

# TRUST FORMATION BASED ON SUBJECTIVE LOGIC AND PGP WEB-OF-TRUST FOR INFORMATION SHARING IN MOBILE AD-HOC NETWORK

Asmidar Abu Bakar, Abdul Rahim Ahmad  
Dept. of System and Networking,  
COIT,UNITEN  
Malaysia  
asmidar@uniten.edu.my  
Roslan Ismail  
Dept. of Software Engineering  
COIT,UNITEN,Malaysia

Jamalul-Lail Abdul Manan  
MIMOS Berhad  
Malaysia

**Abstract**— Trust play important roles in Mobile ad hoc networks since nodes may randomly joined and leave the network at their own pace. In catastrophe like massive accident or earthquake, groups of rescue personnel form a temporary network structure at the rescue site using their portable devices for coordinating the rescue relief. These groups of user from different agency need to use the temporary network for communication and also for sharing the information. Trust plays important roles in these groups since sharing of information must be among trusted and authorized nodes only. In this paper we form trust model adopting the PGP web-of-trust concept with subjective logic. The PGP web-of-trust is suitable method to adopt in mobile ad hoc networks since nodes are communicating based on peer to peer, hence peer recommendation can be use to create trust between peers. The use of subjective logic operators for calculating trust in the proposed trust model is appropriate since there is an element such as uncertainty as part of calculation. Uncertainty is important in this dynamic network since we do not have full information when decision is make. The trust value later is mapped with the access control policy to determine user access privileges.

**Keywords**- Mobile ad hoc network, Trust, Subjective logic, PGP web-of-trust, Group, Uncertainty

## I. INTRODUCTION

The boost of mobile computing and communication devices such as mobile phone, laptops, and handheld devices are making the world of communication and information becomes easy and borderless. Mobile users carry their mobile devices to check e-mail, browse internet, and do transaction online. With the new wireless technology such as Bluetooth or WiFi the mobile users even can play online games or to exchange MP3 songs by creating a so called ad-hoc network. This ad -hoc network is known as Mobile ad-hoc network (MANET) since it is constructed by mobile devices. It is a self-organized wireless network without any fixed infrastructure.

MANET can also be constructed at the disaster place where the network infrastructure is not viable or partially/fully collapse. Example in massive accident, groups of rescue personal gathered at the rescue site to form a temporary network for relief operation. These groups which is structured and trusted since there are all already exists prior to network setup at the disaster area may comprise of Fire Brigade, Policeman and Medical. They formed network for communication and to gathered and shared information. Example of information that needs to exchanged and must be protected are personal and medical information of the victim, information on the threaten areas, the traffics conditions and many more. These groups must trust each other in order to collaborate to make the relief operation successful. As such trust is very vital in this dynamic network structure.

In this paper, we proposed a trust model for information sharing in MANET environment. The used of the trust value is to be mapped with the access control policy to determine the access privileges given to nodes that are not register prior to network setup or called as new node (NN). Taking rescue mission as example, there are possibilities that volunteer (s) exist at the rescue site and wish to do the rescue work. This volunteer is not part of structured group but they may need to use the information that is gathered by structured groups as mentioned above. To allow NN to get an access to data/information shared by structured group, the trustworthiness of NN need to be determined. NN have to bring some credential that can prove his identification.

The proposed trust model is adopting PGP web-of-trust with the used of subjective logic operators and operation. PGP web of trust is choosing since nodes in MANET are collaborated based on peers. The choice of subjective logic is to present trust as opinion since in this network there is an element of uncertainty. This is because we cannot gather perfect knowledge about some entity and thus we can only have an opinion towards it.

This paper is arranged as follow; in Section II we give an overview on trust, PGP web-of-trust model and subjective logic. A proposed trust model is presented in section III and in section IV; we highlighted previous work related to trust and access control in MANET. We conclude this paper in Section V.

