ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 6, December 2013

Predictive Pre-emptive Ad-hoc On Demand Multipath Distance Vector Routing Protocol for MANET

Vijaylaxmi Joshi, Mallangouda Biradar, Sanjeevkumar Jeevangi
M.Tech in Computer science, M.Tech in Computer science, M.Tech in Communication Systems,
Asst.Prof. Dept. of ISE, RRCE, Bangalore, Asst.Prof. Dept. of CSE, AIE &T Gulbarga, Asst.Prof. Dept. of E &CE, AIE&T Gulbarga

***Abstract*— An Ad-hoc network is a collection of mobile hosts with wireless network interfaces that may form a temporary network without the aid of any established infrastructure or centralized administration. In such environment, the nodes operate both as hosts as well as routers. Due to mobility, the topology of the network may change randomly, rapidly and unexpectedly. Because of these aspects and the fact that the resources are limited in mobile nodes, efficient routing in ad hoc networks is a crucial and challenging problem. An ad-hoc network will often change rapidly in topology, this courses for routes in the network to often disappear and new to arise. To avoid frequent route discovery and route failure, various multipath routing protocols has been proposed based on the existing single path routing protocol in ad-hoc networks. Ad hoc On-demand Multipath Distance Vector (AOMDV) is one of extensions to the well-studied Ad-hoc On Distance Vector (AODV). In Predictive pre-emptive Ad-hoc on demand Multipath Distance Vector routing protocol (PPAOMDV) is presented to solve the "route failure" problem in AOMDV .The proposed protocol reduces the route failure problem by pre-emptively predicting the link failure based on received signal power by the receiver. The proposed protocol controls the overhead, increases throughput and reduces the delay.**

I. INTRODUCTION

Ad-hoc network [1] is a collection of wireless mobile nodes without any fixed base station infrastructure and centralized management. Each node acting as both a host and a router moves arbitrarily and communicates with others via multiple wireless links. Therefore, the network topology changes greatly.

In such a dynamic network, it is a challenging issue to be able to get route in time. The routing protocols proposed so far can be classified into two categories: proactive routing protocol and reactive routing protocol. Reactive routing protocol, which initiates route computation only on demand, performs better than proactive routing protocol, which always maintains route to destination by periodically updating, due to its lower control overhead. AODV is a well-known on-demand protocol. Although it outperforms many other routing protocols, it is a single path routing, which needs new route discovery whenever a path breaks. To overcome such inefficiency, several studies have been presented to compute multiple paths. They provide alternative paths to send data packets without executing a new route discovery, if the primary path breaks.

Our goal is to develop a Predictive Pre-emptive Ad-hoc on demand Multipath Distance Vector Routing Protocol (PPAOMDV) that preemptively finds weakening links and switches to an alternate path that is learnt from the earlier Route Discovery. We have extended Ad hoc on demand Multipath Distance Vector Routing Protocol (AOMDV) to show the achieved performance improvement. AOMDV's Route Discovery and Data Transfer process is modified here. In this Protocol if the received power loss is lesser than the threshold value only then RREQ is further broadcasted. This procedure ensures that routes computed does not include links that are not stable.

II. REVIEW OF LITERATURE

Route failures have a significant negative impact on packet delivery. Packet dropping and higher delays are the main consequences of route failures. The time elapsed between link break detection and alternative path establishment can be high. Therefore, many studies have focused on improving route repair.

Mahesh K. Marina and Samir R. Das [2] developed an on-demand multipath distance vector protocol for mobile ad hoc networks. Specifically, he proposed multipath extensions to a well studied single path routing protocol known as Ad hoc On-demand Distance Vector (AODV). The resulting protocol is referred to as Ad hoc On-demand Multipath Distance Vector (AOMDV).

The protocol computes multiple loop-free and link-disjoint paths. AOMDV achieve a remarkable improvement in the end-to-end delay, and they shown the reduction in routing overheads by about 20%.

Goff et al [3] proposed a pre-emptive route maintenance extension to on-demand routing protocols. Its aim is to find an alternative path before the cost of a link failure is incurred. The received transmission power is used to estimate when a link is expected to break. A link is considered likely to break when the power of the signal received over it is close to the minimum detectable power. Route repair is the responsibility of a source node after receiving a warning about the imminence of a link break on an active route to a destination. This mechanism has been applied to DSR; AODV is also considered, but only superficially.

Stephen Mueller, Rose P. Tsang [4] examines the issues of multipath routing in MANETs. Multipath routing allows the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 6, December 2013

establishment of multiple paths between a single source and single destination node. It is typically proposed in order to increase the reliability of data transmission (i.e., fault tolerance) or to provide load balancing. Load balancing is of special importance in MANETs because of the limited bandwidth between the nodes. We also discuss the application of multipath routing to support application constraints such as reliability, load-balancing, energy-conservation, and Quality-of-Service (QoS).

