



Discovery of Path Using Node-Disjoint Multipath Routing Method Based on AODV Protocol

Snehal P. Deulkar

Assistant Professor

Jagadambha College of Engineering & Technology
Computer Science Engineering Department , Yavatmal ,
India

Vishwajit K. Barbudhe

Assistant Professor

Jagadambha College of Engineering & Technology
Master of Engineering (ME), Electronics & Telecomm
Engineering Department, Yavatmal, India

Abstract: Mobile ad hoc networks are typically characterized by high mobility of nodes and frequent link failures within the data transmission. As it is temporary networks that are built up momentarily in order to satisfy a certain emergency. Ad-hoc networks are in a great demand now-a-day and have lots of advantages like emergency control, short-term connection for roaming subscribers etc. Multipath routing can be utilized so that alternate paths are available to reduce link failure. A node-disjoint multipath routing protocol based on AODV was proposed in the paper. The main goal is to discover multiple node-disjoint paths with a low routing overhead during a route discovery. With the proposed approach, 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. The main issue is that security of data during the transmission. 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. The proposed multipath routing scheme provides better performance, scalability and security by computing multiple routes in a single route discovery. Also, it reduces the routing overhead by using secondary paths. This scheme computes combination of the node-disjoint path and fail-safe paths for multiple routes and provides all the intermediate nodes of the primary path with multiple routes to destination.

(*Keywords: Node-disjoint , AODV , Multipath Routing*)

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is an autonomous system of mobile devices connected by wireless links. A Mobile Ad-Hoc network change their topology frequently since it requires the frequent rebuilding of roots so maintaining stable roots may be infeasible. 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.

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. A new multi-path routing protocol [5] in MANET that is composed of high-mobility nodes. The new multi-path routing establishes the main route by the mechanism based on AODV, and then the data transmission starts immediately. The backup route search process is taking place while data is transmitted to reduce the transmission delay. This process finds the route that is node-disjoint from the main route by not selecting nodes participate in the main route. When either of the main route or the backup route is broken, data is transmitted continuously through the other route and the broken route is recovered by the route maintenance process. 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.

When we are in the position to send the data packets an Ad-hoc network is established. But the problem in such network is that when it broadcasts the data packets it is sent to all the nodes in the network. In such case there is possibility of misuse of data and data loss. To prevent the data packets from such problem of misuse of data and data loss we are going to apply the encryption and decryption techniques on AODV protocol for its security. The technique can work as to be sent is encrypted at the source node and intermediate nodes can't identify the data and destination node decrypts the data and gains the required original data.

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.

II. LITERATURE REVIEW

A MANET consists of mobile platforms, known as nodes, which are free to move at any speed in any direction and organize themselves randomly. The nodes in the network function as routers, clients, and servers. These nodes are constrained in power consumption, bandwidth, and computational power. Routing is one of the key issues in MANETs due to their highly dynamic and distributed nature. Multipath routing establishes multiple routes between source and destination nodes.

For fault tolerance, even if one route failure occurs, source node maintain connection by using other routes. So multipath routing protocol can reduce data transmission failure and delay times that are caused by route disconnection.

Multipath routing [5] is the one way of improving the reliability of transmitted information. While multipath routing may be used for various reasons such as load balancing, congestion avoidance, lower frequency to route inquiries and to achieve a lower overall routing overhead. Multipath routing is supposed to reduce the end to end packet delay and increase the packet delivery ratio. There are two types of disjoint paths: link-disjoint and node-disjoint. In node-disjoint paths no node in common other than the source and the destination, while in link-disjoint paths only links are disjoint but may have nodes in common.

