ISSN:0975-9646

Denial of Service Attack Detection and Secure Data Transmission Using Trusted Path in MANET

Shilpa Agnihotri, Prof. Amit Saxena
Truba Institute of Engineering and Information Technology RGPV, Bhopal, M.P. India

Abstract-.An Ad-hoc system is a gathering of wireless movable nodes enthusiastically creating a momentary network lacking make use of any core-existing network centralized or infrastructure management. MANET has some limitations owing to infrastructure, mobility, capabilities of mobile nodes or due to system as a whole. Limitations due to infrastructure or system, relay nature of communications, frequent disconnections / partitions, Limited bandwidth, packet loss owing to transmission error, variable capacity links. This thesis recommend a novel approach to discover the DoS based attack and likewise retain harmless the system from malevolent nodes. The dissertation suggested a protected confidence and trust value which assistances validate the node and also keep safe the system from malevolent nodes. The outcome showing that the initiative security and throughput of the system is enhanced experimentally result indicate that system is all right appropriate for enhanced and confident data communication. The structure also accomplish protected routing to safeguard MANET against malevolent node.

Keywords-Mobile Adhoc Network, DoS attack, network security, trust value, confidence value

I. INTRODUCTION

The concepts dynamic source routing is based on the source routing which means the initiator of the packet provides an orderly list of nodes according to which packet traverses in the network. Utilization of source routing allow the packet to travel in the loop free environment, elude the requirements for updating the routing in sequence in the intermediate node, allows the node to promote the packet to store the routing details in them for future. The key note this routing pattern is that in-between nodes need not to track the details of the routing through which packet will traverse in the network as source node previously has a decision regarding the routes. All aspect of protocol function completely on demand. DSR works in completely self configuring and organizing without pre existence of structured network for a few presented network infrastructure or supervision DSR works a discovery the route and uses that route called source route. DSR utilize the source routes where packet travels according to obtained source route as of the route cache itself or by finding through the flooding in the network. This makes DSR to gain the benefits in provisions of mounted information, free from the loop that to without overhead cost. In route discovery primarily the initiator node will first search the route beginning source to destination by utilizing its route cache. If the initiator fined the path it will start sending the packet in a transmission range by wireless medium. Route maintenance is the method of maintaining the route in network if the link failure occurred. DSR follows this mechanism to delete the broken link from the network while propagating the packet beginning the source in the direction of the destination. Route cache id type of memory storage. DSR protocol uses this for mounting the knowledge of the route into the network from soured to destination. Each node learn the knowledge of routing information by overhearing the communication of other nodes. Also get the information links between the nodes when any route fault message generates in the network. Recognition of malevolent node data Security and in a MANET is an important tasks in any network. To achieve reliability and availability, routing protocols must be powerful against both link lifetime prediction and malicious attacks. Due to the intrinsically self-motivated environment of the mobile network topology, the existing links are recurrently damaged, and fresh links are often recognized. Determination of link lifetime, data security, detection of malicious node and secure information transmission within a MANET be an important tasks in any mobile network. Detection of link lifetime of nodes with the help of routing info is also problematic in an informal network due to its real time altering topology. Improve the data delivery ration and performance of MANET as well as also detect and correct link lifetime is the major difficulty in MANET.

The trustworthiness of distributing data packets from end to end using multi-hop intermediary nodes is a noteworthy problem in the mobile Adhoc network. The scattered mobile nodes create links to structure the MANET, which possibly will comprise mischievous and selfish nodes. Developing the trust based system is extremely demanding problem in MANET. In line to clean out misbehaving nodes we proposes 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.

In mobile Adhoc network, network security plays a serious role in network organization analysis and monitoring. During flooding processes link scanner passively collects hop counts of established investigation messages at MANET nodes. Based on the surveillance that damaged links can result in disparity between received hop counts and network topology. The object of link scanner is near make available a list encompassing all possible links failures. With such a list, more recovery and analysis procedures become possible, including (a) altering routing

policy for the related nodes, (b) discovering the root causes of observed indications within the network, (c) contribution the auxiliary list of lifetime links for every single node. Our procedure guarantees that multi cast data is transported beginning the source toward the associates of the multi cast groups, even in the existence of attacks, as long as the group members are accessible through non adversarial track. Here for authentication trust value be accustomed to remove outside adversaries and guarantee that only approved nodes accomplish certain operation.

