Trust and Cluster based Security architecture in MANET for a Collaborative Computing Environment

S.Sivagurunathan
Department of Computer Science and Applications, Gandhigram Rural Institute-DU, Gandhigram-624302
Email: svgrnth@gmail.com@gmail.com
K.Prathapchandran
Department of Computer Science and Applications, Gandhigram Rural Institute-DU, Gandhigram-624302
Email: kprathapchandran@gmail.com

----------**ABSTRACT**----------

Collaborative computing is the new paradigm of computing in the industry towards saving time and cost. As Information and Communication Technology grows, further digital communication becomes an unavoidable part in a collaborative computing environment and such technologies have become a part of any organization. In this paper, we propose how the collaborative computing for a project environment is carried out with the help of Mobile Ad Hoc Network and security related issues have long been investigated in MANET due to its distinct nature. Moreover traditional security mechanisms are not well suited for MANET because they are centralized, static and they also require huge memory and high computational power and it leads to processing overhead and bandwidth consumption. So in order to overcome such issues, we propose trust in this context to ensure the authentication by the way security can be achieved and selfish nodes can be isolated from the network with less memory and computational capabilities because our proposed algorithm does not involve complex computation. In addition, by making use of trust, clusters can be formed. Hence scalability issues are effectively addressed and we also justify Mobile Ad Hoc Network for project environment over traditional network and discuss its significance.

Keywords – **Authentication, Collaborative Computing, Cluster, Information and Communication Technology (ICT), Mobile Ad Hoc Networks, Security and Trust.**

INTRODUCTION

Collaborative computing allows users to work together on documents and projects usually in real time, by taking the advantage of underlying network communications systems [1]. Here the communication system works on Mobile Ad hoc Networks generally identified as MANET here open and shared mobile nodes are connected together over a structure less wireless network. Henceforth they do not be subjected to any fixed infrastructure similar to the traditional wireless and wired networks. Going to these forms of networks does not demand any dedicated router for forwarding the packets rather each node acts as a router. These types of networks can be easily deployed and it is a temporary network. Nodes in the MANET are moving without any restrictions hence the topology of network could frequently change. We make use of this network for collaborative project environment and this application runs on the top of MANET even if traditional network is available for such collaborative environment, growth of ICT enables us to make use of such distinct network with some benefits.

The project environment is defined around objects those objects may be hierarchically combined together. The objects might be people, teams, locations, tasks, projects or meeting, data or resources [2] and devices to process the data and devices for communication. In this paper we treat objects as communication devices or nodes. In contemporary business and science a project is defined as a collaborative enterprise, involving research or design that is carefully planned to achieve a particular task [3]. Hence our objective is to create a collaborative computing environment with Mobile Ad Hoc Network in such a way that it ensures an authentication between the collaborative devices in this open, shared wireless network by means of trust mechanism and also we address the scalability issue. To secure a MANET, the following goals are to be considered: Availability, Confidentiality, integrity, Authenticity and Non repudiation [4]. Among the goals, authentication is important because it ensures the identity of its peer node with which it is communicating. Once identification is done successfully, the remaining goals can be achieved easily. The main contribution of this paper is to isolate selfish nodes from the network through evaluating trustworthiness of nodes in order to provide authentication. Selfish nodes are free riders that consume other node's resources without supporting the network with their own resources [5] hence overall performance of the network is in question. On the other hand, normal nodes [5] are willing to cooperate with each other to accomplish a particular task. Notwithstanding we identify that this is a first attempt made in providing trust and cluster based security architecture for one of the collaborative computing applications such as project environment.

The organization of this paper is as follows: section 2 justifies why project environment with MANET

over traditional networks, section 3 discusses about the security issues section 4 describes the impact of trust section 5 discuss the impact of clustering section 6 shows the related work section 7 demonstrates the proposed work and final section presents the conclusion.

1. Why Project Environments with MANET over Traditional Networks?

Today's project environments are heavily computerized with networking proficiencies in order to share ideas and information. When compared with traditional network users, users of MANET are not required to be stable in their working area. If traditional network users want to move away from their working place then their business infrastructure is often missing but the need for collaboration among the users should be addressed to attain a task. In some circumstance the requirements of temporary network for rapid communication with minimal configuration among a group of people who are involved in projects are required to share their findings or materials during the work. So it seems that the establishment of an ad hoc network for collaborative mobile user is required even when there may be internet infrastructure support available. When we use infrastructure link, it always leads to overhead, which might involve extremely suboptimal routing back and forth between widely separated office environments [6].

