Mémoire présenté en vue de l'obtention du diplôme

HABILITATION À DIRIGER DES RECHERCHES

de l'Université Pierre et Marie Curie Sorbonne

par

Emmanuel BACCELLI

IP-Disruptive Wireless Networking: Integration in the Internet

Soutenue le 18 décembre 2012, après avis de:

Catherine Rosenberg	Professeur, Waterloo University, Canada
James Kurose	Professeur, University of Massachusetts, USA
Walid Dabbous	Directeur de recherche, INRIA Sophia-Antipolis, France

Devant le jury composé de :

Catherine Rosenberg	Professeur, Waterloo University, Canada	Rapporteur
James Kurose	Professeur, University of Massachusetts, USA	Rapporteur
Walid Dabbous	Directeur de recherche, INRIA Sophia-Antipolis, France	Rapporteur
Serge Fdida	Professeur, UPMC, France	Examinateur
Philippe Jacquet	Alcatel-Lucent Bell Labs, France	Examinateur
David Simplot	Professeur, Universit Lille1, France	Examinateur
Eric Fleury	Professeur, ENS Lyon, France	Président

A thousand thanks to my colleagues and co-authors, for the opportunities to fruitfully work together.

A thousand thanks to my family and to my friends, for their continuous support.

To Olivier Griguer.

Preamble

This thesis describes the research I have recently conducted and participated in. Since I obtained my PhD in 2006, I have spent my time in three environments: I visited FU Berlin in 2006 and 2007, and since then I mainly split my time between two research facilities near Paris: INRIA (Rocquencourt) and Ecole Polytechnique. During my PhD, my contributions included initial work on some types of spontaneous wireless networks, mostly MANETs. The evolution of the technology since then has been driving my research activities and interests, and I have thus completed this initial work with new contributions, tackling other types of spontaneous wireless networks which have emerged, such as sensor networks, delay tolerant networks, or wireless mesh networks. This thesis reviews these contributions, as well as the contexts in which they take place: the super collision between the Internet phenomenon and the wireless communication revolution.

This collision gives birth to a wealth of research problems, design challenges and standardization activities. Within this domain, spontaneous wireless IP networking are probably the most extreme example of new "particles" born from the collision. Indeed, these particles defy the laws of the Internet in many ways. The absorption of such peculiar particles in the global IP network has already started thanks to pioneering algorithmic and protocol work – for instance OLSR [12] – and through the deployment of wireless mesh networks around the world, such as urban community wireless networks [13] [14] [15] [16] [17] [18]. With the recent revolutions in North Africa, and movements such as Occupy Wall Street [19], the prospect of spontaneous wireless IP networking has become even more attractive on social and political grounds. Dedicated conferences have recently been organized [22], and as a result, ambitious, multi-million dollar initiatives have been launched (the US Government-funded project Commotion Wireless [20], or the EU-funded initiative CONFINE [21]). However, spontaneous IP wireless networks are not yet widely deployed because pioneer work such as OLSR is vastly insufficient to fully bridge the gap between the Internet and these new networks. This thesis presents work that analyzes this gap and proposes some solutions as to how to bridge it.

Thesis Contributions & Organization

The contributions are overviewed in Chapters 2, 3, and 4. A list of publications in which my contributions were originally published ends this document. This thesis mainly contains three parts. The first part presents work in the domain of wireless mesh and ad hoc networks. The second part presents work on sensor networks and in the Internet of Things. And the third part presents work in the domain of delay tolerant networking.

In the field of ad hoc and mesh networking, I have contributed to multiple research and standardization efforts, such as ad hoc network characterization and modeling [106] [107], IP address autoconfiguration schemes standardization [108] [109], routing protocol design for hybrid wired/wireless ad hoc networks [110] [114], synchronization of critical data in MANETs and hybrid wired/wireless ad hoc networks [113] [112], as well as analyzing the impact of standard jitter in ad hoc networks [111]. I also took part in several projects in the domain [31] [32] together with industrial partners (Thales, Archos, Cisco). In the field of sensor networks and in the Internet of Things, I have participated in several research and standardization activities, including sensor network routing protocol performance analysis [132] [133] [131], and the design of several new schemes and protocols targeting low-power and lossy networks such as wireless sensor networks targeting home and building automation contexts [127] [129] [136] [137]. I participated in the deployment of two large sensor network experimental testbeds [57] [58], and I collaborate with several industrial partners in the domain (Johnson Controls, Sigma Designs, Orange), in various projects [36] [33]. Finally, in the field of vehicular networks, I have contributed to research activities that analyze the achievable performance of epidemic routing in the context of vehicular DTNs [140] [141] [146], and to the design of OSPF protocol extensions targeting vehicular networks [121]. I took part in national and international projects in the domain [34] [35], through which I collaborated with several industrial partners (Technicolor, Toyota, Alcatel-Lucent).

NOTE WELL: In this manuscript, the term *protocol* will be mentioned on several occasions. In the literature, this term is sometimes used as a generic denomination for any distributed algorithm "which needs to communicate over the network". In contrast, when the term *protocol* is used in this manuscript, it means something more precise, *i.e.* an elaborate specification agreed upon by the community, defining standard operation of a distributed algorithm and compliant network signaling required to run it on IP networks. The interoperability of such a specification with relevant legacy IP protocols has been fully verified, both in theory and in practice, by several independent parties. The auto-compliance of such a specification has moreover also been verified by interoperability tests between independent implementations. Only this level of precision ensures that a protocol is indeed ready to be deployed on the Internet.

Chapter 1

Introduction: IP-Disruptive Wireless Networking

The Internet's success-story takes its roots in the USA in the 1960s, when the concept of packet switching was introduced by Paul Baran as an alternative to circuit switching [1]. In the 1970s, networks of computers using packet switching started to appear. Initial versions of the fundamental protocols IP and TCP [2] were introduced by Robert Kahn and Vinton Cerf and put to use on early Internet – back then, mostly an american-only adventure connecting a few dozens of computers. At the time, the killer application was email.

In the 1980s, the Internet became international, as the community of Internet pioneers formalized open standardization of networks protocols with the creation of the IETF [3]: the organization responsible for elaborating, updating, and maintaining IP protocols specifications, published in documents called RFCs, i.e. Request For Comments – for instance TCP was first specified in RFC 761 [4]. By then, the Internet was connecting thousands of computers in various locations around the world. The killer application was still email.

The democratization of the Internet really took off in the 1990s, with Tim Berners-Lee introducing seminal new concepts such as the web, hypertext and the HTTP protocol [5]. By the end of the decade, the Internet had grown to millions of computers connecting tens of millions of users on all continents (and even in outer-space). The killer application was then web-browsing enabled by HTTP and web search engines, which fueled the growth of Internet content *consumers*.

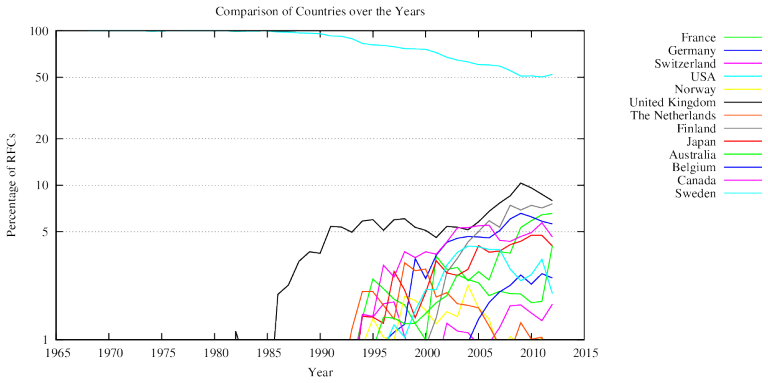


Figure 1.1: RFCs with authors from a given country, semi-logarithmic scale (www.arkko.com, April 2012)

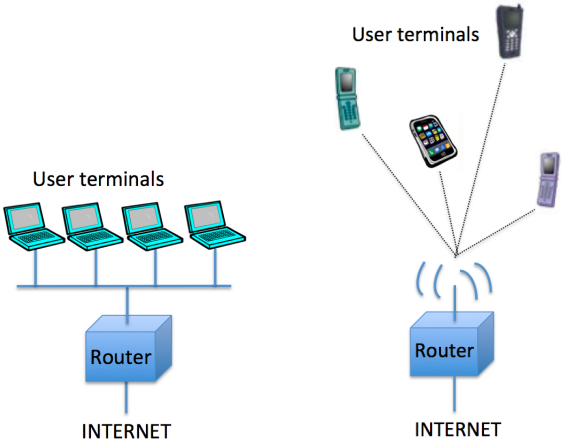
Since the 2000s, Internet content experienced a staggering growth. Billions of devices now connect billions of users who increasingly become Internet content *prosumers* (i.e. producers and consumers at the same time) with new killer applications such as P2P and social networks, as well as other do-it-yourself multimedia content sharing and streaming.

1.1 IP Networks: from Wired to Wireless

Until the 2000s, Internet was essentially based on wired communication. However, inspired on one hand by Norman Abramson's pioneer work on packet radio networks [6] in the 1970s and on the other hand by the democratization of wireless telephony thanks to the availability of cheaper, more efficient hardware stemming from Cold War military industry efforts, wireless Internet access has since become more and more common. For instance, in 2011 in the UK, nearly half of population using Internet accessed it wirelessly with a handheld device [7], while in India, half of the entire population currently accesses the Internet via handheld devices [8].

Wireless Internet access is nowadays mostly provided via technologies such as Wifi (IEEE 802.11 infrastructure mode standards [10]), UMTS or LTE (3GPP standards [11]), on user terminals such as smartphones, tablets, laptops etc. Such technologies have in common a communication model that is similar to the local wired network model, in that, in both models, user terminals (hosts) access the Internet through a dedicated, authoritative infrastructure device: a router. In that sense user terminals are competing *consumers* of the same networking resource, which consists locally in access to the router. Routers, on the other hand, are *providers* of the networking resource, and collaborate with one another to provide this resource, i.e. internetwork connectivity. This similarity enables IPv4 and IPv6 protocol suites to run quite naturally over such wireless

access networks, although IP protocols were in fact designed for wired networks at a time when massive use of wireless Internet access was not yet envisioned. In the following, we will denominate this category of wireless access technology *cellular networking*, a term which is traditionally used for 3GPP standards such as GSM, UMTS, LTE, but which can also apply to Wifi infrastructure mode in the sense of the above-described communication model similarity.



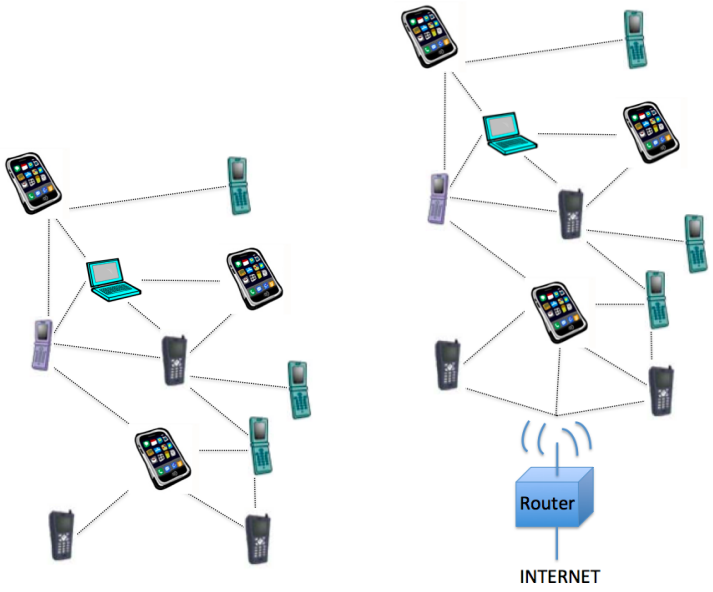
(a) Wired access network. (b) Cellular access network.

