Research Article Impact Factor: 0.621 ISSN: 2319-507X
Snehal Deulkar, IJPRET, 2014; Volume 2 (8): 766-776 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURITY IN NODE-DISJOINT MULTIPATH ROUTING METHOD (NDMP) BASED ON AODV PROTOCOL

SNEHAL P. DEULKAR, PROF. S. Y. GAWALI

1. Assistant Professor, College of Engineering & Technology BabasahebNaik College of Engineering
2. Assistant Professor, Computer Engineering Department ,Yavatmal , India Computer & Science Engineering Dept, Yavatmal, India.

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: In an ad hoc network, identification of all node-disjoint paths between a given pair of nodes is a challenging task. With the proposed approach, all the node disjoint path get discovered in the network and also as soon as the first route for destination is determined, the source starts data transmission. All the other backup routes, if available, are determined concurrently with the data transmission through the first route. This minimizes the initial delay caused because data transmission is started as soon as first route is discovered. Security issues become more challenging in ad hoc network due to its dynamic nature which allows any node to freely join as well as leave the network without having a physical address or getting permission. Ad hoc networks are vulnerable to different kinds of attacks such as: denial of services, impersonation, and eaves dropping. The proposed multipath routing scheme provides better performance, scalability and security by computing multiple routes in a single route discovery.

Keywords: Node-Disjoint, AODV, Multipath Routing

PAPER-QR CODE

Corresponding Author: MR. SNEHAL P. DEULKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Snehal Deulkar, IJPRET, 2014; Volume 2 (8): 766-776

INTRODUCTION

An ad hoc network is a collection of infrastructure less nodes, cooperating dynamically to form a temporary network which meets certain immediate needs. The lack of infrastructure implies that the nodes are connected peer-topeer; therefore, each node plays its role as a host beside its role as a router Since the ad-hoc network establishes at the time of data transfer , so there are many possibilities of attacks which ultimately results into the loss of data packets such as denial of services, signaling attacks flow disruption attacks etc.

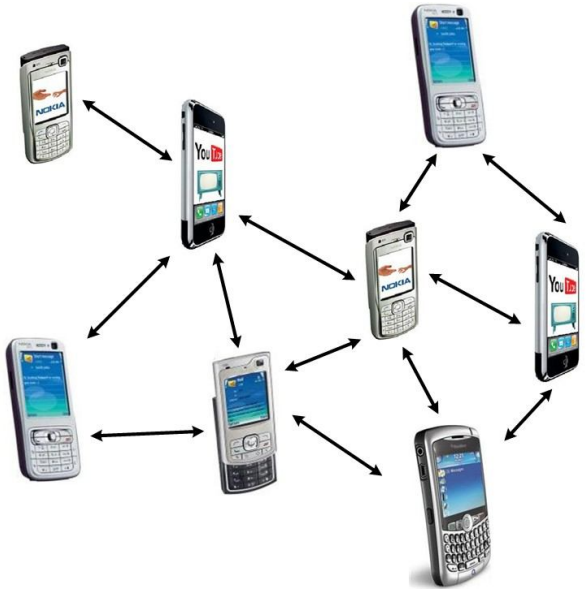


Fig 1.1 :Mobile Ad Hoc Network

Security is one of the main issues for networks. It becomes more challenging in ad hoc networks due to the lack of central access point to monitor node behavior and to manage node membership [4]. Any network security system aims at satisfying the following goals: privacy and confidently, authenticity, integrity, and access control. All security attacks on any system are a violation of one or more of these goals [5]So it becomes mandatory to provide the security to the network or more specifically to the data packets to be sent. Security can be provided by many techniques that are used in many ways for providing the required security to the routing protocol.

In [1] Node-disjoint multipath routing allows the establishment of multiple paths, each consisting of an unique set of nodes between a source and destination. We know that MANETs consist of mobile nodes that cause frequent link failures. This link failure causes two main

problems. Firstly, when a route break occurs, all packets that have already been transmitted on that route are dropped and it decreasing the average packet delivery ratio (PDR). Secondly, the transmission of data traffic is halted for the time till a new route is discovered and it increasing the average end-to-end delay. The main objectives of multipath routing protocols are to provide reliable communication and to ensure load balancing as well as to improve quality of service (QoS) of MANETs. These multipath protocols are broadly classified into five categories based on their major goals. The goals are to improve delay, provide reliability, reduce overhead, maximize network life and support hybrid routing. Multipath routing protocols address issues such as multiple paths discovery and maintaining these paths. In this Paper, we proposed a new multipath routing protocol that is based on the AODV [2] protocol for MANETs and security within NDMP-AODV.

