DOI 10.1007/s11276-007-0029-6

An efficient and flexible MPLS signaling framework for mobile networks

Ramprasad Nagarajan · Eylem Ekici

Abstract Multiprotocol Label Switching (MPLS) has gained momentum in recent years as an effective tool to provide Quality of Service (QoS) in a variety of networks. This has in turn created active interest in the area of recovery in MPLS based networks. A number of recovery schemes for MPLS domains have been proposed in recent years. However, the current schemes lack support for recovery in dynamic network topologies. In this paper, a new flexible signaling protocol for LSP rerouting in dynamic network environments is introduced. The signaling protocol recovers from node and link failures reactively, taking a local approach to LSP reestablishment. The performance of the signaling protocol is evaluated through simulations. Results indicate that the protocol can effectively and efficiently handle rerouting in dynamic networks with a low protocol signaling overhead as compared to contemporary MPLS rerouting protocols. This would enable the MPLS based IP-QoS support mechanisms to extend to dynamic network topologies.

Keywords MPLS · Dynamic LSP rerouting · Mobile networks

1 Introduction

Next generation communication networks are migrating towards a unified network architecture where both wired and wireless network segments will co-exist. This is accompanied by the growing demand on networks to provide QoS, due to the rise in popularity of real time and multimedia applications. Future networks should accommodate a variety of services, cater to different traffic types, provide support for user mobility, and still be able to guarantee QoS. Hence, there is a growing need for end-to-end QoS mechanisms with mobility support to address the requirements of heterogeneous network environments.

The wireless segments in the next generation networks are likely to be based on multi-hop ad-hoc or infrastructure-less networks. The ad-hoc networking concept brings a multitude of unique challenges to be addressed at various layers; wireless channel access, routing, and topology management to name a few. Unlike wired networks, mobile nodes in an ad-hoc network are usually distributed over a given geographical region. This prevents direct communication between all source-destination pairs. Therefore, mobile nodes in ad hoc networks must be able to act as relay nodes to enable end-to-end communication. Also, in wired networks, paths once established, hardly change. On the other hand in mobile networks, calculated routes have limited lifespan since the network connection structure changes due to nodal mobility. The topological changes affect the resource availability directly. Further, wireless resources and topological connectivity are even harder to track accurately because of the nature and transmission effects associated with the shared wireless media. Consequently, adhering to the negotiated QoS guarantees is even more challenging than in static network topologies. The QoS mechanisms for

A preliminary version of this work was presented at the 2004 IEEE International Conference on Communications, Paris.

R. Nagarajan (✉) · E. Ekici
Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210
e-mail: nagarajr@ece.osu.edu

E. Ekici
e-mail: ekici@ece.osu.edu

next generation architectures have to take into account these factors in order to be effective.

MPLS [1], with its Traffic Engineering (TE) [2] capabilities has emerged as a powerful tool to provide QoS support in MPLS enabled networks. MPLS uses the label-swapping paradigm to provide high speed packet switching over various types of networks, including IP [3], ATM [4] and Frame Relay [5]. The basic principle involves assigning short labels with local significance to packets at the input of an MPLS domain. This assignment is done by an ingress router known as the Label Edge Router (LER). A group of packets with similar requirements form a forwarding equivalence class (FEC) [1]. Every packet with the same FEC is assigned the same label and given the same forwarding treatment. The intermediate routers, known as the Label Switched Routers (LSR), map the incoming labels to the outgoing labels and the outgoing interface. This mapping information is maintained in tables created during path setup. In this way, traffic flows in an MPLS path known as a Label Switched Path (LSP). LSPs created using MPLS can also be used to deliver packets across multiple network segments, each with potentially different underlying technologies, making them suitable for next generation network architectures.

We propose to use MPLS as a means to seamlessly extend QoS guarantees into mobile wireless network segments. It is thus worth exploring how the MPLS technology traditionally designed for wired networks with static topologies can be applied to dynamic networks. In such a scenario, MPLS will provide a QoS signaling framework to complement existing routing protocols for both wired and wireless mobile networks. Hence, the implementation of future network architectures would be associated with the need of MPLS to support mobile wireless networks with dynamic topologies. This would enable the benefits of MPLS traffic control and service differentiation to extend to next generation architectures.

Many new routing protocols [6] have been proposed in literature to address the special requirement of handling nodal mobility in ad-hoc networks. On-demand or reactive routing, and source routing are some of the techniques employed at the routing layer of ad-hoc networks. Dynamic Source Routing (DSR) [7] protocol is a very important flagship ad-hoc on-demand routing protocol based on source routing. It is worth mentioning here that another significant advantage of the label switching approach used in MPLS is the ability to provide efficient source routing. In MPLS, the source route is encoded in the labels themselves, alleviating the need for data packets to carry the source route explicitly as in conventional IP source routing. Hence, MPLS can also provide additional benefits of efficiency when used with source routing protocols in dynamic networks.

MPLS control information is distributed via the MPLS signaling plane. As the most basic form of MPLS signaling, labels must be distributed to all MPLS enabled routers that are expected to forward data for a specific Forwarding Equivalence Class (FEC). The Label Distribution Protocol (LDP) [8] deals with this facet of MPLS signaling. MPLS Traffic Engineering (MPLS-TE) [2] is a powerful tool which allows the user traffic to be mapped efficiently to the available network resources. Although no label signaling protocol is imposed by MPLS standards, two signaling protocols for MPLS traffic engineering have been developed, namely CR-LDP [9] and RSVP-TE [10]. A detailed comparison between these two protocols is presented in [11]. Both protocols essentially provide control mechanisms for setup, tear down, and maintenance of LSPs. They enable reservation of different types of resources in order to satisfy the traffic constraints of various flows.

Recent research in MPLS signaling has focused on improving techniques for recovery in MPLS domains. However, the proposed solutions mainly based on the CR-LDP [9] and RSVP-TE [10] signaling framework or extensions thereof, are geared toward wired networks. As discussed earlier, QoS provisioning in dynamic networks is a non trivial problem. Hence, MPLS recovery techniques assume even greater significance in dynamic networks, and form the focus of our research. As will become evident in Section 2, contemporary MPLS recovery techniques are not suitable for dynamic networks as they don't account for nodal mobility. Additionally, there is no efficient way of migrating these techniques to make them more suitable for highly dynamic network topologies. Hence, new approaches to MPLS recovery are required. In this paper, we propose an MPLS LSP rerouting technique suitable for handling mobility in dynamic networks. The signaling protocol recovers from node and link failures reactively, and takes a local approach to LSP reestablishment. Target applications include networks with multihop ad-hoc wireless segments. Considering this, we also evaluate how our protocol can leverage ad-hoc routing protocols in dynamic network environments.

The remainder of the paper is organized as follows: Section 2 gives an overview of existing MPLS recovery techniques. In Section 3, we introduce our Flexible MPLS Signaling (FMS) protocol. The performance comparison of FMS and two possible alternate recovery techniques is presented in Section 4. In Section 5, the behavior of FMS under different routing protocols is studied. Section 6 summarizes relevant network statistics impacting the performance of FMS. In Section 7, we conclude the paper.

2 Related work

The Internet Engineering Task Force (IETF) has developed a framework for MPLS recovery [12], which defines two basic models for MPLS path recovery: *Protection Switching* and *Rerouting*. Recovery by these methods is classified based on the timing of the alternate path calculation and alternate path resource allocation. In protection switching or proactive recovery, the recovery Label Switched Path (LSP) is pre-established (both pre-calculated and pre reserved) before the occurrence of the fault. Rerouting on the other hand employs an on-demand or reactive approach to recovery LSP establishment (on-demand path calculation and on-demand resource allocation). Hence, there is a recovery time versus resource utilization tradeoff between the two approaches in handling failures. Sometimes, the proactive and reactive approaches may converge to an intermediate solution. In this case the path can be calculated before the failure (prequalified) and the actual verification and reservation of the path can happen after the failure.

Additionally, based on the scope of protection on the working LSP, MPLS recovery can be further classified according to the different recovery models described below:

2.1 Global repair

In the global or centralized repair model, the LSP is protected between the ingress and egress nodes by an end-to-end alternate path. As the recovery is activated end-to-end irrespective of where the failure occurs, this model is used to protect the LSP against any link or node failure on the entire path. In global repair, protection switching is preferred over rerouting because the setup overhead and delay to calculate the alternate path increases and may be prohibitive as the length of the alternate recovery path sought increases. Most commonly, global repair is activated at the ingress node. This means that the failure notification has to be propagated to the ingress node before a repair can be activated.

Two recovery schemes using protection switching with global repair have been proposed in [13] by Haskin et al. and in [14] by Huang et al. Haskin's scheme uses a reverse backup recovery technique. In this method, traffic is reversed at the point of failure back to the ingress node. This traffic is then redirected to an alternate LSP which is ready on standby mode. Huang et al. uses a similar technique to the standard global repair model with protection switching and ingress notification.