Figure 1.2: Traditional IP networks: hosts are competing consumers, routers are collaborating providers.

1.2 Wireless IP Networks: from Consumers to Prosumers

Although not quite as successful as cellular networking so far, an alternative type of wireless networks has also emerged: spontaneous wireless networks. Inspired by the Push-To-Talk concept used in walkie-talkies (portable half-duplex radio transceivers developed during the Second World War), spontaneous wireless networks depart from the traditional distinction between routers and hosts, whereby each user terminal is simultaneously a router and a host. In spontaneous wireless networks, user terminals are thus *prosumers* (i.e. both producers and consumers) of networking resources instead of mere consumers. Terminals self-organize to provide multi-hop wireless communications among themselves, with or without help from infrastructure devices. Each terminal may thus simultaneously originate/receive traffic (role of a host), as well as forward traffic on behalf of other terminals (role of a router).

Popular examples of spontaneous wireless networks include mobile ad hoc networks, wireless mesh networks, wireless sensor or actuator networks, wireless smart meter networks, vehicular networks, opportunistic wireless networks or delay tolerant networks. Spontaneous wireless networks are considered as interesting



(a) Spontaneous wireless network. (b) Spontaneous wireless access network.

Figure 1.3: An alternative to wireless cellular networks: spontaneous wireless networks. Each user terminal is simultaneously a router and a host. Each user terminal is thus a networking resources prosumer.

solutions to complement cellular networks hampered by increasingly heavy smartphone data communication loads [9]. Spontaneous wireless networks are also considered for scenarios where infrastructure is not usable, due to a disaster, to the military situation or to the political situation, for instance. Spontaneous wireless networking is also an effective way to extend the reach of wireless Internet access, without costly additional infrastructure deployment. Such scenarios are incentives to enable standard IP protocols operation over spontaneous wireless networks, in order for these to effectively blend in the global network, where appropriate.

1.3 IP-Disruptive Wireless Networking

Originally targeting wired networks, the design of IP protocols (IPv4 as well as IPv6) is implicitly based on a few fundamental assumptions, which include the following axioms:

1. **Axiom 1: IP links are definable.** Atomic elements of the Internet architecture, IP links, are supposed to be rather stable and precisely scoped.

2. **Axiom 2: End-to-end connectivity exists.** If there is currently no path towards a destination, packets towards this destination are deleted.

3. **Axiom 3: Routers are always on, if not dead.** There is no power saving or sleep modes for routers.

4. **Axiom 4: Routers have reasonable memory, CPU, power.** There are minimum requirements in that respect for standard IP protocols to function.

Spontaneous wireless networks break these assumptions, thus causing *disruption*. This thesis reviews some recent work I participated in, aiming at studying IP-disruptive wireless networks and alleviating the disruptions they cause in the realm of IP protocol standards. The following describes work tackling three types of IP-disruptive wireless networks: Chapter 2 presents work on wireless mesh and ad hoc networks, Chapter 3 presents work on sensor networks, while Chapter 4 presents work on delay tolerant networks.

Chapter 2

Wireless Mesh and Ad Hoc Networks

Wireless ad hoc networks can be defined as a collection of devices that each have a radio transceiver, that are using the same physical and medium access protocols, and that are configured to self-organize store-and-forward functionality on top of these protocols, as needed to enable communications between devices [107]. Such capabilities can increase the survivability of a network in face of infrastructure damage, can provide cost-effective coverage extension for existing infrastructure, or can provide users with new means for private networking. In that sense, wireless ad hoc networks can be considered as the archetype of all spontaneous networks. Two types of ad hoc networks are typically distinguished: mobile ad hoc networks where devices move around, and wireless mesh networks where a significant fraction (if not all) of the devices are fixed while only some may move around. In the following, the term *node* will be used to describe such a device, simultaneously router and host.

2.1 How are Wireless Mesh and Ad Hoc Networks IP-Disruptive?

Related publications: [106] [107] [108], joint work with C. Perkins, K. Mase, M. Townsley, S. Ruffino, S. Singh.

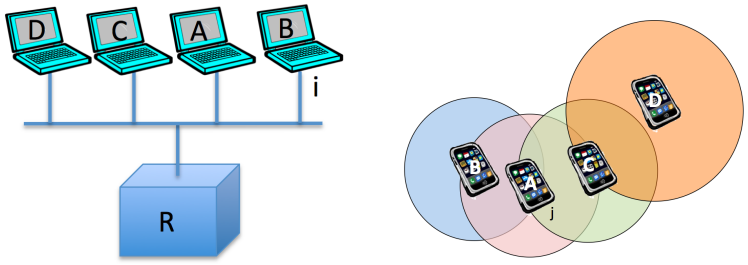
The IP protocol suites (IPv6 as well as IPv4) are based on a key concept: the IP link, *i.e.* a topological area of the network, within which a IP packet can be delivered without IP-layer forwarding [23]. Fundamental to the Internet's scalability is the coincidence between an IP link and an IP subnet: a topological area of the network within which IP addresses stemming from the same IP prefix are assigned to network interfaces. This coincidence allows various levels of IP address aggregation, which enables today's routers at the core of the Internet to function with forwarding tables in the order of 10^5 IPv4 entries, instead of in the order of 10^9 entries, without aggregation.

The IP link concept, however, was designed at a time when IP was primarily targeting wired networks, and essentially models what one would expect over Ethernet interfaces, which can be formalized as follows. Let X and Y be two nodes with each an interface to local network N. If we assume that, when node X transmits a packet through its interface on network N, that packet reaches node Y without requiring storage and/or forwarding by any other node. In this circumstance, we will say that node Y hears node X. Now let A be a node with an interface i on an IP link as depicted in Fig. 2.1(a), let $U(t)$ be the set of devices that hear node A through interface i at time t, and $V(t)$ be the set of devices that node A hears through interface i at time t. Then, the following properties are expected:

1. Symmetry: $S(t) = V(t)$,

2. Stability: node A can reasonably assume that $S(t+1) = S(t)$ and $V(t+1) = V(t)$ for time units of the order of minutes,

3. Transitivity: if on one hand nodes A and B can hear each other on the link, while nodes A and C can also hear each other on the other hand, then node A can reasonably assume that nodes B and C can also hear each other on the link.



(a) Link connecting A, B, C, D, R. (b) Ad hoc network connecting A, B, C, D.

Figure 2.1: Issues with P links on ad hoc networks.

The above set of properties characterize a *determined* link: the connectivity through interface i is predetermined to some extent – a predetermination that is leveraged by IP protocols and applications. Being able to predetermine stable pools of network interfaces that will stick together for some time with the above properties is fundamental to:

- configuration and autoconfiguration schemes allowing IP address aggregation etc.,

- routing protocols,

- applications and protocols that rely on link-local services such as link-local multicast/broadcast (all in all, many applications and protocols).

However, such determined links greatly differ with the general characteristics of ad hoc networks ([107] joint work with C. Perkins) which can be formalized as follows. Let's assume that node A sends and receives packets through its interface j on an ad hoc network as depicted in Fig. 2.1(b), and let's assume that $U(t)$ is now the set of devices that hear node A through interface j at time t, while $V(t)$ is the set of devices that node A hears through interface j at time t. Then:

1. Asymmetry: it cannot be assumed that $S(t) = V(t)$,

2. Variability: it cannot be assumed that $S(t+1) = S(t)$ or $V(t+1) = V(t)$ even for small time units such as seconds,

3. Non-transitivity: even if on one hand nodes A and B can hear each other through interface j, while nodes A and C can also hear each other through interface j on the other hand, this neither implies that node B can hear node C, nor that node C can hear node B through their own interfaces to the ad hoc network.

The above set of properties characterize an *undetermined* link: connectivity through interface j utterly undetermined, a priori. Such undetermined links are obviously a departure from what IP links were supposed to model so far. Asymmetry and non-transitivity properties imply that in general, it is not possible to define the topological area of an IP link in an ad hoc network, and thus traditional link-local services are unavailable, causing *disruption* for all the protocols and applications that depend on them. For starters, prior to routing, communicating devices need appropriate IPv4/v6 configuration (IP address, prefix etc.). However, the standard IP address autoconfiguration schemes DHCP [43], SLAAC [42] and NDP[41] will not function on undetermined links ([108] joint work with K. Mase, S. Ruffino, S. Singh). This analysis highlights for instance that DHCP works with the basic assumption that every node in the ad hoc network can directly communicate with either (i) the DHCP server, or (ii) a DHCP relay which can communicate with either the DHCP server or another relay. As seen earlier in this chapter, assumption (i) is wrong in an ad hoc network, as each node may hear a different set of neighboring nodes. On the other hand, assumption (ii) relies on the guarantee that the recursion will end at some point (by reaching a DHCP server). Because of the natural dynamics in an ad hoc network's topology, where nodes may move about, there is no such assurance: the DHCP server may be unreachable, or a loop may have appeared along the path. Similarly, [108] points out how SLAAC and NDP also rely on the assumption that each node in the ad hoc network can communicate directly with every other node in the ad hoc network, i.e. all the nodes are connected to a single broadcast-enabled link.

As seen earlier in this chapter, this assumption is wrong, as each node an ad hoc network may hear a different set of neighboring nodes. Furthermore, since NDP signaling is not forwarded at the network layer beyond the IP link, there is no guarantee that configured addresses will indeed be unique if topology is or becomes such that the ad hoc network is not contained in a single hop – for the simple reason that signaling will not reach all the concerned nodes.

Such conclusions have lead to a new standard, RFC5889 ([106] joint work with M. Townsley), defining appropriate IPv4 and IPv6 addressing schemes for ad hoc networks. This model scheme specifies the configuration of IP addresses and the IP subnet prefixes on a router's IP interfaces, which connect to links with undetermined connectivity properties. A basic observation on which RFC5889 builds is that, if the link to which an interface connects enables no assumptions of connectivity to other interfaces, the only addresses that can be assumed "on link", are the address(es) of that interface itself. Thus, subnet prefix configuration on such interfaces must not make any promises in terms of direct (one hop) IP connectivity to IP addresses other than that of the interface itself, thus implying that no on-link subnet prefix should be configured on such an interface. Another observation on which RFC5889 is based, is that routing protocols running on a router may exhibit different requirements for uniqueness of interface addresses: some have no such requirements, while others have requirements ranging from local uniqueness only, to uniqueness within, at least, the routing domain. RFC5889 thus specifies a one-size-fits-all approach to IP address configuration: it mandates the configuration of IP addresses that are unique within the routing domain. This approach has the advantage of being generic, as it satisfies both the less stringent uniqueness requirements, as well as the most stringent uniqueness requirements. However, by basically prohibiting the use of IP subnets and of link-local addresses in this context, RFC5889 does not offer a complete solution: the lack of traditional link-local services remains, and a scalable standard mechanism automatically assigning IP addresses on network interfaces connected to ad hoc networks is yet to be developed.

