

Router Handoff: A Preemptive Route Repair Strategy for AODV

Srinath Perur, Abhilash P. and Sridhar Iyer
K.R. School of Information Technology
IIT Bombay
e-mail: {srinath, abhilash,
sri}@it.iitb.ac.in

ABSTRACT

Link failure caused by node mobility is a common feature of multi-hop, wireless ad hoc networks. With a reactive routing protocol such as AODV (Ad hoc On-demand Distance Vector), this leads to increased delay and routing overheads while route repair procedures are carried out. We present a strategy called Router Handoff wherein a node that detects one of its links weakening, preemptively hands off routing information to a suitably situated node. This results in routing around the weak link and prevents the route from being broken. Our simulation results show that this approach leads to increased throughput and reduced routing overheads in most cases.

I. INTRODUCTION

Mobile ad hoc networks are multi-hop, wireless networks that can function without the presence of fixed infrastructure. When two nodes are not within radio range of one another, they use intermediate nodes to route packets for them. A routing protocol is used for route discovery and maintainance. Ad hoc routing protocols can be classified as proactive and reactive. Proactive protocols maintain up to date routes to all destinations, while reactive protocols discover routes to destinations only when needed. One such reactive protocol is AODV (Ad hoc On-demand Distance Vector) [1]. It finds a route to a destination by flooding the network with route request packets till the destination, or another node with a valid route to the destination is found. This node sends a reply which traverses in reverse the path taken by the request packet to reach the destination. All nodes along this reverse path make appropriate entries in their routing tables for the destination and establish a route. Link failure due to node mobility is a common feature in ad hoc networks. When a node that is part of an active route moves, the route breaks and has to be repaired by flooding the network for a new route. While there are several schemes that try to minimize flooding to repair routes, it remains a major source of routing overhead. Further, there is a significant delay in *detecting* a broken link on a route. In this paper, we propose *Router Handoff* as a preemptive approach to deal with route failure. Router Handoff tries to detect a weakening link *before* it fails, and tries to find suitable nodes in the vicinity which can participate in routing around the affected link. Routing information, such as relevant parts of the routing table, are handed off to any such nodes that are found. This happens only in the vicinity of the weakening link and is transparent from other nodes along the route. If no suitable node can be found to perform the handoff, standard AODV route repair occurs as a matter of course after the link breaks. Router Handoff can be thought of as trying to retain routing information in the locality of its use. We have incorpo-

rated Router Handoff into the AODV implementation and have run simulations to assess its impact on routing performance. The main contribution of this paper is in proposing Router Handoff as a mechanism for preemptive route repair in ad hoc networks.

In Section II we present an introduction to the working of the AODV protocol; in Section III we present details of the working of Router Handoff and its incorporation into AODV; in Section IV we provide details of our simulations and their results. Related work is mentioned in V and we conclude with some observations and possible extensions of this work in Section VI.

II. Working of AODV

For convenience, we divide the functioning of AODV into route discovery and route maintainance 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.

A. Route Discovery

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. When a 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 tables 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.

B. Route Maintainance

Each node broadcasts periodic HELLO messages to advertise its presence. A node learns that a link to a neighbour is broken when it does not receive a HELLO from that neighbour 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 re-initiate route discovery.

III. Router Handoff in AODV

The decision to handoff is made by a node based on perceived signal strengths of its neighbours with whom it forms part of an

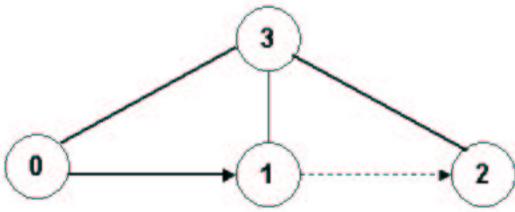


Fig. 1. Link 1-2 becoming weak

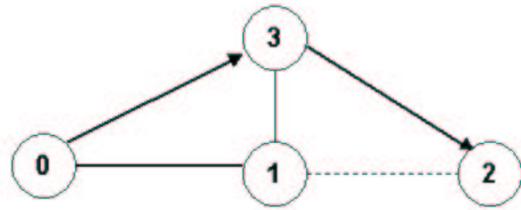


Fig. 2. After Handoff

active route. We maintain power information at nodes in terms of the *ratio of received power to the receive threshold power*. When this ratio drops below 1, a node can no longer be heard. The decision to handoff because of a weak link is made when one end of the link senses that the ratio has dropped below a *Handoff Threshold (HTHRESH)*. This value is typically set slightly greater than 1 to give adequate time to handoff before the link breaks.

