECEIVE, SEND, MODIFY, DELETE)}

This calculated trust value will be updated periodically as once communication established node may start misbehaving in the network so need to track it.

Finally the updated trust score will be displayed for the particular node in the network.

Fig. 5 shows how the factors, considered are changing as the transactions are taking place. And the total trust value will vary accordingly.

VI. PROBABILISTIC MODEL

- Trustworthy communication is to be established in the network
- One of the node in the network requests for the trustworthy communication with another node in the network.
- So the trust value for the second node is to be calculated.
- The trust value for the desired node will depend on the direct trust and indirect trust of the host node who has requested for the communication with one of the node in the network (we will call this as client node).

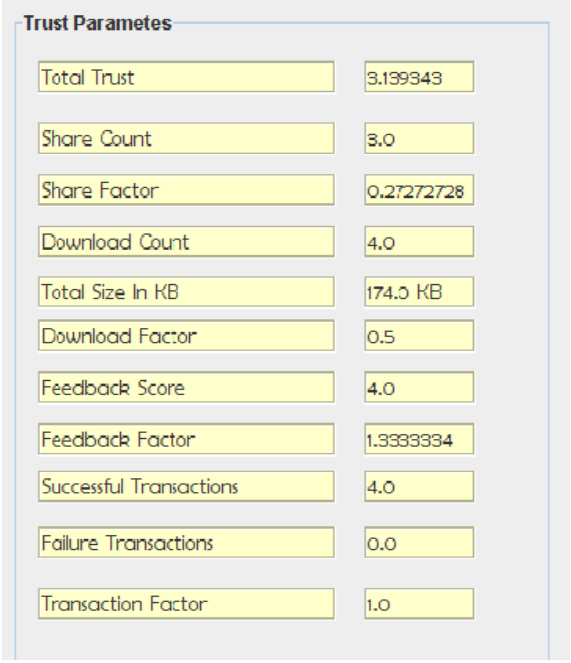


Fig. 5 Display of all the trust parameters for the node.

- Direct trust value is the host's belief on the client's capacities, honesty, and reliability.
- Indirect trust represents the host's belief on the client's capacities, honesty and reliability based on reputation of the client node in the network and review i.e. recommendations from the other witness nodes in network.
- Again reputation of the client node in the network is decided based on the no of successful and unsuccessful transactions of client node in the network.
- Review received from the witness nodes will depend on different parameters in the network like information shared from the client node while their interaction (downloaded or uploaded), speed of downloads or uploads.
- As of now I am considering this as simplest random variable having Boolean value i.e. True or False as the node can be trusted or not.

With the help of Bayesian network I describe the acyclic representation of these random variables as shown in Fig. 6.
In the below Bayesian network conditional relationships between the variables is represented in the graph structure. Here according Markov condition we can have the join probability distribution over all the variables X1, X2,……, Xn in the network.
So using the following formula

$$P(X_1 = x_1,...,X_n = x_n) = \prod_{i=1}^{n} P(X_i = x_i \mid Parents(X_i))$$

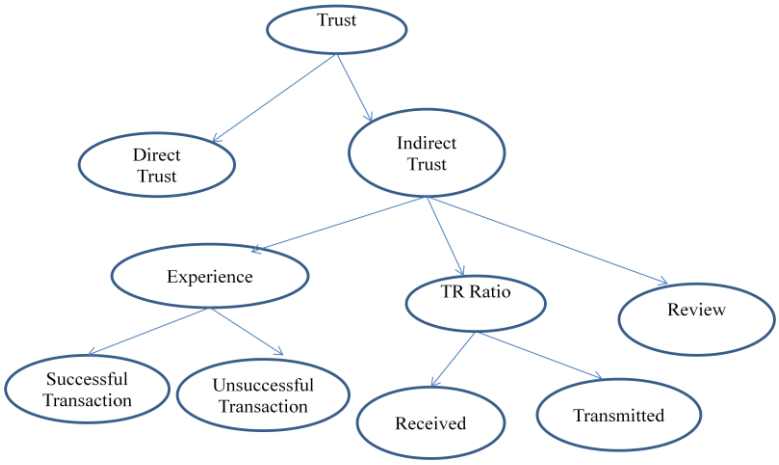


Fig. 6 Bayesian network for Proposed TMS

VII. CONCLUSIONS AND FUTURE WORK

In this proposed model, An Iterative Trust Score is calculated for node in the ad-hoc network based on Review and Reputation. This architecture is for establishment of trustworthy communication between the two nodes in the network. In this network the behaviour of the node will be monitored periodically and its trust value is also updated .So depending on the behaviour of the node in the network trust relation will be established between two nodes .