We are discussing the previous work done on multipath routing methods based on AODV protocol [3]. Multipath routing creates multiple paths between a source-destination pair. These multiple path between source and destination pair can be used to compensate for dynamic and unpredictable nature of ad hoc networks. In case of the failure of first route, the backup routes are used for continues data transmission. In multipath routing protocols, the paths between a source and destination can be link-disjoint, node-disjoint or non-disjoint. a node-disjoint multipath extension for AODV referred as MP-AODV. MP-AODV [3] discovers two routes for each source-destination pair, a main route and a back-up route. The routes are discovered using two RREQ messages, each for one route. Whenever one route is broken, the other is used for data transmission and a RREQ is flooded to replace the broken route [5]

The AODV is inherently a distance vector routing protocol that has been optimized for ad hoc wireless networks. When a source node wants to communicate with a destination node whose route is unknown, a path discovery process is initiated to locate the destination node. The source node broadcasts a route request (RREQ) packet to its neighbors, which then forward the RREQ to their neighbors. The forwarding process continues until either the destination or an intermediate node that has a route to the destination node is located. When a RREQ reaches the destination node, the destination node responds by unicasting a route reply (RREP) back along the path in the reverse direction. As the RREP routes back to the source node, the route from the source node to the destination node is established. In the root maintenance process when a node detects a link failure., it generates a route error (RERR) packet is propagated over routes, while in validating corresponding roots simultaneously. When RERR packet is send back to source node, the source node initiates a new root discovery procedure.

III. 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 IP address 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.

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

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 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_id field 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 seen flag 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 seen flag. 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 seen flag value. Due to this, the intermediate node's can only take part on any one route from the existing multiple routes.

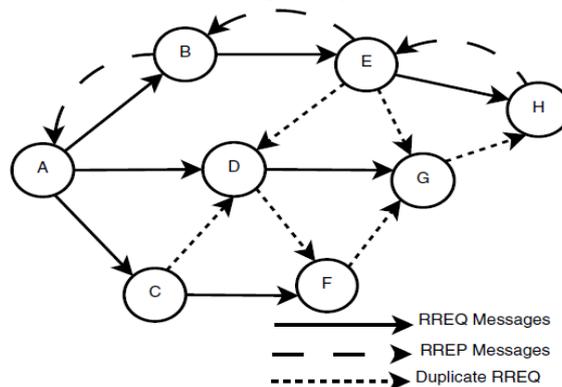


Fig 3.3 : Traditional AODV Route Discovery Process

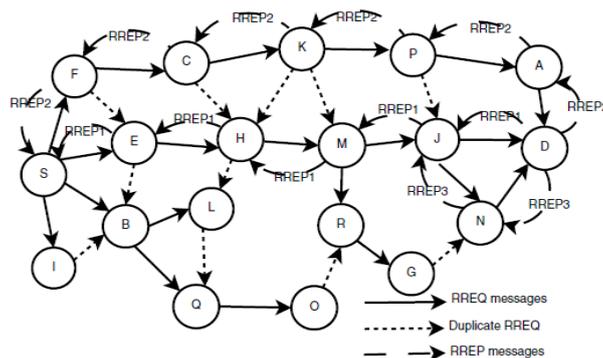


Fig 3.4 : NDMP-AODV Route Discovery Process

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.

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.

IV. 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_id value 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.

N = Node

S = Source Node

D = Destination Node

I = Intermediate Node

S Addr = Source IP Address

S Addr = Destination IP Address

B id = broadcast id field of RREQ

F id = flooding id field of RREP

S flag = FALSE //Initial value of seen flag seen table

n routes

X = FALSE

Count = 0

if *S* has data to send **then**

```
if S has route for D then
startdata transmission()
end if

else
insertRREQ senttable()
insert se() //insert entry in seen table to check
for duplicates
initiate RREQflooding()
end if
if N receives a RREQ message then
if  $N \equiv S \vee N \equiv I$  then
 $X = \text{check } se()$  //check for duplicate RREQs
if X then
discard () //drop RREQ without reboardcasting
else
relay () //reboardcast RREQ
end if
else
N is the destination
B id = F id
initiate () //destination node send unicast
RREP on forward route to create reverse route
end if
```

