HABILITATION À DIRIGER DES RECHERCHES

Efficient Design and Performance Analysis of Wireless Mesh and Overlay Networks

Fabio Martignon

Submitted in total fulfillment of the requirements of the degree of Habilitation à Diriger des Recherches

Defense on December 10, 2010

Committee:

Reviewers:	Philippe Nain	DR INRIA Sophia-Antipolis
	Sergio Palazzo	Prof. Università degli Studi di Catania
	Khaldoun Al Agha	Prof. Université Paris-Sud 11
Examiners:	Prosper Chemouil	R&D Program Director, Orange Labs
	Guy Pujolle	Prof. UPMC Université Paris 6
	Serge Fdida	Prof. UPMC Université Paris 6
	Ahmed Mehaoua	Prof. Université Paris Descartes
	Tijani Chahed	Prof. Télécom SudParis

Abstract

This document summarizes part of the research work I have been developing during the last five years. My research interests focused on two main topics, namely (1) the design and evaluation of wireless networked computer systems (more specifically, of Wireless Mesh and Community networks), and (2) the planning of overlay networks and the distributed overlay formation problem.

Wireless Mesh Networks represent an effective means to provide broadband wireless connectivity without the need of a costly wired network infrastructure. The flexibility provided by this wireless network technology has fostered the development of new communication paradigms, like Wireless Mesh *Community* Networks, where devices owned and managed by different individuals cooperate to extend the network coverage.

In this context, we designed efficient and secure communication protocols at the Medium Access Control (MAC) and routing levels. We developed power-controlled, multi-channel MAC protocols for mesh nodes equipped with directional antennas; these protocols increase the spatial reuse and therefore the overall network performance. We then tackled the routing problem in wireless multi-hop networks using both exact models and heuristics; we further proposed a cross-layer routing protocol, named Directional Deflection Routing, which exploits multiple paths towards the destination based on the MAC layer indication on channel availability in different directions. We further addressed the security issues of these networks by developing robust security architectures, coping with the problem of reliable routing in the presence of selfish participants (typical of community networks).

We then focused our attention on *Overlay networks*, which have emerged as a viable and very effective means to provide a flexible, robust, and scalable platform for distributed applications, while leaving the underlying Internet infrastructure unchanged. A careful planning of the overlay topology and the choice of the routing strategies have obviously a great impact on the performance of such networks.

In this regard, we solved the overlay network design problem considering both centralized and fully distributed approaches. We first introduced several mathematical models for the optimal overlay network design problem, which select the optimal number and location of the overlay nodes to be deployed, while taking accurate account of the traffic routing. We further developed a set of efficient heuristics that obtain near-optimal solutions for large-scale network instances in a reasonable computation time.

Finally, we proposed two novel socially-aware overlay network design games to deal with the fully distributed overlay network formation problem. The first game combines both individual and social concerns in a unified and flexible manner, while the second game uses a Stackelberg (leader-follower) approach, where the overlay network administrator leads the users to a system-wide efficient equilibrium by stimulating the utilization of an appropriate subset of links.

Table of contents

Chapter 1

Introduction

The Internet is undergoing important changes. The wireless technology currently enables almost seamless mobility of network users. A key technology, *Wireless Mesh Networks* (WMNs), has emerged to provide widespread network connectivity with low up-front cost, easy network maintenance, robustness and reliable service coverage. The WMN paradigm has recently fostered the development of Wireless Mesh *Community* Networks (WMCNs), where mesh nodes are owned and managed by community members who cooperate to extend the network coverage.

While Wireless Mesh Networks contribute to provide a wider coverage, supporting service continuity at the network layer, the *overlay network* technology has emerged as a means to guarantee service continuity at the application level, leaving the underlying Internet infrastructure unchanged. In fact, the Internet services are currently being extended using overlay networks, which support enhanced applications like content distribution, multicast, file sharing (to cite a few) by creating a virtual topology on top of existing networks.

Several research challenges need to be faced to improve the performance of these networks, including a careful network planning, the design of efficient communication protocols and the implementation of robust security architectures that stimulate users to subscribe to reliable services.

This document summarizes part of the research activities I have been developing during the last five years. My interests focused on the research problems that characterize the two network scenarios introduced before, i.e.:

- the design and evaluation of Wireless Mesh (Community) networks;
- the planning of overlay networks and the distributed overlay formation issue.

My concern has been to focus on designing new and more efficient communication protocols to satisfy the increasing bandwidth demands and tighter quality of service requirements of user applications while, at the same time, guaranteeing security and confidentiality of the data exchanged in the network.

This chapter introduces the network scenarios in which my research was developed, starting from Wireless Mesh Networks (Section 1.1) and Wireless Mesh Community Networks (Section 1.2), and then moving to overlay networks (Section 1.3). An overview of the main contributions is provided in each section, and the two next chapters will be dedicated to detail the research progress we obtained in these fields.

1.1 Wireless Mesh Networks

Wireless Mesh Networks (WMNs) have been accepted as a new communication paradigm able to provide a cost-effective means to deploy all-wireless network infrastructures [1].

The network nodes in WMNs, named mesh routers, provide access to mobile users, like access points in wireless local area networks, and they relay information hop by hop, like routers, using the wireless medium. The mesh routers form a self-organized and self-configured backbone network by collaborating in the execution of management and control operations. The nodes[1] in the backbone network use the IEEE 802.11 standard as wireless technology to establish the radio links, and maintain connectivity among themselves via routing protocols like DSR [2], AODV [3], and OLSR [4], which are borrowed from the Mobile Ad-Hoc Networks (MANET) paradigm.

Unlike MANETs, mesh routers are usually fixed and do not have energy constraints. Moreover, the gateway functionalities performed by a subset of mesh routers enable the integration of WMNs with several existing technologies, like cellular systems, Wireless Sensor Networks and WiMAX. On the other hand, mesh clients connect to mesh routers and communicate with each other through the multi-hop wireless network formed by mesh routers.

A typical architecture of a Wireless Mesh Network is illustrated in Figure 1.1, where solid and dashed lines represent wired and wireless links, respectively.

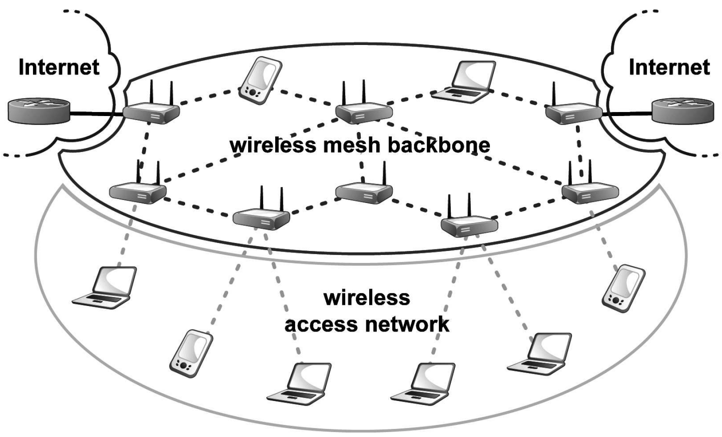


Figure 1.1: Wireless Mesh Network Architecture.

WMNs, like wired networks, are characterized by infrequent topology changes and rare node failures, and thus represent the ideal solution to provide both indoor and outdoor broadband wireless connectivity in several environments without the need for costly wired network infrastructures. Their capabilities of self-organization and self-configuration enable an incremental deployment of the network by installing more nodes only when the demand for an increased network capacity or for tighter quality of service requirements needs to be satisfied.

Contributions

Several technological issues need to be solved to improve the performance of WMNs, while guaranteeing at the same time security and confidentiality of the data exchanged in the network.

[1]The terms *node* and *router* will be used interchangeably.

In our work, we focused both on the MAC and routing layers, which account for high performance improvements, and we further developed enhanced security architectures. More specifically, our contributions in this context can be summarized as follows:

- *Medium Access Control* level. We investigated systematically the impact of different techniques, viz. power control, directional transmissions and multiple channel operation, on the MAC level performance. In this regard, we developed in [5, 6, 7] novel MAC protocols that exploit the increased spatial reuse made possible by such techniques to improve the network performance.

- *Routing* level. Our contribution has been twofold: on the one hand, we proposed in [8, 9] efficient mathematical programming models of the routing problem in multi-hop wireless networks, which take into account quality of service requirements considering bandwidth constraints, power control and directional transmissions. Solving these models permits to obtain optimal routing decisions. On the other hand, we proposed in [5] a novel, cross-layer routing protocol, named Directional Deflection Routing, which exploits multiple paths towards the destination based on the MAC layer indication on channel availability in different directions.

- *Security architectures.* In this regard, we first proposed in [10, 11, 12] MobiSEC, a complete, centralized security architecture that provides both access control for mesh users and routers as well as a key distribution scheme that supports layer-2 encryption to ensure security and data confidentiality of all communications that occur in the WMN.

  Then, in [13], we proposed DSA-Mesh, a fully distributed security architecture which exploits the routing capabilities of mesh routers: after connecting to the access network as generic wireless clients, new mesh routers authenticate to a key management service (consisting of several servers) implemented using threshold cryptography, and obtain a temporary key that is used both to prove their credentials to neighbor nodes and to encrypt all the traffic transmitted on wireless backbone links.

  Finally, we formulated a novel network optimization model to determine the optimal placement of the devices that collaboratively perform the authentication and key management services.

1.2 Wireless Mesh Community Networks

The complete absence of a fixed infrastructure in WMNs has promoted new network paradigms, like Wireless Mesh Community Networks (WMCNs) [14, 15], which, on the one hand, provide an effective, economic alternative to municipal wireless networks for consumers; on the other hand, WMCNs have also introduced new technical problems that are hard to overcome with current communication protocols.

Wireless Mesh Community Networks are characterized by a flexible and low-cost network infrastructure, where heterogeneous mesh routers managed by different users collaborate to extend the network coverage [14]. In particular, the mesh routers that form the infrastructure of the WMCN (the wireless mesh backbone, if we refer again to Figure 1.1) are managed and maintained by different community members.

Such members, though, can exhibit a selfish behavior while providing connectivity through their own mesh router(s) to other network nodes or clients; for example, they might try to greedily consume the available bandwidth by favoring their own traffic while selectively dropping others' [14], setting firewall rules on their devices to drop almost all packets sent by other participants or customer stations, or limit the maximum transmission rates available to the served devices. Such misbehavior can lead to severe unfairness and serious performance degradation, as pointed out for example in [16, 17], where it has been demonstrated that periodic dropping at relaying nodes can decrease the throughput of closed loop connections (such as TCP) established by other nodes, even when the fraction of dropped packets is small.

Packet dropping can be performed by a selfish mesh router both on the outgoing and incoming traffic. Therefore, each network device that participates to the WMCN must evaluate the forwarding behavior of its neighbor mesh routers, controlling whether they actually relay all the network traffic after having confirmed its reception or not. Based on such evaluation, appropriate strategies can be envisaged to limit the consequences of selfish behaviors.

Contributions

In order to detect selfish behaviors and stimulate the cooperation among different community mesh routers, we extended the network layer protocols setting forth two strategies: we first proposed enhanced routing metrics that take into account not only the wireless link quality, but also the nodes' availability in forwarding traffic. Then, we developed an efficient trust and reputation framework that exploits both direct and indirect observations of the nodes' behavior in order to infer their reliability level.

Our contributions in the context of Wireless Mesh Community Networks can therefore be summarized as follows:

- We investigated systematically the impact of the uncooperative behavior of selfish mesh routers in the routing process. Specifically, we evaluated the performance of OLSR, the most widespread routing protocol used in WMCNs, when the path selection is driven by data-link layer metrics that capture only the quality of wireless links, like the well-known ETX metric (Expected Transmission Counter) [18]. Our results show that in the presence of even a low percentage of adversaries, data connections experience severe throughput degradation and unfairness.

- For this reason, we proposed in [19] a new cross-layer metric, named EFW (Expected ForWarding counter), which combines information across the MAC and network layers to select the most reliable and high-performance network paths. The results obtained through both simulations and experiments on real-life testbeds show the validity of the proposed approach.

- We further proposed in [20] an innovative trust and reputation framework that models the trust that mesh routers have in other nodes as vectors of a multi-dimensional space. Through this representation, honest nodes can effectively detect indirect observations that are provided by lying nodes, and reduce significantly their contribution in the evaluation of the real forwarding behavior of the other participants. As a consequence, each node can finally obtain a precise estimate of the level of selfishness of all mesh routers that belong to the WMCN.

1.3 Overlay Networks

Overlay networks have recently emerged as a viable and very effective means to avoid network-level inefficiencies in the Internet, enabling, at the same time, a variety of popular applications including peer-to-peer file sharing, content distribution and server deployment. Overlay networks today represent an alternative and very promising architecture able to provide end-to-end Quality of Service guarantees in the Internet, while leaving the underlying Internet infrastructure unchanged [21, 22, 23, 24].

Overlay networks are virtual topologies that use a combination of shared and dedicated resources, to provide a simple network view that conceals unnecessary details about the underlying topology. A typical overlay network architecture is depicted in Figure 1.2, where overlay nodes reside in the underlying ISP networks, and are interconnected by virtual links which correspond to one or more IP-layer links.

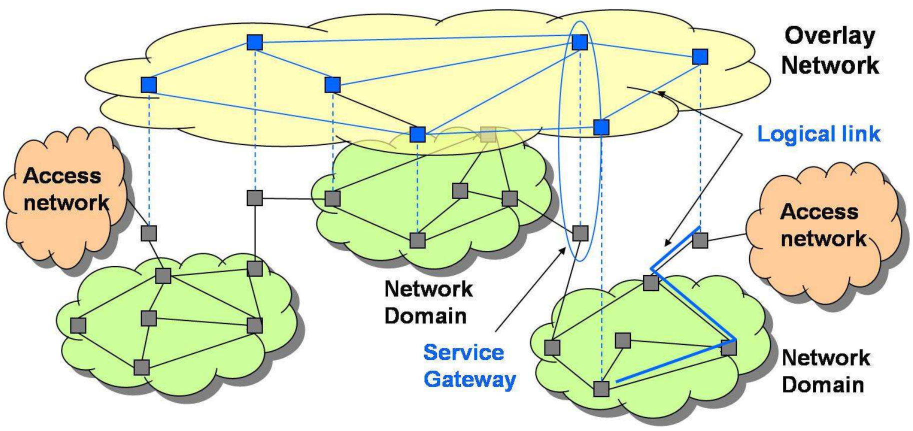


Figure 1.2: Overlay Network Architecture.

The choice of where to install overlay nodes, which links establish between such nodes and, in general, how to allocate resources to the overlay network has a deep impact on the effectiveness of the resulting network and on its overall cost.

