Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Stable AODV Protocol in Mobile Ad-Hoc Network

Shivinder Kapoor*
Department of Electronics & Comm. Engg.
SRMIET, Kurukshetra University, India

Pushparaj Pal
Department of Electronics & Comm. Engg.
SRMIET, Kurukshetra University, India

Sachin Gupta
Department of Electronics & Comm. Engg.
SRMIET, Kurukshetra, University, India

Monika Sharma
Department of Electronics & Comm. Engg.
HCTM, Kurukshetra, University, India

Abstract— An ad hoc network is a mobile wireless network that has no fixed access point or centralized infrastructure as we discussed in introduction. Each node in the network also functions as a mobile router of data packets for other nodes. However, due to node mobility, link failures in such networks are very frequent and render certain standard protocols inefficient resulting in wastage of power and loss in throughput. MANET supports multi hop routing where the nodes other than the source and the destination nodes also take part in packet forwarding from one end to the other end. This results in the energy consumption of the intermediate nodes even though they are not the actual sender or receiver of the data. The available battery power of the nodes decides the life time of the node as well as the whole network. Mobile ad hoc networking is a challenging task due to the frequent changes in network topology as well as the lack of wireless resources. As a result, routing in such networks experiences link failure more often. Hence, it is essential that a routing protocol for an ad hoc network considers the reasons for link failure to improve the routing performance. Link failure stems from node mobility and lack of network resources both resides in wireless medium and in nodes. Therefore it is essential to capture the characteristics to identify the quality of nodes and hence the quality of links.

Keywords— Ad-hoc Network, MANET, Node Mobility, MAC Layer, S-AODV.

I. INTRODUCTION

A mobile ad hoc network is a dynamically self-organizing network without any central administrator or infrastructure support. If two nodes are not within the transmission range of each other, other nodes are needed to serve as intermediate routers for the communication between the two nodes [1]. Moreover, mobile devices wander autonomously and communicate via dynamically changing network. Thus, frequent change of network topology is a tough challenge for many important issues, such as routing protocol robustness, and performance degradation resiliency [2-12].

Proactive routing protocols require nodes to exchange routing information periodically and compute routes continuously between any nodes in the network, regardless of using the routes or not. This means a lot of network resources such as energy and bandwidth may be wasted, which is not desirable in MANETs where the resources are constrained [1-3].

On the other hand, on-demand routing protocols don't exchange routing information periodically. Instead, they discover a route only when it is needed for the communication between two nodes [1, 6, 7].

Due to dynamic change of net- work on ad hoc networks, links between nodes are not permanent. In occasions, a node cannot send packets to the intended next hop node and as a result packets may be lost. Loss of packets may affect on route performance in different ways. Among these packet losses, loss of route reply brings much more problems, because source node needs to re-initiate route discovery procedure. In this study we propose a power aware routing protocol which has a new aspect to find out path between source to destination according to available power of node.

II. RELATED WORK

It is a requirement for every network to have some form of reliable communication where the delivery of the packets to the destination is guaranteed. For wired networks and static wireless networks Transmission Control Protocol (TCP) is the connection-oriented transport layer protocol that guarantees this functionality. It assures in-order delivery of the packet and uses flow control and congestion control mechanisms. For ad hoc networks however the standard TCP does not give satisfactory performance. In the ad hoc network the nodes are travelling and there are no base stations. In other words the topology of the network is constantly changing. The communication between the sender and receiver nodes occur through other nodes in the network and each of the intermediate nodes is acting as a router for the communication. The connection can have multiple hops. This causes performance losses due to the high error rate, network congestion and possible connection failure.

There are various methods for detecting and improving the link failure problem in Ad-Hoc Network.

Explicit Link Failure Notification [7]

One possible solution for the link failure problem is to implement the Explicit Link Failure Notification (ELFN). Since all nodes acting as routers have the full TCP/IP protocols stack, they have access to the routing protocols of the IP layer. The routing protocol can detect the link failure when the next node in the connection goes out of range, and the packet cannot be delivered. It sends the route error notification (RRER), which is flooded to all of the nodes including the source node. This error notification however does not reach the transport protocol, and it is only used by routing protocol to update the routing table. The TCP/IP protocols stack can be altered to use the RRER packet as the link failure notification. After the modifications, when the RRER packet is received, TCP can distinguish this link failure from the congestion. It can enter the "standby" mode by freezing the regular transmission of the packets until the connection is re-established and then resume the transmission.