Another global scheme based on the rerouting technique is LSP Modification using CR-LDP [15]. This scheme can be used to modify the parameters of an existing LSP (like bandwidth, route etc.) without service disruption. Rerouting by this procedure is implemented using a differential bandwidth reservation approach in order to prevent double booking of network resources. This scheme relies on the ingress node to initiate the LSP modification signaling; hence this scheme is also referred to as Ingress Based Rerouting (IBR). When a link or node fails, the upstream node adjacent to it detects the failure. This node then notifies the ingress node of the LSP about the failure. As soon as the ingress node receives the notification message, it calculates a new path between itself and the destination. The recovery LSP passing through the newly calculated path is then setup using CR-LDP signaling [9]. After the new LSP is setup, the resources that are no longer used are released. Bandwidth is allocated in a differential manner, on all links which are common between the old and new LSPs, to prevent bandwidth double booking. An example failure scenario for IBR is shown in Fig. 1

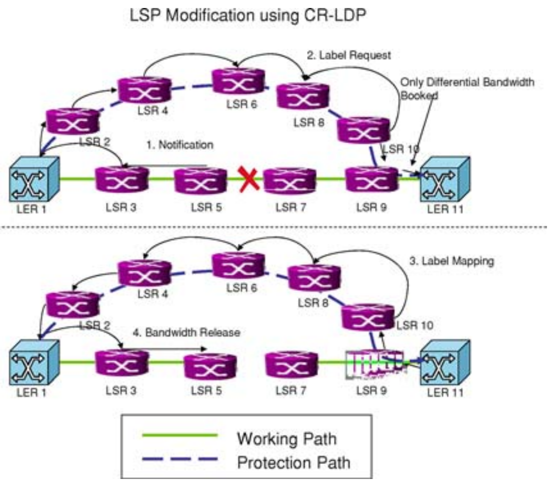

Fig. 1 LSP Modification using CR-LDP (IBR)- Global repair with rerouting

In this example,

- The original working LSP is established using CR-LDP signaling, from source LER1 to destination LER11 passing through LSRs 3, 5, 7 and 9.
- In the event of a link failure between LSR5 and LSR7, LSR5 detects the failure and notifies the ingress LER1 regarding the failure.
- LER1 calculates a new path to egress LER11 passing through LSRs 2, 4, 6, 8, 10, and 9. A label request message is injected through this new path.
- LER11 on receiving the label request message replies with a label mapping message sent back in the reverse direction as the request message. This way the new recovery LSP is established using conventional CR-LDP LSP setup signaling.
- In this case, the link between LSR9 and LER11 is common to the main and recovery LSP. As per this scheme, only the differential bandwidth is reserved on this link during the recovery LSP setup phase.
- LER1 also sends a release message to release unused bandwidth on the old LSP. In this case bandwidth between links LER1-LSR3 and LSR3-LSR5 are released.

Ingress Based Rerouting (IBR) protects the LSP from the ingress to the egress. Hence the entire path has to be recalculated end-to-end after the failure. For mobile networks, a local recovery scheme as opposed to an ingress based rerouting scheme may be more suitable from a recovery time perspective. Also, the global protection switching mechanisms under conditions of nodal mobility would warrant maintenance of the pre-established backup paths. Hence they may not be suitable from a signaling overhead perspective in dynamic networks.

2.2 Local repair

In the local or distributed repair model, protection is provided against a single link or node failure. In this method traffic is redirected around the point of failure. This model is usually used with rerouting from a resource efficiency standpoint. Local repair offers transparency to the ingress node and faster restoration times than the global mechanisms.

In [16] Yoon et al. have proposed an efficient local LSP recovery mechanism. In this scheme, multiple backup LSP's are pre-qualified on a per link basis at the time of LSP setup. An upstream LSR will update this pre-qualified backup path to its downstream LSR whenever there is a change in the network status. In the event of a link failure, the upstream LSR that has detected the failure establishes a recovery path by reserving bandwidth along the pre-qualified backup path.

However, this scheme does not cater to node failures and hence cannot handle nodal mobility. Additionally, this scheme will require heavy overheads, in maintaining several pre-qualified paths for each LSP in dynamic network environments.

2.3 Segment based repair

The segment based model is an intermediate model between local and global repair. In this method, the working path is divided into many segments. Each segment is then protected individually and will have a corresponding alternate recovery path. The protection on segments can be shared between multiple LSPs giving rise to more efficient resource utilization.

One segment protection switching scheme based on CR-LDP is presented in Fast Reroute extensions of CR-LDP (FR) [17]. FR maintains pre-computed and pre-allocated backup LSP tunnels for LSPs established by CR-LDP. Several backup segments may be maintained for a single LSP and they provide link and node failure protection along various segments of the LSP. When a link or node fails, the node adjacent to it detects the failure. The node detecting the failure informs the nearest upstream Path Switch LSR (PSL) about the failure, which in turn switches traffic onto a backup LSP segment. This backup LSP segment is path disjoint from the main LSP segment it protects, and is pre-established and ready in standby mode. It rejoins the working LSP at the Point Merge LSR (PML). An example failure scenario for FR is shown in Fig. 2.

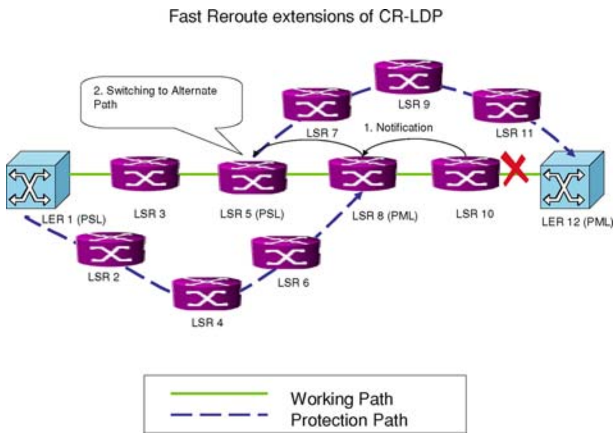

Fig. 2 Fast reroute extensions of CR-LDP (FR)

In this example,

- The original working LSP is established using CR-LDP signaling, from Source LER1 to destination LER12 passing through LSRs 3, 5, 8 and 10.
- Two backup LSP segments are also established using CR-LDP to protect segments from LER1–LSR8 and LSR5 to LER12 respectively. LER1 and LSR8 are the PSL and PML, respectively for the first segment. Similarly LSR5 and LER12 are the PSL and PML, respectively for the second segment.
- In case of a link failure between LSR10 and LER12, LSR10 detects the failure and notifies PSL LSR5 regarding the failure.
- LSR 5 switches the traffic to the backup segment consisting of LSR7-LSR9-LSR11.
- The backup LSP segment rejoins the original working LSP at LER11 which is the PML.

In the possible implementation of FR in mobile networks, along with the original paths, the backup paths would also require maintenance. Furthermore, in mobile environments, all segments of an LSP are subject to mobility. Hence, protection of multiple segments of an LSP increases the vulnerability of the LSPs since the starting point of the backup segments may lose communications with the main LSP. Therefore, FR must protect the entire segment starting at the ingress and ending at the destination. From this perspective, the performance of a practical implementation of the FR scheme under conditions of mobility will be similar to the global schemes with protection switching discussed previously.

3 Introduction and description of flexible MPLS signaling (FMS)

As presented above, the existing LSP recovery schemes discussed, were not intended for use in mobile networks. To the best of our knowledge, no LSP rerouting technique for mobile networks has been proposed in literature. In this paper, we propose a novel Flexible MPLS Signaling (FMS) protocol for mobile networks. FMS recovers from a fault by linking the upstream and downstream nodes around the point of failure. The fault detection takes place at the router immediately downstream to the failure. The LSR detecting failure initiates the recovery and tries to establish an alternative path with the immediate upstream neighbor of the node of failure. This LSR is known as the Initiator of Recovery (IOR). The alternate path is established hop-by-hop using the underlying routing mechanism. The label distribution to establish the recovery path uses downstream unsolicited mode [1]. Using this technique, the recovery can start as soon as the signaling message reaches the upstream LSR. In general, this can take place without the intervention of the ingress or egress node unless the end nodes are part of the alternate recovery path. At the targeted upstream LSR, the recovery path merges with the original LSP. Hence, this LSR is referred to as the merge point (MP) of recovery. The bandwidth is released on the unused portions of the old path, ensuring that the network resources are utilized optimally.

Salient properties of FMS are summarized as follows:

- The recovery scheme is reactive in nature. i.e., it does not rely on any pre-computation or pre-reservation of resources. Instead it establishes the recovery path on demand after the failure has been detected, and can therefore cater to mobile environments.
- The proposed protocol addresses both node and link failures.
- The traffic can be diverted on to the new path as soon as the signaling message reaches the merge point MP.
- The scheme aims to release resources in unused portions of the original LSP.

We propose to employ FMS in a single-domain multi-hop wireless network environment. Each of the individual mobile nodes are MPLS enabled Label Switched Routers (LSRs). The mobile nodes communicate with neighboring nodes that lie within their transmission radii. Additionally, we assume the existence of an underlying routing protocol. This higher layer routing protocol is responsible for re-computing routing tables whenever there is a topology change in the network. The topology change can be caused by node mobility or node and link failures. Only bandwidth constraint parameters are considered in FMS. FMS is composed of the following phases:

3.1 LSP setup phase

Consider a connection that is established from source S to destination D with a bandwidth requirement of B_w. Let there be a shortest path between S and D passing through the LSRs $\{N_1, N_2, N_3, N_4, N_5\}$, which satisfies the bandwidth requirement B_w of the connection. An LSP is explicitly established from S to D passing through the nodes $\{S, N_1, N_2, N_3, N_4, N_5, D\}$ as shown in Fig. 3.

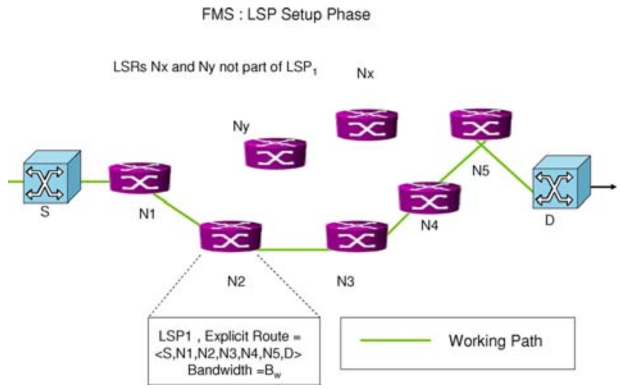

Fig. 3 LSP setup

This LSP is uniquely identified in the MPLS domain by an LSP identifier LSP$_i$. LSP$_i$ setup follows the basic CR-LDP setup procedure. Additionally, information pertaining to the LSP required for local recovery is stored in the LSRs along the LSP. Traces of the explicit route record $\{S, N_1, N_2, N_3, N_4, N_5, D\}$ along with the constraint parameter B_w and LSP identifier LSP$_i$ are stored in each LSR on LSP$_i$.

3.2 Failure detection phase

Failures are detected at the node downstream to the failure. The failures can be detected through a timeout mechanism or based on feedback from the lower layers. FMS does not differentiate between node and link failures. This reduces the protocol overhead required to distinguish between these two possibilities. Link failures are also treated as the failure of the upstream node. For example, let there be a node failure in LSR N_f or a link failure between N_f and N_{f+1}. In both these cases, N_{f+1} detects the failure and initiates the recovery signaling. Hence, N_{f+1} assumes the role of the Initiator of Recovery (IOR).