In addition when we are using traditional network, there is a chance for single point of failure and it will affect the performance of whole organization. Reducing wiring leads to minimizing the maintenance and installation cost, intelligent devices (node acts both computer and router) leading to higher performance and increased functionality such as advanced diagnostics, distributed control providing flexibility to apply control either centrally or in a distributed way for improved performance and reliability [7]. In excess of sustaining the consistency of project environments while natural disaster like flooding and earth quake, these effects may or may not happen but care should always be given. Minimizing time and cost are the two mandatory aspects for any project environment [8] from this time, MANET leads to achieve these aspects because it does not require any fixed infrastructure it can be easily deployed and terminated when not needed.

2. Security Issues

Though MANET architecture is suitable for many applications including collaborative computing environment, it's distinct nature causes some issues such are routing, multicasting, medium access scheme, transport layer protocol, pricing scheme, quality of service, self-organization, security, energy management, addressing and service discovery, deployment consideration and scalability [9]. Among these security is one of the important issues because of the following reasons. According to [10] 32% time is spent towards job communication in an organization and strongly specified, this is the highest percentage of time spent among the various activities involved in a project environment. In order to complete a project effectively we are in circumstances to communicate with each other and supposed to work in collaboration. The information exchange between the devices in the project environment is highly sensitive because it has valuable customer information, internal information of an organization and may be global information and exchange of such information is carried out relatively over unsecured network because wireless channel for any organization is accessible to both legitimate network users as well as malicious attackers. Hence there is a chance of external attack. In an organization collaboration is executed in a loosely coupled manner that means communication between the devices may be short lived, dynamic so the communications change over time subsequently we cannot predetermine the privileges of participating devices though team members of project environment are formerly know.

To work collaboratively devices must exchange services and requests among them and such things are journeyed over multiple intermediate devices hence we cannot predict the reliability of such devices. As MANET, communication is going to be carried out doubtlessly in open and shared environment. The communication is going to take place between devices without knowing each other henceforth securing such environment are obviously in question. Trust relationship among nodes also changes; because a new device may join or leave and that device may be compromised. Finally project environment may consist of hundreds or even thousands of devices. Security mechanisms should be scalable to handle such large networks. As a result, there is no clear line of defense in MANET architecture from the security design perspective. Hereby collaboration wants effective communication then communication needs effective security if there is a lack of security, performance is in question.

3. Impact of Trust

To ensure the security of an organization traditional security mechanisms are used but they are key based where keys are pre-determined and also depend on any third party hence computational and network overhead dramatically increases and it leads to performance degradation in overall network's throughput, availability and robustness [11]. So in order to overcome such problems trust comes into existence. To go ahead with the necessity of trust, we give some formal definition of trust with respect to various aspects. According to the software engineering point of view, trust can be defined as trust is accepted dependability [12]. According to the network and communication field trust is defined as "a set of relations among entities that participate in the protocol which is based on the previous interaction of entities within the protocol [13]. According to ad hoc networks, trust could be defined as the reliability, timeliness, and integrity of message delivery to a node's intended next hop [14]. Simply, trust is reliance on a device or an entity. Authentication is a significant aspect in the security of MANET that enables a device to ensure the identity to the receiver [15].

As mentioned earlier once authentication is achieved, rest of the security requirements could easily be achieved. To ensure the authentication each device must trust other

devices. Hence a trust is a gateway and decision for devices to authenticate each other. Trust is a word which is originally derived from the social sciences. Trust is defined as "one entity (trustor) is willing to depend on another entity (trustee) [16]" or "the trustor abandons control over the actions performed by the trustee [17]". In order to complete the mission successfully each device should cooperate with all the other devices. We can just say each device has trust on other devices. MANET is a decentralized distributed network. Hence achieving cooperation among the devices is a complicated task. The reason being, each device in the network must trust every other device without prior recommendations and interactions. But this blindness in communication will make it more vulnerable to mobile device and affect the network performance greatly. Hence cooperating devices must trust each other in order to achieve the desired security level. Compared with traditional wired network, collecting trust evidence to evaluate a trustworthiness of a particular device in MANET is crucial problem due to its dynamic nature also a new device may join or leave the network at any time [18].

