New trust based security method for mobile ad-hoc networks

Renu Mishra renutrivedi@rediffmail.com
Sr.Lecturer/ GCET/CSE
Gr Noida, 201306, India

Inderpreet Kaur kaur.lamba@gmail.com
Sr.Lecturer/ GCET/CSE
Gr Noida, 201306, India

Sanjeev sharma sanjeev@rgtu.net
School of IT
RGTU Bhopal
Bhopal,422001, India

Abstract

Secure routing is the milestone in mobile ad hoc networks .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 a 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. We design a trust based packet forwarding scheme for detecting and isolating the malicious nodes using the routing layer information. This paper gives an overview about trust in MANETs and current research in routing on the basis of trust. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node will be punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious.
.

Keywords: MANETs, MAC-Layer, Security Protocol, Trust
.

1. INTRODUCTION

Trust management is a multifunctional control mechanism, in which the most important task is to establish trust between nodes who are neighbors and making a routing path. In general, trust management is interchangeably used with reputation management. However, there are important differences between trust and reputation. Trust is active while reputation is passive. We propose a Trust based forwarding scheme in MANETs without using any centralized infrastructure. This scheme presents a solution to node selfishness without requiring any pre-deployed infrastructure. It is independent of any underlying routing protocol. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. Each intermediate node marks the packets by adding its unique hash value and then forwards the packet towards the destination node. The destination node verifies the hash value and check the trust counter value. If the hash value is verified, the trust counter is incremented, other wise it is decremented. If the trust counters value falls below a predefined

trust threshold, the corresponding the intermediate node is marked as malicious. In this paper, we study about trust mechanism in the ad hoc networks and propose a trust evaluation based security solution. The rest of the paper is organized as follows. Section two discusses the routing protocol in the ad hoc networks. Section three presents the Trust mechanism. In section four, a trust evaluation based solution for the ad hoc networks is proposed. In the next section the conclusions and directions of future work are given in the last section.

2. ROUTING PROTOCOLS IN MANETs

In the ad hoc networks, routing protocol should be robust against topology update and any kinds of attacks. Unlike fixed networks, routing information in an ad hoc network could become a target for adversaries to bring down the network. 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.

In this paper, we propose to design a Trust-based Security protocol (TMSP) based on a MAC-layer, approach which attains confidentiality and authentication of packets in routing layer and link layer of MANETs, having the following objectives:

- *Attack-tolerant* to facilitate the network to resist attacks and device compromises besides assisting the network to heal itself by detecting, recognizing, and eliminating the sources of attacks.
- *Lightweight* in order to considerably extend the network lifetime, that necessitates the application of ciphers that are computationally efficient like the symmetric-key algorithms and cryptographic hash functions.
- *Cooperative* for accomplishing high-level security with the aid of mutual collaboration/cooperation amidst nodes along with other protocols.
- *Flexible* enough to trade security for energy consumption.
- *Compatible* with the security methodologies and services in existence.
- *Scalable* to the rapidly growing network size.

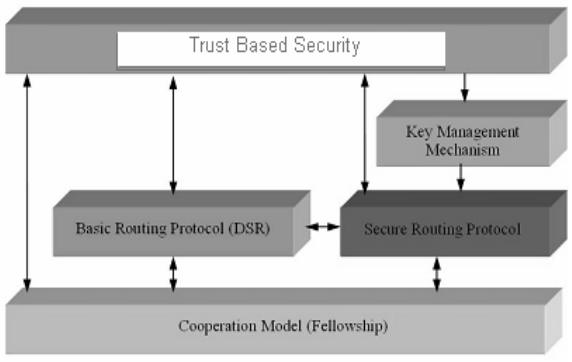

FIGURE 1: Security at different levels

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. Some- times, 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 continuous, trust values are represented in discrete levels ”V.High”, ”High”, ”Mid” and ”Low” which are in a decreasing order of trust.