III. BACKGROUND AND GENERAL CONCEPTS

Mobile Ad-Hoc Network: An ad-hoc network [1] is a collection of wireless mobile nodes that are connected to wireless links, and communicate with each other without requiring the existence of fixed networking infrastructure. The network topology may keep changing dynamically.

A Mobile Ad-hoc Network (MANET) [1] is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANET does not depend on pre-existing infrastructure or base stations. Network nodes in MANET are free to move randomly. Therefore, the network topology of a MANET'S may change rapidly and unpredictably.

A mobile ad-hoc network all network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. Depending on its application, the structure of a MANET'S may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network [9].

A MANET sometimes called a **"mobile mesh network"**, is a self-configuring network of mobile devices connected by wireless links [10].

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router.

Characteristics of MANET: Mobile ad-hoc network nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), omnidirectional (broadcast), probably steerable, or some combination thereof. At a given point in time, depending on positions of nodes, their transmitter and receiver coverage patterns, communication power levels and co-channel interference levels, a wireless connectivity in the form of a random, multihop graph or "ad-hoc" network exists among the nodes. This ad hoc topology may modify with time as the nodes move or adjust their transmission and reception parameters.

IV. AOMDVAND PPAOMDV MECHANISMS

AOMDV Mechanisms: Ad-Hoc on Demand Multipath Distance Vector Routing Protocol is one of the most used Ad-Hoc routing protocol. It is a reactive routing protocol based on DSDV. AOMDV is designed for networks with tens to thousands of mobile nodes. AOMDV is an extension of AODV.

The main idea in AOMDV is to compute multiple paths during route discovery. It is designed primarily for highly dynamic ad hoc networks where link failures and route breaks occur frequently. When single path on-demand routing protocol such as AODV is used in such networks, a new route discovery is needed in response to every route break. Each route discovery is associated with high overhead and latency. This inefficiency can be avoided by having multiple redundant paths available.

In AOMDV a new route discovery is needed only when all paths to the destination break. A main feature of the AOMDV protocol is the use of routing information already available in the underlying AODV protocol as much as possible. Thus little additional overhead is required for the computation of multiple paths. The AOMDV protocol has two main components:

1. A route update rule to establish and maintain multiple loop-free paths at each node.
2. A distributed protocol to find disjoint paths that is route discovery.
3. The Route Maintenance Strategy.

Data Structure: In the AOMDV protocol, each mobile host maintains a multiple path *routing table*. Each entry of the table contains following information: destination address, next hop address, hop count, sequence number, route expiration time, maximum route expiration time, and a pointer to the list of backup paths.

The value of sequence number is for determining the freshness of routes. The list of backup paths is used to store all redundant paths. If there is only a primary path, the value of the pointer to the list of backup paths is NULL. Each element of the backup list contains next hop address, hop count, and route expiration time (RET). The value of route expiration time represents the stability of paths. A route with longer route expiration time is more stable. The "maximum route expiration time" is used to compute loop-free Multipath.

The maximum route expiration is set as zero initially. When backup paths are found, value of the field is set as the maximum RET among multiple paths.

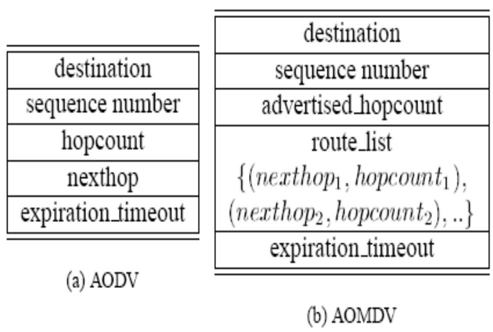


FIG 4.1 STRUCTURE OF THE ROUTING TABLE ENTRIES FOR AODV AND AOMDV.

The figure shows the structure of the routing table of AODV and the AOMDV. Figure 2 shows the structure of the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 6, December 2013

routing table entries for AODV and AOMDV. In AOMDV, advertised_hopcount replaces hop count. A route list replaces the next hop, and essentially defines multiple next hops with respective hop counts. However, all next hops still have the same destination sequence number. The dvertised_hopcount is initialized each time the sequence number is updated.

Route Discovery: The route discovery process has two major phases: route request phase and route reply phase. The route discovery process will be initialed when a route is requested by a source node and there is no information about the route in its routing table.