Contributions

Our work investigated two alternative, and complementary, approaches for the design of efficient overlay networks, namely:

- a *centralized* network optimization approach, which is based on the Service Overlay Network (SON) paradigm [21]; in this regard, we first proposed in [25] two network optimization models that determine the optimal assignment of users to access overlay nodes, as well as the capacity reserved for each overlay link, while taking accurate account of traffic routing. We then formulated in [26, 27] two overlay network design models that further select the optimal number and location of the overlay nodes to be deployed, as well as the optimal coverage of network users to maximize the SON operator's profit. Finally, in [26, 28] we developed a set of efficient SON design heuristics that get near-optimal solutions for large-scale instances in a reasonable computation time, and we performed an extensive evaluation of the proposed centralized optimization framework in several network scenarios.

- A *fully distributed* approach, where the overlay network design and operation is carried out by a large number of independent actors (e.g., the overlay user clients), all of whom seek to selfishly optimize their own utility. In this context, we defined in [29, 30] two novel socially-aware overlay network design games, namely (1) the Socially-Aware Network Design game, which combines both individual and social concerns in a unified and flexible manner, and (2) a Stackelberg (leader-follower) game where the overlay network administrator leads the users to a system-wide efficient equilibrium by buying an appropriate subset of the overlay network links. We then performed a thorough numerical evaluation of the proposed games, through the determination of bounds on the Price of Anarchy, the Price of Stability and the Reachable Price of Anarchy of such games, as well as by simulation of realistic network scenarios, including real Internet Service Provider topologies.

1.4 Outline of the manuscript

The remainder of the manuscript is composed of three chapters and two annexes. Chapters 2 and 3 form the core of this document, since they present the two groups of contributions described in the previous sections, namely, those related to Wireless Mesh and Community networks (Chapter 2), and overlay networks (Chapter 3). In these chapters, I do not get into the details of the topics considered. Instead, I present their main ideas and try to give a global picture of the problem. For more details on each of the proposals, the reader is invited to refer to respective publications.

In Chapter 4, I present a summary of the manuscript and raise a number of issues as a plan for future research.

This manuscript also includes annex A, where I briefly describe other contributions that are related to the research presented in this manuscript. For a more detailed view of my research activities, the best way is to refer to my webpage at http://cs.unibg.it/martignon.

Finally, annex B reports a list of all my publications.

Chapter 2

Wireless Multi-Hop Networks

This chapter presents several contributions related to Wireless Mesh Networks and Wireless Mesh Community Networks, which are characterized by common research issues at the Medium Access Control (MAC) level, the network layer, and the security plane.

Due to their intrinsic heterogeneous nature, though, Wireless Mesh Community Networks further present the problem of stimulating network nodes to cooperate to the packet forwarding process. In these networks, in fact, mesh nodes are managed by community members who can exhibit selfish (or non-cooperative) behaviors.

In the following, we describe the advancements we obtained in the above mentioned research issues, starting from the MAC layer (Section 2.1), moving to the routing problem (Section 2.2), and then illustrating the enhanced security architectures we developed for wireless multi-hop networks (Section 2.3). Finally, Section 2.4 is devoted to the problems typical of Wireless Mesh Community networks, as well as to the solutions we proposed to cope with them (viz., novel routing metrics and trust/reputation frameworks).

2.1 Enhanced MAC protocols with Power Control, Directional Antennas and Multiple Channels

(Publications [5, 6, 7]).

Supporting high throughput is an important challenge in both Wireless Mesh Networks (WMNs) and Wireless Mesh Community Networks (WMCNs), since the IEEE 802.11 standard Medium Access Control (MAC) can lead to poor performance for such networks, due to its unfriendliness with multi-hop operation [31, 32]. It is therefore important to devise efficient MAC schemes which make it possible to operate network nodes in multi-hop mode without excessive performance degradation. On the other hand, the IEEE 802.11 standard is so established by now that any completely new MAC will find it very hard to succeed commercially. Our approach in this context has been therefore to consider small variations to the current standard in order to solve the main performance problems without requiring major hardware modifications.

In recent years, the utilization of power control techniques has been proposed to enhance spatial reuse and wireless medium utilization [33, 34, 35]. Furthermore, directional antenna technology has been studied in 802.11-based networks. The increased spatial reuse with the combination of extended transmission range is especially attractive for 802.11-based mesh networks [5, 36]. Regrettably, directional transmissions can also cause serious problems in a WMN environment, increasing the number of instances of the hidden terminal problem [37]. Therefore, efficient MAC protocols need to be designed, since the IEEE 802.11 standard MAC has been optimized for omnidirectional antennas.

In this regard, we first proposed the Power-Controlled Directional MAC protocol (PCD-MAC) [5, 7], a novel protocol designed for Wireless Mesh Networks where nodes use directional, adaptive antennas and power control.

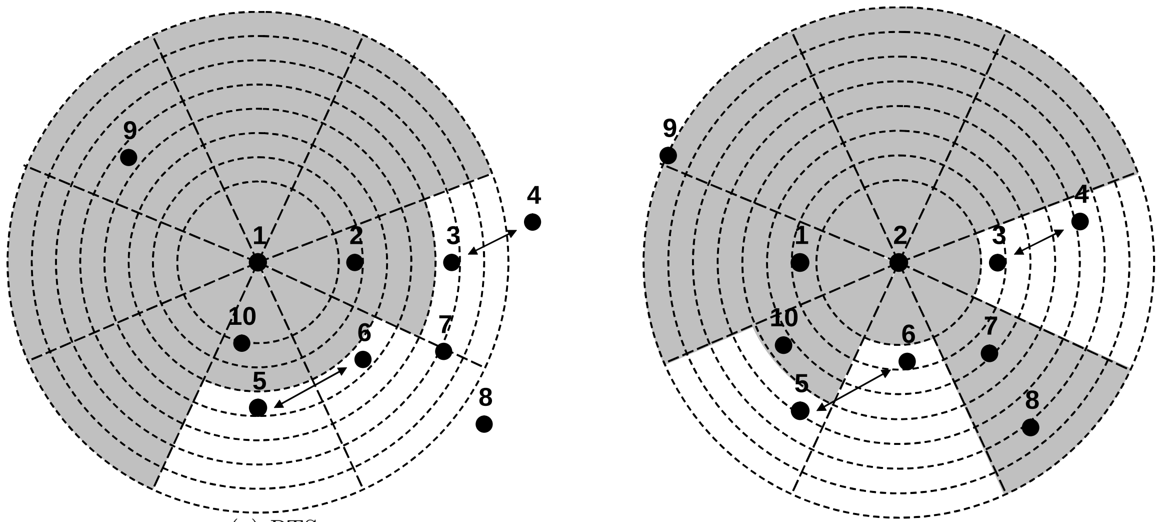
Its key innovative feature is that nodes spread the wireless medium reservation information to the maximum possible extent without interfering with the connections already established in the network. This is achieved by sending RTS/CTS frames in each antenna sector using the maximum power that does not cause interference with ongoing transmissions. Then the DATA/ACK exchange takes place only directionally and at the minimum needed power.

As an example of PCD-MAC operation, let us consider the network scenario shown in Figures 2.1 and 2.2, where two connections are active between nodes 3-4 and 5-6. Each node is equipped with an adaptive antenna having 8 sectors and 8 different transmission power levels, as depicted in the figures.

If node 1 wants to transmit a packet to node 2, it transmits an RTS frame using the adaptive antenna transmission range represented by the gray area in Figure 2.1(a). Similarly, Figure 2.1(b), node 2 transmits the corresponding CTS. The ensuing DATA/ACK exchange then takes place directionally and at the minimum necessary power, as illustrated in Figures 2.2(a) and 2.2(b).

In this example, the power control feature of PCD-MAC permits to establish the connection between nodes 1 and 2, even if there is an ongoing transmission (between nodes 3 and 4) in the sector that contains node 2, thus increasing the overall network performance.

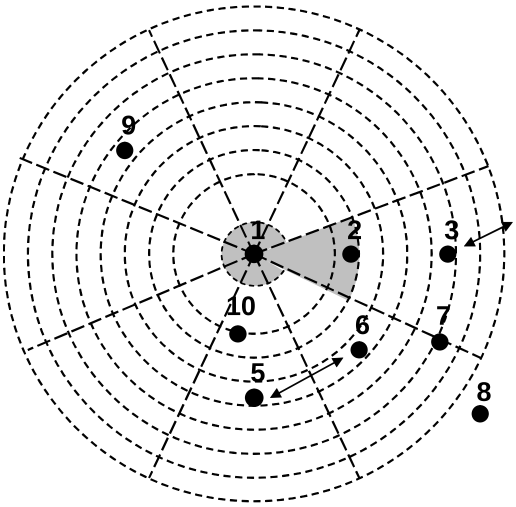
The solution we proposed in [6], the Multi-Channel Power-Controlled Directional MAC protocol (MPCD-MAC), improves over PCD-MAC, since it further leverages on the fact that mul-



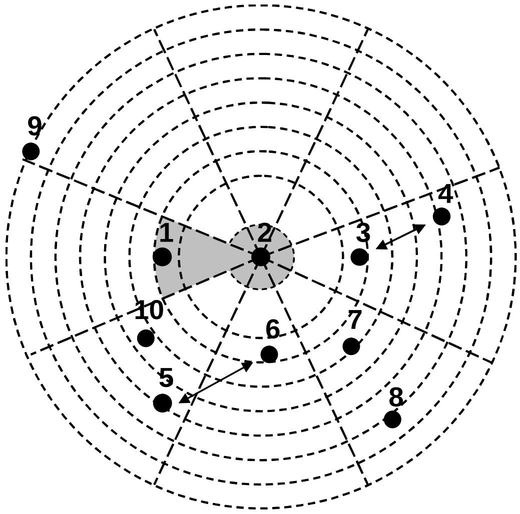
(a) RTS

(b) CTS

Figure 2.1: PCD-MAC: antenna pattern (a) used by node 1 to send the RTS frame (b) used by node 2 to send the CTS frame; two connections are already established, between nodes 3-4 and 5-6.



(a) DATA



(b) ACK

Figure 2.2: PCD-MAC: antenna pattern (a) used by node 1 to send the DATA frame (b) used by node 2 to send the ACK frame; two connections are already established, between nodes 3-4 and 5-6.

tiple channels are available in the industrial, scientific, and medical (ISM) band used for wireless LANs, so that the handshake used for contention and channel allocation can be separated from the actual user traffic. This makes it possible to increase the performance of WMNs using multiple antennas tuned on non overlapping channels and running multiple channels in parallel.

The problems of designing efficient multi-channel MAC protocols [31, 32, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47] and single-channel MAC schemes with directional antennas [37, 48, 49, 50, 51, 52, 53] have been deeply investigated in the research area of ad hoc networks.

MPCD-MAC is a novel MAC protocol designed for Wireless Mesh Networks where nodes use multiple channels, directional antennas and power control. Its key innovative feature is that the transmission of the RTS and CTS packets takes place in all directions at the maximum transmission power on a *separate* control channel, while the DATA and ACK packets are transmitted only directionally on an available data channel at the minimum required power, as for PCD-MAC. Furthermore, a novel connection is established between two nodes only if the interference produced over already active connections is sufficiently low to permit concurrent transmissions to take place.

As a consequence, MPCD-MAC spreads the information on wireless medium reservation (RTS/CTS) to the largest set of neighbors, while data transfers take place only directionally on a separate channel to increase spatial reuse and minimize interference.

In [6] we further proposed several variations to the MPCD-MAC protocol, to gauge the performance gain achieved by the different techniques incorporated in our protocol (viz., directional transmissions, power control and interference awareness). The reader is referred to [6] for more details.

We evaluated extensively our proposed MAC protocols through simulation, comparing their performance with the most notable solutions proposed in the literature. Table 2.1 illustrates sample numerical results measured in a 5×5 grid network scenario with elementary size of 140 m, where nodes use either the standard IEEE 802.11 MAC or our proposed PCD-MAC and MPCD-MAC protocols. The overall network goodput (in Mbit/s) and the Jain's fairness index among competing connections [54] is reported in the table. The latter metric assumes values in the $[0, 1]$ range; value 1 is achieved when all connections obtain exactly the same goodput (perfect fairness). Note that in our simulations we have assumed a radio transmission rate of 11 Mbit/s, and standard MAC settings.

Table 2.1: Average goodput [Mbit/s] and Jain's fairness index for PCD-MAC, MPCD-MAC and the standard IEEE 802.11 MAC in a 5×5 grid network scenario with inter-node spacing of 140 m; 10 connections offer to the network a Poisson traffic. Two orthogonal channels are exploited by MPCD-MAC.

MAC	Goodput	Fairness
IEEE 802.11 MAC	6.13	0.36
PCD-MAC	11.02	0.67
MPCD-MAC	14.55	0.65

These results demonstrate that MPCD-MAC performs consistently better than single-channel MAC protocols (IEEE 802.11 and PCD-MAC). At the same time, PCD-MAC improves over the standard IEEE 802.11 MAC.

More in general, we gathered results in several realistic network scenarios which show that MPCD-MAC outperforms existing schemes both in terms of total traffic accepted in the network and fairness between competing connections, even when a very small number of orthogonal channels is available (like, for example, in the 802.11b 2.4GHz frequency band). On the other hand, PCD-MAC represents a very effective solution when only a single channel is available.

2.2 Routing in multi-hop wireless networks

(Publications [5, 8, 9]).

The problem of routing in multi-hop wireless networks has been deeply investigated in the research area of Mobile Ad-hoc NETworks (MANET). However, the peculiar features of Wireless Mesh Networks and Wireless Mesh Community Networks make the routing problem quite different [1]. As we pointed out before, WMNs have almost static topologies that change mainly due to node failures, which are relatively infrequent. Therefore, the distribution of network state information is not much costlier than in wired networks, and even a centralized control of route selection can be adopted [55, 56, 57, 58, 59]. Moreover, energy consumption is usually not a key issue for network nodes.

In this context, we first proposed in [8] a new model for the Quality of Service (QoS) routing problem in multi-hop wireless networks with bandwidth constraints, considering nodes equipped with *omnidirectional* antennas. The model is an extension of the well known multi-commodity flow problem where link capacity constraints are replaced with new ones that take into account interference constraints among different radio links. As a key innovative feature, and differently from previous work on QoS routing in ad hoc networks [60, 61], our formulation allows to decouple the routing and the scheduling problems that can be solved in different steps.

Then, we focused our attention on wireless nodes equipped with *directional* antenna technology [36]. As we discussed in the previous section, the main advantage of using directional antennas with wireless multi-hop networks is the reduced interference and the possibility of having parallel transmissions among neighbors with a consequent increase of spatial reuse of radio resources.

