Rope Ladder Routing: Position-Based Multipath Routing for Wireless Mesh Networks

Johannes Lessmann, Marcus Schoeller, Frank Zdarsky
NEC Laboratories Europe
Heidelberg, Germany
{lessmann, schoeller, zdarsky}@neclab.eu

Albert Banchs
Universidad Carlos III de Madrid
Madrid, Spain
banchs@it.uc3m.es

Abstract—**In this paper, we present a novel multipath structure called rope-ladder which combines the advantages of path, node and link protection schemes. We also propose a position-based multipath routing protocol in order to efficiently construct rope-ladders in wireless networks. By design, the paths which are constructed by our protocol are closely together which allows to quickly switch back and forth between them in cases of node or link failures. Hence, the size of loss gaps (i.e. the number of consecutively lost packets) can be minimized. Previous works mostly confine themselves to overall packet loss comparisons. However, the loss gap size is crucial to ensure high quality for gap-sensitive traffic like voice flows. Our multipath structure can also tolerate failures of multiple consecutive nodes on the primary path, and has a superior path diversity and path lifetime compared to even perfect braids. We evaluate the performance of our protocol using analysis and simulations[1].**

I. Introduction

The goal of multipath routing is to find not only one, but multiple paths from source to destination. This can have several benefits, like load balancing, fault tolerance (robustness), end-to-end delay speedup, congestion control, bandwidth splitting, security and throughput increase. Our proposition was designed to achieve an increase of resilience to node or link failures caused by equipment failures, signal propagation changes, or node mobility. The intention of our proposed multipath routing protocol is to construct backup paths which can be used when nodes or links on the primary path fail.

While many previous multipath routing protocols could be used to provide backup paths for primary path failures, our proposition is targeted at reducing packet loss. Especially in scenarios with real-time traffic and tight end-to-end delay requirements, it is often difficult to salvage packets which are already on their way when a link failure occurs. This becomes the more severe, the less connections exist between primary and backup paths. The extreme case is where two completely unconnected node-disjoint paths exist between source and destination. This is usually called path protection. The other extreme case is called link or node protection. Link protection means that there is a backup path between any two neighboring nodes of the primary path. With node protection, there is a backup path for any pair of two-hop neighbors on the primary path. A compromise is known as segment protection. Here, segments of the primary path are protected rather than all links or nodes individually. Clearly, more fine-grained protection comes at the expense of more signaling messages. Figure 1 shows the different protection schemes.

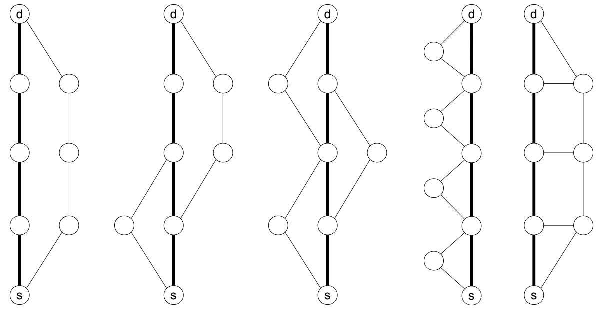

Fig. 1. Different protection schemes. a) path protection. b) segment protection. c) node protection. d) link protection. e) rope-ladder protection.

Imagine the last link towards the destination d fails. Using path protection, this failure must be propagated all the way back to the source s to tell it to direct new packets to the backup path. All packets sent in the meantime will likely be lost. For real-time traffic with small packet interarrival times the gap size (i.e. the number of consecutively lost packets) can become significant. Especially for voice traffic, not only the overall packet loss rate but also the gap size is a crucial factor for high-quality transmissions. Modern voice codecs' loss concealment algorithms cannot cope with more than two or three consecutive losses. Generally, the more connections there are between primary and backup path, the more immediately can packets be redirected to the backup path, avoiding losses or at least larger gaps.

