J Supercomput (2012) 59:268–296
DOI 10.1007/s11227-010-0437-8

Dual paths node-disjoint routing for data salvation in mobile ad hoc

Fuu-Cheng Jiang · Chu-Hsing Lin · Der-Chen Huang · Chao-Tung Yang

Published online: 24 April 2010

Abstract The operational patterns of multifarious backup strategies on AODV-based (Ad-hoc On-Demand Vector) routing protocols are elaborated in this article. To have a broader picture on relevant routing protocols together, variants of AODV-based backup routing protocols are formulated by corresponding algorithms, and also each of them are simulated to obtain the necessary performance metrics for comparisons in terms of packet delivery ratio, average latency delay, and the normalized routing load. Then to make the process of data salvation more efficiently in case of link failure, we explore the possibility of combining the AODV backup routing strategy and on-demand node-disjoint multipath routing protocols. This article proposes an improved approach named DPNR (Dual Paths Node-disjoint Routing) for data salvation, a routing protocol that maintains the only two shortest backup paths in the source and destination nodes. The DPNR scheme can alleviate the redundancy-frames overhead during the process of data salvation by the neighboring intermediate nodes. Our simulation results have demonstrated that DPNR scheme delivers good data delivery performance while restricting the impacts of transmission collision and channel contention. The mathematical rationale for our proposed approach is stated as well.

Keywords Mobile ad-hoc network · Node-disjoint multi-path · Alternative path · Data salvation · Simulation

F.-C. Jiang · D.-C. Huang
Department of Computer Science and Engineering, National Chung-Hsing University, 250 Kuo-Kuang Rd., Taichung, 40204, Taiwan

C.-H. Lin · C.-T. Yang (✉)
Department of Computer Science, Tunghai University, 181 Section 3, Taichung Port Rd., Taichung, 40704, Taiwan
e-mail: ctyang@thu.edu.tw

1 Introduction

A mobile ad hoc network (MANET) [1, 2] is a wireless LAN (Local Area Network) model without the need of central base stations and operated as a self-organized, dynamically changing multihop network. MANETs can be applied in medical emergencies, during natural catastrophes, for military applications and to conduct geographic exploration. Mobile and wireless devices belonging to a MANET are usually called mobile nodes. These nodes are characterized by high mobility, low power, limited storage, and limited transmission range. Mobile nodes communicate through bidirectional radio links and data transmission is a key challenge. MANET communication events are called sessions. The two communicating parties, namely the source node and the destination node comprise a session pair (or source-destination pair). A mobile node can communicate directly with other nodes if such a link exists within the radio transmission range. If the distance between a session pair is too large to establish direct contact, then the data must be sent via intermediate nodes connecting the two parties.

In principle, at least one valid routing path must be established before the source node of a session pair can send data to its destination node. MANET routing protocols can be roughly categorized into two categories [3, 4], namely the table-driven routing and source-initiated on-demand routing. In table-driving routing protocols, each mobile node has to disseminate its routing table to its neighboring nodes periodically. When a node receives the broadcast information, it updates its routing tables based on the received information. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. Although table-driven schemes can promptly provide the routing path using its local routing tables, periodic broadcasting routines would definitely result in considerable overhead cost upon the wireless LAN performance.

Source-initiated on-demand routing protocols resolve the periodic broadcasting overhead found in table-driven schemes by adding a routing procedure before sending data. Unlike table-driven scheme, each node in on-demand routing does not need periodic route table update exchanges and does not have a full topological view of the network. Network hosts maintain route table entries only to destinations that they communicate with. Well-known source-initiated on-demand routing protocols include the Ad-hoc On-demand Distance-Vector (AODV) [5, 6] and Dynamic Source Routing (DSR) [7, 8]. These protocols are based on the strategy of only finding valid routes once they are needed by the source node. This procedure is known as route discovery. Route discovery involves the route request phase and the route reply phase. These protocols construct a single-path route between a source node and a destination node.

The routing protocol elaborated for this article is an AODV-based protocol. The classic AODV routing protocol, defined in RFC 3561 [6], is designed for MANET with population of tens to thousands of mobile nodes. It offers quick adaption to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destination within the MANET. It uses destination sequence numbers to ensure loop freedom at all times, avoiding potential problems associated with classical distance vector protocols. AODV can handle low, moderate, and relatively high mobility rates, as well as a variety of data traffic levels. Moreover, AODV is proposed for use in networks where all the nodes can trust each other, either by use of preconfigured keys, or because it is known that there are no malicious intruder nodes. Above all, AODV has been designed to alleviate the dissemination of control traffic and eliminate overhead on data traffic, in order to improve scalability and performance.

The AODV operation consists of two phases: route discovery and route maintenance phases. The route discovery phase contains two sub-phases: the route request phase and the route reply phase, which involves the communication and processing of two kinds of message formats: route request (RREQ) message and route reply (RREP) message, respectively. To start route discovery phase [6], a source node disseminates a RREQ when it determines that it needs a route to a destination and does not have one available. This can happen if the destination is previously unknown to the node, or if a previously valid route to the destination node expires or is marked as invalid. When a node receives the RREQ, it first creates a reverse route entry for the source node in its route table. It then checks whether it has unexpired route to the destination node. In order to respond to the RREQ, the node would either be the destination itself, or it has an unexpired route to the destination whose corresponding sequence number is at least as great as that contained in the RREQ. If neither of these conditions is met, the node redisseminates the RREQ.

In other word, in response to RREQ messages, either destination node or an intermediate node that knows a route to the destination, sends a RREP message back to the source along the path on which the RREQ message was received. Intermediate nodes rebroadcast the RREQ message only if (1) they do not know a route to the destination and (2) they have not already forwarded the particular RREQ message. Once discovered, a route is recorded in terms of an entry in its route table and maintained as long as needed by the source node. To avoid the unnecessary routing loop, each RREQ message contains a unique broadcast ID called “RREQ ID” with 4 bytes in length specified in the RREQ message format [6]. The RREQ ID field contains a sequence number uniquely identifying the particular RREQ when taken in conjunction with the source node’s IP address. Whenever a node received RREQ message, it will examine whether it has received a RREQ with the same source IP address and RREQ ID within a predefined time limits. If such a RREQ has been received, the node silently discards the newly received RREQ. This discipline can discard duplicated RREQ packets that may be received by an intermediate node.

In the classic AODV protocol, however, there is only a single primary path established during the route discovery phase. The node mobility would be one of major causes to link breakages in MANET. Whenever there is a link break on the primary route, the routing protocol has to invoke a route discovery process. Each route discovery flood is associated with significant latency delay and routing overhead. Moreover, each time when a link fails during transmission period, two performance impacts would take place immediately. One loss is that the data packets are simply discarded by nodes along the broken link. For a time-sensitive traffic, it is not allowable to drop too many packets in the period of path failure. Especially for connection-oriented, reliable delivery service like TCP connection, it may deteriorate the performance considerably due to dropping packets with sequenced numbers.

The other performance impact results from retriggering discovery process. Since the source node has to reinitiate a new route search upon the receipt of a route error, extra network resource would be consumed again due to completing route discovery process. The phenomenon of retriggering the discovery process would deteriorate as the mobile frequency of each node becomes higher according to the mission requirement. Practically, there is a heavy overload for restarting route discovery in AODV, which would result in both power consumptions for every nodes along the primary path and the latency delay for the transmission of data packets queued in the source node's buffer. Therefore, several backup approaches to alleviate such a link maintenance problem are provided to reinforce classic AODV-based protocol.

Based on classic AODV routing protocol, Lee and Gerla [9] proposed a feasible approach, coined as AODV-BR (Backup Routing) in 2000, which can improve the performance of AODV by setting up a mesh structure and providing multiple alternate routes. A backup routing protocol mainly establishes one valid primary path together with several other alternative paths during a successful protocol run. The advantages of AODV BR-based routing protocols are designed to provide data salvation capabilities for the previously mentioned basic AODV protocol. Aside from the benefits of data salvation, much of power consumption due to restarting discovery process can be saved to prolong the node's lifetime for battery-equipped mobile nodes and the negative impact from latency delay for data packets can be considerably alleviated as well. Then Chen and Lee [10] proposed the so-called Two Hops BR (2HBR) in 2005 by employing two-level alternate paths, which can improve the packet delivery ratio and the latency in high mobility case by their simulation results. Many on-demand protocols with backup or multipaths routes have been proposed in order to improve the routing performance [9–18]. Backup or multipaths routes could be formed through multifarious schemes. New route discovery is only performed in case that all alternative paths fail. Hence, the routing performance can be improved in terms of reduction in routing overheads and route discovery latency.

Paths that do not have any common node except the source and destination are known as node-disjoint paths. If multiple paths discovered between a pair of nodes are node-disjoint, then frequency of route discovery can be mitigated [14]. These multipath routing mechanisms [15–17] have tried to identify multiple node-disjoint paths between a given pair of nodes. Most of multipaths routing schemes depend upon the assistance of intermediate nodes within the transmission range. Among them, intermediate nodes within reception range would forward RREQ packets according to a specified RREQ forwarding policy. For geographic regions with higher density of intermediate nodes, excessive intermediate nodes would help forwarding data packets. Consequently, a large amount of redundant copies would spread across the wireless LAN definitely. This phenomenon is termed as "the spread of salvaged data packets." Although the construction of multiple paths can provide reliable delivery service for a pair of nodes, such redundant framework indeed causes considerable routing overheads for excessive paths than what is needed. Hence, one question occurs to us: what does the term "multiple" imply to meet cost-effective requirement? We proposes an effective approach, coined as DPNR (Dual Paths Node-disjoint Routing), for data salvation and routing overhead reduction. To the best of our knowledge, it appears to be the first time such an approach has been proposed with both experimental results and rationale with numerical data.

