An Attack Proof Trust Model for Secure Path Selection with Data Transmission in MANET

Ravi Lodhi, Shiv Kumar, Babita Pathik

Abstract: A mobile ad-hoc network (MANET) is a network of mobile nodes which also act as routers and are connected by wireless links. These routers are free to move and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. The dynamic nature of MANETs makes network open to attacks and unreliability. MANETs are vulnerable to various security attacks. Hence, finding a secure and trustworthy end-to-end path in MANETs is a legitimate challenge. Dynamic source routing set of rules is a functional protocol in wireless mobile ad-hoc network (MANET). Data Safekeeping and detection of malicious node in a MANET is an imperative job in any network. To achieve reliability and availability, routing protocols should be powerful against malicious attacks. This paper provides a trust model that detects attacks while data transmission and finding secure route in MANET. Experimentally outcome indicated that system is fine appropriate for confident and enhanced data communication. The structure also accomplishes protected routing to safeguard MANET against malevolent node. The outcomes exposed that the scheme security and throughput of the system is enhanced.

Keywords: MANET, secure routing, malicious attack, Ad hoc Network, Wireless Routing Protocol, trust value.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of which form a random topology. The routers are free to move randomly and organize themselves at random; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human induced disasters, military conflicts, emergency medical situations etc.[1]The issue of symmetric and asymmetric links is one among the several challenges encountered in a MANET. Another important issue is that different nodes often have different mobility patterns. Some nodes are highly mobile, while others are primarily stationary. It is difficult to predict a node's movement and pattern of movement. The dynamic nature of MANETs makes network open to attacks and unreliability. Routing is always the most significant part for any networks.[3] Each node should not only work for itself, but should also be cooperative with other nodes. MANETs are vulnerable to various security attacks. Hence, Finding a secure and trustworthy end-to-end path in MANETs is a genuine challenge.

The trustworthiness of distributing data packets from end to end using multi-hop intermediary nodes is a noteworthy problem in the mobile Ad-hoc network. The distributed mobile nodes create links to form the MANET, which may include mischievous and selfish nodes. Developing the trust based system is very challenging problem in MANET.[5] In order to filter out misbehaving nodes we propose a model which help in secure route discovery, data transmission and report to the MANET about any mischievous node. And also find secure data path for secure data transmission. We estimate the secure value of each node using timestamp of the operation. Then to select a protected track for message forwarding to identify the damaged and malicious nodes which are supposed to launch network letdown.

II. BACKGROUND

The ideas dynamic source routing is created on the source transmitting which means the motivator of the data packet make available a systematic list of nodes rendering to which data packet pass through in the system. The key note this routing pattern is that intermediate nodes need not to track the information of the routing through which packet will traverse in the network as source node already has a decision regarding the routes. Utilization of source transmitting allows the data packet to travel in the loop free environment, elude the requirements for updating the routing information in the intermediate node, allows the node to forward the packet to store the moving info in them for future. All aspects of protocol operate entirely on demand [8]. DSR works in completely self-configuring and organizing without preexistence of structured network for slightly current system administration or substructure. The protocol works on the two important mechanisms. i.e. 'Route Discovery' and 'Route Maintenance'.

Route discovery is a method of finding out the secure route in the network, when a source node's having a desire to transmit the data packet to the target node, where every node holds a route cache of source routes it has understood or overheard. Route maintenance [11] is the mechanism by which originator device recognize the alteration occurred in the network topology such that it understands about the longevity of the route available to the destination because of the node in the route list is moved out of the range. DSR works on finding a route and uses that route called source route. Sender has a complete knowledge of particular sequence orders of the network nodes to reach at the destination. The initiator than pass this packet into the network interface wireless medium to the first node which is identified by the route in its route cache. If that node is not the destined address, it forward the packet following by the further node mentioned in the route cache [9]. Once after

Revised Version Manuscript Received on January 10, 2017

Ravi Lodhi, M.Tech. Scholar, Department of Computer Science and Engineering, Lakshmi Narain College of Technology Excellence, Bhopal (M.P)-462021, India.

Dr. Shiv Kumar, Professor & Head, Department of Computer Science and Engineering, Lakshmi Narain College of Technology Excellence, Bhopal (M.P)-462021, India.