In this regard, we studied in [9] the *joint routing and scheduling optimization problem* in WMNs where nodes are equipped with directional antennas. We assumed a Spatial reuse Time Division Multiple Access (STDMA) scheme, a dynamic power control able to vary the emitted power slot-by-slot, and a rate adaptation mechanism that sets transmission rates according to the Signal-to-Interference-plus-Noise Ratio (SINR). Traffic quality constraints are expressed in terms of minimum required bandwidth. Since the time frame defined by the TDMA scheme is fixed, the bandwidth requirement can be translated into the number of information units (packets) that must be transmitted on each link per frame. Moreover, according to a discrete set of possible transmission rates, the number of packets that can be transmitted per time slot depends on the SINR at receivers.

To get more insights on the characteristics of the problem and the effect of different control mechanisms, we considered three different versions of the problem with increasing complexity. In the first one we assumed fixed transmission power and rate, in the second one variable power and fixed rate, and finally in the third one variable power and rate. For each version we considered mesh nodes with both omnidirectional and directional antennas.

Given a number of available slots, our model provides an assignment of time slots to links such that bandwidth constraints are satisfied and the number of available slots is not exceeded. To solve such problem, it is possible to look for the minimum number of needed time slots: if it is smaller than the number of available slots, a feasible assignment exists.

Since the classical compact mathematical programming formulation is very hard to solve [62], the solution approach we proposed in [9] is based on an alternative problem formulation where decision variables represent compatible sets of links active in the same time slot. As variables are exponentially many, we used a column generation approach to solve the continuous relaxation of the problem which provides a lower bound of the optimal solution. In several cases the solution provided by the column generation procedure is equivalent to the integer optimum; however, to provide good solutions in reasonable time we proposed two solution approaches with different computational complexity.

We analyzed the proposed models in a set of realistic-size instances and discuss the effect of different parameters on the characteristics of the solution. The results show that the utilization of directional antennas and rate control schemes increases considerably the total traffic accepted by the network.

Finally, in [5] we considered a *fully distributed* approach to the routing problem in wireless multi-hop networks, by proposing the Directional Deflection Routing (DDR). DDR is a routing algorithm for wireless multi-hop networks based on a cross-layer approach that is inspired by a routing protocol (Deflection Routing) first proposed for optical networks [63, 64]. Each node maintains a sorted list of next-hop nodes per destination according to paths lengths, and it forwards packets to the first available node in the list. Node availability is obtained by the MAC layer indication on channel status in different directions.

DDR can be applied on top of any MAC protocol that exploits directional antennas using the Directional Network Allocation Vector (D-NAV), i.e., an extension of the NAV used in the 802.11 standard MAC, where a direction field is further introduced, indicating that the NAV applies only for the specified direction. In particular, it can be implemented over our proposed PCD-MAC and MPCD-MAC protocols.

Formally, DDR operates as follows. Let us consider a directed weighted graph $G = (V, E)$, where nodes represent the wireless routers and directed arcs $(i, j) \in E$ connect routers within transmission range. For each node $n \in V$, we define $N(n)$ as the set of nodes adjacent to n.

Routing tables are computed by each node n based on the procedure detailed in the following. For all possible destination $m \neq n$, and for every adjacent node $h \in N(n)$, node n computes the shortest path between itself and m having (n, h) as first hop. Paths are sorted in increasing cost order, and node n stores in the routing table the ordered list of next-hop nodes that can be used to reach node m. Note that due to fixed mesh routers in WMNs, the routing tables computation can be performed by DDR ideally only once, and in practice only when a topology change occurs.

Packet forwarding then proceeds as follows: when a packet with destination m arrives at node n, the ordered list of possible next-hop nodes for destination m is scanned and the first non-blocked next-hop node is chosen to forward the packet. Blocked nodes are nodes that cannot be currently used as relays according to the information contained in the D-NAV of n, which is provided (in a cross-layer fashion) directly by the MAC layer. If all nodes are blocked, the one that will become non-blocked first is chosen for the forwarding. To reduce complexity, once the next hop is selected it is never changed even if a collision occurs and the packet must be retransmitted.

When node n is directly connected to the destination node m of the packet, no deflection is applied and n transmits directly the packet to m, waiting eventually for m to become non-blocked. Finally, the packet is never forwarded to the node from which it was received.

To illustrate the operation of Directional Deflection Routing, let us refer to the simple network scenario of Figure 2.3, where lines represent wireless links. The cost of each link is equal to 1. Nodes 2-6 are currently involved in a frame exchange, represented with arrows, and node 1 wants to send a packet to node 3.

The routing tables towards node 3 are also reported in the figure for nodes 1, 5 and 4. More specifically, node 1 has two alternate routes to reach node 3, namely passing through node 2 (with cost equal to 2) and through node 5 (with cost equal to 3). However, according to the D-NAV indication in node 1, node 2 is currently blocked, and node 5 is chosen as next hop.

Node 5 then forwards the packet along the shortest path towards the destination, choosing node 4 as next hop; finally, since node 4 is directly connected to node 3, it transmits it directly to the destination.

Since Directional Deflection Routing distributes traffic among multiple routes, the frequency of route switching is a key point. From the network layer perspective, end-to-end throughput

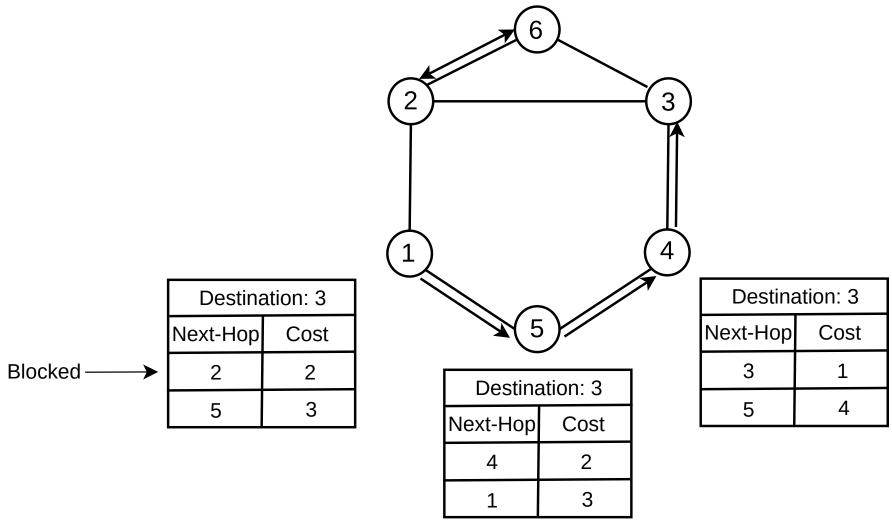


Figure 2.3: Example scenario that illustrates the operation of Directional Deflection Routing: node 1 wants to transmit a packet to node 3, while nodes 2-6 are currently involved in a frame exchange. Forwarding tables towards node 3 for nodes 1, 5 and 4 are also reported.

improves as the frequency of route transitions increases, with the best policy being to distribute traffic on a per-packet basis [65, 66].

To illustrate the effectiveness of DDR, let us consider a grid network (6 × 6) with elementary size equal to 140 m, shown in Figure 2.4(a). We consider multi-hop connections originated at node 13 and destined to 14, 15, 16, 17 and 18, respectively. Only one connection is active at a time and we measure its goodput achieved by either shortest-path routing and DDR.

For a single-hop connection, both routing algorithms are the same. On a two-hop connection the goodput drastically reduces since both hops (13-14 and 14-15) cannot transmit at the same

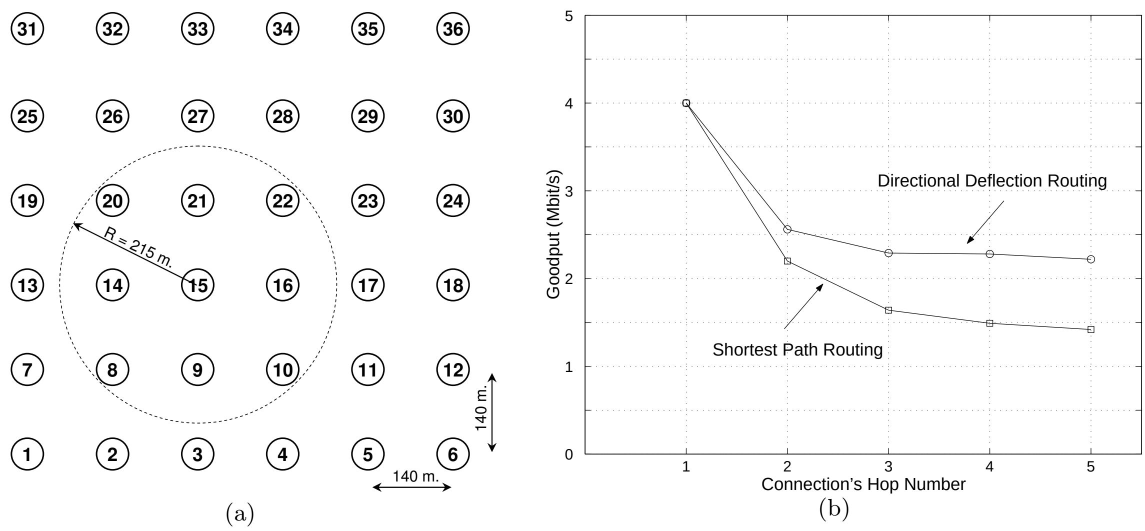


Figure 2.4: (a) Single multi-hop connection established in a grid scenario with 36 nodes. (b) Goodput achieved by a single multi-hop connection as a function of the number of hops.

time. DDR shows an improvement over shortest-path routing since alternate hops, for example 13-20 or 13-8, can be used at the same time as 14-15. This beneficial effect of DDR increases as the number of hops increases as shown in Figure 2.4(b).

An extensive performance evaluation of DDR, which confirms its effectiveness in all the considered network scenarios, can be found in [5].

2.3 Security Architectures for Wireless Mesh Networks

(Publications [10, 11, 12, 13].)

Although in the recent years the design of network protocols has been revisited to consider and capture the inherent features of the wireless technology, *security* and *reliability* are still in their infancy, as very little attention has been devoted so far to these topics by the research community. However, security is a primary concern for any customer that wants to subscribe to reliable and secure wireless services.

Due to the open and shared nature of the wireless technology and the multi-hop communication paradigm, WMNs and WMCNs are more vulnerable to attacks. Outsider adversaries can easily perform a wide variety of attacks, such as eavesdropping, jamming, man-in-the-middle and spoofing. On the other hand, the lack of an authentication and authorization system that limits the access only to authorized mesh nodes may result in internal attacks through which adversary nodes can steal sensible information of users or seriously affect the network operation. Finally, in the design of WMNs and WMCNs, special attention must be also devoted to the protection of the integrity and authenticity of the control information exchanged by mesh routers, like management and routing messages. Without a solution that guarantees these latter properties, attackers can disseminate forged messages to cause network malfunctions and deny access to legitimate users.

We addressed the aforementioned security issues in [10, 11, 12, 13] by designing two security architectures tailored for wireless multi-hop networks. The former architecture, called *MobiSEC* [10, 11, 12], assigns to a mesh router the role of authentication and key management server. All nodes periodically receive from this node the information necessary to generate the sequence of cryptographic keys used to protect the data and control messages transmitted over the backbone. The mutual authentication between the key management server and a mesh router is obtained through the exchange of the certificates that prove their identities.

In MobiSEC, client security is guaranteed using the standard 802.11i protocol, while backbone security is provided as follows: each new router that needs to connect to the mesh network first authenticates to the nearest mesh router exactly like a client node, gaining access to the mesh network. Then it performs a second authentication connecting to a Key Server able to provide the credentials to join the mesh backbone. Finally, the Key Server distributes the information needed to create the temporary key that all mesh routers use to encrypt the traffic transmitted over the wireless backbone.

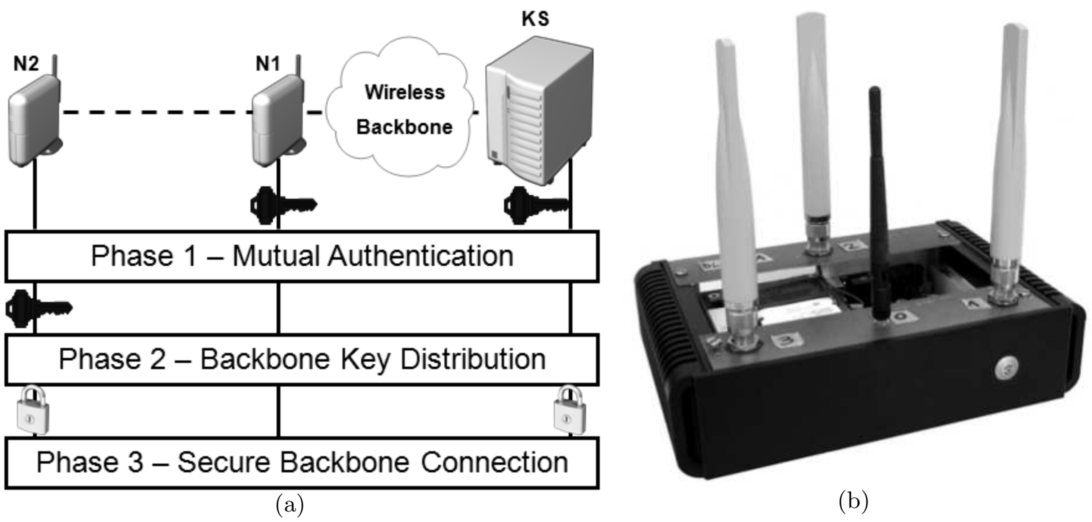
Figure 2.5(a) shows the three phases of the connection process performed by a new mesh router (namely, node N_2). When N_2 wants to connect to the mesh network, it scans all radio channels to detect a mesh router already connected to the wireless backbone, which is therefore able to provide access to all network services (including authentication and key distribution). Let N_1 be such router. After connecting to N_1, N_2 can perform the tasks described by the IEEE 802.11i protocol to complete a mutual authentication with the network and establish a security association with the entity to which it is physically connected (phase 1). At the end of such phase, N_2 obtains the network parameters performing a DHCP request. In phase 2, N_2 establishes a secure connection with the Key Server (KS), using the TLS protocol [67], to obtain the necessary information that will be used to generate the current key used by all mesh routers to encrypt all the traffic transmitted on the mesh backbone. In particular, the device can connect to the wireless backbone in a secure way and begin executing the routing and access functions (phase 3).

The MobiSEC architecture has been implemented on embedded systems based on a VIA Epia Board equipped with a PCI-to-MiniPCI expander that permits the installation of four MiniPCI wireless cards, as depicted in Figure 2.5(b). The black external antenna provides access to the wireless clients, whereas the other antennas form the wireless backbone links with the other mesh routers.