First, the source node generates an RREQ and then floods the packet to networks. The RREQ includes following fields: Source address (the IP address or the host ID of the node that issues the RREQ), Destination address (the IP address or the host ID of destination), Hop count (length of routing path), Broadcast ID (the value can identify an RREQ uniquely), Sequence number (the current sequence number of the originator), Route expiration time (the predicted lifetime of a reverse path) and TTL (the lifetime of an RREQ).

The RREQ's are propagated to neighbors within the source's transmission range. They also broadcast the packets to their neighbors. The process is repeated until the destination receives the RREQ. When an intermediate node receives the RREQ, it performs the following process:

- When an intermediate node receives the information of RREQ, either it sends the route reply if the node is destination, or it rebroadcasts the RREQ to its neighbours.
- The node decreases the TTL of the RREQ by one. If the TTL is smaller than zero, the host will drop the RREQ.
- The node reads the information from the RREQ.

In order to transmit route reply packets to the source, the node builds a reverse path to the source. The node will insert the path to its multiple path lists. Otherwise, the node will ignore the path and discard the RREQ. The node determines whether the RREQ is redundant or not by checking the pair (source address, broadcast ID). If the RREQ is not redundant, the node will refresh the information of the RREQ and forward the packet to neighbouring nodes. On the other hand, it will drop the RREQ.

Route Maintenance Strategy:

Link failures in ad-hoc networks are caused by mobility, congestion, packet collisions, node failures, and so on. In the AOMDV protocol, the link layer feedback from IEEE 802.11 is utilized to detect link failures. If a node sends packets along the broken link, it will receive a link layer feedback. When a node detects a link break, it broadcasts route error (RERR) packets to its neighbours. The neighbours then rebroadcast the packets until all source nodes receive the packets. If a source node receives the RRER, it will remove every entry in its routing table that uses the broken link. Differing from single path routing protocols, the route error packets should contain the information not only about the broken primary path but also the broken backup paths. When the source node receives the RERR's, it removes all broken routing entries and uses the shortest backup paths as primary paths. The source node initiates a route discovery process where all backup paths are broken

Advantages and Disadvantages of AOMDV:

AOMDV shares several characteristics with AODV. It is based on the distance vector concept and uses hop-by-hop routing approach. Moreover, AOMDV also finds routes on demand using a route discovery procedure. The main difference lies in the number of routes found in each route discovery.

V. PPAOMDV

Protocol Assumptions:

The disadvantages of AOMDV are increases delay, reduce the throughput and overheads are more whenever the route failure problem occurs. The proposed protocol reduces the route failure problem by pre-emptively predicting the link failure based on received signal power by the receiver. The proposed protocol controls the overhead, increases throughput and reduces the delay.

Our goal is to develop a PPAOMDV that preemptively finds weakening links and switches to an alternate path that is learnt from the earlier Route Discovery. We have extended AOMDV to show the achieved performance improvement. AOMDV's Route Discovery and Data Transfer process is modified here.

If the power loss is lesser than the threshold value only then RREQ is further broadcasted. This procedure ensures that routes computed does not include links that are not stable. When such RREQ packets reach the destination it selects paths with minimum power loss. The destination waits for further RREQ packets to know about multiple paths. RREP packet is then generated by the destinations and the source is informed about this. The source now has multiple paths to the destination. Data transmission is initiated over the first path generated. While an active link is used for a data transmission the source checks for a warning. Probability of failure of link is found in cost effective way. Every node waits for an acknowledgement for the packet it has sent .Our algorithm uses this acknowledgement packet to detect diminishing received power.

A Route Maintenance process is initiated when a node detects a link failure by broadcasting a RERR packet. This packet travels through all nodes invalidating corresponding established routes. When this RERR packet reaches the source it re-initiates a Route Discovery process. Thus route maintenance procedure again incurs additional overhead. Our work tries to avoid route breaks. If the failure of a link can be predicted in advance, the routing protocol can switch to an alternate path preemptively and save the route discovery or route maintenance overhead. The performance of any routing protocol improves if it can decrease upon the amount of Route Discovery attempts and Route Maintenance attempts. Thus finding paths that have a longer lifetime is crucial. This paper proposes a novel method to store stable multiple paths and preemptively switch to alternate routes by A Preemptive Multipath Routing Protocol for Mobile Ad-hoc Networks

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 6, December 2013

predicting future link failures. Storing such multiple paths enables routes that have longer lifetime thus decreasing chances of route errors.

Data Structure: In the PPAOMDV protocol, each mobile host maintains a multiple path routing table. Each entry of the table contains following information: destination address, next hop address, hop count, sequence number, route expiration time, maximum route expiration time, and a pointer to the list of backup paths.

