Trust Based Security Routing in Mobile Adhoc Networks

K.Seshadri Ramana
Associate Professor of Dept of MCA
G.Pulla Reddy Engineering College
Kurnool-518007
A.P., India.

Dr. A.A. Chari
Professor Dept of OR&SQC
Rayalaseema University
Kurnool-518007
A.P., India

Prof. N.Kasiviswanth
Head Of the Department of CSE
G.Pulla Reddy Engineering College
Kurnool-518007
A.P., India

Abstract: Ad hoc networks are widely used in military and other scientific areas. With nodes which can move arbitrarily and connect to any nodes at will, it is impossible for Ad hoc network to own an fixed infrastructure. It also has a certain number of characteristics which make the security difficult. Routing is always the most significant part for any networks. One way is to transplant ordinary mechanisms in common networks with some improvement while the other way is to find some other factors such as trust to achieve the objective. This paper gives an overview about trust in MANETs and current research in trust based routing.

Key Words: Ad hoc Networks, Trust path

1. Introduction

Mobile Ad hoc Networks are self-organized, temporal networks which consist of a set of wireless nodes. The nodes can move in an arbitrary manner and work as its own opinions[7. They may join or leave the network without no restrictions. Therefore, Ad hoc networks' topologies are dynamic and costly to maintain. Furthermore, wireless channels make the routing and message transmission much more challenging. Nodes of these networks can function as routers that discover and maintain routes to other nodes as well as end-users. They will rely other nodes to relay the messages, which are exposed in an open dangerous situation for any intermediate nodes are able to destroy the integrity or choose as their like to deal with the messages. Last but not least, nodes in ad hoc networks have only limited resource, i.e. Battery power, bandwidth and cpu power. They are usually embedded systems which are produced for certain fixed tasks.

The situation in ordinary networks such as Internet is totally different. There fixed topology of a tremendous number of nodes which are s pre-configured the connections. The routing service is provided by certain Organizations with authority. The users trust them to pass the messages.

Moreover, entities in such networks are powerful and have enough Computational ability. Therefore complicated cryptographic mechanisms can be deployed. And Public Key Infrastructure (PKI) is easily to constructed.

Therefore, it is impossible to transplant the common routing protocols and security infrastructure to MANETs due to above reasons. Trust is recently introduced to solve this problem and used in existing protocols for ad hoc networks to improve security.

The rest of this report will be organized as follows: Section 2 will give an overview about the outing protocols in MANETs and Trust definition and mechanisms will be proposed in Section 3.

In section 4, two routing protocols in research will be presented. Lastly, my preliminary idea to solve certain problems will be discussed.

2. Routing Protocols in MANETs

Existing routing protocols can be classified into mainly two types- proactive routing protocols and reactive routing protocols [7]. Proactive routing protocols such as Destination-Sequenced Distance-Vector Routing (DSDV)[5] maintain routing information all the time and always update the routes by broadcasting update messages. Due to the information exchange overhead, especially in volatile environment, proactive routing protocols are not suitable for ad hoc networks [7]. However, reactive routing is started only if there is a demand to reach another node. Currently, there are two widely used reactive protocols- Ad-hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) which will be

discussed later. But they all suffer from the high route acquisition latencies [7]. That is, messages have to wait until a route to destination has been discovered. Normally, reactive routing protocols include two processes- route discovery and route maintenance.

2.1 Dynamic Source Routing

DSR is a source rooting in which the source node starts and take charge of computing the routes [9].

At the time when a node S wants to send messages to node T, it firstly broadcasts a route request (RREQ) which contains the destination and source nodes' identities. Each intermediate node that receives RREQ will add its identity and rebroadcast it until RREQ reaches a node n who knows a route to T or the node T. Then a reply (RREP) will be generated and sent back along the reverse path until S receives RREP. When S sends data packets, it adds the path to the packets' headers and starts a stateless forwarding [9].

During route maintenance, S detects the link failures along the path. If it happens, it repairs the broken links. Otherwise, when the source route is completely broken, S will restart a new discovery.