The objective of this article is threefold: (i) To have a deeper insight upon these AODV BR-based routing protocols, several relevant simulation results among them are conducted for comparison in terms of packet delivery ratio, average latency delay, and normalized routing load. (ii) Combining good data salvation characteristic in AODV BR scheme with the route independence property of node-disjoint multiple paths, we propose a novel DPNR approach to alleviate the mentioned impacts from the spread of salvaged data packets and improve the robustness on routing paths. (iii) To validate through simulation analyses, we use NS-2 [19] network simulator to implement our proposed approach, and the supporting rationales in mathematical theory are given for the proposed DPNR scheme.

The rest of the paper is organized as follows. Section 2 describes the related works regarding these AODV BR-based routing protocols. In Sect. 3, we present performance effects on relevant AODV BR-based routing protocols, and the corresponding simulation results are conducted for comparison as well. In Sect. 4, our DPNR approach is developed and expressed in the form of feasible and efficient algorithms. The simulation results have been conducted and performance evaluations have been described in details in Sect. 5. In Sect. 6, theoretical rationale for utilizing DPNR scheme is also provided in terms of the reliability enhancement considerations and the quantitative analysis on probability of setting up more numbers of node-disjoint paths than just only two. Finally, in Sect. 7, some concluding remarks are made.

2 Related works and motivations

There is a heavy overload for restarting route discovery in AODV [10], which would result in both power consumptions for every nodes along the primary path and the latency delay for the transmission of data packets queued in the source node's buffer. Therefore, several backup approaches to alleviate such a link maintenance problem are provided to reinforce classic AODV-based protocol. In this section, the relevant AODV-based backup routing protocols are addressed. The technical background regarding the backup structure and the data salvation scenario are described before proposing our approach. The critical defect embedded in the AODV-backup routing protocols due to the spread of salvaged data packets is also described.

2.1 AODV-backup routing (AODV-BR) protocol

In AODV-BR [9], the construction of alternate routes relies on the overhearing of Route Reply (RREP) messages not directed to them via the local radio broadcast. No additional messages are needed during the establishment of the AODV-BR backup structure. When a source node attempts to send data packets to a certain destination node, which has no route information stored in its routing table, it initiates the same search process by flooding a route request (RREQ) as defined in classic AODV protocol. Each RREQ has a unique identifier (RREQ ID) so that nodes can detect and discard duplicate packets. On receiving nonduplicate packets, an intermediate node records the previous hop and the source node information in its routing table. It then disseminates the packet or sends back a route reply (RREP) packet to the source if it has a route to the destination.

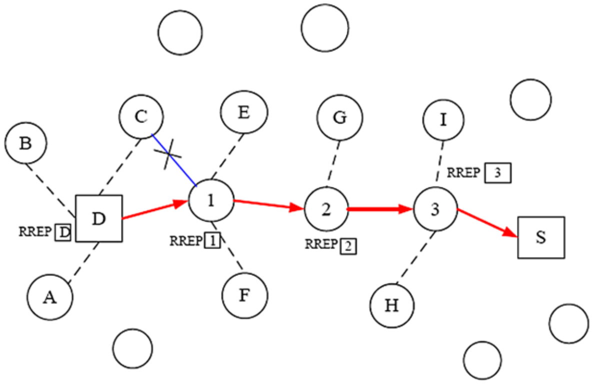


Fig. 1 Construction of AODV-BR backup structure

The destination node sends a RREP via the chosen route when it receives the first RREQ or subsequent RREQs that traversed a shorter or an optimal route than previously replied route. During the backward learning process, a neighboring node (under transmission range) that is not a member of the primary route would overhear a RREP message transmitted by a member of the primary route. It then records that member as the next hop to the destination in its alternate route table. Figure 1 exemplifies the alternate route path construction. The AODV-BR backup structure is formed as the RREQ messages disseminated one by one in time domain along the primary path specified in the destination node. The process of construction of AODV-BR backup structure is stated as follows:

(i) Message RREP$\boxed{D}$ disseminated by node D:
Under the transmission range, nodes A, B, and C overhear this RREP message in addition to node 1, which is the node in the primary path.

(ii) Message RREP$\boxed{1}$ forwarded by node 1:
Nodes C, E, and F obtain alternate path information, and become part of the fishbone-like backup structure. Inside the transmission range, node C will receive two RREP packets from node D and node 1 successively. To prevent routing loop, when node C received RREP, it will check ⟨RREP ID, source IP address⟩ pair. If the RREP had been received, node C will discard duplicated RREP packet as the link between node 1 and C with X symbol shown in Fig. 1.

(iii) Message RREP$\boxed{2}$, $\boxed{3}$ forwarded by node 2, 3, respectively:
Inside the range of transmission, nodes G build alternate path information for RREP$\boxed{2}$, and for RREP$\boxed{3}$, node H and node I store alternate path information. All of them become part of the fishbone-like backup structure.

The primary path is displayed in the form of solid lines, and these one-hop alternate links stored in intermediate (neighboring) nodes are displayed in form of dash lines in Fig. 1. The source node and destination node are depicted by $\boxed{S}$ and $\boxed{D}$, respectively. The blank circles represent the mobile nodes out of the transmission range. The legends are shown in Table 1 which is used for Figs. 1, 2, 3, 4 throughout this article.

The routing information of the alternative path is only stored in the routing table of the intermediate nodes. Intermediate nodes on the primary path can utilize

Table 1 Legends used in Figs. 1–4

X	Link failure
→	Primary route
- - - -	Alternate link
□	Source node or Destination node
⇨	Data salvation
Ⓐ	Level-one node of alternate path to destination (letter inside)
◗	Level-two node of alternate path to destination
○	Mobile node (blank) out of transmission range

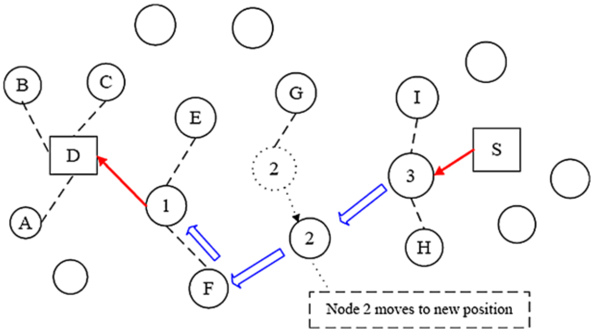


Fig. 2 Scenario of AODV-BR data salvation

the backup structure to find a suitable alternative route to salvage their data if they face a link failure. A link failure might for instance be caused by the next hop of the primary path being out of radio range, or a primary node running out of power, etc. When a node detects a link break, it performs a one-hop data broadcast to its immediate neighbors [9]. The node specifies in the data packet header that the link is disconnected, and thus the packet is candidate for “alternating routing.” Upon receiving this packet, neighboring nodes that have an entry for destination in their alternate route table would unicast the packet to their next hop node. Data packets therefore can be delivered through one or more alternate routes and can be salvaged when link failures occur.

Figure 2 illustrates the usage of an alternate path when the primary route gets disconnected. Node 2 moved out the radio range of its next hop node 1. After receiving the data packet from node 3, node 2 forwards it to node 1. However, the packet will fail to be delivered since node 1 is out of transmission range from node 2. Node 2 then broadcasts the packet to its neighbors for alternate paths to salvage the data. Nodes F and 3 receive the packet, but node 3 drops it upon duplicate detection. Node F then recognizes the primary route disconnection by reading the packet header. It looks up its alternate route table and finds node 1 as its next hop to the destination. It would unicast the packet to node 1, and eventually the packet reaches the destination.

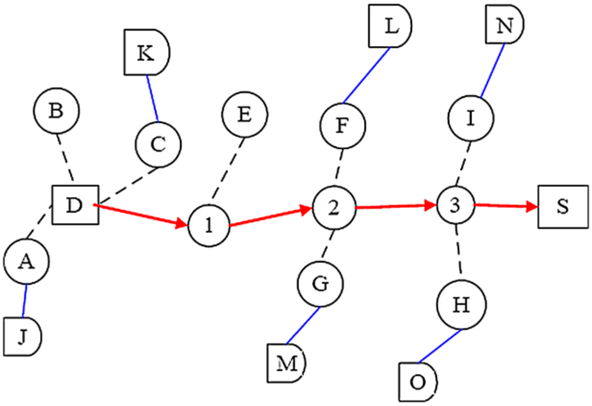
2.2 Two Hops Backup Routing (2HBR) protocol

Two Hops Backup Routing (2HBR) [10] is extended from AODV-BR. 2HBR creates a two-hop backup structure during the routing reply phase. Initially, 2HBR follows the same procedure as AODV-BR where intermediate nodes overhear the routing reply packet to create a one-hop backup structure. Next, the intermediate nodes broadcast the route reply packets to establish a two-hop backup structure. Each intermediate node that overhears the rebroadcasted routing reply packet, is not a member of the primary path, or is the first hop of the backup path, become the second hop of the alternative path. 2HBR requires more time for routing than AODV-BR does since the second hop needs a routing packet broadcast. The establishment of 2HBR backup structure is exemplified in Fig. 3.

2HBR uses a detour assurance policy to ensure that the next hop of a valid alternative path is still active and reachable. A node with a link failure first temporarily stores its data packets into a buffer and then broadcast a routing packet with a request for help. Then neighboring nodes with an alternative path to the destination node will send routing packets to their next hop of the alternative path. The next hop replies to the neighboring node if it is alive and reachable. Then the neighboring node will subsequently reply to the link failure node that the path is valid. The first reply is chosen as this represents the fastest path. Finally, the link-failure node can forward its buffered data packets through the alternative path to the final destination. The data salvation scenario is shown in the Fig. 4. The link breakage happens because node 1 moves to a new position. The circle with dashed lines around node 2 represents the range of transmission of node 2.