We tested the robustness of MobiSEC using both simulation and real network measurements, and the results show that our proposed architecture considerably increases the network security, with a negligible impact on the network performance, thus representing an interesting solution for wireless mesh networking.

While representing an effective security solution for WMNs, MobiSEC, like all centralized solutions, is characterized by a single point of failure (the Key Server) that can be exploited by adversaries to attack the network. We therefore designed a distributed architecture, named *DSA-Mesh* (a Distributed Security Architecture for Wireless Mesh Networks) [13], which improves the robustness of the entire system by increasing the number of mesh routers that are liable for the authentication and key management services.

Similarly to MobiSEC, DSA-Mesh exploits the routing capabilities of wireless mesh routers, adopting a two-step approach: (1) in the first step, new nodes perform the authentication process with the nearest mesh router, like generic wireless clients; (2) in the second step, these nodes can



(a) (b)

Figure 2.5: (a) MobiSEC: phases of the connection process performed by a new mesh router (node N_2); the depicted keys are used to encrypt backbone traffic. (b) Multi-radio mesh router prototype used to implement and test MobiSEC.

upgrade their role in the network (becoming mesh routers) by further authenticating to a key management service, which consists in this case of several servers, obtaining a temporary key with which all traffic is encrypted. As a key innovative feature with respect to existing works, such step is implemented using *threshold cryptography*; this technique permits the distribution of trust in the key management service, allowing n mesh nodes to share the ability to perform a cryptographic operation (e.g., creating a digital signature), so that any t nodes can perform this operation jointly, whereas it is infeasible for at most $t-1$ nodes to do so, even by collusion.

Regrettably, in some network scenarios DSA-Mesh exhibits a greater latency than MobiSEC, due to its distributed nature that requires the collaboration of several network nodes to complete the authentication and key distribution tasks.

For this reason, we further proposed an Integer Linear Programming model to select the mesh routers that minimize the overall latency of the distributed protocols. We showed that a careful planning of the roles assigned to mesh routers can increase the responsiveness of DSA-Mesh, and distributed architectures that adopt a similar collaborative approach.

2.4 Reliability Metrics, Trust and Reputation frameworks for Wireless Mesh Community Networks

Publications [19, 20].

As we pointed out in Section 1.2, Wireless Mesh Community Networks (WMCNs) provide a viable alternative to municipal wireless networks for users; however, such networks also introduce new problems that are hard to overcome with current communication protocols, since the mesh routers that form the WMCN infrastructure are managed and maintained by different community users, and therefore they can exhibit heterogeneous behaviors with regards, for example, to their willingness to perform packet forwarding.

Many applications envisioned to run on WMCNs have high throughput and tight QoS requirements. Recent research [18, 68] has introduced several link layer metrics that capture the quality of the wireless links in order to select the network paths with the highest delivery rates.

However, most of the proposed metrics have been designed assuming that each wireless mesh router participates honestly in the forwarding process. While this assumption may be valid in a network managed by a single network operator, it is not necessarily met in a network where the participants are managed by different entities that may benefit from not forwarding all the traffic. This is what happens in a WMCN, where a selfish community member that provides connectivity through his own mesh router(s) might try to greedily consume the available bandwidth by favoring his traffic to the detriment of others, for example by selectively dropping packets sent by other nodes [14]. Tools like *iptables* can be used to easily implement packet dropping at the network layer even by inexpert users. Such selfish behavior can cause unfairness and severe performance degradation.

Previous works focused mainly on the detection of nodes that exhibit selfish behavior and their exclusion from the network. The routing metrics proposed in this context, however, do not accurately model the quality of the wireless links.

As a result, the community network is left with several link-layer metrics that fail to accurately choose high-throughput paths between a source and a destination in the presence of selfish nodes that drop packets at the network layer.

To cope with this problem, we designed in [19] the Expected ForWarding counter (EFW), a new cross-layer reliability metric that combines information across the routing and MAC layers to cope with the problem of selfish behavior (i.e., packet dropping) of mesh routers in a WMCN. Our metric combines the direct observation of the routing-layer forwarding behavior of neighbors with the MAC-layer quality of the wireless links in order to allow the routing protocol to select the most reliable and high-performance path.

More specifically, our proposed metric extends a widely used routing metric named Expected Transmission Count (ETX), first proposed in [18], which measures the expected number of transmissions, including retransmissions, needed to correctly send a unicast packet over a wireless link.

Formally, the ETX metric is computed as follows. Let (i, j) be a wireless link established between nodes i and j; p_{ij} and p_{ji} denote the packet loss probability of the wireless link (i, j) in forward and reverse directions, respectively [1]. The probability of a successful transmission on the wireless link (i, j) can therefore be computed as $p^s_{ij} = (1 - p_{ij}) \cdot (1 - p_{ji})$, since in wireless networks based on the IEEE 802.11 protocol the destination must acknowledge each received data frame.

To address the problem caused by the dropping behavior of selfish participants in WMCNs, we combine the link quality measurements captured by the ETX routing metric with the forwarding reliability of a relaying node j by improving the probabilistic model on which ETX is based.

Let p^d_{ij} be the *dropping* probability of a community network node j ($1 - p^d_{ij}$ therefore represents its forwarding probability). Note that, since a network node can drop selectively the traffic sent by its neighbors, the dropping probability of any node j is identified both by the sending node i and the relaying node j. The probability that a packet sent through a node j will be successfully forwarded can therefore be expressed as $p^{fwd}_{ij} = p^s_{ij}(1 - p^d_{ij})$.

Then, the expected number of transmissions necessary to have the packet successfully forwarded (Expected ForWarding counter, EFW) can be measured according to the following equation:

$$EFW = \frac{1}{p^{fwd}_{ij}} = \frac{1}{(1 - p_{ij}) \cdot (1 - p_{ji})} \cdot \frac{1}{(1 - p^d_{ij})} \tag{2.1}$$

The EFW metric is estimated in practice by setting each node in promiscuous mode, so that the mesh router can evaluate the relaying behavior of its neighbors by analyzing the eavesdropped traffic, that is, by computing the fraction of packets that are actually forwarded.

For the sake of clarity, we now illustrate a simple example that points out the improvements obtained by our proposed metric with respect to ETX.

Figure 2.6 shows a network topology composed of four nodes; the number above each arrow represents the link quality measured at the MAC layer by the node at the arc's head, whereas the number above each node indicates its forwarding probability at the network layer.

The values of the ETX and the proposed EFW metrics computed by node N1 are reported in Table 2.2. The ETX metric leads to a poor choice of the best relaying node to reach node N4, since, according to this metric, the cost of path $N1-N2-N4$ is lower than that of $N1-N3-N4$. However, the actual number of transmissions that node N1 must perform using the former path is 22.5% greater than that obtained using the latter.

[1] $(1 - p_{ij})$ and $(1 - p_{ji})$ will be referred to as *link qualities* in forward and reverse direction, respectively.

This simple example shows the necessity to represent the forwarding behavior of network nodes in addition to the link quality to model closely the reliability of a network path.

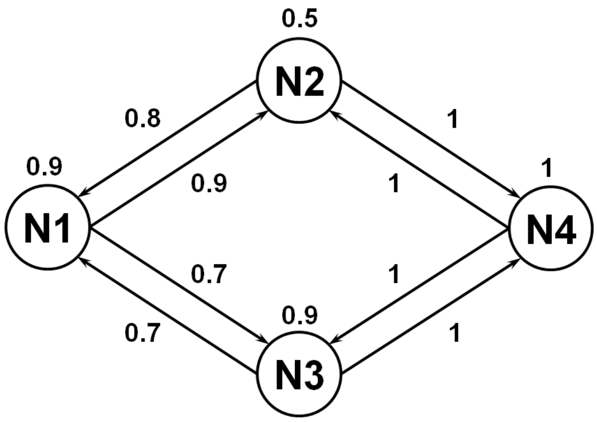


Figure 2.6: Example of network topology. Arrows represent the delivery probabilities in forward $(1 - p_{ij})$ and reverse $(1 - p_{ji})$ directions. The packet dropping rates of nodes N2 and N3 are 0.5 and 0.1, respectively

Table 2.2: ETX and EFW metrics in the example network of Figure 2.6. The cost related to the selected best link is highlighted in bold.

Link	ETX	EFW
N1-N2	**1.39**	2.78
N1-N3	2.04	**2.27**

The EFW metric has been tested both by simulation and real network experiments, and the results demonstrate that the proposed solution increases considerably both the network throughput and fairness with respect to the widely used approach that takes into account only the successful transmissions of the wireless link.

To complement our approach, we then proposed a complete, robust scheme to detect selfish behaviors of mesh routers that participate to the community network, even in the presence of lying nodes (i.e., the so called “bad-mouthing attack”). In this context, each node evaluates the trustworthiness of the other mesh routers by combining the direct observations on the forwarding behavior of neighbor nodes with the *trust* information provided by other mesh routers.

The proposed framework is composed of three core elements: a *monitoring mechanism* (named “watchdog”) able to distinguish between selfish and cooperative actions (i.e., packet dropping and relaying), a *protocol* to exchange trust ratings among the network nodes, and a *trust and reputation model* for quantifying the nodes trustworthiness, filtering out the information likely provided by lying nodes.

Figure 2.7 sketches the architecture of the proposed detection system implemented on all mesh routers of the WMCN.

The monitoring mechanism was implemented exactly as for the EFW metric: each node is set in promiscuous mode, so that it can evaluate the forwarding behavior of its neighbors by

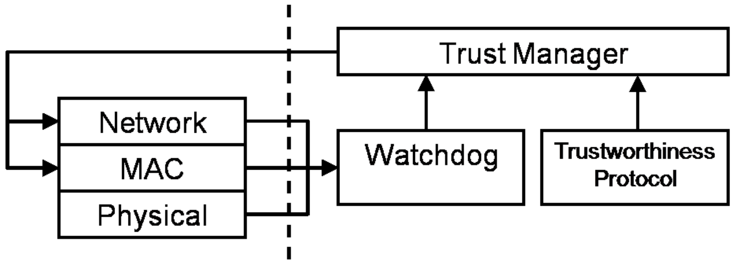


Figure 2.7: Architecture of the proposed detection system.

analyzing the eavesdropped traffic, that is, by verifying that neighbors are actually forwarding packets, and not dropping them [69].

In our trust and reputation model, the direct and indirect observations about the forwarding behavior of mesh routers are represented as vectors of a multi-dimensional space. This representation enables the aggregation of all the observations related to a specific mesh router in a unique trust value. Our proposed reputation model filters out all indirect observations about the forwarding behavior of network nodes that are likely provided by lying nodes.

We performed a thorough numerical evaluation of the proposed framework by simulating typical network topologies and several attack scenarios, and the results show that our scheme offers a very high detection accuracy, even when a high percentage of network nodes provide false trust values. A more detailed discussion of these results can be found in [20].

Chapter 3

Overlay Networks

In this chapter, we summarize the main research contributions related to the planning and management of overlay networks. We first introduce a centralized optimization approach for the overlay network design problem, illustrating at the same time the Service Overlay Network paradigm (Section 3.1). Then, we focus on distributed overlay network management, defining two novel overlay network formation games that lead user clients to form efficient overlay networks in a fully distributed, non-cooperative manner (Section 3.2).

3.1 Service Overlay Network Design

(Publications [25, 26, 27, 28].)

Service Overlay Networks (SONs) have recently emerged as alternative and very promising architectures able to provide end-to-end Quality of Service guarantees in the Internet, while leaving the underlying Internet infrastructure unchanged [21, 22, 23, 24, 70].

A SON is an application-layer network built on top of traditional IP-layer networks. In general, the SON is operated by a third-party ISP that owns a set of overlay nodes residing in the underlying ISP domains. These overlay nodes perform service-specific data forwarding and control functions, and are interconnected by virtual overlay links which correspond to one or more IP-layer links [21].

The service overlay architecture is based on business relationships between the SON, the underlying ISPs, and the users. The SON establishes bilateral service level agreements with the individual underlying ISPs to install overlay nodes and purchase the bandwidth needed for serving its users. On the other hand, the users subscribe to SON services, which will be guaranteed regardless of how many IP domains are crossed by the users' connection. The SON gains from users' subscriptions. Although the quality requirements that a SON must satisfy may be different (e.g. bandwidth, delay, delay jitter, packet loss), we assume they are mapped to an equivalent bandwidth [21, 70]. To assure the bandwidth for the SON, the underlying ISPs have several technical options: they can lease a transmission line to the SON, use bandwidth reservation mechanisms or create a separate Label Switched Path if MPLS [71] is available in their networks.

Obviously, the deployment of Service Overlay Networks can be a capital-intensive investment. It is therefore imperative to develop efficient network design tools that consider the cost recovery issue for a SON. The main costs of SON deployment include the overlay nodes installation cost and the cost of the bandwidth that the SON must purchase from the underlying network domains to support its services.

The topology design problem for Service Overlay Networks has been considered by very few works [70, 72, 73, 74, 75, 76, 77, 78] which make several limiting assumptions:

- the number and location of overlay nodes are pre-determined, while the overlay node placement is a critical issue in the deployment of the SON architecture.
- A full coverage of all traffic demands must be provided, while the main goal of a SON operator would be to maximize its profit by choosing which users to serve based on the expected revenue.
- The capacities of overlay nodes/links are unlimited, thus assuming that the underlying ISPs will always be able to provide bandwidth to the SON.
- Only small network instances are considered, with a limited number of connections and overlay nodes.

Our work overcomes all these limitations by first addressing in [25] the joint user assignment and traffic routing problem, proposing two novel optimization models that determine the optimal assignment of users to access overlay nodes, as well as the capacity reserved for each overlay link, while taking accurate account of traffic routing. The first model minimizes the network installation cost while providing full coverage to all the network's users. The second model maximizes the SON profit by further selecting which users to serve in order to make its operation profitable, and also includes a budget constraint that the SON operator can specify to limit its economic risks in the deployment of the overlay network.

We then extended such models in [26] to consider the more complex SON design problem, where the number and positions of overlay nodes to be deployed are optimized. To this end we presented two SON design models that jointly optimize (1) the number and location of overlay nodes, (2) the user assignment to access overlay nodes, (3) the traffic routing and (4) the capacity dimensioning of overlay links.

The SON design problems are NP-hard, however, the proposed Mixed Integer Linear Programming formulations can be solved to the optimum for realistic-size instances in reasonable time. More specifically, the formulation that considers only the user assignment and routing problem can be solved to the optimum even for large-scale instances in a short computing time.

To tackle large-size instances for the global SON design problem, we proposed two simple but effective heuristic approaches able to provide near-optimal solutions in a reasonable computation time. The proposed algorithms are based on the decomposition of the model into sub-problems and on the solution of the continuous relaxation. 0-1 feasible solutions are then obtained using a randomized rounding technique.