## II. OVERVIEW OF TRUST, PGP WEB-OF-TRUST AND SUBJECTIVE LOGIC

We first present the concept of trust and PGP web of trust. A few trust definition from other researcher are list here and ways trust are formed also been documented. A related work on trust is also mention here and we end this part by explaining the subjective logic concept.

### A. Trust

Trust is a very important element in wireless network especially when it is involved communicating or exchanging private and secret information among nodes. This is because in wireless network the medium is open to all nodes that within the radio range and therefore can eavesdrop the message. In MANET, groups of user can create a network to fulfil their needs for example having the downloaded music or exchanging document electronically. However the network is open to intruder and malicious node. There will be a situation where new node will come and wished to share the information thus before an access is given to this new node, the trustworthiness on this new node need to be determine.

### B. Definition of trust

Many researchers have defined trust. Below are few of trust definition. Josang in his paper [3] defines trust as subjective belief and can be expresses as an opinion. Gambetta [1] defines trust as "*trust/distrust is a particular level of the subjective probability with which an agent evaluate that another or group of agents will perform particular action both before he can monitor such action and in a content in which it affects his own action*". Based on this trust have a certain degrees of possibility or belief in which people will evaluate trust based on action or things that others do and it will influence our judgment towards the actions that we will carry on later. Grandison and Sloman[2] defined trust as "the firm belief in the competence of an entity to act dependably, securely and reliably within a specified context" (assuming dependability covers reliability and timeliness). Based on these three definitions, we define trust as *the belief that one node has towards another nodes and it is presented in term of opinion*.

### C. Trust formation

Trust can be gathering from direct experience and / or with the recommendation from other nodes. Direct experience is MG experience with the node itself whereby the recommendation is the peer's opinion based on peer interaction with the node. However in MANET especially in rescue mission environment, trust based on direct experience may not achievable since MG may not have enough time to interact and monitor's node behaviour before derived the trust value. The best solution is to rely on peer's recommendation. As peers may interact with NN previously, peers may have knowledge about NN's reputation thus NN can give recommendation

about NN to MG. In this work, we adopt peer recommendation and MG opinion towards peers in forming the trust model.

### D. PGP Web-of-trust concept [17]

In PGP, there is no central authority which everybody trusts. In this trust model, individuals sign each other's keys and gradually build a web of individual public keys interconnected by links formed by this signature. PGP adopt the web-of-trust concept. Example in PGP, assume that Carol, a researcher, requires some data from a source named Bob whom Carol has never met before. Alice, a colleague of Carol's, signs Bob's public-key certificate which she knows is authentic. Bob then forwards his signed certificate to Carol who wishes to communicate with Bob privately. Carol, who knows and trusts Alice as an *introducer*, finds out, after verification, that Alice is among Bob's certificate signer hence Carol can be confident that Bob's public key is authentic. Therefore Carol can trust that Bob is trusted entity since Carol trust Alice.

There are two areas where trust is explicit in PGP. These are listed below:

1. Trustworthiness of public-key certificate.
2. Trustworthiness of an introducer

Trustworthiness of public-key certificate refers to the binding between the user ID and the public key itself which contained in the certificate/credential of the new node.

In PGP, the trustworthiness of public key can be categorizes into three levels which stated below:

- *undefined*: we cannot say whether this public key is valid or not.
- *marginal*: this public key *may* be valid be we cannot be too sure.
- *complete*: we can be wholly confident that this public key is valid.

As for trustworthiness of introducer meaning how much we can trust the peer to recommend the new node. There are four levels of trustworthiness which stated below:

- *full*: this public-key is fully trusted to introduce another public-key.
- *marginal*: this public-key can be trusted to introduce another public-key, but, it is uncertain whether it is fully competent to do that.
- *untrustworthy*: this public-key should not be trusted to introduce another and should be ignored.
- *don't know*: there are no expressions of trust made about this public-key.