2.2 Ad-hoc On-demand Distance-Vector

It is similar to DSR when RREQ is broadcast over the network. When either a node knowing a route to T or T itself receives RREQ, it will send back RREP. The nodes receiving RREP add forward path entries of the destination T in their route tables.

According to [9], there are many differences between DSR and AODV. Firstly, destination T in DSR will reply to all RREQ received while T in AODV just responds to the first received RREQ. Secondly, every node along the source path in DSR will learn routes to any node on the path. But in AODV, intermediate nodes just know how to get the destination.

3. Trust Mechanisms

There is a common assumption in the routing protocols that all nodes are trustworthy and cooperative[4]. However, the fact is different. Malicious nodes can make use of this to corrupt the network. A lot of attacks such as man-in-the-middle, black hole, DoS may be deployed to destroy the network. As we discussed above, the nodes in MANETs are not as powerful as desk PCs and there is no fixed infrastructure. It is difficult to establish PKI. Even if PKI is in use, it is also needed to make sure the nodes are cooperative. Furthermore, sometimes other factors such as reliability and bandwidth are included in the route discovery besides the shortest path. Trust is introduced to solve the problems.

However, there is no clear consensus on the definition of trust. Commonly, it is interpreted as reputation, trusting opinion and probability [4]. Simply, we can consider it as the probability that an entity performs an action as demanded.

3.1 Trust Properties

According to [2, 6], there are four major properties of Trust:

• Context Dependence

The trust relationships are only meaningful in the specific contexts [6].

• Function of Uncertainty

Trust is an evaluation of probability of if an entity will perform the action.

• Quantitative Values

Trust can be represented by numeric either continuous or discrete values.

• Asymmetric Relationship

Trust is the opinion of one entity for another entity. That is, if A trusts B, it is unnecessary to hold that B trusts A.

3.2 Trust classification and computation

Trust is extracted from social relationship. When we have some interactions with somebody, although not so much, a general opinion will be formed. However, if somebody is completely new for us and we have to do business with him, what should we do? Perhaps, there are some friends of ours knowing him. Then we collect their opinions. From the information gathered, we get our own choice. It is the same in MANETs.

The trust in MANETs can be classified into two -First-hand trust and recommendation. Sometimes, when there is not enough first-hand evidence, recommendation should be taken into consideration, too. The combination of the two will be the final trust. Of course, there are several

methods to concatenate the two types of trust. One of them will be discussed in the following sections.

3.3 Trust representation

There are some different representations of trust. Basically, they can be divided into two categories- continuous and discrete numbers. It is also probable that different ranges can be adopted. There are two examples.

• In [2], the trust value is a continuous real number in [-1, +1] where -1 denotes completely no trust, 0 complete uncertainty, +1 complete trust respectively.

• In [1], trust values are represented in discrete levels "V.high", "High", "Mid" and "Low" which are in a decreasing order of trust.

There is some debate on the representations. The author of [8] argue that although discrete values are simple, straightforward and easier to represent categories, they are not suitable to be used in ad hoc networks because the dynamic topology. Continuous values make it easier to compare two entities.

4. Current Research Work

In this section, two trust based routing protocols are presented. Each of them makes use of different trust quantification and embedded trust in different context. The goals that two of them intend to achieve are also not the same.

4.1 Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks

This protocol is described in [2]. It provides a complete framework from trust evaluation to trust routing. In order to have a good understanding of trust, the whole general idea of this paper will be discussed as following.

4.1.1 Trust Evaluation

T {subject: agent, action} is used to denote the trust value that subject has for action with regard to agent. Similarly, P {subject: agent, action} denotes the probability subject estimate if agent will perform action correctly.

In order to get a correct comprehensive trust, both first-hand and second-hand evidence should be considered. Therefore, we need to concatenate the trust. Two contexts exist in this situation. One is whether another node will transmit the packet correctly while the other is whether it will give a good recommendation. The respective trust values are presented as T {subject: agent, transmit} and T {subject: agent, recommend}.