The value of sequence number is for determining the freshness of routes. The list of backup paths is used to store all redundant paths. If there is only a primary path, the value of the pointer to the list of backup paths is NULL. Each element of the backup list contains next hop address, hop count, and route expiration time (RET). The value of route expiration time represents the stability of paths. A route with longer route expiration time is more stable. The "maximum route expiration time" is used to compute loop-free multipath.

The maximum route expiration is set as zero initially. When backup paths are found, value of the field is set as the maximum RET among multiple paths.

Route Discovery: The route discovery process has two major phases: route request phase and route reply phase. The route discovery process will be initialed when a route is requested by a source node and there is no information about the route in its routing table.

First, the source node generates an RREQ and then floods the packet to networks. The RREQ includes following fields: Source address (the IP address or the host ID of the node that issues the RREQ), Destination address (the IP address or the host ID of destination), Hop count (length of routing path), Broadcast ID (the value can identify an RREQ uniquely), Sequence number (the current sequence number of the originator), Location information (the velocity, position, and movement direction of the source), Route expiration time (the predicted lifetime of a reverse path) and TTL (the lifetime of an RREQ).

The RREQs are propagated to neighbours within the source's transmission range. They also broadcast the packets to their neighbours. The process is repeated until the destination receives the RREQ. When an intermediate node receives the RREQ, it uses the same process as the AOMDV with some modification they are described below:

1. The node measures its received power (Pr) first. If the received power loss of a host is greater than threshold, the host will discard the RREQ. The node will run out of battery soon so routes with the node will be broken quickly. Therefore, the routes that are less received power can be avoided.

Algorithm 1: Algorithm for Route updates Rule for Route Discovery

Definitions:

RREQ: A route request packet.

RREP: a route reply packet from the destination D to source S.

RRER[1]:Route error packet.

CSThreshold: carrier sense threshold.

Prl: Received power loss.

Begin

Broadcast RREQ to all its neighbours at source node

Receive RREQ at intermediate nodes

C

ompute power loss experienced by RREQ packet at intermediate nodes

If(Prl > CSThreshold) then

Drops the RREQ packets

Else

Forward the RREQ packet

Generate the RREP packet from Destination

Select multiple node disjoint path at the source

End

The flow diagram is as shown below

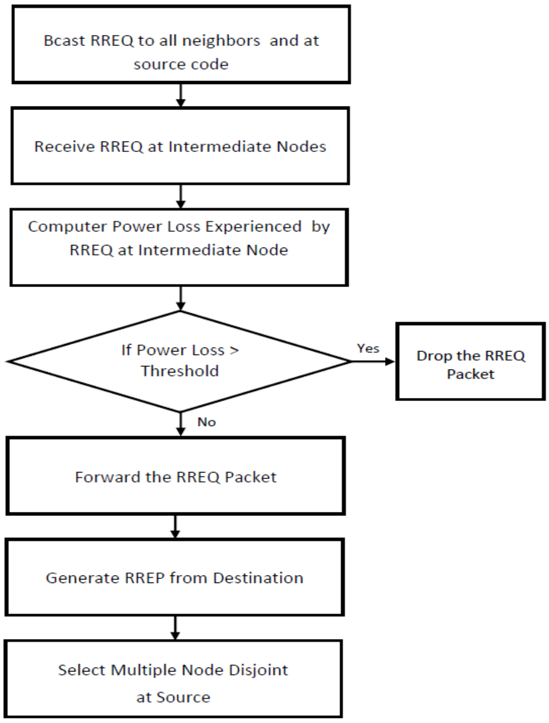


Figure 4.2 Improved Route Discovery Process

Route Reply: When the destination receives the route request packet, it sends route reply (RREP) packet to the source along the reverse paths created previously. The RREP includes the following fields: Source address (The IP address or the host ID of the node that originates the RREQs), Destination address (the IP address or the host ID of the node that initiates the route reply packets), Hop count (The number of hops from the destination to the node that handles the RREP), Destination sequence number (the destination sequence number that represents the freshness of a route), Location information (the velocity, position, and moving direction of the sender) and Route expiration time (the predicted lifetime of a route).

The destination sends RREPs to next nodes of reverse paths. They also forward the packet to next nodes until the source receives the RREP. During processing route reply

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 6, December 2013

packets, each intermediate node performs the following process:

 Thenode reads the location information from the RREP and calculates the received power (Pr) for the sender. If the received power is smaller than threshold then it forwards the warning message to the source.

