2010 International Conference on Communications and Mobile Computing

AODV-Based Backup Routing Scheme in Mobile Ad Hoc Networks

Tsung-Chuan Huang, Sheng-Yu Huang and Lung Tang
Department of Electrical Engineering National Sun Yat-Sen University
Kaohsiung, Taiwan
tch@mail.nsysu.edu.tw, {m963010059, d953010007}@student.nsysu.edu.tw

Abstract*—As effective routing is critical in mobile ad hoc networks (MANETs), the Ad hoc On-demand Distance Vector (AODV) has been extensively studied in recent years. Given that AODV requires a new route discovery procedure whenever a link breaks, such frequent route discoveries incur a high routing overhead and increase end-to-end delay. Therefore, by modifying the AODV protocol, this work presents a novel backup routing scheme capable of repairing disrupted links locally without activating a route re-discovery procedure. Additionally, backup paths are established based on 2-hop neighbor knowledge. These backup paths are geographically close to the primary path in order to provide efficient recovery from route failure and maintain an adequate routing length. Simulation results indicate that the proposed backup routing scheme obtains a lower average end-to-end delay and less routing overhead than those of the Ad hoc On-demand Multipath Distance Vector (AOMDV) and the conventional AODV.

Keywords-MANET; AODV; multipath routing; backup route

I. INTRODUCTION

A mobile ad hoc network (MANET) is a flexible, self-organizing wireless network consisting of a collection of wireless mobile nodes without a centralized control or infrastructure. Mobile nodes in such a network are capable of moving independently and communicating with other nodes using direct wireless links or multi-hop wireless links through a series of intermediate nodes. This network architecture is very useful in such environments as highly dynamic topologies without base stations. Some examples of MANET applications include battlefields, emergency services, moving vehicles, and conference rooms.

However, MANET characteristics, such as a dynamically changing topology, absence of a central coordinator and bandwidth-constrained wireless links, make its routing more complex than that of conventional wired networks. Generally, MANET routing protocols can be classified as *proactive*, *reactive*, and *hybrid*, based on the routing information update mechanism. *Reactive* routing protocols establish routes only when routes are needed by a source node; each node maintains individual routing information to destinations, but does not have a full topological view of the network. The reactive routing protocols typically minimize the number of required broadcasts by only creating routes on demand, as opposed to maintaining up-to-date routing information from each node to all other nodes in the network as in proactive routing. The Ad hoc On-demand Distance Vector (AODV) [1], one of the most popular reactive routing protocols, offers quick adaptation to dynamic link conditions and low network utilization [2, 3]. However, AODV is a single path routing that requires a new route discovery procedure whenever a link breaks along the route. Such frequent route discoveries result in a high routing overhead and increase end-to-end delay.

Multipath routing increases network resilience to link failure. Multiple paths are either *end-to-end disjoint paths* or *braided paths* [4]. For end-to-end disjoint paths, multiple paths are constructed between source and destination nodes where backup paths do not intersect the primary path. Conversely, braided paths typically have no completely disjointed paths from a source to destination, but many partially disjoint backup paths; these backup paths are not independent of the primary path. Recent studies demonstrated that braided paths are more resilient and energy-efficient than end-to-end disjoint paths [5, 6].

This work revises the AODV protocol to provide braided paths structure. The 2-hop neighbor knowledge is utilized to establish backup paths. These backup paths are geographically close to the primary path in order to provide efficient recovery from route failure and reduce the number of route discovery procedure.

The remainder of this paper is structured as follows. Section II introduces related work. Section III details our proposed scheme. Simulation results are shown in Section IV. Finally, conclusions are drawn in Section V.

II. RELATED WORK

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

978-0-7695-3989-8/10 $26.00 © 2010 IEEE
DOI 10.1109/CMC.2010.313

route maintenance process, when a node detects a link failure, it generates a *route error* (RERR) packet. This RERR packet is propagated over routes, while invalidating corresponding routes simultaneously. When a RERR packet is sent back to a source node, the source node initiates a new route discovery procedure.