We have incorporated Router Handoff into the AODV protocol by making these changes:

- Each node maintains a *Neighbour Power List (NPL)* containing the last received signal strength for packets originating from each neighbour. This table is updated whenever a packet is received, and happens at least once every Hello interval.
- Each node also maintains a *Power Difference Table (PDT)*. This table consists of the rate at which power is changing between each pair of neighbours. Entries for links of which this node is one end, are filled directly by calculating the difference in powers between a received packet and the entry in the NPL for the last received packet from that neighbour. Entries for links between two neighbours are received in the modified Hello packet.
- Hello packets are modified to contain neighbour power information. While sending out a Hello packet, each node examines its NPL and PDT and finds neighbours with whom it has a strong link. Here, a strong link is defined as one whose strength is not decreasing and is above HTHRESH. Power entries are stored in power levels ranging from 0 to 255. Hence, for each strong link, a Hello packet contains the address of the neighbour and a single byte representing the the rate of change of that link as determined from the PDT.

Since power information is communicated through Hello packets, and Hello packets are sent at intervals of approximately one second, we found that this information was often not fresh enough for purposes of performing Router Handoff. Therefore, *predicted link strengths* are used as determined from the NPL and PDT.

A. Handoff

Every node that is part of an active route, checks its predecessor link and next link strengths periodically for each route. This is timer driven and occurs every 0.25 seconds in our implementation. If a node detects that *either* the previous or next link along an active route is predicted to fall below the HTHRESH before the next execution of the handoff timer, it initiates Router Handoff. For every predecessor node P , and next hop N , it searches the PDT for a neighbour H that has a link with stable or increasing link strength with both P and D . This node H is the handoff node. Next, it prepares a Handoff packet with the addresses of itself, P ,

H , the destination for that route, D , and the routing table entry for D containing hop-count, sequence number and route lifetimes. This handoff packet is broadcast with the Time To Live (TTL) field in the IP header set as 1. Several such handoff packets may be sent since a link may be participating in multiple active routes simultaneously. If no suitable handoff node is found, no action is taken and the route is allowed to fail following which standard AODV route repair procedures are used.

When P receives a handoff packet, it changes its next hop for destination D from the sending node to H . H on receiving the handoff packet, checks if it already has a better route to destination D , and if not, creates a route with details from the handoff packet.

B. Example

In Fig. 1, node 0 is routing packets to node 2 through node 1. This can be thought of as an entire route, or part of a longer route. While examining link strengths, node 1 detects that its link with node 2 is weakening and decides to handoff. This may be due to the mobility of node 1, node 2, or both. After looking through its PDT, node 1 finds that node 3 has non-decreasing link strengths and can be heard by both node 0 and node 2. Node 1 broadcasts a handoff packet containing the addresses of nodes 0, 2 and 3 as predecessor, next, and handoff nodes respectively. It also contains the address of the destination and the corresponding routing table entries. Node 0 on receiving the handoff changes its next hop for the destination indicated to node 3, if it was node 1 earlier. Node 3 enters node 2 as a next hop to the destination indicated in the handoff packet, if it lacks a better route to that destination. Figure 2 shows the same route after handoff.

After handoff, the old route continues to be functional and this prevents routing errors due to the predecessor node routing a packet to the handoff node before the handoff node has received the handoff packet. It is also possible that two nodes attempt to handoff on detecting that the link between them is weakening. The chances of this happening are minimized by introducing a random delay before each node checks for handoff. As a result, one node hands off earlier than the other. In the rare event of a simultaneous handoff, the route may be broken and standard AODV route repair procedure is used.

IV. Simulations

We have incorporated Router Handoff into the AODV implementation in the network simulator, ns-2.1b8a [2]. We performed several experiments to assess the impact of Router Handoff on throughput and routing overhead. The default implementation of

