INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY (IJCET)

ISSN 0976 – 6367(Print)
ISSN 0976 – 6375(Online)
Volume 4, Issue 3, May-June (2013), pp. 359-369
© IAEME: www.iaeme.com/ijcet.asp
Journal Impact Factor (2013): 6.1302 (Calculated by GISI)
www.jifactor.com

IJCET

©IAEME

TRUST MANAGEMENT SCHEME FOR AD-HOC NETWORKS USING A SOCIAL NETWORK BASED APPROACH FOR SECURE ROUTING

M V Rathnamma*, Dr. P.Chenna Reddy**

*Research Schalor, JNTUA, Anantapur-AP-India.
** Assoc. Professor, JNTUCEP, Pulivendula-YSR-AP-India.

ABSTRACT

A social network is a social structure made up of actors which includes individuals or organizations. These actors are called "nodes", which are tied (connected) by one or more specific types of interdependency, such as friendship, information exchange, kinship, common interest, financial exchange, dislike, sexual relationships, or relationships of beliefs, knowledge or prestige.

Social Network analysis is the mapping and measurement of relationships (ties) and flows between the actors (nodes) in terms of network theory.

In this paper we propose a Trust Management Scheme for Ad-Hoc Networks using a Social Network Based Approach for secure routing.

Keywords: Trust Management, Social Network, Ad-Hoc Networks (MANETs), Attacks, Security**.**

1. INTRODUCTION

In social networks, trust can refer to a behavior that one person voluntarily depends on another person in a specific situation. Trust can also be an intention, that is, one party is willing to depend on the other party.

Mobile ad-hoc network’s special characteristics such as limited memory, battery power, and bandwidth can cause nodes to act selfishly (refuse to participate in routing and provide services to other nodes, for example). Trust management can help mitigate this selfishness and ensure the efficient utilization of network resources.

2. TRUST ESTABLISHMENT

Trust value of node Ni on node Nj is given by

$$T_{i,j} = \alpha.\mathrm{F}_{\mathrm{i,\,j}} + \beta.\mathrm{S}_{\mathrm{i,\,j}} \qquad (1)$$

In the above equation, Ti, j is evaluated as a function of two parameters:

- Direct Trust ($F_{i,\ j}$): NODE i's self evaluated trust on NODE j; i computes this by directly monitoring j.
- Indirect Trust ($S_{i,\ j}$): Weighted sum of other nodes' trust on NODE j evaluated by NODE i.

In eq. (1), α and β are weighting factors such that α + β = 1. Thus, by varying α and β, Node i can vary the weight of self evaluated direct trust vs. other nodes' trust in calculating its total trust on Node j. Here, $0 \leq \{T_{i,\ j},\ \ F_{i,\ j},\ \ S_{i,\ j}\} \leq 1$, and thus eq. (1) is normalized. α is the proportion of Direct Trust and β = 1 – α is the proportion of Indirect Trust [3, 4].

2.1 Evaluating Direct Trust (Fi. j)

NODE I computes this value by directly monitoring NODE j when NODE j is in its sensing range.

$$\mathrm{F}_{\mathrm{i,\,j}} = (\mathrm{w}_{\mathrm{sf}} \cdot \chi_{\mathrm{sf}} + \mathrm{w}_{\mathrm{fc}} \cdot \chi_{\mathrm{fc}} + \mathrm{w}_{\mathrm{l}} \cdot \chi_{\mathrm{l}} + \mathrm{w}_{\mathrm{pw}} \cdot \chi_{\mathrm{pw}})*\chi_{bl} \qquad (2)$$

Such that,

$$\sum_{i=sf,fc,l,pw} \mathrm{w}_{\mathrm{i}} = 1 \qquad (3)$$

χ_{bl} - Battery Life
χ_{l} - No. of links of the destination node
χ_{pw}- Packet Weightage Factor
χ_{fc}- Frequency of communication
χ_{sf} - Success Factor

2.2 Parameters

2.2.1 Packet Weightage Factor

This value indicates how successfully a highly secure or important data is transmitted. Higher the importance of the data to be transmitted, higher the trust needed by the nodes to transmit the packet. It takes a value in the range 1 to 10.