2.2 Adding Wireless Ad Hoc Networking Capabilities to Internet Routers

Related publications: [112] [113] [110], [123], joint work with J.A. Cordero, P. Jacquet, D. Ngyuen, T. Clausen.

The variability of connectivity through a network interface on an ad hoc network has the consequence that standard IP routing protocols running on such interfaces are facing a challenge: they must track much more topological changes than usual, with much less control traffic than usual, in order to fit the bandwidth available wireless communications (much smaller than bandwidth available on wires). During my PhD, I had been

involved in analyzing the scalability of OSPF [24], one of the most widely deployed IP routing protocol. We have shown that OSPF can only manage less than a dozen neighbors on an ad hoc network [115] (joint work with C. Adjih, T.Clausen, P. Jacquet, R. Rodolakis). Since IP routing protocols such as OSPF are not agile enough to track topology changes in ad hoc networks, new routing protocols had to be designed, tailored for ad hoc networks. Among the many proposed, OLSR [25] and AODV [26] have emerged as the most prominent ad hoc routing protocols.

However, the best way to add ad hoc networking capabilities to state-of-the-art Internet routers may not be to add another protocol just for the wireless ad hoc domain, as analyzed in [117] (joint work with F. Baker, M. Chandra, T. Henderson, J. Macker, R. White). Indeed, routers will typically have to run another protocol (eg. OSPF, IS-IS, EIGRP) on their interfaces to another routing domain, and this would thus require intricate management of route leakage between routing domains. An alternative way is to extend a protocol such as OSPF to enable its operation on ad hoc networks. Initial work [118] [90] had pointed out the algorithmic similarities between OSPF and OLSR, and thus, it seemed indeed possible to design a protocol inspired from OLSR but still OSPF-compatible. However, OSPF compatibility has its price in terms of performance on an ad hoc network, and the following overviews work I have participated in, aiming to analyze this performance, and to design efficient OSPF protocol extensions for operation on wireless mesh and ad hoc networks.

Hybrid Wired/Wireless Networking with OSPF

OSPF is proactive link-state routing protocol, and thus uses periodic exchanges of control messages for topology discovery and maintenance. *Hellos* are exchanged locally between neighbors to establish bidirectional links, while Link State Advertisements (*LSA*) reporting the current state of these links are flooded (i.e. diffused) throughout the entire network. This results in a topology map: the link state database (*LSDB)*, a copy of which is present in each node in the network, from which a routing table can be constructed. An additional mechanism provides explicit pairwise synchronization of the LSDB between neighbors, via additional control signaling (*database description* messages and *acknowledgements*). Synchronized neighbor pairs are then called *adjacent* neighbors, while other bidirectional neighbors are called *2-WAY*. In order to fit better the characteristics of ad hoc networks, in particular the available bandwidth constraints, the amount of OSPF control traffic [115] must be trimmed. This can in fact be achieved in several ways:

1. Flooding Optimization and Backup. Instead of the vanilla flooding scheme, use more sophisticated techniques that reduces redundant retransmissions.

2. Adjacency Selection. Instead of attempting to become adjacent with all its neighbors, a router becomes

adjacent with only some selected neighbors.

3. Topology Reduction. Report only partial topology information in LSAs, instead of full topology information.

4. Hello Redundancy Reduction. In some Hello messages, report only changes in neighborhood information instead of full neighborhood information.

We have studied the impact of a variety of techniques in each area listed above. For instance, we have studied in [114] (joint work with J.A. Cordero, P. Jacquet) the impact of Hello redundancy reduction techniques Incremental Hellos [27] and Differential Hellos [28] proposed by some OSPF protocol extensions for MANETs, and we found this impact to be negligible, saving less than 2% of the control traffic in relevant scenarios.

In fact, the largest contributor in terms of control traffic is not Hello traffic, but rather LSA traffic, via flooding, or via database synchronization. We have thus proposed to use multipoint relaying techniques derived from OLSR to optimize adjacency selection, LSA size and flooding costs. This proposal was not only analyzed and simulated but also implemented and used on a real testbed in Ecole Polytechnique, comprising of wired routers, wireless routers as well as wired/wireless hybrid routers ([126], joint work with J.A. Cordero and M. Philipp) . The protocol we designed, called MPR-OSPF, has been standardized as RFC 5449, an OSPF protocol extension ([110] joint work with T. Clausen, P. Jacquet, D. Nguyen). An open source implementation of the standard is available ([125], joint work with J.A. Cordero). This implementation was demoed on the testbed in Ecole Polytechnique in the context of MOBISIC [31], a project which targeted specific event security (football world cup, political meeting), and which aimed at conceiving, developing and experimenting mobile, modular ('plug and play') security systems enabling fast deployment by non-specialized operators. MOBISIC partners included INRIA, Thales, Alcatel-Lucent and CEA.

Critical Data Synchronization in Hybrid Wired/Wireless Networks

In a hybrid wired/ad hoc network, containing wired routers, wireless routers as well as hybrid wired/wireless routers as shown in Fig. 2.2, node and link heterogeneity becomes a challenge. For instance, the LSAs generated by wired nodes running basic OSPF will have long generation periods (up to 1 hour) because the changes they track are infrequent, while LSAs generated by wireless nodes (running MPR-OSPF) will typically have a period of less than a minute because the changes they track are much more frequent. The loss of a wireless LSA is negligible because an updated LSA will soon be generated and flooded anyway. The loss of a wired LSA, however, can have an impact: the information it contains will not be repeated or updated for

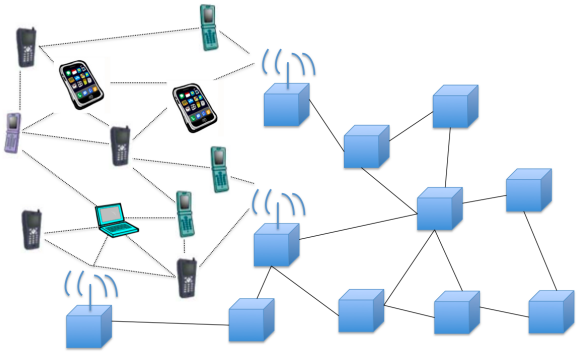


Figure 2.2: Hybrid wired/ad hoc network: wired routers, wireless routers and hybrid wire/wireless routers.

a long time, and if this information is critical, not being aware of this information may substantially damage connectivity. This observation calls for a novel mechanism conducting efficient critical data synchronization in OSPF on hybrid wired/ad hoc networks, which suits both the constraint of heterogeneity in LSA periods and the constraint of wireless bandwidth limits.

The basic mechanisms ensuring critical database synchronization in OSPF are explicit LSA acknowledgements, and database exchange. These mechanisms can however generate unmanageable amounts of control traffic on ad hoc networks. We thus proposed in [123] (joint work with P. Jacquet and T. Clausen) a mechanism called Database-Signatures, based on periodic exchanges of compact signatures (hashing of the link state database) between neighbors: when a discrepancy is detected between signatures, the bits of information required to synchronize the link state databases of the involved nodes are then identified and exchanged. This mechanism thus provides reliable diffusion of link-state information replacing OSPF acknowledgements with a mechanism suitable for mobile wireless networks, while reducing overhead for performing database synchronization in an ad hoc network. Additionally, Database-Signatures reduce overhead and convergence time when new nodes pop up in the network, or when distinct network partitions merge. The Database-Signatures method is inspired from a technique used in the other prominent standard link state routing protocol, IS-IS [29], which enables the exchange of recently received LSA sequence numbers between neighbors to identify database discrepancies. We have significantly improved this technique by introducing much more compact information exchanges based on hashing, and on the use of the age of LSAs to distinguish long-lived LSAs that need to be synchronized, from short-lived LSAs that need not be synchronized because they will be updated before soon.

Critical Data Synch in Mobile Ad Hoc Networks

A simple mechanism guaranteeing the dissemination of critical data (whether it be control or application data) is to use an overlay network as backbone, i.e. a subgraph of the ad hoc network, over which each critical message is acknowledged hop-by-hop, in a peer to peer fashion, in order to verify the actual dissemination, or, absent expected acknowledgement, retransmit the corresponding critical message. Such an approach ensures that overlay nodes' local databases remain synchronized over time, at least concerning critical data. Depending on the characteristics of the overlay, in terms of edge count, or edge life-time, critical data synchronization along this overlay may be more or less efficient in terms of overhead: the less edges and the longer their life-time, the better, because less overhead is incurred.

We have thus analyzed the performance of various overlays in [112] [113] , including multipoint relays (MPR), connected dominating sets (CDS) and overlays selected based on a category of Gabriel graph called Relative Neighbor Graph (RNG), which we called Synchronized Link Overlay - Triangular (SLOT). We have shown that SLOT has some very interesting properties, in that it produces an overlay made of a number of links per node that is independent of the node density ν and of the topology based on the unit disk graph model, while the total number of non-overlay links is proportional to the node density, i.e. $O(\nu)$. We have also shown that the per node synchronization rate with SLOT is independent of the node density ν, but proportional to the average node speed s. These properties are interesting when one aims at identifying a small number of links for the synchronization overlay, with a low overlay link change rate.

We have then applied SLOT to OSPF over 802.11b, and compared via simulations the performance of IP protocols standards RFC 5449 and RFC 5614 (OSPF extensions for ad hoc networks [110] [28]) with that of SLOT-OSPF, an alternative OSPF protocol extension we proposed, using SLOT. The simulations show that SLOT-OSPF produces drastically less control traffic than RFC 5449 or RFC 5614 which are based on other synchronization overlays (respectively MPR and CDS). This allows SLOT-OSPF to function correctly as RFC5449 and RFC 5614 stall, when the density and/or the number of routers in the domain is large, above 100 nodes.

2.3 Complementary Notes & Summary

Ad hoc and mesh networks are disruptive for standard IP protocols because they do not allow atomic link-local services on which many IP protocols and applications rely. Ad hoc and mesh networks are also disruptive

because they require network protocols to track much more topology changes than usual, with much less control traffic than usual. For these reasons, new IP standards are being developed to accommodate such characteristics. Within this effort, I have participated in several research and standardization activities, such as ad hoc network characterization and modeling, IP address autoconfiguration schemes design and standardization, routing in hybrid wired/wireless ad hoc networks, or synchronization of critical data in MANETs and hybrid wired/wireless ad hoc networks.

My other activities in this domain, which I do not detail in this document, include for instance analyzing the delay incurred by the use jitter in wireless ad hoc networks ([111] joint work with J.A. Cordero and P. Jacquet), contributing to the standardization of OLSRv2 [30], and to the E-COMP@GNON project [32] which aimed at adding ad hoc networking capabilities to Archos hand-held devices, together with industrial partners SNCF and Archos.

Chapter 3

Machine to Machine Communications: Sensor Networks & Internet of Things

The Internet of Things (IoT) is expected to soon connect billions of communicating machines, including devices ranging from actuators to home appliances, from smart meters to smart dust. The outcome of on-going debates and deployments will shape the proportion of such devices that will actually be connected to the Internet and be assigned an individual IP address. Efforts such as Auto-ID Labs [38] and EPC Global [39] propose approaches, while the IETF currently pushes towards solutions where most devices would be identified and reachable via an IPv6 address. Nevertheless, even if a small fraction of these devices blends into the global IPv6 network in the end, it would still have a very significant impact on the Internet. The advent of the IoT is indeed expected to drastically increase communication without human source or destination (so-called machine-to-machine communications, or M2M communications) to the point where the amount of M2M communications would dwarf communications involving humans. Optimizing M2M communications thus seems a high priority.