In this paper, we propose a new protection scheme called *rope-ladder* (cf. Figure 1e)) which combines the advantages of link, node and path protection. Basically, a rope-ladder consists of primary and backup paths (the "*ropes*") and connections between them (the "*rungs*"). As with path protection, primary and backup path are node-disjoint. However, the rope-ladder structure ensures that each link and each node can be protected individually.

Note that Figure 1 shows idealized schematic versions of the different protection schemes. In practical networks, it might

[1] The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreements no. 224619 (ResumeNet) and 214994 (CARMEN).

978-1-4244-7265-9/10/$26.00 ©2010 IEEE

not always be feasible or desirable to construct such perfect multipath structures. However, for the sake of simplicity, we confine ourselves in this paper to the ideal versions. Yet our results apply to non-ideal variants as well.

In addition to introducing rope-ladders as a new multipath structure, in this paper we also propose a routing protocol to construct rope-ladders. We call this protocol Rope-Ladder Routing (RLR). RLR is position-based. This means that each node must know its position and also that of its one-hop neighbors. In general mesh networks, position information can be obtained using GPS, or a localization protocol. However, both options are costly (in terms of hardware or sigaling). The advantage of most carrier-grade mesh networks, where mesh nodes are stationary, is that coordinates can typically be hardcoded, avoiding these costs. Position-based routing protocols generally have the advantage that routing decisions can be made almost statelessly with only local knowledge. Section V will show that this is very favorable in terms of message complexity.

This paper is organized as follows. Section 2 discusses previous research in the domain of multipath QoS routing protocols and its relation to our proposition. Section 3 introduces rope-ladders and our proposed routing protocol to construct them in more detail. Section 4 presents the results of various simulations. Finally, Section 5 gives a short summary.

II. Related Work

There is quite a number of works in the domain of multipath routing protocols. An overview of this diverse field can be found in [1]. One of the most well-known multipath protocols is called AODVM [2]. It is based on AODV, but intermediate nodes send no RREP and do not discard any RREQ but rather record all RREQs in a RREQ table. The destination replies to all RREQs, intermediate nodes forward the RREPs to that neighbor in their RREQ table with the shortest path to the source. If a node overhears a RREP broadcast by a neighbor, that neighbor is deleted from its RREQ table. Hence, each node can be part of at most one route which is equivalent to node-disjointness. The individual paths do not know each other and cannot support direct switch-over in case of link failures.

Another established multipath protocol is called SMR (Split Multipath Routing) [3], which is based on DSR. Intermediate nodes do not maintain route caches, i.e. do not reply to RREQs to allow the destination to receive all routes, from which it selects the first one (shortest-delay route) and the one which is maximally disjoint from the first, i.e. with as few links or nodes in common as possible. As opposed to RLR, SMR aims for maximal disjointness. This is especially beneficial to protect against regional correlated failures of multiple nodes. However, it is a path protection scheme which is unfavorable in terms of loss gaps.

MP-DSR [5] is a DSR based QoS aware multipath protocol which aims at fault tolerance, like RLR. There, the destination sorts the RREQs according to a path reliability metric and selects a set of disjoint paths which together satisfy the reliability requirements and sends a RREP along each path back to the source. However, repair is only done end-to-end (intermediate nodes have no dedicated alternate path, thus even error propagation to the source can take long) which is very different to RLR. While the goal is also fault tolerance, the intention is more to choose stable links/paths right away instead of quick and loss-less repair.

A special variant of multipaths are called braided multipaths [6]. Instead of aiming at disjoint paths, in braided multipaths as few as one single node may differ between primary and alternate path. Generally, primary and alternate paths are more intertwined and alternate paths may accompany the primary path only for a small section of the complete route between source and destination. The most prominent benefit of braided multipaths is higher resilience to node failures compared to node-disjoint paths. Actually, braided multipaths are a variant of node or link protection schemes. The node protection scheme depicted in Figure 1c)) is exactly what [6] calls perfect braids. Despite the cited resilience of braids, we will show in this paper that the path diversity and path lifetime of rope-ladders are higher than perfect braids for a comparable number of involved nodes and links.