Regrettably, in some scenarios the proposed heuristics are unable to provide a good solution to the SON design problem due, in particular, to huge memory consumption and computational effort. For this reason, we further proposed in [28] an efficient tabu search based approach that uses polynomial size and Very Large-Scale Neighborhoods (VLSN). VLSN is used once the local minimum is reached, to "escape" from it and widen the set of explored solutions; it can therefore be seen as a diversification step for the tabu search. We demonstrated in [28] that the proposed VLSN-based heuristic is able to design efficient overlay networks even in very large-scale topology scenarios.

3.2 Distributed Overlay Network Formation

(Publications [29, 30].)

In many scenarios, the overlay network design is not enforced by a central authority, but arises from the interactions of several self-interested agents: each user client can decide the set of connections to establish.

Network design with selfish users has been the focus of several recent works [79, 80, 81, 82, 83, 84], which have modeled how independent selfish agents can build or maintain a large network by paying for possible edges. Each user's goal is to connect a given set of terminals with the minimum possible cost. Game theory is the natural framework to address the interaction of such self-interested users (or players). A *Nash Equilibrium* is a set of users choices, such that none of them has an incentive to deviate unilaterally; for this reason the corresponding networks are said to be *stable*.

However, Nash equilibria in network design games can be much more expensive than the optimal, centralized solution. This is mainly due to the lack of cooperation among network users, which leads to design costly networks.

Actually, the majority of existing works assume that users are completely non-cooperative. However, this assumption is not entirely realistic, for example when network design involves long-term decisions (e.g., in the case of Autonomous Systems peering relations). Moreover, incentives could be introduced by some external authority (e.g., the overlay administrator) in order to increase the users' cooperation level.

In our work [29, 30], we overcome this limitation by first proposing a novel overlay network design game, the Socially-Aware Network Design (SAND) game, where users are characterized by an objective function that combines both *individual* and *social* concerns in a unified and flexible manner.

More specifically, in the SAND game each player i picks a path from its source node s_i to its destination t_i, minimizing its objective function J^i, which is a combination of its own path cost (the *selfish* component) and the overall network cost, which represents the *social* component. A parameter (α) weights the relative importance of the network cost with respect to the user path cost. Changing the value of α permits to take into account different levels of social awareness or user cooperation.

Formally, the cost function J^i has the following expression:

$$J^i = \sum_{e \in S_i} \pi_e + \alpha \sum_{e \in \cup_j S_j} c_e, \tag{3.1}$$

where the first term takes into account the *selfish* nature of each player, since it is the cost for user i to buy the edges belonging to the chosen path, S_i; in particular, if edge e lies in x_e of the paths used by the whole set of players, then each player choosing such an edge pays a proportional share $\pi_e = \frac{c_e}{x_e}$ of the cost, c_e being the edge cost. On the other hand, the second term represents the total network cost (i.e., the *social* cost).

We investigated systematically in [29, 30] the impact of cooperation among network agents on the system performance, through the determination of bounds on the *Price of Anarchy* (*PoA*), the *Price of Stability* (*PoS*) and the *Reachable Price of Anarchy* (*RPoA*) of the proposed game. They all quantify the loss of efficiency as the ratio between the cost of a specific stable network and the cost of the optimal network, which could be designed by a central authority.

In particular the PoA, first introduced in [85], considers the worst stable network (that with the highest cost), while the PoS [79] considers the best stable network (that with the lowest cost); finally, the $RPoA$ considers only Nash equilibria reachable via best response dynamics from the empty solution [84]. Hence, PoA and $RPoA$ indicate the maximum degradation due to distributed users decisions (anarchy), while the PoS indicates the minimum cost to pay to have a solution robust to unilateral deviations.

Table 3.1 summarizes the bounds we derived for these performance figures, considering a network created by k users, where $\mathcal{H}_k$ is the k-th harmonic number (i.e., $\mathcal{H}_k = \sum_{i=1}^{k} 1/i$).

Table 3.1: Bounds to the Price of Anarchy (PoA), Price of Stability (PoS) and Reachable Price of Anarchy ($RPoA$) for the proposed Socially-Aware Network Design Game.

Metric	PoA	PoS	$RPoA$
Bound	$k(1+\alpha)$	$\frac{\mathcal{H}_k+\alpha}{1+\alpha}$	$k\frac{\alpha+1}{\alpha+\frac{1}{k}}$

Our analytical results show that as α increases, i.e., when users are more sensitive to the social cost, the PoS converges to 1, i.e., the best stable network is more efficient, as expected. Surprisingly, an opposite result holds for the worst case. Indeed, for large α values (highly socially-aware users) the worst stable network can be much more expensive than the networks designed by purely selfish users (the $\alpha = 0$ case).

For this reason, we further proposed in [29, 30] a Stackelberg (leader-follower) approach, the Network Administrator Driven Socially-Aware Network Design game (NAD-SAND), which enables very efficient Nash equilibria, avoiding worst-case scenarios: a leader (e.g., the network administrator) buys an appropriate subset of the network links (i.e., those belonging to the minimum cost generalized Steiner tree [86] covering all source/destination pairs), inducing the followers (the network users) to reach an efficient Nash equilibrium.

More formally, in the NAD-SAND game, the Network Administrator plays first, choosing a subset of network links (referred to as E^{opt}) for which he pays an equal share of their cost, thus providing an incentive for all other "ordinary" players to choose them. The goal is to stimulate all other players to build an efficient and stable network. Then, each player plays exactly as in the SAND game described above, picking a path from its source node s_i to its destination t_i, minimizing its objective function J^i, given in expression (3.1).

Since computing the optimal Stackelberg strategy for the Network Administrator is NP-hard, we presented in our works [29, 30] a simple strategy that achieves consistent performance improvements. Such approach is implemented via the following heuristic:

1. Given the network topology, the network administrator solves a generalized Steiner Tree problem [86], determining the minimum-cost subnetwork such that the source/destination nodes of each player are connected by a path. Let E^{opt} be the set of edges belonging to such optimal subnetwork.

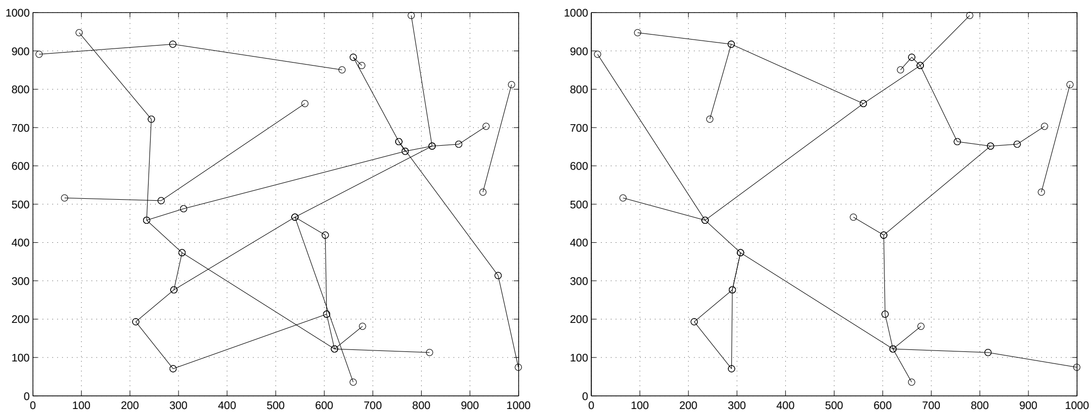
2. The network administrator chooses all links belonging to E^{opt}, thus offering to share eventually their cost with the other players. Therefore, using the notation introduced before, after this step we have $x_e = 1, \forall e \in E^{opt}$ (that is, the network administrator has already chosen all links that are *optimal* from a social point of view).

3. At this point, all the k users play the SAND game, each trying to optimize its own objective function, which is the same of expression (3.1).

The rationale behind the proposed NAD-SAND game is the following: the network administrator tries to motivate all players to use the links that belong to the socially optimal solution by sharing their cost with network users. Our heuristic is very effective, and permits to obtain dramatic performance improvements with respect to the SAND game, as we will illustrate in the following.

Summary of the main results

We now discuss a sample network scenario that shows the effectiveness of our proposed network design approaches. Figure 3.1 shows the networks resulting at the Nash equilibria with the SAND game in a random geometric graph scenario (i.e., a graph where links exist between any two nodes located within a range R, the link cost being equal to its length) with $N = 50$ nodes, range $R = 500$, 20 source/destination pairs, and two different α values (viz., $\alpha = 0$ and $\alpha = 50$), which correspond, respectively, to completely selfish and socially-aware behaviors.



(a) $\alpha = 0$ (b) $\alpha = 50$

Figure 3.1: Nash equilibria obtained by the SAND game in a random geometric network with 50 nodes, $R = 500$, 20 source/destination pairs, and different α values ($\alpha = 0$ and $\alpha = 50$).

We observe that for $\alpha = 50$ the topology is much closer to a tree-like topology than that obtained by completely selfish users ($\alpha = 0$). This is reflected in the total network cost, which is equal to 7046.3 for $\alpha = 0$ and to 5336.2 for $\alpha = 50$, thus resulting in a gain of more than 24%.

Table 3.2 shows the numerical results obtained in the same network scenario. The total network costs are illustrated in the table for both the SAND and NAD-SAND games, while the ILP column reports the optimal network cost. Although there is still room for improvement, in this scenario the SAND game improves consistently the quality of network equilibria with respect to the $\alpha = 0$ case. The NAD-SAND game performs consistently better than the SAND game, lowering the overall network cost and reaching the socially optimal outcome for $\alpha \geq 10$.

Note that we measured the performance of the proposed distributed overlay network formation games in several network topologies, including realistic scenarios where players build an overlay on top of real Internet Service Provider networks, and we observed that socially-aware

Table 3.2: Random geometric graphs; random networks with 50 nodes, $R = 500$ and 20 players: average network costs for the SAND and the NAD-SAND games. The optimal network cost is also reported (the ILP column).

Game	$\alpha = 0$	$\alpha = 1$	$\alpha = 10$	$\alpha = 50$	$\alpha = 100$	$\alpha = 1000$	**ILP**
SAND	6567.73	6074.57	5708.95	5724.18	5736.17	5706.09	**4213.82**
NAD-SAND	5645.44	4675.13	4213.82	4213.82	4213.82	4213.82	

users always generate better networks. Furthermore, we observe that the proposed Stackelberg approach achieves dramatic performance improvements in all the considered scenarios, even for small α values, since it leads most of the times to the optimal (least cost) network. The reader is referred to [30] for more details.

Hence, we can conclude that introducing some incentives to make users more socially-aware can be an effective solution to achieve stable and efficient networks in a distributed way.

Chapter 4

Conclusion and Perspectives

This chapter first presents the conclusions of this manuscript, and then lists a number of perspectives for future work.

4.1 Conclusion

This manuscript presented the main research activities I carried out in the past five years. The main goal of my research activity has been to individuate the principles underlying the design of efficient networks. In this regard, I tackled the research issues related to the main problems that have a significant impact on the performance of wireless multi-hop and overlay networks, with particular attention to channel access, network formation, routing, and network security.

I structured this manuscript in two main chapters corresponding to two classes of contributions: wireless multi-hop networks and overlay networks.

In **Chapter 2** we considered different research issues related to *Wireless Mesh Networks* (WMNs) and *Wireless Mesh Community Networks* (WMCNs); in particular, we focused our attention on the Medium Access Control (MAC) level, the routing layer, and we proposed effective security architectures to protect the integrity and confidentiality of the data exchanged in such networks. Finally, we considered the problem of coping with selfish behaviors exhibited by members of the community network.

We first focused our attention on the *MAC layer* of multi-hop wireless networks, proposing PCD-MAC [5, 7], a Power-Controlled Directional MAC protocol for nodes equipped with adaptive antennas. PCD-MAC uses the standard RTS-CTS-DATA-ACK exchange procedure. The novel difference is the transmission of the RTS and CTS packets in all directions with a tunable power, while the DATA and ACK frames are transmitted directionally at the minimal required power.

We then extended this protocol in the context of multi-channel wireless networks, proposing the Multi-Channel Power-Controlled Directional MAC protocol (MPCD-MAC) [6] for nodes equipped with multiple network interfaces and directional antennas. The novelty of this protocol lies in the transmission of the RTS and CTS packets in all directions on a separate control channel, while the DATA and ACK packets are transmitted only directionally on an available data channel at the minimum required power, taking into account the interference generated on already active connections.

Both protocols achieve significant performance improvements with respect to the most notable solutions proposed in the literature. Furthermore, they only require small variations to the current standard, so that they can be implemented without requiring major hardware modifications.

We then considered the *routing level*, first proposing mathematical models for the Quality of Service routing problem in multi-hop wireless networks with bandwidth constraints [8]. These models were then extended to Wireless Mesh Networks equipped with directional antenna technology, solving the joint routing and scheduling optimization problem in such networks [9].

Finally, we proposed the Directional Deflection Routing (DDR) [5], which is a routing algorithm for wireless multi-hop networks based on a cross-layer approach that is inspired by a routing protocol first proposed for optical networks. Each node maintains a sorted list of next-hop nodes per destination according to paths lengths, and it forwards packets to the first available node in the list. Node availability is obtained by the MAC layer indication on channel status in different directions.

As for wireless network *security*, we first designed two security architectures for wireless multi-hop networks (namely, MobiSEC and DSA-Mesh [10, 11, 12, 13]) which provide authentication and access control of all devices that join the network, as well as the distribution of the cryptographic information used to secure all communications that occur in the backbone of a WMN. We further formulated a network optimization model to determine the optimal placement of the devices that collaboratively perform the authentication and key management services.

To tackle the issue of *selfishness* in Wireless Mesh Community Networks, we designed a novel reliability metric [19], named EFW (Expected ForWarding counter), which combines information across the routing and MAC layers to cope with the problem of selfish behavior (i.e., packet dropping) of mesh routers in a WMCNs. Our metric combines direct observation of routing-layer forwarding behavior of neighbors with the MAC-layer quality of the wireless links in order to allow a routing protocol to select the most reliable and high-performance path. Finally, we proposed a new reputation model [20] to filter out all indirect observations about the forwarding behavior of network nodes that are likely provided by lying nodes.

In **Chapter 3**, dedicated to *overlay networks*, we first focused on a *centralized optimization approach* for the overlay network design problem, with particular application to the Service Overlay Network (SON) paradigm. More specifically, we first proposed two mathematical programming models for the user assignment problem, the traffic routing optimization and the dimensioning of the capacity reserved on overlay links in SONs [25, 27].