Basically, the backup routing approach is established in initial creation of a backup structure, which can be utilized to salvage data packets that pass through nodes in case of link failure. Since the alternative path, in numbers of hops, is usually longer than that of the primary path, it will almost always take longer for the data packets to reach the destination. If a mobile node disseminates data packets to be salvaged to its neighbors and also if there are a large number of neighboring nodes, then there would be a dramatically increases in wireless traffic resulted from the assistance provided by these neighboring nodes. When excessive neighbors help forwarding the data packets,

Fig. 3 Construction of 2HBR backup structure



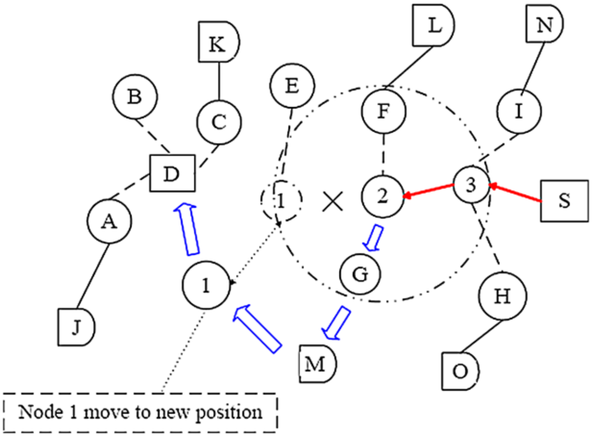


Fig. 4 Scenario of 2HBR data salvation

there will be lots of copies of the redundant data packet spread across the wireless LAN. The scenario of so-called "spread of salvaged data packets" would inexorably happen, and this will incur considerable routing overheads.

The major motivation behind this article is to mitigate such an overhead from the impacts of salvaged data packets. Moreover, unwise or careless selection of next hopping node by the forwarding node will worsen this problem. This impact includes the deterioration of collision frequencies of duplicated data packets, lower packet delivery ratio, higher delay, and network congestion for the wireless LAN. To mitigate such an impact, we present an improved approach called "Dual Paths Node-disjoint Routing (DPNR)" to reduce the redundancy-frames overhead during the process of data salvation by neighboring intermediate nodes, and the DPNR scheme will be addressed in detail in Sect. 4. A preliminary version of our work was reported in [20]. In this article, we extend our earlier work in several aspects. Firstly, we add more details in the development of our proposed algorithms. Secondly, to get deeper insight on existing routing schemes, performance comparisons and analysis of AODV-based backup routing schemes are conducted in Sect. 3. Finally, we also present the rationales for proposed DPNR strategy in terms of redundancy economy, which results from both the cost-effective reliability need and the probability of disjointness having k node-disjoint paths.

3 Performance comparisons and analysis of AODV-based backup routing policies

3.1 Algorithms construction

AODV-BR [9] can be employed with either a fixed next hop policy (AODV-BR 1) or one of any next hop policy (AODV-BR 2), as indicated in Algorithm 1 and Algorithm 2, respectively. The words "my" or "I" in Algorithms 1 and 2 indicate the neighboring node itself. The key difference between AODV-BR 1 and 2 is the selection of next hop on the alternative path. While AODV-BR 2 forwards a packet to

Algorithm 1 Backup strategy 1 for AODV-BR (action to be taken by neighboring nodes)

```
The next hop of my valid alternate path must be the disconnected node.

if (condition 1) and (condition 2) and (condition 3) then
    decrease the value of time to live by 1;
    set the next hop to the one of my valid alternate path;
    increate the lifetime of my valid alternate path;
    send out the data packet to the next hop;
endif

Conditions:
1. I have a valid alternate path.
2. The next hop of my valid alternate path is not the hop that needs help.
3. The next hop of my valid alternate path is exactly the disconnected hop.
```

Algorithm 2 Backup strategy 2 for AODV-BR (action to be taken by neighboring nodes)

```
Any next hop of my valid alternate path is welcome.

if (condition 1) and (condition 2) then
    decrease the value of time to live by 1;
    set the next hop to the one of my valid alternate path;
    increate the lifetime of my valid alternate path;
    send out the data packet to the next hop;
endif

Conditions:
1. I have a valid alternate path.
2. The next hop of my valid alternate path is not the hop that needs help.
```

any next hop on the alternative path in order to bypass the faulty link, AODV-BR 1 requires that the next hop leads to the same node as the failure link.

When a mobile node, say node A, encounters a link failure, it would first issue "one-hop data broadcast" packets to its neighboring nodes. In AODV-BR 1, only the neighboring nodes that have a valid alternate route (in their routing table) with a link to the disconnected hop can forward these data packets for node A. Other neighboring nodes without valid routing entry do not forward data packets. We call this form of forwarding scheme: the *fixed next hop policy*. In AODV-BR 2, the neighboring nodes will forward these data packets to any next hop of the valid alternate routes to the destination node. Both strategies are outlined in the following two algorithms. And the performance effects about these two approaches will be assessed in the subsequent section.

In 2HBR [10], it would also create an alternate path to be the backup of primary path as AODV-BR does. Moreover, it broadcasts the RREP packet again to enlarge the geographical range of the alternate-path structure to two hops. If a mobile node faces the link failure, it will seek a detour and use extra routing packets to make sure the detour is still active before it sends out any data packets.

Algorithm 3 Detour assurance by 2HBR protocols (action to be taken by a node with a link failure)

```
if (link failure) then
    temporarily store the data packets into route queue;
send out a help-asking routing packet to neighboring nodes;
    if (help-asking reply) then
        set the detour as the new direction of buffered data packets;
        sent buffered data packets out;
    else if (out of waiting time)
        then drop buffered data packets;
    endif
endif
```

Algorithm 4 2HBR (action to be taken by neighboring nodes)

```
if (condition 1) and (condition 2) and (condition 3) then
    send out a help-asking reply packet to the node with link failure;
    break;
endif
```

Conditions:
1. I have a valid alternative path.
2. My valid alternative path's next hop is still within my radio range.
3. My valid alternative path's next hop is not the hop that needs help.

In addition to broadcasting extra RREP packets for establishing the second hop backup structure during the route reply phase, 2HBR also relies on extra routing packets to examine detour assurance during link failure. Algorithm 3 shows the alternative path assurance process for a node that experiences a link failure, and Algorithm 4 depicts the backup process used by the neighboring nodes of the node with the link failure.

3.2 Simulation environment and performance metrics

This research employs NS-2 [19] utility for network simulations. Basically, we adopted most of parameters of simulation environment used in [10], and made adjustments on some key parameters like topology size, simulation time, etc. The simulations are based on constant bit rate (CBR) traffic sources and 64 packet send buffers. The data packet payload is 512 bytes. Packets are dropped if they remain in the send buffer for more than 30 seconds. All packets sent by the routing layer are queued in the interface queue which has a maximum capacity of 50 packets. Routing packets have higher priority than data packets. Our simulation places 50 nodes in a 1000 meter × 1000 meter field. Each data point on the simulation curves in the figures represents the average of five protocol runs with identical traffic/mobility scenarios. Identical mobility or traffic scenarios are assumed across the protocols discussed herein. The pause time is varied in the simulations to change the mobility of mobile

Table 2 Simulation parameters

Transmission range	250 m	Topology size	1000 × 1000 m^2
Channel capacity	2 Mb/sec	Traffic type	CBR
Mobile nodes	50	Rate of data packet	4 packets/sec
CBR sources	10	Size of data packet	512 bytes
Speed of mobile nodes	0–20 m/s	Simulation time	180 sec

nodes. Longer pause time implies less mobility. The pause time is increased from 0 seconds to 180 seconds in steps of 20 seconds. Table 2 lists the simulation parameters used in our simulation.

Quality of Service (QoS) is an important design consideration in any communication system. It can be measured in several ways depending on the applications or mission requirement. In our cases, as key parameters cited in [13–18], the following three QoS-related performance metrics of wireless LAN are defined and used during our simulation process:

(1) Packet delivery ratio (PDR): defines the ratio of data packets received by the destination nodes successfully divided by the total amount of packets generated by the CBR sources. The PDR can be used to show the throughput level in packet delivery.

$$\text{PDR}\ (\%) = \frac{\text{number of packets received by destination node}}{\text{total number of packets transmitted by CBR sources}} \times 100\% \quad (1)$$

(2) Average latency delay (ALD): includes all possible latency delays caused by buffering during route discovery latency and link recovery phase, queuing at the interface queue, retransmission delays at the MAC, data salvation latency, and propagation and transfer time. The ALD is defined as follows:

$$\text{ALD (sec/packet)} = \frac{\text{all possible latency delays}}{\text{total number of packets received by destination node}} \quad (2)$$

(3) Normalized routing load (NRL): defines the number of routing packets transmitted per data packet delivered at the destination node. Each hop-wise transmission of a routing packet is counted as one transmission. The NRL can be utilized to evaluate the efficiency of the interested routing protocol.

$$\text{NRL} = \frac{\text{number of routing packets}}{\text{total number of packets received by destination node}} \quad (3)$$

Obviously, these three performance metrics are somewhat correlated in an empirical sense. For instance, lower PDR implies that the throughput is poor, and the ALD metric is evaluated with fewer received samples. And also larger ALD value may imply that it would take much longer time to reach the destination for every data packet on the average, hence it would have the potential influences on the number of packets received successfully, which would impact both the PDR and NRL together.

