Multipath Routing for Wireless Mesh Networks

Cristina Neves Fonseca
cristina.fonseca@ist.utl.pt

Instituto Superior Técnico
(Advisor: Professor Luís Rodrigues)

Abstract. This report addresses the problem of supporting applications with high bandwidth requirements in Wireless Mesh Networks (WMN). For this purpose, we use multipath routing, which has been widely studied. In this report we survey and discuss multipath routing protocols, and propose a new one that uses zone-disjoint links (to avoid interferences between multiple path transmissions). Our approach attempts to avoid the scenario where the choice of the primary path makes it impracticable to find another path that does not interfere with the first. Also, it makes the best to minimize the interference between transmissions from different source nodes.

1 Introduction

A Wireless Mesh Network (WMN) is formed by a set of gateways, mesh routers, and mesh clients. Gateways and mesh routers form the backbone of the network, where mobility is reduced. Mesh clients can be cell phones, laptops or other wireless devices. Routers communicate with the external network (e.g. the Internet) by forwarding each other's traffic (including clients traffic) towards the gateway nodes, which are directly connected to the wired infrastructure. In a WMN, each router, forwards packets on behalf of other nodes (that may not be within direct wireless transmission range of their destinations). Moreover, the gateway functionalities enable the integration of WMNs with various existing wireless networks such as Wi-Fi, cellular networks, WiMax, among others.

In this type of networks, the nodes automatically establish and maintain mesh connectivity among themselves (creating an ad hoc network). Therefore, a WMN is self-organized, self-configured and redundant (if one node fails, the other ones are still able to communicate). This brings many advantages, such as low up-front cost, easy network maintenance, robustness, resilient and reliable service coverage. Moreover, and comparing meshes with traditional ad hoc networks, routers in meshes are not limited in terms of resources, and thus can be exploited to perform more resource intensive functions.

WMNs are expected to improve significantly the performance and circumvent the limitations of many ad hoc networks, including wireless local area networks (WLANs), wireless personal area networks (WPANs), and wireless metropolitan area networks (WMANs). They are undergoing rapid progress and inspiring numerous deployments. WMNs will deliver wireless services in a large variety of scenarios of different scale, including personal, local, campus, and metropolitan areas. Mesh technology finds many applications in wireless multi-player gaming, campus connectivity, military communication, municipal networks, etc.

Given that these networks are usually multi-hop, in order to forward data to other nodes each node has to make routing decisions. Intuitively, routing algorithms designed for a WMN aim at choosing the path with the best links from each router to the gateways. All the traffic coming from mesh routers and mesh clients must be forwarded to mesh gateways. Consequently, certain nodes or links can be heavily loaded while some nodes/links can be seldom used. This may lead to an undesirable situation in which the best paths eventually degrade due to excessive load, consequently resulting in suboptimal performance. This scenario may be avoided if mutipath routing is used to balance traffic among multiple paths that may exist to reach the gateways. Multipath routing can also be used as a fault tolerance mechanism or to provide error resilience. The goal of our research is to analyze the existing solutions for multipath routing in Wireless Mesh Networks and explore the viability of exploring multiple paths to enhance throughput of high bandwidth requirement applications, by combining the bandwidth provided by multiple paths.

The rest of the report is organized as follows. Section 2 briefly summarizes the goals and expected results of our work. In Section 3 we present all the background related with our work. Section 4 describes the proposed architecture to be implemented and Section 5 describes how we plan to evaluate our results. Finally, Section 6 presents the schedule of future work and Section 7 concludes the report.

2 Goals

This work addresses the problem of providing high bandwidth transmissions in Wireless Mesh Networks. In particular, we are interested in supporting reliable applications, like video transmission or bulk file distribution.

> *Goals:* This work focuses on the designing of a new multipath routing protocol for Wireless Mesh Networks that operates efficiently under heavy traffic situations.

As it will become clear later in the text, our protocol will consider multiple paths that do not interfere with each other, minimizing interferences between transmissions of neighbouring nodes. In order to evaluate the proposed solution we will use the widely adopted NS-2 simulator. An extensive experimental evaluation of the protocol in different scenarios will be performed using this tool. In parallel with this work, a WMN test-bed is being developed [1], in which we plan to evaluate our work considering more realistic scenarios.

The project will produce the following expected results.

> *Expected results:* The work will produce i) a specification of the protocol; ii) an implementation for the NS-2 simulator and, iii) an extensive experimental evaluation using simulations.

3 Related Work

Although mesh networks are a relatively new subject, multipath routing is a concept that was introduced in 1984, when it was applied in the telecommunication industry [2]. Known as alternate path routing in traditional circuit switched telephone networks, the technique has been used to decrease the call blocking probability. In this scheme, the shortest path between two entities is used until it fails, after which calls are routed through another backup path. Multipath has also been used in ATM networks, specifically in the PNNI signaling protocol, during the reservation process to find multiple alternate paths. Other known protocols, such as OSPF [3] have proposed techniques using multipath, although with some restrictions (the paths must have equals cost) [4].

This section starts by addressing mesh networks characteristics and routing protocols. Then, we survey multipath routing including protocol operation, main multipath routing problems, evaluation of routing protocols and some examples.

3.1 Wireless Mesh Networks

Wireless Mesh Networks combine static mesh routers (mesh routers and gateways) operating in ad hoc mode with mobile wireless nodes (mesh clients). These networks are, for instance, appropriate to expand network connectivity in regions where access to an infra-structured network is limited. Gateways and mesh routers communicate with the external network (e.g. the Internet) by forwarding each other's traffic (including clients traffic) towards the gateway nodes, which are directly connected to the wired infrastructure. They form the backbone of the network, where mobility is reduced. Mesh clients can be cell phones, laptops or other wireless devices.

A mesh network can be characterized according to its architecture in one of the following types [5]:

- *Infrastructure or backbone mesh:* is formed by a set of mesh routers connected by self-configuring and self-healing wireless links. Some of the routers have gateway function, providing Internet connectivity for other routers, and consequently for clients that connect to them.
- *Client mesh:* is a pure mobile ad hoc network, since each mesh client (mobile clients) act as an independent router with no centralized routing control. Clients are able to perform network functionalities like routing and forwarding.
- *Hybrid mesh:* is the most generic and interesting type of architecture (and the focus of this work), as it combines both infrastructure and client mesh, as represented in Figure 1. While infrastructure provides connectivity to other networks such as Internet, clients provide a dynamic extension of the network.

Wireless Mesh Networks can be seen as a particular case of an ad hoc network, characterized by the following set of unique properties[6, 5]:

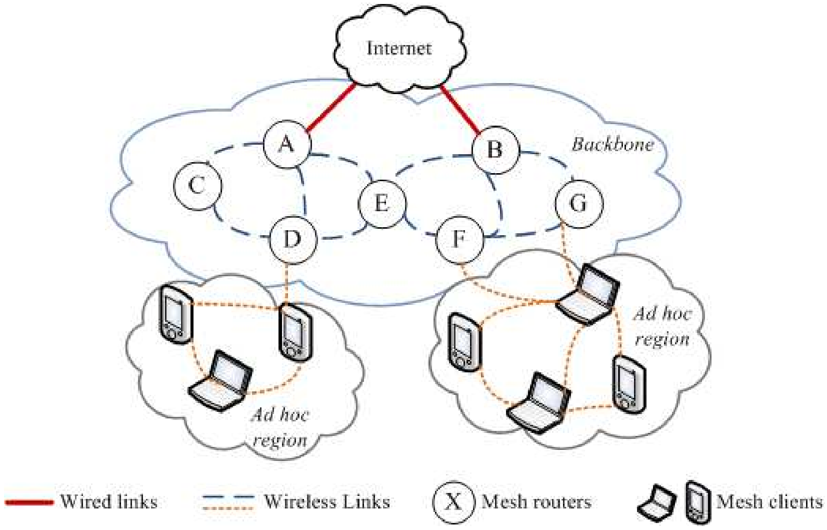


Fig. 1. Representation of a Hybrid Mesh Network.

