Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol 1, No.1, 2011

Trust Management In Ad-hoc Networks: A Social Network Based Approach

Bhat Tejas (Corresponding author)
N.I.T.K. Surathkal, Karnataka, India.
Tel: +919743286276 E-mail: tejasmbhat@gmail.com

Murugesan Rajkumar
N.I.T.K. Surathkal, Karnataka, India.
Tel: +919742020255 E-mail: : rajthegreat1989@gmail.com

Kottari Sushan
N.I.T.K. Surathkal, Karnataka, India.
Tel: +919480123425 E-mail : sushanmilanista@gmail.com

K Chandrasekaran
N.I.T.K. Surathkal 575025
Karnataka, India.

Abstract

A social network is a social structure made up of individuals 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. There can be many kinds of ties between the nodes. 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.

We propose a social network based approach for trust management in ad-hoc networks, where nodes trust, help and interact with each other to create a complex trust-worthy network.

Keywords: Trust management, ad-hoc network, social network, attack.

1. Introduction

Trust is defined as an agent’s belief in attributes such as reliability, honesty and competence of the trusted agent. An Ad-hoc network consists of nodes called base stations which are not connected to a single access point. Mobile ad hoc networks have distinct characteristics, which make them very insecure like the lack of network infrastructure, no pre-existing relationships, unreliable multi-hop communication channels,

resource limitation; and node mobility. Users cannot rely on an outside central authority, like a trusted third party (TTP) or certificate authority (CA), to perform security and network tasks. The responsibility of networking and security is distributed among the network participants.

2. Social Network Model

The model uses a typical distributed approach, but it also makes use of the advantages in cluster and sensor based approach with the concepts of social network relationship. Memory is a limited quantity, so it is taken care of.

Figure 1 shows an ad-hoc network with nine nodes.

2.1 Assumptions in the model:

- Each node has a unique ID.
- Nodes which can directly communicate with each other are connected with a line.
- If two nodes are connected with a line, then the distance between them is less than a limit L, where L is the max sensing range of wireless network.
- Each Node maintains Trust Information table (TI) of its Neighbouring Nodes.
- Each Node maintains a Global Service table (GS).
- Each node knows its location details.

2.2 Tables used in the model:

2.2.1 Trust Information Table (TI):

Table 1 is maintained by each Node with a record for each of its neighbouring node in the network.

2.2.2 Global Service Table (GS):

Table 2 is maintained by each Node with a record for all the nodes in the network.

2.3 Parameters on which trust can be evaluated:

Trust is continuous value changing dynamically based on the condition of the nodes and infrastructural changes of the ad-hoc network. Trust value basically depends on the past experience of a node with another node. In addition to work experience Trust value also depends some of the parameters listed below.

- Work done by a Node (TW)
- Battery Life or Link Strength (TB)
- Number of Neighbor Links (TL)
- Response Time (TR)
- Frequency of Communication (TF) Decay over Time

2.3.1 Work done (TW):

Initially when a node joins a network, other's trust on it is 0. If the target node does some useful work, then other's trust on it increases and vice versa. It ranges between 1 and -1. 1 indicating the node can be fully trusted, and -1 indicating a non-trusty node.

2.3.2 Battery life (TB):

It is a boolean value 1 or 0.A node broadcasts it battery status if it is in a critical state (15%) to the neighbors. After going to critical state, if it recovers and gets charged up, then it sends its status to its neighbors. Just before selecting a node to send the packet, a source node should check the battery status(TB) of all its neighbors to choose the reliable node. Even if a node has a high trust factor, but if its battery life is

in critical status, it won't be chosen.

2.3.3 Number of links for a destination node (TL):

This factor shows how many neighbors a node has. It ranges from 0 to 1, 0 implies the target node has only one link, and 1 implies it has maximum number of links (say 10 links). It implies the social relationship of the node in the network. On evaluating trust this factor can also be used and assigned a certain amount of weightage.

2.3.4 Response time

Tells how busy a node is. After evaluating the trust values for all the neighbors, the source node selects the best trusted node and sends the packet. If a node responds quickly, say within 1ms then it can be given more weightage. This tells the amount of traffic a node is handling at that time. As the load on a node increases response time decrease, which intern decreases the number of tasks forwarded to it by decreasing trust value.

2.3.5 Frequency of communication (TF):

Depending on the frequency of communication the source node with the target node, the source node evaluates the Friendship factor in Trust evaluation. It ranges from 0 to 1, 0 indicating the node rarely communicates and 1 indicates the nodes often communicates. The value can be increased during communication accordingly.