In our work, we only utilise complete and marginal trust level and assigned appropriate value for each level. As for full /complete trust the assigned value is 1 and 0.5 as for the marginal. This will further discuss in our propose trust model below. We do not consider the untrustworthy and don't know level since we applied subjective logic in our calculation for

peer opinions and with this it covers these two levels since in subjective logic there is portion for disbelief and uncertainty.

### E. Subjective Logic

In subjective logic, trust is way to express beliefs, or relatively uncertain beliefs about the truth of the statements. Since we have imperfect knowledge about a statement, example like “*NN tag is valid and NN is trusted*” thus we can only have an opinion about it and it can be translate into degrees of belief or disbelief as well as uncertainty [15]. In mathematic we can write it as below:

$$b+d+u=1, \{b,d,u\} \in [0,1]^3 \quad (1)$$

Josang[15] defines opinion as below:

Let  $\omega = \{b,d,u\}$  be a triplet satisfying (1) where the first, second and third component correspond to belief( $b$ ), disbelief ( $d$ ) and uncertainty ( $u$ ) respectively. Then  $\omega$  is called an opinion.

### III. PROPOSED TRUST MODEL

During disaster either caused by nature like hurricane or earthquake or man-made disaster such as bombing explosion, most or partially existing network infrastructures are collapsed. Hence a temporary network needs to be created to support communication and information sharing among groups that involved in the rescue works.

In rescue mission scenario, there are two types of groups of user. One group is structured and well organized such as group of army, policemen, firemen and medical and the other one is un-structured group, which is a group that is randomly created by users like volunteers or groups of non government agencies. These volunteers are not part of any structure/trusted group and their formation is basically ad-hoc. To make the relief operation successful they need to communicate and share information. Therefore in order to allow nodes from non-trusted groups to share the information with the trusted groups, a trust model needs to be constructed. This trust model is used to evaluate the trustworthiness of the nodes in the non-trusted groups before an access to information is given.

In figure 1, assumed that the structured/trusted group which is comprised of group of fireman (GF), group of policeman (GP) and group of medical (GM). There are members (M) and group leader known as Master Group (MG) in each of these groups. Prior to network setup all members registered with their MG and MG registered with Root Certification Authority (R-CA). All of them are given tag as member identification. Each MG in each group broadcast their secret key to their members which they obtained prior to network setup to establish the temporary network at the rescue site. All MG are also temporary CA at this temporary network. MG keeps data/information related to their roles in the rescue site, such as GP keeps data on road /traffics surrounding the rescue site and many more. Request to share information is between MG and members from trusted groups. Any node from non-trusted group (GV) can also make request to MG since only MG is holding the data/information. This simulates client-server interaction.

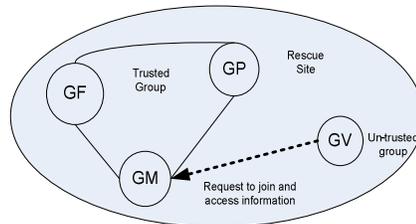


Figure 1: Structured group and un-structured group in MANET at rescue site

An access to information between members in trusted groups is achieved using the tag they obtained during registration at the rescue area. The tag binds member identity with group and the tag also contains the authorization’s status. As for nodes from GV, as showed in fig.1, in order to get an access to information held by any MG in the network, NN from GV needs to bring credential that can prove his identification to the MG. This is important since information could contain sensitive data that involved confidentiality and also privacy.

The proposed trust model for trust recommendation is based on PGP web-of-trust model and subjective logic. In our model, the concept of the trustworthiness of an introducers and the trustworthiness of the key are both applied. The trustworthiness of the key in our model refers to introducer’s opinion about NN credential/tag. Tag is token that NN used for authentication or it can be perceived as referral letter (Peers verified the tag belong to NN by signed the tag and assigned their opinion on tag) and as for the trustworthiness of introducers is how much Master Group (MG) trust introducer’s (peers) opinion. The MG’s opinion is divided into two types which are complete and marginal. We assigned value 1 for complete and 0.5 for marginal. We assigned this value based on the condition below:

- i. If both introducers are members of MG, example both peers from group M, then MG M have full trust on introducers. As a result value 1 is assigned for MG opinion.
- ii. If one introducer is a member but the other one is not (The other one is a member from other group that setup the network) then MG M will have only marginal trust on both introducers. As a result the value 0.5 is assigned for MG opinion.