3.3 Failure recovery phase

The IOR N_{f+1} attempts to establish a link with the upstream router N_{f-1} around the failure. At LSR N_{f-1}, the recovery path joins the original LSP. Hence, LSR N_{f-1} is called the Merge Point of Recovery (MP). In the special case where the link between S and N_1 goes down, the ingress itself becomes the MP. IOR sends a Recovery LSP Setup message (RLS) directed towards the MP. The fields of the RLS message are described as follows:

1. Recovery flag: A bit denoting whether or not the recovery mode is active.

2. Destination flag: A bit denoting whether or not the RLS message is triggered by a destination movement.
3. Merge point: A value containing the IP address of the MP. This address is obtained from the explicit route record.
4. LSP ID: A value containing LSP ID of the path to be recovered.
5. Route record: The list of the nodes contained in the original LSP.
6. Label mapping message: An unsolicited label-mapping message [18] containing the label bindings for the recovery path.

The RLS message travels hop by hop towards MP, aided by the underlying routing mechanism. During this phase, there is an interaction between the network and MPLS layers at every hop. The network layer is responsible for obtaining the forwarding address of the next hop towards MP. The MPLS layer is responsible for the constraint-based establishment of the next hop. We assume that the original explicit LSP is also created using a shortest path routing algorithm. When a node N_r receives the RLS message, it becomes aware that it is to accept labels in the unsolicited mode. Consequently N_r performs the following set of functions:

1. N_r accepts the label contained in the RLS message, stores the value of the label and binds it with LSP_i
2. N_r updates the route record by inserting itself into the appropriate location in the route record if $N_r \notin \mathrm{LSP}_i$
3. If $N_r \notin \mathrm{LSP}_i$
   (a) Try to establish an equal resource path to the next hop satisfying bandwidth constraint parameter B_w
   (b) If B_w is not available, renegotiate another parameter $B'_w < B_w$
   (c) If B_w is allocated, send updated RLS message to next hop, the new N_r
   (d) Otherwise, send failure notification to IOR to abort recovery.
4. If $N_r \in \mathrm{LSP}_i$, & $r > f + 1$, i.e., if N_r lies downstream of the IOR, there is a potential for double bandwidth allocation after recovery phase. In this case, N_r releases the bandwidth between itself and N_{r-1}
5. If $N_r \in \mathrm{LSP}_i$, & $r < f - 1$, i.e. N_r lies upstream of MP
   (a) If recovery flag is set, i.e., if N_r is the first node on the original LSP_i upstream to the failure receiving the RLS message
      (i) Replace binding with new LSP binding
      (ii) Reset recovery flag
      (iii) Send the RLS message to N_{r+1}
      (iv) Release the Bandwidth allocation between N_r and N_{r+1}

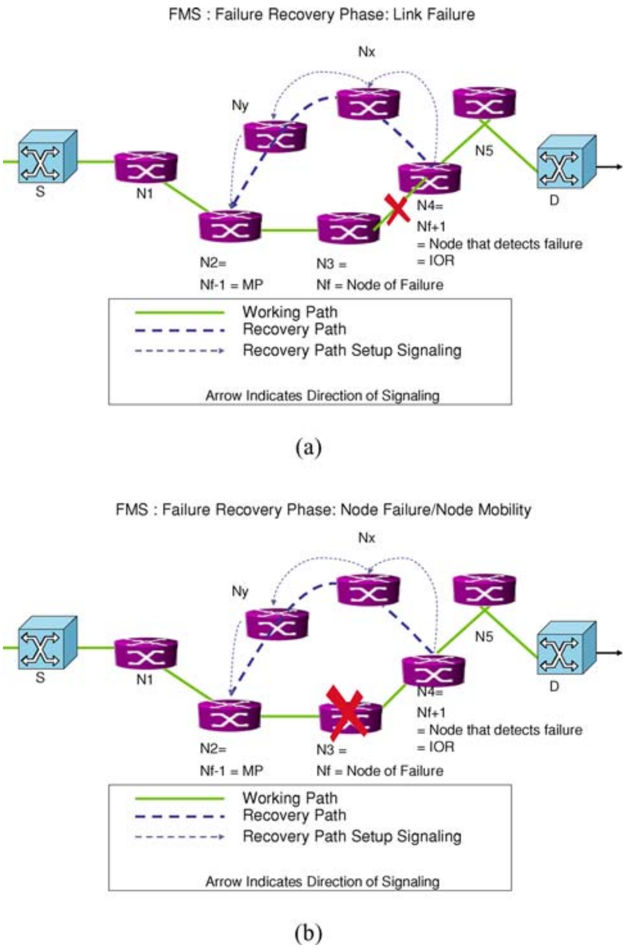
FMS : Failure Recovery Phase: Link Failure
Nx
Ny
S
N1
N5
D
N4=
Nf+1
= Node that detects failure
= IOR
N2=
Nf-1 = MP
N3 =
Nf = Node of Failure
Working Path
Recovery Path
Recovery Path Setup Signaling
Arrow Indicates Direction of Signaling
(a)
FMS : Failure Recovery Phase: Node Failure/Node Mobility
Nx
Ny
S
N1
N5
D
N4=
Nf+1
= Node that detects failure
= IOR
N2=
Nf-1 = MP
N3 =
Nf = Node of Failure
Working Path
Recovery Path
Recovery Path Setup Signaling
Arrow Indicates Direction of Signaling
(b)

Fig. 4 Failure recovery phase

   (b) If recovery flag is not set, i.e., N_r is on the unused part of the LSP_i upstream to the failure.
      (i) Remove label bindings with LSP_i
      (ii) Send the RLS message to N_{r+1}
      (iii) Release the Bandwidth allocation between N_r and N_{r+1}
6. If $N_r = \mathrm{MP}$, Recovery flag is set
   (a) Replace binding with new LSP binding
   (b) If N_f is down, terminate
   (c) If N_f is up, release the bandwidth allocation between MP and N_f, send RLS to N_f. At N_f remove bindings and terminate.
7. If $N_r = \mathrm{MP}$, Recovery flag was reset
   (a) If N_f is down, remove bindings and terminate
   (b) If N_f is up, release the bandwidth allocation between MP and N_f, remove bindings from cross-connect tables and send RLS to N_f. At N_f remove bindings and terminate.

In Fig. 4, a sample failure scenario is depicted. Upon failure of the link between N_3 and N_4 as shown in Fig. 4(a)

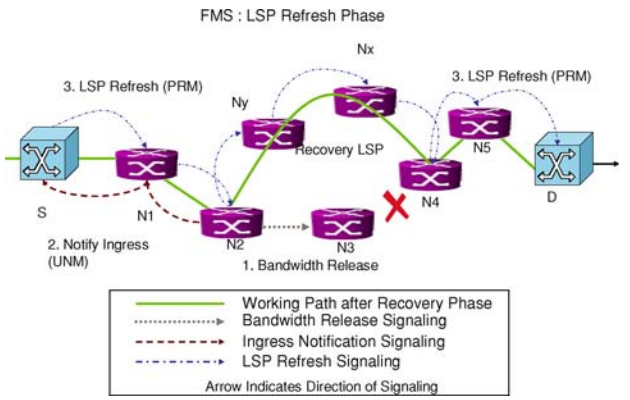

Fig. 5 LSP refresh phase

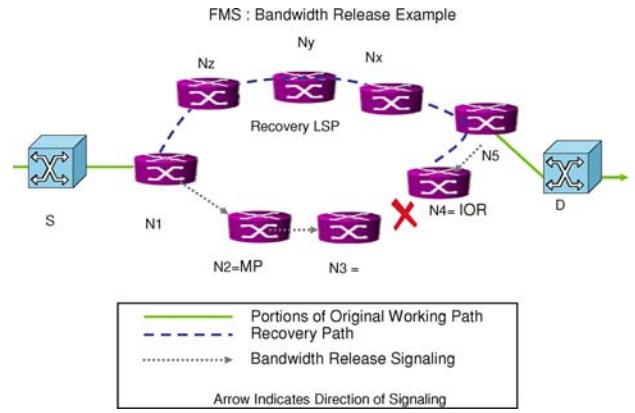
FMS : Bandwidth Release Example
Ny
Nz
Nx
Recovery LSP
N5
S
N1
N4= IOR
D
N2=MP
N3 =
Portions of Original Working Path
Recovery Path
Bandwidth Release Signaling
Arrow Indicates Direction of Signaling

Fig. 6 Bandwidth release example

or the node N_3 as shown in Fig. 4(b), N_4 assumes the role of the IOR. It sends an RLS message to N_x on the shortest path to MP $= N_2$. The message traverses N_x and N_y and is finally received by N_2. As soon as the label binding in N_2 is done, the traffic can be diverted to the new path. After that, N_2 proceeds with the release of the bandwidth between N_2 and N_3.

3.4 Ingress coordination and LSP refresh phase

The MP creates an Update Notification Message (UNM) with the updated route record and constraint parameter values. MP sends UNM to the ingress node S. Upon receiving UNM, the ingress node S sends an LSP Parameter Refresh Message (PRM) across the new path. LSRs receiving the PRM update their route record trace and B'_w value. An example ingress coordination and LSP refresh phase is depicted in Fig. 5. The UNM is sent by N_2 to S (dotted hops). After that, S triggers the LSP refresh process sending PRM to N_1. This message is forwarded to N_2, N_y, N_x, N_4, N_5 and D. These nodes refresh the LSP traces of LSP$_i$ and adjust the new bandwidth allocations.

3.5 Recovery abort phase

If a suitable path to the merge point can not be found, a failure notification message is sent to the IOR. The IOR will then send a release message to release up any bandwidth that may have been reserved in the attempt to establish a recovery path to the MP. In the example Fig. 5, assume that bandwidth negotiations have failed between N_y and N_2. Considering that the recovery path setup was unsuccessful and aborts at LSR N_y, the IOR releases bandwidth in links between N_y and N_x and between N_x and IOR. IOR then sends a failure notification for LSP$_i$ to ingress S through another path in the network. S then makes an attempt to modify the entire LSP using CR-LDP LSP modifications [15].