After the above operations, multiple routing paths are obtained. The PPAOMDV selects the shortest one as the primary path. If there is more than one shortest path, a source will select the path found first. When the primary path is broken, a host switches data traffic to the shortest backup path. During data transmission, the host measures the distance to the next hop using the location information stored in its neighbour table. The host can adjust the transmission power dynamically. Additionally, to improve the effectiveness of backup paths, each host periodically removes invalid backup paths according to the predicted lifetime.

When source node receives the RREP it starts the transferring the data packet from source to destination using the same path. Again while transferring the data packet it goes on checking the Received power (pr). If the Pr is greater than the Threshold then it transfers the data packet otherwise stops transferring the data packet along with this path else selects another path to transfer the DATA packet. The received power is goes on checking at every node.

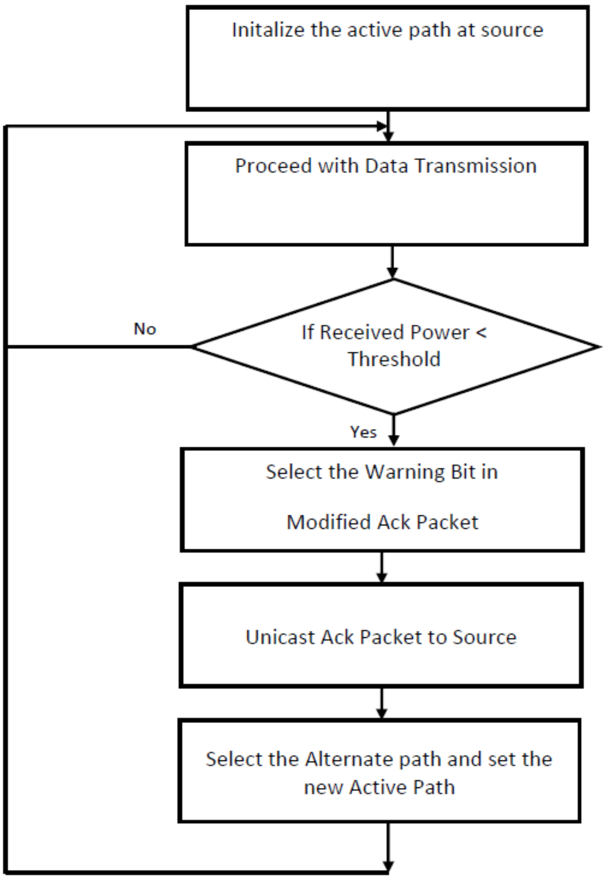


Figure 4.3 Data Transfer Process in PPAOMDV

Algorithm 2: Algorithm for Data transfer Process in PPAOMDV:

Definitions:

RREQ: A route request packet.

RREP: a route reply packet from the destination D to source S.

Ack: Acknowledgement.

CSThreshold: carrier sense threshold.

Pr: Received power.

1. Begin

Intiate the active path at the source

3. Proceed with the data transfer

4. If(pr < CSThreshold) then

5. Set the warning bit in our modified Ack packet

6. Else go to step 3

7. Unicat Ack packet to source

8. Select an alternative path and set a new active path

9. End

Route Maintenance Strategy: Link failures in ad-hoc networks are caused by mobility, congestion, packet collisions, node failures, and so on. In the PPAOMDV protocol, the link layer feedback from IEEE 802.11 is utilized to detect link failures. If a node sends packets along the broken link, it will receive a link layer feedback. When a node detects a link break, it broadcasts route error (RERR) packets to its neighbors. The neighbours then rebroadcast the packets until all source nodes receive the packets. If a source node receives the RRER, it will remove every entry in its routing table that uses the broken link. Differing from single path routing protocols, the route error packets should contain the information not only about the broken primary path but also the broken backup paths. When the source node receives the RERRs, it removes all broken routing entries and uses the shortest backup paths as primary paths. The source node initiates a route discovery process when all backup paths are broken. However, a link failure cannot be detected unless a packet is sent along the link. To solve the problem, a dynamic route maintenance mechanism is used to detect failures pre-emptively in PPAOMDV protocol. When a host receives a data packet from its neighbour, it computes the received power (Pr) of the link. If the host finds that the value of Pr is lower than threshold, the host will send warning message to the source Nodes.

VI. SYSTEM DESIGN

This Section explains the implementation of AOMDV and PPAOMDV in .NET and steps to analyze the AOMDV and PPAOMDV protocols.

Description of AOMDV and PPAOMDV C# Files

.NET consists of many files. Each file corresponds to one basic aspect of the simulator .This section focuses on those files that support the basic AOMDV and PPAOMDV mechanisms.

1.**MANETUI.cs** - This is the main file where all the necessary AOMDV and PPAOMDV Protocols are implemented.