The simplest model of concatenation trust is shown in figure 1.The final trust is

T (A: C, action) = RAB TBC

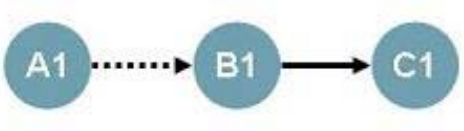

Figure 1: Concatenation trust propagation

If there is more than one recommendations, just like the situation shown in figure 2. The final trust is

$T \{A: C, action\} = w1 (R_{AB} T_{BC}) + w2 (R_{AD} T_{DC})$

Where

$w1 = R_{AD} / R_{AB}+R_{AD,}$
$w2 = R_{AB} / R_{AB}+R_{AD}$

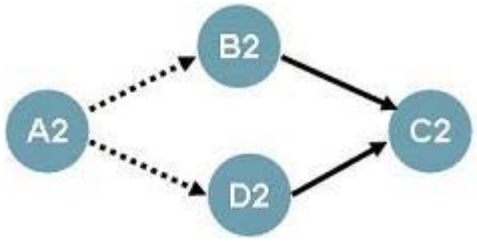

Figure 2: combining multiple recommendations.

Now, assume that A is going to evaluate the first-hand trust of B. suppose A requires B to perform the action N times while B actually performs k times. There is a common approach in probability from which we get

P {A: B, action} = k/n

Then according to this paper, using bayesian method, at last we get

P {A: B, action} = k+1/n+2

From P {A: B, action} we can get the corresponding trust values through the entropy formula.

4.1.2 Trusted routing

The routing process can be summarized into the following steps:

1. Route discovery: it is just like the route discovery in DSR. Suppose A starts this process to communicate with D. At the end, A collects all the available routes to D;

2. Validate routes: Node A check the trust values of the intermediate nodes along the path. Assuming node B's trust value is missing in A's trust table or its trust values is below a certain threshold, put B into a set X;
3. During the transmission, node A updates its trust table based on the observations. When some malicious behavior is found, A will discard this path and find another candidate path or restart a new discovery.
4. Compute trust values for every node in X based on the trust graph.
5. Among all paths, A chooses the one with the max $(\Pi_{i}^{n}{}_{=1}p_i)$ where n is the number of nodes along with path.

h	High	Medium	Low
9,10	Medium encryption	low encryption	no encryption
6,7,8	high encryption	medium encryption	no encryption
2,3,4,5	high encryption	high encryption	no encryption
0,1	--	--	--

Table 1: Security level description

4.2 Trust Based Adaptive On demand Ad Hoc Routing Protocol

This section gives a general analysis of [3]. This paper aimed to hide the source node's identity from intermediate nodes in route discovery. There is an assumption that there are well-defined cryptographically mechanisms and each node has several mechanisms to choose. It is certain that different mechanisms have different complexity and consume different amount of power. Therefore, trust is introduced to determine which mechanism to use. The discipline is that if the next node is more trustworthy, a simpler method will be choosing. Of course the choice is also based on the security level demanded by the application. As is shown in table 1, the security level and the trust levels cooperate to decide the encryption policy.

The protocol proposed is based on AODV as we discussed above. In order to give a more detailed example of routing in MANETs, the route discovery process will be described as follows

1. Source S wants to communicate with node D. It broadcasts the request message RREQ.

RREQ includes the level of security it requires and D's id, a sequential number and S's id encrypted by D's public key. RREQ is like this :{ RREQ, seqnum, Pb D [Si d], Di d, SL}

2. Node A receives RREQ. It looks up its trust list for the trust values of the neighbors. And A will encrypt if own id with proper policy and append in the message. The message which will sent by A is like this:{RREQ, seqnum, Pb D[Pv A[Aid], Pb D[Sid], Did , SL} where Pv A is the private key of A

3. D receives RREQ. It uses its private key and the public key of the intermediate nodes to authenticate them. D checks if there are any bad nodes. If they are all trusted, D generates
a number for the flow Fid , and broadcasts the following message(suppose A and B are the intermediate nodes): {RREP,Pb B[Fid , Pb A[Fid , Pb S[Pv D[Fid]]]]};

4. Intermediate node that receives the RREP uses its private key to decrypt the message and gets the flow id. Then it updates its route table with Fid designated to destination D;

5. S receives RREP, uses its private key to decrypt the message and D's public key to identify the destination. Afterwards, it will send message with the flow id Fid.