To facilitate multipath support in the AODV protocol, a number of extensions have been developed. Marina and Das [7] developed an extension for AODV, called *Ad hoc On-demand Multipath Distance Vector* (AOMDV) routing. It provides loop-free and disjointed alternate paths. In the AOMDV protocol, each recipient node creates multiple reverse routes while processing RREQ packets received from multiple neighbors. Similarly, one or more RREP packets are generated via a loop-free path by the destination node or any node that has a route to the destination node in response to each received RREQ packet. These RREP packets, when received from the source or intermediate nodes, result in creation of multiple forward routes leading to the same destination node. However, with distance-vector-based protocols, the topology information a node can obtain is further limited. Thus, constructing disjointed alternate paths from a source to a destination is difficult.

III. AODV-BASED BACKUP ROUTING SCHEME

This work modified the conventional AODV protocol to enable discovery of backup paths from a source to a destination (Fig. 1). The 2-hop neighbor knowledge is utilized to generate backup paths during route discovery. The destination selects a route depending on which route has the maximum number of backup paths. In the proposed scheme, when the primary route fails, the connection can be recovered utilizing these backup paths.

The AODV-based backup routing scheme has three main components: local connectivity management, path discovery and path maintenance. The following describes each of these three components in detail.

A. Local connectivity management

In the conventional AODV protocol, a node may provide local connectivity information by broadcasting HELLO messages periodically. Each node periodically broadcasts HELLO messages to inform its neighbors that it has not moved away. When a node receives a HELLO message from a neighbor, a route to this neighbor is only added to the routing table when the neighbor does not already exist. If the neighbor exists, its lifetime is increased. When the network topology changes and HELLO messages are not received for a defined period of time, the route expires.

This work modified the HELLO message to generate 2-hop neighbor knowledge. Each node periodically broadcasts a HELLO message containing a list of all neighbors it can reach in one hop. When a node receives a HELLO message, it updates its local routing table with the HELLO message information. Nodes that cannot reach neighbors in two hops directly can learn about 2-hop neighbors from the neighbor that sent the HELLO message. After a node receives a HELLO message from all of its neighbors, it has 2-hop neighbor knowledge. In the proposed scheme, each node uses 2-hop neighbor knowledge to generate backup paths during route discovery and maintain up-to-date knowledge of such links.

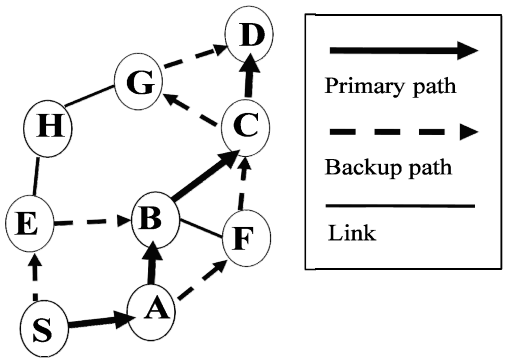

Figure 1. Structure of AODV-based backup routing scheme.

B. Path discovery

In this proposed scheme, backup paths intersect the primary path to establish a braided paths structure. The primary path and backup paths are established during the route request phase; this work revises the conventional AODV protocol in this procedure. When a node exists on the primary path, the node next to its downstream node is defined as the *border* node and the node next to its upstream node is defined as the *reverse border* node. Taking advantage of 2-hop neighbor knowledge, each node belonging to the primary path can compute backup paths with its upstream node and reverse border node. These backup paths are geographically close to the primary path to establish a braided paths structure.

To implement the modified AODV protocol, the format of the RREQ messages of the original AODV is modified accordingly (Fig. 2(a)). Two additional fields, called the *reverse_border* and *backup_count*, are appended to the original RREQ message. The *reverse_border* field records the reverse border node of the current node along the primary path. The *backup_count* field sums the number of backup paths along the primary path from the source node to the current node. The format of the RREP messages of the original AODV is also modified accordingly (Fig. 2(b)). An additional field, called the *border* field, is appended to the original RREP message. The *border* field records the border node of the current node along the primary path. Besides, the format of the routing table entry of the original AODV is modified (Fig. 2(c)). Two additional fields, the *backup_count* field of RREQ and the *border* field of RREP are appended to the original routing table entry.