2. **DataPacket.cs** - In this file the packet transmission from source to destination is done.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 6, December 2013

3. **Multipath Routing.cs** – This file shows the multipath routing and its parameters for both AOMDV AND PPAOMDV.
4. **ADHOCNW_Tstparams.cs** – In this file we can test parameter such as time, speed,nodes,packets etc.
5. **TopologyDisplayControl.cs-** In this file we can increase or decrease the nodes.

Implementation

The implementation phase of any project development is the most important phase as it yields the final solution, which solves the problem at hand. The implementation phase involves the actual materialization of the ideas, which are expressed in the analysis document and developed in the design phase. Implementation should be perfect mapping of the design document in a suitable programming language in order to achieve the necessary final product. Often the product is ruined due to incorrect programming language chosen for implementation or unsuitable method of programming. It is better for the coding phase to be directly linked to the design phase in the sense if the design is in terms of object oriented terms then implementation should be preferably carried out in a object oriented way. The factors concerning the programming language and platform chosen are described in the next couple of sections. The implementation stage in a system project has its own right. It involves

1. Careful planning
2. Investigation of the current system and the constraints on implementation.
3. Training of staff in the newly developed system.

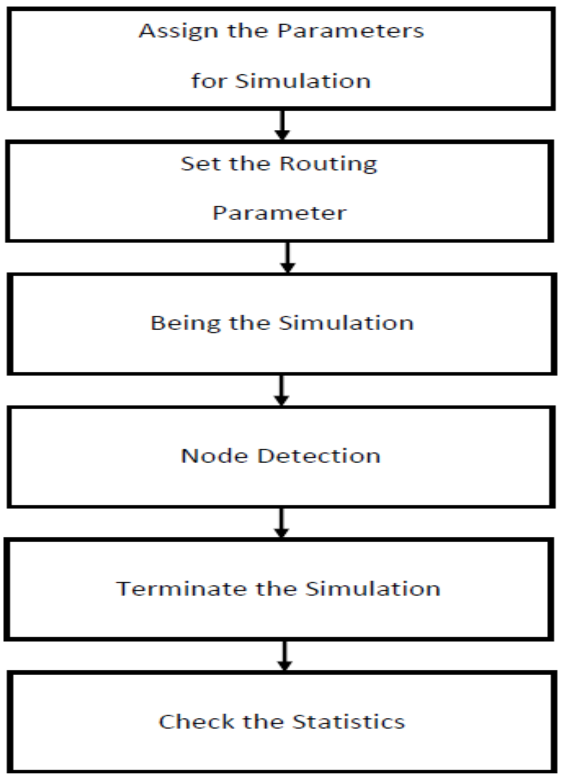


Figure 5.1: Sequence Diagram

VII. SIMULATION AND PERFORMANCE ANALYSIS

Simulation Environment: We have taken two On-demand (Reactive) routing protocols Ad hoc On-Demand Multipath Distance Vector Routing (AOMDV) and Predictive Pre-emptive Ad-hoc on demand Multipath Distance Vector Routing Protocol (PPAOMDV). The mobility model used is Random waypoint mobility model because it models the random movement of the mobile nodes. For all the simulations, the same movement models were used, the traffic source TCP.

Table 6.1: Simulation Parameters

S. No	Parameters	Value
1.	Routing Protocols	AOMDV, PPAOMDV
2.	MAC Layer	802.11
3.	Terrain Size	1000mX580m
4.	Nodes	10,15,20,25
5.	Node Placement	Random
6.	Mobility Model	Random Waypoint
7.	Data Traffic	TCP

Performance Metrics: The following performance metrics used to evaluate the two routing protocols (AOMDV and PPAOMDV):

Throughput: the total size of data packets that are received in destinations per second. It

$$\textbf{Throughput} = \frac{Data\,Transferred}{Simulation\,Time}$$

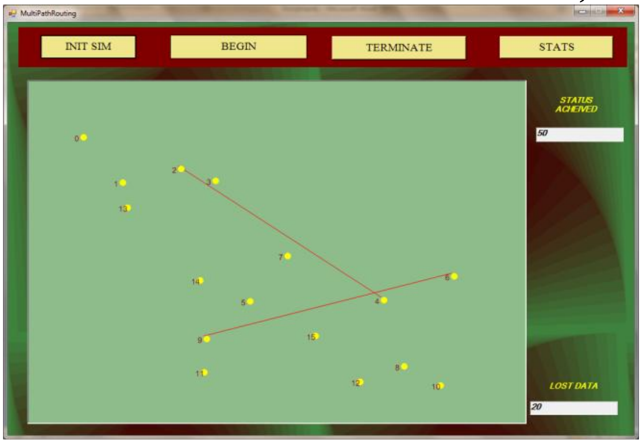
Packet Drop Ratio: Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is distinguished as one of the three main error types encountered in digital communications the other two being bit error and spurious packets caused due to noise.