3.6 Special cases

Example of bandwidth release

One of the highlights of the protocol is its ability to free up bandwidth to avoid potential double allocation of resources after the recovery phase. Here, we present an example to illustrate the bandwidth release mechanism in further detail. In the example shown in Fig. 6, link between N_3 and N_4 is down. Hence, N_3 is the node of failure. N_4, the node detecting the failure assumes the role of IOR and selects N_2 as MP. As illustrated in the Figure, the recovery LSP overlaps with the original LSP on links between the IOR and N_5 downstream to the fault, and between N_1 and MP upstream to the fault. For this scenario, N_5 will release bandwidth between itself and IOR and N_1 will release bandwidth between N_1 and MP during the Recovery LSP path setup.

Movement of the source node

In case there is a movement of the ingress LER itself as shown in Fig. 7, a new LSP establishment is initiated following a similar procedure to the LSP setup phase. However, the setup message will contain the old LSP ID. This would trigger a bandwidth release phase on the old path as soon as the destination D receives the LSP setup request message.

Movement of the destination node

In case the egress LER moves, one of two things may happen. If the new neighbor of D is part of the original LSP, the egress sends an RLS message to its neighbor as the MP. Standard neighbor discovery techniques employed in the MAC layer can be used to sense the presence of neighbors. Such systems use beacon messages to transmit information pertaining to neighbor discovery. One such technique is discussed in [19]. The beacon messages can be modified to include the node ID of the neighbor. The augmented beacon is then co-related

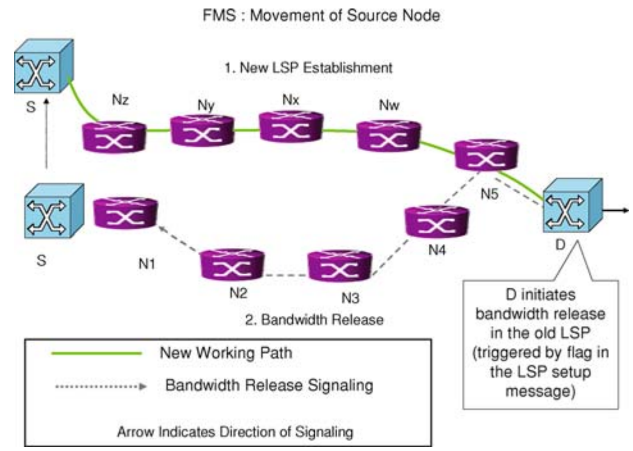
FMS : Movement of Source Node
1. New LSP Establishment
S
Nz
Ny
Nx
Nw
N5
D
S
N1
N2
N3
N4
2. Bandwidth Release
New Working Path
Bandwidth Release Signaling
Arrow Indicates Direction of Signaling
D initiates bandwidth release in the old LSP (triggered by flag in the LSP setup message)

Fig. 7 Source node movement example

with the source route database information to take a local decision on how to forward the RLS message. For example, in case there are more than one neighbors who are part of the original LSP, the egress will choose the nearest neighbor to the source as the MP. It will obtain the neighbor node ID from the beacon messages and compare that to the source route database for that LSP.

Alternatively, if a new neighbor is not part of the original route, D will initiate an RLS message with MP = the ingress LSR S. In both cases, as the RLS message will show the destination flag to be set, the MP will initiate bandwidth release on the old LSP in the downstream direction. Figure 8(a) depicts the case where the LSP moves to a neighbor which is part of the original LSP. Figure 8(b) shows the second case where the destination selects the source itself as the MP.

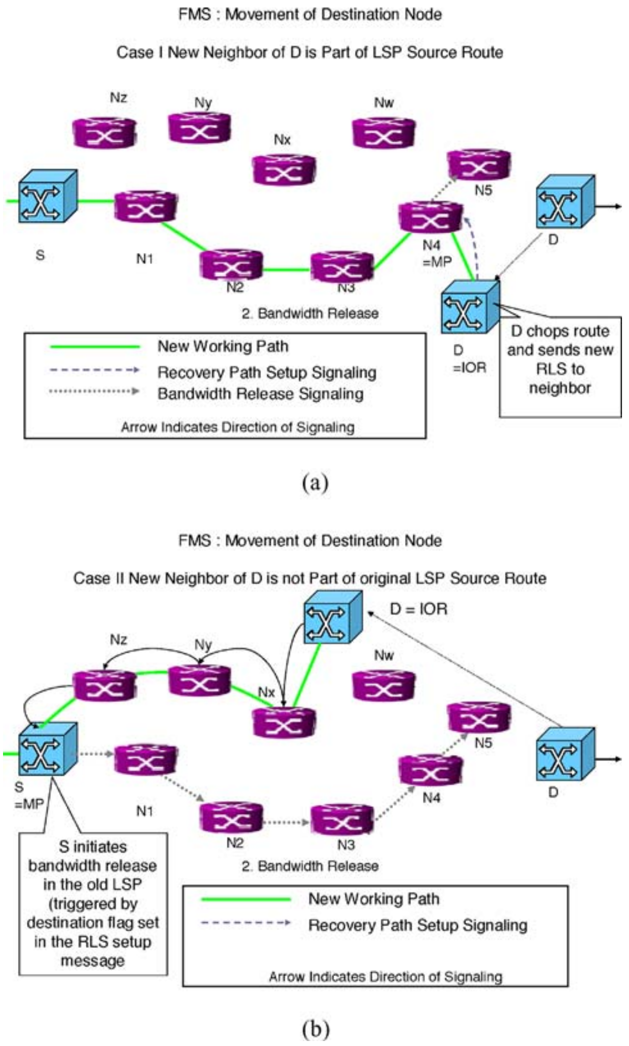
FMS : Movement of Destination Node
Case I New Neighbor of D is Part of LSP Source Route
Nz
Ny
Nx
Nw
N5
S
N1
N2
N3
N4 =MP
D
D =IOR
2. Bandwidth Release
D chops route and sends new RLS to neighbor
New Working Path
Recovery Path Setup Signaling
Bandwidth Release Signaling
Arrow Indicates Direction of Signaling
(a)
FMS : Movement of Destination Node
Case II New Neighbor of D is not Part of original LSP Source Route
D = IOR
Nz
Ny
Nx
Nw
N5
S =MP
N1
N2
N3
N4
D
S initiates bandwidth release in the old LSP (triggered by destination flag set in the RLS setup message)
2. Bandwidth Release
New Working Path
Recovery Path Setup Signaling
Arrow Indicates Direction of Signaling
(b)

Fig. 8 Destination node movement example

4 Performance comparison of FMS and alternative protocols

In this section, the performance evaluation of the proposed FMS algorithm is presented. The performance of the new FMS algorithm has been compared with the performance of existing Ingress Based LSP Rerouting (IBR) [15] and Fast Reroute (FR) [17] algorithms via simulations.

Simulation environment

An event based simulator was built in VC++ to implement the FMS protocol along with competitor protocols IBR and FR. The Custom Built Network Simulator (CBNS) was built in order to implement the various recovery schemes.

The CBNS was built using VC++ in the windows environment. It is a discrete event simulator. Following modules were implemented and are briefly described below:

- Network topology module: This module was responsible for the creation of the initial network topology, nodes, neighbor lists, and links. In case of changes in the network, the network topology and associated entities were updated to reflect changes in the network state.
- LSP traffic module: An LSP creation (traffic injection) and tear down mechanism was implemented in this module.
- Mobility module: This module handled the nodal mobility based on the random walk mobility model [20].
- FMS/IBR/FR module: The FMS/IBR/FR modules were implemented in this module. This core module implements the recovery protocol and in turn calls the Bellman Ford Shortest Path algorithm in order to establish the recovery path.
- Routing module: The routing protocols are implemented in this module.
- Event sequencer : This module is responsible for sequencing events in the simulator.

Table 1 Simulation parameters

Type	Number of nodes	Node density (Nodes/m^2)	Area (m^2)	Transmission radius (m)
Denser	150	.00060	500 × 500	90
Dense	150	.00042	600 × 600	90
Coarse	150	.00031	700 × 700	90

Simulation experiments

The main experiments which were conducted for the purpose of this evaluation:

- **Experiment I:** We compare the difference between the shortest paths after failure compared to the paths set up by each rerouting technique.
- **Experiment II:** We measure the time between occurrence of failure and instance of traffic resumption and observe the response time for each technique.
- **Experiment III:** We measure and compare the total rerouting overhead for each technique.
- **Experiment IV:** We measure the total number of packets arriving out of sequence for each rerouting scheme.
- **Experiment V:** We compare the failure ratio of rerouting for each technique.
- **Experiment VI:** We estimate the additional database requirements on the mobile nodes, needed to perform local recovery.

Experiments were performed on random network topologies with specific size, area and node density parameters as presented in Table 1. For each topology generated, we randomly distribute 150 mobile nodes over three different areas creating three different node densities.

We assume that communication between a mobile node and its neighbor nodes takes place within a fixed transmission range, which is chosen as 90 m. LSPs are established between randomly selected source-destination pairs in the network.

Initial LSP path setup follows minimum hop paths between the source and destination, calculated using Bellman Ford shortest path algorithm [21]. A random walk mobility model [20] is used to simulate node mobility. Mobility events are injected randomly within the simulation interval. The mobility of a node may cause it to move out of the communication range of its neighbors, which will cause a link failure. A neighbor discovery technique employed at the MAC layer can be used to detect the failure and provide feedback to the upper layers. All LSPs that pass through a failing link must be rerouted. Readings pertaining to the original LSP and the modified LSP after rerouting are noted for each rerouting event. All data points presented in this section reflect the average of 1000 independent simulation runs.