When a source node requires a route to a destination, the source node broadcasts a RREQ packet to initiate route discovery. An intermediate node receiving the first arriving RREQ sets up a reverse route to the source. This is the same step as in the conventional AODV, which sets up a reverse route using the RREQ that arrives first. However, unlike the conventional AODV, the intermediate node computes the

backup path using the *reverse_border* field of the RREQ and the 2-hop neighbor table.

The intermediate node analyzes the neighbor table; any path that can bypass the upstream node to connect to the reverse border node is a backup path (Fig. 3(a)). This backup path can repair link failures between 2 hops, and the value of the *backup_count* field is increased by 2 unless the intermediate node does not contain this backup path. Thus, the intermediate node looks for another backup path in the neighbor table that can pass through another node to connect to the upstream node (Fig. 3(b)). If this backup path exists and can repair link failure 1 hop away, the value of the *backup_count* field is increased by 1, and the intermediate node will not change the value of the *backup_count* field only when it does not contain any backup path. After determining the *backup_count* field in the RREQ packet and recording it in the routing table entry, the intermediate node updates the *reverse_border* field of the RREQ to its upstream node and rebroadcasts this RREQ packet.

When an intermediate node receives a duplicate RREQ packet, instead of discarding it immediately as in the conventional AODV, each copy is analyzed to determine whether it provides more backup paths to the source node than previous route. The *hop count* and *backup_count* piggybacked on the RREQ are examined. If the *hop count* equals the previous *hop count*, but *backup_count* is larger than the previous *backup_count*, the reverse route that forwards the RREQ will be adopted as the new reverse route. The other duplicate RREQs are discarded to prevent the generation of an additional routing loop. The purpose is to find the shortest reverse path containing the most backup paths to the source.

When a destination receives the first RREQ packet from a neighbor, the destination updates its routing table entry and generates a RREP packet. This RREP packet is then sent back to the source node to initialize data transmission. When the destination receives a duplicate RREQ packet from its neighbors, the new route is used when the value, *backup_count* - *hop count*, piggybacked on the RREQ is greater than that of the previous route. (The value is defined to select a route that has the shortest routing length and many backup paths to the source.) The destination generates a RREP packet with a new sequence number and replies the RREP to the source. This work discards all the other duplicate RREQs. Thus, a proper shortest path with the largest number of backup paths can be acquired.

When an intermediate node receives a RREP packet from a neighbor, it adds a routing entry to its routing table to record the discovered route to the destination. The routing entry sets the value of *next hop* field to the node from which the RREP came, sets the *border* field to that field piggybacked on the RREP, updates the *border* field of the RREP to the *next hop* field and forwards the RREP message. As the RREP returns to the source, each node along the path not only contains a *next hop* field to indicate the downstream node but also contains another field called

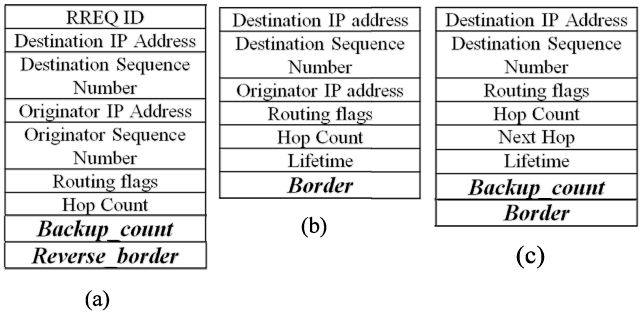

Figure 2. (a) The format of revised RREQ message. (b) The format of revised RREP message. (c) The structure of revised routing table entry.

the *border* field to indicate the border node. Both of the *next hop* field and the *border* field are utilized during the path maintenance phase. If an intermediate node receives duplicate RREPs, it updates its routing information and propagates the RREP only when the RREP contains a greater sequence number than the previous RREP. In this way, intermediate node can suppress all the other RREPs received. This decreases the number of RREPs propagating toward the source node while also ensuring that information for the quickest route is up-to-date. The source node can then begin data transmission as soon as the first RREP is received, and can update its routing information when it learns of a route containing more backup paths than previous route.