Sensor networks are a substantial part of this new galaxy of communicating devices expected to make the Internet of Things. Sensors are devices used for distributed and automated monitoring of various parameters such as temperature, movement, noise or radioactivity levels etc., depending on the type of sensor. While some of these sensors will connect to the network via wire or power line communication, many sensors will use radio communications. Typically, a number of such devices, identical to one another, are scattered in the zone to be monitored. Each sensor then monitors the parameters to be measured in its vicinity and communicates through its single radio interface with its peers, spontaneously creating a wireless network. Using

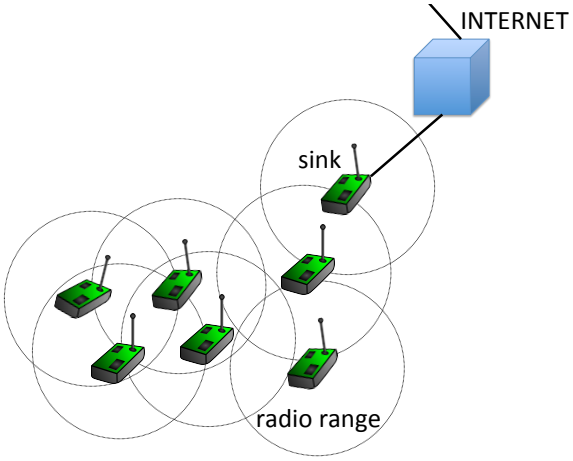


Figure 3.1: Sensor network with a sink, connected to the infrastructure and the Internet.

this network, sensors self-organize distributed computations, or convergecast, *i.e.* information gathering at a central control point – which is generally called the *sink*, in this context.

From a networking point of view, scattered sensors may be more or less remote from one another – a given sensor may for instance require some peers to forward information towards the sink, because the sink is outside of its radio range. Appropriate network protocols are thus required to enable each sensor to, on one hand, directly communicate with peers that are within its radio range, and on the other hand, indirectly communicate with other devices that are only reachable through some peer with which the sensor can directly communicate, as shown in Fig. 3.1. Several different technologies can be used to enable direct wireless sensor communication at the link layer (layer 2), the most typical to date being IEEE 802.15.4, often preferred for its low power needs. The way sensors are scattered is generally unplanned (aside of the central role of the sink), and may evolve over time as sensors are added or removed from the network, or as they move about. Complementary mechanisms are thus used to enable indirect wireless sensor communication [95] at the network layer (layer 3), i.e. routing protocols for multi-hop wireless sensor networks, which are the focus of this chapter.

3.1 How are Wireless Sensor Networks IP-Disruptive?

Sensor networks are IP-disruptive because, similarly to ad hoc networks (see Chapter 2), they do not allow atomic link-local services on which many IP protocols and applications rely. In this chapter, we will consider scenarios where sensors are not mobile. However, even for such scenarios, sensor networks require network protocols to discover and track topology with extremely little control traffic in order to meet stringent power

constraints: transmitting or receiving drain batteries that are generally expected to last months or years before being replaced. With standard IP protocols, sensor batteries typically fail to last that long.

On top of that, sensor networks have the following disruptive characteristics:

1. **Drastic memory constraints**. Today's wireless sensors are typically cheap devices that have a few kilobytes of RAM and and a few tens of kilobytes of ROM [40], slightly less than what was available on the first computers (Honeywell DDP-516) on the ARPANET in the early 1970s! This is a rather small amount of memory to run on for a single protocol nowadays. The challenge is that *the whole protocol stack and applications* must share that little memory.

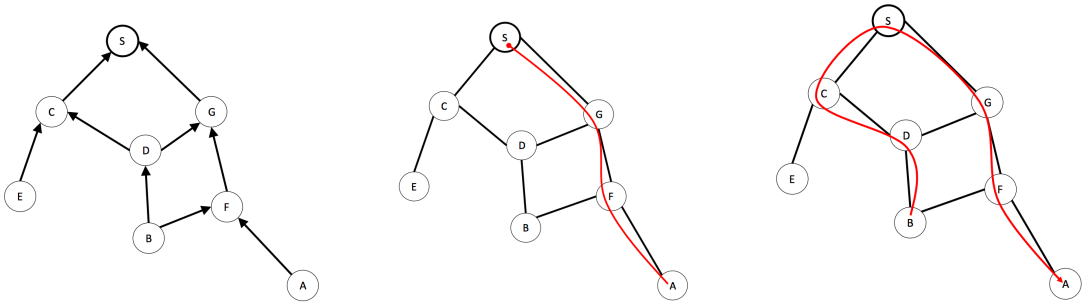
2. **Drastic frame-size constraints**. The most common link layer technology used today by wireless sensors is 802.15.4-2006, which communicates with packets that carry a maximum payload of 102 bytes (81 bytes if link layer security is on). This is an order of magnitude less than the standard IPv6 packet size of 1280 bytes. Standard IPv6 and UDP headers alone require 48 bytes, a meager 33 bytes of payload is thus left for applications and other protocol headers [37], which is typically not enough.

The community has thus recently engaged into multiple efforts aiming to address the limitations of standard IP protocols on wireless sensor networking. For instance, the 6LOWPAN [44] working group has focused on developing an intermediate layer between 802.15.4 and the IP layer, enabling IPv6 to operate on wireless sensor networks with IPv6 formats compression. Meanwhile, efforts such as Contiki [48] [49] and Tiny OS [50] proposed small foot-print IP stacks that aim at fitting the memory constraints of sensors, and very recently, a working group dedicated to light-weight implementations of IP protocols, has taken shape at the IETF: the LWIG working group [46]. Other standards in development aim at adapting HTTP to constrained devices such as sensors: the CORE working group [47] currently develops a specific protocol called COAP, also based on REST. Yet another family of standards under construction aim at providing multi-hop wireless sensor communication with IPv6, which requires specific routing protocols: this is the focus of the ROLL working group [45], in which I have been actively participating.

3.2 Routing in Low-Power and Lossy Networks

Related publications: [127] [133], [132], joint work with M. Goyal, M. Philipp, A. Brandt, J. Martocci

The IETF (through the ROLL working group) has recently published a new standard routing protocol targeting sensor networks: RPL [51]. RPL is currently being deployed at large scale by many companies



(a) DAG rooted at router S. (b) DAO or data traveling from A towards S. (c) Basic RPL path from B to A.

Figure 3.2: Basic RPL characteristics.

around the world. This routing protocol organizes routers along a Destination Oriented Directed Acyclic Graph (DODAG), a category of Directed Acyclic Graph [53], rooted at the sink (router S in Fig. 3.2(a)). The DODAG root initiates the DODAG formation by periodically originating DODAG Information Object (DIO) messages which it advertises via link-local multicast. DIO messages carry information such as the DODAG root's identity, the routing metrics in use, as well as the originating router's depth (called the "rank") in the DODAG. A router joins the DODAG taking in consideration these factors, determines its own rank in the DODAG based on the information advertised by its neighbors in their DIOs. The router chooses as parent(s) in the DODAG the neighbor(s) through which its resulting rank is the smallest, amongst neighbors advertising DIO messages. Once a router has joined the DODAG, it has a path to the sink through its parent(s), and the router can then originate its own DIO messages. RPL thus provides paths from routers to a sink while requiring routers to store very little forwarding and routing table information, essentially information about its parent in the DODAG, a characteristic which is compatible with the most drastic memory constraints in wireless sensors. The transmission rate of DIO messages furthermore follows a Trickle [52] relaying policy which aims at pruning unnecessary transmissions by monitoring information consistency between neighbors. When a node's data does not agree with its neighbors, that node communicates quickly to resolve the inconsistency. When nodes agree, they slow their communication rate exponentially, such that nodes send packets very infrequently. This characteristic aims at compatibility with wireless sensors' portable power supply capacities, which are drained too fast if they need to transmit too often.

RPL Tradeoffs Analysis

In order to keep the size of forwarding and routing tables small, RPL provides only convergecast by default, *i.e.* by default RPL does not provide paths towards destinations other than the sink. Such paths are however desired in many cases. For instance, paths from the sink to individual sensors are necessary in scenarios such as industrial actuators and selective sensor queries [56]. In order to address this lack, an RPL router that re-

quires a path from the sink to itself must send a Destination Advertisement Object (DAO) message upwards along the DODAG, all the way up to the root, which thus records and install this path (see Fig. 3.2(b)). The DAO mechanism can be operated either in storing or in non-storing mode. In storing mode each router needs to store routing information in order to forward packets hop-by-hop. In contrast, the non-storing mode employs source-routes which are managed only at the sink, in order to further reduce the size of forwarding tables on the other sensors.

Similarly, RPL does not by default provide paths between arbitrary sensor pairs. Such paths are however needed in several scenarios, including home and automation use cases [55] [54]. A simple example of such a use case is a remote control (or a motion sensor) that suddenly needs to communicate with a lamp module, whose network address it knows a priori. In order to address this lack, an RPL router A that requires a path from another router B to itself must send a Destination Advertisement Object (DAO) message upwards along the DODAG to establish a path from the sink to router A, and router B can then communicate with router A via the first ancestor common to router A and B in the DODAG that has a path to A – at worse, via the sink (see Fig. 3.2(c)). If RPL is operated in non-storing mode, the worst case happens systematically: all communications are via the sink, which is the only router in the network to store source routes to other nodes.

We have shown in [132] (joint work with M. Goyal et al.) that RPL provides sensor-to-sensor paths that are thus often much longer than the shortest available paths. This performance analysis shows that in a network of 1000 sensors, RPL provides paths that are up to 17 times longer than the shortest available path, and that on average, for short range sensor communications (topologically 2 to 5 hops away), RPL provides paths that are 3,5 times longer than the shortest path available (see for instance Fig. 3.3). In many applications [55] [54], sensor-to-sensor communication typically takes place between nodes that are located close to each other although not necessarily in each others radio range. Therefore, the observed substantial routing stretch is a real problem. Involving more intermediate sensors than necessary in path wastes energy and increases delays, while severe traffic congestion near the DODAG root is experienced as all paths go though the root. Moreover, the constraint for every possible destination in the DODAG to originate a DAO is problematic because it results in a proactive destination-initiated process which is not compatible with many Home and Building Automation scenarios [55] [54]: for example, a remote control suddenly needing to communicate with a lamp module – a fundamentally reactive, source-initiated process.

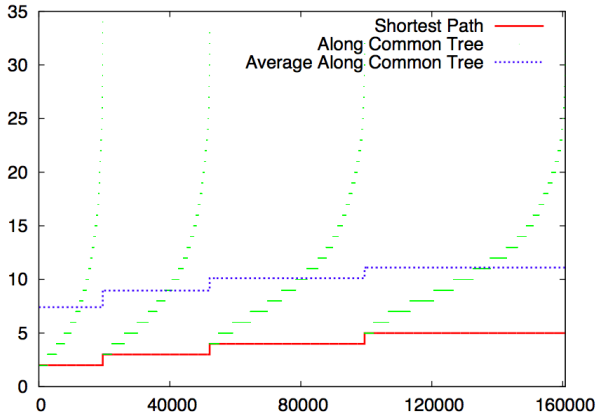


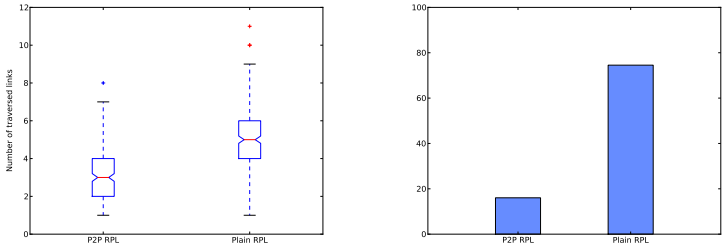
Figure 3.3: Path lengths provided by RPL, compared to the shortest available paths of length 2, 3, 4 or 5 in a 1000 node network (lengths of about 160k paths are thus displayed in total).