III. Rope-Ladder Routing

In this section, we describe how RLR constructs and maintains routes between a source and a destination node. First, we introduce the route discovery process. Then, we explain how routes are repaired in case of breakage.

A. Route Discovery

When a source s needs a route to a destination d, it sends a connect message to the neighbor n_1 which is closest to d in order to make it part of the primary route. The second closest neighbor n_2 is sent a message to become part of the backup route. Both messages contain a reference to the respective other node. When n_1 receives the message, it tries to find a route, namely the rung, to n_2 using DFS based geographic routing (in most cases, n_1 and n_2 will be neighbors anyway). In the following, we will call the current node on the primary path p, and the current node on the backup path b. Hence, in the current state, $p = n_1$ and $b = n_2$. We also say, that p is a *partner* of b and vice versa (since there will be a rung between them). In Figure 2a), p is node 3, b is node 2. Since p and b exchange messages to set up the rung between them, they are both aware of the current state of the route discovery process. Thus, the rung setup is a natural point of synchronization between the two paths. Note that, in Figure 2, the thick black lines mark the primary path, the thick gray lines mark the backup path, and the dashed lines represent rungs.

Each subsequent discovery step towards d works as follows. Node p sorts its neighbors according to their geographic proximity to the destination. It then selects the closest one as its forwarding candidate p_0 and informs node b about its choice. Node b tries to find a route to p_0 using DFS based geographic routing (in most cases, b and p_0 are either one- or two-hop neighbors). This route must be at least two hops long. This is because at least one hop will be part of the backup path, while at least one hop must be used for the rung. When no node-disjoint route at all can be found between b and p_0, there might be a *cut-off problem* (cf. node 9 in Figure 2c)). A cut-off problem occurs when the primary path is constructed in a way that it becomes an obstacle for the backup path. Consider Figure 2c). Since the primary path goes through nodes 3 and 10, it cuts off any remaining route leaving node 1 via node 2. This means that in Figure 2c), it is not possible to construct a node-disjoint backup path for the given primary path, although the whole example clearly shows that there exist two node-disjoint paths from s (node 1) to d (node 12) in the network.

In such cases, p_0 backtracks and p proceeds with a different forwarding candidate. If a route between b and p_0 was found which has at least two hops, p_0 becomes the new p and the i-th last node on the found route becomes the new b. We call this i-th last node the *contender* (in Figure 2e), $i = 1$ and the contender is node 14). Further, we refer to the previous p and b as $p*$ and $b*$, respectively (i.e. $p*$ is node 5, $b*$ is node 10 in Figure 2e)). The tricky part is how to determine i. Intuitively, the contender defined by i is the node on the rung candidate route which marks the splitting point between rung and rope. We apply the following strategy. Initially, $i := 1$ (i.e. p is node 7, and b is node 14 in Figure 2e)). With this, we proceed with the next forwarding step as described above. Only if it turns out, that no suitable path can be established with our contender, we backtrack and choose $i := 2$, and so on.

If we cannot find a suitable multipath no matter which intermediate node on our rung candidate route we choose, we have to backtrack completely to $p*$ which has to choose another forwarding candidate. By this algorithm, we have a deterministic and complete search order of all nodes in our graph. Hence, we can say that, if there exists a rope-ladder in the graph between s and d, RLR will find it.

However, complete exploration of the network in order to construct rope-ladders could lead to much backtracking. This raises the question whether it is worth the effort. In many cases, non-ideal rope-ladders (e.g. with some missing rungs) might be fully sufficient. To account for this, we introduce a *backtracking threshold* τ. Note that τ only refers to backtracking on the backup route. Backtracking on the primary route is not restricted. Whenever no suitable forwarding candidate (on the backup route) can be found at some node n, backtracking is done, albeit only at most τ times.