This protocol improves the packet transmission rate and reduces the end-to-end delay by utilizing backup route that is node disjoint from the main route. In this situation security of routing protocol in MANET is essential key factor. The main thing in this case is that when the path is broken from source to destination , data at the intermediate node should be removed before selecting another back-up path which will prevent any intruder from accessing those crucial data. Also, it reduces the packet transmission delay by establishing the backup route while data is transmitted.

PROPOSED SYSTEM

We proposed NDMP-AODV protocol with addition of the security to data while transmitting data from source to destination .The main goal of NDMP-AODV is to find all available node-disjoint routes between a source-destination pair with minimum routing overhead. To achieve this goal, NDMP-AODV protocol works in three phases: (A) Route Discovery Phase, (B) Route Selection Phase and (C) Route Maintenance Phase.

A . Route Discovery Phase :

When a source node has a data packet to send, it checks its routing table for the next-hop towards the destination of the packet. If there is an active entry for the destination in the routing table, the data packet is forwarded to the next hop. Otherwise, the route discovery phase begins. In route discovery phase, routes are determined using two types of control messages: (i) Route request messages (RREQs) and (ii)Route reply messages (RREPs). The source node floods the RREQ message into the network. Each intermediate node that receives a RREQ, checks whether it is a duplicate or a fresh one by searching an entry in the Seen Table. Seen Table stores two entries (i.e. source IPaddress and RREQ flooding ID (f_id) that uniquely

identifies a RREQ message in the network. If an entry is present in the Seen Table for the received RREQ message, it is considered a duplicate RREQ message and discarded without further broadcasting. Otherwise, the node creates an entry in the Seen Table and updates its routing table for forward path before broadcasting the RREQ message.

In NDMP-AODV, only the destination node can send RREPs upon reception of a RREQ message. The intermediate nodes are forbidden to send RREPs even if they have an active route to destination. This is done so as to get the node-disjoint routes. In NDMP-AODV, the destination node has to send a RREP message for each RREQ received, even if the RREQ is a duplicate one. We change the data structure of Seen Table and RREP message as shown in Figures 1 and 2. In Seen Table, we add an extra field that works as a flag known as seenflag. This flag is set to FALSE at start i.e. when an entry is first inserted in the Seen Table after a

Source IP Address	Flooding ID	**Seen Flag**
---	---	---

Fig 3.1 : NDMP-AODV Seen Table Structure

Type	R	A	Reserved	Prefix Size	Hop Count
Destination IP Address					
Destination Sequence Number					
Source IP Address					
Source Sequence Number					
Broadcasting ID					

Fig 3.2 : NDMP-AODV RREP Structure

node gets its first RREQ message. The RREP messages initiated by destination node in NDMP-AODV contain one extra field known as broadcast ID(b_id).

The route discovery method used to discover node-disjoint paths is shown in Figure 3.4. When a destination node receives a RREQ message, it creates the corresponding RREP message. The destination node copies the f_id from the received RREQ message into the b_idfield of sent

RREP message. This RREP is unicast towards the originator of the RREQ using the reverse path to construct the forward path. For every RREQ received (i.e. either first or duplicate), the destination does the above mentioned process. When the intermediate nodes in the reverse path receive the RREP message, they check the seen flag value in their Seen Table. If the seenflag is set to FLASE, this indicates that this is the first RREP message on the reverse path towards the source node. So, the intermediate nodes relay the RREP towards the source and reset the value of seenflag. When the intermediate node gets a RREP message for the same RREQ message it got earlier, the node simply discards the RREP message on the basis of seenflag value. Due to this, the intermediate node's can only take part on any one route from the existing multiple routes.