Wireless Mesh Networks can be seen as a particular case of an ad hoc network, characterized by the following set of unique properties[6, 5]:

- Mesh routers are relatively static, so links used to support communication in the backbone are relatively static too.
- Mesh routers are not power constrained. Since mesh routers are typically connected to the electrical grid, mesh routing protocols do not have energy consumption restrictions.
- The traffic model is different and may concentrate in certain paths, predominantly between mesh routers and gateways. In other words, the backbone of the network, specially the zones near the gateways, are the ones where links are most used.
- The traffic volume and the number of users in a WMN can be high, as it aims to provide broadband connections for Internet access to large communities.

3.2 Routing in Wireless Mesh Networks

Routing protocols are used to find and maintain routes between source and destination nodes, in order to forward traffic. To perform well in Wireless Mesh Networks, a routing protocol must be tailored to deal with the characteristics enumerated before. More precisely, WMNs must consider:

- Transmission errors: the unreliability of the wireless medium may lead to transmission errors.
- Link and node failures: nodes and links may fail at any time due to different types of hazardous conditions in the environment.

– Incorrect routes: due to node/link failures or additions to the network, routes may become obsolete or based on an incorrect system state.
– Congested nodes or links: due to the topology of the network and the nature of the routing protocols, certain nodes or links may become congested, which will lead to higher delay or packet loss.

When considering route creation process, routing protocols can be classified in three main categories: proactive, reactive and hybrid, as described below.

Proactive Routing. Each node maintains a routing table, containing routes to all other nodes in the network. Thus, routes are computed and stored, even when they are not needed, incurring in a considerable overhead and bandwidth consumption due to the number of messages that have to be exchanged to keep routing information up-to-date. Proactive protocols may be impractical for large and dynamic networks.

Reactive Routing. Also called on-demand, reactive protocols only compute routes when they are needed. The process of finding a suitable route requires the transmission of route requests and the wait for replies with a path to the destination. Due to the delays incurred in this process, this approach is not suitable for operations that require immediate route availability.

Hybrid routing. Neither proactive nor reactive protocols provide an optimal solution for the hybrid WMNs we aim at addressing. Ad hoc regions, the ones formed by clients, have some mobility and thus reactive protocols are most suitable because route updates are frequent. On the other side, the backbone has reduced mobility, thus proactive routing allows to maintain routes with low overhead.

Hybrid approaches aim at providing an optimal solution by combining the best properties of both proactive and reactive protocols. Hybrid routing uses different routing protocols in different parts of the hybrid WMN: reactive protocols for ad hoc zones and proactive ones in the backbone.

3.3 Routing Protocols for Wireless Mesh Networks

In the next paragraphs we describe some relevant routing protocols used in wireless mesh networks. We start by giving a brief overview of OLSR, AODV, and DSR, given that many of the multipath routing protocols discussed in this report are an extension of one of these three protocols.

OLSR Optimized Link State Routing [7] is a proactive protocol designed for large and dense networks, where communication is assumed to occur frequently. OLSR uses two key concepts to compact the amount of control information sent in the messages and to reduce the number of retransmissions required to propagate them: multipoint relay and multipoint relay selectors.

The purpose of *multipoint relays* is to optimize the flooding of packets and reduce duplicate retransmissions in the same region. As represented in Figure 2, each node has various multipoint relays, selected among its one-hop neighbours in such a manner that the set covers all the nodes that are two hops away. For instance, the multipoint relays of node A are nodes B, C and D given that via one of these nodes A can reach all nodes that are two hops away from it (note that only relevant links are represented in the figure). Symmetrically, B, C and D will have A in its multipoint relay selector set.

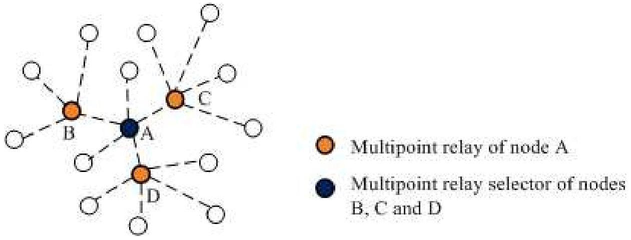

B
A
C
D
Multipoint relay of node A
Multipoint relay selector of nodes B, C and D

Fig. 2. Multipoint Relays and Multipoint Relay Selectors.

For a node to choose its multipoint relay selectors, it needs first to detect the set of neighbours with which it has a bidirectional link. This is done by broadcasting periodic HELLO messages, to all one hop neighbours. By receiving HELLO messages from an one-hop neighbour N, a node can record the following information about N: i) the status of the link to/from N; ii) a list of the two-hop neighbours that N gives access to. Based on this information, a node can choose its multipoint relay selectors. The selected nodes are listed in HELLO messages (so the multipoint relays know they have been selected). This information is refreshed when a change is detected in a one or two-hop neighbourhood.

OLSR maintains two tables to support its operation: the topology table and the routing table. The topology table is constructed with the information obtained from periodic TC (Topology Control) messages, sent by each node in the network. A TC message contains the list of nodes that have selected the source as a multipoint relay, so a node receiving this message has information of two-hop links, through the TC sender. Each entry in the table contains the address of a potential destination (a MPR selector received in the TC message) and the address of the last hop to that destination (the source of the TC message).

The routing table is the one used to forward traffic. Its construction is based on the topology table, by tracking the connected pairs in a descending order. For example, let S be the source and D the destination; consider that the route S to D is a 2-hop route via an intermediate node R; if a link (R,D) connecting R to D is already known, then one needs to search for a connected pair (S,R) in order to get a complete route from source to destination. Each node will select only the connected pairs on the minimal path, and create an entry in the routing table with the following information: the destination address, the next hop address, and the distance to destination.

AODV Ad hoc On-Demand Distance Vector [8] is a reactive protocol. Therefore it consists of two main phases: route discovery and route maintenance. Route discovery is the process to find a route between two nodes. It is initiated only when a node wants to communicate with another node and does not have the required routing information in its routing table. Route maintenance consists of repairing a broken route or finding a new one, and is initiated when a route failure occurs.

During the route discovery, two paths have to be considered, the forward path and the reverse path. According to the way protocols record these paths, we can consider two different approaches:

- Source routing: the list of hops traversed are stored in the messages directly. In source routing, more overhead is added to data packets, as the entire route must be specified in the packet header.
- Hop-by-hop routing: the reverse path is stored in a table (routing table) in the nodes along the path. In hop-by-hop routing, the header overhead is replaced by the need to maintain routing tables in the intermediate nodes, with forwarding information.

AODV is based on hop-by-hop routing, i.e., it maintains routing table entries at intermediate nodes, which means it uses hop-by-hop routing to forward traffic.

Route discovery. The source node broadcasts a route request packet (RREQ) to its neighbours, which is uniquely identified by the pair (source address, broadcast id). When a node receives a RREQ, it can act the following way:

- If the RREQ was already received, it is dropped;
- If the RREQ has not been received and the node does not have a path to the destination, the RREQ is re-broadcasted (with an increased hop count);
- If the RREQ has not been received and the node is the destination or has a route to the destination, a RREP (route reply) is sent to the source of RREQ.