2.2.2 Success Factor

This is the factor which indicates the proportion of successful communication between two nodes. If the communication is successful through a node, then the trust value of that node increases. If there is a communication failure the trust value decreases.

2.2.3 Frequency of Communication

This indicates how often nodes communicate with each other. Higher value indicates that the nodes often communicate while lower value indicates that the nodes rarely communicate. Unlike the success factor this just counts how regularly the nodes communicate and doesn't bother to check if the acknowledgment is received or not.

2.2.4 Number of Links for the destination node

If the number of links for the destination node is higher, it indicates that there are multiple paths from it and hence the source node builds higher trust on it. It also implies the social relationship of the node in the network.

2.2.5 Battery life

If the link strength of a node falls below 10% of the total strength then the node cannot communicate with its neighbors and hence will leave the network. It takes a value 0 to 1.

Zero (0) indicates that the link strength is weak (below 10%) and the node will have to leave the network.

One (1) indicates that the link strength is strong (above 80%) and will be a part of the network.

Remaining values indicate link strength is between 10% and 80% and will continue to be a part of the network.

2.2.6 Decay of Trust

Trust value on a node should be reduced with respect to time. This is done so that if a node remains idle its trust value should be reduced and finally removed from the network. To implement it we exponentially decrease the Success Factor of the node. If a non-trusty node having negative trust value does not do any useful work, then it can be thrown out of the network over a period of time.

Procedure 1: Calculating Direct Trust of NODE i on NODE j after links have been established.

1: The NODE I sends a REQ_TRUST message to all its neighbors except NODE j, asking them to send their trust value parameters on NODE j.

2: Upon receiving the parameters NODE i computes each of the parameters average and calculates the Direct Trust using the formula (1).

2.3 Evaluating Indirect Trust (S_{ij})

The value of Si,j is the weighted average of Ti,x over all the nodes in the set O [5]. The weight associated with each Tx,j is Ti,x. O is the set of other nodes whose trust on j is utilized by i in evaluating its own trust on j.

$$S_{i,j} = \frac{\sum_{x \in o} T_{x,j} * T_{i,x}}{\sum_{x \in o} T_{i,x}} \qquad (4)$$

Where,
O is other = $\{ \forall N_{x\in}$ other $\Rightarrow \square T_{i,\,x}$, s.t.$T_{i,\,x} \square T_H\}$
Where, T_H is a threshold of trust [3].

Procedure 2:NODE i wants to establish indirect trust with NODE j

1: NODE i requests the nodes in NODE i'ssensing range for trust values about NODE j. (If NODE X is in NODE i's sensing range and has established direct trust in j, node X will send it's trust on Node j to NODE i.)

2: NODE i puts all received trust values in a buffer, and calculates indirect trust on NODE j using formula (3).

3. SOCIAL NETWORK MODEL

A social network is a social structure made up of individuals (or organizations) called "nodes", which are connected by one or more specific types of interdependency, such as friendship, kinship, common interest, financial exchange, dislike, or relationships of beliefs, knowledge or prestige.

Social network analysis views social relationships in terms of network theory consisting of nodes and ties (also called edges, links, or connections). Nodes are the individual actors within the networks, and ties are the relationships between the actors. The resulting graph-based structures are often very complex. Research in a number of academic fields has shown that social networks operate on many levels, from families up to the level of nations, and play a critical role in determining the way problems are solved, organizations are run, and the degree to which individuals succeed in achieving their goals [2, 11].

3.1 Assumptions in the model

- Each node should have a unique identification number.
- Direct wireless communication between two nodes is represented by a line joining the 2 nodes. Two nodes are said to communicate directly if the distance between them is less than a limit L, where L is the max sensing range of wireless network.
- Importance will be given to secure message passing (trust based communication) rather than fast message passing (shortest path communication). This is made because trust is the most important aspect in our model, a secure social trust approach. If time is given more importance, then it will be similar to a routing network.
- Each Node maintains Local trust table (LT) of its Neighboring Nodes.
- Each Node maintains a Global Service table (GS) of all the nodes.