4. Impact of Clustering

Another issue in MANET environment is scalability. We do not expect that all the participating devices in a project environment are in the same communication range because each node's communication range may vary depending on its configuration and also for a large projects number of participating devices will extremely high but at these situation we are in need of effective communication that is information should reach to all the nodes in the network. Brooks [10] stated that number of communication paths among programmers in a software development grows as n (n-1)/2 where n denotes number of programmers. A small project normally has only less than 20 members, hence the communication path is relatively low. Very large or extremely large projects have more than 100 members. So obviously as the communication path is increased then managing communication among the devices is infeasible. Therefore overhead increases with overall productivity. To overcome such problem clustering technique is used. The idea is to; divide the network into number of sub groups named as clusters [19].

A cluster may also communicate with other clusters and also it serves as a temporary base station. This scheme typically utilizes three types of nodes that are having specific roles. First one is cluster head; an efficient cluster head performs overall coordination within a cluster and its task is channel access, routing, calculation of routes for long distance messages, bandwidth allocation, forwarding inter cluster packets and power control. Second one is cluster gateway node; it acts as a mediator between two cluster heads [20, 6]. For instance, a node in a cluster wants to communicate with another node, which belongs to some other cluster, in this situation, cluster gateway is used to carry out the communication between these two nodes. Hence cluster gateway should be in the communication range of these two clusters. In our work we don't take cluster gateway into account. Finally, ordinary nodes that do not perform any coordination function. They are only the members of clusters that are directly connected with cluster heads [21, 22]. Also, nodes are dependent within the cluster and independent to other clusters. In addition to this cluster based approach is used to address the nodes heterogeneity and to limit the amount of routing information within a cluster, managing wireless transmission among multiple nodes to reduce channel contention, forming routing backbones to reduce network diameter and abstracting network state information to reduce its quantity and variability. Hereby we make use of these clustering concepts into our proposed project environment to avoid communication overhead and increase the coordination among the members by the way we can achieve higher performance and we treat cluster as team and ordinary nodes are team members (i.e.) people who are involved in the project.

5. Related Work

In this section we discuss some existing work that focus on security aspect of collaborative computing environment.

Agarwal et.al [23] proposed a security model that concentrated on traditional security mechanism such as certificates and password. Trust is calculated based on the pre-determined registration. It comprises of self-registration, user registration and administrative registration phases and each phase depends on traditional security mechanisms. Their ultimate aim is to achieve authentication and authorization and collaborative computing is based on client server model. Hence this work obviously relies on wireless with access point network. Colin English [24] proposed a trust based security architecture for e-purse applications where owner of the bus, the user and the bank are involved. The objective is to model the trust relationship between the bus company and the user. Trust is assessed based on personal experience and recommendations. Alvaro E.Areans e.al [25] proposed a repudiation management for virtual organizations where the collaborative works are involved. Trust and reputation is based on utility computing and that can be used to rate users, therefore user's resource usage and their providers according to the quality of service they deliver. Sepandar D.Kamvar et.al [26] proposed a trust algorithm for point to point networks. The purpose of this algorithm is to decrease the number of downloads of inauthentic files in a peer to peer file sharing network by assigning a global trust value to each peers in the network then global trust value is calculated based on power iteration. Moreover global trust value is used to isolate malicious nodes form downloading activity as well as from the network.

Brian shand et.al [27] proposed a trust and risk framework to facilitate secure collaboration in ubiquitous and pervasive computing systems. Trust is evaluated from user's own trust information and recommendations by forming a policy function. Finally these policy functions are combined together to attain a final trust. Then actions are moderated by a risk assessment. Based on the final trust and risk assessment participants can safely share their information. Vinny cahill et al [28] proposed a trust based security

collaboration in uncertain environment. Here trust is calculated based on personal observations of the entity's behavior through recording outcomes of interactions and experience. Indirect trust is evaluated from recommendations from trusted third party also there is a risk evaluator for assessing the cost. Finally request analyzer is used to combine both direct and indirect trust with cost to make decisions. Xu Wu [29] proposed a distributed trust management model for mobile point to point networks based on the distributed hash table networks. The aim is to predict the future availability of wireless links and leads to fast generating valid trust evidence. Trust value is evaluated based on the interaction and feedback values from the neighboring peers.