When the RREQ is forwarded in the network, each intermediate node stores the previous hop, thus forming the route to the sender (i.e. the reverse path). Control messages have two additional control fields worth of notice, namely a destination sequence number and a source sequence number. Destination sequence numbers (also stored in RREP and routing tables) are used to maintain freshness information about routes; a larger sequence number indicates a more recent route. Source sequence numbers are used to maintain freshness information about the required reverse route to the source, specifying how fresh a route to the destination must be. A route is only accepted by the source if it has a sequence number greater or equal to the source sequence number contained in the RREQ packet.

Route Maintenance. Due to mobility or other factors, sometimes routes have to be reconstructed. If a node is detected to be unreachable by one of its neighbours, the node sends an unsolicited RREP with special characteristics that erases all the routes using the link along the way. This message is broadcasted until it reaches all the source nodes. If the route is still needed, a new RREQ is sent to build a new fresh route. Additionally, there are also other mechanisms used to manage routes, like timeouts to remove temporary or obsolete paths in routing tables.

DSR Dynamic Source Routing [9] is, like AODV, a reactive protocol. However, as the name implies, it is a source routing protocol: the full path is included in the packet header, and this information is used to forward traffic.

Route discovery. Is initiated by a route request packet (RREQ) containing the destination address. When an intermediate node receives a RREQ, it can act in one of the following ways:

- If it has already received the RREQ, or if the node is still in the route contained in the packet header, the RREQ is dropped (to prevent routing loops);
- If it has a route to the destination in its cache, it may append that route to the route record in the RREQ header and send a RREP (route reply) back to the source. Although this mechanism helps to reduce the overhead caused by the flood of RREQ, if the cache is out-of-date, it can provide a wrong route;
- Otherwise, it re-broadcasts the RREQ packet.

RREP packets can follow the reverse advertised route, or can be forwarded through another route, if the destination has another route to the source in its route cache (this allows DSR to operate when links are not bidirectional).

Route maintenance. When a link is detected to be broken, all routes containing the link must be removed from the route cache, and a route error packet (RERR) should be sent back to the source with an indication of the broken link. When a node receives a RERR, all the routes containing the broken link are deleted.

3.4 Multipath Routing

Most of the routing protocols that have been proposed for mesh and ad hoc networks are unipath, which means only a single route is used between a source and a destination node.

The main goal of multipath routing is to allow the use of several good paths to reach destinations, not just the best path. This should be achieved without imposing excessive control overhead in maintaining such paths. The availability of multiple paths between a source and a destination can be used to achieve the following benefits:

- *Fault tolerance:* introducing redundancy in the network [10] or providing backup routes to be used when there is a failure [11], are forms of introducing fault tolerance at the routing level in mesh networks. To this end, some techniques may be applied like packet salvaging [12, 13], which consists in modifying the route of a packet if the actual route is broken.
- *Throughput enhancement:* in a mesh network, some links can have limited bandwidth. Routing along a single path may not provide enough bandwidth for a connection. Therefore, using simultaneously multiple paths to route data can be a good approach to satisfy the bandwidth requirement of some applications. By increasing the throughput, a smaller end-to-end delay is achieved and quality of service is improved [14].
- *Load balancing:* as traffic distribution is not equal in all links in the network, spreading the traffic along multiple routes can alleviate congestion in some links and bottlenecks [15].
- *Error resilience:* multipath protocols can be used to provide error resilience by distributing traffic (for instance, using data and error correction codes) over multiple paths. In [16] a *M-for-N diversity coding scheme* is proposed, which consists of using M additional links to send traffic, coded in a way that the system can tolerate $M - 1$ simultaneous link failures at any time.
- *Security:* with single path routing protocols, it is easy for an adversary to launch routing attacks, but multipath offers attack resilience [17].

Proactive Multipath Routing Proactive multipath routing protocols have two operation phases: network setup and network maintenance.

- *Network Setup:* This phase consists of the steps required to build the routing table needed to forward traffic.
- *Network Maintenance:* This phase is executed when the routing table has already been created and consists of the steps required to maintain and repair the existing routes in face of topology changes.

Reactive Multipath Routing To the best of our knowledge, most of the multipath routing protocols are reactive. The operation of these protocols can be split in three components: route establishment, route maintenance, and traffic allocation. In the following paragraphs we discuss each of these components.

Route Establishment. Consists in finding multiple routes between a source and a destination node. This is performed by flooding a route request (RREQ) with unique sequence number. To limit the message cost, nodes drop a RREQ they have already received. New RREQs are re-broadcasted until they reach the destination that, in turn, will answer to the RREQ by sending one or more route replies (RREP). As the destination has collected information about multiple existing paths, it can apply one of the following criteria to choose the ones to use:

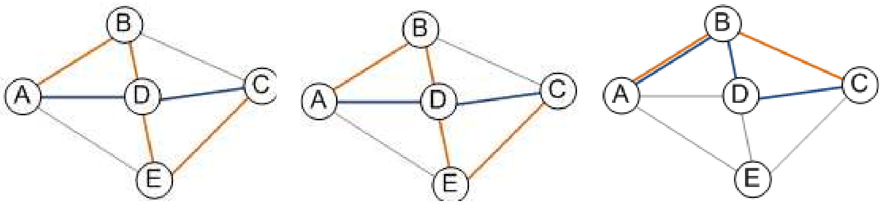
- *Minimum cost paths [18]:* are minimum cost paths amongst all available paths (shortest paths according to piggybacked information on the RREQ).
- *Non-disjoint paths [4]:* paths that can have nodes and links in common. Non-disjoint routes can be more easily discovered (as no restrictions are imposed, more disjoint routes may be discovered). Moreover, it was shown that a network becomes more reliable and better amortizes the cost of on-demand path discovery over many links, by exploiting rich mesh connectivity, in spite of using disjoint paths [2]. As the distance between nodes increases, the probability of finding node and link-disjoint routes decreases, so non-disjoint paths have to be used. But this scheme has also disadvantages: since we are considering wireless communication, it can be more difficult to choose routes that do not interfere with each other.
- *Link disjoint paths:* paths that have no links in common but may have nodes in common.
- *Node disjoint paths:* paths that have no nodes (and, consequently, no links) in common. In principle, node disjoint routes offer a better use of network resources, because neither links nor nodes are shared between two paths. For fault-tolerance, node disjoint routes offer the highest availability, because when using link disjoint routes, a failure of a node may cause the failure of several routes.
- *Zone-disjoint paths [19]:* paths are said to be zone-disjoint when data communication over one path does not interfere with other paths, meaning that route coupling [20] (interference) between the considered paths is zero.

When the paths have been selected, the corresponding RREPs have to be sent back to the source. For this purpose, the information about the reverse path has to be set up during the RREQ forwarding, using one of the schemes referred in Section 3.3: source routing or hop-by-hop routing. Note that multiple RREQ can reach the destination, and the destination can only reply to a subset of them, according to the criterion mentioned above.

As an optimization, if an intermediate node receives a RREQ and it has a route to the destination, it can send a RREP with the known route. However, in order to let the destination select disjoint or minimum cost paths, sometimes multipath routing protocols have to inhibit the reply to RREQ by intermediate nodes [4].