3.2 Data structures used in the model

3.2.1 Local Trust Table (LT)

Table 1 shows the Local Trust Table, which is given below. This table is maintained by each Node with a record for each of its neighboring node in the network. Every time an operation is performed, this table is updated accordingly.

Table 1: Local Trust Table

N_i	**Pac wt Factor**	**Success Factor**	**Freq of Comm.**	**No. of Links**	**Bat Life**
N_{x1}	$\chi_{pw}(i, x1)$	$\chi_{sf}(i, x1)$	$\chi_{fc}(i, x1)$	$\chi_{l}(i, x1)$	0-1
N_{x2}	$\chi_{pw}(i, x2)$	$\chi_{sf}(i, x2)$	$\chi_{fc}(i, x2)$	$\chi_{l}(i, x2)$	0-1
..	..	..	..	..	..
N_{xj}	$\chi_{pw}(i, xj)$	$\chi_{sf}(i, xj)$	$\chi_{fc}(i, xj)$	$\chi_{l}(i, xj)$	0-1
..	..	..	..	..	..
N_{xk}	$\chi_{pw}(i, xk)$	$\chi_{sf}(i, xk)$	$\chi_{fc}(i, xk)$	$\chi_{l}(i, xk)$	0-1

In the above table,

- N_{xj} represents the Node xj and x1, x2, …,xj, … xk are the indexes of the neighbors of Node Ni such that xjis not equal to i.
- P (i, xj) represents the value of the parameter of Node i on Node xj. Where P = χ_{pw}or χ_{sf}or χ_{fc}or χ_{l}.
- 0-1 represents that the value lies between 0 and 1.

3.2.2 Global Service Table (GS)

Table 2 shows the Global Service table, which is given below. This table is maintained by all the nodes with a record of each node in the network.

Table 2: Centralized Global service table

	Parameter	Definition
1	Destination Node Id	Unique Id of the Destination node in the network
2	Service	Set of services provided by the node.

4. GENERAL OPERATIONS ON THE NETWORK

4.1 Node joining the network

If a node wants to establish link with another node, a handshake mechanism similar to the TCP-IP model is used. The initiating node sends a REQUEST to other nodes, which on receiving sends ACK and REQUEST. The first node sends ACK again. This is the handshake process. If a node wants to join the network, it broadcasts a HELLO message with a timer set. This message will contain the position of the node, its configuration and the number of neighbors (this value is 0 for new node joining the network). The nodes in the network which receive this message will broadcast it to all the members of the network. Every node will calculate the distance between the new node and itself. If it is less than the limit L (the max sensing range) then, the new node will become a neighbor of it. In such a case, it will acknowledge the new node with a message which will contain its service and node ID. The new node will update the data in its LT and GS tables.

The new node waits till the timer lapses. Now, the new node will come to know all its neighbors. The neighboring node will set the Success Factor, Packet Weightage factor and Frequency of communication of the new node to zero, but the same cannot be done by the new node. To find the trust parameters of a neighbor, the new node sends a REQ_TRUST message all its neighbors except the target node (node whose trust parameters are required). Upon receiving the values, the new node calculates the average and updates its LT table.

In the Figure 2 given below, node 16 wants to join the network, so it broadcasts HELLO message which will be received by node 11 and 7. Node 11 and 7 will then become neighbors of node 16.

4.2 Node leaving the network

If a node, say X wants to leave the network, it has to send a LEAVE message to all its neighbors. The neighbors will send an ACK to node X and X will acknowledge back. The neighbors on receiving this message will erase the X node's entry in GS and LT tables. It will also broadcast LEAVE message to all its neighbors, so that they can update their GS table. The node X can now safely leave the network.