end if

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. If the node that receives the RREP is the source node, we insert the discovered node-disjoint path as primary or secondary, based on the value of seen flag and number of routes already present for this destination in routing table.

```
if NreceivesRREP then
```

```
if  $N \neq S$  then
```

```
 $X = \text{check } s()$  //check and return the value of seen flag from the seen table
```

```
if . X then
```

```
insert primary () // Insert first route in routing table
```

```
change s() //reset the value of seen flag in seen table to detect duplicate RREPs
```

```
relay () // forward RREP to next hop towards source
```

```
else
```

```
insert secondary () //if multiple routes are stored at intermediate nodes
```

```
discard () //drop the duplicate RREP to ensure the finding of node-disjoint routes
```

```
end if
```

```
else
```

```
 $X = \text{check seenflag}()$ 
```

```
if  $N \neq S$  then
```

```
insert primary route()
```

```
change seenflag()
```

```
else
```

```
Count = count () // count the numbers of active routes for destination in routing table
```

```
if Count < n routes then
```

```
insert secondary () // insert secondary routes and sort them in ascending hop count
```

```
else  
discard RREP()  
end if  
end if  
end if  
end if
```

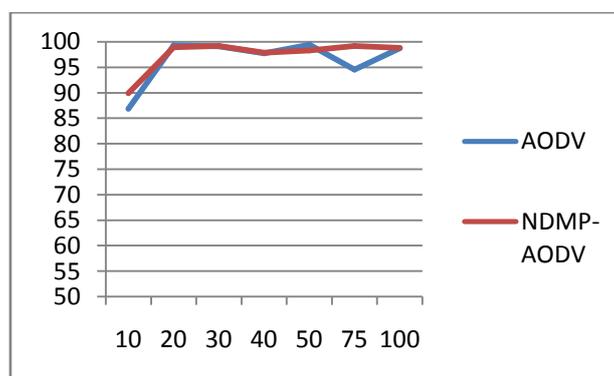
In addition to this system, we are providing the security. As the data is transmitted from source to destination. During this transmission if the failure occurs, then before transmitting that from another route, we are not freeing that intermediate unique node which is having the particular data in the 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.

V. RESULT:

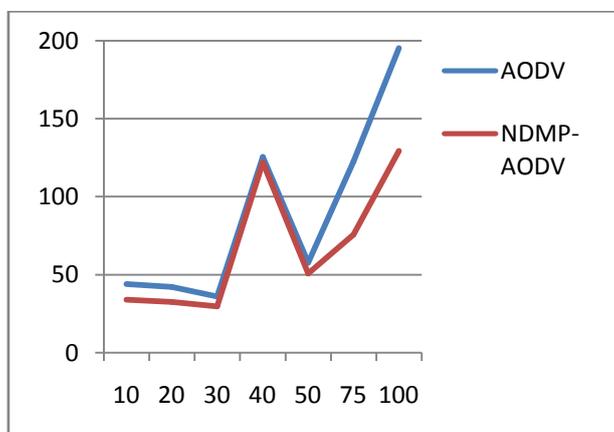
This paper focuses on result and its analysis based on the simulation performed in Network Simulator 2.32.

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.

Routing Overhead:



No. of Nodes VS Packet Delivery Rate



Number of Nodes Vs Routing Overhead

VI. 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.

REFERENCES

- [1] Chhagan Lal1, V.Laxmi2, M.S.Gaur3, “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] Shunli Ding1 , 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 Fubao Yang, Baolin Sun , “Ad hoc On-demand Distance Vector Multipath Routing Protocol with Path Selection Entropy”, IEEE transaction
- [4] M.T.Toussaint, “ Multipath Routing in Mobile Ad-Hoc Networks “ , TU-Delft/TNO Traineeship ReportRajendra 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
- [5] 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
- [6] V. Zangeneh, S. Mohammadi , “New Multipath Node-Disjoint Routing Based on AODV Protocol”, World Academy of Science, Engineering and Technology 2011
- [7] Xuefei Li and Laurie Cuthbert , “On-demand Node-Disjoint Multipath Routing in Wireless Ad hoc Networks” , 29th Annual IEEE International Conference on Local Computer Networks