Route Maintenance. The purpose of route maintenance is to validate existing routes and find suitable replacements when one of the existing routes fail. There are multiple ways to maintain routes, from which we highlight two:

- *Periodic beacons (HELLO messages):* each node periodically transmits a HELLO message. If a node does not receive a HELLO from a neighbour after a certain amount of time, it assumes that the link connecting the node to the neighbour is broken and sends an error notification to the predecessor nodes affected by the failure. As HELLO messages consume bandwidth that could be better utilized for data traffic, this is not a desirable scheme.



(a) Node disjoint (b) Link disjoint (c) Non-disjoint

Fig. 3. Route establishment

- *MAC layer acknowledgements:* the procedure is almost the same, but no additional messages are sent. A node that does not receive an ACK for a data packet for a certain number of retries, assumes the link to the neighbour to be broken, and an error notification is sent.

If any of the previous mechanisms suggests that there is a route failure, in order to find a new route, route discovery process must be performed. In the specific case of multipath, route discovery can be triggered each time one of the routes fails or only when all the routes have failed. None of the schemes is best for all scenarios, as waiting for all the routes to fail before performing a route discovery would result in a delay before new routes are available, and initiating a route discovery every time a path fails may incur in excessive overhead. An alternative approach that can be a compromise between these two extreme options consists in initiating route discovery only when a threshold of n paths fail.

To prevent routes from being removed as a result of inactivity, route utilization becomes important, as on-demand routing protocols tend to drop routes if they have not been utilized for a certain amount of time.

Traffic Allocation Once the source node has selected a set of paths to the destination, it can begin to send data to the destination along these paths. To choose the way data is distributed among the existing paths, an allocation strategy is needed. There are two relevant aspects of an allocation strategy: granularity and scheduling. The granularity specifies the smallest unit of information allocated to each path [21]:

- *Per source-destination pair:* consists in using the same path to forward all traffic belonging to a certain pair of source and destination nodes.
- *Per-connection:* consists in allocating all traffic for the same connection to a single path.
- *Per-packet:* consists in distributing the packets from multiple connections among the existing paths.
- *Per-segment:* consists in splitting a packet into segments and forward each segment using a different path.

A finer granularity allows more efficient load balance, as it allows for a better control over the network resources. At the same time, granularity per-packet or per-segment requires reordering at the destination.

Paths obtained in the route discovery process can be scheduled using the following strategies:

- *Round robin:* in this strategy a node just sends each packet using a different path. In spite of being simple, this scheme suffers from setback due to the possibility of out of order delivery of packets belonging to the same flow. Out of order delivery leads to the maintenance of a large buffer by TCP and can lead to unnecessary loss. Nevertheless it can be used for effective load balancing because load will be uniformly distributed.
- *Congestion aware:* this scheduling scheme proposes to send traffic using non-congested links to avoid losses and additional delays. Congested routes can be measured, for example, by the average queue length and improving the performance significantly [6].
- *Backup path:* during the route discovery procedure, a source can establish a primary path as well as several backup paths to the desired destination. Multipath can be used to reduce the delay in recovering from a failure, thus using the backup paths to switch the on-going traffic to these alternative paths, instead of shooting down the end to end connection, when the primary path fails.
- *Unequal cost scheme:* proposes to distribute traffic based on a joint measurement of distance and link quality. The path with best metrics is selected according to a probability distribution (Boltzmann distribution used in [2]). This becomes the most used path, but sometimes other routes are selected to forward traffic. The advantage of this approach is that, as all routes are used, they are not removed from routing tables, which prevents route discovery procedures.
- *Concurrent delivery:* refers to sending traffic at the same time in more than one path. This scheme is used, for example, to enhance throughput [15].

3.5 Cross-layer Issues

Routing is just one of the needed functions for communication to take place between two nodes. Additionally, data link and transport functions are needed, among others. The way these other functions are implemented may affect the performance of a routing scheme. In this section we address some issues that multipath routing must consider.

Link Layer Issues The wireless medium is normally shared among all the nodes that are within radio range of each other. When a node wants to transmit and the channel is being used by another node, it has to wait until the medium is free (if they could hear the transmission) or, in the worst case, if it cannot hear the on-going transmission, it transmits blindly and may cause a collision (this is known as the hidden terminal problem).

The quality of transmissions within the same radio neighbourhood may degrade due to interferences, even if multiple channels are used. Nodes that affect each other by transmissions, are said to be in the same collision domain. This means that, even using multiple paths to route traffic, transmissions may interfere if they share the same collision domain. Therefore, the use of multipath routing to achieve higher bandwidth may not be as effective as it is in wired networks, as radio interference must be taken into account. Therefore, it is preferable to choose paths that are as independent as possible to avoid this interference [4].

This problem is known as the route-coupling problem [20]. The mutual interference of routes in a common wireless channel causes a dependence between a given flow and every other flow using the same radio region. The cost of maintaining low-coupled routes in an on-demand protocol is high [2].

Transport Layer Issues As we have seen, multipath routing can provide some robustness to link failures, and facilitate the transmission of packets along paths, avoiding congestion regions. As a consequence, we would expect that the network performance would be better in terms of achieved throughput, when multiple paths are used simultaneously. Unfortunately, this may not be the case, especially if we use TCP as transport protocol. In [22, 23] it has been shown that the use of multiple paths simultaneously degrades TCP performance.

In fact, although TCP is presently used for all networks, the optimizations for its operation were developed considering wired networks. Therefore, when operating over an unreliable radio medium, in face of external interference, multiple access contention and some mobility, its performance is not stable.

We can consider two main features of the TCP protocol that cause its poor performance in these scenarios:

- *RTT estimation problem:* TCP uses average Round Trip Time (RTT) to set a timeout and decide when packet loss occurs. When we have multiple paths, the RTT in the longest one can be much shorter than the average RTT (used for the estimation). As a result, TCP can prematurely timeout packets taking the longest path.
- *Out of order problem:* if multiple paths are used to forward traffic from the same connection, packets going through different paths may arrive at the destination out of order, which generates duplicate ACKs. TCP protocol reacts to this by reducing the congestion window, and consequently limiting the throughput, which is an action contrary to the one we are trying to achieve with multipath routing.

Another issue has been described in [23]: sometimes long TCP connections steal some bandwidth from short TCP connections (as bandwidth resources are shared between the nodes in an ad hoc network). It is commonly assumed that multipath routing is good to be used in long connections, in terms of hop count (not considering the higher volatility on this routes) where recovery using the default TCP mechanisms is longer than recovery from failures with multipath.

However, as proposed in [22], if multipath routing is used only as a way of providing backup routing it brings advantages, because using one path at a time reduces the probability of out of order packets. In the same paper, it was shown that two paths offer the best TCP performance, but they have to be chosen carefully in order to achieve good results.

It is also possible to use SCTP [24], whose multi-streaming function allows data to be partitioned into multiple streams that have the property of independent sequenced delivery, so that message loss in any stream will only initially affect delivery within that stream, minimizing TCP problems referred above.

3.6 Routing Metrics

The route establishment phase includes the choice of paths among all the available to forward traffic. If various paths are available we may want to choose a limited number: to use only the one with the best metric or to choose the n best ones. The path evaluation and selection according to certain metrics are discussed in this section. Hop count is a widely used metric since it allows quick path discovery in presence of mobility.

However, in WMNs, the stationary topology benefits from *quality-aware routing* metrics [25], because radio communication is often unpredictable.