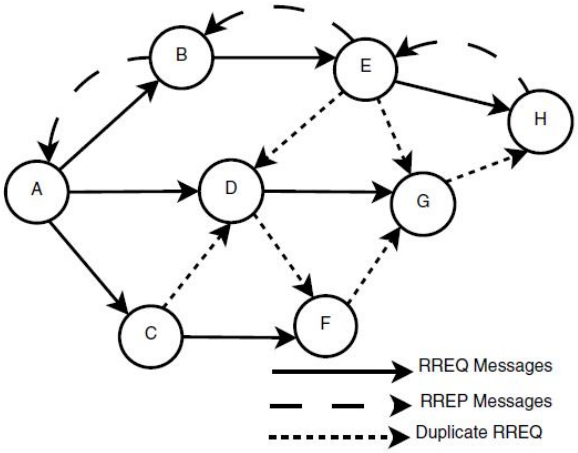


Fig 3.3 : Traditional AODV Route Discovery Process

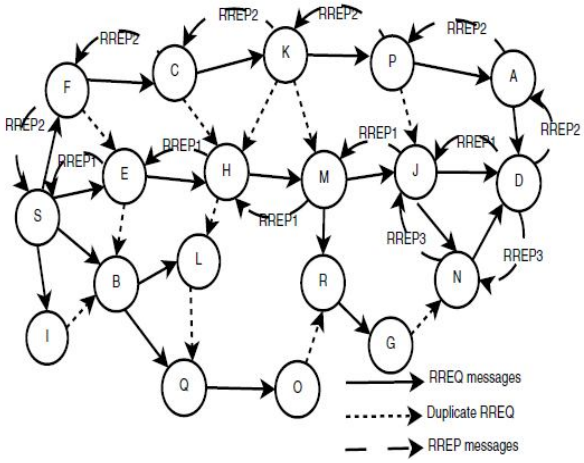


Fig 3.4 : NDMP-AODV Route Discovery Process

B. Route Selection Process and Data Packet Transmission:

When source node has data packets to send and there is no route available in routing table, the node initiates the route discovery process. The source node starts data transmission as soon as it gets the first route for destination node known as primary route. All the other node-disjoint routes that are discovered will be stored in the routing table as secondary routes. After storing the primary route and an specified number of secondary routes in the routing table, all the other routes (if any) are not stored. All the other routes that are discovered after storing the primary and secondary paths can replace the existing secondary paths if they have lower hop count for destination as compared to existing ones. The route selection function works in such a way that whenever a route is required for data transmission, it always selects the primary route if it is available. If the primary route is not active, then the route selection function selects the route with lowest hop count from the available secondary routes.

C. Route Maintenance Process:

Route maintenance process is invoked when an active route is broken during completion of a data flow. We implement and analyze the performance of three route maintenance methods in case of route breaks. In the first method, when the primary route is broken, transmission of data is continued using the secondary routes. To keep the secondary routes active while using the primary route, we increase the lifetime of each active secondary route after a fixed amount of time. When all the secondary routes are also broken, the source starts a new route discovery process. In this way, we can minimize the routing overhead caused in finding and maintaining multiple routes. Because in this case, only one RREQ is used to find all available node-disjoint paths as compared to one RREQ required for each path. In second route maintenance method, the source node starts the route discovery process as soon as it finds out that there is only one active path (i.e the one which is currently being used for data transmission) remaining in routing table. In this way, the source has routes for destination at all time. This greatly reduces the delay caused by the rerouting process which is triggered by a route break. But, this method increases the routing overhead.

Advantages:

*In NDMP-AODV, multiple routes between source-destination pairs allow the source to select a backup route in case current route is broken, without initiating a route discovery process. This reduces the routing overhead.

*Minimizes Routing overhead as compaired to other existing multipath AODV Protocols.

Security In NDMP- AODV

As MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks. Wireless links make MANETs more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is required. They can also directly attack the network to delete messages, inject false packets, or impersonate a node. This violates the network's goals of availability, integrity, authentication, and non-repudiation. In the proposed method , We are providing security to system while the transmission of data from source to destination and link failure occurs in midway during the transmission .In this system ,So as the route is discovered by using route discovery phase and after discovery of path , the data is ready to follow along the path which is containing the intermediate unique node. In this situation if the sudden link failure occurs during transmission, the data get lost meanwhile before reaching to the destination .In this case, firstly it recover the primary path otherwise it go the secondary path from the back-up table as soon as the root destroyed..But before going for the secondary path, We are giving the security to the system .In the proposed work ,We are not releasing the unique node having the data of the previous transmission before removing that data from the node to the another network .So that the security to the data is implemented.