Babita Pathik, Assistant Professor, Department of Computer Science and Engineering, Lakshmi Narain College of Technology Excellence, Bhopal (M.P)-462021, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

another, process is continuous, until not reached to the final destination. After reaching to its desire end it will deliver the packet to the transport layer of the host.

III. PROPOSED WORK

The proposed work suggested a supervision model to safely transmit the data between source node and destination node which depends on the confidence value of individual node in the passageway. The proposed work considers the timestamp and location of the node for computing the confidence value of the node. In Ad-hoc network every node observes each other's behavior in order to make association which ultimately defines the level of consistency single node can lay on one more node. These associations are in a way favorable to support the nodes to either accelerate the data packets to a particular neighbor or not. Now, the confidence value is compared between neighbors and if the value is matched then it is marked as authenticated and data can be transferred and if the value is not matched then it marked as unauthenticated and data cannot be transferred.

In the proposed scenario set up 50 nodes are used in the network. DSR is used as a routing method in algorithm. The initial threshold data value is set as 0.5 in algorithm which will be used to calculate the confidence value. This calculated value is applied for protected data transmission. If the network authenticates a node, then the data is transmitted to the destination node otherwise further neighbor is selected for secure data transmission.

Input: List of neighbour nodes
Output: A secure path
Source generate the neighbour search query
if search query issuing node guarantees nearest path according to trusted value
then
search is completed and secure path is confirmed
else
calculate search area
send query for searching neighbours
set waiting time for search
end if
if node receives Query for the first time and if node is within search area and not in maintenance mode then
store ID of source node as parent, send Query, set replay delay time
end if
node receives Reply or Empty Reply
if node is query-issuing node then store data items
else if node is not in maintenance mode then
store reply node and update replay delay
if node is parent of source node then
send Reply or Empty Reply to parent
end if
if Assignment node is not covered then and within search area
send Empty Reply to parent
else
send Reply to parent
end if
end if
if data items are acquired and area of neighbour node is covered then
complete search
else
calculate new search area, send Query refine, set waiting time
end if
Secure path is established and data transmission started
End

In the scenario setup the nodes are placed and source and destination nodes used in the system are selected. Then the threshold value for packet delivery ratio is set. The routing parameters, routing protocols, packet size, dimensional area, and rate of transmission are also fixed.

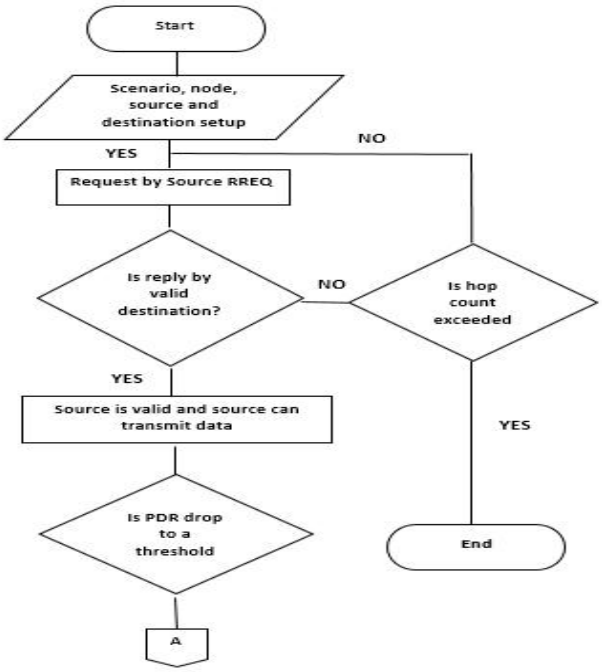
Then the next step is to send the request generated by source RREQ and is to check whether the source get the reply RREP by valid and authenticated node. The trust value is compared between neighbors and if the value is matched then it is marked as authenticated source can transmit data to the specified and secured path. If RREP reply is from invalid or unauthenticated node, then first count the number of hops. If number of hop counts exceeded, then marked system is invalid and exit from the network.

Now, to find another secure neighbor node go to the RREQ source request step. Source node randomly choose bait address of one hop neighbor to bait malicious node. Create backup node list, select nearest neighbor from trusted backup node. The subsequent stage is to check data packet distribution ratio of the network. The proposed method assigned initial belief value to each node which helps to find authenticate neighbors.