Path reliability and link quality are performance metrics used by a considerable number of quality-aware routing schemes. We can define path reliability as the probability of having a successful data transmission between two mobile nodes within a certain amount of time [21]. This success is dependent of many factors, that have motivated the use of the following metrics that can be used to evaluate mesh routing protocols [26, 27]:

- *ETX (Expected Transmission Count)* is the expected number of transmissions a node needs to do to successfully transmit a packet to a neighbour. It is based on the delivery ratio of a number of packets, in a certain time interval.
- *ML (Minimum Loss)* refers to the route with the lowest end-to-end packet drop probability.
- *ETT (Expected Transmission Time)* considers link quality as a function of the time a data packet takes to be successfully transmitted to each neighbour.
- *mETX (modified ETX)* works at bit level, by computing the bit error probability. This metric aims to solve a problem related to fast link-quality variation in wireless networks (that makes ETX, ETT, among others less suitable). Metrics based on a time-window interval may not follow the link-quality variations or may produce excess in overhead.
- *ENT (Effective Number of Transmissions)* measures the number of successive retransmissions per link, considering the variance. It was also defined to consider link-quality variations.
- *iAWARE* estimates the average time the medium is busy because of transmissions from each interfering neighbour, considering aspects like medium instability, data-transmission time, and interferences.

- *WCETT (Weighted Cumulative ETT)* reflects the interference among links (inter-flow interference) that operate on the same channel. Reduction of the throughput is a reflection of the considered interference.
- *MIC (Metric of Interference and Channel-switching)* improves WCETT, considering not only inter-flow interference but also intra-flow. MIC consists of two principal components: the first one captures the potential for the path to interfere with other paths and the second one captures the potential for the path to interfere with itself.

Although there are so many metrics to evaluate these protocols, and some of them more complex and complete than others, most of routing protocols implementations prefer metrics with simpler designs such as ETX or ETT.

Considering multipath routing protocols, the following metrics are most suitable:

- *Degree of route coupling [28]:* defines the grade of interference between paths in multipath routing. In wireless transmissions, it is known that packet transmission may result in degraded quality of a simultaneous transmission on a neighbouring link. If two routes have nodes or links in common, they are highly coupled, but this effect may occur even if there are no shared nodes or links. Low coupling links are the best in terms of transmission quality, which means that disjointness between links must be achieved.
- *Path correlation [29]:* correlation factor describes the interference of traffic between two node-disjoint paths which is relevant when all the nodes use the same radio spectrum and compete for the radio channel. The total correlation factor of a set of multiple paths (we are considering multipath protocols) is defined as the sum of the correlation factor of each pair of paths. The lower the path correlation, the better.

Other approaches use combinations of some metrics, especially in QoS routing, where a subset of paths is selected only if the combined metric satisfies the QoS requirements.

3.7 Multipath Routing Protocols for Wireless Mesh Networks

In the next paragraphs we describe some significant routing protocols that use multipath.

MOLSR Multipath Optimized Link State Routing Protocol (MOLSR) [30] is a proactive protocol based on OLSR that aims to achieve lower delay and packet drop by using multipath routing. As seen in Section 3.3, OLSR uses multipoint relays and multipoint relay selectors to limit broadcasts. The operation of MOLSR is almost the same as OLSR, although the network setup phase has some differences. In this section we explain the differences between the two protocols.

OLSR maintains two tables: the topology table and the routing table. The topology table records the organization of the whole network, but does not store any link state parameter, so precise routing selection is hard to be made based on this table only. In MOLSR, SNR and Delay are added to the TC (Topology Control) message and these parameters, representing the link state between the MPR selector and the TC originator, are also stored in the topology table. The routing table is constructed based on the topology table and stores no more than two routes to every destination. These routes represent the best ones at that moment. A node can choose the best route to transmit data, but if it fails the other one can be used without route discovery.

The main differences between OLSR and MOLSR lie in the procedure to compute the routing table. In MOLSR, more than one route is calculated and two best routes are chosen according to the link metrics announced in TC messages. Routes with more than 2 nodes in common are not considered (node disjoint paths).

AODV-DM AODV-based Decoupled Multipath [31] proposes an algorithm that defines an insulate region around the primary path, to avoid interference between adjacent routes, trying to minimize the route coupling problem [20]. Moreover, it uses SCTP [24] instead of TCP because the latter is designed for single-path routing and cannot adapt to the network layer multipath structure and SCTP can independently control the traffic rate of each path.

Route establishment. The primary path is discovered in the following way: a RREQ is flooded to the entire network.

Each node upon receiving a message, stores the information about it in its routing table. Multiple RREQs may reach the destination, coming from different paths. The destination first responds to the request that has followed the shortest path (this is also called primary path), by sending a primary route reply (pRREP).

The packet follows the shortest path; intermediate nodes along the route broadcast the packet to neighbour nodes, which mark themselves as "in-region" nodes. When the pRREP reaches the source, the primary path formation is complete and an insulating region is established. To prevent future RREPs entering this region, neighbours outside the insulating region remove the "in-region" nodes from their table.

After waiting a period of time to allow the insulating region to be established, the destination responds to other RREQs. The response packet is called second route reply (sRREP) and the propagation process of this message is almost the same as the pRREP. The exception is that, a node receiving a broadcast sRREP does not mark itself as an "in-region" node. Intermediate nodes shall broadcast the packet to their neighbours in order to remove themselves from their neighbours' tables, as is represented in Figure 4. If an "in-region" node receives one of these packets, but has no available entry in its table to forward the packet, it sends a route reply rejection packet (RREJ), so the sRREP sender can try other entries in its table. This procedure is represented in Figure 4.

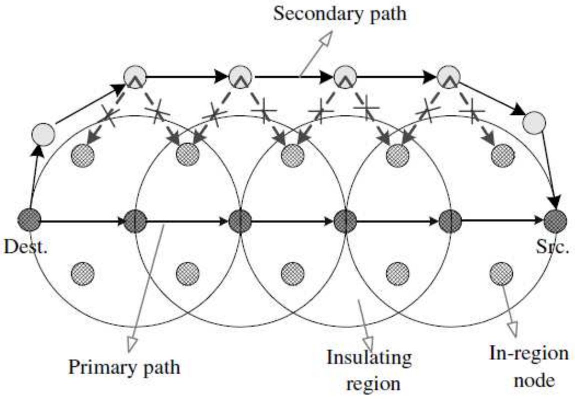


Fig. 4. AODV-DM illustration (extracted from [31]).

Route maintenance. Is done in the same way as in the base protocol, AODV.

Traffic distribution. The protocol may use a single path or multiple paths, when the available bandwidth between a source/destination pair in not enough. When multiple paths are used, traffic is distributed concurrently.

The decoupled features, and the use of path-aware SCTP scheme, make the protocol suitable for concurrent data transfer in dense networks, otherwise, the delay can compromise the efficiency of the protocol.

AODV-BR AODV-Backup Routing [11] proposes a backup route mechanism to improve the performance of existing on-demand protocols that discover routes through a query/reply procedure.

Route construction. Route construction is done almost in the same way as in AODV [8], but multiple paths are formed in the following way. When a node receives a RREP not directed to itself transmitted by a neighbour, it adds the neighbour as the next hop to the destination in its alternate route table (if it receives more than one it chooses the best). The resulting structure resembles a fishbone, as depicted in Figure 5. The primary path is used until a failure occurs.

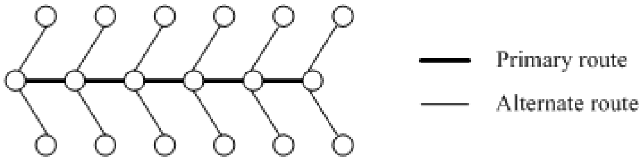


Fig. 5. Multiple routes forming a fish bone structure [31].