In Figure 3 shown below, node 3 leaves the network. First it broadcasts LEAVE message to its neighbors 1, 6 and 5. Nodes 1, 6 and 5 break links with node 3 and delete its entries in LT table. Node 3 leaves the network.

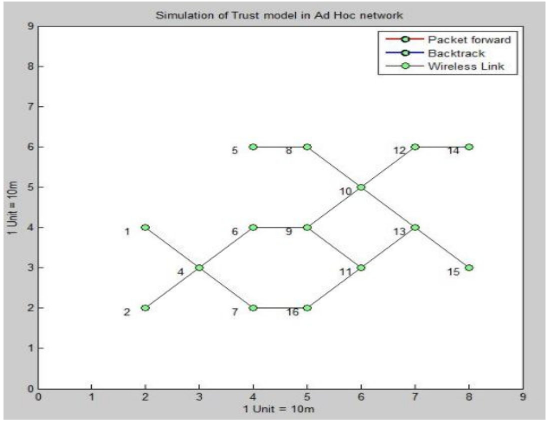

Figure 1: Node 3 left the network.

4.3 Communication between Nodes

Node X wants to communicate with node Y and it knows the type of service provided by node Y. Depending on the importance of the data, the source node (X) will forward the packet by considering only the trust values or both trust values and the packet weightage factor. The important of data is valued based on a scale and if the value is above a threshold value then, the nodes will consider the packet weightage factor of the node and the trust value to forward the data. If the importance is below the threshold then the nodes consider only the trust value. The source node will look-up its LT table and find the neighboring nodes with the highest trust value evaluated using the trust factors such as Battery life, Frequency of communication, No. of Links of neighboring node, Success Factor and Packet Weightage. The source node will append the selected neighbor node's Id and then send COMMUNICATE message to it. It sets a timer value to processing delay plus two times transmission delay. This message has fields like destination node Id, data and nodes reached till now. A node W which receives this message will first check if the destination node is its neighbor. If so, it sends the message to Y. If Y is not its neighbor, then node W will find a neighbor with the highest trust value which is not in the travelled list, and forwards the packet by appending the selected neighbor node's Id. This makes sure there will be no looping in the network. This procedure is followed till the message is received by node Y.

In case the message is received by a pendent node (a node with only one link), the message will be sent back (backtracked) if it is not the destination. When the node Y gets the message, it has to send ACK to node X. To do this, it simply sends the message to the last node (node Id) in the travelled list. This is a back-tracking procedure. Also the SUCCESS message is broadcasted by all the nodes in the list to its own neighbors when they get the ACK. This is done so as to tell the neighbors that the particular node has successfully forwarded the message.