When backup by an alternate path in case of link failure, the alternate path will be longer than the primary path in most of operational cases. The longer the data packet roams in the wireless LAN, the higher probability of packet drop it will have. Thus, a lower NRL would hint that the route is shorter, and also higher PDR and lower ALD may emerge.

3.3 Simulation results and performance comparisons

Figure 5 illustrates the packet delivery ratio for different backup strategies, which including four schemes: AODV, 2HBR, AODV-BR 1, and AODV-BR2. From the simulation result in Fig. 5, AODV-BR 1 performs better than the other backup strategies. At least 75% of the AODV-BR 1 data points are higher than those of AODV. AODV-BR 1 therefore achieves the design purpose of enhanced data delivery rate. Although salvaged data packets are sent through a different path, the probability of the packets reaching the destination node is high.

Having a closer look at Fig. 5, it reveals that there is a large gap between the data delivery performance of AODV-BR 1 and 2. Note that they only differ in the choice of *alternative next hop* and this difference greatly affects performance. It is noted that AODV-BR 2 forwards a packet to any next hop on the alternative path in order to get around the broken link. One explanation is that the any next hop policy of AODV-BR 2 may result in more resource demanding activity for every overhearing neighbor in the neighborhood during a high mobility situation. When a mobile node of AODV-BR encounters a link failure, it broadcasts those data packets to its neighbors. There are therefore many duplicates of the same data packets situated in the network. Some of these are sent along different paths toward the destination node, and others are lost. Such a phenomenon is also the so-called *spread of salvaged data packets*.

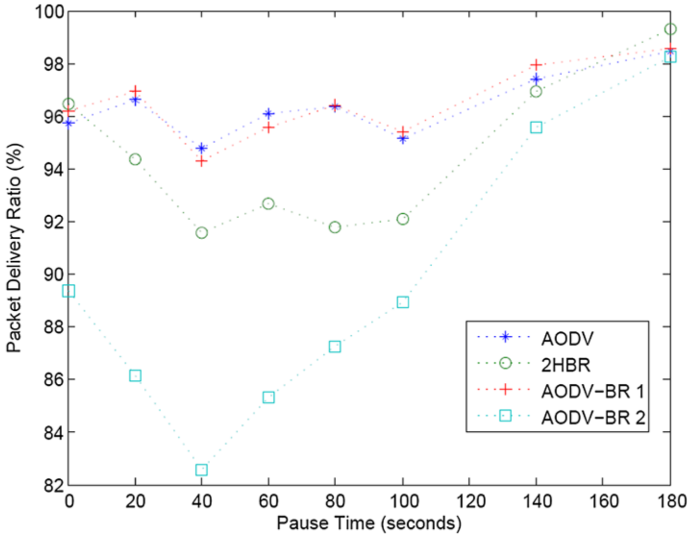


Fig. 5 PDR for different backup strategies

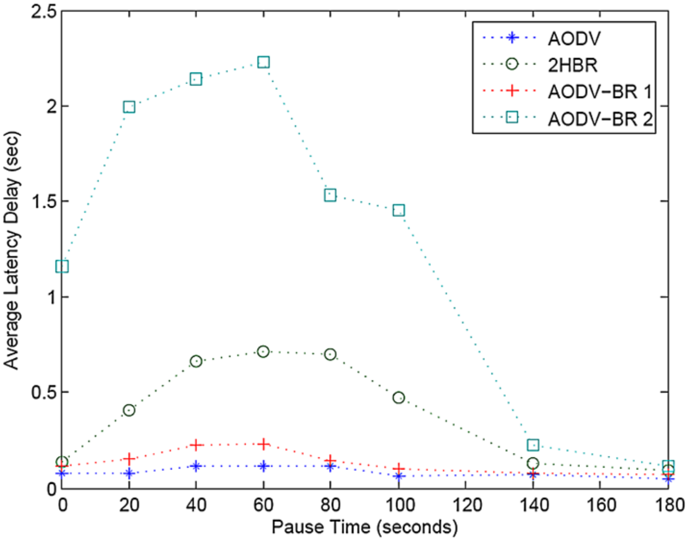


Fig. 6 ALD for different backup strategies

The patterns of average delay of four variants schemes are shown in Fig. 6. Backup routing introduces latencies due to the detour, and the data salvation procedure will therefore take longer time than basic routing schemes such as AODV. As Fig. 6 shows that AODV-BR 1 has the lowest average latency delay except classic AODV.

Next, AODV-BR 2 has the longest average latency delay. As previously mentioned, the spread of salvaged data packets would introduce excessive resource demanding activity that contribute to the delays due to more transmission collision and channel contention. Hence, larger ALD would be observed, which is much higher than that of AODV-BR 1. Furthermore, the ALD for 2HBR is also larger than that for AODV-BR 1. In addition to the time associated with the extra routing packets, 2HBR is also dependent on waiting delays introduced when checking if a path is still valid. Unlike AODV-BR 2, the latency of 2HBR mainly includes the waiting delays associated with detour assurance. 2HBR generally do not suffer from transmission collision and contention as data packets are not duplicated across the network.

Figure 7 depicts the simulated patterns regarding NRL of the different routing schemes. The routing load indicates the quantity of routing packets needed to determine if a data packet is received by its destination node. Routing overheads are unavoidable since routing packets are needed to create and maintain the necessary route information for data transmission.

Figure 7 also shows that the routing cost of AODV-BR 2 and 2HBR are similar. Their routing costs are larger than those of AODV-BR 1 and AODV. Although they are similar, the causes are different. AODV-BR 2 relies on the any next hop policy to salvage data packets, which would incur resource demanding distribution of salvaged data packets across the network. The network chaos produced by the node with link failure will also result in an increase in routing packets to handle the data packet

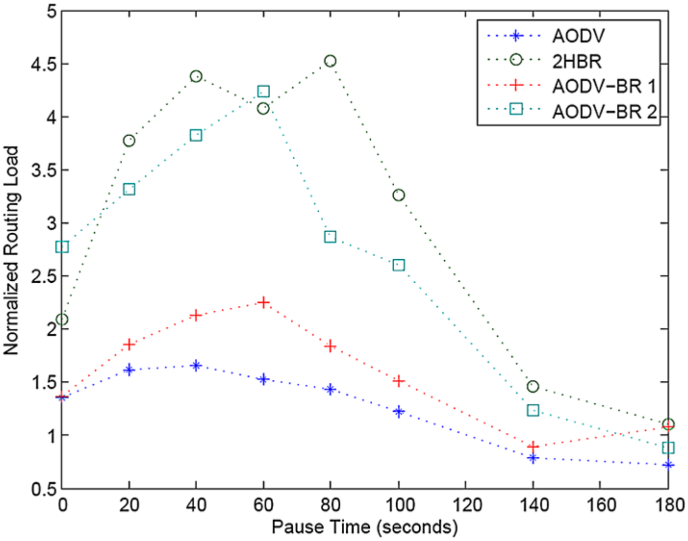


Fig. 7 Normalized routing load for different backup strategies

broadcasts on its neighboring nodes. Thus, the total routing cost of AODV-BR 2 increases. 2HBR relies on a detour assurance to ensure that path is still valid, and this validation step involves extra routing packets. Consequently, 2HBR has a higher routing load.

The simulation results show that different policies for data salvation can have profound effects on the performance of the network. Strengthening of data delivery may increase transmission collision and contention and consequently increase the transmission delay and routing load. AODV-BR 1 expresses better performance than that of the other backup strategies, i.e., AODV-BR 2 and 2HBR. AODV-BR relies on just one-hop alternative paths during the route reply phase, and no extra routing packets are needed. AODV-BR 1 relies on a fixed next hop policy to do its data salvation. According to the simulation results, this policy has the capability of enhancing the data delivery rate and preventing the spread of salvaged data packets. The spread of salvaged data packets is one of the main causes of transmission collision and contention.

The weakness of AODV-BR, including AODV-BR 1 and 2, has the need to duplicate data packets in its one-hop data broadcast during the data salvation phase. When a mobile node encounters a link failure, a one-hop data broadcast is used to send out the target data packets in the hope that other neighboring nodes possess alternative paths. Duplicates of the data packets spread in the neighborhood and the neighboring nodes' resources are consumed in the process. Some of the resources are wasted as only one of these duplicates is eventually used by the destination node. The fixed next hop policy of AODV-BR 1 limits this spread.

4 Proposed Dual Paths Node-disjoint Routing (DPNR) approach

From the simulation results in Figs. 5–7, AODV-BR 1 scheme has shown better performances over AODV-BR 2 and 2HBR in terms of performance metrics: PDR, ALD, and NRL. Hence, the backup routing protocol proposed herein is derived from AODV-BR 1. Remembering that AODV-BR 1 creates only one-hop alternative paths to form its backup structure in route reply, and it does not use extra routing packets during the route reply or data salvation phase. AODV-BR 1 is based on a fixed next hop policy which enhances the rate of data delivery and prevents the spread of salvaged data packets which lead to an increase in transmission collisions and contention. AODV-BR 1 will hereafter be referred to simply as AODV-BR for simplicity.

4.1 Overview of DPNR approach

An undesirable side effect of some backup routing protocols is performance degradation due to transmission collision and channel contention incurred from the increased communication among nodes. Basically, AODV-BR is not as effective and efficient in heavily loaded network as in lightly loaded network because of increased packet collision and channel contention. One obvious drawback of the AODV-BR fixed next hop policy is that there is only one alternative path, i.e., the disconnected next hop. Although this policy prevents the spread of salvaged data packets, it results in resources being consumed by neighboring nodes. To alleviate these impacts and to improve performance as well, the Dual Paths Node-disjoint Routing (DPNR) approach is presented and described as follows.