Network Utilization: Network utilization is the amount of traffic on the network compared to the peak amount that the network can support. This is generally specified as a percentage.

Simulation Results and Analysis:

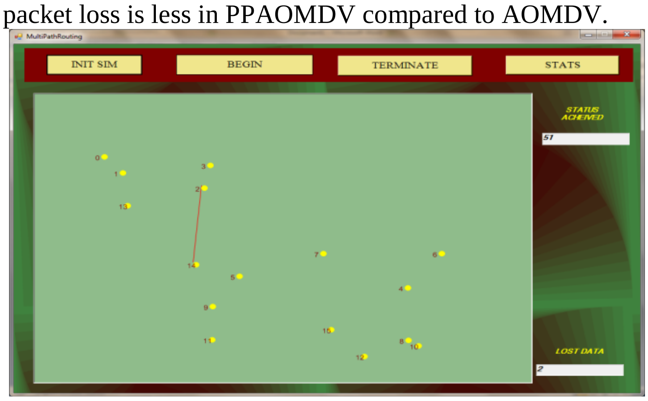
Simulation Result: Begin The Simulation For Node Detection: In AOMDV protocol the nodes are displayed when we click on the INIT SIM button. The data packets are transmitted when click on BEGIN button. The packet loss is more in AOMDV compared to PPAOMDV.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 6, December 2013



Begin the Simulation for Node Detection in AOMDV.

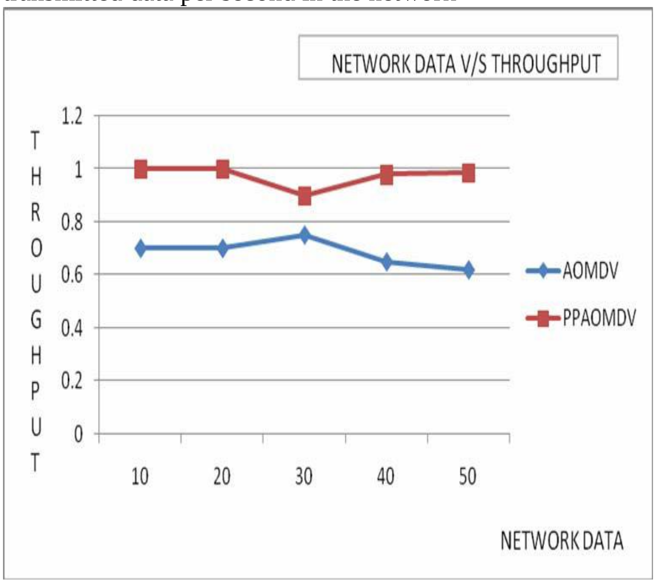
- **Begin the Simulation for Node Detection in PPAOMDV:** In PPAOMDV protocol the nodes are displayed when we click on the INIT SIM button. The data packets are transmitted when click on begin button. The packet loss is less in PPAOMDV compared to AOMDV.



Begin the Simulation for Node Detection in PPAOMDV.

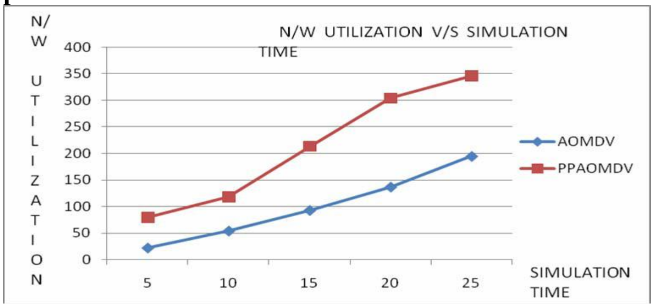
Performance Analysis:

A. Network Throughput: From the above figure 6.3 we conclude that as the traffic load increases both on-demand protocols work better. Throughput of PPAOMDV is high at higher than AOMDV. It is defined as rate of successfully transmitted data per second in the network



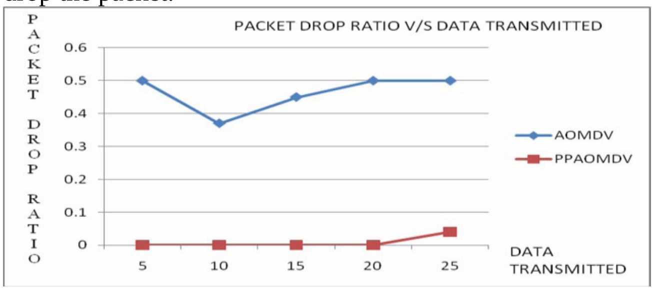
Throughput Comparison of AOMDV and PPAOMDV by varying Network Data.