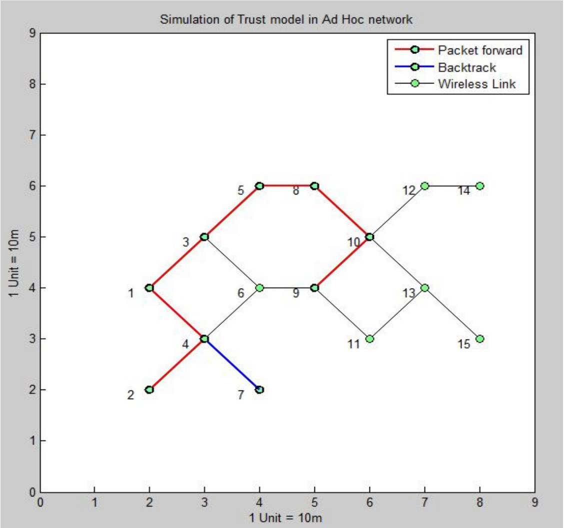

Figure 2: Node 2 wants to communicate with node 9

In the Figure 4 given above, node 2 wants to send a message to node 9. The travelled list is 2-4-7-4-1-3-5-8-10-9. Node 2 will forward the packet to node 4. Now node 4 will calculate its trust on node 1, 7, 6, since node 4 has maximum trust on node 7 packet is forwarded to node 7. Node 7 is a pendant node and no path to destination node 9, hence packet back tracked to node 4. Node 4 will again calculate its trust on node 1 and 6, and forwards the packet to maximum trust node. The packet is forwarded through path 4-1-3-5-8-10. After the packet reaches node 10 it checks if the destination node is its neighbor or not, if yes then it is forwarded to it. Now since node 9 is a neighbor of node 10 the packet is forwarded to the destination. After the packet reaches the destination, node 9 sends the ACK. Node 9 first forwards it to node 10, while broadcasting the SUCCESS message to node 6, 10 and 11. This SUCCESS message increases the Success Factor of 10 in its neighbor's LT Table. Node 10 sends the ACK to 8, while broadcasting the SUCCESS message to its neighboring nodes 5 and 10. Similarly the ACK is forwarded to 5, 3, 1, 4, and then 7.

When SUCCESS messages are sent, the Success Factor of the sending node in the neighbor's LT table increases.

4.4 Recommendation procedure to explore Service Providers

A node needs recommendation from other nodes when there is more than one node in the network providing the same service.

We assume that a node knows all service providers by its neighbor nodes. A node X wants a service A in the network. So, the node X broadcasts a RECOMMENDATION_SEEK message to its neighbors, which contains the sender node ID, service required. A node Y upon receiving this message will check if its neighbor provides the required service or not. If not, it will forward the message by attaching its ID in the travelled list. If its neighbor provides the service, then it attaches the trust value of the service provider and sends it back. If more than one node provides the service, then it will attach trust values of all the nodes.

Node X waits for a certain time to collect all RECOMMENDATION_SEEK messages. It will then calculate average of all values for a service provider and selects the best service provider node. It will then follow the communication procedure as mentioned above.

In the Figure 5 given below, say node 2 wants a service of Service Type A, so it sends the RECOMMENDATION_SEEK message to node 4. This node 4 will forward it to its neighbor and so on. Node 1 provides trust of node 4. Node 6 provides trust of 4. Node 7 provides trust of node 4. Node 14 provides trust of 12. Node 13 provides trust of 15.

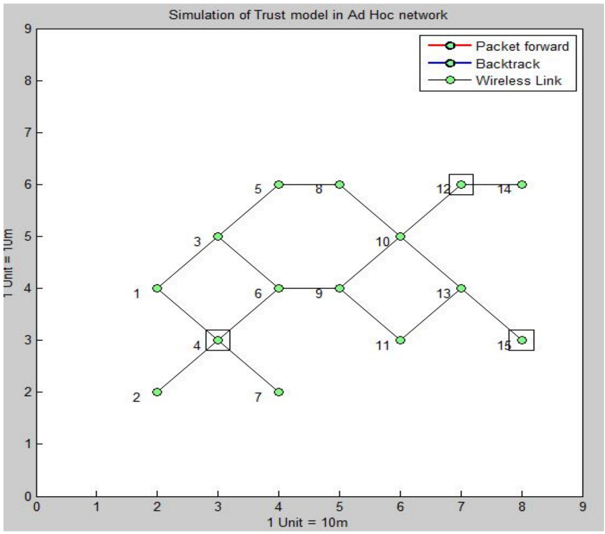

Figure 3: Request for Service Provider.

5. ATTACKS

The lack of central coordination and shared wireless medium in the wireless ad-hoc networks makes them vulnerable to attacks than wired networks. The attacks may be passive or active attacks. The passive attacks are caused by malicious nodes without disturbing the network operation. The active attacks disturb the operation. The attacks take place when routing the control information and data. We can neglect the link breakages, as the nodes are connected via WIFI and if a node wants to change its position, it has to inform other nodes.

5.1 Black Hole Attack

Black Hole is a node in the network which receives the packet but never forwards it the other nodes nor sends ACK to its sender. If a node X wants to communicate with a node Z, it sends a message to node Z. If the timer times out, but still the node X does not receive the acknowledgement for its message. So, X can deduce that something is wrong with either the destination node Z or any node in its path. In a social network, people ask the most trustful neighbors to do the same and so on. A similar approach is used here.