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

4. PROPOSED SCHEME (TRUSTED ROUTING):

In our proposed protocol, by dynamically calculating the nodes trust counter values, the source node can be able to select the more trusted routes rather than selecting the shorter routes.

The routing process can be summarized into the following steps:

1. Discovery of routes: 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. Validation of 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 (□in=1pi) where n is the number of nodes along with path.

Our protocol marks and isolates the malicious nodes from participating in the network. So the potential damage caused by the malicious nodes are reduced. We make changes to the AODV routing protocol. An additional data structure called Neighbors’ Trust Counter Table (NTT) is maintained by each network node.

Let {Tc1, Tc2…} be the initial trust counters of the nodes {n1, n2…} along the route R1 from a source S to the destination D. Since the node does not have any information about the reliability of its neighbors in the beginning, nodes can neither be fully trusted nor be fully distrusted. When a source S wants to establish a route to the destination D, it sends route request (RREQ) packets. Each node keeps track of the number of packets it has forwarded through a route using a forward counter (FC). Each time, when node n_k receives a packet from a node ni, then n_k increases the forward counter of node n_i

FCni = FCni + 1, i=1, 2…… (1)

Then the NTT of node nk is modified with the values of FCni . Similarly each node determines its NTT and finally the packets reach the destination D. When the destination D receives the accumulated RREQ message, it measures the number of packets received Prec. Then it constructs a MAC on Prec with the key shared by the sender and the destination. The RREP contains the source and destination ids, The MAC of Prec, the accumulated route from the RREQ, which are digitally signed by the destination. The RREP is sent towards the source on the reverse route R1.Each intermediate node along the reverse route from D to S checks the RREP packet to compute success ratio as,

SRi = FCni / Prec (2)

Where Prec is the number of packets received at D in time interval t1. The FCni values of ni can be got from the corresponding NTT of the node. The success ratio value SRi is then added with the RREP packet.

The intermediate node then verifies the digital signature of the destination node stored in the RREP packet, is valid. If the verification fails, then the RREP packet is dropped. Otherwise, it is signed by the intermediate node and forwarded to the next node in the reverse route. When the source S receives the RREP packet, if first verifies that the first id of the route stored by the RREP is its neighbor. If it is true, then it verifies all the digital signatures of the intermediate

nodes, in the RREP packet. If all these verifications are successful, then the trust counter values of the nodes are incremented as

$$Tci = Tci + \delta 1 \quad (3)$$

If the verification is failed, then

$$Tci = Tci - \delta 1 \quad (4)$$

Where, δ1 is the step value which can be assigned a small fractional value during the simulation experiments. After this verification stage, the source S check the success ratio values SRi of the nodes ni. For any node nk, if SRk < SRmin, where SRmin is the minimum threshold value, its trust counter value is further decremented as

$$Tci = Tci – \delta 2 \quad (5)$$

Which involve regulation of transmission by a centralized decision maker? A distributed access protocol makes sense for an ad-hoc network of peer workstations. A centralized access protocol is natural for configurations in which a number of wireless stations are interconnected with each other and some sort of base station that attaches to a backbone wired LAN.

For all the other nodes with SRk > SRmin, the trust counter values are further incremented as

$$Tci = Tci + \delta 2 \quad (6)$$

Where, δ2 is another step value with δ2 < δ1. For a node nk, if Tck < Tcthr,

where Tcthr is the trust threshold value, then that node is considered and marked as malicious.

If the source does not get the RREP packet for a time period of t seconds, it will be considered as a route breakage or failure. Then the route discovery process is initiated by the source again.

The same procedure is repeated for the other routes R2, R3 tc and either a route without a malicious node or with least number of malicious nodes, is selected as the reliable route.