Based on figure 1 above, assumed that NN is working at organization X and X has created tag for NN however since this temporary network is created on the spot and there is possibility that MG cannot verify the tag due to facts that X is unreachable, then NN needs to get peers in this network to verify the tag/credential. Peers endorsed the credential by signing it and assigned their opinion on it. Peer opinion is presented to MG and using consensus operator, MG will obtained the consensus opinion of peers about NN credential. To get the overall opinion value which later becomes the recommendation trust value, the MG’s opinion and the peer’s opinions are considered. Both opinions are added together and get an average value. This value later will be mapped with the access control policy to determine the type of object that NN can accessed.

We recommended at least two introducers since this will give fairness for both party. The protocol below show how NN

obtained the introducers for certifies his identity and signed his credential/tag.

#### A. Protocol:

- NN enters the network and broadcast his identity to members in the network.

$NN \rightarrow$  Send Hello packet, request for Group M

- After getting the broadcast packet from NN, assume now we have two peer nodes, P1 and P2 from Group M know NN and give response.

$P1, P2 \rightarrow NN$ : Response Hello packet, Group M

- NN now can query P1 and P2 to sign his credential (Cre).

$NN \rightarrow P1, P2$ : Request Sig (Cre)

- P1 and P2 sign NN credential using their secret keys (SK).

$P1, P2 \rightarrow NN$ : (Cre)SignSK p1, SignSK p2

$P1, P2 \rightarrow NN$ : Send (Cre)

- NN received credential signed by P1 and P2. The signed credential consist P1 and P2 opinion. NN can now show the signed credential to MG M.

#### B. Applying subjective logic to propose trust model

For every peer node (P) they have to measure NN's credential based on three inputs which are their belief on NN's credential (his identity and info in the tag) their disbelief on the credential and their uncertainty on the credential following the mathematical statement in (1). P1 and P2 may communicate with NN previously thus they obtained direct experience with NN. The mathematical statement on P1 and P2 opinion towards NN's credential is as below:

- $\omega_{NN}^{P1} = \{b_{NN}^{P1}, d_{NN}^{P1}, u_{NN}^{P1}\}$
- $\omega_{NN}^{P2} = \{b_{NN}^{P2}, d_{NN}^{P2}, u_{NN}^{P2}\}$

These two opinions are combined to get the consensus opinion [15]. Using the consensus operator in subjective logic, we get the below mathematical statement:

$$\omega_{NN}^{P1, P2} = \omega_{NN}^{P1} \oplus \omega_{NN}^{P2} = \{b_{NN}^{P1, P2}, d_{NN}^{P1, P2}, u_{NN}^{P1, P2}\} \quad (2)$$

= T1

Where,

$$\left\{ \begin{array}{l} b_{NN}^{P1, P2} = (b_{NN}^{P1} u_{NN}^{P2} + b_{NN}^{P2} u_{NN}^{P1}) / (u_{NN}^{P1} + u_{NN}^{P2} - u_{NN}^{P1} u_{NN}^{P2}) \\ d_{NN}^{P1, P2} = (d_{NN}^{P1} u_{NN}^{P2} + d_{NN}^{P2} u_{NN}^{P1}) / (u_{NN}^{P1} + u_{NN}^{P2} - u_{NN}^{P1} u_{NN}^{P2}) \\ u_{NN}^{P1, P2} = (u_{NN}^{P1} u_{NN}^{P2}) / (u_{NN}^{P1} + u_{NN}^{P2} - u_{NN}^{P1} u_{NN}^{P2}) \end{array} \right.$$

We used the continuous value 0 to 1 to indicate the opinion values and peers and also MG may assigned any value from 0 to 1 to belief, disbelief and uncertainty with 1 for fully belief and 0 for fully disbelief or uncertain.