2.3.6 Decay over time:

Trust needs to be reduced over time. Say every minute trust of a node (TW) reduces by 5%. This is done to eliminate the non-trusty nodes. 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.

2.4 Trust evaluation:

To evaluate trust, the source node has to calculate the below for every neighbor node and selects the node with highest trust value.

TB*(TW + TL+ TF + TR)*alpha

Alpha=a constant

2.5 General Operations:

Figure 2: Node 10 wants to join the network.

2.5.1 Node joining the Network

A hand-shake mechanism similar to tcp-ip is used. 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 to all the members of the network. Every node will calculate the distance between the new node and itself. If it is less than L, 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 TI 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 trust TW of the new node to zero, but the same cannot be done by the new node. To find the trust value of a neighbor, the new node sends a REQUEST_TRUST message to its neighbors except the target node. After receiving the trust values, it calculates the average of all the values for initial trust value TW. In the figure, node 10 wants to join the network, so it broadcasts HELLO message to node 4 and 5. Node 4, 5 and 9 will be neighbors of node 10.

2.5.2 Node leaving the network:

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

2.5.3 Communication between Nodes:

Figure 3: Node 10 wants to communicate with node 1.

Assumptions: Importance will be given to secure message passing rather than fast message passing. 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.

Node X wants to communicate with node Y and it knows the type of service provided by node Y. The source node (X) will look-up its TI table and finds the neighbor node with the highest trust value evaluated using the trust factors such as Battery life(TB), Frequency of communication(TF), Number of neighbors(TL), Work done(TW) in past and the nodes response time. 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, 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 and 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 the node Y.

In case the message is received by a pendent node (a node with only one link), the message will be sent back, if it is not for it. 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 name (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 neighbours that that particular node has successfully forwarded the message.

In the above figure, node 10 wants to send a message to node 1. The travelled list is 10-5-9-7-1. To send the ACK, node 1 has to send it to node 7, while broadcasting the SUCCESS message to node 2, 6, 7. Node 7 sends the ACK to 9, while broadcasting the SUCCESS message to node 1, 9 and 8. It is then sent to node 5 and 10.

SUCCESS messages are sent, so that neighbor's trust on that a node TW increases.

2.5.4 Recommendation procedure to explore Service Providers:

A node needs recommendation from other nodes in the following cases:

- If the node does not know which node provides the required service.
- If there are 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, node X broadcasts 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 (which includes TW, TB, TF, TL) 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.

Figure 4: Request for Service Provider.

Say node 10 wants some service A, so it sends the RECOMMENDATION_SEEK message to node 4, 5, 9. These nodes will forward to its neighbor and so on. Node 3 provides trust of node 2. Node 6 provides trust of 2 and 1. Node 7 provides trust of node 1.

2.5.5 Eliminating Enemy node in a suggested Path:

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 an acknowledgement back to its sender. In this way, the source node will get to know the node which is untrustworthy and the sending path can be deviated.

Figure 5: Eliminating node 1

Say node 10 wants to send a message to node 2, but it does not get the acknowledgement from 5. So, it sends a QUERY packet to 5. Node 5 appends its node_id in the Traveled_List and sends a ACK to 10 and forwards it to node 6 also. Node 6 appends its ID and forwards QUERY packet to node 1 and acknowledges back to 5. But in-case node 1 fails to reply back to 6(the sender). Now 6 will generates PathError packet indicating problem in node 1 and sends it to node 10(the Source Node).So node 10 can assume that node 1 does not forward the packets, so it will not further communicate with it. Now, the neighbors' trust (TW) on node 1 is reduced.

2.6 Attacks:

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.

2.6.1 Ad-hoc Flooding Attack:

Figure 6. Node 5 floods messages

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. All the node processes the request but no node will generate a RREP (Route Request Reply) since no node knows the Destination node or simply orwards 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, TF comes into picture. If a node X exceeds the limit of broadcasting the messages, for its neighbour say Y, the TF value increases and reaches close to 1. 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 5 times 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 neighbour of X) cross checks and takes necessary action.

2.6.2 Black hole attack:

A Wireless ad-hoc network is a temporary network and consists of mobile nodes moving arbitrary in the places that have no network infrastructure. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. Thus the nodes find a path to the destination node using routing protocols such as Ad hoc on-demand distance vector (AODV) routing, dynamic source routing (DSR) and Destination sequence vector routing (DSDV).

The lack of central coordination and shared wireless medium makes them vulnerable to attacks than wired

networks. The attacks may be passive or active attacks. The passive attacks 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. In ad hoc wireless networks each node acts as host as well as router.