Since RLR makes use of depth-first search (DFS) based routing, it is straightforward to change our current metric which determines the order in which a node chooses its forwarding candidates. The way we described it above uses euclidean distance to the destination node d as a metric. However, other metrics like QoS-related metrics could be taken (in addition to this) as well. This would allow considering reliability or latency aspects in the rope-ladder construction, for example.

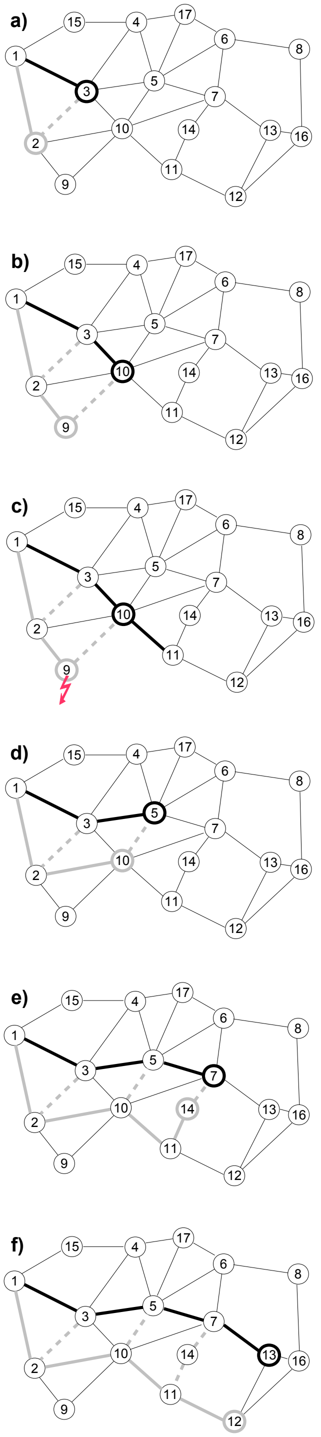

Fig. 2. RLR from node 1 to 12, highlighted nodes depict p and b.

B. Route Repair

When a link on either primary or backup path fails due to node failure, signal degradations or node mobility, the path in question must be repaired. Since we always have two paths which are close together, packets from the broken path can be immediately switched to the other path without loss. This generally gives us enough time to repair the broken path. Once the latter is repaired, packets can be sent along that path again. Generally, if one of the two paths breaks, it is repaired locally. That is, starting from the node which detects that its recipient is not responding, a new rope ladder is constructed towards the destination. For this, the same procedure as described in the previous Section is used. Since it is a geographic routing approach, the closer we get to the destination, the more likely it becomes that we can converge with the old rope ladder again. Normally, this is the case very soon, so repair overhead can be kept to a minimum. As soon as the repair process encounters a node of the old rope-ladder, it stops. As said above, during repair, the unbroken segments of the rope ladder can still be used. In most cases, repair can be done without loosing packets.

IV. Analytical Results

From the very design of the different protection schemes, we can immediately derive a number of properties. Table I gives an overview of how the different protection schemes from Figure 1 compare. While all schemes protect against single and multiple consecutive link failures, none except path protection (PP) and rope-ladder protection (RLP) protect against multiple consecutive node failures. Link protection (LP) does not even protect in case of single node failures. The third row shows the number of critical links on the backup path, i.e. the number of links which must not fail in case of a single primary link failure. Clearly, the higher this number, the less robust the protection scheme. The critical scheme here is PP, since the failure of any single primary link requires all backup links to be there, otherwise connectivity between s and d will be lost. The last row indicates the worst case number of hops which a link failure must be propagated back towards the source to allow a redirection of packets from the primary to the backup path. The higher this number, the higher the potential loss gap size. Again, PP and SP perform poorly, while NP, LP and RLP can switch to the backup path at any node.