From this literature review to best of our knowledge nobody ever did trust and cluster based security architecture for collaborative project environments. Therefore we try to fill the gap in this paper.

6. Proposed Work

These following sections describe the proposed security architecture and fig. 1 illustrates the overall architecture proposed.

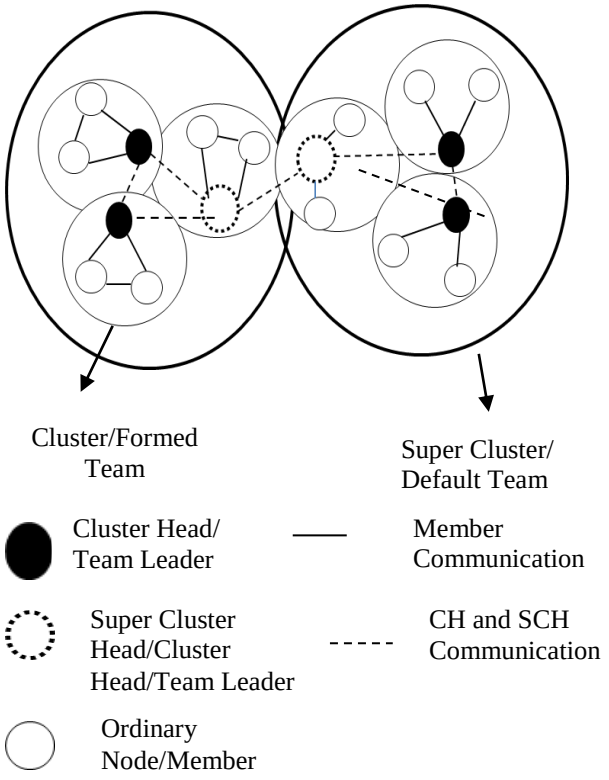

Figure 1. Cluster/Team Formation of Project Environment runs on top of MANET

7.1. Cluster formation

We assume that all the project members are holding their current project id, team id and member id because more than one project can be handled by an organization at a time. The reason behind our assumption is, typically every organization has pre-determined knowledge that, where they are going to work and what is their demand accordingly they will place the people who is going to be involve in the project. From this point we can understand that all the users' formerly known their current project and team that they are going to work with. Since manual team will be formed by default, that particular team is called super cluster [6] and again team formation is required within a super cluster and forms a sub team named as cluster [6] by using cluster formation algorithm here we do not attempt to make it manually.

For a large project within a team all the devices may not be in the same communication range and moreover if any device wants to communicate with its own team which is not in its communication range then the information will travel across intermediate devices, hence processing overhead increases as well as consumption of battery power and data may also be dropped. So as to avoid this problem clustering technique is used to form sub group within a super cluster.

For understanding of the readers, a software development involved with various activities such are analysis, design, implementation, test and maintenance. So team will be formed based on their knowledge. Within team there may be so many members depending on the size of the project hence we are in situation that we make effective communication between them so that clustering technique is used.

Cluster formation will be formed within a super cluster based on [30] the device which is having highest trust value will be acting as a cluster head. Before that if we want to make cluster formation, as mentioned earlier each node should know their trust values of its neighboring nodes in order to form a cluster and this will be explained in next section. The communication within cluster members named as intra cluster [6] and will be managed by cluster head or team leader. On the other hand, communication between the clusters is managed by super cluster head [6]. The super cluster head is the one which is having highest trust value among all the members of clusters.