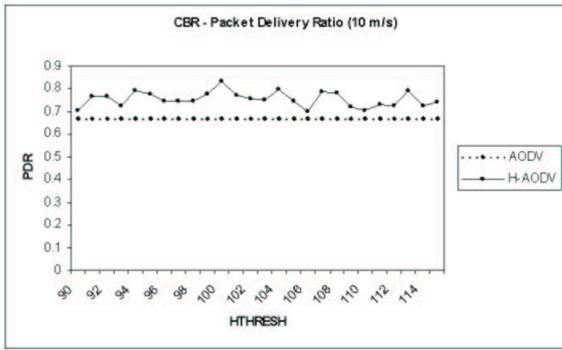


Fig. 3. CBR - Packet Delivery Ratio

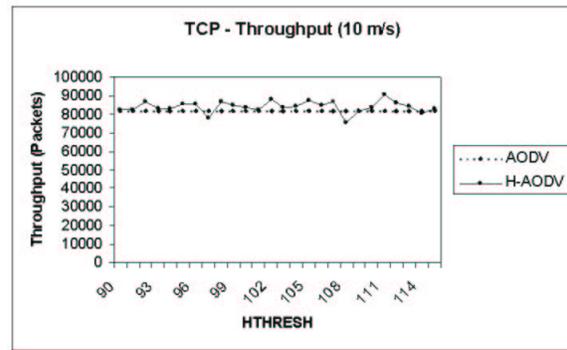


Fig. 5. TCP - Throughput

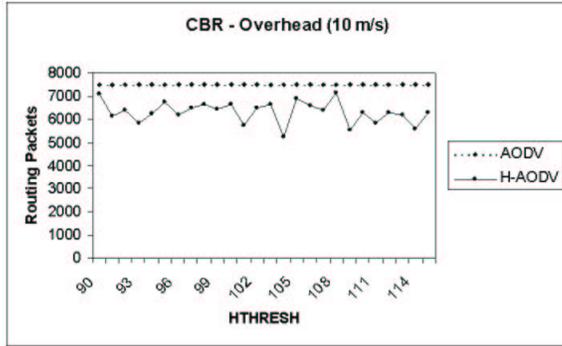


Fig. 4. CBR - Routing Overhead

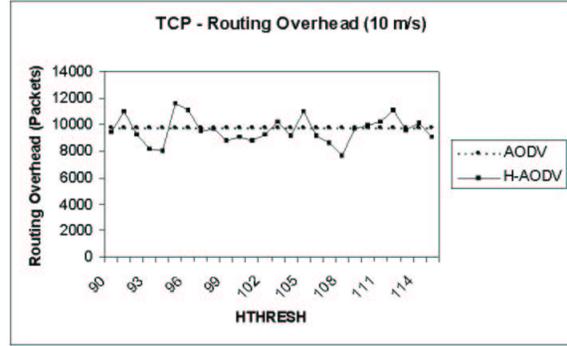


Fig. 6. TCP - Routing Overhead

AODV in the simulator was used in our experiments. We refer to the version of AODV with Router Handoff incorporated as H-AODV. For the results we present in this paper, we ran simulations with 80 nodes spread randomly over an area of 2000m x 500m for 300 seconds. The nodes moved with a maximum velocity of 10 m/s following the random-waypoint model. Pause time was set at 7 seconds. We conducted simulations for CBR (Constant Bit Rate over UDP) and FTP (over TCP) sources. For both CBR and TCP experiments we used 40 connections of 30 seconds each. All data packets were 512 bytes in length. The CBR source rate was 4 packets per second. Maximum TCP window size was 32. In case of CBR, we measured the Packet Delivery Ratio (PDR) as a performance indicator. For TCP, we used total number of packets received at destinations as a measure of throughput. Routing overhead for AODV was calculated as the total number of RREQ packets sent in the simulation, while for H-AODV it was taken as total number of RREQ and Handoff packets sent. We neglected RREP and RERR packets since they are unicast and do not contribute significantly to the overhead. We also neglected Hello packets since they typically add a large constant overhead regardless of mobility or traffic.

Figures 3 and 4 show the PDR and routing overhead for CBR traffic for various values of HTHRESH. A HTHRESH of 100 indicates the ratio of received power to receive threshold to be 1. We found that H-AODV consistently showed a larger PDR and smaller routing overhead compared to AODV. For TCP traffic (Figs. 5 and 6), while the throughput for H-AODV was higher for most values of HTHRESH, the routing overhead was greater than AODV. We believe that the reason for increased overhead could

be due to the large volume of traffic in TCP connections which might cause collisions leading to the loss of handoff packets. If a handoff packet reaches a predecessor node and does not reach the handoff node, it would lead to a route failure, thus increasing overhead. Another point of interest is the irregular nature of the H-AODV plots. We would expect maximum throughput and least overhead for a value of HTHRESH close to 100. While this is seen for the CBR plots, it is not very pronounced.

V. Related Work

An alternate implementation of Router Handoff for AODV that does not use Hello messages to spread power information appears in [3]. To the best of our knowledge, the only work related to the work presented in this paper is *Preemptive Routing* [4]. Preemptive routing keeps track of signal strengths and resorts to route repair procedures before a link breaks. The difference between Router Handoff and Preemptive Routing is that the latter does a normal route repair procedure involving flooding whereas Router Handoff tries to locally find an alternate node and hands off existing routing information to it. Of the two techniques, only Router Handoff reduces overheads of route repair but both Router Handoff and Preemptive Routing attempt to reduce delays due to route breakages.

VI. Conclusions

In this paper we presented a preemptive route repair strategy for AODV called Router Handoff. We found that in most cases tested it reduces routing overhead and improves throughput. We are currently in the process of refining the criteria for performing

handoff and assessing the impact of Router Handoff on network latency and average path length. We also believe that the concept of handoff could be used in contexts other than link failure. For instance, a node that is low on power, or a node that knows it is going to switch off could handoff without affecting the rest of the ad hoc network. It might also be interesting to incorporate Router Handoff into other ad hoc routing protocols.

REFERENCES

- [1] Charles Perkins and Elizabeth Royer, "Ad Hoc On-Demand Distance Vector Routing," *Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999*.
- [2] "Network Simulator, ns-2," <http://www.isi.edu/nsnam/ns/>
- [3] Abhilash P., Srinath Perur and Sridhar Iyer, "Router Handoff: An Approach for Preemptive Route Repair in Mobile Ad Hoc Networks", *Proc. of High Performance Computing, 2002*.
- [4] T. Goff, N.B. Abu-Ghazaleh, D.S. Phatak and R.Kahvecioglu, "Preemptive Routing in Ad Hoc Networks," *Proc. of ACM MobiCom, 2001*.