One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. In this attack the malicious node exploits the routing protocol by advertising itself as possessing the shortest secure path to destination node to the Route Request message generated by the source node. As the reply from the malicious node reaches the source node earlier, it forwards the packets in the route suggested by the malicious node. Now the malicious node in the route intercepts the packets and drops it. After receiving the data packets the black hole may drop the packets selectively (leads to data loss) or intercept the packets (change destination ID, add its own information etc) and forward it to destination. Hence confidentiality of the message is disclosed in the presence of the black hole attack

3. Conclusion

The web enables users to get information, obtain services and communicate with others in new ways. As a consequence, it accesses not only the information and services but also people: who a user knows, trusts and stays in touch with. Some of the most exciting new activity on the web is social, with social networks and collaborative interaction. The open and decentralized nature of the web raises issues with respect to trust. A commonly used solution to tackle the problem of trust management is to build a "web of trust". In a "web of trust", each participant is allowed to express the degree of its trustworthiness in others. By doing so, a participant helps the other in deciding which participants are to trust or to distrust, without prior interaction. This exact approach we have used in our model.

In this report we maintain a information table for every node with respect to its neighbouring nodes which contains important parameters such as destination node and factors on which trust depends on like trust value(-1,1), frequency of communication, number of links, battery life of the node. We then discuss how exactly these parameters determine the trust. Upon completion of this we compute the trust and select the node with the highest trust value.

General operations which are also discussed for such nodes are joining and leaving the network. Joining the network has a mechanism similar to TCP/IP. A hello message is broadcasted from the new node to all the current nodes and nodes which are in close proximity to it(d<L) become its neighbors after the timer is set. Communication between nodes relies on secure transmission rather than fast transmission as discussed earlier.

In conclusion this paper uses the advantages of a social network and the "web of trust" to effectively manage trust in a network as shown in our model.

References

Tao Jiang and John S. Baras, “Trust Evaluation in Anarchy: A Case Study on Autonomous Networks”,2-8.

Seunghun Jin, Chanil Park, Daeseon Choi, Kyoil Chung, and Hyunsoo Yoon (2005), “Cluster-Based Trust Evaluation Scheme in an Ad Hoc Network”, *ETRI Journal*, 465-468.

Chunhung Richard Lin and Mario Gerla (2006),“Adaptive Clustering for Mobile Wireless Networks”, 4-8.

Junbeom Hurt, YounhoLeet, HyunsooYoont, DaeseonChoit and SeunghunJ, “Trust Evaluation Model for Wireless Sensor Networks”, 491-494.

Elmar Schoch, Michael Feiri, Frank Kargl, Michael Weber ,“Simulation of Ad Hoc Networks:ns-2 compared to JiST/SWANS”,39-48.

Yonglin Ren and AzzedineBoukerche (2008),“Modeling and Managing the Trust for Wireless and Mobile Ad hoc Networks”, 2129-2133.

Dawoud D.S., Richard L. Gordon, Ashraph Suliman1 and Kasmir Raja S.V.,"Trust Establishment in Mobile Ad HocNetworks: Key Management.", 151-161

Zheng Yan1, Peng Zhang and Teemupekka Virtanen,"Trust Evaluation Based Security Solution in Ad Hoc Networks", 1-5.

Anand Patwardhan, Jim Parker, Michaela Iorga and Tom Karygiannis (2005),"Secure Routing and Intrusion Detection in Ad Hoc Networks", 1-3

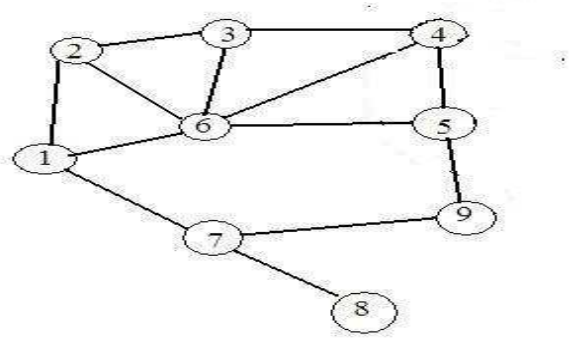

Figure 1: An ad-hoc network with nine nodes.

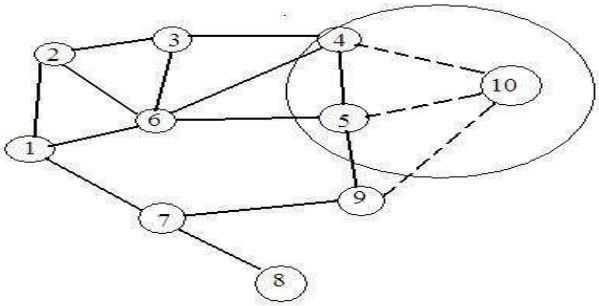

Figure 2: Node 10 wants join the network.