RPL Protocol Extension for Sensor-to-Sensor Communication

In order to provide more efficient routing for several Home and Building Automation use cases [55] [54] and to address RPL's identified issues concerning short-range sensor-to-sensor communication, we have proposed an RPL protocol extension called P2P-RPL ([127], joint work with M. Goyal, A. Brandt, J. Martocci and M. Philipp) that provides a reactive mechanism enabling source-initiated discovery of sensor-to-sensor paths that are not necessarily along the DODAG and through the sink. When a router S needs to discover a path to another router D, router S originates a message similar in functionality to an AODV Route-Request [26] indicating it seeks a path to S. This message is piggy-backed on DIO messages, and disseminated throughout the network using Trickle and usual DIO signalling, effectively creating a temporary DODAG rooted in S. While traveling across the network, the message installs temporary next-hop information towards S on the traversed routers, and may accumulate information about the path travelled so far. Upon receiving such a message, router D sends a message back to S, similar in functionality to an AODV Route-Reply, along the recorded path, thus establishing a path between S and D, and the temporary DODAG eventually expires. P2P-RPL allows to use source routes as well as hop-by-hop routes and it is possible to specify metric constraints for the discovered routes. This mechanism provides much shorter sensor-to-sensor paths than basic RPL.

In order to study the behavior of RPL and P2P-RPL in vivo, we have implemented P2P-RPL ([128] joint work with M. Philipp). The implementation is open-source and based on Contiki. This OS was chosen because it benefits from a wide and active industrial and academic user community, and because it includes a small IPv6 stack with 6LoWPAN support, as well as ContikiRPL (an implementation of basic RPL) which was leveraged as basis for our P2P-RPL implementation. In order to test P2P-RPL, we have carried out experiments

on real hardware: sensors based on MSP430 micro-controllers and operating at 2.4 GHz with IEEE 802.15.4 radio interfaces. We used the Senslab testbed [57] to evaluate the improvements brought by P2P-RPL. We collaborated with Johnson Controls Inc., to identify typical scenarios in which short-range sensor-to-sensor communication would be used in a building automation context, that we then reproduced on Senslab. We compared the performance of basic RPL and P2P-RPL in non-storing mode, and we observed that even for small networks (a few tens of sensors, and a maximum RPL DAG depth of 5 hops), P2P-RPL provides paths that are about half as long as paths provided by basic RPL, as shown in Fig. 3.4(a). This improvement gets more massive in bigger networks incurring a deeper DAG, as shown in [132] (joint work with M. Goyal et al.). We also observed in [133] (joint work M. Goyal, M. Philipp) that P2P-RPL also drastically decreases traffic going through the sink. Even in storing mode where basic RPL routes traverse the common ancestor instead of the root systematically (which is thus the mode that is most favorable to basic RPL for this comparison) we observed that about 75% less flows went through the sink with P2P-RPL, compared to basic RPL, as shown in Fig. 3.4(b). The P2P-RPL protocol specification we elaborated in [127] is expected to become an RFC this year. The P2P-RPL protocol is currently being tested in the on-going project SMARTMESH [33] in which I take part (with industrial partners including SAGEM and CEA). SMARTMESH focuses on elaborating a new multi-sensor prototype with spontaneous wireless communication capabilities, targeting sensor-enhanced, autonomous surveillance purposes [96], to secure construction sites.



(a) Path length for P2P-RPL and basic RPL. (b) Paths through the sink (percentage).

Figure 3.4: P2P-RPL improvements over basic RPL.

3.3 Adapting Proactive Link-State Routing to Sensor Networks

Related publications: [135] [136], joint work with J. Schiller, T. Zahn.

Link state routing protocols are currently the dominating technology for establishing paths within Autonomous Systems in IP networks. Link state routing protocols such as OSPF, ISIS, OLSR are preferred for their small

buffer requirements (no route acquisition delays before forwarding user data) and for their robustness: they don't diverge (even better: they converge rather fast while avoiding routing loops). Such properties are of course desirable in sensor networks. The RPL routing protocol, for instance, can install loops when sensors move, or when a sensor unilaterally decreases its rank in order to be able to select an alternative parent in the DAG ([131] joint work with M. Goyal et al.). It is thus interesting to investigate how link-state routing could be adapted to sensor networks. Two fundamental issues arise quickly however:

1. the stringent memory constraints of most sensors is a challenge for link-state protocols, which typically need to store information about the whole network in order to function properly. This means that the maximum manageable network size is limited to a few tens of sensors with such an approach.

2. the amount of periodic control traffic with link-state protocols is a problem in terms of energy consumption for sensors.

While OLSR is the designated candidate among standard link state routing protocols to provide paths in a wireless sensor network – it is the lightest both in terms of control traffic and of memory requirements – OLSR as-is still suffers from the above-described limitations. I have thus explored various mechanisms that would allow OLSR to scale to bigger networks of memory constrained nodes, such as sensors. In order to decrease the amount of memory that a sensor needs to store, clustering (such as in [59]) is typically used to allow most nodes to store information describing topology within a limited scope only, instead of the whole network. Following some work I participated in during my PhD, on limiting the amount of control traffic in large spontaneous wireless networks during my PhD (such as F-OLSR ([115]) I have thus introduced a mechanism that provides dynamic clustering and hierarchical routing across clusters with OLSR [137]. This mechanism is however intrinsically not fair in the sense that some nodes (cluster heads) have to devote much more resources than others. I have thus studied other more decentralized mechanisms that could help OLSR scale better.

An alternative scheme to which I have contributed is DHT-OLSR ([136], joint work with J. Schiller, T. Zahn), a hybrid scheme using dynamic OLSR clustering enhanced with distributed hash tables unicast routing based on MADPastry [61]. The latter was chosen over other DHT approaches (such as VRR [60]], Pastry [62], Ekta [63], SSR [64]) because it considers physical locality in the construction of its routing tables. The principle of this hybrid protocol is that each sensor running DHT-OLSR maintains a regular OLSR routing table, providing efficient and low-delay routing. However, in order to avoid large amount of maintenance traffic and memory lack as the network size increases, DHT-OLSR nodes confine their OLSR signaling to a local scope. This is achieved by limiting the TTL of OLSR messages. For instance, nodes might set the TTL of the TC

messages that they issue to 3, which effectively places each node at the center of its own OLSR cell with a diameter of 6 hops. Hence, whenever a node forwards a data packet, it first tries to lookup the route in its OLSR routing table. If a valid route is found, the data packet is forwarded to the next hop on the path towards the destination. In case no route could be found in the OLSR routing table, the node engages into a DHT routing scheme, whereby packets are no longer routed based on an IP destination address but rather based on a virtual ID from the MADPastry ID space as described in [65]. Our simulations with networks of 250 nodes show that DHT-OLSR reduces the amount of traffic (data+control) by about half compared to OLSR and AODV. We expect this ratio to drop lower for bigger networks – networks of 1000 nodes are for instance envisioned by many deployments, and this order of magnitude is targeted by the ROLL working group. An implementation on real hardware is currently under way (joint work with F. Thiant), based on the Contiki OS, and running on sensors with MSP430 micro-controllers. The goal of this work is to compare our simulation results with practical experiments measuring the performance of DHT-OLSR (including traffic load, route stretch and routing table size) on a network of 250 sensors operating at 2.4 GHz with IEEE 802.15.4 radio interfaces on the Senslab testbed, and compare it to the performance of similar approaches, including Ekta [63], CrossROAD [66].

3.4 Complementary Notes & Summary

Wireless sensor networks are disruptive for standard IP protocols because of characteristics similar to wireless ad hoc and mesh networks (see Chapter 2): wireless sensor networks do not allow atomic link-local services on which many IP protocols and applications rely, and require schemes functioning with much less control traffic than that generated by standard IP protocols. On top of that, wireless sensor networks are also disruptive because sensors typically have extreme memory constraints (less than the first computers ever connected to the ARPANET) and must function with extremely small frame sizes (an order of magnitude less than standard IPv6 packet size). For these reasons, new IP standards are being developed to accommodate these characteristics. Within this effort, I have participated in several research and standardization activities, including sensor network routing protocol performance analysis, and the design of several new schemes and protocols targeting low-power and lossy networks such as wireless sensor networks.

My other activities in this domain, which I do not detail in this document, include for instance the development and standardization of a protocol measuring the quality of existing paths towards a given destination in a wireless sensor network ([129], joint work with M. Goyal, A. Brandt, J. Martocci), and participation in the deployment of two large sensor networks testbeds: Senslab [57] and FIT [58], which provide accurate and

effective experimental tools facilitating the design and development of protocols and applications suitable for sensor networks. I am also involved in a european project SAFEST [36], which is just starting and aims at developing novel sensor-enhanced distributed electronic security systems targeting public-spaces safety.

Chapter 4

Delay Tolerant Networks

Pioneer analytical work by Grossglauser and Tse [67] showed that when relaxing delay constraints and exploiting the nodes' mobility in spontaneous wireless networks, interesting gains could be achieved in terms of throughput. Such gains would benefit delay-tolerant applications such as background database synchronization, non-urgent large file transfers or messaging. This work hinted at a novel networking paradigm which was coined Delay-Tolerant Networking (DTN), and has since been further explored by various research efforts, including, but not limited to [74] [73] [72] [70] [69] [68] [71]. The idea behind DTNs is simply that if data communication can wait for better paths to become available due to network topology changes, substantial gains in throughput will be obtained – if by "better" we mean "more throughput". Recent work has focused on a radical version of this paradigm: even if the network graph is such that no path to the destination ever exist at any given time, data could still be stored and carried by a sequence of nodes that will eventually end up in the vicinity of the destination and deliver the data, thus improving the throughput from 0 to something strictly positive. Such networks are sometimes referred to as Intermittently Connected Networks (ICNs), but more commonly also called DTNs – in the following we will use the latter denomination. The DTN paradigm stems from a variety of industrial contexts, ranging from sparse spontaneous wireless network connecting mobile nodes (such as vehicular ad hoc networks), to networks gathering fixed nodes that may suddenly switch to sleep mode at any time in order to save energy (such as sensor networks), or even to deep space internetworking, where nodes can only infrequently communicate with one another, and round-trip times are extremely long.

4.1 How are Delay Tolerant Networks IP-Disruptive?

Spontaneous wireless networks such as DTNs are IP-disruptive because, similarly to ad hoc networks (see Chapter 2), they do not allow atomic link-local services on which many IP protocols and applications rely. DTNs are furthermore disruptive because they do not allow IP protocols to assume end-to-end connectivity exists, which, in practice, means the following:

1. **Instantaneous replies cannot be expected.** Schemes based on instantaneous request/response (used by many protocols, including HTTP, DNS, TCP, DHCP, ARP to name a few) do not function because they cannot estimate appropriate response time-out, and thus give up, failing to proceed correctly.