An interesting property of any multipath routing protocol is the path diversity of the multipath. The path diversity can be intuitively understood as the number of distinct (not disjoint) paths which the multipath provides between source and destination. In node-disjoint cases with n node-disjoint paths, the path diversity is obviously n. More interesting are link-disjoint or, even more, braided multipath variants. Hence, we compare rope-ladders here only with perfect braids [6] (or NP) as the most challenging competitor. In the following, as in Table I, the value of n is defined as the number of intermediate nodes between source and destination along the primary route.

Theorem 1: The number of links $r(n)$ of a rope-ladder of length n is $r(n) = 2 \cdot (n+1) + n$.

Proof. By induction. It is apparent that $r(1) = 5 = 2\cdot(1+1)+1$. If $r(n) = 2\cdot(n+1)+n$ and we add one intermediate node (pair), we get two additional links (right and left rope) plus one new rung. Hence, $r(n+1) = r(n)+2+1 = 2\cdot(n+1)+n+2+1 = 2\cdot(n+1+1)+n+1 = 2\cdot((n+1)+1)+(n+1)$ which yields our assumption. ■

Theorem 2: The number of links $b(n)$ of a perfect braid of length n is $b(n) = 2 \cdot (n+1) + (n-1)$.

Proof. By induction. Again, it is apparent that $b(1) = 4 = 2\cdot(1+1)+0$. If $b(n) = 2\cdot(n+1)+(n-1)$ and we add one intermediate node (pair), we get two new backup links and one new primary link. Hence, $b(n+1) = b(n)+2+1 = 2\cdot(n+1)+(n-1)+2+1 = 2\cdot(n+1+1)+(n-1+1) = 2\cdot((n+1)+1)+((n+1)-1)$ which yields our assumption. ■

As a consequence, we can immediately gather that $r(n) - b(n) = 2\cdot(n+1)+n-(2\cdot(n+1)+(n-1)) = 2\cdot(n+1)+n-2\cdot(n+1)-(n-1) = n-n+1 = 1$, i.e. our rope-ladder has one link more than a perfect braid of the same length.

Theorem 3: The number of distinct paths $r_d(n)$ of a rope-ladder of length n is $r_d(n) = 2^{n+1}$.

Proof. By induction. For $n = 1$, we have 4 distinct paths, namely two which use only ropes, and two more which switch sides via the rung. Hence, $r_d(1) = 4 = 2^{1+1}$. If our assumption holds for n and we add one intermediate node (pair), we effectively double the number of distinct paths. This is because the new rung which is introduced provides an additional "switching point" where paths can change sides. Thus, at the new rung, paths can now continue along the rope or change sides. After this decision, they face as many combinations of links as for the previous case, i.e. for a rope-ladder of length n. Hence, $r_d(n+1) = 2\cdot r_d(n) = 2\cdot 2^{n+1} = 2^{(n+1)+1}$ which yields our assumption. ■

Theorem 4: The number of distinct paths $b_d(n)$ of a perfect braid of length n is $b_d(n) = F(n)$ where $F(n)$ is the n-th Fibonacci number.

Proof. By induction. For $n = 0$, there is no alternate path, which means $b_d(0) = 1$. For $n = 1$, we have 2 distinct paths. For $n = 2$, the number of distinct paths is apparently 3 (cf. Figure 1c)). Hence, $b_d(2) = 3 = 2+1 = b_d(1)+b_d(0)$. If our assumption holds for n and we add one intermediate node (pair), the number of distinct paths $b_d(n+1)$ increases as follows. If we start at the source, and take the primary link, we reach a node which we call s_r. The number of distinct paths from s_r to d is now exactly $b_d(n)$, as the structure between s_r and d is basically a perfect braid of length n. If we take the left link from the source to node s_l and from there the only subsequent link to node s'_l, the remaining number of distinct paths to d will be $b_d(n-1)$ as the structure between s'_l and d is nothing but a perfect braid of length $n-1$. Hence, $r(n+1) = r(n)+r(n-1) = F(n)+F(n-1) = F(n+1)$ which yields our assumption. ■