Based on equation 2, assume now P1 opinion towards NN is {0.7, 0.2, 0.1} and P2 opinion is {0.6, 0.1, 0.3}, and using the consensus operator in (2), we get the consensus opinion of P1 and P2 as {0.73, 0.19, 0.08}. This opinion is denoting as T1.

Next the opinion from MG towards peers needs to determine. As explained earlier, the opinion is expressed as complete or marginal, with value 1 represent complete and 0.5 for marginal. The MG's opinion is denoting as T2.

#### C. Trust value (TV) calculation

The calculation for trust value is showed in equation 3 below. We take an average of these two opinions as showed below.

$$TV = (T1 + T2) / 2 \quad (3)$$

The trust value will be mapped with the access control policy based on Discretionary Access Control (DAC) model. DAC is adopted in this model since it allowed the owner of the subject to determine the access privileges. Table 1 below showed the level of object sensitivity with trust value.

Table 1: Trust value and Object sensitivity level

Trust value	Level of sensitivity
$0.5 \geq TV < 0.80$	Less sensitive object
$1.0 \leq TV \leq 0.80$	Sensitive object

Based on table 1 above, the trust value for less sensitive object is ranging from 0.5 to 0.79, while as for sensitive object; the rank for trust value is very stringent since it involved highly confidential data that may involve integrity as well as privacy. Any value below 0.5 is considered as not trusted and no access to information is granted. Example below showed the relationship between the trust values with level of sensitivity of object that new node can access. Regardless accessing sensitive or less sensitive object, the new node only allowed to READ the data and not to READ/WRITE. This is important to maintain data integrity.

Example 1: Both peers are members of Group M. In this case, MG M really trust the opinion given by his members. Assume now both peers, P1 and P2 give opinions towards NN = 0.5 since they not really sure about NN tag even they may have history of interaction or have knowledge about NN reputation previously.

$$\begin{aligned} TV &= (Peer\ opinions(T1) + MG's\ opinion(T2)) / 2 \\ &= (0.5 + 1.0) / 2 \\ &= 0.75 \end{aligned}$$

This means NN only can access less sensitive object.

Example 1 showed that, given peers from group M that MG fully trust, but since peers only believe NN up to minimum value, 0.5 then MG cannot allowed NN to access sensitive info.

Example 2: One peer is MG M member and the other is not, this makes MG's opinion on peers become 0.5. Assume

now both peers, P1 and P2 give opinions towards NN =0.5 since they not really sure about NN tag even they may have history of interaction or have knowledge about NN reputation previously. Thus the calculation of trust value is as below:

$$\begin{aligned} TV &= (Peer\ opinions(T1) + MG's\ opinion(T2))/2 \\ &= (0.5 + 0.5)/2 \\ &= 0.5 \end{aligned}$$

In example 2, worst opinion is given by all parties and NN able to get minimum trust value and thus is able to access less sensitive data. For example accessing information related to general info that is sharable by all participants in the rescue work.

Example 3: Both peers are members of MG M (hence MG trusts the opinion and gives value 1 for T2), and both peers also know NN and based on equation 2, the T1 is 0.8. Thus the trust value is as below:

$$\begin{aligned} TV &= (Peer\ opinions(T1) + MG's\ opinion(T2))/2 \\ &= (0.8 + 1)/2 \\ &= 0.9 \end{aligned}$$

In the best conditions with good opinions value given by peers and MG then NN obtained a very good trust value. With this it showed that NN's credential is highly recommended and can access sensitive data.