2. **Routes cannot be derived from individual network topology snapshots.** Standard IP routing protocols do not function because they establish paths based on ”snapshots” of the network topology, and if none such snapshot includes a path to a remote destination, they give up and declare this destination unreachable.

3. **Routers cannot be expected to be always on.** Standard IP routing protocols may even fail to establish local communication between neighbor routers. Indeed, these protocols expect routers to be always on and responsive, if not out-of-service. However, in some DTN scenarios such as networks of battery-saving sensor nodes, routers often switch to sleep mode during which they are unresponsive.

The principle of DTNs is to exploit topology accumulation over time: after some delay, accumulated topology becomes connected and paths can be discovered. However, the delay before topology has sufficiently accumulated has severe consequences on router hardware designs. Indeed, so far, the end-to-end connectivity assumption allowed a simple memory management policy: if a router receives a packet but currently has no path available to reach the destination of this packet, it just erases this packet. This policy enabled routers to function with rather small memory, even if they have to handle of lot of data traffic (such as the biggest routers at the core of the Internet). A departure from this policy, whereby routers must on the contrary store en-route data for a while until an appropriate path becomes available, would bring many new issues in the picture. One of these issues is that routers' memory size requirements would change radically: their needs in terms of memory would sky-rocket in an unmanageable way if user traffic is substantial.

The community has recently initiated efforts addressing the limitations of standard IP protocols concerning DTNs. Initially targeting Interplanetary Internet (standard communication protocols between spacecrafts, satellites and ground stations in support of deep space exploration), Vint Cerf *et al.* have developed a delay-tolerant networking architecture [75] which defines an intermediate layer between transport and application

layers, called the *bundle layer*. The bundle layer enables nodes to split data to be transmitted into variable length units called bundles, and to take temporary custody of some bundles during the time topology is accumulated, before they can be transmitted further towards their destination. This architecture is the base on which the DTNRG research group [77] builds to elaborate new IP standards targeting DTNs, such as standard bundle formats with the Bundle Protocol [78], or reliable transport with the Licklider Transmission Protocol [79], a protocol providing transport between pairs of nodes within radio range of one another in a DTN. The DTNRG research group is also currently working on the specification of a routing protocol targeting delay tolerant networks: PRoPHET ([80], Probabilistic Routing Protocol for Intermittently Connected Networks). PRoPHET is an enhanced version of the epidemic routing protocol [81], based on a pruning mechanism which aims at reducing data dissemination costs and router memory requirements while still achieving a performance close to the optimal, plain epidemic routing. I have recently been focusing on this routing aspect in the context of delay tolerant vehicular networks.

4.2 Information Propagation Speed in Vehicular DTNs

Related publications: [140] [141] [146], joint work with P. Jacquet, B. Mans, R. Rodolakis.

Ad hoc vehicular networks (VANETs) have recently been the subject of a number of studies, targeting applications such as safety on the road. Delay tolerant architectures have therefore been considered in this context, and various analytical models have been proposed. Studies such as [82, 83, 84] have for instance focused on information propagation speed in vehicular DTNs. These studies develop a model based on space discretization, and derive upper and lower bounds on the information propagation speed with epidemic routing in the highway scenario, under the assumption that the radio propagation speed is finite. These bounds, although not converging, indicate the existence of a phase transition for the information propagation speed, with respect to the density of vehicles on the road.

We have thus analyzed the highway scenario further. More precisely, we have considered a bidirectional vehicular network, such as a road or a highway, where vehicles move in two opposite directions (say east and west, respectively) at speed v, as depicted in Fig. 4.1. We considered eastbound vehicle density as Poisson with intensity λ_e, and westbound vehicle density is Poisson with intensity λ_w (an approximation that makes sense since [85] shows that inter-vehicle distance is very close to being exponentially distributed on highways with fluid traffic condition). Furthermore, we considered that the radio propagation speed (including store and forward processing time) is infinite, and that the radio range of each transmission in each direction is of length R. A packet propagates such as an epidemic headed eastbound: it moves toward the east jumping from

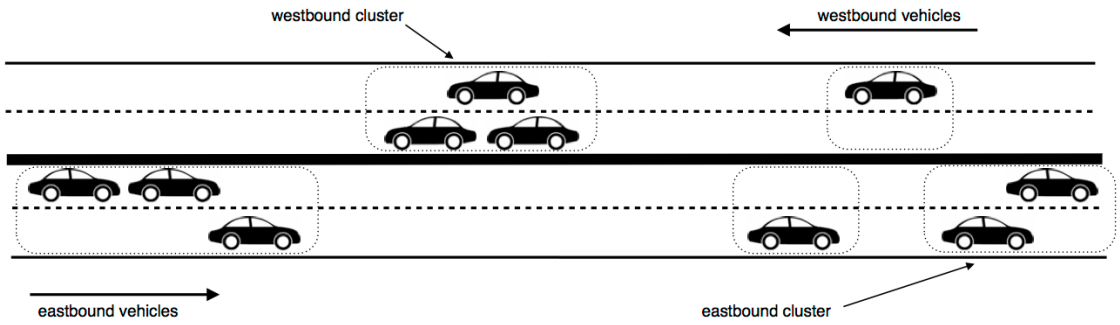
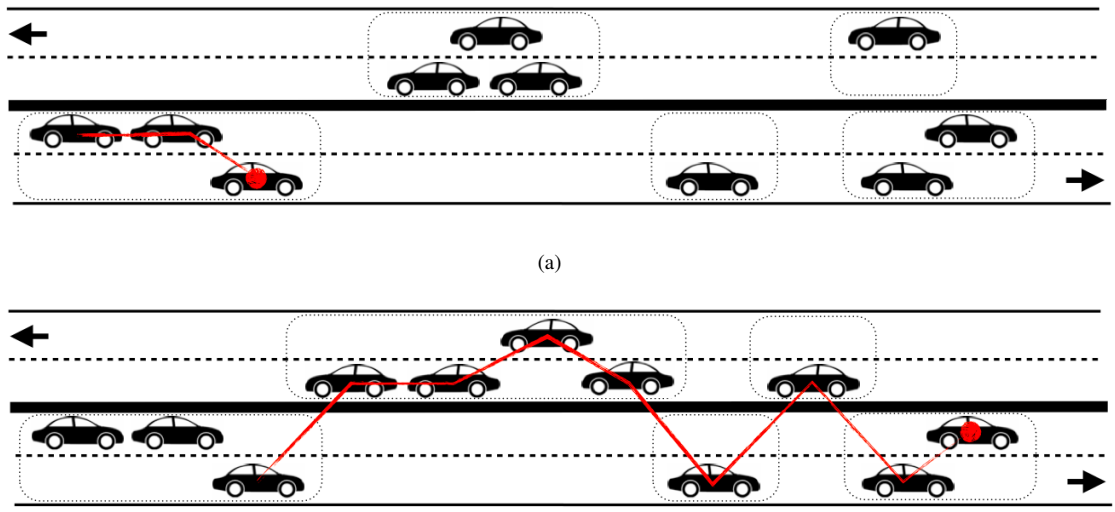


Figure 4.1: Model of a bidirectional vehicular network on a highway.

car to car until it stops because the next car is beyond radio range, as shown in Fig. 4.2. The propagation is instantaneous, since we assume that radio routing speed is infinite. The beacon waits on the last eastbound car until the gap is filled by westbound cars, so that the beacon can move again to the next eastbound car. By analyzing the distribution of the clusters of cars on each lane, we have shown in [140] and [141] (joint



(a)

(b)

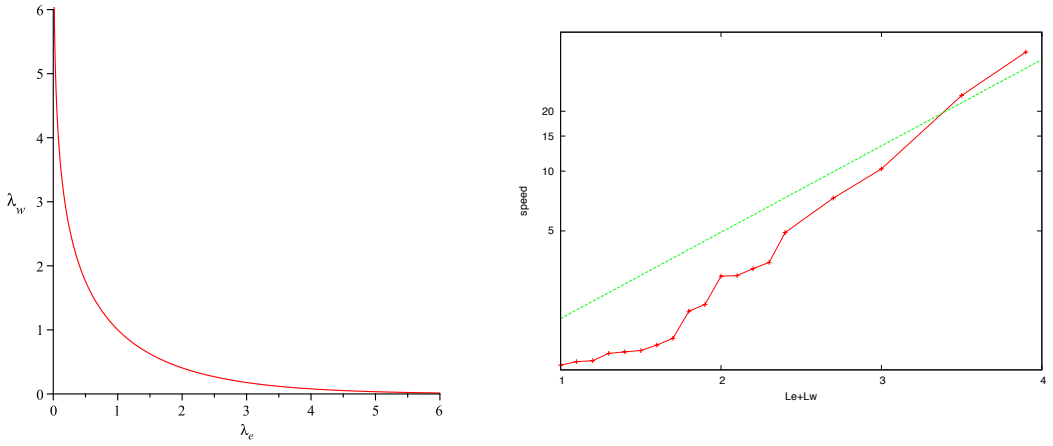
Figure 4.2: Eastbound information propagation: the beacon waits on the last eastbound car (a), until the gap is bridged by westbound cars so that the beacon can move eastwards again (b).

work with P. Jacquet, B. Mans, R. Rodolakis) that, concerning the information propagation speed in such an environment, a phase transition occurs when the vehicle densities per lane, λ_e and λ_w, satisfy the equation $\lambda_e R e^{-\lambda_e R} = \lambda_w R e^{-\lambda_w R}$, an expression which can be simplified without loss of generality by considering that the transmission range $R = 1$, and which thus becomes the very simple identity: $\lambda_e e^{-\lambda_e} = \lambda_w e^{-\lambda_w}$. We have also extended this result when relaxing assumption about the radio propagation speed, and derived a similar

simple identity when radio propagation speed is finite.

What this model predicts is that when the vehicle density (λ_e, λ_w) is below the threshold defined by the identity we derived, depicted in Fig. 4.3(a), information propagation speed is 0 in the referential of the eastbound cars, while above the threshold, information propagates much faster on average, in $O(e^{\lambda_e+\lambda_w})$ when densities are large.

We have verified this characteristic via simulation results we obtained on several platforms (ONE [100] and Maple [101]) which have confirmed the model, as shown for instance in Fig. 4.3(b), where we observed the expected exponential growth. This model and the results derived from it are useful in order to evaluate the performance of future standard IP protocols targeting DTNs based on epidemic routing (such as PRoPHET), by providing upper bounds to measure up with. The above results stem from an analysis we performed for the



(a) (b)

Figure 4.3: Information propagation threshold with respect to (λ_e, λ_w). (a) Below the curve, the average information propagation speed is limited to the vehicle speed (*i.e.*, the propagation speed is 0 in the referential of the eastbound cars), while above the curve, information propagates faster on average. (b) ONE simulations, information propagation speed for $\lambda_e = \lambda_w$, with respect to $\lambda_e + \lambda_w$, in semi-log scale, compared to the theoretically predicted asymptotic exponential growth.

european project OPNEX [34] in which I took part (with partners including INRIA, Technicolor, CERTH, PUT and FU Berlin). OPNEX focused on protocol design and experimentation for spontaneous wireless network, based on systems and optimization theory, used as the foundation for underlying algorithms that provably achieve full transport capacity of wireless systems.