Detection of Failed Link in Mobile Ad Hoc Network [9]

Ad hoc routing protocols may detect broken links using 1) hello messages , 2) feedback provided to the protocol by the MAC layer and 3) passive acknowledgements

1. Hello messages

The reason of using hello messages to determine link existence come from the assumption that receiving of a hello message signifies link availability with the source of the hello. This method works well on wired networks, which suffer from few packet losses and topology changes. In order to keep up routes, AODV usually demands that each node transmits a hello message at regular intervals (if the node has not broadcasted any other control messages during the previous second), with a default rate of e.g. once per second. Inability to receive three successive hello messages from a neighbor is interpreted as a sign that the link to the given neighbor is failed. When AODV is run over IEEE 802.11, Hello messages do not need to be used due to the MAC layer feedback of unreachable next hops. When combined with the other MAC protocols, however, Hello messages are needed since such feedback is not available. Many current implementations of routing protocols rely on hello messages.

2. MAC Feedback

Alternatively, the AODV standard proposes that a station may use MAC layer methods to find out link failures to neighboring nodes**.** This approach gives the routing protocol the possibility to quickly find broken links. MAC layer feedback are callbacks to the network layer sent by the MAC layer explicitly declaring a transmission error indicating that a packet could not be forwarded to its next hop node.

3. Passive acknowledgements

If MAC layer feedback is not available, DSR specifies other approach, known as passive acknowledgments, in which a node, after a packet transmission to the next hop on the route, continues to listen the channel and overhears whether the next hop forwards the packet further along the path. If it doesn't hear the forwarding of the packet during predefined time, it draws a conclusion about link failure. The mechanism of passive acknowledgments suffers from the fact that it requires from WLAN network cards a support of promiscuous mode, which is extremely energy-expensive. Ericsson Simulation Work [10] showed that low power devices such as Bluetooth consume roughly 50% more energy as the receiver would frequently need to decode all packets besides its own packets.

Local Route Repair Algorithm Based On Link Failure Prediction In Mobile Ad Hoc Network [10]

AODV has been proposed by IETF and it is intended for use by mobile nodes in an Ad Hoc Network. It provides local repair to recover the route when a link break in an active route occurs. But local repair is only performed when a node has already detected broken link and the detection consumes too much time. There is also other proposal in which the node listens in all frames including data packets and routing control packet to maintain local route cache. The fast route discovery and local recovery is achieved by local route cache when a broken link occurs. The drawback of this scheme is that nodes maintain backup routes would consume additional energy. LRR scheme assumes that the relative movement of only one node on the route causes the link error. AODV-BR is the modified protocol from AODV literally. The basic route discovery process has not been changed. In this, every node in the network operates as promiscuous mode. The continuous operation in a promiscuous mode can cause excessive energy consumption and reduce network efficiency. Some researchers use directional antennas to improve routing. But in reality most of the antennas are Omni-directional antennas.

Working of AODV

For convenience we divide the functioning of AODV into Route discovery and Route maintenance Phases. After a route is discovered, actual routing occurs by looking up the routing table and sending the packet to the next hop for its destination Route Recovery .A source node initiates route discovery only when it has a packet to send to a destination to which it does not possess a valid route. Route discovery is initiated by the source flooding Route Request (RREQ) packets through the network. Every node that receives a RREQ creates a short-lived reverse route to the source with the next hop being the node from whom the RREQ was just received. RREQ reaches the destination or a node with a valid route, that node responds with a Route Reply (RREP) which travels to the source along the reverse path. All nodes that route the RREP to the source also make corresponding forward entries in their routing table such that the next hop to the destination is the node from which the RREP was just received. The source, on receiving the RREP starts sending data. Each RREP also contains a destination sequence number, which is used to prevent routing loops and helps nodes determine the freshness of routing information.

Route Maintenance

Each node broadcasts periodic HELLO messages to advertise its presence. A node learns that a link to a neighbor is broken when it does not receive a HELLO from that neighbor for a predetermined time. When a broken link is detected, the detecting node sends Route Error (RERR) messages to all predecessor nodes that use the broken link to reach their respective destinations. This RERR packet travels back to the sources who reinitiate route discover.