ALGORITHM

NDMR-AODV route discovery method when a node receives RREQ message:

This Algorithm shows the procedure used by a node after getting a RREQ message. When a source node has a data packet to send, it checks its routing table for any active route available for destination. If an active route exists, data packet is forwarded to the next hop towards its destination. Else, it creates a RREQ message and inserts the entry in sent table. This is done to avoid re-sending RREQ messages before getting the RREP for the already sent RREQ. Each node also updates its Seen Table before broadcasting the RREQ message to avoid duplicate broadcasting. When a RREQ message is received by a node, the algorithm checks whether the node is a source, intermediate or destination node. If it is a source or intermediate node, RREQ message is processed in the same way as is done in the traditional AODV protocol. When a destination node receives the RREQ, it creates a RREP message and copies the b_idvalue from RREQ into the extra field provided in RREP. Destination node replies to every RREQ it receives to establish multiple routes. It does not check the received RREQ messages for duplicity as is

done in AODV protocol. When a node receives a RREP message during NDMR-AODV route discovery process.

NDMR-AODV route discovery method when a node receives RREP Message :

This Algorithm is applied to discover multiple node-disjoint routes. The algorithm checks whether the node that receives a RREP message is an intermediate or source node. If it is an intermediate node, its seen flag status is checked from its Seen Table. A FALSE value of seen flag indicates that it is the first RREP message that this node has received for this particular source-destination pair. If this is the case, the algorithm resets the value of seen flag corresponding to this source-destination pair and inserts this route as the primary route for the destination node. Then, the node forwards the RREP to the next hop towards source. On the other hand, if the value of seen flag is TRUE for this source-destination pair, we may or may not insert the

route in the routing table as a secondary route, depending upon the route maintenance process used. This duplicate RREP message is then discarded to ensure that all the discovered routes are node-disjoint.

In addition to this system, we are providing the security. As the data is transmitted from source to destination. During this transmission if the failure occurs , then before transmitting that from another route, we are not freeing that intermediate unique node which is having the particular data in the previous transmission to the another network till removing all data that it is previously contained. As in the MANET, due to the mobility of nodes frequent link failure takes place that why securing of the data is essential issue.

PERFORMANCE EVALUATION

This explains the various performance metrics required for evaluation of protocols and also focuses on result and its analysis based on the simulation performed in Network Simulator 2.32. To reiterate the black hole attack, we begin with the overview of performance metrics that includes End-to-end delay, Throughput and Network load. These matrices are important because of it performance analysis of network. Furthermore, implementation of the simulation setup, tools and its design are explained.

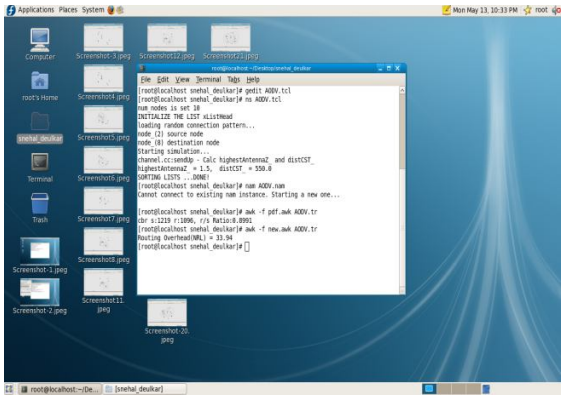


Fig 5.1 Performance evaluation parameter

Performance Metrics :

The performance metrics chosen for the evaluation of black hole attack are packet delivery ratio and routing overhead.

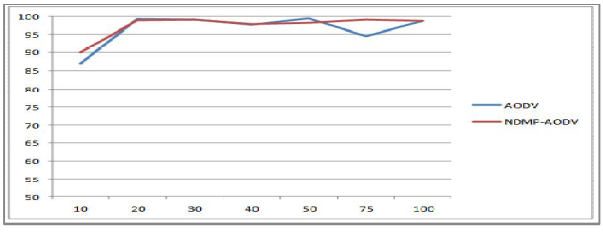
Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.