II. BACKGROUND

DSR is created on the source transmitting which means the motivator of the data packet make available a systematic list of nodes rendering to which information packet pass through in the system. The key note this routing pattern is that in-between nodes need not to track the details of the routing through which packet will traverse within the network as source node by now have a decision regarding the routes. Utilization of source transmitting allows the packet to travel in the loop free environment, elude the requirements for updating routing details in the intermediate node, allows the node to forward packets to store the moving info in them meant for future. the entire aspect of protocol work completely on demand. DSR works in completely self configuring and organizing without pre existence of structured network for slightly current system administration or substructure. The protocol works on the two important mechanisms. i.e. 'Route Discovery[5]' and 'Route Maintenance'. Route detection is a way of finding out the secure route into the network, when a source node's having a desire to transmit the packet toward the target node, where every node holds a route cache of source routes it has understood or overheard. Route maintenance be the means by which originator device recognize the alteration occurred within the network topology such that it understands about the longevity of the route available in the direction of the destination because of the node within the route list is moved out of the range.

DSR works a discovery the route and uses that route called source route. Sender has a complete knowledge of particular sequence orders of the nodes to reach at the destination. The initiator than pass this packet into the network interface wireless medium to the first node which is recognized by the path in its route cache. If the node is not the destined address, it promote the packet following by the further node mentioned in the route cache. Once after another, process is continuous, until not reached to the final destination. After reaching to its desire end it will deliver packet to transport layer of the host. Since the routing decision is made at source which make easy to obviate the loops in route. It's a Starmark feature of DSR. Source route traverse into the network on control packets in the form of route request and route reply while traversing if any node hears source route than it can include the information within its route cache. Protocol itself broadcast the topological knowledge into the network between the nodes. Source route carries the correct information of route as it being tested by the packet flowing within the network along with them. DSR utilize the source routes where packet travels according to obtained source route to the route cache itself or by finding through the flooding in the network. This makes DSR to gain the benefits in conditions of mounted information, free from the loop that to without overhead cost.

Route maintenance is the procedure of maintaining routes in network if the link failure occurred. DSR follows this mechanism to delete the broken link from the network while propagating the packet starting from the source on the way to the destination. The basic concept of route protection in DSR is that each node is in charge for acknowledging the next node within the source path had received the packet. If some node does not received such confirmation it will send fault message to the initiator in the network. After when the originator receives the error message from the particular node, it deletes that route from route cache and opt the other best route available in its cache. Suppose A is the originator it will send the data according to route inside its route cache. As each node is in charge for confirmation or receiving the request, the further nodes B and C will do the same. In case if C is not getting confirmation message it will wait for time and retransmit the request but after sending request to some time it will send error message to the initiator by sequential counts within its route cache. And source nodes will listen route error message and then delete the link, the same other nodes will do by overhearing the message. Now node A will use another best route by utilizing route cache otherwise it will initiates the route discovery.

III PROPOSED WORK

A. Proposed Algorithm

The projected algorithm is represented in this section. In this algorithm we have provided all the steps of our proposed work. Determination of DoS attack, data security, link failure, detection of malicious node and secure information transmission in MANET ,it is an important tasks in any mobile network. The proposed work will detect DoS based attacks within the network and informed to the network. The belief value is compared between neighbors if value is matched then it marked as authenticated and data can be transferred. In this algorithm we includes backup node to find different secure path if there is an attack in the system. The packet delivery ratio is also checked to find performance of the network.

B. Algorithm

Step 1: Scenario setup, Node setup, Routing protocol setup, Source and destination setup setting initial trust value, threshold value setup

Step 2: Apply flooding process in a mobile ad hoc network to check condition of the links, link scanner infers all links statuses on the basis of data collection from a prior probe flooding process.