C. Path maintenance

Data packets are delivered via the primary route unless the primary route is disconnected. When a node detects link failure, it utilizes the backup paths contained in its 2-hop neighbor table to repair the disrupted link. If the backup path can connect to the border node in the routing entry, link failure can be repaired by this backup path (Fig. 4(a)). However, when the node does not contain this backup path, the node looks for another backup path that can connect to the downstream node through another node to repair the failed link (Fig. 4(b)). Data packets can therefore be delivered through one or more backup paths and are not dropped when route breaks occur.

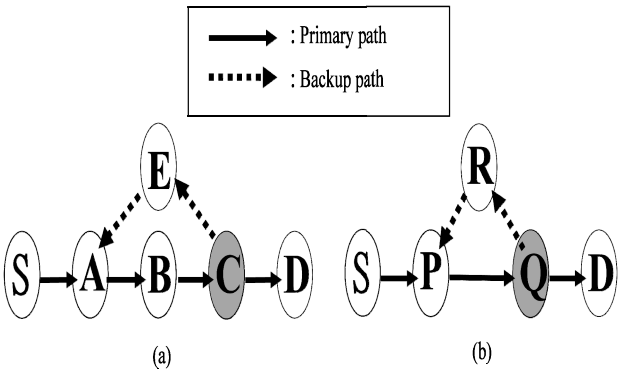

Figure 3. (a) Backup path discovery of node C with reverse border node A. (b) Backup path discovery of node Q with upstream node P.

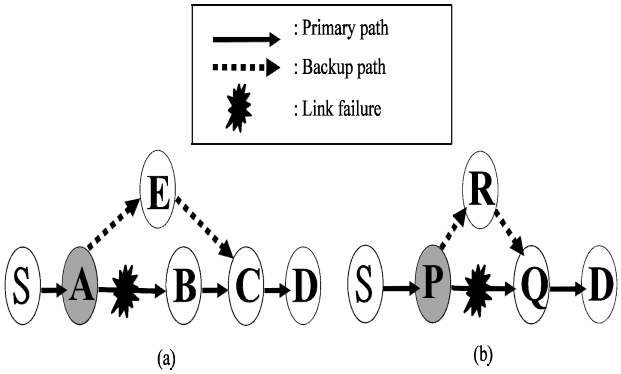

Figure 4. (a) Link failure repair of node A with border node C.
(b) Link failure repair of node P with downstream node Q

The node that detected the link break but does not contain any backup path sends a RERR packet to the source to initiate a route re-discovery procedure. The advantage of these backup paths is that they are geographically close to the primary path, thereby providing efficient recovery from route failures and maintaining an adequate routing length.

IV. SIMULATION

In this section, we evaluate and compare the performance of the modified AODV scheme to the AOMDV and the conventional AODV using NS-2 [8].

The schemes are evaluated using the following three performance metrics:

1) *Packet delivery fraction* — the number of received data packets divided by the number of generated data packets.
2) *Average end-to-end delay* — the average time taken for all data packets to be transmitted across a network from source to destination.
3) *Control overhead* — the number of control packets transmitted per data packets delivered.

A. Simulation environment

In our simulation, the MAC protocol is based on IEEE 802.11 and the propagation model is a two-ray ground reflection model. Table I lists the simulation parameters. The simulation scenario consisted of 100 mobile nodes randomly distributed in a 1000m × 1000m square area. Maximum speed of the nodes is varied in five different maximum moving speeds: 0/5/10/15/20 m per second. We consider only the continuous mobility case. The transmission range of each node is 250m. There are 20 constant bit rate (CBR) traffic sources distributed randomly over the network. The CBR data packets are 512 bytes, and the sending rate is 4 packets per second. Simulations are run for 300 seconds.