Which involve regulation of transmission by a centralized decision maker. A distributed access protocol makes sense for an ad-hoc network of peer workstations. A centralized access protocol is natural for configurations in which a number of wireless stations are interconnected with each other and some sort of base station that attaches to a backbone wired LAN. The DCF sub layer makes use of a simple CSMA (carrier sense multiple access) algorithm. The DCF does not include any collision detection function (i.e. CSMA/CD). The dynamic range of the signals on the medium is very large, so

that a transmitting station cannot effectively distinguish incoming weak signals from noise and the effects of its own transmission. To ensure smooth and fair functioning of the algorithm, DCF includes a set of delays that amounts a priority scheme.

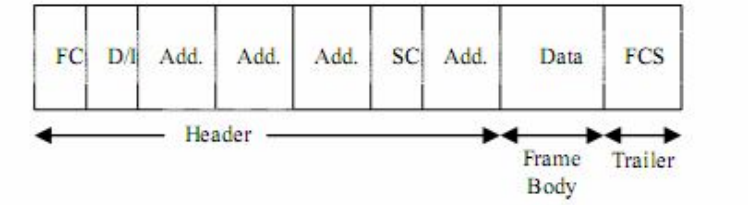

Figure 2: MAC frame format

FC- frame Control,
SC- sequence Control,
Oct. - Octets D/I-duration/connection control,
FCS-frame checks sequence.

Frame control indicates the type of frame and provides control information. Duration/connection ID indicates the time the channel will be allocated for successful transmission of a MAC frame. Address field indicates the transmitter and receiver address, SSID and source & destination address. Sequence control is used for fragmentation and reassembly.

5. CONCLUSION

In this paper, we have proposed a trust based security protocol which attains confidentiality and authentication of packets in both routing and link layers of MANETs. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. A node is punished or rewarded by decreasing or increasing the trust counter. If the trust counter value falls below a trust threshold, the corresponding intermediate node is marked as malicious Although trust is widely researched nowadays, there is not a consensus and systematic theory based on trust. The proposed solution tries to simulate human being's social contact procedure on decision-making and introduces it into the ad hoc networks. The perfect security solution is hard to reach. But the average security level (for a node) can be achieved as expectation based on accumulated knowledge and as well as the trust relationship built and adjusted. With this way, it could greatly reduce security threats.

6. REFERENCES

FOR JOURNALS: [1] Rajneesh Kumar Gujral, anil kumar kapil, "*A Trust Conscious Secure Route Data Communication in MANETS",* International Journal of Security (IJS**)** Volume: 3 Issue: 1,Pages: 9 – 15, 2009

FOR CONFERENCES: [1] 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

[2] Farooq Anjum,Dhanant Subhadrabandhu and Saswati Sarkar "*Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols*" in proceedings of IEEE 58th Conference on Vehicular Technology, 2003.

[3] Rajiv k. Nekkanti, Chung-wei Lee, "*Trust Based Adaptive On Demand Ad Hoc Routing Protocol",* ACMSE '04, April2-3,2004, 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] L.Abusalah, A.Khokhar,"*TARP:Trust-Aware Routing Protocol*", IWCMC'06, July 3-6, 2006, ACM 2006, pp135-140

[6] 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

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

[8] Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis *"Secure Routing and Intrusion Detection in Ad Hoc Networks*" Third IEEE International Conference on Pervasive Computing and Communications, March 2005.

[9] Li Zhao and José G. Delgado-Frias "*MARS: Misbehavior Detection in Ad Hoc Networks*", in proceedings of IEEE Conference on Global Telecommunications Conference,November 2007.

[10] Tarag Fahad and Robert Askwith *"A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks*", in proceedings of the 7th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, June 2006.

[11] Chin-Yang Henry Tseng, *"Distributed Intrusion Detection Models for Mobile Ad Hoc Networks"* University of California at Davis Davis, CA, USA, 2006.

[12] Bhalaji, Sivaramkrishnan, Sinchan Banerjee, Sundar, and Shanmugam, *"Trust Enhanced Dynamic Source Routing Protocol for Adhoc Networks"*, in proceedings of World Academy Of Science, Engineering And Technology, Vol. 36, pp.1373-1378, December 2008