LRAODV_LP Routing protocol

We have incorporated following changes in LRAODV_LP(Local Repair AODV based on Link Prediction) Each node maintains two tables NPL (Neighbor Power List) and PDT (Power Difference Table), Link failure Threshold (LFTHRSH) and one LFF(Link Failure Flag) NPL contains the last received signal strength for packets originating from each neighbor. This table is updated whenever a packet is received and happens at least once every Hello interval. PDT contains the rate at which power is changing between each pair of neighbors. PDT describes whether the link signal strength which is changing between each pair of neighbors is increasing or decreasing. This table is also update whenever a packet is received. In our Algorithm, when the link strength is under LFTHRSH, the quality is so poor that we think the link is already broken. A node checks the two tables periodically. When it finds the link strength is decreasing and is under LFTHRSH for a defined time, Let the LFF of the link equal to one that means link is broken and a local route repair algorithm is executed. If route is established, the route reply RREP is sent to the source node which in turn sends the data to the destination. Otherwise a route error message is sent and let the LFF of the link is equal to zero.

Improving Reliability of Packet Delivery in MANETs by a Holistic Routing Approach[13]

Link Quality

In a multi-hop MANET, packets in transmission may be received with noise and interference. It is the physical layer and data link layer protocols' responsibility to decode individual bits from the interfered signals. All bits can be decoded correctly if the SNR is higher than a threshold. When the SNR is lower than the threshold, bit errors occur during the transmission, causing the receiver to drop some data packets. Using different types of physical and data-link layer protocols may change the probability of packet losses at each link among different systems. To compare the performance of different routing protocols in terms of the PDR, we assume that similar lower layer protocols are employed such that all peer routing protocols share an identical packet loss probability, P, in a connected link. In order to simplify the simulations, we also assume that the probability, P, is identical for all connected links. The only condition when this probability may change is when a link is disconnected due to node mobility.

Node Mobility

Nodes may move arbitrarily inside MANETs. This unbounded nature of nodes in MANETs makes MANETs exible in deployment. However, it also makes links in MANETs instantaneous. The probability of successful packet transmissions between two nodes using wireless channels can be low when the distance between these two nodes is large. The link between these two nodes can be regarded as completely failed when their separation is larger than a threshold. Generally, the threshold is referred to as the communication range. In the rest of this report, we assume that a link between two nodes ceases to exist when the distance between these two nodes is larger than the communication range. Otherwise, all links have a constant quality, in which the probability of successful transmissions through this link is equal to P. To handle packet losses caused by node mobility or network congestion, the holistic routing protocol does not depend on any previous knowledge of its neighbors. Instead, it integrates the next-hop forwarder discovery function with the lost link recovery approach in its operation to dynamically replace failed links or links to congested nodes.

Network Density

The network density, which is represented by the average number of neighbors of a node, may change dramatically in different application scenarios. Some protocols control the density of wireless networks by putting nodes into sleep mode, thus saving energy and controlling channel conflicts. However, to keep the network fully connected, the average node's degree should not be too small. There may be more than one node that can receive a transmitted data packet. Due to the multicasting nature of wireless communications, it is possible that when a transmission failure happens at one link, other neighbors of the transmitter can overhear the data packet by opportunistic reception, improving the reliability of packet transmissions in a multicasting network. The holistic routing protocol takes advantage of this feature to improve the success rate of each packet-delivery hop.

On the other hand, when a network becomes dense, the probability of channel contention increases. If no mechanism controls packet losses caused by the increased channel contention, the PDR may go down. The holistic routing protocol uses the joint decision-making mechanism to select the optimal forwarding candidate as its next-hop forwarder in every packet transmission hop. Simulation results demonstrate that this can improve the reliability of packet transmissions in a network where multiple packet-loss types coexist.

PROBLEM DEFINITION

If source A want to send data to the destination D then first of all source A must have a path between source to destination. If source have a path between source A to destination D then source does not knew how match amount of time this path remain alive. When source a send data packet to D then it may be deliver to destination or may be not deliver due to link failure and this link failure occur due to lake of power of the node.

So we are proposing a power aware routing protocol that provides accurate power information of current path used by source for communication.

III. PROPOSED WORK

Ad hoc On Demand Distance Vector (AODV) is a routing protocol designed for ad-hoc mobile networks. AODV is a reactive protocol, capable of both unicast and multi-cast routing. It searches for routes between nodes only when desired by source node and maintains these routes only as long as they are needed by the sources. We are proposing a new routing technique to find out a stable route from source to destination in terms of power of current path. In this technique we calculate the stable path based on available power of node which is going to use for communication.

In this algorithm following terms are used for calculation.

i. Broadcast ID:

The broadcast id is a number stored in packet header which is incremented before a new request is disseminated.

ii. Source Address:

Source address is address of source node which is used to send the request between source and intermediate node.

iii. Destination Address:

Destination Address is address of destination node which is used to receive the reply from the source or intermediate nodes.

iv. **Available Power list**:

This field contains the available power of the node which is used in current path for communication.