Paths that do not have any common node except the source node and destination node are termed as node-disjoint paths. In the works [21], authors proposed a routing scheme called NDMR (Node-Disjoint Multipath Routing). NDMR mainly modifies AODV to integrate path accumulation technique which records the accumulated address list into the route record of RREQ packets. When a RREQ packet is generated and forwarded by the source and intermediate nodes sequentially, their addresses would be appended in the route record of the RREQ packet. When the RREQ packet arrives at its destination, the destination node is responsible for selecting and recording multiple node-disjoint route paths. The NDMR approach would record the shortest hop count (to the source node) to establish better routes to the destination node in a session pair. In order to decrease the overall of the route table in each node, we limit the number of node-disjoint route paths to two in our DPNR scheme although more than two node-disjoint routes can be searched. The proposed DPNR adopt two node-disjoint paths for the routing framework.

The proposed DPNR approach combines both advantages of AODV-BR scheme and of dual paths node-disjoint routing scheme together. Supporting reasons for adopting DPNR are stated as follows. Firstly, the good data salvation characteristic in AODV BR is selected to be the foundation of the proposed DPNR scheme. Secondly, DPNR adopts “node-disjoint route paths” because the route independence property of node-disjoint multiple paths allow data transmissions on different paths of the session pair without affecting each other. This route discovery mechanism with node-disjoint paths has been shown to reduce the frequency of route discovery and has small routing costs [14]. Thirdly, node-disjoint dual paths of a session pair are established by the destination node at the same routing protocol run and are therefore both guaranteed suitable for data transmission. And also the load balancing can easily be incorporated into the scheme such that larger part of the network can be utilized under heavy traffic conditions. Finally, the redundancy economy for choosing only one standby can be theoretically explained in terms of the probability of disjointness of having k node-disjoint paths (NDPs) and the reliability enhancement factor in Sect. 6.

4.2 Route Request Phase

In principle, AODV-BR would only establish the related alternate paths around the primary path. The dual paths node-disjoint routing scheme provides an effective way to add another node-disjoint primary path nearby the first primary path. Due to excellent feature of route independence, these two primary routes would not interference each other during data packet delivery. Figure 8(a) exemplifies the operational pattern after two valid node-disjoint primary routes have been selected by the destination node. Basically we adopt the similar technique in the works of Li and Cuthbert [21]. Algorithm 5 describes the procedure for recording the shortest hop count. The word “my” in Algorithm 5 indicates the neighboring node itself. The steps regarding the route request phase are listed as follows:

Route Request Phase

1. We adopt the route request mechanism of NDMR to conduct the path accumulation process for recording useful route information.

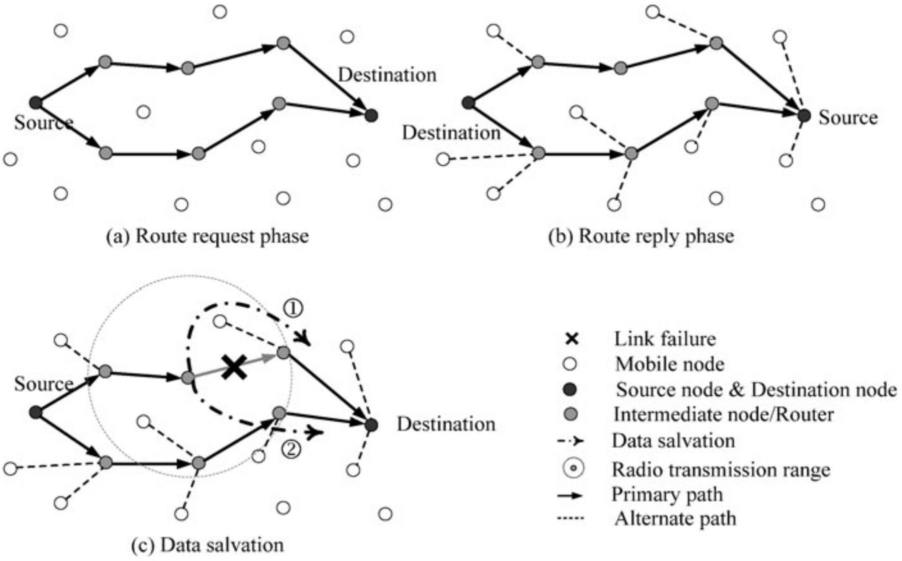


Fig. 8 DPNR route discovery and maintenance phases

Algorithm 5 Recording the shortest hop count to source node (action performed by intermediate nodes)

```
if (duplicated RREQ packet) and (the path is longer) then
    drop it;
else if (the shortest path to the source) then
    Shortest_Hop : = RREQ_Hop_Count;
Previous_Hop_to_Source : = RREQ_Previous_Hop;
    Route_Record.append(My_Address);
    RREQ_Hop_Count += 1;
    re-broadcast the RREQ packet;
else drop it;
endif
```

Definitions:
RREQ_Hop_Count : the hop count within the RREQ packet.
RREQ_Previous_Hop: the previous hop that sent the RREQ packet.
Shortest_Hop: the shortest hop count of the same RREQ packet.
Previous_Hop_to_Source : my reverse path's next hop.
Route_Record: accumulated address list within the RREQ packet.

2. A source node without a valid path to the destination node originates a RREQ packet and appends its own address into the route record of this RREQ packet before broadcasting it.
3. Any intermediate node who receives this RREQ packet will execute the following process (Algorithm 5) to deal with this RREQ packet. Algorithm 5 is applied by intermediate node that receives the RREQ packet.

4.3 Route Reply Phase

As the destination node receives some identical RREQ packets from different accumulated routes, it would assess the distances (hop counts) of these routes. Only two node-disjoint and shortest routes will be kept in the route table of the source and destination node. It is noted that we do not need excessive node-disjoint multiple primary paths in the proposed DPNR scheme. In the route reply phase, the proposed DPNR would also perform basic process in AODV-BR protocol to establish one-hop alternate paths around the two primary node-disjoint paths for data salvation. Figure 8(b) exemplifies the operational pattern in the route reply phase. The alternate paths are formed and depicted with dash lines in Fig. 8(b). Basic steps regarding the route reply phase are listed as follows:

Route Reply Phase

1. As the destination node receives the first RREQ packet, it will record this packet into its route table and then send a RREP packet back to the source node based on the route record of the RREQ packet.

2. When the destination node receives some duplicated RREQ packets, it will compare these RREQ packets to the first RREQ packet and then choose one shortest and node-disjoint path into its route table. Finally it unicasts a RREP packet back to the source node again along the primary path.
3. Any intermediate nodes, who overhear the RREP packet not directed to them, will create an alternate path and provide the backup function for data salvation of the primary path.

4.4 Route maintenance and backup strategy

Once a mobile node on the primary path encounters a link failure, it would first modify the header of data packets and then use one-hop broadcast to deliver data packets to one-hop neighboring nodes. Those neighboring nodes who overhear these data packets would conduct the following process (Algorithm 6) to handle with the data salvation task. The word “my” in Algorithm 6 indicates the neighboring node itself. The neighbors have two choices, namely to use the second primary path or the alternative paths. Combining NDMR scheme with the backup function provided by DPNR data salvation, there are two choices for the neighboring nodes to forward these data packets to the destination node. The default one is the active alternate path

Algorithm 6 DPNR data salvation backup strategy (action performed by neighboring nodes)

```
if (active alternative path to destination) then
    if (condition 1) and (condition 2) then
        DataPkt_Next_Hop : = Alternative_Next_Hop;
        forward data packets;
        break;
    endif
else if (active primary path to destination) then
    if (condition 1) then
        DataPkt_Next_Hop : = Primary_Next_Hop;
        forward data packets;
        break;
    endif
else drop it;
endif
```

Definitions:
DataPkt : the broadcasted data packet sent by the node with a link failure.
DataPkt_Next_Hop : the next hop of the broadcasted data packet.
Alternative_Next_Hop : my alternate path’s next hop to destination
Primary_Next_Hop : my primary path’s next hop to destination

Conditions:
1. My active path’s next hop is not the hop that needs help.
2. My alternative path’s next hop is exactly the disconnected hop.

with fixed next hop, and the option one is the second active node-disjoint primary path to the destination.

In spite of adding the second primary node-disjoint path to help forwarding data packets in the proposed DPNR scheme, we use the beneficial spirit in AODV-BR protocol to maintain those salvaged data on the right way and direction to the destination node. This combining advantages would be verified to be effective on improving performance in the simulations conducted in the following section. Figure 8(c) exemplifies the operational pattern in the data salvation scenario of the proposed DPNR scheme. Data packets could be salvaged through the alternate path with route number ① or the second node-disjoint primary path with route number ② in sequence.

5 Simulations and performance evaluations

We study the system performance via simulation using the network simulator NS-2. The wireless channel is modeled as described in Sect. 3.2. To evaluate the proposed DPNR scheme, two sets of simulations are conducted with two key parameters, which are the network mobility and the traffic load. The network mobility is characterized by the maximum speed of mobile nodes in the network. The domain of node speed is ranged from 0 meter/sec to the maximum speed throughout the simulation. The traffic load of the network is characterized by the "rate of data packet (transmission rate)." For each set of simulations, we focus on the influential patterns of three performance metrics by the key parameter. Three performance metrics are packet delivery ratio (PDR), average latency delay (ALD) and normalized routing load (NRL), which are described in (1)–(3) of Sect. 3. The classic AODV and AODV-BR are selected as the counterparts of routing protocol for comparison for brevity. Two sets of simulations are conducted and the experimental results are described in the following paragraphs.

