Global Journal of Engineering Science and Research Management

TRUST BASED DSR PROTOCOL FOR SECURE DATA TRANSMISSION IN MANET

R. Shalini[*1] Dr. S. Ravimaran[2]
[1*]Computer Science and Engineering, M.A.M. College of Engineering, Trichy.
[2]M.A.M. College of Engineering, Trichy.
*Correspondence Author: **R. Shalini**

Keywords: MANET, Modified DSR Protocol, Trust-Based DSR Protocol, IDS.

Abstract
Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. Routing is an important component in mobile ad hoc networks and several routing protocols in MANET, which are affected from attacker/malicious nodes. Dynamic Source Routing (DSR) is one of the most suitable routing protocols for the MANETs and it is more vulnerable to gray hole, black hole attack by the malicious nodes. This project presents Trust-based Dynamic Source Routing Protocol (TDSR) that enable a node to reason about trustworthiness of other node based on past interactions and recommendations also uses the concept of MDSR for initial transaction. Two contexts of trust are service and recommendation. Recommendation context rests on satisfaction value and satisfaction value depends on packet transmission rate and time taken to send packets. Service context rests on link weight, channel fading effect and satisfaction value. IDS maintain the service value and nearby nodes maintain the recommendation value. Based on the trustworthiness the data will send in a secured manner. For the new transaction, Intrusion Detection Systems (IDS) are used to detect the anomaly, and then reduce its trust value.

Introduction
Wireless ad-hoc networks are also called Mobile ad-hoc multi-hop networks without any predetermined topology. A MANET is a type of ad hoc network that can change its own network locations and configure itself while on the move. All nodes in this network are mobile and they use wireless connections to communicate with various networks. Every mobile node acts both as a host and as a router to establish a route.

Routing is one of the core problems of networking for delivering data from one node to the other. The currently available routing protocols of MANET are mainly categorized into proactive and reactive routing protocols. Proactive routing protocol includes DSDV (Destination Sequence Distance Vector) and OLSR (Optimized Link State Routing Protocol) each node maintains one or more tables containing routing information to every other node in the network. All the nodes involved in maintaining latest view of the network by keep on updating these tables. Reactive protocol includes AODV (Ad hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing) routes are created as and when required. When a transmission occurs from source to destination, it invokes the route discovery procedure that is source routing. The route remains valid till destination is achieved.

Most of these routing protocols assume cooperation between nodes for packet forwarding, a malicious node can inject routing attacks that will affect the normal routing operations or Denial-Of-Service (DOS) attacks such as black hole or gray hole attack that Leads to packet loss, denies the service to the legitimate nodes on MANET.

Black hole attack is one in which the intruders can exploit the vulnerability in route discovery procedures of on-demand routing protocols. The intruder, once chosen as an intermediate node, drops the packets instead of forwarding or processing them, causing a black hole (BH) in the network.

Gray hole (GH) attack or selective black hole attack is a special kind of black hole attack, which can be easily launched on reactive routing protocols like DSR or AODV. In black hole attack, a malicious node can attract all data packets by falsely claiming a fresh route or shortest route to the destination and then absorbs them without forwarding it to the destination; whereas in gray hole attack, the malicious nodes participate correctly in route discovery process. But once a route is selected through them to reach destination, they will drop the data packets selectively. As because only partial data packets are dropped, gray hole attack is even harder to detect than black hole attack.

Malicious nodes have more attack opportunities in MANET due to lack of central authority. Trust model that aims to decrease the malicious activity of nodes in MANET. Service trust and recommendation trust are two primary metrics to measure trustworthiness in the network. The service trust metric is used when sender send the data packets to destination. The recommendation trust metric is collected from neighbors during route selection/discovery process.

Global Journal of Engineering Science and Research Management

Related work

Routing protocols are vulnerable to routing attacks because they route based on the assumption that all nodes cooperate to find the best and effective path. Consequently, a malicious node can exploit the vulnerabilities of the cooperative routing algorithms and the lack of centralized control to launch routing attacks. In particular, the on-demand (reactive) MANET routing protocols, such as AODV and DSR, allow intruders to launch a wide variety of attacks.