Routing Overhead : The total number of routing packets transmitted during the simulation. For packets sent over multiple hops, *each* transmission of the packet (each hop) counts as one transmission. Routing overhead is an important metric for comparing these protocols.

SIMULATION RESULT:

This paper focuses on result and its analysis based on the simulation performed in Network Simulator 2.32.

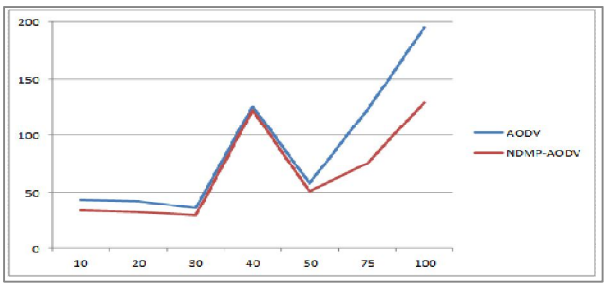
Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.



No. of Nodes VS Packet Delivery Rate

Fig6.1 Comparison of Packet Delivery Ratio

Routing Overhead: The total number of routing packets transmitted during the simulation. For packets sent over multiple hops, *each* transmission of the packet (each hop) counts as one transmission. Routing overhead is an important metric for comparing these protocols. It gives the number of routing packets over the number of received data packets. Each routing packets are sent or forwarded by a mobile node.



Number of Nodes

Fig 6.2Comparison of Routing Overhead

CONCLUSION

We are proposing a node-disjoint multipath routing method based on AODV protocol with the addition of data security during transmission and link failure. The proposed route discovery method identifies all the available node-disjoint routes using a single flooding of a RREQ message. This greatly reduces the routing overhead caused by route discovery and maintenance processes thus increasing the network capacity. To reduce the initial delay, source node can send data as soon as it gets the primary route. Due to multiple routes stored in routing table backup routes are always available for continuous data transmission when the primary route is broken. As per the security is concerned during transmission and link failure , We are taking care of that unique node within the ad-hoc network.

APPLICATIONS AND CHALLENGES

Ad hoc wireless networks play a major role in armed services. These have made information exchange much easier than any. Also in small vehicular devices, this technique is made a beneficial one like with cameras - to deploy the targeted regions which helps us in gathering important location and environmental information's which will be communicated back to a processing node via ad hoc mobile communications.

Ad hoc wireless networks include certain commercial scenarios:

- Emergency services
- Seminars/conferences
- Law enforcement

REFERENCES

1. ChhaganLal, V. Laxmi, M. S. Gaur, "A Node-Disjoint Multipath Routing Method based on AODV protocol for MANETs", 2012 26th IEEE International Conference on Advanced Information Networking and Applications

2. G. rajkumar, Dr. K. Duraisamy**,"** A Review of Ad- Hoc On-Demand Distance Vector Routing Protocol For Mobile Ad-Hoc Networks" Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1

3. Chang-Woo Ahn, Sang-Hwa Chung, Tae-Hun Kim and Su-Young Kang. A node-Disjoint miltipath routing protocol based on aodv in mobile ad hoc networks.In Information Technology : New Generation (ITNG) , 2010 Seventh International Confernece on pages 828-833, april 2010

4. Shunli Ding, Liping Liu," A node-disjoint multipath routing protocol based on AODV" ,2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science

5. Fubao Yang, Baolin Sun , "Ad hoc On-demand Distance Vector Multipath Routing Protocol with Path Selection Entropy", IEEE transaction

6. M.T.Toussaint, " Multipath Routing in Mobile Ad-Hoc Networks " , TU-Delft/TNO Traineeship Report

7. Rajendra Kumar Gupta , "Node Disjoint Minimum Interference Multipath (ND-MIM) Routing Protocol for Mobile Ad hoc Networks" ,International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2,Issue 3, March 2012 ISSN: 2277 128X

8. Tsung-Chuan Huang, Sheng-Yu Huang and Lung Tang , "AODV-Based Backup Routing Scheme in Mobile Ad Hoc Networks" , International Conference on Communications and Mobile Computing 2010.