5.1 Influential patterns by network mobility (simulation set 1)

In this simulation set, the maximum speeds of mobile nodes are control parameters to reflect different degree of node mobility in the network. Each mobile node is configured to start its journey from one random location to another random location with preconfigured speed. The range of the pre-configured speed is set from 0 meter/sec to the maximum speed. Each time when a mobile node arrives some location, it would keep moving to another new location immediately (0-second pause time). Such a process will be conducted in every mobile node of the network until the simulation time is ended. The maximum speed is configured and increased from 0 meter/sec to 40 meter/sec at an interval of 5.0 meter/sec.

The simulated results for performance metrics: PDR, ALD and NRL are illustrated in Figs. 9, 10 and 11, respectively. In Fig. 9, the simulated results show that PDR metric can be improved by the proposed DPNR scheme. The PDR metric is related with the rate of packet-loss during routing process. The data salvation function in DPNR scheme can mitigate the packet-loss phenomenon. And the second primary node-disjoint path can assure the routing path still applicable in case of link breakage in the first primary node-disjoint path, which obviously the packet-loss rate can

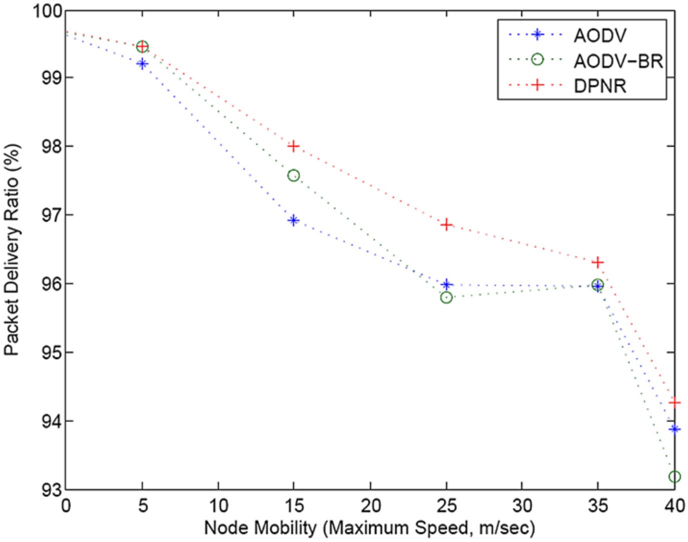


Fig. 9 Packet delivery ratio

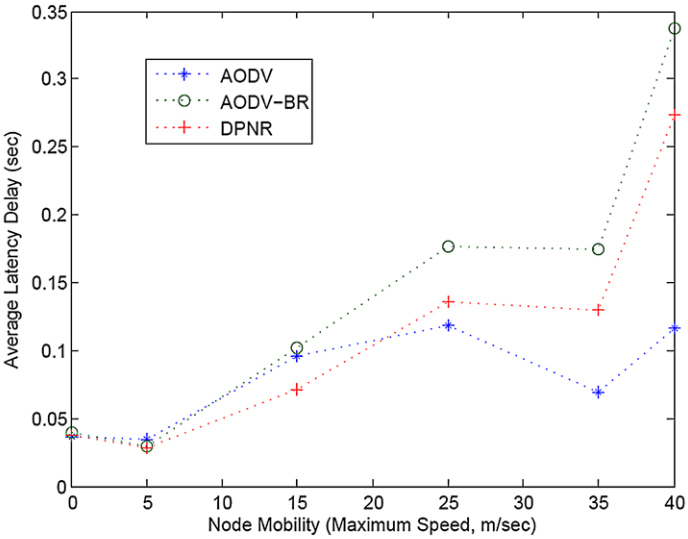


Fig. 10 Average latency delay

be reduced. Both data salvation function and second primary node-disjoint path are provided by our DPNR scheme, hence the simulation result in Fig. 9 shows that our DPNR outperforms AODV and AODV-BR schemes.

In Fig. 10, the proposed DPNR has a better performance in ALD than AODV-BR scheme for the entire domain of node mobility. But AODV scheme outperforms DPNR scheme when the node mobility is approaching 25 meter/second. As defined

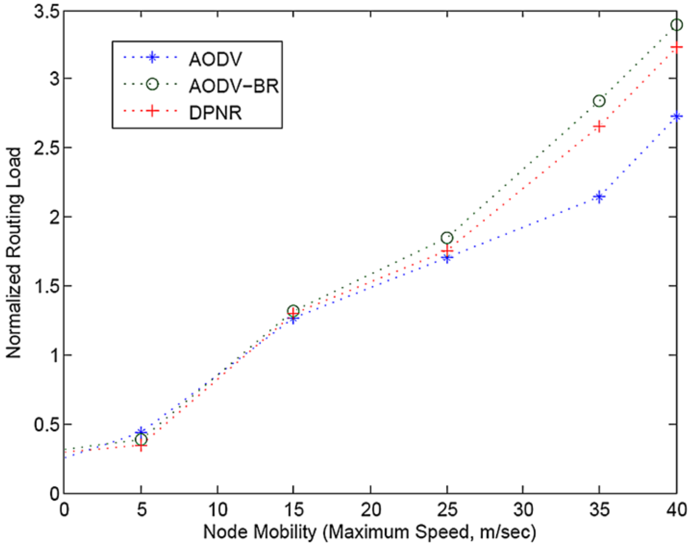


Fig. 11 Normalized routing load

in (2), ALD metric includes all possible delays: buffering during route discovery and link recovery phases, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer time. We describe the impacts on ALD when the node mobility becomes larger. It is assumed that a one-hop link exists between nodes A and B. The probability of A-B link breakage would be affected by the node mobility of nodes. The distance between nodes A and B would become larger as node mobility becomes larger. When the distance of A-B link exceeds the range of transmission, the link breakage will happen.

The larger the node mobility becomes, the higher the frequency on creation of new node-disjoint paths becomes higher. The classic AODV scheme sets up only one primary routing path by its protocol while the DPNR scheme has to create dual routing paths. The incurred latency delay of DPNR scheme would be larger than that of classic AODV scheme on the average. Hence, such an increasing rate would deteriorate ALD in link recovery phase for DPNR scheme. In Fig. 10, the simulation results show that the DPNR scheme has a worse performance in ALD than AODV scheme when the node mobility exceeds 25 meter/second.

In Fig. 11, the proposed DPNR scheme has a better performance in NRL than AODV-BR scheme for the entire domain of node mobility. But AODV scheme outperforms DPNR scheme when the node mobility is approaching 25 meter/second. The NRL metric defines the number of routing packets transmitted per data packet delivered at the destination node. Each hop-wise transmission of a routing packet is counted as one transmission. Because the frequency of recovering links would be increased as the node mobility becomes larger, the numbers of hops for each packet from source to destination node is then increased. The above simulation results demonstrate that the proposed DPNR scheme outperforms AODV-BR scheme and classic AODV scheme in the domain of medium and small node mobility, while

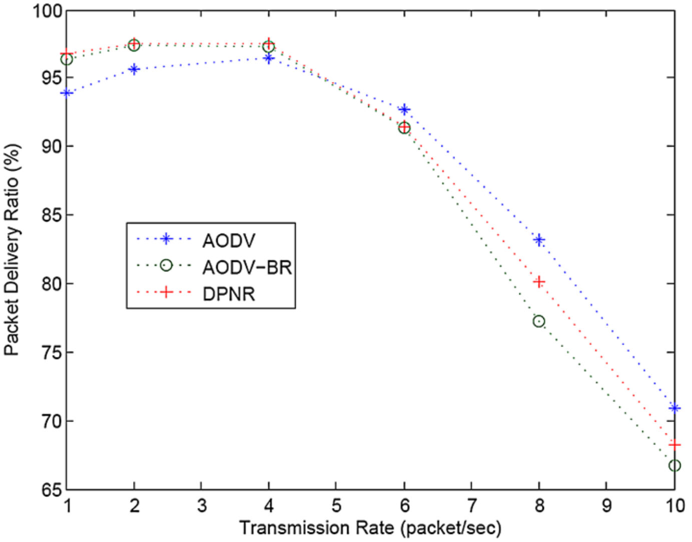


Fig. 12 Packet delivery ratio

DPNR scheme does not perform better than classic AODC scheme under large node mobility.

5.2 Influential patterns by traffic loads (simulation set 2)

In this simulation set, we configure multifarious transmission rates of all session pair to vary the traffic load of the network. Each mobile node is set to start its journey from one random location to another random location with preconfigured speed (0–20 meter/sec.), i.e., the maximum speed is fixed at 20 meter/sec. Each time when a mobile node arrives some location, it would keep moving to another new location immediately (0-second pause time). Such a process will be performed for every mobile node of the network until the simulation time is completed. The transmission rates are configured and scaled from 2 to 10 packet/sec with an incremental step of 2 packet/sec.

