Multipath Extension of AODV with Enhanced Route Establishment and Proactive Route Management

西林　泰如　　櫻井　祐介　　甲藤　二郎
Yasuyuki Nishibayashi　　Yusuke Sakurai　　Jiro Katto

早稲田大学理工学研究科
Graduate School of Science and Engineering, Waseda University

1. Introduction

In this paper, we propose two new schemes to improve AODV [1] performance. Firstly, we extend RREQ/RREP messages by adding source routing information in order to establish loop-free multiple routes without overhead increase. Secondly, by proactively predicting link-break by tracking received power from neighbors, we propose a route management mechanism that dynamically changes data packet direction toward valid routes. Finally, we evaluate our proposal compared to conventional methods and attest its effectiveness.

2. Conventional Methods and Problems

2-1. AODV [1]

In AODV, a source node (S) firstly broadcasts route request (RREQ) packets towards a destination node (D) and, as a response, the node D unicasts a route reply (RREP) packet to the node S. When link-break occurs, route error (RERR) packets are propagated and the RREQ process is restarted. However, this recovery process sometimes causes huge degradation of communication performances (loss, delay, …) due to its packets overheads. To solve this problem, multipath extension of AODV has been considered.

2-2. AOMDV [2, 3]

AOMDV is a multipath routing protocol which is based on AODV. When each node receives duplicate copies of RREQ, it checks whether the packets' hop counts are less than the hop count already in a routing table. This check avoids routing loops. Also, if this check is passed, additional route information is added to the routing table. However, this method strongly restricts the number of multiple routes. For example, as shown in Figure1, a node "6" discards the second RREQ packet and it can't make multiple reverse routes.

Figure 1.
Problem of AOMDV

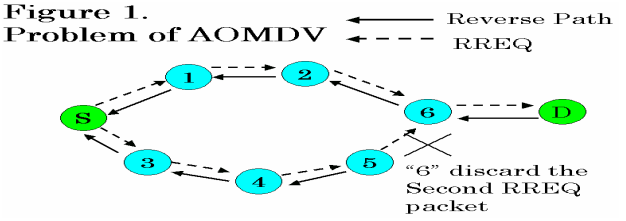
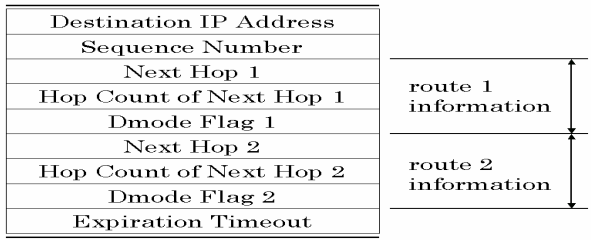


Figure 2.
Modified routing table entries



3. Proposed Method

3-1. Multiple Routes Establishment by RREQ/RREP Enhancement

We extend RREQ/RREP messages by forcing source routing information in order to establish valid multiple routes. Note that, unlike other source routing protocols like DSR, we use source routing information only in the case of RREQ/RREP messages. Any data packets are forwarded in a hop-by-hop manner without source routing option similar to AODV.

(a) RREQ Extension

In this extension, each node which forwards RREQ packets inserts its own IP address into a packet header. After receiving a RREQ packet, it also checks source routing information field in the packet. If there exists its own address, it detects routing loop and discards the RREQ packet. Otherwise, it updates its routing table with the RREQ information. Unlike AODV, duplicate copies of RREQ are not discarded immediately. If the second path information of the routing table is empty, and loop check is passed, the RREQ information is adopted as the second reverse path.

(b) RREP Extension

Similar to the RREQ extension, each node that forwards RREP packets inserts source routing information and updates its routing table accordingly. The RREP packets are forwarded along reverse routes. If there are multiple (two) reverse routes, the node bicasts RREP packets to each of them. We call direction going to a destination "upstream", and direction returning to a source node "downstream". When a node receives a RREP packet, it checks that next hop (1 or 2) of

the reverse route (to the node S) exists in an address information field in the RREP packet. If the next hop is found, this means that the RREP packet was forwarded from the downstream nodes and routing loop occurred. In this case, the node discards the RREP packet immediately.

3-2. Proactive Routing Management

When a node moves away from its neighbors, received power will be attenuated. We predict link-break occurrence proactively by tracking the received power of control packets (RTS/CTS messages in 802.11, or Hello packets in AODV...) and carry out additional route management. This enables effective use of backup routes as follows.

(a) "Notification" process

If the received power from a neighbor has declined, a node sets a "Dmode" ("danger mode", 1 or 2) flag "ON" as shown in Figure2. This indicates that the relevant neighbor may be served as a next hop (1 or 2) to several destinations.