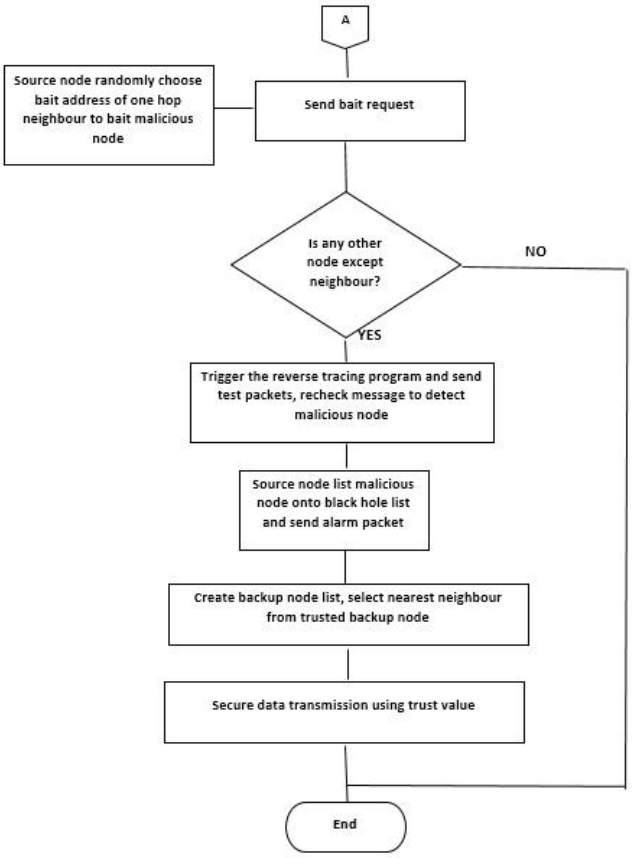
The components of the proposed model are trust value, recommended trusted neighbors, and secure path. The threshold data value is measured as 0.5. The confidence key is designed as $\sqrt{(\text{node} * \text{trust value} * \text{threshold value})}$ Suppose node 25 have to check for authentication then its trust value is calculated according to the threshold value as

Confidence value = $\sqrt{(25 * 0.714285714 * 0.5)}$
= 1.78571885

FLOWCHART



Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.



IV. RESULT & DISCUSSION

The proposed work is implemented with the help of NS2 simulator. NS2 provides simulation environment for MANET network. For simulation we have used i5 3.0 GHz machine with 8GB RAM. The program is developed in TCL language and some functions are also implemented in C/C++ language.

Table: 1. Simulation Parameter

Simulation area	700m X 450m
Simulation duration	500 s
No. of Ad-hoc nodes	50
Transmission range	400 m
Movement-Model	Random-Waypoint
Traffic-type	CBR
Max. mode-speed	15 m/s
No. of connections between nodes	3 – 30
Pause time	8 s
MAC	802.11
Source Destination Pair	15
Radio Range	250 m
Rate (packet per sec)	2 pkts/s
Data pay-load	30 – 512-bytes
Seed	1.0
Protocol	DSR

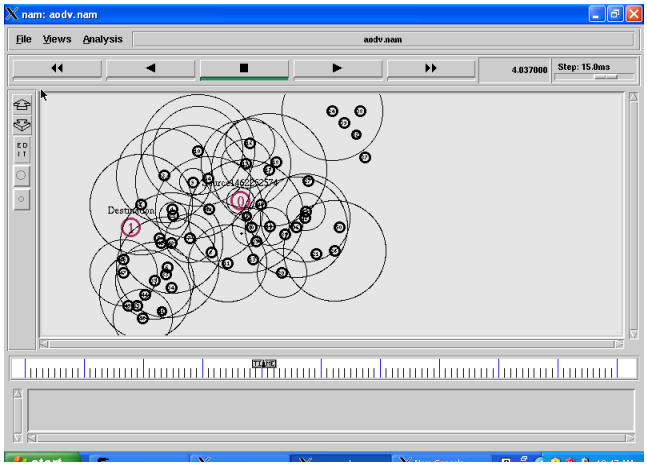


Figure: 1. Data Transmission between Source and Destination node

The above figure represents the data transmission between source and the destination node after the secure path is established between them.

