Journal of Mobile Communication 5 (1): 1-5, 2011
ISSN: 1990-794X

New Trust Based Security Approach for Ad-Hoc Networks

[1]Sanjeev Sharma, [2]Renu Mishra and [2]Inderpreet Kaur
[1]School of IT, RGTU, Bhopal, 462021 M.P., India
[2]Department of Computer Science and Engineering,
Galgotia's College of Engineering and Technology, Greater Noida, U.P., 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 study 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.

Key words: MANETs, MAC-layer, security protocol, trust, ad-hoc networks, India

INTRODUCTION

Trust management is a multifunctional control mechanism in which the most important taskt is to establish trust between nodes who are neighbors and making a routing path. 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, otherwise it is decremented. If the trust counter value falls below a predefined trust threshold, the corresponding the intermediate node is marked as malicious. In this study, the researchers study about trust mechanism in the ad-hoc networks and propose a trust evaluation based security solution.

Routing protocols in MANETs: In the ad-hoc networks, outing protocol should be robust gainst 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 (Doshi and Kilambi, 2003). Proactive routing protocols such as Destination-Sequenced Distance-Vector Routing (DSDV) (Abusalah *et al*., 2006) 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 (Doshi and Kilambi, 2003). 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 (Doshi and Kilambi, 2003). 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 study, we propose to design a Trust-based Security Protocol (TMSP) based on a MAC-layer (Fig. 1) approach which attains confidentiality and authentication of

Corresponding Author: Sanjeev Sharma, School of IT, RGTU, Bhopal, 462021 M.P., India

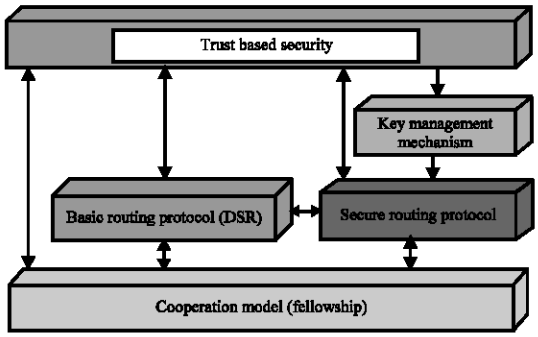

Fig. 1: Security at different levels

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
- Light-weight in order to considerably extend the network life time that ecessitates 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

Dynamic source routing: DSR is a source rooting in which the source node starts and take charge of computing the routes (Sun *et al*., 2006). 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 (Sun *et al*., 2006).

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.

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 Sun *et al*. (2006), 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.

Trust mechanisms: There is a common assumption in the routing protocols that all nodes are trustworthy and cooperative (Just and Kranakis, 2003). 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 discussed earlier, 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 (Just and Kranakis, 2003). Simply, we can consider it as the probability that an entity performs an action as demanded.

Trust properties: According to Anjum *et al*. (2003), there are four major properties of trust:

Context dependence: The trust relationships are only meaningful in the specific contexts.

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.

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 the knowing him. Then we collect their opinions. From the information gathered, we get the 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.

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; very 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

Proposed scheme (trusted routing): In the 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:

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.

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:

- 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
- Compute trust values for every node in X based on the trust graph
- Among all paths, A chooses the one with the max (in = 1 pi) where n is the number of nodes along with path

The 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:

$$FCni = FCni+1, i = 1, 2 \quad (1)$$

Then, the NTT of node n_k 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:

$$SRi = FCni/Prec \quad (2)$$

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 1st 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, $\delta 1$ 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 n_k, 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, $\delta 2$ is another step value with $\delta 2<\delta 1$. For a node n_k 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 sensefor 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 sublayer makes use of a simple CSMA (Carrier Sense Multiple Access) algorithm.

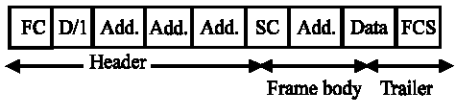

Fig. 2: MAC frame format (FC: Frame Control; SC: Sequence Control; Oct: Octets D/1-duration/ connection control; FCS: Frame Checks Sequence)

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. 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 (Fig. 2).

Address field indicates the transmitter and receiver address, SSID and source and destination address. Sequence control is used for fragmentation and reassembly.

CONCLUSION

In this study, 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 now-a-days, 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.

REFERENCES

Abusalah, L., A. Khokhar, G. Ben Brahim and W. El-Hajj, 2006. TARP: Trust-aware routing protocol. Proceedings of the International Conference on Wireless Communications and Mobile Computing, IWCMC, July 3-6, Canada, pp: 135-140.

Anjum, F., D. Subhadrabandhu and S. Sarkar, 2003. Signature based intrusion detection for wireless Ad-Hoc networks: A comparative study of various routing protocols. Proceedings of the IEEE 58th Conference on Vehicular Technology, Oct. 6-9, Morristown, New Jersey, USA., pp: 2152-2156.

Doshi, J. and P. Kilambi, 2003. SAFAR: An adaptive bandwidth-efficient routing protocol for mobile Ad Hoc networks. Proceedings of the 2nd International Conference, Ad-Hoc, Mobile and Wireless Networks, Montreal, Canada, Oct. 8-10, Springer-Verlag, Berlin, Heidelberg, pp: 12-24.

Just, M. and E. Kranakis, 2003. Resisting malicious packet dropping in wireless Ad Hoc networks. Proceeding of the ADHOCNOW Conference, Oct. 8-10, Montreal, Canada, pp: 151-163.

Sun, Y.L., W. Yu, Z. Han and K.J.R. Liu, 2006. Information theoretic framework of trust modeling and evaluation for Ad Hoc networks. IEEE J. Selected Areas Commun., 24: 305-317.