B. Simulation results

This work evaluates the ability of AODV, AOMDV and the proposed scheme to change the topology dynamically by changing the node mobility through variation of the maximum speed.

TABLE I. SIMULATION PARAMETERS

Simulator	NS2
Simulation time	300 s
Simulation area	1000m x 1000m
Number of nodes	100
Transmission range	250 m
Max speed	0, 5, 10, 15, 20 m/s
CBR flows	20
Data payload	512 bytes
Sending rate	4 packets/s
Movement model	Random waypoint

Although the performances of all protocols resemble those in the static case, their differing performances become more apparent at higher speeds.

Figure 5 illustrates the comparison of data delivery ratio, in which AODV-BBS represents the proposed AODV-based backup routing scheme. Simulation results indicate that both AODV-BBS and AOMDV outperform AODV since AODV does not use a backup route; thus, data loss occurs whenever a link is disrupted along the route. AOMDV and AODV-BBS utilize backup scheme to repair the disrupted link such that data delivery ratio is increased obviously. However, in mobile cases, AODV-BBS loses fewer packets than AOMDV. The observation of a higher packet delivery fraction in AODV-BBS implies that it can select a route containing more available backup paths than AOMDV does.

Figure 6 demonstrates the comparison of average end-to-end delay where AODV incurs the largest delay among these protocols due to frequent route discoveries for a dynamically changing topology. Since both AODV-BBS and AOMDV utilize backup path to reduce route re-discovery procedure whenever a link is disrupted along the route, the average end-to-end delay is reduced. However, the average end-to-end delay of AODV-BBS is slightly lower than that for AOMDV. This observation is owing to that, in AODV-BBS, the backup paths are geographically close to the primary path and an adequate routing length is maintained. Consequently, the link failure can be repaired efficiently and the average end-to-end delay reduced as well.

Figure 7 compares the control overhead. Simulation results indicate that when nodes stop or move slowly, control overhead of AODV-BBS and AOMDV resembles that of AODV. An increasing mobile rate lowers the control overhead in AODV-BBS and AOMDV than that in AODV owing to reduction of the route discovery by using backup routes. Restated, in both AODV- BBS and AOMDV, a new route discovery is invoked only when all paths fail. Therefore, AODV-BBS and AOMDV outperform AODV. The overhead of AODV-BBS is slightly lower than that of AOMDV owing to that, in AODV-BBS, backup paths are maintained by a neighbor table periodically. Doing so can

avoid use of unavailable backup paths to initiate a new route discovery procedure and produce additional overhead.

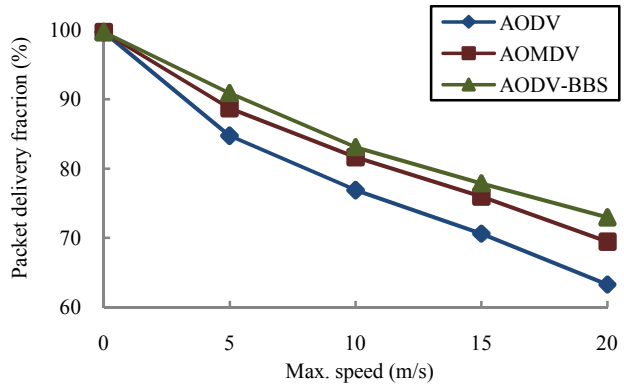

Figure 5. Comparison of packet delivery fraction.

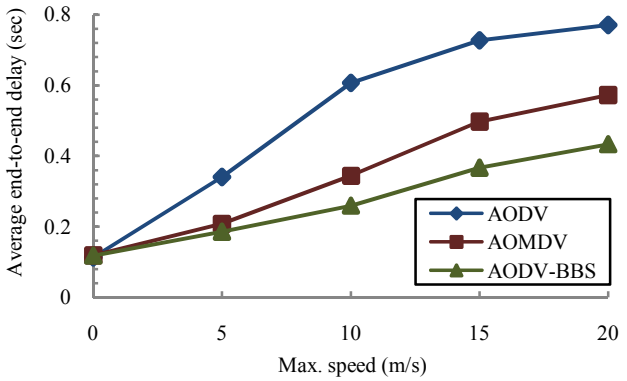

Figure 6. Comparison of average end-to-end delay.