After that, when a data packet is forwarded by a node of which Dmode flag is ON, the node unicasts a "Notification" packet to the node S only once instead of forwarding the data packet. Each node which forwards the Notification packet sets the Dmode flags ON respectively.

On the other hand, data packets must be forwarded to the next hop of which Dmode flag is OFF. Herewith, each node can avoid the effect of link-break proactively. When both Dmode 1 and 2 are ON, the node forwards the packet to the next hop 1.

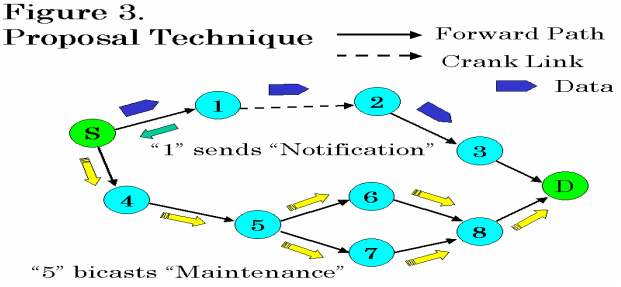
(b) "Revival" process

If the received power was attenuated but link-break didn't occur (a neighbor comes back again), a node (which has sent a Notification before) broadcasts a "Revival" packet. Revival packets are forwarded like RERR packets. When a node receives a Revival packet, it sets the associate Dmode flag OFF.

(c) "Maintenance" process

In AOMDV, an alternative route without packet transmission for a definite period of time becomes obsolete due to timeout and is removed from routing tables. This degrades multipath routing performance drastically. To solve this problem, if the node S has multiple routes, it sends a "Maintenance" packet to a backup route which is unused periodically. When other nodes receive a Maintenance packet, they update its expiration timeout field and forward the Maintenance packet. If there are multiple routes to the node D, the intermediate node bicasts Maintenance packets to multipath routes. As a result, all nodes (S, D and intermediate nodes) stand a good chance of holding valid routes. (Figure 3)

Figure 3.
Proposal Technique



4. Performance Evaluations

We evaluated our proposal compared to AODV and AOMDV as shown in Figures 4 and 5 using ns-2 [4]. Simulated field is $1500[m] \times 300[m]$ with 50 nodes. Each node moves randomly with random speed (0-20[m/s]) after a pause time. 10 traffic sources send 500-byte data packets every 0.25 seconds continuously assuming CBR transmission. Link speed is 2Mb/s assuming conventional 802.11 wireless LANs. We use "AODV-Hello" to predict link-break proactively.

Figure4. Packet delivery fractions

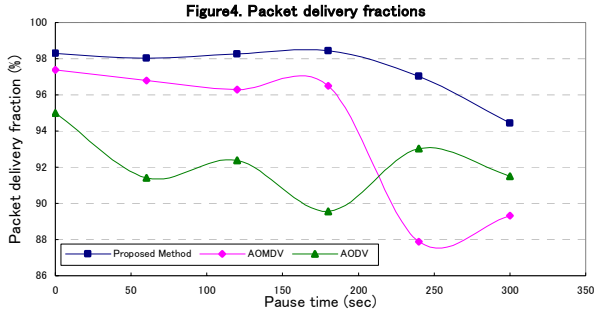
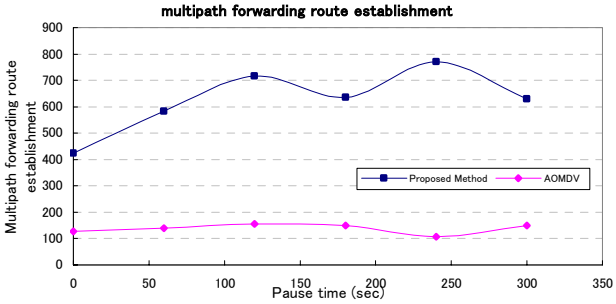


Figure5. Number of success in multipath forwarding route establishment



5. Conclusion

This paper proposed novel multipath extensions of AODV. By simulations, it was attested that our proposal outperforms conventional methods in various scenarios.

6. References

[1] C.Perkins, et al. "Ad Hoc On Demand Distance Vector(AODV)Routing", draft-ietf-manet-aodv-12.txt, 2002.
[2] S.R.Das, et al. "On-demand Multipath Distance Vector Routing for Ad Hoc Networks", ICNP 2001.
[3] S.Motegi, et al. "Proposal on Multipath Routing for Ad hoc Networks", IN2002-125 (in Japanese).
[4] http://www.isi.edu/nsnam/ns/index.html.