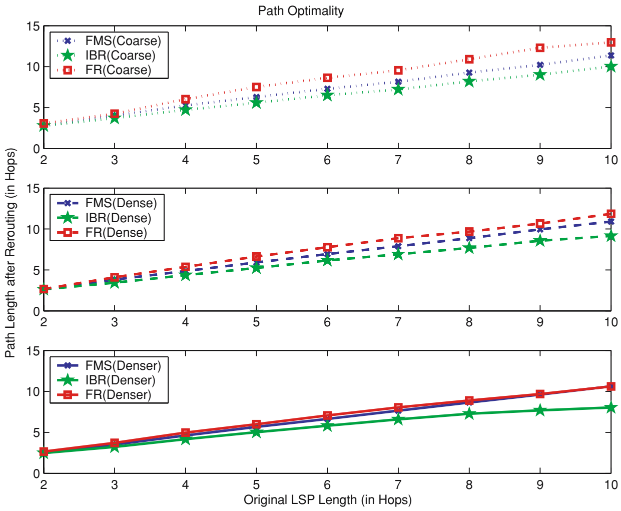

Fig. 9 Path optimality under different node densities

4.1 Path optimality

We define an optimal path as a path that has the minimum number of hops between a given source-destination pair. Based on this definition, the recovery LSP created after rerouting by various algorithms may be sub-optimal. In this experiment, we measure the length of the recovery LSPs after rerouting for each technique. We also show the deviation of the recovery LSPs established for each rerouting technique from minimum hop paths. For this purpose, data pertaining to the length of the LSP was collected before and after a rerouting event for each of the schemes under three node densities. While the IBR scheme selects the minimum hop path in the network at the time of rerouting, recovery paths produced by FMS and FR are potentially suboptimal.

Figure 9 depicts the length of LSPs after rerouting for each rerouting technique. The recovery LSP established by IBR is the same as the shortest path in the network. The FR recovery LSPs are longest and farthest away from optimal paths. This is because, there is a higher probability that the shortest link-disjoint LSP, which is used by FR, is much longer than the original LSP. The length of the recovery LSP in the case of FMS lies between these two techniques. The decrease in network density has the effect of increasing the length of the rerouted LSP for all three schemes. This increase is caused by the lack of short alternative paths in sparsely populated networks.

4.2 Response time

The response time is measured between the instant of failure and the instant when traffic can resume on the rerouted LSP. The total response time (T_r) until traffic can resume is calculated as $T_r = T_d + T_n + T_s$, where

- T_d (Detection time): The time taken to detect failure.
- T_n (Notification time): The time to notify the failure processing node about the failure
- T_s (Switch over time): The time taken to switch to the new LSP.

In the following simulations, failure detection time T_d is not considered as it adds the same offset to the total response time for all three algorithms. Additionally, the path calculation times accounted for in this analysis, assumes DSR as the underlying routing protocol. Figure 10 depicts measured response time for varying LSP lengths. For FMS, the processing node (IOR) and the node detecting the failure are the same, resulting in short notification time T_n independent of the LSP length. Also, since FMS uses unsolicited label distribution mode to setup the recovery LSP between the IOR and MP, the switch over time T_s is also greatly reduced. For all original LSP lengths considered, response time of FMS is significantly shorter than IBR. This can be attributed to FMS employing intermediate node recovery approach as opposed to IBR, which relies on the ingress to initiate and coordinate LSP modification signaling. Furthermore, IBR scheme uses conventional CR-LDP signaling to reestablish the recovery path starting over from the ingress, which increases the response time. Response time of FR is shorter than FMS because it employs pre-established recovery LSPs, enabling negligible switch-over time T_s as no path calculation is involved after recovery. However, the fast response time of FR comes at the cost of valuable bandwidth resources needed to establish and maintain a backup LSP for each LSP in the network, as will be presented in Section 4.3.

As the original LSP length increases, the position of the node of failure in the LSP can potentially be further away from the ingress, increasing the average notification time for FR. Hence, overall response time of FR increases with the increase in original LSP length. On the other hand, for a given density, response time of FMS is fairly constant. The switch-over under FMS happens when the notification packet is received by MP. This time period is independent of the original LSP length. Also, response times of FMS and IBR decrease with increasing node density. On the other hand, FR response time is fairly constant for different node densities because the response time under FR is mainly made up of the notification component T_n and is independent of the node density.

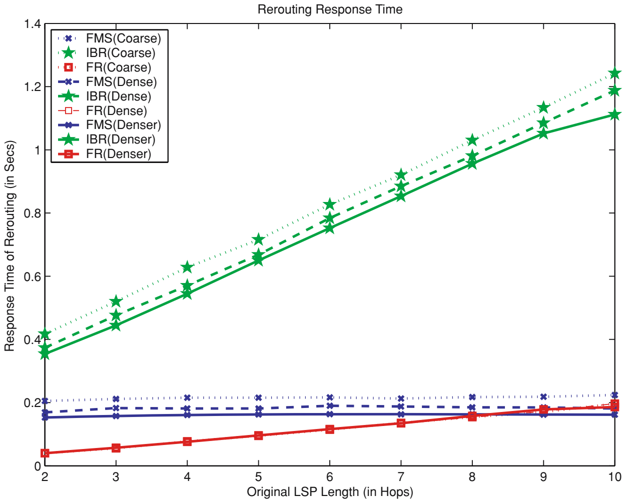

Fig. 10 Rerouting response time under different node densities

4.3 Protocol overhead

The total protocol overhead for the signaling is measured in this experiment for each rerouting technique for the three node densities. The overhead is expressed as the number of control packets exchanged during the entire signaling process. The total signaling overhead (O_s) is expressed as $O_s = O_n + O_{rs} + O_{rm} + O_{rl} + O_{rf}$, where

- O_n (Notification overhead): The overhead required to notify a particular node in the network regarding the failure.
- O_{rs} (Recovery LSP setup overhead): The overhead required to setup the new LSP.
- O_{rm} (Recovery LSP maintenance overhead): The overhead required to maintain the new LSP, if required.
- O_{rl} (Original LSP release overhead): The overhead required to release unused bandwidth on the old LSP.
- O_{rf} (Recovery LSP refresh overhead): The overhead required to refresh the new LSP.

The signaling overhead of all three schemes is depicted in Fig. 11. Signaling overhead of FMS is found to be extremely competitive of all three rerouting techniques. FMS has a very small notification overhead since the recovery is started by the immediate neighbor of the point of failure. The notification in FR and IBR is sent to the ingress node. Hence, the notification overhead is comparable between the two, but always larger than FMS. The IBR and FR LSP setup overhead is higher than FMS since the entire recovery LSP is signaled from source to destination and back. In FMS, the recovery LSP setup overhead is restricted to a portion of the LSP between IOR and MP. This explains the steeper rise in the IBR and FR overhead when compared to FMS. The path maintenance overhead O_{rm} is present only in the FR scheme and is mobility dependent. O_{rm} can be prohibitively high under high mobility conditions since the backup LSP is subject to multiple refreshes due to mobility before the main LSP warrants rerouting. The release overhead O_{rl} under FMS is limited to releasing bandwidth on portions common with the original LSP. O_{rl} for IBR consists of releasing the old LSP after setup of the new LSP. O_{rl} is again very large for FR due to multiple reroutes on the backup LSP, each associated with the requirement of bandwidth release. The refresh overhead O_{rf} for FMS is required to update parameters in the new LSP regarding the new route and bandwidth parameter. In the case of FR and IBR, the refresh takes place in the LSP setup phase itself. Hence, there is no additional refresh overhead component. When all overhead components are taken into consideration FR has the highest overhead, followed by IBR. Our proposed FMS technique has the lowest overhead as shown in Fig. 11.

Figure 12 shows the cumulative signaling overhead taken over the lifetime of an LSP of length 5 for different mobility rates (low-0.12 m/s, medium 0.23 m/s, high-1.04 m/s). The cumulative protocol overhead increases over the lifetime of the LSP because the number of rerouting events for the LSP increases over time. An increase in mobility rate increases the frequency of rerouting events. Hence, as the mobility rate increases, so does the total protocol overhead for all three schemes. Note that, in the case of FR, the average overhead of a single reroute event increases faster with the mobility since higher mobility rates increase refresh requirements on the backup LSPs. FMS has the lowest overhead performance along both mobility and LSP lifetime axes because of its low average overhead performance per reroute event.

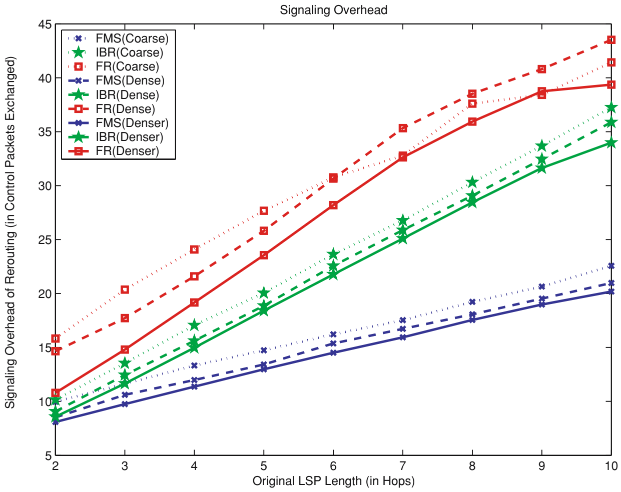

Fig. 11 Signaling overhead of rerouting

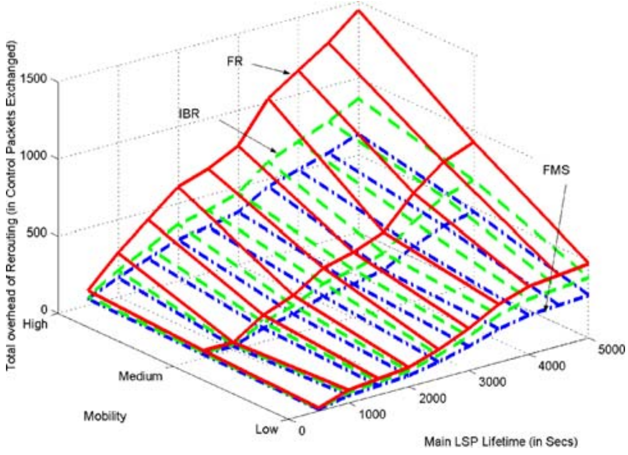

Fig. 12 Cumulative signaling overhead

4.4 Packets arriving out of sequence

During the recovery LSP establishment phase, there is a buildup of packets in the buffer of each of the intermediate routers and there are packets in transit in the failed segment of the original LSP. The objective of any good rerouting scheme would be to recover all such packets. Hence, following recovery LSP establishment, all such packets are diverted to the MP in case of FMS and to the ingress in case of IBR and FR from where they are redirected to the destination node via the new recovery LSP. Consequently, these recovered packets arrive at the destination, out of sequence. In this experiment we measure the extent of such packets and compare the three schemes again under the three specified densities.