B. Network Utilization: **In figure 6.4 PPAOMDV has better network utilization compared to AOMDV protocol.**



Network Utilization Comparison of AOMDV and PPAOMDV by varying Simulation time.

C. Packet Drop Ratio: We note that from the figure 6.5 PPAOMDV has a better packet delivery ratio value compared to AOMDV for each set of connections. The PPAOMDV packet drop is very less compared to AOMDV because if power loss is more than threshold means it will drop the packet.



Packet Drop Ratio comparison of AOMDV and PPAOMDV by varying Data Transmitted.

VIII. CONCLUSION AND FUTURE WORK

We proposed a Predictive Pre-emptive Ad-hoc on demand Multipath Distance Vector Routing Protocol (PPAOMD).This was proposed to enhance the benefits of multipath routing protocols by reducing the Route Discovery overhead. The performance of the proposed protocol is better than AOMDV even when the mobility of the nodes is high. The Route Maintenance procedure is triggered less frequently as compared to the AOMDV. This is because source would always have multiple paths in its repository and if the power loss in a path degrades then immediately it can select from the other available paths.

The proposed protocol enhances the benefits of multipath routing protocols by reducing the Route Discovery overhead. The performance of the proposed protocol is better than AOMDV even when the mobility of the nodes is high. The Route Maintenance procedure is triggered less frequently as compared to the AOMDV. This is because source would always have multiple paths in its repository and if the power loss in a path degrades then immediately it can select from the other available paths.

Future Work

1. Can be defined in physical constraints for military mobile devices.

2. New applications call for both bandwidth and capacity, which implies the need for a higher frequency and better spatial spectral reuse.
3. As it is Suitable for MANET can be implemented on other routing protocol and can be utilized in multimedia applications.
4. **Quality of service (QoS) –** Ad-hoc routing protocols must meet the desired requirements of QoS to achieve lower end-to-end delay, high throughput improved delivery ratio, reduced routing overhead and more energy efficiency.
5. **Security-** A vital issue that has to be addressed is the security in Ad hoc networks. Applications like Military and Confidential Meetings require high degree of security against enemies and active /passive eavesdropping attackers. A new protocol must have authentication headers and necessary key management to distribute keys to the members of Ad hoc networks.
6. **Energy Aware Routing –** Since mobile nodes are working on small portable batteries in most of the applications, developing an energy aware routing protocol, which maximizes the life of batteries, is of paramount importance.

REFERENCES

[1] Internet Engineering Task Force (IETF) MANET working group, "Mobile Ad-hoc Networks (MANET. Available at http://www.ietf.org/html.charters/manet-charter.html),"December, 2001.

[2] Marina, M.K., Das, S.R.: "On-demand Multipath Distance Vector Routing in Ad Hoc Networks", Proceedings of the International Conference for Network Protocols (2001).

[3] T. Goff, N.B. Abu-Ghazaleh, D.S. Phatak and R. Kahvecioglu, "Preemptive Maintenance Routing in Ad Hoc Networks", Journal of Parallel and Distributed Computing, Special Issue on Wireless Mobile Communication and Computing, 2003 (extends the Mobicom'01 paper).

[4] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal, Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges.

[5] Lee, S.-J., Gerla,M,"SplitMultipath Routing with Maximally Disjoint Paths in Ad Hoc Networks", IEEE International Conference on Communications, Vol. 10 (2001).

[6] Mrs.Sujata V.Mallapur, Prof. Sujata .Terdal "Enhanced Ad-Hoc on Demand Multipath Distance Vector Routing Potocol (EAOMDV)". Proceedings of the International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010.

[7] Sujatha P. Terdal1, V.D Mytri2, and A Damodaram3 "A Preemptive Multipath Routing Protocol for Mobile Adhoc Networks". Proceedings of the International Journal of Computing Science and Communication Technologies, VOL. 2, NO. 1, July 2009. (ISSN 0974-3375).

[8] Manoj Kumar Singh, Brajesh Kumar, Chiranjeev Kumar, Manish Gupta "Preemptive Multipath—Adhoc on Demand Distance Vector Routing Protocol". Proceedings of the International Journal of Computer Science & Information Technology Vol. 1 No. 1 Jan. 2011 Proc. of the Seventh CaberNet Radicals Workshop, October 2002.pp. 36-40 36.