Based on these theorems, we can compare the path diversity of rope-ladders and perfect braids as follows:

$$\begin{aligned} b_d(n) = F(n) \overset{!}{=} \frac{\varphi^n - \frac{1}{-\varphi^n}}{\sqrt{5}} &\leq \frac{\varphi^n + \frac{1}{\varphi^n}}{\sqrt{5}} < \frac{\varphi^n + 1}{\sqrt{5}} \\ &\ll \frac{\varphi^n \cdot \varphi^2}{\sqrt{5}} < \frac{\varphi^n \cdot \varphi^2}{\varphi} \\ &= \varphi^{n+1} < 2^{n+1} = r_d(n) \end{aligned}$$

TABLE I
FEATURES OF PROTECTION SCHEMES

	PP	SP	NP	LP	RLP
single link failure	✓	✓	✓	✓	✓
multiple consecutive link failures	✓	✓	✓	✓	✓
# critical backup links, given primary link failure	n	$2/n$	2	2	2
single node failure	✓	✓	✓	–	✓
multiple consecutive node failures	✓	–	–	–	✓
worst case failure propagation hop count	n	0 - n	0	0	0

where $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.62$ is the golden ratio. As $b_d(n) \ll r_d(n)$ for large values of n, we can conclude that the path diversity of our rope-ladder is far higher than that of perfect braids even though rope-ladders use only one additional link. This means that, regarding message complexity, the construction of perfect braids and rope-ladders will be comparable, while rope-ladders outperform perfect braids with respect to path diversity. In Section V, we will show that this is actually reflected in terms of path lifetime, which is a very important metric for the robustness of a multipath. Thus, rope-ladders seem to be a superior multipath variant compared to perfect braids. Additionally, an increased path diversity can be beneficial for security issues, amongst others.

V. SIMULATION RESULTS

We simulated RLR using ShoX [7]. 100 nodes were distributed according to a random distribution across a field of 560×520 meters. For signal propagation, we assumed the Unit Disk Graph Model using transmission ranges of 100 meters. For MAC and PHY layer, the IEEE 802.11g standard was used.

To model link failures, we used node mobility models. This might seem surprising, as we are considering mesh networks with mostly stationary nodes. However, there are several advantages to this. First, the reason of a link failure (e.g. mobility, equipment failure, deteriorated radio wave propagation conditions) does not really matter for a routing protocol (unless quality degradations are measured and used for proactive re-routing, which we do not assume). Second, mobility-induced link failures are very dynamic and often lead to concurrent failures of multiple links, which is particularly challenging (hence, this allows to expose weaknesses and different performance of protocols under high stress more clearly). Third, using mobility models to simulate link failures in a mesh network allows us to evaluate at the same time, to what extent our protection scheme and routing protocol are applicable also to dynamic networks like MANETs. Fourth, there are many mobility models already available and, using standard ones, the implications of our measurements can be easily grasped by people familiar with them. Specifically, for mobility modeling, we used both the Random Waypoint Model (RWP) with a node speed between 1 and 1.8 m/s and the model introduced in [8] called OBM. Real-time traffic is modeled based on G.729 CBR traffic, i.e. 164 bit or approximately 21 bytes per packet payload.

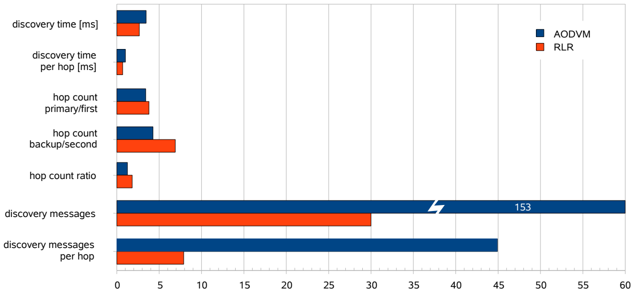

Fig. 3. Major results for RLR vs. AODVM in static networks.