We then extended such models in [26] to consider the more complex SON design problem, where the number and positions of overlay nodes to be deployed are optimized. We therefore proposed two novel optimization models for the topology planning of SONs that jointly optimize (1) the number and location of overlay nodes, (2) the user assignment to access overlay nodes, (3) the traffic routing and (4) the capacity dimensioning of overlay links. The first model minimizes the SON installation cost while providing full coverage to all network's users. The second model maximizes the SON operator's profit by further choosing which users to serve, based on the expected gain, and taking into consideration budget constraints. We also introduced two efficient heuristics to get near-optimal solutions for large-scale instances in a reasonable computation time.

Finally, we presented an efficient tabu search based approach [28] that uses polynomial size and Very Large-Scale Neighborhoods (VLSN) to tackle large-scale topology scenarios. In summary, VLSN is used once the local minimum is reached, to “escape” from it and widen the set of explored solutions. We demonstrated the effectiveness of the proposed heuristic in designing efficient overlay networks even in very large-scale topology scenarios.

We then focused on a *fully distributed* approach to the overlay network formation problem, by proposing two novel socially-aware network design games [29, 30]. In the first game, we incorporated a socially-aware component in the users utility functions, while in the second game we used additionally a Stackelberg (leader-follower) approach, where a leader (e.g., the overlay network administrator) architects the desired network buying an appropriate subset of network links, driving in this way the users to overall efficient Nash equilibria. We provided bounds on the Price of Anarchy and other efficiency measures, and studied the performance of the proposed schemes in several network scenarios, including realistic topologies where players build an overlay on top of real Internet Service Provider networks. Numerical results demonstrate that (1) introducing some incentives to make users more socially-aware is an effective solution to achieve stable and efficient networks in a distributed way, and (2) the proposed Stackelberg approach permits to achieve dramatic performance improvements, designing almost always the socially optimal network.

4.2 Perspectives

My work in the past has been focused on some of the most notable research problems related to Wireless Mesh (Community) Networks and overlay networks. I used both a theoretical and a practical approach, complementing theoretical results derived from mathematical formulations with real network observations obtained in experimental testbeds and real-life implementations.

In the next years, I plan to strengthen my research activities with particular attention to some of the most interesting issues that are currently emerging in the wireless community, like for example resource sharing, routing, incentives to cooperation in distributed environments and transport protocols.

As for the research methodology, I will consider more in depth Game Theory applications to telecommunication networks, since Game Theory represents a powerful tool to study distributed systems built by a set of independent actors. In the past years, I applied this technique to study some notable problems, including overlay network formation, resource sharing and pricing in cognitive radio networks. I plan to complement the experimental studies I will perform in the field of Wireless Networks using game theoretical approaches, analyzing in particular:

1. *Resource sharing problems*, where many users (wireless nodes/clients) contend for access to the shared wireless medium; this problem lends itself naturally to a game theoretic formulation. In these medium access control games, selfish users seek to maximize their utility by obtaining an unfair share of access to the channel. This action, though, decreases the ability of other users to access the shared resource. This problem has relevant applications in currently emerging network paradigms, like for example Cognitive Radio Networks, besides immediate applications to Wireless Ad Hoc, Sensor, Mesh and Community Networks.

2. *Routing strategy behaviors*. In particular, I will investigate novel *green* routing schemes, able to obtain energy savings in wireless and wired networks. I will focus mainly on fully distributed approaches, designing incentives for users to form and maintain energy-efficient

networks. This topic will be increasingly important in the next future, since communication networks account for non-negligible energy consumption.

3. *Incentive mechanisms* to improve cooperation in distributed network environments. The establishment of routes in multi-hop wireless networks (including ad hoc networks, wireless mesh and community networks) relies on nodes forwarding packets for one another. However, as we pointed out in Chapter 2, a selfish node, in order to conserve its limited energy or bandwidth resources, could decide not to participate in the forwarding process, thus potentially leading to network collapse. I plan to tackle more in depth this research issue, which is vital for building and maintaining any distributed (wireless) network, by further studying effective incentive mechanisms that stimulate an active participation to the network forwarding process.

4. *Transport protocols.* Designing efficient transport protocols for wireless multi-hop networks is a challenging task, especially in a community environment. The reduced reliability at the network level calls for innovative solutions, based for example on cross-layer approaches, where MAC and routing level information is combined to improve the performance at the transport layer.

Finally, I plan to extend the work on *network formation*, a problem which has become increasingly important given the continued growth of computer networks such as the Internet. Previous works, including mine, have addressed this problem considering only networks designed by self-optimizing (selfish) users, which can be consistently suboptimal. I will therefore formulate the network formation problem as a *cooperative* game, where coalitions (groups of players) coordinate their actions and pool their cost savings. In particular, I will start by investigating a Nash bargaining approach to solve this problem.

This is only a short list of medium term research I intend to develop.

As for my research strategy, I plan to pursue and intensify my research visits to top-level universities and laboratories, with special regard to European centers, in order to establish contacts that will help building consortia for common research projects.

Some research grants I already obtained (listed in my CV), along with project proposals under review, are currently allowing me to build a research team able to contribute to the research issues mentioned above. Part of my effort will be devoted to maintain and reinforce the fund raising activity.

Appendix A

Summary of other works

In this manuscript, I focused on the contributions that form the core of my research work. However, I have been involved in a number of other activities that are related to the work presented in this manuscript. They are briefly described in the following. For more details, the reader is invited to consult the papers and references therein.

Competitive Spectrum Access in Cognitive Radio Networks [87] (with Jocelyne Elias, Eitan Altman, Antonio Capone). Cognitive radio networks provide the capability to share the wireless channel with licensed (primary) users in an opportunistic manner. Primary users have a license to operate in a certain spectrum band; their access can only be controlled by the Primary Operator and is not affected by any other unlicensed (secondary) user. On the other hand, secondary users (SUs) have no spectrum license, and they attempt to exploit the spectral gaps left free by primary users. This work studies the spectrum access problem in cognitive radio networks from a game theoretical perspective. The problem is modeled as a non-cooperative spectrum access game where secondary users access simultaneously multiple spectrum bands left available by primary users, optimizing their objective function which takes into account the congestion level observed on the available spectrum bands. As a key innovative feature with respect to existing works, we model accurately the interference between SUs, capturing the effect of spatial reuse. We demonstrate the existence of the Nash equilibrium, and derive equilibrium flow settings. Finally, we provide numerical results of the proposed spectrum access game in several cognitive radio scenarios, and study the impact of the interference between SUs on the game efficiency.

Dynamic Bandwidth Allocation in Quality of Service Networks [88, 89, 90] (with Jocelyne Elias, Antonio Capone, Guy Pujolle). Efficient dynamic resource provisioning algorithms are necessary to the development and automation of Quality of Service (QoS) networks. The main goal of these algorithms is to offer services that satisfy the QoS requirements of individual users while guaranteeing at the same time an efficient utilization of network resources. In this work we introduce a new service model that provides per-flow bandwidth guarantees, where users subscribe for a guaranteed rate; moreover, the network periodically individuates unused bandwidth and proposes short-term contracts where extra-bandwidth is allocated and guaranteed exclusively to users who can exploit it to transmit at a rate higher than their subscribed rate. To implement this service model we propose a dynamic provisioning architecture for intra-domain Quality of Service networks. We develop a set of dynamic on-line bandwidth allocation algorithms that take explicitly into account traffic statistics and users utility functions to increase users benefit and network revenue. Further, we propose a mathematical formulation of the extra-bandwidth allocation problem that maximizes network revenue. The solution of this model allows to obtain an upper bound on the performance achievable by any on-line bandwidth allocation algorithm. We demonstrate through simulation in realistic network scenarios that the proposed dynamic allocation algorithms are superior to static provisioning in providing resource allocation both in terms of total accepted load and network revenue, and they approach, in several network scenarios, the ideal performance provided by the mathematical model.

Enhanced Protection Techniques for Optical Networks [91, 92, 93] (with Wissam Fawaz, Ken Chen, Guy Pujolle). One of the major concerns of optical network operators is related to improving the availability of services provided to their highest-class clients. Achieving this objective is possible through managing faults using the different classical protection schemes, namely the so-called dedicated and shared protection schemes. However, the majority of the work concerning protection schemes has considered the primary connections as equally important when contending for the use of the backup resources. As a main contribution, we therefore propose an improvement of the existing protection schemes through the introduction of relative priorities among the different primary connections contending for the access to the protection path. To evaluate numerically the benefits of the service differentiation feature introduced in our proposal, we first develop a mathematical model, based on which we derive explicit expressions for the average connection availabilities that result from both the classical protection schemes and the proposed priority-aware one. Through this model, we show how the availability of the highest-class clients is improved when deploying the proposed priority- aware protection scheme. Finally, we develop a simulation study, which shows that the priority-aware protection strategy satisfies service-availability requirements in a cost-effective manner compared with the classical protection schemes

Dynamic Online QoS Routing Schemes [94, 95] (with Antonio Capone, Luigi Fratta). Several dynamic QoS routing techniques have been recently proposed for new IP networks based on label forwarding; however, no extensive performance evaluation and comparison is available in the literature. This work analyzes their performance referring to several networks scenarios. In order to set an absolute evaluation of the performance quality we have obtained the ideal performance of any routing scheme using a novel and flexible mathematical programming model that assumes the knowledge of arrival times and duration of the connections offered to the network. This model is based on an extension of the maximum multi-commodity flow problem. Being an integer linear programming model, its complexity is quite high and its evaluation is constrained to networks of limited size. To overcome the computational complexity we have defined an approximate model, based on the multi-class Erlang formula and the minimum multi-commodity cut problem, that provides an upper bound to the routing scheme performance. The performance presented in this work, evaluated by measuring the connection rejection probability, shows that the schemes considered reach, in several scenarios, the ideal performance, showing that no much gain is left for alternate new schemes.

Appendix B

List of publications

International Journals

1. F. Martignon, S. Paris, I. Filippini, L. Chen, A. Capone, “Efficient and Truthful Bandwidth Allocation in Wireless Mesh Community Networks,” *IEEE/ACM Transactions on Networking*, article in press, November 2013.

2. J. Elias, F. Martignon, L. Chen, E. Altman, “Joint Operator Pricing and Network Selection Game in Cognitive Radio Networks: Equilibrium, System Dynamics and Price of Anarchy,”, *IEEE Transactions on Vehicular Technology*, vol. 62, issue 9, pages 1-14, November 2013.

3. S. Paris, C. Nita-Rotaru, F. Martignon, A. Capone, “Cross-Layer Metrics for Reliable Routing in Wireless Mesh Networks,”, *IEEE/ACM Transactions on Networking*, vol. 21, issue 3, pages 1003-1016, June 2013.

4. J. Elias, F. Martignon, A. Capone, E. Altman, Non-Cooperative Spectrum Access in Cognitive Radio Networks: a Game Theoretical Model, Elsevier Computer Networks, vol. 55, issue 17, pages 3832-3846, December 2011.

5. J. Elias, F. Martignon, and G. Carello, “Very Large-Scale Neighborhood Search Algorithms for the Design of Service Overlay Networks,” *Telecommunication Systems*, vol. 49, issue 4, pages 391-408, June 2012.

6. F. Martignon, S. Paris, and A. Capone, “DSA-Mesh: a Distributed Security Architecture for Wireless Mesh Networks,” *Wiley Security and Communication Networks*, vol. 4, issue 3, pages 242-256, March 2011.

7. J. Elias, F. Martignon, K. Avrachenkov, and G. Neglia, “A Game Theoretic Analysis of Network Design with Socially-Aware Users,” *Elsevier Computer Networks*, vol. 55, issue 1, pages 106-118, January 2011.

8. F. Martignon, “Multi-Channel Power-Controlled Directional MAC for Wireless Mesh Networks,” *Wireless Communications and Mobile Computing*, vol. 11, issue 1, pages 90-107, January 2011.

9. S. Paris, C. Nita-Rotaru, A. Capone, and F. Martignon, “A Cross-Layer Reliability Metric for Wireless Mesh Networks with Selfish Participants,” *ACM Mobile Computing and Communications Review*, vol. 14, issue 3, 2010.

10. F. Martignon, S. Paris, and A. Capone, “Design and Implementation of MobiSEC: a Complete Security Architecture for Wireless Mesh Networks,” *Elsevier Computer Networks*, vol. 53(12), pp. 2192–2207, August 2009.

11. A. Capone, J. Elias, and F. Martignon, “Routing and Resource Optimization in Service Overlay Networks,” *Elsevier Computer Networks*, vol. 53(2), pp. 180–190, February 2009.

12. A. Capone, J. Elias, and F. Martignon, "Models and Algorithms for the Design of Service Overlay Networks," *IEEE Transactions on Network and Service Management*, vol. 5(3), pp. 143–156, September 2008.

13. A. Capone, F. Martignon, and L. Fratta, "Directional MAC and Routing Schemes for Power Controlled Wireless Mesh Networks with Adaptive Antennas," *Elsevier Ad Hoc Networks*, vol. 6(6), pp. 936–952, August 2008.

14. J. Elias, F. Martignon, A. Capone, and G. Pujolle, "A New Approach to Dynamic Bandwidth Allocation in Quality of Service Networks: Performance and Bounds," *Elsevier Computer Networks*, vol. 51(10), pp. 2833–2853, 11 July 2007.

15. A. Capone and F. Martignon, "A Multi-Commodity Flow Model for Optimal Routing in Wireless MESH Networks," *Journal of Networks*, vol. 2(3), pp. 1–5, June 2007.

16. J. Elias, F. Martignon, A. Capone, and G. Pujolle, "Distributed Algorithms for Dynamic Bandwidth Provisioning in Communication Networks," *Journal of Communications*, vol. 1(7), pp. 47–56, November-December 2006.

17. W. Fawaz, F. Martignon, K. Chen, and G. Pujolle, "A Novel Fault Management Approach for DWDM Optical Networks," *ACM International Journal of Network Management*, vol. 16(5), pp. 337–349, September-October 2006.

18. A. Capone, L. Fratta, and F. Martignon, "Dynamic Online QoS Routing Schemes: Performance and Bounds," *Elsevier Computer Networks*, vol. 50(7), pp. 966–981, 15 May 2006.

19. A. Capone, L. Fratta, and F. Martignon, "Bandwidth Estimation Schemes for TCP over Wireless Networks," *IEEE Transactions on Mobile Computing*, vol. 3(2), pp. 129–143, April-June 2004.

20. A. Capone, L. Fratta, and F. Martignon, "Dynamic Routing of Bandwidth Guaranteed Connections in MPLS Networks," *International Journal on Wireless and Optical Communications*, vol. 1(1), pp. 75–86, June 2003.

Patent

1. A. Capone, F. Martignon, and F. Borgonovo, "Distributed Bandwidth Allocation Method for Passive Networks with CSMA/CD Access," Patent number BG06A000022, filed on April 28, 2006, Italy.