The packets arriving out of sequence P_{os} is given by,

$$P_{os} = P_t + P_b$$

Where,

- P_t (Packets in transit): The number of packets in transit in the original LSP, during the recovery phase. P_t is calculated as the product of the response time and transmission data rate.
- P_b (Packets in buffer): The number of residual packets stored in buffers in the intermediate nodes of the failed segment of the original LSP. P_b is the sum of the average number of queued packets in each of the intermediate nodes. Packets stored in the buffers of all nodes between the point of diversion and point of failure are rerouted.

For the purpose of this experiment three loads were considered (light 200 Kbits/sec, Medium-5.5 Mbits/sec, Heavy-10 Mbits/sec). It is assumed that the packet lengths are distributed with a mean of 1000 bytes. M/M/1 queueing model [21] is used in the analysis to calculate the average number of packets in buffer.

The average number of packets in queue at each node N_Q is calculated as,

$$N_Q = p^2/(1 - p)$$

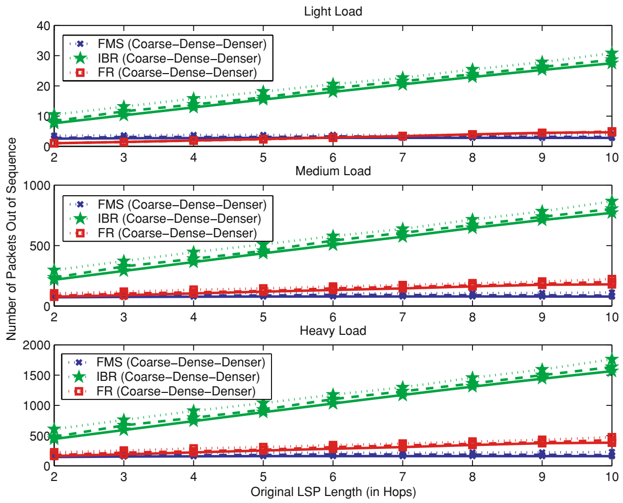

Fig. 13 Packets out of sequence

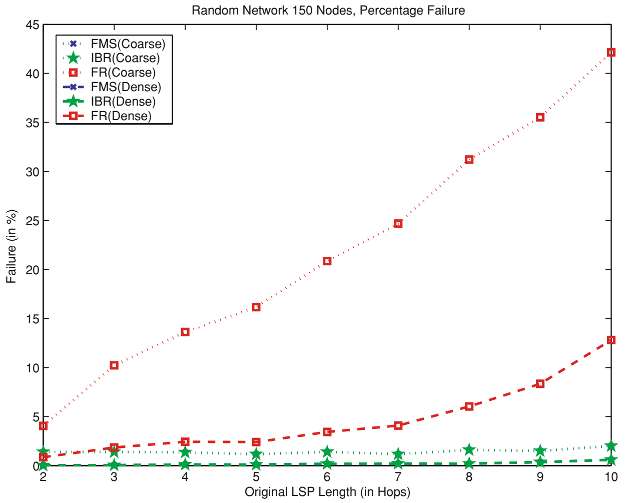

Fig. 14 Failure ratio

Where,

- *p* (Utilization factor of the queuing system): Utilization factor is a ratio of the arrival rate (lambda) and service rate (mu).

The transmission capacity is assumed to be 11 Mbits/sec.

Figure 13 shows the measured out of sequence packets, each subplot representing the metric for each of the three different loads. Within each subplot, the number of packets is plotted as a function of the original LSP length for the three schemes under the three densities. For the light load, the average buffer size is very small, hence the P_t component is negligible and the packets in transit (P_t) dominate the curve characteristics. For medium and high loads the P_b component is more pronounced. Since IBR has a very large response time it has the highest number of out of sequence packets for all three loads and all densities. FR has a low response time but for medium and high loads the overall P_{os} is greater than that for FMS. This can be attributed to the second component, namely P_b. Under medium and high loads the average buffer sizes are significantly large. Further in the case of FR and IBR, the number of nodes from which the residual packets are to be extracted are more. This is because the failure segment from which packets are to be redirected starts from the node of failure right up to the node downstream to the ingress. In FMS this segment starts from the node of failure to the node downstream to the MP. Thus the larger P_b component increases the P_{os} difference between IBR and FMS further, and also keeps the overall FR curve above FMS for medium and high loads.

Within each subplot the rise in the P_{os} curves with decreasing density is attributed to the increase in the response times due to larger recovery LSP lengths. Also between each subplot it can be observed that there is an increase in the corresponding P_{os} curves with the increase in load, for all schemes. Further, the spread between the various density lines for each scheme increases with the increasing load. This is because of larger buffer sizes and delays with increasing loads.

4.5 Failure in rerouting

In this experiment, the failure ratio of rerouting is measured. The failure ratio is defined as the ratio of the number of unsuccessful reroute attempts by the total number of rerouting attempts. Expressed Mathematically,

$$\mathcal{F} = \text{Rerouting failures / Total reroute attempts}$$

A failure in rerouting occurs when the rerouting path cannot be established because of unavailability of alternate paths between the target source and destination of the recovery LSP. FMS is said to fail when there is no alternate path between IOR and MP. Similarly IBR fails when there is no alternate path between the source and destination. FR failure is caused by the absence of an alternate disjoint path between the source and destination.

Figure 14 depicts the failure ratio for each of the three schemes under the three densities. The failure ratio of FR is the highest of all the three schemes. The failure ratio of FMS and IBR is identical and is much less than the FR failure ratio. The reason for FRs high failure ratio is due to the additional constraint that the alternate recovery path needs to be link disjoint to the original LSP. This constraint makes finding alternate paths more difficult. The IBR and FMS ratio is comparable for the case were there is a single failure per LSP. In such a case, a path available between IOR and MP implies the availability of a path between source and destination, and visa-versa. Hence, in Fig. 14 the failure ratio curves of IBR and FMS coincide with each other. Consequently the FMS curves cannot be seen in the figure. As the node densities

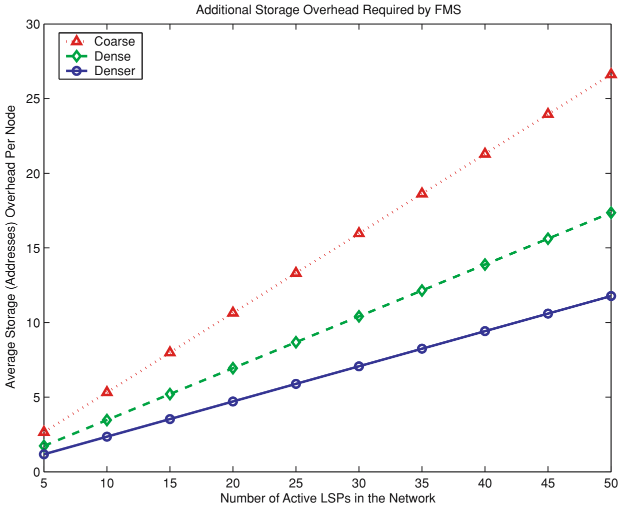

Fig. 15 Additional database requirements for FMS

decrease the failure ratio increases for all three cases. This is due to the general increase in the scarcity of alternate paths as the network becomes coarser. Note the steep increase in the failure ratio for the FR coarse curve, due to the low availability of alternate disjoint paths. It can also be observed that for a given density, while the FR curves show an increase in failure ratio with the increase in original LSP length, the FMS and IBR curves are fairly independent of the increase in original LSP length. This is because, in a single failure per LSP scenario, the ability to find a path between the IOR and MP under a local recovery technique is independent of the path length of the original LSP. Failure ratio for the denser node density was found to be very small and hence is excluded from the analysis.

4.6 Additional database requirements

The additional database storage requirements in the case of FMS stems from the requirement of storing the explicit route at each of the nodes that form part of an LSP. The storage demanded by FMS is a function of the number of active LSPs in the network and the length of each LSP. In this experiment we estimate the database storage requirements by randomly running 10,000 LSP setup/recovery operations for the 3 network configurations and estimating the average LSP length for each case. The database requirements are then plotted as a function of the active LSPs in the network as shown in Fig. 15.

In denser networks the average LSP length is shorter requiring less storage overhead. As the density decreases the LSP lengths increases, thus increasing the overhead to store the explicit route information on the intermediate mobile nodes. The overhead increases linearly with the increase in the number of active LSPs for all three network densities.

5 Performance analysis of FMS under different routing protocols

As mentioned previously, there is an interaction between the routing protocol and FMS as the recovery message travels hop-by-hop towards the MP. This indicates that the rerouting performance of FMS will depend on the underlying routing protocol. For example the rerouting time for FMS is tied to the routing protocol timing mechanisms such as timeout handling etc. The use of FMS is envisaged for mobile networks. In this section we investigate the performance of FMS rerouting under different ad-hoc routing protocols. For the purpose of this study, a traditional table driven routing protocol Distributed Bellman Ford (DBF) and two on-demand protocols Ad-hoc On demand Distance Vector routing (AODV) [22] and Dynamic Source Routing (DSR) [7] were selected.

A network size of 150 nodes in a 500 × 500 m area was used for the simulation. A radio propagation range of 90 m was used in the simulations. Mobility events were randomly injected into the simulation environment to generate link failures. The 802.11 [23] was used as the Medium Access Layer protocol (MAC). Constant Bit Rate (CBR) sources were used to generate traffic in the network. For each simulation run on random topologies, the same configuration was applied to different routing protocols and the desired timing measurements were made. The graphs in the following section reflect the average of 1000 independent runs with different random seeds.