The simulation results for performance metrics: PDR, ALD, and NRL are displayed in Figs. 12, 13, and 14, respectively. In Fig. 12, the simulation results show that PDR metric can be improved by the proposed DPNR scheme. For the entire domain of transmission rate, the proposed DPNR scheme has better performances in PDR than AODV-BR scheme. Also DPNR has better performance in PDR than AODV scheme before transmission rate of 4 packet/sec. But AODV scheme outperforms DPNR in performance metric PDR when transmission rate exceeds 4 packet/sec. In higher traffic load situation, every intermediate node receives excessive data packets than it does in lower traffic load case. Each intermediate node does the one-hop broadcast and these broadcasted packets might become excessive burdens to its neighboring nodes as transmission rate becomes larger. Adoption of data salvation technique would increase the node's burdens in higher traffic load situation. One case is that neighboring nodes might lack enough time, bandwidth, or buffer to process these

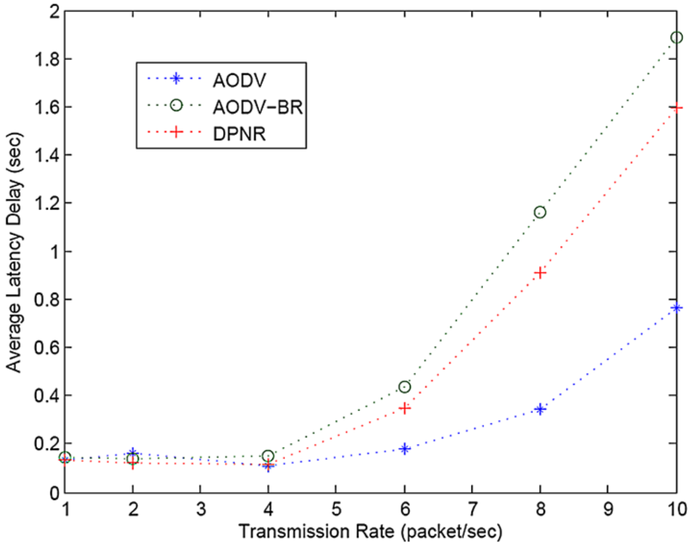


Fig. 13 Average latency delay

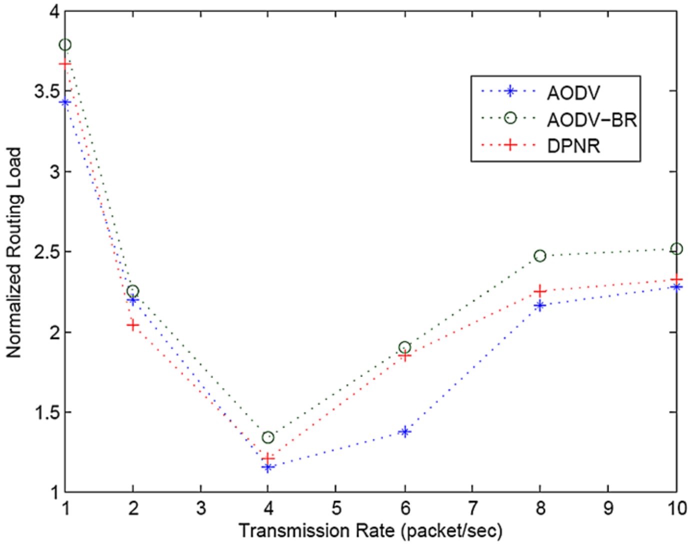


Fig. 14 Normalized routing load

over-abundant broadcasted packets, and these packets are dropped during routing process. Hence, the proposed DPNR shows worse performance in PDR than AODV scheme in higher traffic load environment.

In Fig. 13, the proposed DPNR scheme has a better performance in ALD than AODV-BR scheme for the entire domain of transmission rate. Also, DPNR has better performance in ALD than AODV scheme before transmission rate of 4 packet/sec.

But AODV scheme outperforms DPNR scheme in performance metric ALD when transmission rate exceeds 4 packet/sec. In higher traffic load situation, each mobile node has to process excessive data packets than it does in lower traffic load case. Adoption of data salvation technique may increase timing burdens in higher traffic load environment. The incurred time-consuming factor due to processing excessive packets may impact the ALD metric. Also, the increased packet-forwarding needs may increase the probability of packet collision, and hence the ALD metric would be deteriorated. In Fig. 14, the proposed DPNR scheme has a better performance in NRL than AODV-BR scheme throughout the entire domain of transmission rate. It is observed again that AODV scheme outperforms DPNR scheme in performance metric NRL when transmission rate exceeds 4 packet/sec. The above simulation results demonstrate that the proposed DPNR scheme outperforms AODV-BR scheme and classic AODV scheme in the domain of medium and small traffic loads, while DPNR scheme does not behave better than classic AODC scheme under large traffic loads because of increased packet processing, packet collision, and channel contention.

6 Rationales for dual paths in proposed approach (redundancy economy—why only one standby?)

Based on the spirit of the DPNR scheme, two primary node-disjoint paths of a session pair are established by the destination node at the same routing protocol run. One might question that the possibility of setting up more numbers of node-disjoint paths (NDPs) than just only two. Why don't we select more numbers (three or more) of NDPs in order to make the routing architecture more robust? We explore the theoretical reasons for the choice of the DPNR scheme in terms of the probability of disjointness of having k NDPs and the reliability enhancement factor.

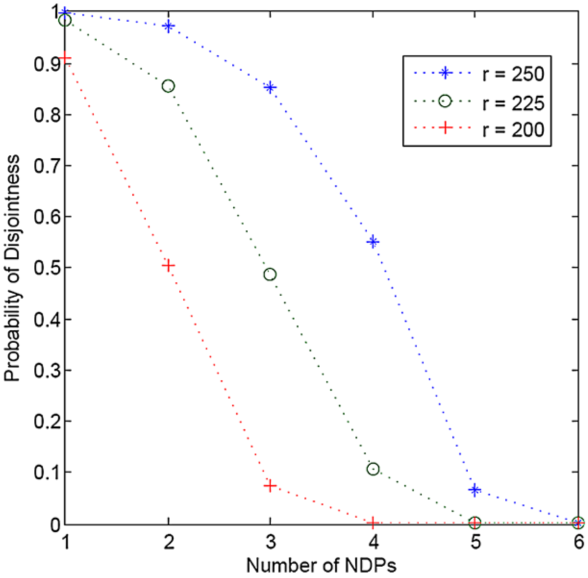
6.1 Probability of disjointness for k NDPs

In this subsection, we show that 2 NDPs would have much higher probability of disjointness than that of 3 or larger NDPs, and this supporting factor compels us to select two node-disjoint paths for our approach. It is assumed that a group of n mobile nodes each with transmission range r uniformly distributed in an area A where $(\pi r^2) \ll A$, with node density $\rho = n/A$. Following the result of [22, Sect. 4], the probability of each node has at least k neighbors, is given by

$$P[d_{\min} \geq k] = \left(1 - \sum_{j=0}^{k-1} \frac{(\rho\pi r^2)^j}{j!} \cdot e^{-\rho\pi r^2}\right)^n \tag{4}$$

It is noted that $d_{\min}$ stands for the minimum node degree of the network. The degree of a node is the number of neighbors, i.e., its number of links. Since the number of disjoint paths in a network for any given source and destination cannot exceed the minimum degree $d_{\min}$ of the network, $P[d_{\min} \geq k]$ can be regarded as an upper bound on the probability that there are k NDPs in the network for any pair of nodes. Hence, the expression (4) can be used to compute the probability that there are k NDPs in

Fig. 15 Probability of disjointness vs. number of NDPs searched



the network between a given source-destination pair. An illustrative example using (4) is presented to quantify the relations between the probability of disjointness and the number of NDPs found.

Using the same parameters in Table 2, we have $A = 1000 \times 1000\ \mathrm{m}^2$, $n = 50$, and $\rho = 5 \times 10^{-5}/\mathrm{m}^2$. With three different transmission range: 250 m, 225 m, and 200 m, Fig. 15 shows the probability of disjointness versus the number of NDPs searched. As the number of NDPs to be searched increases, the corresponding probability is decreased substantially, especially in the case of shorter transmission range.

As revealed in Fig. 15, the average probabilities of having two, three, and four NDPs are about 0.78, 0.47, and 0.22, respectively. Obviously, the probability value 0.78 gives us the concrete confidence and feasibility to implement the DPNR in the application scenario. This forms the first supporting rationale for adopting two NDPs, not three or larger, in the DPNR approach.

6.2 Reliability enhancement consideration on number of node-disjoint paths

The second supporting rationale would be described in terms of the reliability enhancement consideration on number of NDPs. For each source-destination pair, the multiple NDPs during a route discovery process can be treated as a model of parallel-backup configuration. From the basic reliability theory [23], the reliability expression for a parallel-backup system may be expressed in terms of the probability of success of each NDP. Because the node movements are almost ubiquitous for intermediate nodes along the NDP, each backup NDP can be considered as the so-called "hot standby unit" with the same failure rate as the active NDP. Generally, the node mobility has an essential impact on the failure rate of the node-disjoint path. The higher the node mobility is, the worse the failure rate of the NDP has. For simplicity, the failure of the switching device for parallel-backup system is neglected. Hence, for

Table 3 Numerical data on REF (%) for various (λ, L) pairs

λ	1/20	1/40	1/60	1/80	1/100	1/120	1/140	1/160	1/180	1/200	REF(L)
$L=1$	95.02	77.69	63.21	52.76	45.12	39.35	34.86	31.27	28.35	25.92	49.35
$L=2$	46.30	33.97	24.48	18.22	14.03	11.11	9.01	7.45	6.26	5.33	17.61
$L=3$	30.07	19.70	12.43	8.13	5.55	3.93	2.88	2.17	1.67	1.31	8.78
$L=4$	21.97	12.78	6.99	3.97	2.37	1.49	0.98	0.66	0.47	0.34	5.20
$L=5$	17.11	8.81	4.13	2.01	1.05	0.58	0.34	0.21	0.13	0.086	3.44
$L=6$	13.89	6.29	2.51	1.04	0.47	0.23	0.12	0.064	0.0037	0.0023	2.47

L NDPs connected in parallel: $R(t) = 1 - [1 - R_1(t)] \cdot [1 - R_2(t)] \cdots [1 - R_L(t)]$, where $R_i(t)$: the reliability of ith NDP.