The source node X sends a QUERY packet to its most trust worthy neighbor. The node which receives this message should append its node Id in the Traveled List field of the QUERY packet and send a copy of it to its most trust worthy neighbor, and send ACK back to its sender. In this way, the source node will get to know the node which is untrustworthy.

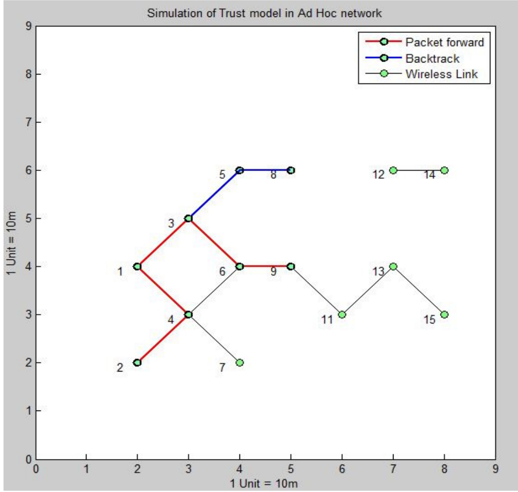

Figure 4: Eliminating a Black Node.

In the above Figure 6, say node 2 wants to send a message to node 9, but it does not get the acknowledgement from 4. So, it sends a QUERY packet to 4. Node 4 appends its node Id in the Travelled List and sends ACK to 2 and forwards it to node 1 also. Node 1 appends its ID and forwards QUERY packet to node 3 and acknowledges back to 4. Node 3 will send a QUERY packet to node 5 and ACK to node 4. Node 5 will send a QUERY packet to node 8 and ACK to node 3. Node will send QUERY packet to node 10. But in case node 10 fails to reply back to 8(the sender), then node 8 will generate PathError packet indicating problem in node 10 that is node 10 being a Black Node and sends it to all nodes. The neighboring nodes of node 10 will break links with node 10 and it will be removed from the network. Then node 2 will resend the message to node 9 through another path.

5.2 Ad-hoc Flooding Attack

In this attack a compromised node in the network generates random RREQ (Route Request Packet) to a Destination node which is not in the network or simply broadcasts messages.

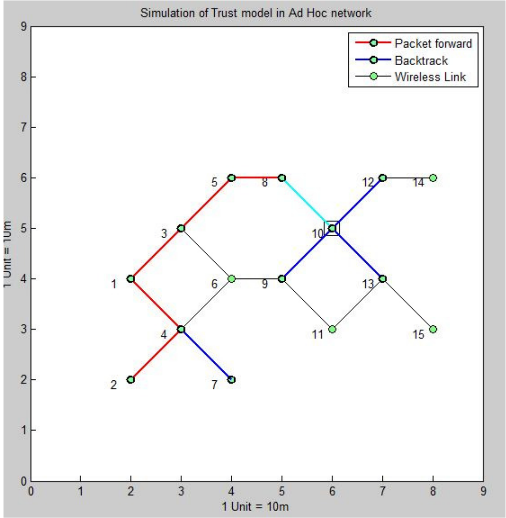

Figure 5: Flooding attack

All the nodes processes the request but no node will generate a RREP (Route Request Reply) since no node knows the Destination node or simply forwards the packet. Flooding RREQ packets in the whole network will consume a lot of resource of network. The intruder node consumes the network bandwidth.

Using social network approach, Frequency of Communication comes into picture. If a node X exceeds the limit of broadcasting the messages, for its neighbor say Y, the Frequency of Communication value increases and reaches close to 10. When it encounters such a situation, it keeps the packet sent by X and when it gets the next packet it cross checks to determine if it is the same packet or not. This process is repeated till a threshold value is reached and after which the node Y assumes that X is non-trusty and breaks the link. Even if the packet numbers are different and if the node occupies more bandwidth than a predetermined quantity, the same can be done. Y also broadcasts that X is non-trusty and a node Z (which is a neighbor of X) cross checks and takes necessary action. In the above Figure 6, node 10 is flooding packet.