PHASES OF ANALAR

There are three phase in this protocol

i. Route discovery
ii. Route Reply
iii. Route maintenance

1. Route discovery

Procedure of proposed technique: This technique has following step to process the route request process

- When a node receive route request packet (RREQ) then it check for TTL of the packer.
- If TTL is less than zero the node have to drop this packet.
- Else it receives the packet and check for destination node. If node id is equal to destination id then node accept the RREQ packet and perform following calculation by using received packet.
    a. Calculate Average up time of current path.
    b. Calculate minimum power node of current path.
    c. If minimum power node is greater than the threshold power then node sends RREP to source node by using same path with current path and up time value.
- If node id is not equal to destination id then node process the RREQ packet as follows:
    a. Node add the node id to visited node list in the RREQ packet header.
    b. Node add up time value of node in to up time list of packet header.
    c. Node add available power of the node into available power list.
    d. After adding these information into packet header, node flood RREQ packet to their neighbor node.

2. ROUTE REPLY PHASE

In route reply phase if destination receives the RREQ packet then it check the packet header destination address. If destination address is the address of node then it check the power of the node. If power is greater than or equal to the minimum power the destination consume the RREQ packet and sent RREP packet to source node via same path which path is use to receive RREQ packet from source to destination. Otherwise discard the RREQ packet. Path shows the Route Reply Phase in which reply is sent back from Destination to Source with the help of intermediate nodes D-7-4-1-S

3. ROUTE MAINTENANCE

In Ad-hoc network there is high mobility of nodes, links between nodes are likely to break. Thus, we need to maintain the routing path. When the node move outside to the reach of its neighbor then route from source to destination is break i.e RERR is occurred. In this case route maintenance process is use to maintain the route from source to destination. In this phase when a node does not receive a RREP packet it will break the path. In this case, the node sends a route error (RERR) packet to the source node. When the source node receives the packet, it will reconstruct a new path to the destination node. In path node 4 does not contain the sufficient minimum power so path is break. Then again new path is created by using node 2. So the source to destination path after maintenance is S-1-2-5-7-D.

IV. SIMULATION

In order to validate the proposed protocol and show its efficiency we present simulations using MATLAB. MATLAB is a very popular network simulation tool. MATLAB is an interactive software package which was developed to perform numerical calculations on vectors and matrices.

Parameter	Setting Value
Network Area	150-150
Number of mobile nodes	10 to 35
Mobility model	random
Node transmission range	20

Table 4.1 Simulation Environment Settings

The simulation environment settings used in the experiments are shown in Table4.1. The network area is 150 pixels x 150 pixels that include variable number of mobile nodes ranging from 15 to 35. The radio transmission range is assumed to be 20 pixels. The scenario of nodes mobility is generated randomly based on random way point model where a mobile node moves to a new position and pauses there for time period between 0 to 3 seconds, then it move to another position.

Simulation Results For Packet Delivery Ratio With Number Of Nodes

Figure 4.1 shows the packet overhead with different number of node. It suggests that when the number of node increases then packet overhead is also increases.

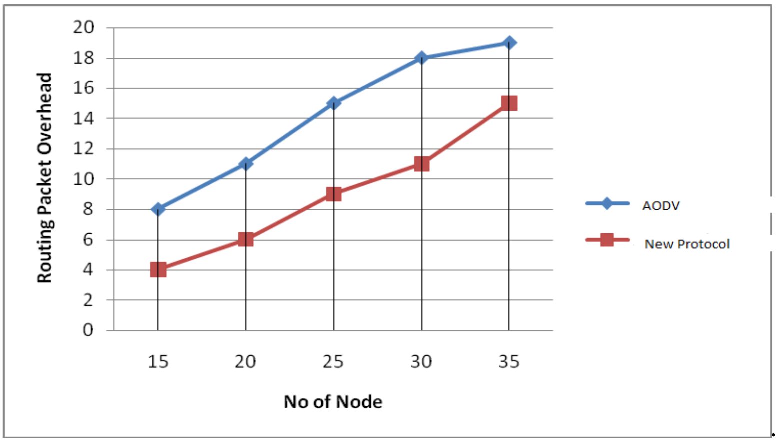

Fig 4.1 Chart between packet overhead and number of node

Simulation Result for Packet Delivery Ratio With Number Of Nodes Between S-AODV And Shortest Path Protocol

Figure 4.2 show the compression between S-AODV and shortest path protocol in terms of packet delivery ratio (%) and different number of mobile nodes. When number of node increase then packet delivery ratio is increases in both the protocol but S-AODV provide more better packet delivery ratio than shortest path protocol.