5.1 Route acquisition times for different routing protocols

We measured the route acquisition times for the different protocols for different route lengths. This metric gives an indication of how efficiently a new route can be discovered in the network by the routing protocol. Different flows of various lengths were setup and the time for the route to be discovered was measured. For the on-demand protocols, in the absence of any previous route information, it is the time required for the Route Request (RREQ) to be sent and the Route Reply (RREP) with route information to be received. We time stamp the sending and reception of these messages to measure the difference to give the time required for route discovery. For the table based protocols it is the time required for the nodes to exchange table information and converge on the network topology. This time is measured by sending a continuous stream of packets and noting the time it takes for the first packet to arrive at the receiver node.

Route acquisition times are shown for different protocols in Fig. 16. Initial route acquisition is expected to be higher for table routing protocols, as the protocol, in its startup phase, takes time to exchange update messages and converge on the network state. For the same hop length, the DBF protocol takes more time to discover a route when compared to DSR.

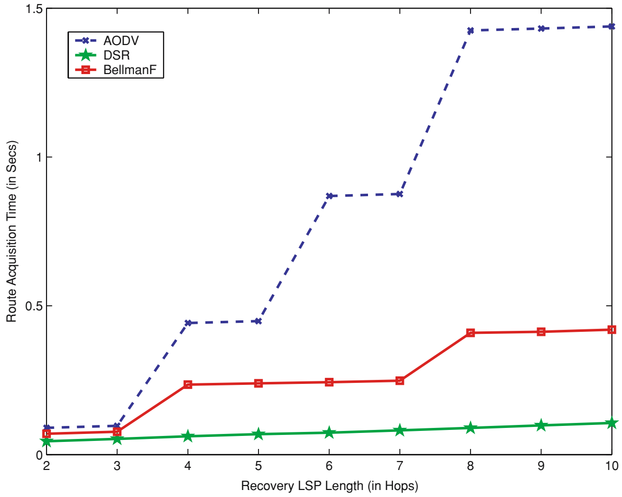

Fig. 16 Route acquisition time for different ad-hoc routing protocols

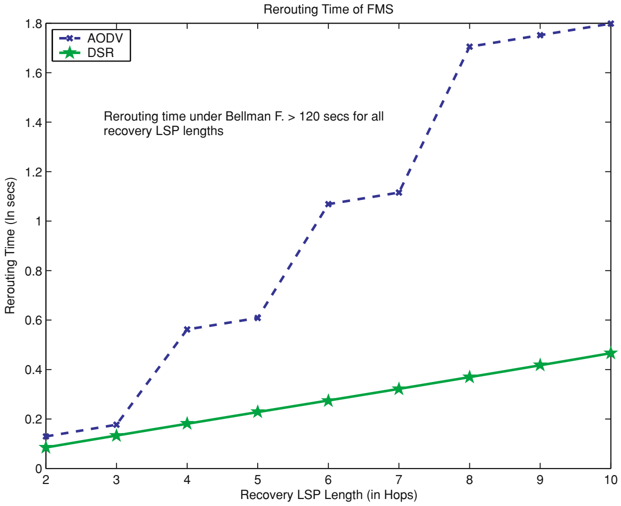

Fig. 17 FMS rerouting time under different ad-hoc routing protocols

However DBF route discovery is faster than the AODV route discovery because AODV uses a technique of expanded ring search for the purpose of reducing protocol message exchanges. In an expanding ring search, the originating node initially uses a TTL = TTL START in the RREQ packet IP header. If the RREQ times out without a corresponding RREP, the originator broadcasts the RREQ again with the TTL incremented by TTL INCREMENT which enables the RREQ to travel further. At each intermediate node receiving the RREQ message the TTL is decremented by one. An intermediate node will only re-broadcast the RREQ if the TTL in the IP header ≥1. In the simulations the default parameters for AODV were used, TTL START = 1 , TTL INCREMENT = 2. This explains the jump in the AODV curve as the recovery LSP length transitions from 3, 5 and 7. For these cases RREQ wasn't able to propagate to the destination at the first attempt and multiple retransmissions were necessary.

5.2 FMS rerouting time under different routing protocols

In the next experiment, we mimic the behavior of the FMS rerouting for various routing protocols and measure the time taken for rerouting subsequent to a mobility induced failure. For each flow created, mobility events are injected leading to link failures. The link failure is detected by the 802.11 MAC, which in turn informs the network layer. A packet is then initiated from IOR and the time it takes to reach the MP is noted for different routing protocols for varying lengths between IOR and MP. For DSR and AODV it is the time taken for a route to be discovered on demand between IOR and MP, followed by the time taken for the Recovery LSP Setup message (RLS) to reach the MP. As the DSR route acquisition is faster than the AODV route acquisition based on expanded ring search, FMS with DSR results in the lowest rerouting time as shown in Fig. 17. The DBF routing time is very high in the order of 120 secs for all recovery LSP lengths and hence excluded from the graph. The reason for such a large delay is because of the way DBF handles link failures. According to the DBF protocol functioning, when a node does not receive periodic update messages from its neighbors, it treats it as a link failure. However it initiates event based updates only after the periodic updates are not received for six consecutive times. This delay dominates the rerouting time and is the reason why the time is fairly constant for all lengths of recovery LSP. Based on the results obtained it can be concluded that the on-demand routing protocols DSR and AODV are more suitable for FMS from a rerouting time perspective.

5.3 FMS induced routing protocol control overhead

The following experiment measures the total routing protocol control packets which are induced by FMS during the rerouting phase. For the on-demand protocols AODV and DSR, the control packets at a node are the RREP and RREQ messages sent by that node for route discovery between the IOR and MP. The total control packets are the sum of the control packets at all nodes network-wide. For DBF, we measure the periodic and trigger based updates at each node. The total control packets is again the sum of the control packets of all the nodes.

Figure 18 shows the total control packets as a function of the recovery LSP length. AODV has a lower control packet overhead than DSR for lower recovery LSP lengths. This is because the AODV expanding ring search prevents the route discovery messages to propagate the entire network. After hop-length = 7 the expanding ring search mechanism is disabled (TTL THRESHOLD = 7 for the simulation). This explains the sudden increase in the control

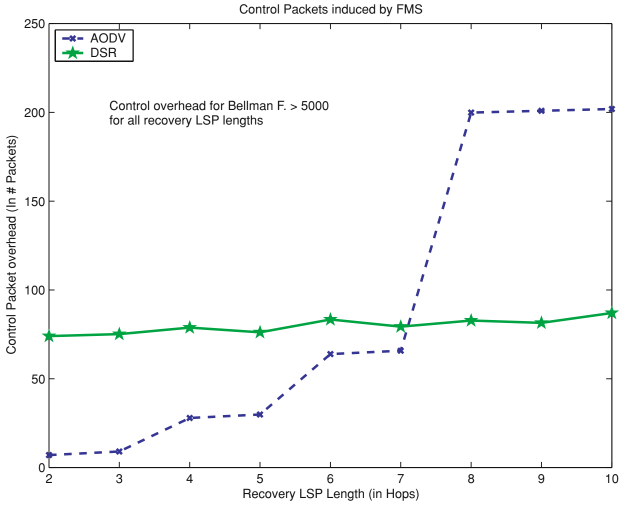

Fig. 18 FMS induced control packets for different ad-hoc routing protocols

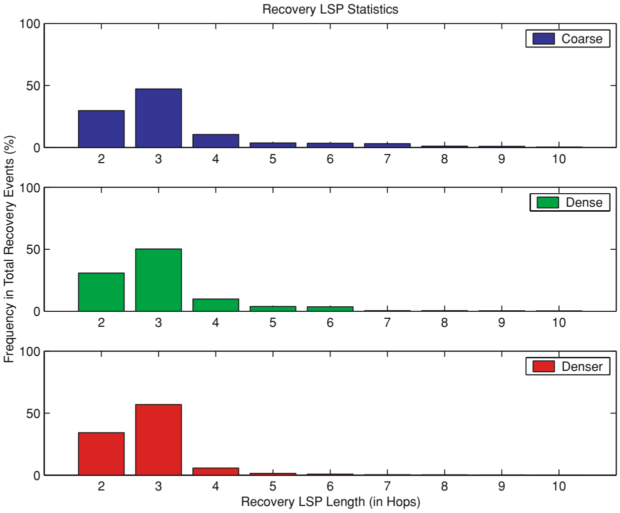

Fig. 19 Statistics from rerouting events

packets for recovery LSP lengths greater than 7. In DSR, the overhead is fairly constant over all recovery LSP lengths. This is because the flooding of the route discovery packet is controlled by a maximum search diameter, which is the maximum number of hops the RREQ message is allowed to propagate for route discovery. This prevents the route discovery messages to propagate network wide and keeps the control packets in check. The maximum search diameter was chosen to be 12 hops for these simulations. For DBF, periodic updates are exchanged at regular intervals. Additionally, triggered updates are propagated network wide. Hence for DBF control overhead is very large and is found to be greater than 5000 packets for all recovery LSP lengths.

6 Network statistics

In this section, we summarize relevant network statistics from the simulation study. While the previous section focused on comparing FMS with incumbent protocols and analyzing the performance of FMS under different routing protocols, this section aims to statistically measure the frequency of occurrence of network conditions that are best suited for the FMS protocol in a practical scenario. Under conditions where the recovery LSP length turn out to be small, or when DSR route caching can be utilized, the FMS rerouting performance is optimum.

6.1 FMS recovery LSP statistics

In this experiment we collect statistics on the length of the FMS recovery LSP (the recovery patch between IOR and MP). The objective is to estimate the frequency of recovery LSPs with smaller lengths. For this purpose, 1000 FMS rerouting events were gathered for random topologies for the three different densities and the length of the recovery LSP was noted for each event. The experiment was repeated 100 times to get an unbiased sample space and the average frequency of each recovery LSP length was plotted for each density as shown in Fig. 19. Recovery LSP lengths below 5 hops occurred with frequency 85% in the case of coarse and 95% in the case of the very dense networks. Results indicate that the FMS recovery LSPs with shorter lengths are in majority. Correlating this with the response time graph of Fig. 17, it can be concluded that the recovery LSP setup time will be in check for majority of the rerouting events.