7.2. Trust Computation

We assume that everyone involved in project having their current project id, team id and member id and each node has predefined trust at the time of network deployment and also assume that node's movement occurs randomly. Over time, nodes will establish a level of trust with other nodes based on the task assigned to them. Each node maintains a trust table based on the observed behavior of its neighbors. For example, if node A is observing node B, which is within its transmission range, it understands that the number of tasks that have been assigned to be accomplished and number of tasks actually completed by node B. In our approach, each node has to evaluate the trust of all the neighboring nodes; at the same time the trust value of that node is also being

evaluated by every other node. To complete a particular task each node should communicate with other nodes at regular interval of time or when needed. Over time, a node's trust value is being evaluated based on direct observation and each node should calculate the trust value of its neighboring nodes using the following formula.

$$Trust\ (T) = NTC/NTA \quad (1)$$

Where *NTC* denotes number of task actually completed and *NTA* denotes number of tasks assigned. Equation 1 denotes a direct trust value of Node B calculated by node A at certain time interval t_i. Likewise all the nodes will evaluate their trust values of neighboring nodes at regular intervals or when needed. A node can perform some actions in a particular time interval and may not perform in another time so that the aggregation of trust value is used to evaluate a node's final trust value. The following equation is used to evaluate an aggregated trust value over a period of time and this equation is based on normalization of data set [31].

$$AT = (IT\text{-}N_{min}) / (N_{max} - N_{min}) \quad (2)$$

Where *AT* denotes aggregated trust, *IT* denotes node's initial trust value, N_{min} denotes node's minimum trust value and N_{max} denotes node's maximum trust value. We also consider number of feedback values [29] from its neighboring nodes as a factor for evaluating trust because those neighbors are active neighbors and even if they are not involved in any action. We assume that initial feedback value for all the nodes are zero. Over time node A evaluates node B's feedback value based on the given formula.

$$FV = \sum_{T=1}^{N} AR_T / \sum_{T=1}^{N} TR_T \quad (3)$$

Where *FV* denotes feedback value, *AR* denotes actual response and *TR* denotes total number of requests made by node A to node B over time. By means of taking the average of aggregated trust and feedback value we can evaluate an overall trust of node.

$$OT = (AT+FV)/2 \quad (4)$$

Where *OT* denotes overall trust, hence the overall trust value is used to make decision on a particular node, trust value is calculated at regular intervals of time as mentioned earlier such that $T = (t_1, t_2, t_3 \ldots t_n)$, and we assumed that node's trust level as a continuous real numbers in the range [0, 1] with 1 indicating complete trust and 0 indicating no trust so that $\sum$ Overall Trust <= 1. Therefore each node maintains a trust table which contains trust value of neighbor nodes, project id, team id and member id.

7.3. Identifying Selfish Nodes

Over time, trust value of any node can change depending on behavior.

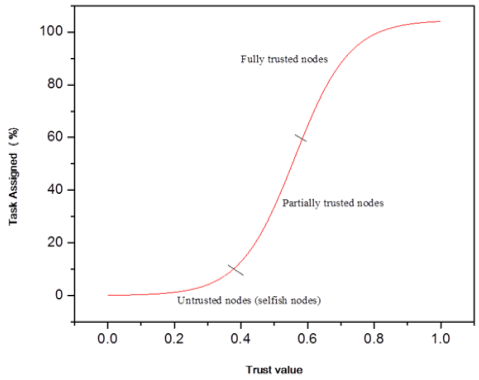

Figure.2 Different trust level and task assignment

The fig. 2 shows the different trust levels and its corresponding task assignment over time. After evaluating a node's final trust we can make a decision. At this point three levels of trust can be assigned for any node such as trusted nodes, partially trusted nodes and untrusted nodes (Selfish nodes). Trusted nodes means we can completely allow that node to involve in accomplishing a task and also for interaction. Partially trusted node means it is allowed only for interaction and no task will be assigned to it and finally untrusted node is completely avoided. Once the selfish nodes are identified, they will be isolated and information about the selfish nodes are immediately reported to the neighbors by the way it can be deleted from node's trust table. By the way selfish nodes will be isolated from the project environment. The Table 1 illustrates different levels of trust and its task assignment.

Table 1. Trust level and Task Assignment

Level	Trust Value	Meaning	Task Assignment and Interaction
1	(0.0,0.4)	Untrusted node	Selfish nodes hence avoided
2	(0.4,0.6)	Partially trusted node	Allow to Interaction only but no task assigned
3	(0.6,1)	Trusted node	Allow to both task and interaction

7.4. Trust management

Trust management is involved in two circumstances first when member node(s) leaves from the network; second new node(s) joins the network. When a new node joins the network, it sends a hello message to the current network. A node with highest trust evaluates or assigns the requesting node's trust. After that, if the requesting node meets the network requirements such as predermined threshold, allow that node to participate in the network by sending a response message which contains member nodes details

along with their corresponding trust values. Otherwise request will be cancelled. While leaving, each node sends leave message to all its neighbors, therefore entry about the leaving node is deleted from the network.