Route maintenance. Applies when a node detects a link failure. In this case, the node performs a one hop data broadcast to its intermediate neighbours, classifying the packet for alternate routing. Also, the node that detects the failure sends a route error (RERR) packet to the source to initiate a route rediscovery (in order to build a fresh and optimized path).

Traffic distribution. Only one path at a time (the primary path) is used. When it breaks, a backup route is used to forward traffic.

AODV-BR was shown to have improved throughput and protocol effectiveness, in mobile scenarios. Moreover, as the number of data sessions is increased, the protocol becomes less efficient due to collision and contention problems, so it does not perform well under heavy traffic.

AOMDV The Ad-hoc On-demand Multipath Distance Vector protocol [32] is a AODV-based protocol, proposed to reduce routing overhead when a route fails. It is able to discover multiple routes with a single route discovery procedure.

Route establishment. As in AODV [8], route discovery procedure is triggered when a node wants to communicate with a destination to which a path is not known. The route establishment procedure is the same as in the base protocol with the following change: to form multiple routes, all duplicates of the RREQ arriving at a node are examined (but not propagated), as each one defines an alternate route.

The protocol can find node-disjoint or link-disjoint routes. To find node-disjoint ones, intermediate nodes do not reject duplicate RREQs. To get link-disjoint routes, the destination replies to duplicate requests even if they have the same last hop. To ensure link-disjointness in the first hop of the RREP, the destination only replies to RREQs arriving via unique neighbours. After the first hop, the RREPs follow the reverse paths, which are node-disjoint and thus link-disjoint.

Route maintenance. To preserve connectivity information, each node executing AOMDV can use link-layer feedback or periodic HELLO messages to detect broken links to nodes that it considers as its immediate neighbours. As in AODV, in case a broken link is detected, a RERR message is sent to the active neighbours that were using that particular route.

Traffic distribution. With multiple redundant paths available, the protocol switches routes to a different path when the path in use fails. Thus a new route discovery is avoided. Route discovery is initiated only when all paths to a specific destination fail. For efficiency, only link disjoint paths are computed so that the paths fail independently of each other.

MP-DSR The MP-DSR is a DSR-based protocol that addresses path reliability requirements. MP-DSR [14] first collects application path reliability requirements. Then it determines the number of paths needed and the lowest path reliability requirement each path must provide.

Route establishment. The source sends RREQ messages, containing information regarding the requirements, to the destination node via its immediate neighbours. The RREQ message also contains the traversed path (as this is a source routing protocol), and the accumulated path reliability. The intermediate nodes use the information included on the RREQ message to check if reliability requirements are still satisfied. If so, the node updates the accumulated path reliability based on the availability of the link just traversed, and re-broadcasts the message to its neighbours. Otherwise, the RREQ message is dropped. The destination waits until it receives all the RREQ packets, sorting them according to the path reliabilities. Then, a set of disjoint paths are selected according to the reliability required. A RREP is sent to the source, via each selected path.

Route maintenance. The route maintenance procedure differs for each of the following scenarios: when all routes fail or when one of the used paths fails. If all routes fail, the route establishment process is simply re-initiated. If only one route fails, the source sends a route check messages along the paths to collect the path reliabilities. The destination replies to the route check messages. The source collects all the replies, and checks to see if the paths still meet the reliability requirement. If not, route discovery is performed. MP-DSR collects QoS characteristics using local information available at intermediate nodes, which means global knowledge is not required.

Traffic distribution. Traffic is sent along more than one path if multiple paths are required to meet QoS requirements.

SMR Split routing [15] is protocol similar to DSR, and is used to construct maximally disjoint paths, to be used concurrently.

Route establishment. The RREQ is flooded in order to find routes. Intermediate nodes forward RREQ without replying, even if they have routes to the destination (this is to allow the destination to select disjoint paths). Intermediate nodes do not need to discard duplicate RREQs. Instead, they forward RREQs that are received through a different incoming link, and whose hop count is no larger than the previously received RREQs. The proposed algorithm selects two routes, but it can be easily extended to return more routes. The selection procedure is done the following way. The destination node replies to the first RREQ, which represents the shortest path. Then, it waits to receive more RREQs and selects the path that is maximally disjoint from the shortest delay path. If more than one exists, the shorter is selected. Then, a RREP for the selected path is sent.

Route maintenance. When a link is detected to be failed, a RERR packet is sent to notify nodes using the link that is broken. They can then delete the entry from their routing tables. When there is a failure, a new route discovery procedure may be triggered, or this can be done only when both routes of the session are broken.

Traffic distribution. The protocol considers splitting the traffic into two available routes, using a simple per-packet allocation scheme.

MMESH MMESH protocol [6] is essentially a proactive routing protocol for wireless meshes to balances the traffic load uniformly over multiple paths.

Network Setup. In the initial setup phase, nodes discover routes to gateways by hearing advertise messages of Internet connectivity. Based on performance metrics that are included in these advertisements, mesh routers select the routes that are acceptable to them and add them to the routing table. Then, each node notifies the mesh router that has announced the route about the chosen routes. Mesh routers update the routes to forward traffic to and from the child mesh router, and notify other routers along the route, including the gateway. To limit the amount of possible paths to reach a node, each router can only announce its n best disjoint path routes (where n represents a tradeoff between load balancing capacities and complexity in route finding). To avoid additional overhead, when routing tables are already established, each route is labeled and is assigned a sequence number to identify its freshness.

Network Maintenance. As WMNs are not static, when new mesh routers join the network or paths degrade to a level that they cannot be used to forward packets, network maintenance is needed. Each router continuously monitors the performance of paths to the gateway and propagates this information to the neighbouring nodes. By analysing changes in the observed performance, new routes can be found or existing ones suspended. If new routes are found, routers update the routing table and propagate these changes to their neighbours. In order to adapt the algorithm to the changes that can occur in the network (mobility even if reduced, new mesh routers, reboot), if one node fails and one of its neighbours detects the failure, it suspends the routes that include the node. It then forwards the traffic through another node. This mechanism makes the protocol more stable, by only removing routes when a timeout occurs.

MMESH applies a congestion aware approach by using link metrics and variance to select the best path to forward traffic. If the product of variance by the metric of the best path is no less than the metric of the selected path, the packet is sent through the selected path. Otherwise, the route is temporarily suspended and a different path is selected to send the packet.

MHRP MHRP [17] is a hybrid routing protocol for wireless mesh networks, where multipath is used as a backup mechanism. It combines proactive and reactive approaches, and makes use of the four following sub-protocols, each one used in a different zone, as depicted in Figure 6:

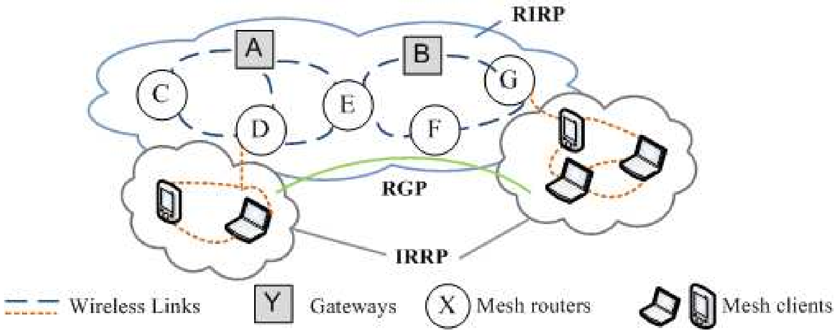


Fig. 6. Protocol architecture of MHRP.