Based on three examples presented above, we can conclude that in rescue operation, where accessing data is critical and important in order for the rescue works to be successful, thus in worst scenario such as in example 2, given the worst opinion (both T1 and T2 is 0.5) there is still chance to get access to data. This is applicable for data that is considered as general and not involved any confidentially. As for accessing data that is sensitive it required both opinions given by MG and peers to be relatively high. Therefore the range of trust value and level of data sensitivity created in table 1 able to secure the data in term of confidentiality, privacy and also integrity.

#### IV. RELATED WORKS

Current research on MANET are focusing on forming trust for authenticating unknown nodes used in routing protocol [6], [7],[11] and [12] also for collaboration among nodes in the network [5], [8] and [13]. In [6], researchers proposed a method to detect and isolate those misbehave nodes at the network layer for routing and forwarding packets in the network. This approach work well for network layer but lack of subjectivity limits its applicability to work at other layer i.e. application layer. While in [7], the researchers develops trust model for evaluating known routes and choose the route that best meets the security requirements of the message being transmitted.

Pirzada et al. [11], proposed a framework for trust establishment in ad-hoc environment which applicable for routing and in [12], the researchers used trust model to detect malicious packet dropping attack in MANET. Michiardi [5] proposed an organic reputation-based framework to enforce collaboration in ad-hoc networks. The works used reputation information of nodes to force nodes to collaborate. In [8], the

researchers relate human trust in forcing the collaboration to take place among mobile systems. They introduced h-trust, a human-based trust management model and framework that a mobile system can exploit to form trust opinions.

In [13], they used the trust based access control mechanism to drive quicker coalition among nodes so that the group can cooperate easily to work in the network. In [9], the researchers proposed a hierarchical trust model that work with RBAC. The trust model comprises of basic trust which is build by resource constrained trust negotiation (RCTN) and application trust which will activate the roles for users and it is based on context data. Different context data will change the application trust value and different roles will be activated.

In [15], algebra for assessing trust in certificate chains is proposed. In this paper, the researcher has introduced an authentication algebra that takes relative trust in key-to-owner binding and trust in the ability to recommend. This method offers a practical solution to the authentication problem in open network. While in [16] they introduce the notion ignorance as uncertainty during the establishment of trust relationship with other nodes. The researchers also use subjective logic in derive trust and introduce new operators in order to express ignorance. This model is design to work in routing algorithm in MANET. Researchers in [4] also derive trust for routing algorithm and develop a framework that defines trust metrics using information theory.

Keoh et al.[14] in their paper also adopt PGP's web-of-trust concept. They used it to build trust in a community. They represent trust as the expectation that the participants will enforce the rules defined in the community specification or doctrine and that the membership of the community will be governed by clearly defined constraints. Our work is different from the rest since we use trust to make decision on information sharing. The opinion of peers towards new node and MG opinion on introducers (peers) are used to derive trust on nodes and mapped it policy hold by MG based on Discretionary Access Control (DAC). Using this policy, MG will decide whether an access to request an object is permissible or not based on trust value.

#### V. CONCLUSIONS

We proposed the trust model for information sharing in rescue operation in MANET following the PGP trust model and subjective logic. In PGP web-of-trust there are two ways to derive trust which are trust of the introducers and trust of the key binding to the owner. We adopt this concept as it suit MANET features which are based on peer's collaborations. We have showed how we able to utilize the consensus operators from subjective logic for calculating the trust. The used of trust model here is to show how NN can prove his trustworthiness before an access to request object is granted. MG mapped the trust value calculated with level of sensitivity of the requested object. With this MG can decide either to allow or block the access. Our future work is to simulate the value obtained from this trust model and do a graph comparison with exiting PGP trust model. We want to demonstrate that by incorporating subjective logic in a PGP web of trust model it give us better trust result in rescue operation as compared to PGP alone in MANET environment.

## ACKNOWLEDGEMENT

We like to thanks the anonymous reviewers for their comments.