Figure 3 shows a summary of some results for static scenarios, i.e. without any failures. This is to give an impression of the performance of our position-based RLR versus AODVM, which constructs node-disjoint paths. As can be seen, while the discovery time of RLR is only slightly smaller than AODVM, the discovery overhead in terms of signaling is much smaller for RLR. AODVM needs an average of 45 messages per hop of the final primary path, while RLR needs only 8. This is because of RLR's position-based discovery which uses dedicated unicast messages to only selected neighbors, while AODVM (and many other multipath protocols for that matter) is based on flooding. The lengths of the primary paths constructed by AODVM and RLR are comparable, but RLR generally produces longer backup paths. This can be explained, however, when taking into consideration, that rungs also count as backup sections in RLR, and AODVM does not have any connections between primary and backup paths.

Note that Figure 3 is based on RLR with a backtracking threshold $\tau = \infty$, i.e. unlimited backtracking. Hence, even when trying to find "optimal" rope-ladders in realistic mesh networks, the message complexity is low. Due to space limitations, we can unfortunately not present the detailed effect of τ on the message complexity. However, it is clear, that smaller values for τ lead to more incomplete rope-ladders, but also faster route discovery, i.e. less messages. Also note that, while many position-based routing protocols (like perimeter routing or face-based routing) might eventually fail to converge at the destination node in some cases, DFS-based routing with $\tau = \infty$ will always find the destination node due to exhaustive search in the worst case.

Since one of the main advantages we expect from rope-ladders are improved robustness and reduced packet loss gaps (i.e. number of *consecutively* lost packets), we simulated RLR

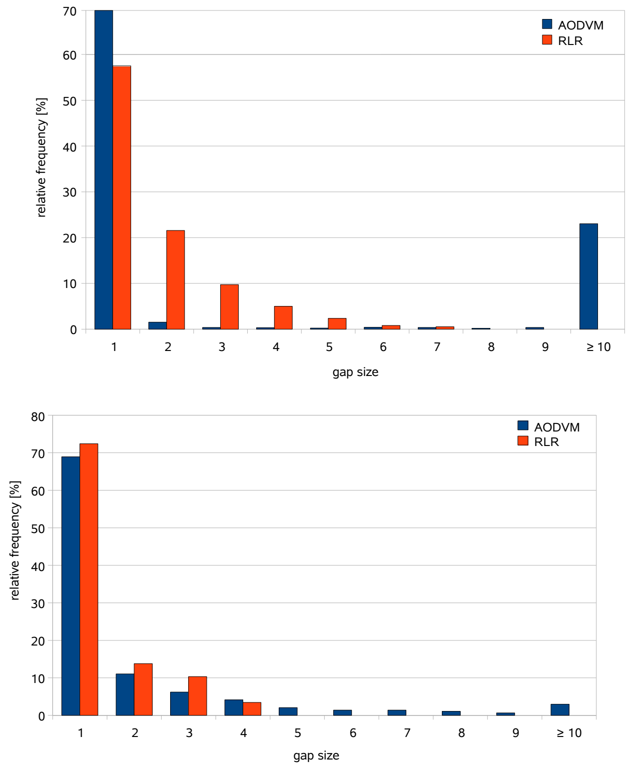

Fig. 4. Packet loss burst size histograms. (a) With OBM. (b) With RWP.

and AODVM using OBM and RWP over a simulated time of about 24 hours. Figure 4 clearly indicates that RLR produces significantly smaller loss gaps compared to AODVM. With OBM, which is more realistic, AODVM leads to loss gaps of more than 10 packets in more than 20% of the cases. Since this seems a significant number, we validated this result using RWP based node mobility. RWP is more commonly used in the literature, and it is known to lead to a concentration of nodes in the center of the deployment area over time. Hence, RWP should lead to less disruptions in the long run compared to OBM, since all nodes stay closer together on average. Even so, the loss gap comparison of Figure 4(b) exhibits the same qualitative behavior as with OBM, though less extreme. With RWP, RLR produces no gaps larger than 4 consecutive packets. AODVM leads to gaps of more than 5 consecutive packets in a combined 10% of all cases.