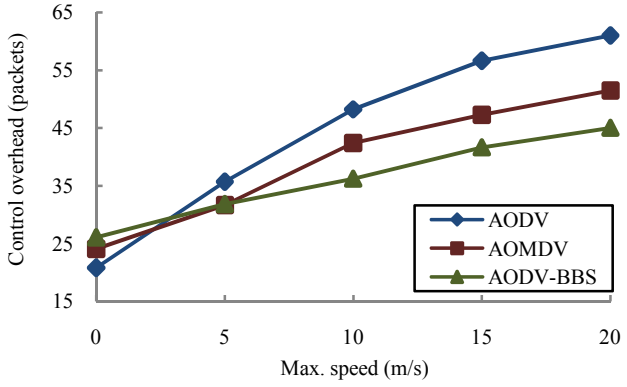

Figure 7. Comparison of control overhead.

V. CONCLUSION

This work presents a novel AODV-based backup routing scheme for MANETs. The proposed scheme utilizes 2-hop neighbor knowledge to establish backup paths during the route discovery phase and maintain updated knowledge of such links. These backup paths are geographically close to the primary path that can repair disrupted links locally without activating a route re-discovery procedure. Additionally, the proposed scheme selects the shortest path containing the largest number of backup paths to provide efficient recovery from route failure and maintain an adequate routing length. Simulation results indicate that the proposed backup routing scheme obtains a lower average end-to-end delay and less routing overhead than those of the AOMDV and the conventional AODV.

REFERENCES

[1] C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector (AODV) routing", in *Proc. IEEE workshop on Mobile Computing Systems and Applications (WMCSA)*, Feb. 1999. pp. 90-100.

[2] C.E. Perkins and E.M. Royer, "RFC3561: Ad hoc on-demand distance vector (AODV) routing", *Internet RFCs*, RFCs, Jul. 2003.

[3] E.M. Royer and C.K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks", in *Proc. IEEE Wireless Communications*, Apr. 1999, pp. 46-55.

[4] H. Liu and D. Raychaudhuri, "Label switched multi-path forwarding in wireless ad-hoc networks", in *Proc. IEEE International Conference on Pervasive Computing and Communications Workshops*, Mar. 2005, pp. 248–252.

[5] Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A Framework for Reliable Routing in Mobile Ad Hoc Networks", in *Proc. IEEE INFOCOM*, Mar. 2003, pp. 270 - 280.

[6] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks", in *Proc. ACM SIGMOBILE Mobile Computing and Communications Review*, Oct. 2001, pp. 11–25.

[7] M. K. Marina and S. R. Das, **"**On-demand multipath distance vector routing in ad hoc networks", in *Proc. International Conference for Network Procotols (ICNP)*, Nov. 2001, pp. 14–23.

[8] VINT Group, UCB/LBNL/VINT Network Simulator ns-2. [Online]. Available: http://www.isi.edu/nsnam/

[9] S. Motegi and H. Horiuchi, "AODV-based multipath routing protocol for mobile ad hoc networks", in *Proc. IEICE Transactions on Communications,* Sep.2004, pp.2477–2483.

[10] J. Li, J. Jannotti, D. De Couto, D. R. Karger, and R. Morris, "A scalable location service for geographic ad hoc routing," in *Proc. ACM Int. Conf. Mobile Computing and Networking*, Aug. 2000, pp. 120–130.

[11] A. A. Pirzada, C. McDonald, and A.Datta, "Performance Comparison of Trusted-Based Reactive Routing Protocols," in *Proc. IEEE Trans. On Mobile Computing*, Jun. 2006, pp. 695–710.

[12] A. Valera, W. Seah and S.V. Rao, "Cooperative packet caching and shortest multipath routing in mobile ad hoc networks," in *Proc. IEEE INFOCOM*, Apr. 2003, pp. 260–269.