## REFERENCES

[1] Gambetta, Diego,” Can We Trust Trust ? In Gambetta, Diego (ed.) *Trust: Making and Breaking Cooperative Relations*, electronic edition, Department of Sociology, University of Oxford, chapter 13, pp.213-237,2000.<http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf>

Date access: 4 February 2008

[2] T. Grandison, M. Sloman, A Survey of Trust in Internet Applications, IEEE Communications Surveys and Tutorials, Fourth Quarter 2000, <http://www.comsoc.org/pubs/surveys/>

[3] A. Josang , S.J. Knapskog,” A metric for trusted systems”, In Proceedings 21th NIST-NCSC National Information System Security Conference, 1998,pp. 16-29.

[4] Y. Sun, W. Yu, Z. Han, and K.J. Ray Liu. Information theoretic framework of trust modeling and evaluation for ad hoc networks. IEEEJournal on Selected Areas in Communications, 24(2):305–317, 2006.

[5] R.Michiardi, P. Molva,” Core :A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks”, In proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, Kluwer, B.V., 2002. pp. 107-121

[6] S. Buchegger,I.L.Boudec., “ The effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks”, In Proceeding of WiOpt 2003: Modeling and Optimization in Mobile , Ad –Hoc and Wireless Networks, IEEE Trans. On Mobile Computing, 2(1):52-64, 2003.

[7] Z.Liu, A.W.Joy, R.A.Thompson,”A Dynamic Trust Model for Mobile Ad Hoc Networks”, Proceeding of the 10<sup>th</sup> IEEE International Workshop on Future Trends of distributed Computing Systems (FTDCS’04), 2004.

[8] L.Capra., “Engineering Human Trust in Mobile System Collaborations”, SIGSOFT ‘04/FSE-12, ACM, Newport Beach, CA, USA, 2004

[9] Gua Yajun, Wang Yulin, “Establishing Trust Relationship in Mobile Ad-Hoc Network”, International Conference on Wireless Communication, Networking and Mobile Computing (WiCom), 2007.

[10] Goecks J., Mynatt T., “Enabling Privacy Management in Ubiquitous Computing environments through Trust and Reputation Systems”, Gvu Center, College of Computing , Georgia Tech,Atlanta GA. 2002.

[11] A. A.Pirzada., C.McDonald,” Establishing Trust in Pure Ad-Hoc Networks”, 27<sup>th</sup> Australasian Computer Science Conference, Vol.26, 2004.

[12] J. Sen., P.R.Chowdhury ., I.Sengupta.” A Distributed Trust Mechanism for Mobile Ad Hoc Networks”, International

Symposium on Ad Hoc and Ubiquitous Computing (ISAUH’06),2006.

[13] W.J.Adams, N.J.Davis., “Towards a Decentralized Trust-based Access Control System for Dynamic Collaboration”, proceedings of the 2005 IEEE Workshop on Information Assurance and Security, NY, 2005.

[14] Keoh, S.L. and Lupu, E.,Trust and the establishment of ad-hoc communities., 2nd Internal, iTrust Workshop on Trust Management in Dynamic Open Systems, London, UK,September 2003.

[15] A.Josang,An Algenra for Assessing Trust in Certificate Chains, Proc. of NDSS’99, Network and Distributed System Security Symposium, The Internet Society, San Diego, 1999.

[16] V.Balakrishnan, V. Varadharajan,U.Tupakula, Subjective Logic Based Trust Model for Mobile Ad Hoc Networks, Securecomm’08,September 22-25,2008, Istanbul, Turkey, ACM.

[17] A. Abdul-Rahman. The PGP Trust Model, 13 August 1996  
[http://netresearch.ics.uci.edu/Previous\\_research\\_projects/agent\\_os/related/security/abdul-rahman-pgp-trust.pdf](http://netresearch.ics.uci.edu/Previous_research_projects/agent_os/related/security/abdul-rahman-pgp-trust.pdf). Date access: 4 March 2010.