6.2 DSR route cache statistics

Results on rerouting time and routing protocol control overhead suggest that DSR is a good protocol choice as the underlying routing layer for FMS. Additional advantages of FMS and DSR combination are described below. DSR is a route caching protocol. It can potentially store more than one route for any given source-destination pair, in case multiple alternate paths are available in the network for that pair. Once a route is discovered by an RREQ-RREP sequence the route is stored in the route cache database for a specific time period or till the route is active. The data path that is selected is the min delay path between source and destination determined by the first RREP that the source receives. However the source may receive subsequent RREP messages each carrying a different route to the destination. The source can also store such routes in the route cache. Partial route information is also stored in the intermediate nodes. If a destination route is already available in the route cache the route acquisition phase can be bypassed. From an FMS rerouting perspective

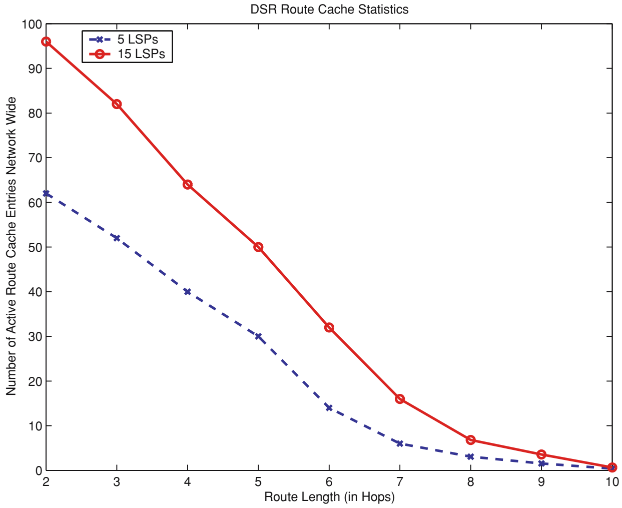

Fig. 20 Route cache statistics

there could be instances where the alternate route between the IOR and MP is already in the route cache of the IOR. For all such cases the rerouting time will be greatly minimized. Figure 20 shows the statistics of the active route cache entries in the network for the dense network under different active LSP loads of 15 and 5. As there are more active LSPs in the network, there will be more route requests and consequently greater path learning by nodes. Hence in the case where there are 15 active LSPs in the network the route cache entries are more than when there are only 5 active LSPs. Another notable pattern is that the number of route cache entries is higher for lower LSP lengths (2, 3 and 4 hops). This is because there is a higher awareness of nearby routes. DSR also employs passive listening to discover routes in the near vicinity. Hence the probability that FMS, with a high population of short length recovery LSPs , finds a route cache entry is higher as compared to IBR or FR with longer recovery LSP lengths.

Another advantage of using MPLS with DSR is to achieve greater efficiency in source routing. In MPLS, once the explicit route is established, the source route is encoded in the label itself. The source routes are only carried in the control packets during LSP setup and maintenance phases. Hence each data packet does not have to tag the entire source route with it as in conventional DSR or IP source routing.

7 Conclusion

In this paper, a novel rerouting technique (FMS) for MPLS based mobile networks is introduced. The proposed algorithm takes a reactive approach to LSP recovery and combines intermediate node rerouting with unsolicited label distribution to establish the recovery LSP. The performance of the proposed scheme has been evaluated and compared with two existing rerouting schemes, FR and IBR, via simulations. FMS has been found to be very effective in mobile environments with a low protocol overhead per rerouting event, compared to existing rerouting schemes. Additionally, the cumulative signaling overhead over the lifetime of an LSP under different mobility conditions was found to be significantly lower than that of existing recovery schemes. The response time is also low as traffic can be diverted onto recovery LSPs as soon as the signaling message reaches an intermediate node MP, rather than the ingress node. Additionally, LSPs rerouted via FMS were found to be close to the shortest paths available. Other parameters such as out of sequence packets were also measured. The out of sequence packets are found to be less in the case of FMS compared to IBR and FR. This is a significant parameter for real time applications were the ordering of the packets is crucial. The paper also investigates actual rerouting time of FMS under different ad-hoc routing protocols. It was found that the timeout mechanisms play an important role in the end-to-end rerouting time. Of all the routing protocols evaluated, FMS combines specifically well with DSR in what can be termed as a mutually symbiotic relationship. The end-to-end rerouting delay was found to be least in the case were FMS uses DSR as the underlying routing protocol. MPLS provides DSR with an efficient source routing mechanism, wherein the source route is encoded in the label itself. The DSR route caching mechanism can also be leveraged by FMS to further reduce the rerouting time. Network statistics collected from FMS rerouting events indicate that the recovery LSP shorter than 5 hops occur with a frequency of 85–95 percent for the densities studied. This is an important result and directly correlates to a lower average value of FMS rerouting time. The FMS rerouting scheme is geared towards effectively and efficiently addressing the problem of rerouting in dynamic network environments.

References

1. E. Rosen, A. Viswanathan and R. Callon, Multiprotocol label switching architecture, RFC 3031 (January 2001). [Online]. Available: http://www.ietf.org/rfc/rfc3031.txt
2. D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell and J. McManus, Requirements for traffic engineering over mpls, RFC 2702 (September 1999).
3. Internet protocol, RFC 793 (September 1981).
4. David E. McDysan and Darren L. Spohn, *ATM: Theory and Application*, 2nd edn. (McGraw-Hill, 1999).
5. Jeff T. Buckwalter, *Frame Relay: Technology and Practice*, 2nd edn. (Addison-Wesley, MA, 2000).
6. E.M. Royer and C.-K. Toh, A review of current routing protocols for ad hoc mobile wireless networks, IEEE Personal Communications (April 1999).
7. D.B. Johnson, D.A. Maltz and Y.-C. Hu, The dynamic source routing protocol for mobile ad hoc networks (dsr), Internet Draft (April 2003).
8. L. Andersson, P. Doolan, N. Feldman, A. Fredette and B. Thomas, Ldp specification, RFC 3036 (January 2001).

9. B. Jamoussi, L. Andersson, R. Callon, R. Dantu, L. Wu, P. Doolan, T. Worster, N. Feldman, A. Fredette, M. Girish, E. Gray, J. Heinanen, T. Kilty and A. Malis, Constraint-based lsp setup using ldp, RFC 3212 (January 2002).
10. D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan and G. Swallow, Rsvp-te: Extensions to rsvp for lsp tunnels, RFC 3209 (December 2001).
11. Mpls traffice engineering: A choice of signaling protocols, White Paper, Data Connection Ltd. (2000).
12. V. Sharma and F. Hellstrand, Framework for multi-protocol label switching (mpls)-based recovery, RFC 3469 (February [Online]). Available: http://www.faqs.org/rfcs/rfc3469.html
13. D. Haskin and R. Krishnan, A method for setting an alternative label switched paths to handle fast reroute, Internet Draft (November 2000).
14. C. Huang, V. Sharma, K. Owens and S. Makam, Building reliable mpls networks using a path protection mechanism, IEEE Communications Magazine (March 2002).
15. J. Ash, Y. Lee, P. Ashwood-Smith, B. Jamoussi, D. Fedyk, D. Skalecki and L. Li, Lsp modification using cr-ldp, RFC 3214. [Online]. Available: http://www.faqs.org/rfcs/rfc3214.html
16. S. Yoon, H. Lee, D. Choi, Y. Kim, G. Lee and M. Lee, An efficient recovery mechanism for mpls-based protection lsp, in: *IEEE ICATM: The 4th International Conference on ATM and High Speed Intelligent Internet* (2001).
17. C. Vijayanand, Fast reroute extensions to constraint based routed label distribution protocol, Internet draft. (2003) [Online]. Available: http://www.ietf.org/internet-drafts/draft-vijay-mpls-crldp-fastreroute-02.txt
18. U. Black, *MPLS and Label Switching Networks*, 2nd edn. (Pearson Education, Inc., Singapore, 2002).
19. L. Raju, S. Ganu, B. Anepu, I. Seskar and D. Raychaudhuri, Beacon assisted discovery protocol (bead) for self-organizing hierarchical wireless ad-hoc networks, in: *IEEE Global Telecommunication Conference (GLOBECOM 2004)*, Dallas, TX (2004).
20. T. Camp, J. Boleng and V. Davies, A survey of mobility models for ad hoc network research, Wireless Communications and Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, 2(5) (2002) 483–502.
21. D. Bertsekas and R. Gallager, *Data Networks*, 2nd edn. (Prentice Hall, Upper Saddle River, NJ, 1992) pp. 396–400.
22. C. Perkins, E. Belding-Royer and S. Das, Ad hoc on-demand distance vector (aodv) routing, RFC 3561 Experimental (July 2003).
23. B. Crow, I. Widjaja, J.G. Kim and P. Sakai, Ieee 802.11 wireless local area networks, IEEE Communications Magazine, 35 (1997) 116–126.

Ramprasad Nagarajan has received his B.E. degree in Electronics and Telecommunications from Pune University, India in 1999. He received his M.S. degree in Electrical and Computer Engineering from the Ohio State University, Columbus, OH in 2004. Currently, he is a Wireless Network Engineer in Nortel Networks, specializing in the area of network architecture and design of wireless packet core networks. Ramprasad's current research interests include the study of wireless network evolution trends, next generation wireless networks, network capacity planning, performance analysis, and optimization. He is a member of the IEEE.

Eylem Ekici has received his B.S. and M.S. degrees in Computer Engineering from Bogazici University, Istanbul, Turkey, in 1997 and 1998, respectively. He received his Ph.D. degree in Electrical and Computer Engineering from Georgia Institute of Technology, Atlanta, GA, in 2002. Currently, he is an assistant professor in the Department of Electrical and Computer Engineering of the Ohio State University, Columbus, OH. Dr. Ekici's current research interests include wireless sensor networks, vehicular communication systems, next generation wireless systems, and space-based networks, with a focus on routing and medium access control protocols, resource management, and analysis of network architectures and protocols. He also conducts research on interfacing of dissimilar networks.