7.5. Algorithm for proposed work

Step 1: Assign;
Project id is represented as pid
Team id is represented as tid
Member id is represented as mid
Node movement occurs in random fashion
Mobile nodes have predetermined trust in the initial network deployment
Initial Trust is represented as IT, Aggregated Trust is represented as AT
Feedback value is represented as FV; Overall Trust is represented as OT
Number of task actually completed is represented as NTC
Number of task assigned is represented as NTA
Total number of request is denoted by TR
Actual response is denoted by AR, T1 and T2 denote threshold values.
Initialize;
IT = n; (n is any arbitrary value), FV=0; (for each node)

Step 2: Cluster formation and cluster head selection phase;

- Default: Super cluster formation phase
- Execution cluster formation phase algorithm: Go to Step3;
  - Each node updates their neighbor's trust values in its respective trust tables then chooses one node as cluster head that has highest trust value.
  - Chooser nodes will become members of cluster head hence cluster is formed.
  - If cluster head is already a member of another cluster, choose second highest trust value node as a cluster head.
  - If two or more clusters have same trust values then one node is elected as cluster head the remaining nodes will relinquish their roles.
  - Node with highest trust value among members in the entire cluster will be elected as super cluster head.

(After some period of time each node assess its neighbor's trust in order to find untrusted nodes)

Step 3: Trust Computation
Each node calculates trust value on other nodes at certain time period
T= NTC/NTA
Aggregated trust is used to evaluate a node's overall trust
$AT = (IT\text{-}N_{min}) / (N_{max} - N_{min})$
Feedback value is used to ensure the active neighbors

$$FV = \sum_{T=1}^{N} AR_T / \sum_{T=1}^{N} TR_T$$

At last, node's final trust is calculated
$OT = (AT + FV)/2$

Step 4: Decision made based on final trust value
If (OT >T1) then
Allow to do task and interaction
Else if (OT>T2) then
Allow only for interaction
Else
Untrusted node= Selfish node
Delete entry of that node from each node's trust table
End if
End if

7. Conclusion

Our proposed work is easy to implement but powerful for project environments. The reasons behind this, most of the organizations spend their time and cost towards establishing their infrastructure but our model leads to saving of time and cost because of MANET. In the processing point of view, we make use of simple calculations to evaluate a trust with less memory and processing power and moreover we do not focus on recommendations because it always leads to processing over head higher. In our proposed model trust plays a vital role because it is used for cluster formation as well as assessing the participating node. We do not fully avoid the partially trusted nodes instead of that we give chance to interact with others by the way productivity is increased. In addition, cluster formation does not require any complex algorithm instead of that we make use of trust in order to form a clustering and cluster head selection is also very simple and easy to understand. In future we extend our work by simulation for analyzing the performance of our proposed work

8. Acknowledgment

This research work is supported by University Grant Commission, India, through a Major Research Project, Grant (UGC.F.No: 42-128/2013 (SR)).

9. Reference

[1] Jeff Shapiro, *Collaborative Computing: Multimedia across the Network*, (Morgan Kaufmann 1995).
[2] Danesh, Arman, and Kori Inkpen. *"Collaborating on Ad Hoc Wireless Networks"* Submitted to SIGCHI 2001 Workshop: Building the Ubiquitous Computing User Experience, (2001).
[3] Www.oxforddictionaries.com
[4] William Stallings, *Cryptography and Network Security*, (Pearson Education, 2003).
[5] Marcela Mejia, Nestor Pens, Jose L.Munoz, Oscar Esparza and Marco A. Alzate, "*A game theoretic trust model for online distributed evolution of cooperation in MANETs*, (Elsevier,2011)
[6] E. Perkins, *Ad Hoc Networking*, (Addison-Wesley Professional, 2008).

[7] Lawrence M.Thompson, *Industrial Data Communications*, (The Instrumentation, Systems and Automation Society, 2008).

[8] Roger pressman, *Software Engineering: A Practitioner's approach*, (McGraw-Hill, 2009).