Step 3: After that step is to count no of nodes.

Step 4: Check any node mismatch in network

If hop count exceeded then

System is invalid

Goto End

Else If any node is dropping data or mismatched in hop count then

DoS attack and link failure detected inside the network then report to the system

Else

Source can transmit data, Marked system is valid

end if

Step 5: Generation of encrypted secure key in which node initialization time is taken as a secure key. After getting the secure key the node is marked as authenticated node.

Step 6: Calculation of confidence value.

The confidence value is derived by using node * threshold value * trust value.

This confidence trust value is use to authenticate nodes.

Step 7: Check whether node have secure key then authentication successful for data transmission and node is marked as secure node.

Step 8: Test data packet distribution ratio

If data packet distribution ratio drop to the given threshold then

Starting source node arbitrarily pick the supportive address of any one node
neighbour to malicious node

Send request toward the node

If anyone node reply from other path except neighbour node then take the
reverse locating program and direct check data packets

Check messages to detect DoS malicious node

Data source node give list of DoS attack malicious node

Set alarm packet
Goto End

Else

Goto End

End if

Step9: After that is to find route for secure data transmission. The shortest path is discovered across the node.

Step 10: Select a node to destination

If selected node is found in route_list then

Selected node is marked as secure node and route detection is successful. Route is confirmed for data transmission

Else

Select another new node, check authentication

End if

Step 11: During data transmission any link may fail so backup node selection method is always used by system for backup node setup.

Step 12: After successful data transmission the route record is maintained by system for future use.

Step 13: End

The initial step in our proposed work is to setup the scenario i.e. to setup the node used in algorithm. To setup the intiator and destination used in the system. Set the threshold value for packet delivery ratio. It also set the routing parameters, routing protocols, packet size, dimensional area, and rate of transmission. The subsequent step is to transmit the request generated by source RREQ. Subsequently is to test whether the source get the reply RREP by valid and authenticated node. Because the DoS attacked node be able to generate the RREP signal. The belief value is compared between neighbors if value is matched then it marked as authenticated and data can be transferred. If message from the authenticated node then system is marked as an authenticated and source be able to transmit packet to the specified and secured path. If RREP reply is from invalid or unauthenticated node then first count the no. of hops. If number of hop counts exceeded then marked system is invalid and exit from the network. To find another secure neighbor node go to the RREQ source request step. Source node randomly choose bait address of single hop neighbor to bait malicious node. Create backup node list, select nearest neighbor from trusted backup node. Check messages to detect DoS dependent malevolent node and source node list malevolent node onto DoS based attack malicious nodes. The subsequent stage is to check data packet distribution ratio of the network.

IV. IMPLEMENTATION

In implementation work, network used 50 nodes, which are arbitrarily positioned in dissimilar parts of positioning part with a static density. For this implementation, network parameters, such as Dimension, Number of nodes, traffic, transmission rate, Routing protocol, transmission range, sensitivity, transmission power etc., are used.

For simulation we have use PIV2.4 GHz machine with 2GB RAM. The program is developed in TCL language and some functions are also implemented in C/C++ language.

Table I. Simulation parameter

Simulation area	500m X 500m
Simulation duration	500 s
No. of Adhoc nodes	50
Transmission range	300 m
Traffic-type	CBR
Max. mode-speed	12 m/s
No. of links between nodes	50
Pause time	10 s
MAC	802.11
Radio Range	250 m
Rate (packet per sec)	2 pkts/s
Data pay-load	30 – 512-bytes
Protocol	DSR

Table II. Trust value and Confidence value

Node	Trust Value	Confidence Value
1	1462252574	1316027316.6
5	1462252574	6580136583.0
8	1462252574	10528218532.8
14	1462252574	18424382432.4
16	1462252574	21056437065.6
20	1462252574	26320546332.0
24	1462252574	31584655598.4
35	1462252574	46060956081.0
39	1462252574	51325065347.4
44	1462252574	57905201930.4
49	1462252574	64485338513.4