International Conferences

1. M. Mangili, F. Martignon, A. Capone, "A Comparative Study of Content-Centric and Content-Distribution Networks: Performance and Bounds," in *Proceedings of IEEE Globecom 2013*, Atlanta, GA, USA, December 2013.

2. M. Mangili, F. Martignon, S. Paris, A. Capone, "Efficient Joint Bandwidth and Cache Leasing in Information Centric Networks," in *Proceedings of IEEE Globecom 2013*, Atlanta, GA, USA, December 2013.

3. S. Paris, F. Martignon, I. Filippini, L. Chen, "A Bandwidth Trading Marketplace for Mobile Data Offloading," in *Proceedings of IEEE INFOCOM 2013*, Turin, Italy, April 2013

4. A. Barbato, A. Capone, L. Chen, F. Martignon, S. Paris, "A Power Scheduling Game for Reducing the Peak Demand of Residential Users," in *Proceedings of IEEE GreenComm 2013 (IEEE Conference on Green Communications)*, October 2013.

5. S. Paris, F. Martignon, I. Filippini, A. Capone, "A Truthful Auction for Access Point Selection in Heterogeneous Mobile Networks," in *Proceedings of ICC 2012*, Ottawa, Canada, June 2012.

6. J. Elias, F. Martignon, E. Altman, "Joint Pricing and Cognitive Radio Network Selection: a Game Theoretical Approach," in *Proceedings of WiOpt 2012*, Paderborn, Germany, May 2012.
7. F. Martignon, S. Paris, I. Filippini, A. Capone, "Efficient Bandwidth Allocation in Wireless Community Networks," in *Proceedings of Wireless Days 2011*, Niagara Falls, Ontario, Canada, October 2011.
8. S. Paris, F. Martignon, I. Filippini, A. Capone, "A Bandwidth Marketplace for Heterogeneous Mobile Networks," in *Proceedings of the International Conference on NETwork Games, COntrol and OPtimization Wireless Days (NetGCoop 2011)*, Paris, France, October 2011.
9. F. Martignon, S. Paris, A. Capone, "Optimal Node Placement in Distributed Wireless Security Architectures," in *Proceedings of Networking 2011*, Valencia, Spain, May 2011
10. K. Avrachenkov, J. Elias, F. Martignon, G. Neglia, L. Petrosyan, "A Nash bargaining solution for Cooperative Network Formation Games," in *Proceedings of Networking 2011*, Valencia, Spain, May 2011
11. S. Paris, C. Nita-Rotaru, F. Martignon, A. Capone, "EFW: A Cross-Layer Metric for Reliable Routing in Wireless Mesh Networks with Selfish Participants," in *Proceedings of the 30th IEEE Conference on Computer Communications (INFOCOM 2011)*, Shangai, China, April 2011.
12. J. Elias, F. Martignon, A. Capone, and E. Altman, "Competitive Interference-aware Spectrum Access in Cognitive Radio Networks," *Proc. of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt 2010)*, Avignon, France, June 2010.
13. J. Elias and F. Martignon, "Joint Spectrum Access and Pricing in Cognitive Radio Networks with Elastic Traffic," in *IEEE International Conference on Communications (ICC 2010)*, Cape Town, South Africa, May 2010.
14. J. Elias and F. Martignon, "Joint QoS Routing and Dynamic Capacity Dimensioning with Elastic Traffic: A Game Theoretical Perspective," in *IEEE International Conference on Communications (ICC 2010)*, Cape Town, South Africa, May 2010.
15. J. Elias, F. Martignon, K. Avrachenkov, and G. Neglia, "Socially-Aware Network Design Games," *Proc. of the 29th IEEE Conference on Computer Communications (INFOCOM 2010)*, March 2010, San Diego, CA, USA.
16. E. Altman, J. Elias, and F. Martignon, "A Game Theoretic Framework for joint Routing and Pricing in Networks with Elastic Demands," in *Proc. of the 4th International Conference on Performance Evaluation Methodologies and Tools (VALUETOOLS 2009)*, Pisa, Italy, October 2009.
17. F. Martignon, S. Paris, and A. Capone, "A Framework for Detecting Selfish Misbehavior in Wireless Mesh Community Networks," *Proc. of the 5th ACM International Symposium on QoS and Security for Wireless and Mobile Networks, (Q2SWinet 2009)*, Tenerife, Spain, October 2009.
18. F. Martignon and S. Paris, "Experimental Study of Security Architectures for Wireless Mesh Networks," *Proc. of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON 2009*, Rome, Italy, June 2009.
19. F. Martignon, S. Paris, and A. Capone, "MobiSEC: A Novel Security Architecture for Wireless Mesh Networks," *Proc. of the 4th ACM International Symposium on QoS and Security for Wireless and Mobile Networks, (Q2SWinet 2008)*, Vancouver, Canada, October 2008.
20. A. Capone, I. Filippini, and F. Martignon, "Joint Routing and Scheduling Optimization in Wireless Mesh Networks with Directional Antennas," *Proc. of the IEEE International Conference on Communications (ICC 2008)*, Beijing, China, May 2008.

21. A. Capone, J. Elias, and F. Martignon, "Optimal Design of Service Overlay Networks," *Proc. of the 4th International Workshop on QoS in Multiservice IP Networks (QoS-IP 2008)*, Venice, Italy, 13-15 February 2008.
22. J. Elias, F. Martignon, and A. Capone, "An Efficient Dynamic Bandwidth Allocation Algorithm for Quality of Service Networks," in *Autonomic Networking 2006 (INTELLCOMM 2006)*, Paris, France, Sept. 27-29, 2006, also published in Springer Lecture Notes in Computer Science vol. 4195.
23. A. Capone, J. Elias, F. Martignon, and G. Pujolle, "Dynamic Resource Allocation in Communication Networks," *Proc. of Networking 2006*, Coimbra, Portugal, 15-19 May 2006.
24. A. Capone, J. Elias, F. Martignon, and G. Pujolle, "Dynamic Resource Allocation in Quality of Service Networks," *Springer Lecture Notes in Computer Science*, vol. 3883(6), May 2006.
25. A. Capone and F. Martignon, "Power-Controlled Directional Medium Access Control for Wireless Mesh Networks," *Springer Lecture Notes in Computer Science*, vol. 3883(6), pp. 34–46, May 2006.
26. A. Capone, J. Elias, F. Martignon, and G. Pujolle, "Distributed Dynamic Bandwidth Provisioning in Quality of Service Networks," *in Proc. of the 3rd EuroNGI Workshop on QoS and Traffic Control*, ENS, Paris, France, 7-9 December, 2005.
27. W. Fawaz, F. Martignon, K. Chen, and G. Pujolle, "A Novel Protection Scheme for QoS Aware WDM Networks," *Proc. of the IEEE International Conference on Communications (ICC 2005)*, Seoul, Korea, May 2005.
28. W. Fawaz, F. Martignon, K. Chen, and G. Pujolle, "A Priority-Aware Protection Technique for Quality of Service Enabled WDM Networks," *Proc. of Networking 2005*, Waterloo, Ontario, Canada, May 2005.
29. W. Fawaz, F. Martignon, K. Chen, and G. Pujolle, "Une Technique de Protection à Base de Priorité pour Les Réseaux Optiques WDM," in *CFIP'05*, March 2005, Bordeaux, France.
30. A. Capone, L. Fratta, and F. Martignon, "On the Performance of Dynamic Online QoS Routing Schemes," in *Proc. of QoS-IP 2005*, Catania, Italy, February 2005.
31. F. Martignon and L. Fratta, "Loss Differentiation Schemes for TCP over Wireless Networks," in *Proc. of QoS-IP 2005*, Catania, Italy, February 2005.
32. F. Martignon, "Improving TCP Performance over Wireless Networks using Loss Differentiation Algorithms," in *Proc. of IEEE MWCN'04*, Paris, October 2004.
33. A. Capone and F. Martignon, "Analysis of Dynamic Quality of Service Routing Algorithms," *Proc. of the IEEE International Communications Conference (ICC 2004)*, Paris, France, June 2004.
34. S. Bregni, D. Caratti, and F. Martignon, "Enhanced Loss Differentiation Algorithms for Use in TCP Sources over Heterogeneous Wireless Networks," in *IEEE Global Communications Conference (Globecom 2003)*, December 2003, San Francisco, Ca, USA.
35. A. Capone, L. Fratta, and F. Martignon, "Virtual Flow Deviation: Dynamic Routing of Bandwidth Guaranteed Connections," in *Proc. of the 2nd International Workshop on Quality of Service in Multiservice IP Networks*, Milan, Italy, February 2003.
36. A. Capone, L. Fratta, and F. Martignon, "Enhanced Bandwidth Estimation Algorithms in the TCP Congestion Control Scheme," in *Proc. of IFIP Conference on Network Control and Engineering for QoS, Security and Mobility (NET-CON 2002)*, Paris, October 2002.
37. F. Martignon and A. Capone, "TCP with Bandwidth Estimation over Wireless Networks," *IEEE VTC Fall 2002*, Vancouver, Canada, September 2002.
38. A. Capone and F. Martignon, "Bandwidth Estimates in the TCP Congestion Control Scheme," *Tyrrhenian International Workshop on Digital Communications*, Taormina, Italy, September 2001.

References

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47(4), pp. 445–487, March 2005.

[2] D. Johnson, D. Maltz, J. Broch, *et al.*, "DSR: The Dynamic Source Routing Protocol for Multi-hop Wireless Ad Hoc Networks," *Ad Hoc Networking*, vol. 5, pp. 139–172, 2001.

[3] C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," *RFC 3561*, July 2003.

[4] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," *RFC 3626*, October 2003.

[5] A. Capone, F. Martignon, and L. Fratta, "Directional MAC and Routing Schemes for Power Controlled Wireless Mesh Networks with Adaptive Antennas," *Elsevier Ad Hoc Networks*, vol. 6(6), pp. 936–952, August 2008.

[6] F. Martignon, "Multi-Channel Power-Controlled Directional MAC for Wireless Mesh Networks," *Wireless Communications and Mobile Computing*, article in press, September 2009.

[7] A. Capone and F. Martignon, "Power-Controlled Directional Medium Access Control for Wireless Mesh Networks," *Springer Lecture Notes in Computer Science*, vol. 3883(6), pp. 34–46, 2006.

[8] A. Capone and F. Martignon, "A Multi-Commodity Flow Model for Optimal Routing in Wireless MESH Networks," *Journal of Networks*, vol. 2(3), pp. 1–5, June 2007.

[9] A. Capone, I. Filippini, and F. Martignon, "Joint Routing and Scheduling Optimization in Wireless Mesh Networks with Directional Antennas," *Proc. of the IEEE International Conference on Communications (ICC 2008)*, Beijing, China, May 2008.

[10] F. Martignon, S. Paris, and A. Capone, "Design and Implementation of MobiSEC: a Complete Security Architecture for Wireless Mesh Networks," *Elsevier Computer Networks*, vol. 53(12), pp. 2192–2207, August 2009.

[11] F. Martignon and S. Paris, "Experimental Study of Security Architectures for Wireless Mesh Networks," *Proc. of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON 2009*, Rome, Italy, June 2009.

[12] F. Martignon, S. Paris, and A. Capone, "MobiSEC: A Novel Security Architecture for Wireless Mesh Networks," *Proc. of the 4th ACM International Symposium on QoS and Security for Wireless and Mobile Networks, (Q2SWinet 2008)*, Vancouver, Canada, October 2008.

[13] F. Martignon, S. Paris, and A. Capone, "DSA-Mesh: a Distributed Security Architecture for Wireless Mesh Networks," *Wiley Security and Communication Networks*, article in press, October 2009.

[14] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. Agrawal, "Wireless Mesh Networks: Current Challenges and Future Directions of Web-In-The-Sky," *IEEE Wireless Communications*, vol. 14(4), pp. 79–89, 2007.

[15] P. Antoniadis, B. Le Grand, A. Satsiou, L. Tassiulas, R. Aguiar, J. Barraca, and S. Sargento, "Community building over neighborhood wireless mesh networks," *IEEE Technology and Society Magazine*, vol. 27(1), no. 1, no. 1, pp. 48–56, 2008.

[16] I. Aad, J.-P. Hubaux, and E. Knightly, "Impact of denial of service attacks on ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 16(4), pp. 791–802, August 2008.

[17] A. Kuzmanovic and E. W. Knightly, "Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants," *IEEE/ACM Transactions on Networking*, vol. 14(4), pp. 683–696, 2006.

[18] D. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing," *Wireless Networks*, vol. 11(4), pp. 419–434, 2005.

[19] S. Paris, C. Nita-Rotaru, A. Capone, and F. Martignon, "A Cross-Layer Reliability Metric for Wireless Mesh Networks with Selfish Participants," *Proc. of the 16th Annual International Conference on Mobile Computing and Networking (MobiCom 2010), Poster Session*, Chicago, Illinois, USA, September 2010.

[20] F. Martignon, S. Paris, and A. Capone, "A Framework for Detecting Selfish Misbehavior in Wireless Mesh Community Networks," *Proc. of the 5th ACM International Symposium on QoS and Security for Wireless and Mobile Networks, (Q2SWinet 2009)*, Tenerife, Spain, October 2009.

[21] Z. Duan, Z.-L. Zhang, and Y. Hou, "Service Overlay Networks: SLAs, QoS, and Bandwidth Provisioning," *IEEE/ACM Transactions on Networking*, pp. 870–883, vol. 11(6), December 2003.

[22] Z. Li and P. Mohapatra, "QRON: QoS-aware Routing in Overlay Networks," *IEEE Journal on Selected Areas in Communications*, pp. 29–40, vol. 22(1), January 2004.

[23] L. Subramanian, I. Stoica, H. Balakrishnan, and R. H. Katz, "OverQoS: Offering Internet QoS Using Overlays," in *Proc. of the 1st Workshop on Hot Topics in Networks HotNets-I*, Princeton, New Jersey, USA, October 2002.

[24] J. Touch and S. Hotz, "The X-Bone," in *Proc. of the 3rd Global Internet Mini-Conference*, pp. 75–83, Sydney, Australia, 1998.

[25] A. Capone, J. Elias, and F. Martignon, "Routing and Resource Optimization in Service Overlay Networks," *Elsevier Computer Networks*, vol. 53(2), pp. 180–190, February 2009.

[26] A. Capone, J. Elias, and F. Martignon, "Models and Algorithms for the Design of Service Overlay Networks," *IEEE Transactions on Network and Service Management*, vol. 5(3), pp. 143–156, September 2008.

[27] A. Capone, J. Elias, and F. Martignon, "Optimal Design of Service Overlay Networks," *Proc. of the 4th International Workshop on QoS in Multiservice IP Networks (QoS-IP 2008)*, Venice, Italy, 13-15 February 2008.