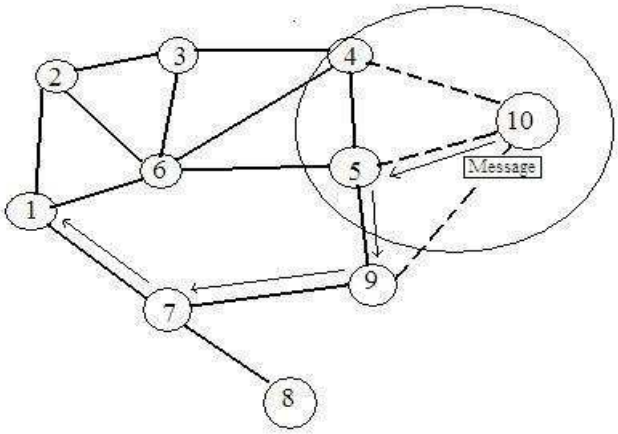

Figure 3: Node 10 wants to communicate with node 1.

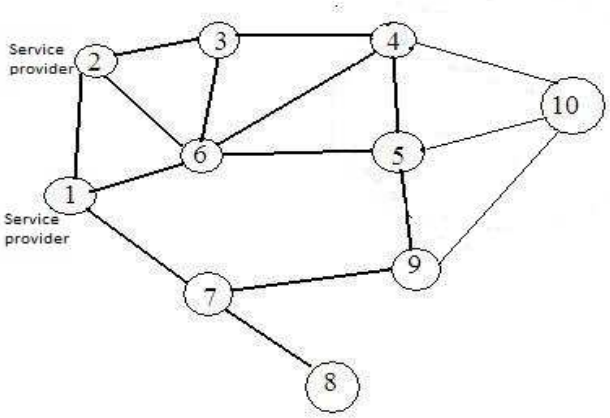

Figure 4: Request for Service Provider.

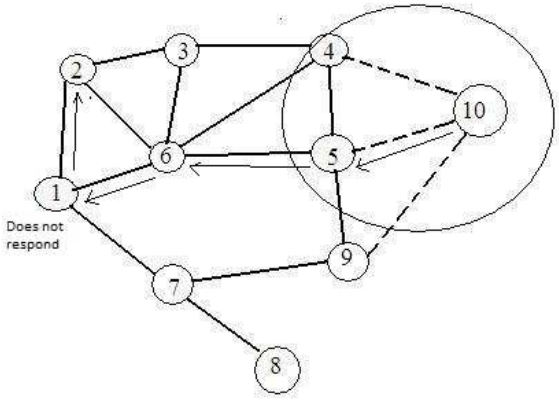

Figure 5: Eliminate node 1

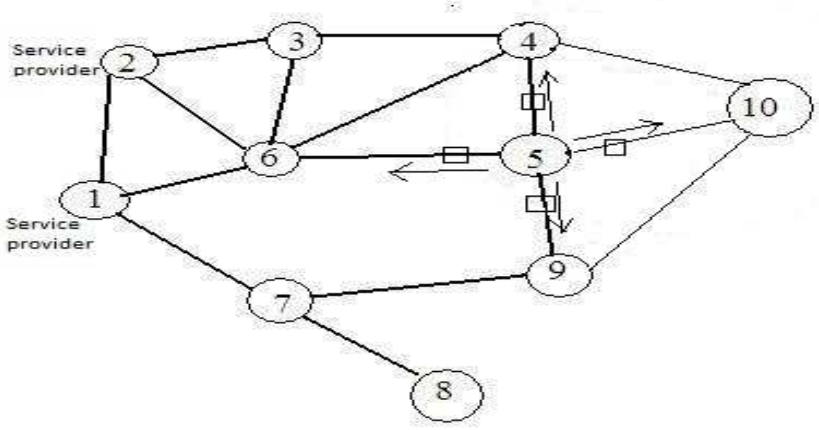

Figure 6. Node 5 floods messages

Table 1. Trust information table (TI)

	Parameter	Definition
1	Destination Node Id (DnId):	Unique Id of the Destination node's in the network
2	Trust Communication (TW):	Continues value between -1 to +1. Implies how successfully a node communicates and works in a network.
3	Frequency of communication (TF)	Number of times the destination node communicates with the source node.
4	Number of Links(TL)	Degree of Friendship-ness of a node
5	Battery Life (TB)	Strength to support future task request by the node
6	Position	Location x,y.

Table 2. Global service table(GS)

	Parameter	Definition
1	Destination Node ID (DnId)	Unique Id of the Destination node's in the network
2	Service	Set of services provided by the node.