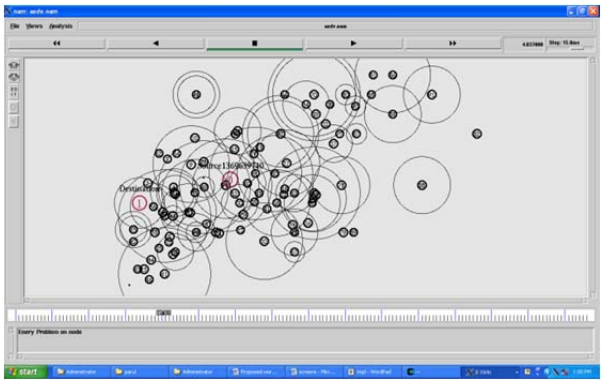

Fig 1. A Sample Topology generated by NS-2 with trust key generation

Figure on top of shows the trust value generation by different nodes. This trust value used in secure data transmission.

Fig 2. Performance Graph for Multilevel Vs No. of Nodes

Figure on top of show the average data packet delivery delay meant for each level node within a fixed area with fixed no. of nodes using multilevel scheme. As the level increases, the delay also increases. But since protocol try to reduce the no. of levels so the delay is also reduced as compared to other multihop protocols.

V. CONCLUSIONS AND FUTURE WORK

Ad-hoc network doesn't be determined by on any principal administration or stable infrastructure such as base. Real time application in MANET require certain QoS , as minimal end to end info packet interval and acceptable data loss. Determination of link letdown, detection of malevolent node, data safety and protected info communication in MANET is commanding work in any movable network. The excellence of service must fulfil source end to destination end data transfer without packet loss. DSR set of rules is a sensible procedure in mobile ad-hoc system. The trustworthiness of distributing data packets from source to end using multi-hop intermediary nodes is a remarkable difficulty in the mobile Adhoc network. Owing to the innately enthusiastic character of movable system topology, the prevailing routes cannot be secure. Adhoc network using DSR under malicious attack with safe routing and data transmission. The proposed protocol discover the DoS 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 assistances validate the node and also retain safe the system from malevolent nodes. The thesis proposed detection of DoS attack in Ad hoc network. It increases performance and trustworthiness of mobile Ad hoc network using DSR under DoS and link failure due to DoS attack with confident routing and info transmission. The simulation outcomes discovered that the system performance, protection and throughput is enhanced. In future we are development to diminish the energy consumption and to control the traffic of a network. A direction of future investigation is to break the message in small parts and transmits using multipath algorithm and secure data distribution using encryption technique.

REFERENCES

[1] Markku Antikainen, Tuomas Aura, and MikkoSärelä, Denial-of-Service Attacks in Bloom-Filter-Based Forwarding, IEEE/ACM Transaction on net., Vol. 22, No. 5, October 2014, pp-1463-1478

[2] Amit N Thakre ,MrsM.Y.Joshi "Performance Analysis of AODV & DSR routing Protocol in Mobile ad-hoc network", IJCA special Issue on "mobile ad-hoc network", MANETs 2010

[3] Elizabeth M Royar and Chai Kunhtoh,"A Review of current routing protocol for ad-hoc mobile Wireless network",Technical report, Georgia Institute of Technology,USA,1999.

[4] 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,PA152133891,http://www.monarch.cs.cmu.edu.

[5] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks andcountermeasures in mobile ad hoc networks," in Wireless Network Security. New York, NY, USA: Springer, 2007, pp. 103–135.

[6] 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.

[7] 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.

[8] Antesar M. Shabut, Keshav P. Dahal, Sanat Kumar Bista, and Irfan U. Awan, Recommendation Based Trust Model with an Effective Defence Scheme for MANETs, VOL. 14, NO. 10, OCTOBER 2015, pp-2101-2115

[9] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless adhoc networks," IEEE Commun. Mag., vol. 40, no. 10, pp. 70–75,Oct. 2002.