Thus, the intermediate nodes will never know who the source is and just pass data according to Fid.

5. Trusted Path Selection

I find that the path selection in the above document is not convincing in some situations. Let us see an extreme example in figure 3. There are two paths and the trust of either path equals 0.216. However, it is easy for us to choose the former one. For the node with trust 0.3 is more likely to break sometime later. Therefore, we have to find some methods to choose the better path automatically.

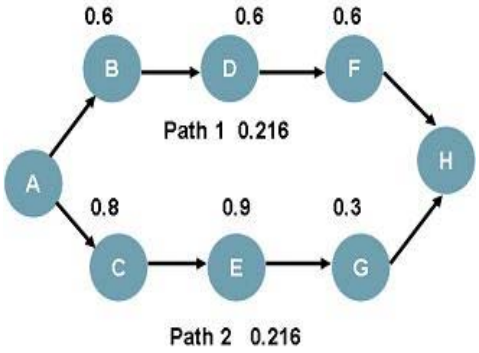

Figure 3: An extreme example

Firstly, suppose Ti is the ith node's trust value along the path. Then the initial trust value of the path is computed as:

$$T' = \frac{1}{n}\sum_{i=1}^{n} T_i$$

A parameter that can reflect the fluctuation of the trust values need to be introduced. Let σ2 denote the variant:

$$\sigma^2 = \frac{1}{n}\sum_{i=1}^{n} (T_i - T')^2$$

Last we can combine the two above parameters together to show the trust of the path. The lengths of paths are also taken into consideration. What we want to get is the one with fewer nodes and bigger trust value. The final path trust is like follows:

$$T = T' - \mu \frac{n}{hop_max}\sigma^2$$

Where hop max is the maximal number of hops among all available paths. μ is a punishment factor. Finally, we will choose the path with the biggest path trust value.

6. Conclusion

Although trust is widely researched nowadays, there is not a consensus and systematic theory based on trust. Trust has some specific and unique characteristics but not all research respects these basic properties. Furthermore, the trust establishment methods are not so convincing and based on similarities to social networks, more effective mechanisms should be implemented. The trust combination methods are various and lack comparison among them.

References

[1] L.Abusalah, A.Khokhar, "TARP:Trust-Aware Routing Protocol", IWCMC'06, July 3-6, 2006, ACM 2006, pp135-140

[2] Yan L. Sun, Wei Yu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks", 2006 IEEE, pp305-317

[3] Rajiv k. Nekkanti, Chung-wei Lee, "Trust Based Adaptive On Demand Ad Hoc Routing Protocol", ACMSE '04, April 2-3,2004, ACM 2004, pp88-93

[4] Mike Just, Evangelos Kranakis, "Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks", IN proceeding of ADHOC-NOW 2003,pp151-163

[5] Charles E. Perkins, Pravin Bhagwat, "Highly dynamic Destination-Sequenced Distance-Vector routing(DSDV) for mobile computers", pages 234-244, In proceeding of the SIGCOMM '94 Conference on Communications Architectures

[6] Marc Branchaud, Scott Flinn,"x Trust: A Scalable Trust Management Infrastructure"

[7] Jigar Doshi, Prahlad Kilambi, "SAFAR:An Adaptive Bandwidth-Efficient Routing Protocol for Mobile Ad Hoc Networks", Proceeding of ADHOC-NOW 2003, springer 2003, pp12-24

[8] A.A Pirzada, C. Mcdonald,"Trusted Route Discovery with TORA Protocol", 2004 IEEE

[9] P Narayan, V R. Syrotiuk,"Evaluation of the AODV and DSR Routing Protocols Using the MERIT Tool", InIn proceeding or ADHOC-NOW 2004, pp25-36