In [1], authors first proposed selective forwarding attacks and suggested that multi path forwarding can be used to counter these attacks in sensor networks. However, the algorithm fails to detect and isolate the attackers from the network. In [2], the IDS nodes are set in sniffing mode in order to estimate the suspicious value of a node within the communication range, according to the routing messages transmitted by the node. When the suspicious value of a node exceeds a threshold, an IDS nearby will broadcast a block message to its neighbor IDS and to inform all nodes on the network, asking them to cooperatively isolate the malicious node.

In [3], the author proposed Self-Organizing Trust Model (SORT) for peer-peer system. Open nature of peer-to-peer systems exposes them to malicious activity. Building trust relationships among peers can mitigate attacks of malicious peers. This paper presents distributed algorithms that address a peer to reason about trustworthiness based on past interactions and recommendations. Our approach uses this concept to build a trust model for MANET. In [4], channel aware detection (CAD) approach has been proposed two strategies, hop-by-hop loss observation and traffic overhearing. Each intermediate node in the forwarding path observes the behavior of its previous-hop and next-hop neighbors to detect the misbehaving nodes. In this approach, every node in the forwarding path has to observe both its upstream and downstream neighbors by promiscuous overhearing which results in more energy loss at individual nodes. Whereas our approach does not employ any promiscuous monitoring by upstream nodes in the source route and the nodes in forwarding path observe other nodes behavior by means of QREQ and QREP packets.

In [5], the authors presented the Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack. Intrusion Detection System (IDS) nodes are set in promiscuous mode only when required, to detect the abnormal difference in the number of data packets being forwarded by a node. In that system, if IDS nodes are out of range of transmission it is difficult to detect the gray hole attack. In the approach proposed in [6], to detect and isolate the gray hole nodes, all nodes involved in a session of data forwarding must create a proof for receiving the data packets. When the source node suspects some misbehavior, it initiates the checkup algorithm to verify intermediate nodes.

In [7], before sending any block of data, source node sends a prelude message to destination node to alert it. The neighbor nodes monitor flow of traffic. After end of transmission, destination sends postlude message containing the number of data packets received. If the data loss is out of tolerable range, initiate the process of detecting and removing all malicious nodes by aggregating response from neighbor nodes of the source route in the network. In this approach all nodes surrounding the nodes in the source route turn into promiscuous mode to monitor their data forwarding behavior even when there is no attack which results in loss of energy in individual nodes. Whereas in our approach the IDS nodes turn into promiscuous mode only after the detection of presence of gray hole nodes in the source route.

In [8], Anti Black Hole mechanism (ABM) has been proposed. ABM estimates the suspicious value of a node, according to the amount of abnormal difference in RREQs and RREPs transmitted between source and destination. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the IDS node to all nodes in the network in order to isolate the suspicious node cooperatively. Previously, they are suspected to be malicious nodes and if the suspected value exceeds threshold, they are isolated. But the gray hole nodes participate correctly in route discovery process by forwarding RREQ packets for finding route to any destination node. Once the route established through that node, it drops data packets selectively. So this approach cannot detect gray hole nodes.

In [9], the authors propose a scheme that randomly selects part of the intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgments for each packet received. If suspicious behavior is detected, it will generate an alarm packet and deliver it to node. However, the algorithm suffers from high overhead because for each received packet the intermediate nodes need to send an acknowledgment back to the source node.

The security of the AODV protocol is compromised by a particular type of attack called ‘Black Hole’ attack. In this attack a malicious node advertises itself as having the shortest path to the node thereby all the packets are dropped. To reduce the probability of black hole attack [10], proposed to wait and check the replies from all the neighboring nodes to find a safe route. Our approach used to prevent the Black hole attack, by making use of a ‘Fidelity Table’ wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a ‘Black hole’ node and is eliminated.

Global Journal of Engineering Science and Research Management

Proposed system

To achieve secure transmission in MANET, follows MDSR and TDSR Protocol. First all the nodes must be registered with ID and range to enter into the MANET as authenticated node. Group splitting process occurred, according to the node range. IDS is chosen for every group based on its efficiency and energy level. Data transmission takes place in secured manner.