[28] J. Elias, F. Martignon, and G. Carello, "Very Large-Scale Neighborhood Search Algorithms for the Design of Service Overlay Networks," *Telecommunication Systems*, vol. 50(2), June 2012.

[29] J. Elias, F. Martignon, K. Avrachenkov, and G. Neglia, "Socially-Aware Network Design Games," *Proc. of the 29th IEEE Conference on Computer Communications (INFOCOM 2010)*, March 2010, San Diego, CA, USA.

[30] J. Elias, F. Martignon, K. Avrachenkov, and G. Neglia, "A Game Theoretic Analysis of Network Design with Socially-Aware Users," *Elsevier Computer Networks*, article in press, July 2010.

[31] P. Kyasanur and N. Vaidya, "Routing and Link-Layer Protocols for Multi-Channel Multi-Interface ad Hoc Wireless Networks," *Mobile Computing and Communications Review*, vol. 10(1), pp. 31–43, January 2006.

[32] F. Fitzek, D. Angelini, G. Mazzini, and M. Zorzi, "Design and performance of an enhanced IEEE 802.11 MAC protocol for multihop coverage extension," *IEEE Wireless Communications*, vol. 10(6), pp. 30-39, December 2003.

[33] R. Ramanathan, J. Redi, C. Santivanez, D. Wiggins, and S. Polit, "Ad hoc networking with directional antennas: A complete system solution," *IEEE Journal on Selected Areas in Communications (JSAC)*, pp. 496–506, vol. 23(3), March 2005.

[34] A. Muqattash and M. Krunz, "A Distributed Transmission Power Control Protocol for Mobile Ad Hoc Networks," in *IEEE Transactions on Mobile Computing*, pp. 113–128, vol. 3(2), April-June 2004.

[35] E.-S. Jung and N. Vaidya, "A Power Control MAC Protocol for Ad Hoc Networks," in *Wireless Networks*, pp. 578–587, vol. 11(1), January 2005.

[36] G. Li, L. Yang, W. Conner, and B. Sadeghi, "Opportunities and Challenges for Mesh Networks Using Directional Antennas," in *WiMESH'05*, September 2005, Santa Clara, California, USA.

[37] R. Choudhury, R. Ramanathan, and N. Vaidya, "Using Directional Antennas for Medium Access Control in Ad Hoc Networks," *Proc. of ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, Atlanta, Georgia, USA, September 23-28 2002.

[38] J. Mo, H.-S. So, and J. Walrand, "Comparison of Multichannel MAC Protocols," in *IEEE Transactions on Mobile Computing*, pp. 50–65, vol. 7(1), January 2008.

[39] J. So and N. Vaidya, "Multi-channel MAC for ad hoc networks: handling multi-channel hidden terminals using a single transceiver," *Proc. of the 5th ACM international symposium on Mobile ad hoc networking and computing*, pp. 222–233, May 2004.

[40] Z. Tang and J. Garcia-Luna-Aceves, "Hop-Reservation Multiple Access (HRMA) for Ad Hoc Networks," *Proc. of IEEE INFOCOM*, vol. 3, pp. 1402–1406, September 1999.

[41] P. Bahl, R. Chandra, and J. Dunagan, "SSCH: slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks," *Proc. of the 10th annual international conference on Mobile computing and networking (MobiCom 2004)*, pp. 216–230, September 2004.

[42] A. Arora and M. Krunz, "Power-controlled medium access for ad hoc networks with directional antennas," *Ad Hoc Networks*, vol. 5(2), pp. 145–161, March 2007.

[43] P.-J. Wu and C.-N. Lee, "Connection-oriented multi-channel MAC protocol for ad-hoc networks," in *Computer Communications*, pp. 169–178, vol. 32(1), January 2009.

[44] A. Nasipuri, J. Zhuang, and S. Das, "A multichannel CSMA MAC protocol for multihop wireless networks," *Proc. of IEEE INFOCOM*, New York, NY, USA, March 1999.

[45] P. Kyasanur, J. Padhye, and P. Bahl, "On the efficacy of separating control and data into different frequency bands," *Proc. of the 2nd International Conference on Broadband Networks*, vol. 1, pp. 602–611, October 2005.

[46] S. Wu, Y. Tseng, C. Lin, and J. Sheu, "A Multi-channel Mac Protocol with Power Control for Multi-hop Mobile Ad Hoc Networks," *The Computer Journal*, vol. 45(1), pp. 101–110, 2002.

[47] A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, "A multi-radio unification protocol for IEEE 802.11 wireless networks," *Proc. of the International Conference on Broadband Networks (BroadNets 2004)*, California, USA, October 2004.

[48] Y. Ko and N. Vaidya, "Medium Access Control Protocols Using Directional Antennas in Ad Hoc Networks," *Proc. of IEEE INFOCOM*, Tel-Aviv, Israel, March 2000.

[49] T. Korakis, G. Jakllari, and L. Tassiulas, "A MAC Protocol for full exploitation of Directional Antennas in Ad Hoc Wireless Networks," *In ACM MobiHoc 2003*, pp. 98–107, June 1-3, Annapolis, Maryland, USA 2003.

[50] M. Takai, J. Martin, A. Ren, and R. Bagrodia, "Directional Virtual Carrier Sensing for Directional Antennas in Mobile Ad Hoc Networks," in *ACM MobiHoc 2002*, Lausanne, Switzerland, June 2002.

[51] K. Kobayashi and M. Nakagawa, "Spatially Divided Channel Scheme using Sectored Antennas for CSMA/CA - "Directional CSMA/CA"," *Proc. of IEEE PIMRC*, London, September 2000.

[52] M. Sekido, M. Takata, M. Bandai, and T. Watomabe, "Directional NAV Indicators and Orthogonal Routing for Smart Antenna Based Ad Hoc Networks," *Proc. of IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW)*, Columbus, USA, June 6-10 2005.

[53] N. Fahmy, T. Todd, and V. Kezys, "Ad Hoc Networks With Smart Antennas Using IEEE 802.11 - Based Protocols," *Proc. of the IEEE International Conference on Communications (ICC 2002)*, New York City, NY, April-May 2002.

[54] R. Jain, *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation and Modeling.* New York: Wiley, 1991.

[55] K. Jain, J. Padhye, V. Padmanabhan, and L. Qiu, "Impact of interference on multi-hop wireless network performance," in *Proc. of ACM Mobicom 2003*, San Diego, California, USA, September 2003.

[56] M. Kodialam and T. Nandagopal, "Characterizing the achievable rates in multihop wireless networks," in *Proceedings of ACM Mobicom 2003*, San Diego, California, USA, September 2003.

[57] A. Raniwala, K. Gopalan, and T. Chiueh, "Centralized channel assignment and routing algorithms for multi-channel wireless mesh networks," in *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 8(2), pp. 50–65, April 2004.

[58] A. Capone, L. Coletti, and M. Zambardi, "Routing in multi-hop wireless networks: New model and algorithm," in *Proc. of 3rd International Workshop on QoS in Multiservice IP Networks, QoS-IP 2005*, Catania, Italy, February 2005.

[59] M. Kodialam and T. Nandagopal, "Characterizing the Capacity Region in Multi-Radio Multi-Channel Wireless Mesh Networks," in *Proc. of ACM Mobicom 2005*, Cologne, Germany, August 28 - September 2, 2005.

[60] S. Chakrabarti and A. Mishra, "Qos issues in ad hoc wireless networks," *IEEE Communications Magazine*, vol. 39(2), pp. 142–148, February 2001.

[61] C. Lin and J.-S. Liu, "Qos routing in ad hoc wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 17(8), pp. 1426–1438, August 1999.

[62] A. Capone and G. Carello, "Scheduling Optimization in Wireless MESH Networks with Power Control and Rate Adaptation," in *IEEE SECON*, 2006.

[63] F. Borgonovo and L. Fratta, "Deflection Networks: architectures for metropolitan and wide area networks," *Computer Networks and ISDN Systems*, vol. 24(2), April 1992.

[64] G. Albertengo, F. Borgonovo, P. Civera, L. Fratta, R. L. Cigno, G. Panizzardi, G. Piccinini, and M. Zamboni, "Deflection Networks: principles, implementation, services," *European Transactions on Telecommunication and Related Technologies*, vol. 3(2), March-April 1992.

[65] M. Pearlman, Z. Haas, P. Sholander, and S. Tabrizi, "On the Impact of Alternate Path Routing for Load Balancing in Mobile Ad Hoc Networks," in *ACM MobiHoc*, Boston, Massachusetts, USA, August 2000.

[66] R. Krishnan and J. Silvester, "Choice of Allocation Granularity in Multipath Source Routing Schemes," in *IEEE Infocom'93*, March 1993, San Francisco, California, USA.

[67] T. Dierks and C. Allen, "The TLS protocol version 1.0," *RFC 2246*, January 1999.

[68] S. Roy, D. Koutsonikolas, S. Das, and Y. Hu, "High-Throughput Multicast Routing Metrics in Wireless Mesh Networks," *Ad Hoc Networks*, vol. 6(6), pp. 878–899, 2008.

[69] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *ACM MobiCom*, pp. 255–265, 2000.

[70] H. Tran and T. Ziegler, "A design framework towards the profitable operation of service overlay networks," *Computer Networks*, pp. 94–113, vol. 51(1), 2007.

[71] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," in *RFC 3031*, January 2001.

[72] S. L. Vieira and J. Liebeherr, "Topology Design for Service Overlay Networks with Bandwidth Guarantees," in *Proc. of the 12th IEEE International Workshop on Quality of Service, IWQoS*, pp. 211–220, Montreal, Canada, June 2004.

[73] Z. Li and P. Mohapatra, "On investigating overlay service topologies," *Computer Networks*, pp. 54–68, vol. 51(1), 2007.

[74] J. Han, D. Waston, and F. Jahanian, "Topology Aware Overlay Networks," in *Proc. of IEEE Infocom'05*, Miami, Florida, 13-17 March 2005.

[75] J. Fan and M. Ammar, "Dynamic Topology Configuration in Service Overlay Networks: A Study of Reconfiguration Policies," in *Proc. of IEEE Infocom'06*, Barcelona, Spain, April 2006.

[76] S. Shi and J. Turner, "Placing servers in overlay networks," in *Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2002)*, San Diego, CA, July 2002.

[77] B. Vleeschauwer, F. Turck, B. Dhoedt, and P. Demeester, "On the construction of QoS enabled overlay networks," in *Proc. of the 5th International Workshop on Quality of future Internet Services (QofIS04)*, pp. 164–173, Barcelona, Spain, October 2004.

[78] S. Roy, H. Pucha, Z. Zhang, Y. Hu, and L. Qiu, "Overlay Node Placement: Analysis, Algorithms and Impact on Applications," in *Proc. of the 27th International Conference on Distributed Computing Systems*, Toronto, Canada, June 2007.

[79] E. Anshelevich, A. Dasgupta, J. Kleinberg, E. Tardos, T. Wexler, and T. Roughgarden, "The price of stability for network design with fair cost allocation," in *Proc. of the 45th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 295–304, Rome, Italy, October 17-19, 2004.

[80] E. Anshelevich, A. Dasgupta, E. Tardos, and T. Wexler, "Near-optimal network design with selfish agents," in *Proc. of the 35th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 511–520, San Diego, CA, USA, 2003.

[81] H.-L. Chen and T. Roughgarden, "Network design with weighted players," in *Proc. of the 18th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA'06)*, Cambridge, MA, USA, July 30-August 2, 2006.

[82] S. Albers, "On the value of coordination in network design," in *Proc. of the 19th annual ACM-SIAM symposium on Discrete algorithms (SODA)*, pp. 294–303, San Francisco, CA, USA, 2008.

[83] A. Epstein, M. Feldman, and Y. Mansour, "Strong equilibrium in cost sharing connection games," in *Proc. of the 8th ACM conference on Electronic commerce*, pp. 84–92, San Diego, CA, USA, June 2007.

[84] H. L. Chen, T. Roughgarden, and G. Valiant, "Designing networks with good equilibria," in *Proc. of the 19th annual ACM-SIAM symposium on Discrete algorithms*, pp. 854–863, San Francisco, CA, USA, January 2008.

[85] E. Koutsoupias and C. Papadimitriou, "Worst-case equilibria," in *Proc. of the 16th Annual Symposium on Theoretical Aspects of Computer Science*, pp. 404–413, Trier, Germany, March 1999.

[86] B. Awerbuch, Y. Azar, and Y. Bartal, "On-line generalized Steiner problem," *Theoretical Computer Science*, pp. 313–324, vol. 324, no. 2–3, September 2004.

[87] J. Elias, F. Martignon, A. Capone, and E. Altman, "Competitive Interference-aware Spectrum Access in Cognitive Radio Networks," *Proc. of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt 2010)*, Avignon, France, June 2010.

[88] J. Elias, F. Martignon, A. Capone, and G. Pujolle, "A New Approach to Dynamic Bandwidth Allocation in Quality of Service Networks: Performance and Bounds," *Elsevier Computer Networks*, vol. 51(10), pp. 2833–2853, 11 July 2007.

[89] J. Elias, F. Martignon, A. Capone, and G. Pujolle, "Distributed Algorithms for Dynamic Bandwidth Provisioning in Communication Networks," *Journal of Communications*, vol. 1(7), pp. 47–56, November-December 2006.

[90] A. Capone, J. Elias, F. Martignon, and G. Pujolle, "Dynamic Resource Allocation in Communication Networks," *Proc. of Networking 2006*, Coimbra, Portugal, 15-19 May 2006.

[91] W. Fawaz, F. Martignon, K. Chen, and G. Pujolle, "A Novel Fault Management Approach for DWDM Optical Networks," *ACM International Journal of Network Management*, vol. 16(5), pp. 337–349, September-October 2006.

[92] W. Fawaz, F. Martignon, K. Chen, and G. Pujolle, "A Novel Protection Scheme for QoS Aware WDM Networks," *Proc. of the IEEE International Conference on Communications (ICC 2005)*, Seoul, Korea, May 2005.

[93] W. Fawaz, F. Martignon, K. Chen, and G. Pujolle, "A Priority-Aware Protection Technique for Quality of Service Enabled WDM Networks," *Proc. of Networking 2005*, Waterloo, Ontario, Canada, May 2005.

[94] A. Capone, L. Fratta, and F. Martignon, "Dynamic Online QoS Routing Schemes: Performance and Bounds," *Elsevier Computer Networks*, vol. 50(7), pp. 966–981, 15 May 2006.

[95] A. Capone and F. Martignon, "Analysis of Dynamic Quality of Service Routing Algorithms," *Proc. of the IEEE International Communications Conference (ICC 2004)*, Paris, France, June 2004.