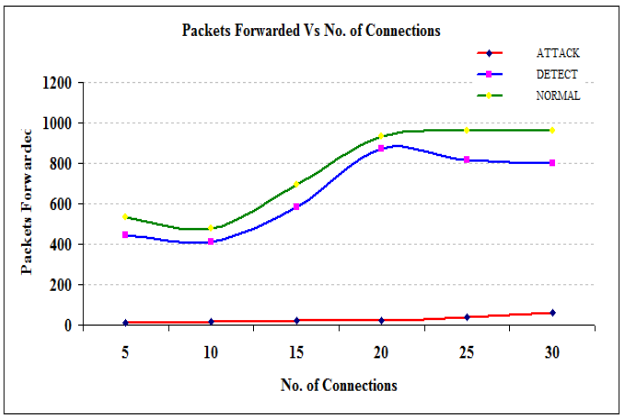


Figure: 2. Graph for packets forwarded vs maximum number of connections

Above is the graph plotted for number of packets forwarded vs maximum number of connections. Number of connections varies from 5 to 30. Scenarios G to L, at 15 m/s of node speed, are plotted for DSR under routing attack and DSR with detection module and normal DSR.

V. CONCLUSION AND FUTURE WORK

Finding link failure, securing data, detecting malicious node and secure information transmission in an Ad-hoc like MANET is an important task. Ad-hoc network using dynamic source routing under malicious attack with secure routing and data transmission. The proposed algorithm discovers the attack and if original route is interrupted then different protected node is recognized and info is transported from recently formed path. The thesis suggested a protected confidence value which validate the node and also retain safe the system from malicious nodes. The simulation outcomes discovered that the system throughput, security and system performance is enhanced.

In future the proposed system can me more modified by combining with other techniques so that the performance of the network could be increased like advancement using some encryption techniques so that the security level in the ad-hoc network can be increased.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

REFERENCES

1. Amit N Thakre ,Mrs M.Y.Joshi "Performance Analysis of AODV & DSR routing Protocol in Mobile ad-hoc network", IJCA special Issue on "mobile ad-hoc network", MANETs 2010
2. David A. Maltz, "On demand routing in multi-hop wireless mobile ad-hoc network" CMU-CS-01-130, PhD. Desertion, School of computer science Carnegie Mellon University, Pittsburgh PA- 2001.
3. Tanvi Arora, Amarpreet Kour, Mandeep Singh," Review of various routing protocols and routing Models for MANRTs", International Journal of Innovation & Advancement in CS ,IJIACS,ISSN 2347-8616,Vol.4 Special Issue, MAY 2015.
4. Elizabeth M Royar and Chai Kunh toh,"A Review of current routing protocol for ad-hoc mobile Wireless network", Technical report, University of California and Georgia Institute of Technology,USA,1999.
5. David B Johnson, David A. Maltz , Josh Broch ,"DSR: The dynamic source routing protocol for Multi-Hop wireless Ad-hoc network", Computer Science Department, Carnegie Mellon University, Pittsburgh,PA 15213-3891,http://www.monarch.cs.cmu.edu.
6. Antesar M. Shabut, Keshav P. Dahal, Sanat Kumar Bista, and Irfan U. Awan, Recommendation Based Trust Model with an Effective Defence Scheme for MANETs, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 10, OCTOBER 2015, pp-2101-2115
7. H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," IEEE Commun. Mag., vol. 40, no. 10, pp. 70–75, Oct. 2002.
8. B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in Wireless Network Security. New York, NY, USA: Springer, 2007, pp. 103–135.
9. N. Pissinou, T. Ghosh, and K. Makki, "Collaborative trust-based secure routing in multihop ad hoc networks," in Proc. Netw. Netw. Technol., Services, Protocols; Perform. Comput. Commun. Netw.; Mobile Wireless Commun., 2004, pp. 1446–1451.
10. S. Buchegger and J. Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," IEEE Commun. Mag., vol. 43, no. 7, pp. 101–107, Jul. 2005.
11. G. V. Crosby, L. Hesterand, and N. Pissinou, "Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks," Int. J. Netw. Security, vol. 12, no. 2, pp. 107–117, 2011.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.