Assume that each and every node has transmission range as 50. So split the group as,

a. Transmission range 0-50 as Group1
b. Transmission range 51-100 as Group2
c. Transmission range 101-150 as Group3 etc…

Split the region in MANET, each region contains Host-based Intrusion Detection System (HIDS). An IDS is a device that monitors the network for policy violations or malicious activities. Assume that every nodes in particular region within the transmission range of an IDS, an IDS node will always be neighbor to some other IDS node. IDS nodes in different group have a direct link and they are assumed to be trusted nodes and it detects the malicious node within the network.

General Procedure

1. If Sender ready to send the packets/data to destination
2. Choose the destination and route selection/discovery process which includes,
3. Path to destination with intermediates nodes
4. Recommendation Metric for the intermediates
5. If more than one intermediate node is stranger in the route then
6. Follows MDSR Protocol
7. Else
8. Follows TDSR Protocol.

MDSR Protocol

For MDSR Protocol, in route selection process first chooses two different route then send packets in one route, then send the number of packets in another route to destination thereby it will find the malicious node. If any mismatch occurs in the count then destination will send QREQ at 2-hop distance and the node will send the QREP with that it will find the malicious node. Once the malicious node was found then reduce its trust value and recommendation metrics. In successive transaction this node will be eliminated.

Procedure for MDSR

Route selection/discovery process

1. Get two different paths from source to destination by sending RREQ and RREP
2. If any failure occurs in transmission path then uses the trust-based route.

Action of source, destination and IDS during data forwarding

1. If Source node
2. Send the count of data packets in a block of data to destination in one path.
3. Then send one block of data through the other path selected through route selection process.
4. Else if destination node
5. Compare the data packets received with the data count sent by the source.
6. Calculate the probability of packets received at the destination node as PD.
7. If PD < TPL (the value of TPL is between 0 and 0.2) Let ND denotes the number of packets received at the destination node, NS denotes the number of packets sends by the sender and then the probability of packets received at the destination Node is calculated as follows: PD = (ND/NS) (1) In (1), TPL represents the packet loss threshold value and takes values between 0 and 0.2.
8. Send positive acknowledgement back to source node.
9. Else
10. Find malicious node in the network by,

i. Send a QREQ packet to a node, say A, at 2-hop distance from it in the source route.
ii. Receive the QREP packet from node A.
iii. From the QREP packet, verify the count of data packets forwarded by all nodes from node A to itself.
iv. If data packets count matches, then

- Repeat step i to a node, say B, which is at 2-hop distance to node A in source route.

Global Journal of Engineering Science and Research Management

- Repeat the step ii, iii and iv.Else if data packets forwarded count does not matches, then
- Move both the node that sends QREP and its next node in the source route, to the suspected list.
- Then send the other block of data, IDS will detect the malicious node.
- Stop the process.

11. End if

Here, out of range problem of IDS will be eliminated by maintaining at least one IDS node for each range. In future, IDS node information are replicated in more efficient node in that region, if any instant failure occur in IDS node, it will be easy to hand over the control to the replicated node. Then the replicated node act as IDS.

TDSR Protocol

Trust-Based DSR Protocol is used only after past transaction occurred in the route. But it is useful to send the data in less time, secured manner and more efficient. This protocol is more efficient than MDSR but for initial transaction TDSR is not suitable, for that purpose only chooses the MDSR for initial transaction and for the remaining/successive transaction uses TDSR Protocol.

Trust value based on past interaction and recommendation. Two contexts of trust metrics, service and recommendation contexts, are defined to measure trustworthiness in route that sending packets efficiently. Creating long-term trust relationships among nodes can provide a more secure environment by reducing risk and uncertainty.

Service Trust Metric or Competence Belief (cb_{ij}):

IDS will continuously monitoring the nodes in the network. Service metric is calculated by link weight, channel fading effect and satisfaction value. Satisfaction value depends on packet transmission rate and time taken to send packets. Service trust metric is denoted by st_{ij} .