- *Router Infrastructure Routing Protocol (RIRP):* as the routes in the infrastructure mesh are relatively static, this is a proactive based protocol. To keep the routing table fresh and accurate, periodic HELLO packets are sent by each router to its neighbour routers at a constant interval. Each node maintains all the possible paths to the other nodes and uses the best one to communicate.
- *Intra-region Protocol (IRRP):* since it is used in the ad hoc region, it is reactive, based on AODV, and uses forward selection to find an alternate route when link is down. Multiple reverse paths are created when a RREQ flows in the network. These paths are stored for future use, decreasing the latency of finding a new route.
- *Region Gateway Routing Protocol (RGP):* is used when routes between two ad-hoc regions are required. The protocol is based on the information provided by RIRP and IRRP. When a node requires a route, it sends a route request to the router responsible for its ad hoc region (who runs the RGP protocol). The router gets the information of the destination node from other protocols and constructs the available multiple routes, sending them to the source node. As messages pass to and from clients to routers, routing tables are updated.
- *Route maintenance Protocol:* maintains the routing table and provides alternate routes whenever required.

The route discovery mechanism, performed when a node wants to communicate with another and does not have a route to it, can be divided in three stages. The first one is the route request, during which a request is sent to the neighbours of the client, using IRRP. They forward the request if they do not know the route to the destination. During route formation, after de destinations have been found, routes are formed even if the destination node is in another ad hoc region and the operation of RGP is needed. The last phase is the route reply in which a message containing the whole route is sent back to the source. One node-disjoint path is used at a time.

3.8 Discussion and Comparison

Table 1 summarizes the routing protocols presented.

Table 1. Summary of the protocols presented.

Protocol	MOLSR	AODV-DM	AODV-BR	AOMDV	DSR-MP	SMR	MMESH	MHRP
Base protocol	OLSR	AODV	AODV	AODV	DSR	DSR	-	-
Motivation	Lower delay and packet loss	Deal with high bandwidth requirements	Improve on-demand protocols	Reduce routing overhead	Deal with reliability requirements	Use network resources efficiently	Balance the traffic load	Security in mesh networks
Proposed function	Backup routing	Avoid route-coupling	Backup routing	Backup routing	Reliability	Throughput enhancement	Congestion avoidance / backup routing	Backup routing
Source or hop-by-hop	Source	Hop-by-hop	Hop-by-hop	Hop-by-hop	Source	Source	Source	
Proactive, reactive or hybrid	Proactive	Reactive	Reactive	Reactive	Reactive	Reactive	Proactive	Hybrid
Traffic distribution	Single path	/ Single path	Single path	Single path			Single path	Single path
Route rediscovery	-	-	-	When all/one path fails	When all/one path fails	When all/one path fails	-	-
Route relations	Node-disjoint	Node-disjoint	Non-disjoint/Best path	Link/node-disjoint	-	Disjoint paths	n best disjoint paths	Node-disjoint

Comparing multipath routing protocols with unipath routing protocols, first we can observe that they add complexity and additional overhead. Also, the maintenance of routing tables in intermediate nodes results in larger routing tables. In routing there is also an additional phase needed in the protocols, which is traffic allocation, resulting in more time needed to establish routes.

Based on the survey presented, we consider that a well designed routing protocol should address the following aspects:

- *Multiple paths:* in a limited number, multiple paths should be used in order to establish a balance between the number of used paths and negative aspects like interferences or overhead.
- *Low overhead:* as we referred previously, one of the goals of routing is to discover and use multiple paths, thus benefiting from this, but with lower additional overhead.
- *Good performance:* when multiple paths are used there are more routes and state to maintain. Sending traffic over the paths in function of its quality is a way of maintaining paths alive [2]. Having mechanisms to manage routing tables avoiding unnecessary information is also needed to achieve a well designed protocol.
- *Low degree of route coupling:* as in wireless medium interferences among different channels are a conditional factor in transmissions, in an optimal protocol, these interferences must be minimized.

4 Architecture

As discussed in the previous section, multipath routing protocols are typically based on existing protocols for ad hoc networks, mainly reactive ones. However, the delay of finding a route in a reactive protocol may not be acceptable in the mesh backbone, where communication occurs frequently. So, for the mesh backbone, proactive protocols are most suitable. Although there are some multipath proactive protocols used in wireless mesh networks (OLSR and MMESH, for example), they use one path at a time (multiple paths are used as a backup mechanism).

The problem addressed in this report is to design a proactive routing protocol that performs well in networks where applications have high bandwidth requirements (as video transmission or bulk file distribution, for example). Given that in mesh networks multiple links between a source node and a destination can be found, and sometimes a single one cannot offer enough bandwidth for a certain application, more than one link can be used to satisfy high bandwidth requirements.

As we are considering sending traffic simultaneously in two alternative paths, we have to consider the following problems:

- Route Coupling Problem: as the wireless medium is shared among all the users in the network, if we are using two paths at the same time, we have to avoid that they interfere with each other. So, paths must have low degree of route coupling. AODV-DM can define insulating regions but has to perform two RREQ-RREP cycles, which adds overhead and delay in finding routes. We propose to define such regions within the normal route finding procedure.
- Optimal number of alternate paths: another issue is to determine the number of optimal routes to use at the same time (assuming that a great amount exists), and how to use them to maximize its occupation. As the topologies of the network we are considering can be very different: networks can be dense

or sparse with more or less nodes, the number of alternate paths with zone disjoint links may vary a lot, depending on the network topology. Sometimes, by choosing a path, we may invalidate the choice of any other path in the network (if all the other possible paths interfere with the first one). So we also propose to optimize path choice in such situations.
- Transport Protocol Problem: reliable transmission requires a reliable transport protocol. In spite of being designed to operate in wired networks, TCP is still the main transport protocol and is widely used. As we have discussed previously, when multipath is used, packets can be incorrectly considered to be lost or they may arrive out of order (which requires TCP to use long buffers). Instead of improving throughput, this protocol may reduce it, which is not desirable. TCP problems come from the fact that this protocol cannot distinguish two different flows, as SCTP (which we plan to use) does.

The main challenge of our proposal is related with the coexistence of multiple transmissions simultaneously between different source/destination pairs, which can lead to undesirable interferences between transmissions from different nodes. In particular, the following problem has no trivial solution:

- Minimize the interference between multiple concurrent transmissions of different source nodes, as it is not enough to consider zone disjoint links for a single source/destination pair.

5 Evaluation

As described in the previous section, our main goal is to improve Wireless Mesh Networks, by designing a system that performs better than the existing ones. To evaluate our proposal we can proceed the following way:

- Analytical models: although there are some models used to evaluate this kind of systems, they are complex to be derived analytically, so this solution may not provide the best results.
- Network simulators: are widely used in this area. The most used simulators are NS-2, GloMoSim and Opnet.
- Practical testbeds: as simulations sometimes do not consider interferences and other real transmission characteristics, practical testbeds are also good evaluation mechanisms. However, such a platform it requires a long deployment time, and the few ones that exist have a small number of nodes, thus increasing the difficulty of comparing the system with others.

Therefore, we plan to evaluate our protocol experimentally using the NS-2 simulator, thus making it easier to compare our work with competing results. To enrich the evaluation of our work, as a practical testbed is being developed in parallel [1], we also plan to use it, if time allows.

6 Scheduling of Future Work

Future work is scheduled as follows:

- January 9 - March 29: Detailed design and implementation of the proposed architecture, including preliminary tests.
- March 30 - May 3: Perform the complete experimental evaluation of the results.
- May 4 - May 23, 2009: Write a paper describing the project.
- May 24 - June 15: Finish the writing of the dissertation.
- June 15, 2009: Deliver the MSc dissertation.