[9] C.Siva Ram Muruthy and B.S.Manoj, *Ad Hoc Wireless Networks Architectures and Protocols*, (Pearson Education, 2004).

[10] Richard Fairley, *Software Engineering Concepts*], (Tata McGraw –Hill Edition, 1997).

[11] Wei Gong, Zhiyang You,Danning Chen, Xibin Zhao,Ming Gu and Kwok-Yan Lam, *"Trust based Malicious nodes Detection in MANET,"* IEEE, (2009).

[12] Avizienis, A., Lapire,J.C Randell, B ,. And Landwehr,c. *"Basic concepts and taxonomy of Dependable and Secure Computing"* , IEEE Transactions on Dependable and Secure Computing, **1**(1) (2004), 11-33.

[13] J S Baras and T Jiang, *"Managing Trust in Self-Organized Mobile Ad Hoc Networks,"* Proc. 12th Annual Network and Distributed System Security Symposium Workshop, (2005).

[14] Liu, z.,Joy,A.w., and Thompson,R.A, "*A Dynamic Trust Model for Mobile ad hoc Networks*", proceeding of the 10 th IEEE International Workshop on Future trends of distributes computing systems, (2004),80-85.

[15] Ngai, Edith Ch and Michael R. Lyu, *"An Authentication Service based on Trust and Clustering in Wireless ad hoc Networks: Description and Security Evaluation,"* IEEE, (2006).

[16] R C Mayer, J H Davis and F D Schoorman, *"An Integrative Model of Organizational Trust-Academy of Management Review",* **20** (3), (1995), 709-734.

[17] Bamberger and Walter, *"Interpersonal Trust – Attempt of a Definition"* Scientific Report, (2010).

[18] Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen, *"A Survey on Trust Management for Mobile Ad Hoc Networks",* IEEE Communications Surveys & Tutorials, **13**(4), (2011).

[19] Jane Y Yu and Peter H J Chong, *"A Survey of Clustering Schemes for Mobile Ad Hoc Networks,"* IEEE Communication Surveys & Tutorials, **7** (1), (2005).

[20] Http://Www.Ukessays.Com/Essays/Communications/Clustering-Benefit.Php

[21] Preetida Vinayakray-Jani and Sugata Sanyal, *"Security Architecture for Cluster based Ad Hoc Networks"*, International Journal of Advanced Networking and Applications, **04** (1), (2012), 1523-1527.

[22] M Anupama and Bachala Sathyanarayana, *"Survey of Cluster Based Routing Protocols in Mobile Ad Hoc Networks"*, International Journal of Computer Theory and Engineering, **3** (6), (2011).

[23] Agarwal, Lrch,Thompson and Perry, *"A New Security Model for Collaborative Environment",* Lawrence Berkeley National Laboratory,(2003).

[24] Colin English, Sotirios Terzis,Waleed Wagealla,Helen Lowe,Paddy Nixon and Andrew McGettrick, *" Trust Dynamics for Collaborative Global Computing"*, Proceedings. Twelfth IEEE International Workshops on. IEEE, (2003).

[25] Alvaro E.Arenas, Benjamin Aziz and Gheorghe Cosmin Silaghi, *"Reputation Management in Collaborative Computing Systems"*, Security and Communication Networks, (2008), 1-18.

[26] Kamvar SD,Schlosser MT, Molina HG, *" The Eigen Trust Algorithm for Reputation Management in p2p Networks"*,In.Proc.12th International Conference on World Wide Web,Budapest,Bulgaria, (2003),640-651.

[27] Brain Shand, Nathan Dimmock and Jean Bacon, *"Trust for Ubiquitous, Transparent Collaboration"*, Wireless Networks, 10, (2004), 711-721.

[28] Cahill, Vinny, Brian Shand, Colin English and Macro Carbone, *"Using Trust For Secure Collaboration in Uncertain Environments"* IEEE, (2003).

[29] Xu Wu, "*A Distributed Trust Management Model For Mobile P2p Networks*", Springer, (2012).

[30] Seunghun Jin, Chanil Park, Daeseon Choi, Kyoil Chung, and Hyunsoo Yoon, *"Cluster-Based Trust Evaluation Scheme in an Ad Hoc Network"*, ETRI Journal, **27**(4), (2005).

[31] WWW.Wekipedia.Com