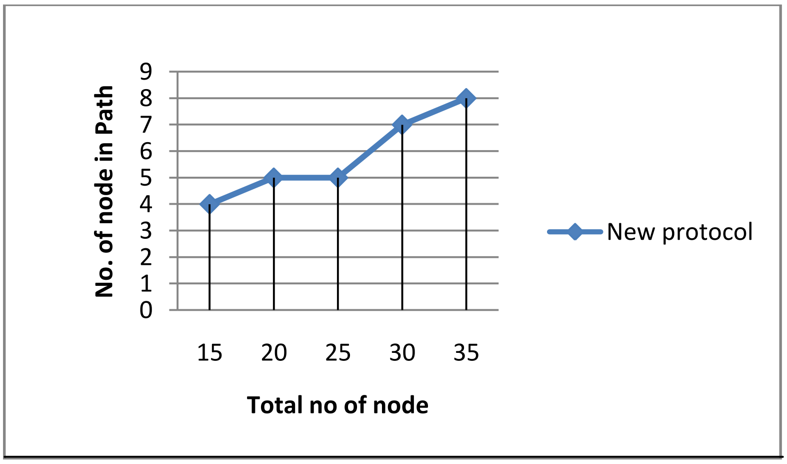

Fig 4.2 chart between average number of node in path and number of node

V. CONCLUSION & FUTURE WORK

In this thesis we outline the characteristics of ad hoc mobile networks and present previous work on different methods to resolve the problem of broken link in MANET. Most of the protocols have concentrated on how to quickly reorganize the ad hoc network during times of mobility and how to find the best route without increasing control overhead. However, since mobile hosts have limited battery resources, ad hoc mobile networks should consume battery power more carefully and efficiently to prolong network operation lifetime. In this thesis, I propose routing protocol is use to improve the link failure prediction in terms of power between source to destination. This routing protocol determines the minimum available power between source to destination. Then source node decided the path which has maximum available power between source node to destination node. By using the S-AODV protocol, improve the link failure problem due to power in between source to destination.

Future Perspective:

Our S-AODV (Stable AODV) protocol only provides service in terms of link failure improvement due to power. But link failure is also occur due to transmission range and movement of nodes and congestion etc . So in future our proposed protocol can be reconstruct to generate new protocol in terms of transmission range and movement of nodes that will improve the problem of link failure in Mobile Ad Hoc Network.

REFERENCES

[1]. Natrajan Meghanathan, ”A Location Prediction-Based Reactive Routing Protocol to Minimize the Number of Route Discoveries and Hop Count per Path in Mobile Ad Hoc Networks” *Department of Computer Science, Jackson State University, Jackson, MS 39217, USA.*

[2]. Y.B. Ko and N. H. Vaidya, "Location-Aided Routing in Mobile Ad Hoc-Scale for Ad Hoc Networks," *Proceedings of the second ACM international symposium on Mobile ad hoc networking & computing, Long Beach, CA, USA, pp. 22-32, October 2001*

[3]. G. Dommety and R. Jain. "Potential Networking Applications of Global Positioning System (GPS)," *Technical Report TR-24, Computer Science Department, The Ohio State University, April 1999*

[4]. M. Mauve, J. Widmer, and H. Hartenstein. A Survey on Position-Based Routing in Mobile *Ad-Hoc Networks. IEEE Network, 15(6):30–39, November/December 2001*

[5]. D. D. Perkins and H. D. Hughes, “A survey on quality-of-service support for mobile ad hoc networks,” *Wireless Communications and Mobile Computing, 2002*

[6]. P.K.Suri Dr. M. K. Soni, Mrs. Parul Tomar” Location Based Power Aware Routing”

[7]. Martin Mauve and Jörg Widmer, “A Survey on Position-Based Routing in Mobile Ad Hoc Networks”, *IEEE November/December 2001, pp. 31-39*

[8]. Wenzhu Zhang, Jiandong Li and Xuan Wang, “Cost-Efficient QoS Routing Protocol for Mobile Ad Hoc Networks”, *Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA’05).*

[9]. Nen-Chung Wang , Si-Ming Wang, “An Efficient Location-Aided Routing Protocol for Mobile Ad Hoc Networks”,*11th International Conference on Parallel and Distributed Systems (ICPADS'05), 2005*

[10]. Tzay-Farn Shih , Hsu-Chun Yen, “Location-aware routing protocol with dynamic adaptation of request zone for mobile ad hoc networks”, *Springer Wireless Netw (2008) 14:321–333,DOI 10.1007/s11276-006-9955-y*