7 Conclusions

Multipath routing protocols have been used to enhance the performance of Wireless Mesh Networks in different ways. In this work we have surveyed the relevant related work on this type of routing. To the best of our knowledge, current solutions include mostly reactive protocols, and those who are proactive only consider the use of a single path at a time.

So we propose a solution that aims to improve the backbone of mesh networks, by using a proactive protocol that uses multiple zone disjoint paths to deal with high bandwidth requirements of applications.

We have also presented the architecture of the proposed solution. Its detailed specification, implementation, and experimental evaluation are left for future work, whose schedule has also been presented.

Acknowledgments We are grateful to J. Mocito, O. Denysyuk and R. Pinto for the fruitful discussions and comments during the preparation of this report. This work was partially supported by project “Redico” (PTDC/EIA/71752/2006).

References

1. Pinto, R.: Wmm - wireless mesh monitoring. Technical report, INESC-ID (2009)
2. Marc Mosko, J.G.L.A.: Multipath routing in wireless mesh networks. In: in Proc. IEEE Workshop on Wireless Mesh Networks (WiMesh). (2005)
3. Moy, J.: OSPF Version 2. RFC 2328 (Standard) (April 1998) Updated by RFC 5709.
4. Mueller, S., Tsang, R., Ghosal, D.: Multipath routing in mobile ad hoc networks: Issues and challenges. In: In Performance Tools and Applications to Networked Systems, volume 2965 of LNCS, Springer-Verlag (2004) 209–234
5. Akyildiz, I., Wang, X.: A survey on wireless mesh networks. Communications Magazine, IEEE **43**(9) (Sept. 2005) S23–S30
6. Nandiraju, N.S., Nandiraju, D.S., Agrawal, D.P.: Multipath routing in wireless mesh networks. In: Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on. (2006) 741–746

7. Jacquet, P., Mühlethaler, P., Clausen, T., Laouiti, A., Qayyum, A., Viennot, L.: Optimized link state routing protocol for ad hoc networks. In: Proceedings of the 5th IEEE Multi Topic Conference (INMIC 2001). (2001)
8. Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: IEEE Workshop on Mobile Computing Systems and Applications. (1999) 90–100
9. Johnson, D.B., Maltz, D.A.: Dynamic source routing in ad hoc wireless networks. In: Mobile Computing, Kluwer Academic Publishers (1996) 153–181
10. Amir, Y., Danilov, C., Kaplan, M., Musaloiu-Elefteri, R., Rivera, N.: On redundant multipath operating system support for wireless mesh networks. In: Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2008. SECON Workshops '08. 5th IEEE Annual Communications Society Conference on. (June 2008) 1–6
11. Lee, S.J., Gerla, M.: Aodv-br: backup routing in ad hoc networks. Volume 3. (2000) 1311–1316 vol.3
12. Nasipuri, A., Das, S.R.: On-demand multipath routing for mobile ad hoc networks. In: Computer Communications and Networks, 1999. Proceedings. Eight International Conference on. (1999) 64–70
13. Valera, A., Seah, W.K.G., Rao, S., Rao, S.: Champ: A highly-resilient and energy-efficient routing protocol for mobile ad hoc networks. IEEE MWCN (2002) 79–85
14. Leung, R., Liu, J., Poon, E., Chan, A.L., Li, B.: Mp-dsr: a qos-aware multi-path dynamic source routing protocol for wireless ad-hoc networks. In: Local Computer Networks, 2001. Proceedings. LCN 2001. 26th Annual IEEE Conference on. (2001) 132–141
15. Lee, S.J., Gerla, M.: Split multipath routing with maximally disjoint paths in ad hoc networks. In: Communications, 2001. ICC 2001. IEEE International Conference on. Volume 10. (2001) 3201–3205 vol.10
16. Tsirigos, A., Haas, Z.: Multipath routing in the presence of frequent topological changes. Communications Magazine, IEEE **39**(11) (Nov 2001) 132–138
17. Siddiqui, M.S., Amin, S.O., Kim, J.H., Hong, C.S.: Mhrp: A secure multi-path hybrid routing protocol for wireless mesh network. In: Military Communications Conference, 2007. MILCOM 2007. IEEE. (Oct. 2007) 1–7
18. Rangarajan, S.: On demand loop free multipath routing in ad hocnetworks using source sequence numbers (2007)
19. Roy, S., Saha, D., Bandyopadhyay, S., B, S., Tanaka, S., Ueda, T.: Improving end-to-end delay through load balancing with multipath routing in ad hoc wireless networks using directional antenna. In: in Proc. IWDC 2003: 5th International Workshop, LNCS v2918. (2003) 225–234
20. Pearlman, M.R., Haas, Z.J., Sholander, P., Tabrizi, S.S.: On the impact of alternate path routing for load balancing in mobile ad hoc networks. (2000) 3–10
21. Tsai, J., Moors, T.: A review of multipath routing protocols: From wireless ad hoc to mesh networks. (2006)
22. Lim, H., Xu, K., Gerla, M.: Tcp performance over multipath routing in mobile ad hoc networks. In: Communications, 2003. ICC '03. IEEE International Conference on. Volume 2. (May 2003) 1064–1068 vol.2
23. Ye, Z., Krishnamurthy, S., Tripathi, S.: Effects of multipath routing on tcp performance in ad hoc networks. In: Global Telecommunications Conference, 2004. GLOBECOM '04. IEEE. Volume 6. (Nov.-3 Dec. 2004) 4125–4131 Vol.6
24. Ong, L., Yoakum, J.: An Introduction to the Stream Control Transmission Protocol (SCTP). RFC 3286 (Informational) (May 2002)
25. Koksal, C., Balakrishnan, H.: Quality-aware routing metrics for time-varying wireless mesh networks. Selected Areas in Communications, IEEE Journal on **24**(11) (Nov. 2006) 1984–1994

26. Campista, M.E.M., Esposito, P.M., Moraes, I.M., Costa, L.H.M.K., Duarte, O.C.M.B., Passos, D.G., De Albuquerque, C.V.N., Saade, D.C.M., Rubinstein, M.G., Rubinstein, M.G.: Routing metrics and protocols for wireless mesh networks. Network, IEEE **22**(1) (2008) 6–12
27. Yang, Y., Wang, J., Kravets, R.: Designing routing metrics for mesh networks. Proceedings of the IEEE Workshop on Wireless Mesh Networks (WiMesh). IEEE Press (2005)
28. Pearlman, M., Haas, Z., Sholander, P., Tabrizi, S.: On the impact of alternate path routing for load balancing in mobile ad hoc networks. In: Mobile and Ad Hoc Networking and Computing, 2000. MobiHOC. 2000 First Annual Workshop on. (2000) 3–10
29. Wu, K., Harms, J.: Performance study of a multipath routing method for wireless mobile ad hoc networks. Modeling, Analysis, and Simulation of Computer Systems, International Symposium on **0** (2001) 0099
30. Xuekang, S., Wanyi, G., Xingquan, X., Baocheng, X., Zhigang, G.: Node discovery algorithm based multipath olsr routing protocol. Information Engineering, International Conference on **2** (2009) 139–142
31. Hu, X., Lee, M.J.: An efficient multipath structure for concurrent data transport in wireless mesh networks. Comput. Commun. **30**(17) (2007) 3358–3367
32. Marina, M., Das, S.: On-demand multipath distance vector routing in ad hoc networks. In: Network Protocols, 2001. Ninth International Conference on. (Nov. 2001) 14–23