We have recently extended the above results with a study of the cases of roads or highway with k lanes

of vehicles with various speeds and real-time radio communication range variations at the MAC layer. In this context, we have shown in [146] (joint work with P. Jacquet, B. Mans, R. Rodolakis) that the behavior remains essentially the same. We have shown that a phase transition exists as soon as there are $k > 1$ lanes with different vehicle speeds and appropriate densities. We derived bounds on the corresponding threshold as a simple, similar relationship between the vehicle density on the fastest lane and the sum of the vehicle densities on the other lanes. These characteristics were also verified via simulations on several platforms.

4.3 Complementary Notes & Summary

Delay tolerant networks are disruptive for standard IP protocols because they do not allow IP protocols to assume end-to-end connectivity exists. This means in particular that instantaneous request/reply schemes (on which many protocols are based) will not function. Moreover, standard routing protocols will fail to find paths towards destinations to which end-to-end connectivity never exists, though it is still possible to deliver data to this destination, with some delay. For these reasons, new IP standards are being developed to accommodate these characteristics. Within this effort, I have participated in research activities that analyzes the achievable performance of epidemic routing in the context of vehicular DTNs. The achievable speed of information propagation we derived can serve as an upper bound to measure up with for evaluating the performance of routing protocols currently considered for standardization, targeting DTNs, which are based on similar mechanisms.

My other activities in this domain include my contributions to OSPF protocol extensions targeting vehicular networks ([121], joint work with T. Clausen, P. Jacquet, D. Nguyen), and analyzing the limitations of IPv6 operation over wireless access in vehicular environments ([142], joint work with T. Clausen, R. Wakikawa). I am also taking part in the GETRF project [35] within which I will focus on opportunistic routing schemes applicable in delay-tolerant environments such as vehicular networks. The GETRF project aims at energy efficiency, delay tolerance and network capacity improvements in networks where user experience is inferior due to node mobility.

Chapter 5

Conclusions & Perspectives

The research contributions described in this document were driven by the recent evolutions of wireless communications, and by the recent trends towards more collaborative network layer paradigms. The thread I followed is the compatibility, in practice, with standard IP protocols currently at work in today's Internet. Indeed, absent such compatibility, slim are the chances a given solution would actually be employed in real life and have a concrete impact. If one cannot just "reboot" the Internet to accommodate a convenient fresh start, one can nevertheless drive a continuous evolution of the Internet towards what is needed to allow seamless spontaneous wireless networking. In other words, research in this domain has to not only discover an alternative state in which things would work better, but also discover smooth transitions towards this alternative state, starting from the state we are currently in. The IETF is one of the important venues where such transitions are discussed, evaluated and designed. Within this community, I have contributed in multiple ways to IP protocols' standardization – an activity which I intend to further develop in the future. Considering the various efforts that have taken place so far to alleviate IP-disruptive aspects of spontaneous wireless networks, one can identify 4 main categories of solutions, as described below.

Adaptation layer developments. This type of solution proposes to design intermediate layers, which interface between two of the legacy layers, i.e. from bottom up: (1) the physical layer, (2) the MAC layer, (3) the network layer, (4) the transport layer and (5) the application layer. Such approaches enable interoperability with legacy software by providing a black-box which emulates an appropriate behavior, compatible with upper layers, operating on top of disruptive lower layers. The system that results from such an approach is thus significantly more complex than the legacy system, in that it introduces a whole new "world" of protocols in addition to the legacy protocols. However, this approach can be effective in practice: a current example

is 6LOWPAN [44], which designed a series of mechanisms at layer 2.5 (i.e. sitting between layer 2 and 3), enabling the operation of standard IP protocols at layers 3 and above on the IEEE 802.15.4 MAC layer. For instance, Fig. 1 in [102] depicts this adaptation layer, and compares the performance of mesh-under and route-over, two approaches coping with the disruption of axiom 1 (see Section 1.3). On one hand, the mesh-under approach aims at emulating an ethernet link via routing below the network layer (similarly to 802.11s [103]) to enable protocols at the network layer and above to function as usual. On the other hand, the route-over approach aims at leveraging routing protocols in the network layer, as usual, to provide connectivity in spontaneous wireless networks. The analysis in [102] concludes that the route-over approach is preferable in terms of reliability and performance. The route-over approach is actually an example of a second type of solution, described below.

Intra-layer optimizations. This type of solution proposes to modify or replace specific protocols currently in use within a legacy layer, to cope with IP-disruptive characteristics from lower layers. Several of the efforts I have contributed to fall in this category, including for instance the protocols MPR-OSPF [110], P2P-RPL [127], scalability techniques such as DHT-OLSR [136] or OLSR-Trees [137]. I have also contributed to performance analysis of proposed solutions of this type in [132] [133] [131]. The advantage of this type of solution is that interoperability with legacy software is easier to assess, since one is just replacing a spare part of the whole ”engine”, instead of changing the way the engine functions. There are however limits to what one can achieve when taking this approach: it is unlikely that one can reach the moon, propelled by a regular diesel car engine, if one is allowed to replace only a single, small part of that engine. Yet other types of solutions have thus been proposed, described in the following.

Cross-layer optimizations. This type of solution proposes to partially or totally abolish the distinction between two or more legacy layers, to produce a radically new system that performs significantly better, thanks to new protocols that can leverage cross-layer information to better cope with IP-disruptive lower layers. I have participated in a project [145] [34] that aimed at studying and experimenting with various cross-layer approaches targeting spontaneous wireless networking, such as systems based on back-pressure [104] [105] [139], among others. This approach is probably the most disruptive, as its deployability and interoperability with standard legacy software is in general difficult to assess if at all possible – lack of interoperability is often the price to pay for radical performance improvements. There is however yet another type of solution proposing drastic changes while maintaining interoperability with legacy layers, as described below.

Top layer developments. This type of solution aims at building a radically new system sitting on top of

the legacy protocol stack, at the application layer. This is an ”Internet-as-a-cable” approach, with novel mechanisms efficiently using this ”cable” to cope with IP-disruptive characteristics. The advantage of this approach is that it can easily be designed to be compatible with current and future IP standards, without being confined in what it endeavors, because above the application layer, the sky is the limit, so to speak. For instance, we have recently witnessed how application layer constructions such as P2P networks [97] or social networks have had an enormous impact on today's Internet. One example of such construction to which I have been interested in, is the DTN architecture [77] [78] [79] designed above the transport layer by the IETF. I have participated in this realm, targeting vehicular delay tolerant networks, to performance evaluations [140] [141] [146] of epidemic routing, the base of the proposed DTN architecture's routing protocol [80]. In the near future, I intend to continue working on solutions of this particular type, if for one thing, because of the freedom they allow, and the enormous potential impact they can have.

Going further, it is perhaps worthy to observe the algorithmic trends that have developed, as a response to IP-disruptive characteristics of spontaneous wireless network, and violations of axioms listed in the beginning of this document (see Section 1.3). In response to violations of Axiom 1, which means no stable IP link to build on, fast-pace algorithms using shorter monitoring periods have been developed in conjunction with smarter topology information compression such as [113] [112] [94] [93], in order to curb the amount of control traffic necessary for the system to operate. More opportunistic and more distributed paradigms are favored to cope with the specific dynamics of spontaneous networks [107]. The price of these algorithm is however a poorer scalability in terms of practical network size and number of users, compared to wired and cellular networks. In response to violations of Axiom 2, which means no end-to-end connectivity, predictive algorithms and more opportunistic techniques have been developed such as smart epidemic dissemination [80] [88]. The price to pay is however increased overhead, and delays due to the time needed to accumulate an appropriate time-space continuum from source to destination [89]. In response to violations of Axiom 3, which means that routers are not always on, more agile and more distributed MAC layer mechanisms have been developed such as distributed node coloring for self-organized TDMA [87] , or opportunistic algorithms that dynamically control on/off periods of a node depending on its usefulness in the network [86]. The price to pay is however more control traffic, and longer convergence time. On the contrary, in response to violations of Axiom 4 (which means that routers have very low CPU, power, memory capacities) more centralized approaches have been employed, outsourcing duties to one or more nodes with superior capacities (for instance the sink in a sensor network, using source routing with RPL in non-storing mode [51]). More opportunistic mechanisms, such as reactive schemes [26] [127] which provision resources only on-demand, instead of systematic pre-provisioning, aim at saving resources when pre-provisioning is too wasteful. The price to pay is

the delay one needs to wait until a new resource is allocated, when its need is detected.

Perspectives

At various scales, from the biggest routers of the Default-Free Zone at the core of the Internet down to the smallest sensors of the Internet of Things, one can observe similar issues: state of the art algorithms and protocols incur too much memory to store the necessary network layer information, even when projected hardware evolutions and Moore's law are taken into account. The amount of control traffic becomes unmanageable due to the sheer number of devices joining the network, their mobility or the flickering patterns of their activity. In the near future, I am planning to take part in the emergence of new standard protocols that will overcome these limitations. Since I have joined INRIA, I have started tackling some aspects of this issue with several collaborators, via the analysis and development of several new routing schemes and protocols. Much remains however to be done in this domain, the biggest scientific challenge being to elaborate new algorithms and feed them to IP-interoperable protocols that are agile enough to scale from small to quasi-infinite network sizes (10^{10} elements) with small convergence time, while providing optimal paths through the network, with very little control traffic and memory requirements. Current approaches make compromises on at least one of these constraints. Future protocols will have to provide ultimate agility and satisfy all of these constraints at once. New levels of agility will also be needed for protocols aside of just routing protocols: transport protocols optimizing performance on spontaneous networks when they are integrated in the Internet, or IP autoconfiguration in spontaneous wireless networks are other examples of open problems of interest in this field, because these issues need to be addressed in order to fully, natively integrate spontaneous networking in the global network – a goal I believe is worth pursuing.

A future can be envisioned, where the simultaneous convergence of mobile operating systems (in particular Android, open-source, based on Linux) and the proliferation of smart phones on one hand, combined on the other hand with the emergence of independent community wireless networks such as Freifunk [13] or similar concepts such as Commotion [20], give birth to the deployment of countless "social wireless networks" directly plugged at layer 3 (i.e. spontaneous wireless networks), providing a real complementary alternative to infrastructure networks. This new variety of networks would support new trends feeding on viral developments, distributed smartphone CPUs and autonomous communication capabilities. This new variety of networks would probably be intermittently connected to the Internet's giant component, either by

force (unavailable uplink due to difficult environmental, political context) or by choice (privacy preservation [99][98]), and connectivity inside such networks may itself be opportunistic and intermittent depending on the density of users. Such scenarios highlight the need for new protocols optimizing the use of intermittent connectivity in IP networks, leveraging smart predictive topology strategies for instance. Such optimization is quite a challenge with many aspects, including analytical, algorithmical and interoperability aspects which promise to give birth to a wealth of novel problems and solutions – a field currently in its infancy, in which I intend to actively participate in the near future.

As we have seen, the approach considered currently to absorb DTNs in the Internet architecture consists in the elaboration of a new, dedicated layer in the protocol stack, between the application layer and the transport layer. In this realm, I intend to take part in application layer work – a layer on which I have not focused much so far. I expect this new field of my activity will give me other opportunities to contribute at the application layer outside of the realm of DTNs. Such opportunities may incidentally unveil new business models in an Internet of the future which will natively run new paradigms such as spontaneous wireless networks, as well as other types of social networks. Current industrial heavyweights such as, among others, Google, Samsung, Apple, Facebook, HTC or Cisco will surely take advantage of these new business models yet to come, based on this future type of connectivity. However, they will surely not be the only players: history shows that grassroots movements often shuffle the landscape on the Internet.