Finally, we measured the path lifetimes (time between construction and first disconnection of s and d) of rope-ladders using RWP with different pause times (0 means: node is constantly moving). In this case, we compare rope-ladders not only with AODVM based multipaths, but also with perfect braids (cf. Section II). We do this because perfect braids are advertised by their inventors to be particularly optimized for resilience towards node and link failures. Actually, perfect braids are a representation of the protection scheme NP. Looking at Table I, NP and thus perfect braids seem to be indeed the most competitive alternative to rope-ladders.

All three multipath protocols path lifetime markedly deteriorates with increasing mobility. In case of RLR and perfect braids, it approximately halves, in case of AODVM it decreases by a factor of 6. Hence, the first conclusion is that AODVM is more susceptible to node mobility variations than the other two. In terms of absolute lifetimes, RLR is clearly superior and performs in a league of its own. Compared to perfect braids, rope-ladders last about 1.5 times longer for low mobility and about 1.7 times longer for high mobility. Consequently, we can say that rope-ladders are a superior multipath structure compared to both perfect braids and the node-disjoint multipaths produced by AODVM, even though the latter easily produces 5 or 6 paths in one discovery.

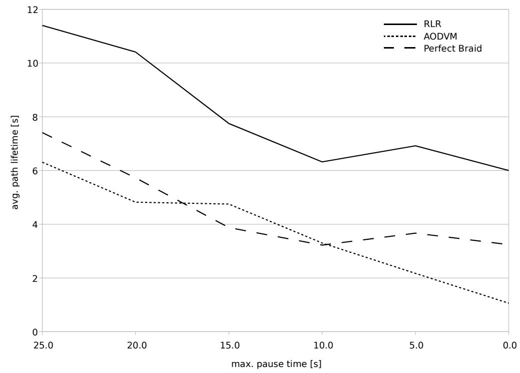

Fig. 5. Path lifetime of RLR (RLP), AODVM (PP) and Perfect Braids (NP) with different node mobility.

VI. Conclusion

In this paper, we presented rope-ladders as a new multipath protection scheme in wireless networks. Their architecture combines the advantages of path, node and link protection. Rope-ladders also have a much higher path diversity than perfect braids (node protection) while using only one additional link. They can be constructed using comparably few messages, and simulations show that they indeed reduce packet loss gaps significantly, which is essential especially for gap-sensitive traffic like voice streams. Their path lifetime is superior to existing path as well as node protection schemes.

References

[1] Mueller, S., Tsang, R.P., Ghosal, D.: Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges. Lecture Notes in Computer Science 2965, 209–234 (2004)

[2] Ye, Z., Krishnamurthy, S.V., Tripathi, S.K.: A Framework for Reliable Routing in Mobile Ad Hoc Networks. Proc. IEEE INFOCOM (2003)

[3] Lee, S., Gerla, M.: Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks. Proc. IEEE International Conference on Communications (ICC), 3201–3205 (2001)

[5] Leung, R., Liu, J., Poon, E., Chan, A., Li, B.: MP-DSR: A QoS-Aware Multi-Path Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks. Proc. 26th Annual IEEE Conference on Local Computer Networks, 132–141 (2001)

[6] Ganesan, D., Govindan, R., Shenker, S., Estrin, D.: Highly-Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks. Mobile Computing and Communications Review 4 (2001)

[7] ShoX, http://shox.sourceforge.net, accessed December 2009

[8] Lessmann, J., Lutters, S.: An Integrated Node Behavior Model for Office Scenarios. Proc. 41st Annual Simulation Symposium (2008)