This paper presents step by step calculation of the parameters which will be considered while calculating the trust.

Future work includes handling the misbehaviour of the nodes who was trusted earlier and then started misbehaviour in trusted communication.

REFERENCES

[1] Ryma Abassi , Sihem Guemara El Fatmi, Higher School of Communication, Sup'Com University of Carthage Tunis, Tunisia*" Towards A Genric Trust Management Model"* , 19th International Conference on Telecommunications (ICT 2012), 978-1-4673-0747-5/12/$31.00 ©2012 IEEE

[2] Erman Ayday, Student Member, IEEE, and Faramarz Fekri, Senior Member, IEEE *"Iterative Trust and Reputation Management Using Belief Propagation"* IEEE Transactions on dependable and secure computing, Vol. 9, No. 3, May/June 2012

[3] Pandule Amruta, Poonam N. Railkar & Parikshit N. Mahalle, Smt. Kashibai Navale College of Engg. Pune, University of Pune. "*Review and Reputation Based Trust Score Calculation (RRTSC)*" International Journal of computer applications(IJCA), Nov 2013

[4] *"Reputation-based Trust Update in Network Environment"* Shufen Peng, Jingsha He and Yao Meng , International Symposium on Electronic Commerce and Security, 2008

[5] F.Cornelli, E.Damiani, S.C. Vimercati, S. Paraboschi, and P. Samarati, "*Choosing reputable systems in a P2P network"*. In the proceedings of the eleventh international conference on World Wide Web, Honolulu ,Hawaii ,USA, 2002.

[6] DMRep- K.Aberer, Z. Despotovic, *"Managing Trust in peer to peer Information System",* In Proc of the IX International Conference on Information and Knowledge Management, Atlanta, Georgia, 2001.

[7] S Marsh "Formalising Trust as a Computational Concept", Ph.D. Thesis University of Stirling.

[8] J. Pujol, R. Sanguesa, "Extracting reputation in multi gent systems by means of social network topology", First International Joint Conference on Autonomous Agents and Multi-Agent Systems, Bologna, Italy.

[9] L. Page, S. Brin, R. Motwani, and T. Winograd, "The Pagerank Citation Ranking: Bringing Order to the Web," technical report, Stanford Digital Library Technologies Project.

[10] S. Buchegger and J. Boudec, "Coping with False Accusations in Misbehavior Reputation Systems for Mobile Ad Hoc Networks," Technical Report IC/2003/31, EPFL-DI-ICA, 2003.

[11] A. Whitby, A. Josang, and J. Indulska, "Filtering Out Unfair Ratings in Bayesian Reputation Systems," Proc. Seventh Int'l Workshop Trust in Agent Societies (AAMAS '04), 2004.

[12] Amit Mathur, Suneuy Kim, Mark Stamp, "*Role based access control and JXTA peer-to-peer Framework*" www.truststc.org,2005

[13] Kui MENG, Xu ZHANG, Xiao-chun XIAO, Geng-du ZHANG "*A Bi-rating Based Personalized Trust Management Model for Virtual Communities*" 1-4244-0065-1/06/$20.00 2006 IEEE

[14] Wenjing Cui, Haiyang Wang, Qi Sui, Lizhen Cui, School of Computer Science and Technology, Shandong University, China "Towards a Trust Management Model for E-travel" 1-4244-0963-2/07/$25.00 ©2007 IEEE.

[15] Jianli Hu1, Xiaohua Li, Bin Zhou, Yonghua Li, "*A Reputation Based Attack Resistant Distributed Trust Management Model in P2P Networks*", 2010 Third International Symposium on Electronic Commerce and Security

[16] *Hui Xia, Zhiping Jia *, Xin Li, Feng Zhang* School of Computer Science and Technology Shandong University Jinan, P.R. China "*A Subjective Trust Management Model based on AHP for MANETs*", 2011 International Conference on Network Computing and Information Security