Then, IDS calculates cb_{ij} or st_{ij} as follows:

$$st_{ij} \text{ or } cb_{ij} = \frac{1}{\beta_{cb}} \sum_{k=1}^{sh_{ij}} (s_{ij}^k . w_{ij}^k . f_{ij}^k) \qquad (2)$$

Where,

$\beta_{cb} = \sum_{k=1}^{sh_{ij}} (w_{ij}^k . f_{ij}^k)$ is normalization coefficient.

If p_j completes all interactions perfectly ($s_{ij}^k = 1$ for all k), the coefficient β_{cb} in (2) ensures that $cb_{ij} = 1$. Since $0 \le s_{ij}^k, w_{ij}^k, f_{ij}^k \ge 1$ by definition, cb_{ij} always take a value between 0 and 1.

Service trust metric or competence belief represents how well an acquaintance node satisfied the needs of past interactions.

Table i. Notations on trust metrics

Notation	Description
s_{ij}^k	p_i 's satisfaction about k^{th} interaction with p_j
w_{ij}^k	Link weight of p_i 's k^{th} interaction with p_j
f_{ij}^k	Fading effect of p_i 's k^{th} interaction with p_j
st_{ij}	p_i 's service trust value about p_j
rt_{ij}	p_i 's recommendation trust about p_j

Global Journal of Engineering Science and Research Management

sh_{ij}	Size of p_i 's service history with p_j

These are the notations used to calculate trust value and for secure transmission in Mobile Ad hoc Network.

Recommendation Metric (rt_{ij}):

In TDSR, nodes are assumed to be strangers to each other at the beginning. A node becomes an acquaintance of another node after transmitting packets via that node. The recommendation metric measures an acquaintance's trustworthiness based on past interaction.

Declaration
{
th = 0.8
rt_{ij} = 0
}

1. Gather Recommendation trust by,
   a. rec = Request Recommendation (p_i, p_j)
   b. rt_{ij} = rec
2. Calculate the average of Recommendation trust(rt)
3. Get st_{ij} from the IDS
4. Calculate the average of Service trust(st)
5. Data transmission,
   a. IF $((rt + st)/2) < th$ then
   b. IF there is no trusted route available then
      Go to mdsr(procedure for MDSR)
   c. ELSE
      Send the packects in other trusted route

Creating long-term trust relationships among nodes can provide a more secure environment by reducing risk and uncertainty.

Conclusion

Secure data transmission in MANET is achieved by this model. The Intrusion Detection System plays an important role to find the attacker while it is in promiscuous mode. Here out of range problem of IDS will be eliminated by maintaining at least one IDS node for each group. Comparing with several existing protocols it is an effective way to find the malicious nodes in the network. In this modified dynamic source routing protocol, the destination node detects the presence of malicious nodes in the source route and reduce the trust value of malicious node. Using trust-based dynamic source routing protocol, time consumption for packet transmission will be minimized and transmission occurred in a secured manner resulting in less energy loss, packet loss which makes our method suitable for the resource constrained characteristics of MANET.

References

1. *Ming-Yang Su. A study of deploying intrusion detection systems in mobile ad hoc networks. Proc World Congr Eng 2012.*
2. *Shila Devu Manikantan, Cheng Yu, Anjali Tricha. Channel-aware detection of gray hole attacks in wireless mesh networks. In: IEEE global telecommunications conference, December 2009.*
3. *Ahmet Burak Can, Bharat Bhargava SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems. In: IEEE transactions on dependable and secure computing, February 2013.*
4. *Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. Elsevier's Ad hoc Networks J September 2003.*
5. *Mohanapriya M, Ilango Krishnamurthi Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers and Electrical Engineering 2014.*
6. *Xiaopeng Gao, Wei Chen. A novel gray hole attack detection scheme for mobile ad-hoc networks. In: IFIP international conference on network and parallel computing workshops, 2007.*

Global Journal of Engineering Science and Research Management

7. *Sukla Banerjee. Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. World Congr Eng Comput Sci 2008.*
8. *Ming-Yang Su. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems, 2010.*
9. *Xiao B, Yu B, Gao C. CHEMAS: identify suspect nodes in selective forwarding attacks. J Parallel Distributed Comput 2007.*
10. *Tamilselvan Latha, Sankaranarayanan V. Prevention of co-operative black hole attack in MANET 2008.*