In the case of constant failure-rate NDP, path's failure rate $= \lambda i$, $i = 1, \ldots, L$, and the expression becomes $R(t) = 1 - [\Pi_{i=1}^{L}(1 - e^{-\lambda_i t})]$. If NDPs are independent and identical paths with constant failure-rate ($\lambda i = \lambda, i = 1, 2, \ldots, L$), then the reliability function contains two independent variables: time to failure (t) and number of backups (L), hence, the reliability function regarding the NDPs can be expressed as follows:

$$R(t, L) = 1 - (1 - e^{\lambda t})^L, \quad L = 1, 2, 3, \ldots \tag{5}$$

To assess the degree of reliability enhancement by various L values instead of the absolute reliability values, an reliability enhancement factor REF(L) is defined as follows:

$$\text{REF}(L) \equiv \frac{R(t, L+1) - R(t, L)}{R(t, L)}, \quad L = 1, 2, 3, \ldots \tag{6}$$

Putting (5) into (6), the REF(L) becomes

$$\text{REF}(L) = \frac{e^{-\lambda t}(1 - e^{-\lambda t})^L}{1 - (1 - e^{-\lambda t})^L}, \quad L = 1, 2, 3, \ldots \tag{7}$$

The REF(L) may aid in the decision-making process for the optimal L value under limited budget. This is the case for the guideline for the DPNR. The REF(1) means that two NDPs are adopted, and REF(2) for three NDPs, etc. Noting that the function REF(L) is a multivariate function with three independent variables: failure rate (λ), mission time (t), and the numbers of NDPs. For example, assuming that a single NDP has the following operational parameters:

(1) Failure rates (λ) are assumed to be 1/20 to 1/200 (seconds)$^{-1}$ in step of 20 (seconds)$^{-1}$
(2) NDP mission time = 60 seconds.

The computed numerical data for REF(λ, L) in percentage (%) are listed in Table 3. The λ value represents the failure rate of NDP. The L value implies the numbers of backup NDPs used.

Table 3 has revealed that the average REF in last column for each assigned L can be from 49.35% to 2.47% for the chosen L values. Based upon the above modeling analysis, one can see that the substantial improvement (up to 49%) on reliability can be achieved by taking $L = 1$, i.e., taking two NDPs totally. Such a significant improvement level on the reliability of NDPs has strengthened the effectiveness and feasibility of applying the proposed DPNR approach. To meet the most cost-effective goal for deciding the number of NDPs, we select two NDPs for redundancy economy in DPNR design, and also this is the case that has been utilized in our experiments.

7 Conclusions

This article addresses the characteristics of AODV-based routing protocols, and how different backup strategies affect network performance. To have a deeper insight on relevant routing protocols, the AODV, AODV-BR1 AODV-BR2, and 2HBR are modeled and formulated by corresponding algorithms. And also each of them is simulated by NS-2 network simulator to obtain the necessary performance metrics for comparisons in terms of packet delivery ratio, average latency delay, and normalized routing load. Although AODV-BR delivers an acceptable data delivery ratio, its backup policy limits the choices during data salvation, the negative impacts of the spread of salvaged data packets should be alleviated. To mitigate such an impact, we present an improved approach called DPNR to reduce the redundancy-frames overhead during the process of data salvation by neighboring intermediate nodes. The proposed DPNR approach combines both advantages of AODV-BR scheme and of dual paths node-disjoint routing scheme together. To the best of our knowledge, it has not been applied before to improve quality of service in a cost-effective manner on reliable routing schemes in MANET.

The novel advantages for DPNR scheme combines good data salvation characteristic in AODV BR scheme with the route independence property of node-disjoint multiple paths. To validate the feasibility and effectiveness of the proposed approach, simulation experiments has been conducted and shown that the proposed DPNR scheme can provide a better performance metrics compared with its counterpart AODV-BR scheme. The simulation results demonstrate that the proposed DPNR scheme outperforms AODV-BR scheme and classic AODV scheme in the domain of medium-small node mobility and loaded network. It is also observed that compared with classic AODV scheme, DPNR scheme is not as effective and efficient in heavily loaded network as in lightly loaded network because of increased packet processing, packet collision and channel contention. The theoretical rationale for adopting DPNR scheme is also provided in terms of the reliability enhancement considerations and the quantitative analysis on probability of setting up more numbers of node-disjoint paths than just only two. This mathematical rationale can provide us with solid theory to meet the need of redundancy economy.

Acknowledgements The authors are partially supported by Taiwan Information Security Center (TWISC), National Science Council (NSC) under the grants NSC 95-2218-E-001-001, NSC95-2218-E-011-015, and NSC95-2221-E-029-020 -MY3.

References

1. Corson S, Macker J (1999) Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations. IETF RFC 2501, January 1999. URL: ftp://ftp.rfc-editor.org/in-notes/rfc2501.txt
2. Perkins CE (2001) Ad hoc networking. Addison-Wesley, Reading
3. Royer EM, Toh CK (1999) A review of current routing protocols for ad hoc mobile wireless networks. IEEE Pers Commun Mag 6(2):46–55
4. Chen C-W, Weng C-C (2009) Bandwidth-based routing protocols in mobile ad hoc networks. J Supercomput. doi:10.1007/s11227-008-0260-7
5. Perkins CE, Royer EM (1999) Ad hoc on-demand distance vector routing. In: The 2nd IEEE workshop on mobile computing systems and applications (WMCSA'99), New Orleans, LA, 25–26 Feb 1999, pp 90–100
6. Perkins CE, Royer EM, Das SR (2003) Ad hoc on-demand distance vector (AODV) routing. IETF Experimental RFC 3561, July 2003. URL: ftp://ftp.rfc-editor.org/in-notes/rfc3561.txt
7. Johnson DB, Maltz DA (1996) Dynamic source routing in ad hoc wireless network. In: Imielinski T, Korth H (eds) Mobile computing. Kluwer Academic, Dordrecht, pp 153–181
8. Johnson DB, Hu Y, Maltz DA (2007) The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. IETF Experimental RFC 4728, February 2007. URL: ftp://ftp.rfc-editor.org/in-notes/rfc4728.txt
9. Lee S-J, Gerla M (2000) AODV-BR: backup routing in ad hoc networks. In: Proceedings of IEEE wireless communications and networking conference (WCNS 2000), vol 3, Chicago, IL, 23–28 Sept 2000, pp 1311–1316
10. Chen H-L, Lee C-H (2005) Two hops backup routing protocol in mobile ad hoc networks. In: Proceedings of the 11th IEEE international conference on parallel and distributed systems (ICPADS 2005), vol 2, Fukuoka, Japan, 20–22 July 2005, pp 600–604
11. Chen W-T, Lee W-T (2004) Dynamic AODV backup routing in dense mobile ad hoc networks. In: IFIP international conference on wireless on-demand network systems (WONS 2004), Trento, Italy, 21–23 Jan 2004, LNCS, vol 2928. Springer, Berlin, pp 158–170
12. Perkins CE, Royer EM, Das SR, Marina MK (2001) Performance comparison of two on-demand routing protocols for ad hoc networks. IEEE Pers Commun Mag 8(1):16–28
13. Nasipuri A, Castañeda R, Das SR (2001) Performance of multipath routing for on-demand protocols in mobile ad hoc networks. ACM/J Mobile Netw Appl (MONET) 6(4):339–349
14. Abbas AM, Khandpur P, Jain BN (2003) NDMA: a node disjoint multipath ad hoc routing protocol. In: Proceedings of 5th world wireless congress (WWC), 2003, pp 334–339
15. Ye Z, Krishnamurthy SR, Tripathi SK (2003) A framework for reliable routing in mobile ad hoc networks. In: The 22nd annual joint conference of the IEEE computer communications societies (INFOCOM 2003), San Francisco, California, March/April 2003, pp 270–280
16. Pham P, Perreau S (2003) Performance analysis of reactive shortest path and multi-path routing mechanism with load balance. In: Proceedings of IEEE conference on computer and communication (INFOCOM), April 2003, pp 251–259
17. Abbas AM, Jain BN (2005) Analysis of disjoint multipath routing for mobile ad hoc networks. In: Proceedings of 7th IEEE international conference on personal wireless communications (ICPWC 2005), New Delhi, India, 23–25 Jan 2005, pp 42–46
18. Xu W, Yan P, Xia D (2005) Similar node-disjoint multi-paths routing in wireless ad hoc networks. In: Proceedings of 2005 IEEE international conference on wireless communications, networking and mobile computing (WCNM 2005), vol 2, Wuhan, China, 23–26 Sept 2005, pp 731–734
19. Fall K, Varadhan K (eds) (1999) Ns notes and documentation. http://www-mash/cs.berkeley.edu/ns/
20. Lin C-H, Jiang F-C, Chang J-C, Sandnes FE (2008) Node-disjoint alternative dual-path routing for data salvation in mobile ad hoc networks. In: Proceedings of the ninth international conference on parallel and distributed computing, applications, and technologies (PDCAT 2008), December 1–4, 2008, Dunedin, Otago, New Zealand
21. Li X, Cuthbert L (2004) On-demand node-disjoint multipath routing in wireless ad hoc networks. In: Proceedings of the 29th annual IEEE international conference on local computer network (LCN'04), Tampa, FL, 16–18 Nov 2004, pp 419–420
22. Bettstetter C (2002) On the minimum node degree and connectivity of a wireless multihop network. In: Proc of ACM mobile ad hoc networking and computing (MobiHoc), 2002, pp 80–91
23. Shooman ML (1990) Probabilistic reliability: an engineering approach, 2nd edn. Krieger, Melbourne