6. CONCLUSION

In this paper, we have presented a social network mechanism for trust management and evaluation in mobile ad hoc networks by relating some features of nodes in MANET with social life. Our scheme is distributed, effective and storage-saving without reliance on any trustworthy party or centralized storage. No centralized infrastructure is required, although the presence of one can certainly be utilized. Also, users need not have personal, direct experience with every other user in the network in order to compute an opinion about them. They can base their opinion on second-hand evidence provided by intermediate nodes, thus benefitting from other nodes' experiences.

We have identified and presented the parameters on which trust depends in Social Network approach. A formula to evaluate trust using Frequency of communication, Number of links, Work done and Battery life of the node is presented. We then discussed how exactly these parameters determine the trust. The simulation results performed show that the proposed trust evaluation system can improve network throughput as well as help malicious node detection. Simulations are also performed to investigate various malicious attacks.

Ad-hoc networks are vulnerable to several kinds of possible attacks that have recently been classified as critical problems. Solution has been given to flooding and to eliminate non trusty node. Five types of other attacks are bad mouthing, on-off, conflicting behavior, Sybil, selective misbehavior and newcomer [6-9], for which solutions are yet to be found.

Public key and private key can be introduced in the network, so that a message intended to a particular node cannot be read by any other node.

7. REFERENCES

[1] Zheng Yan, Peng Zhang, TeemupekkaVertanen, “Trust Evaluation Based Security Solution in Ad Hoc Networks”, pp. 1-5.

[2] BhatTejas, MurugesanRajkumar, KottariSushan, K Chandrasekaran, “Trust Management In Ad-Hoc Networks: A Social Network Based Approach”,Network and Complex Systems, vol. 1, no.1, pp. 3-5, 2011.

[3] MohitVerendra, MurtuzaJadliwala, MadhusudhananChandrasekaran, ShambhuUpadhyaya, “Quantifying Trust in Mobile Ad-Hoc Networks,” IEEEInternational Conference on Integration of KnowledgeIntensive Multi-Agent Systems, Waltham, MA, USA, pp.65-70, 2005.

[4] Kun Wang, Meng Wu, SubinShen, “A Trust Evaluation Method for Node Cooperation in Mobile Ad Hoc Networks”, Fifth International Conference on Information Technology: New Generations, pp. 1000-1003.

[5] The weighted average definition,http://www.mathwords.com/w/weighted_average. htm.

[6] Yan Lindsay Sun and Yafei Yang, “Trust Establishment in Distributed Networks: Analysis and Modeling”,ICC 2007 proceedings**,** pp. 2-5.

[7] Yan Lindsay Sun, Zhu Han, Wei Yu and K. J. Ray Liu, “A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defence Against Attacks”, pp. 6-14.

[8] Abhay Kumar Rai, Rajiv RanjanTewari, Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET- Internet Communication”, International Journal of Computer Science and Security, Vol. 4: Issue 3, pp. 2-9.

[9] Po-WahYau, Shenglan Hu and Chris J. Mitchell,” Malicious attacks on ad hoc network routing protocols”, pp. 3-19.

[10] PriyankaGoyal, SahilBatra, Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hocNetworks”, International Journal of Computer Applications (0975 – 8887), vol. 9, no.12, pp. 2-4, November 2010.

[11] Yu,B., Singh,M.P., ”Searching Social Networks”, pp. 1-3, 2003.

[12] M. Ahmed, S. Yousef and Sattar J Aboud, “Bidirectional Search Routing Protocol for Mobile Ad Hoc Networks”, International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 1, 2013, pp. 229 - 243, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[13] Thaker Minesh, S B Sharma and Yogesh Kosta, “A Survey: Variants of Energy Constrained Reactive Routing Protocols of Mobile Ad Hoc Networks”, International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 3, Issue 2, 2012, pp. 248 - 257, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472.