The ”new world” currently emerging at the application layer, combined with the increasing pervasiveness of sensing and computing devices, composes a meta-system that produces more and more data, more and more detailed and real-time. Novel problems arise pertaining to how to handle this system. Data becomes so quickly unmanageable because of its sheer volume: issues related to big data are currently the dreams and nightmares of countless start-ups and bigger companies around the world, and this just the beginning. However, I have become more and more aware of another problem that I would like to start tackling in the future: privacy. We used to say Internet has transformed the world in a ”global village” in the good sense of the term: bringing people together. The system we are building now tends to highlight the bad sense of this term: there is no privacy anymore. Indeed, the system we are building dynamically extracts more and more detailed information about our private life as it happens, to the point where this is obviously becoming an issue – and again, this is just the beginning. The massive exploitation of updated, detailed information about our private life is the oil that powers a fast-growing part of our economy. Typically, the right to extract and exploit this information is (more or less implicitly) traded for free on-line services which people are in general addicted to, but paradoxically, no longer ready to pay for. We are thus in a deadlock, in dire need

for revamped global privacy policies that will give obvious choices to people, based on novel mechanisms that will explicitly offer various levels of privacy as a service – similarly to a firewall for instance. Several intermediate levels (the definition of which are the heart of the problem) would ensure accurately scoped privacy or anonymity characteristics, while still providing a signal that is exploitable, to a precise, controlled extent (see for instance [91] [92]), by companies ready to offer on-line services in exchange for that signal. The optimization challenges stemming from this type of problems are of high interest for me not only scientifically, but also socially because, for a wide spectrum of key activities in the near future, including cloud services, or smart-metering for instance, trust in such ”privacy-level-agreements” are needed to avoid a world where privacy has utterly disappeared – another goal I believe is worth pursuing.

Bibliography

References

[1] Baran, P., et al, ”On Distributed Communications”, Volumes I-XI, RAND Corporation Research Documents, August 1964.

[2] Cerf V., and R. Kahn, ”A Protocol for Packet Network Interconnection”, IEEE Trans. on Communications, Vol. COM-22, No. 5, pp. 637-648, May 1974.

[3] The Internet Engineering Task Force (IETF), www.ietf.org

[4] J. Postel, Ed., ”Transmission Control Protocol”, IETF Request For Comments, RFC 761, January 1980.

[5] T. Berners-Lee, R. Fielding, H. Frystyk, ”Hypertext Transfer Protocol – HTTP1.0”, RFC 1945, May 1996.

[6] N. Abramson, ”The ALOHA System - Another alternative for computer communications”, AFIPS 37, pp. 281285, April 1970.

[7] UK Office for National Statistics 2011 Report on Internet Access - Households and Individuals, August 2011.

[8] ”More Indians Using Mobiles to Access Facebook, Twitter”, study published in The Times of India on Jul 16, 2012.

[9] ”Customers Angered as iPhones Overload AT&T”, article published in The New York Times on Sept. 2, 2009.

[10] IEEE Standards Association, http://standards.ieee.org/about/get/802/802.11.html, April 2012.

[11] 3GPP Telecommunications Standards Body, www.3gpp.org, April 2012.

[12] T. Clausen, Ed., P. Jacquet, Ed., ”Optimized Link State Routing Protocol (OLSR)”, IETF Request For Comments, RFC 3626, October 2003.

[13] The Freifunk Wireless Community Networks, http://www.freifunk.net

[14] Austrian Wireless Community Network, http://www.funkfeuer.at

[15] Athens Wireless Community Network, http://awmn.net

[16] Barcelona Wireless Community Network, http://www.guifi.net

[17] Rome Wireless Community Network, http://www.ninux.org

[18] Boston Wireless Community Network, http://openairboston.net/

[19] The Occupy Wall Street Affinity Group, http://occupywallst.org/

[20] The Commotion Wireless Project, https://code.commotionwireless.net/projects/commotion

[21] The A FIRE experimental testbed on Community Networks, http://confine-project.eu

[22] The International Summit for Community Wireless Networks, http://www.wirelesssummit.org

[23] D. Thaler, ”Evolution of the IP Model,”IETF Request For Comments, RFC 6250, May 2011.

[24] R. Coltun, D. Ferguson, J. Moy, ”OSPF for IPv6,” IETF Request For Comments, RFC 2740, December 1999.

[25] T. Clausen, P. Jacquet, ”Optimized Link State Routing (OLSR) Protocol,” IETF Request For Comments, RFC 3626, October 2003.

[26] C. Perkins, E. Royer, S. Das, ”Ad Hoc On-Demand Distance Vector (AODV) Routing,” IETF Request For Comments, RFC 3561, July 2003.

[27] A. Roy, M. Chandra, ”Extensions to OSPF to Support Mobile Ad Hoc Networking,” IETF Request For Comments, RFC 5820, March 2010.

[28] R. Ogier, P. Spagnolo, ”Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding,” IETF Request For Comments, RFC 5614, August 2009.

[29] D. Oran,”OSI IS-IS Intra-domain Routing Protocol,” IETF Request For Comments, RFC 1142, 1990.

[30] T. Clausen, C. Dearlove, P. Jacquet, U. Herberg, ”The Optimized Link State Routing Protocol version 2,” IETF Internet Draft, March 2012.

[31] The MOBISIC Project, www.systematic-paris-region.org/fr/projets/mobisic

[32] The e-compagnon Project, www.systematic-paris-region.org/fr/projets/e-compgnon

[33] The SMARTMESH Project, www.systematic-paris-region.org/fr/projets/smartmesh

[34] The OPNEX Project, www.opnex.eu

[35] The GETRF Project (DGA/ANR), Gestion Efficace des Transmissions dans les Réseaux sans Fil.

[36] The SAFEST Project (ANR/BMBF), Structure pour des Alertes Rapides de Sécurité dans les Espaces Publics. http://safest.realmv6.org

[37] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF Request For Comments, RFC 4944, September 2007.

[38] The Auto-ID Laboratories, www.autoidlabs.org

[39] Electronic Product Code Global, www.epcglobalinc.org

[40] C. Bormann, "Guidance for Light-Weight Implementations of the Internet Protocol Suite," IETF Internet Draft, January 2012.

[41] T. Narten, E. Nordmark, W. Simpson, H. Soliman, "Neighbor Discovery for IPv6", IETF Request For Comments, RFC 4861, September 2007.

[42] T. Narten, S. Thomson, T. Jinmei, "IPv6 Stateless Address Autoconfiguration", IETF Request For Comments, RFC 4862, September 2007.

[43] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, "Dynamic Host Configuration Protocol for IPv6", IETF Request For Comments, RFC 3315, July 2003.

[44] IPv6 over Low power WPAN (6lowpan) IETF Working Group, https://datatracker.ietf.org/wg/6lowpan/

[45] Routing Over Low power and Lossy networks (roll) IETF Working Group, https://datatracker.ietf.org/wg/roll/

[46] Light-Weight Implementation Guidance (lwig) IETF Working Group, https://datatracker.ietf.org/wg/lwig/

[47] Constrained RESTful Environments (core) IETF Working Group, https://datatracker.ietf.org/wg/core/

[48] The Contiki Operating System, www.contiki-os.org/

[49] A. Dunkels, B. Gronvall, T Voigt, ”Contiki - a lightweight and flexible operating system for tiny networked sensors,” in Proceedings of the First IEEE Workshop on Embedded Networked Sensors (Emnets-I), Tampa, Florida, USA, November 2004.

[50] The TinyOS Operating System, http://www.tinyos.net/

[51] T. Winter, P. Thubert, ”RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” IETF Request For Comments, RFC 6550, March 2012.

[52] P. Lewis, T. Clausen, J. Hui, O. Gnawali, J. Ko, ”The Trickle Algorithm,” IETF Request For Comments, RFC 6206, March 2011.

[53] J. Martin, “Distribution of the time through a directed acyclic network,” Oper. Res., vol. 13, pp. 44-66, 1965.

[54] A. Brandt, J. Buron, G. Porcu, ”Home Automation Routing Requirements in Low-Power and Lossy Networks,” IETF Request For Comments, RFC 5826, April 2010.

[55] J. Martocci et al., ”Building Automation Requirements in Low-Power and Lossy Networks,” IETF Request For Comments, RFC 5867, June 2010.

[56] K. Pister, P. Thubert et al., ”Industrial Routing Requirements in Low-Power and Lossy Networks,” IETF Request For Comments, RFC 5673, October 2009.

[57] Senslab: Very Large Scale Open Wireless Sensor Network Tesbed, http://www.senslab.info/

[58] FIT: The Future Internet (of Things) Platform, http://fit-equipex.fr/

[59] Z. J. Haas, M. R. Pearlman, and P. Samar, ”The Zone Routing Protocol (ZRP) for Ad Hoc Networks,” IETF Internet Draft, 2002.

[60] M. Caesar, M. Castro, E. Nightingale, G. OShea, and A. Rowstron, ”Virtual Ring Routing: Network routing inspired by DHTs,” in Proc. of ACM SIGCOMM06, September 2006.

[61] T. Zahn and J. Schiller, ”MADPastry: A DHT Substrate for Practicably Sized MANETs,” in Proc. of ASWN, June 2005.

[62] A. Rowstron, P. Druschel. ”Pastry: Scalable, distributed object location and routing for large scale peer-to-peer systems,” In Proc. of Middleware, November 2001.

[63] H. Pucha, S. M. Das, and Y. C. Hu, ”Ekta: An Efficient DHT Substrate for Distributed Applications in Mobile Ad Hoc Networks,” in Proc. of WMCSA 2004, December 2004.

[64] T. Fuhrmann, ”Scalable Routing for Networked Sensors and Actuators,” in Proc. of SECON 2005, September 2005.

[65] T. Zahn, J. Schiller, ”DHT-based Unicast for Mobile Ad Hoc Networks,” MP2P Proceedings, 2006.

[66] F. Delmastro. ”From Pastry to CrossROAD: CROSS-layer Ring Overlay for AD hoc networks”. In Proc. of PerCom, March 2005.

[67] M. Grossglauser and D. Tse, ”Mobility increases the capacity of ad hoc wireless networks”, Infocom, 2001.

[68] A. Lindgren, A. Doria, and O. Schelén, ”Probabilistic routing in intermittently connected networks,” in Proceedings of The First International Workshop on Service Assurance with Partial and Intermittent Resources (SAPIR 2004), August 2004.

[69] J. Leguay, T. Friedman, and V. Conan, ”Evaluating mobility pattern space routing for DTNs,” in Proc. INFOCOM, 2006.

[70] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, ”Impact of human mobility on the design of opportunistic forwarding algorithms,” in Proceedings of IEEE INFOCOM, 2006.

[71] P. Hui, A. Chaintreau, R. Gass, J. Scott, J. Crowcroft, C. Diot, ”Pocket Switched Networking: Challenges, feasibility and implementa- tion issues,” in Proceedings of the Workshop on Autonomic Communi- cations, ser. LNCS, vol. 3457. Springer-Verlag, 2005.

[72] S. J. Rahul C Shah, Sumit Roy and W. Brunette, ”Data mules: Modeling a three-tier architecture for sparse sensor network,” in IEEE Workshop on Sensor Network Protocols and Applications (SNPA), May 2003.

[73] M. A. Wenrui Zhao, E. Zegura, ”A message ferrying approach for data delivery in sparse mobile ad hoc networks,” in ACM Mobihoc, May 2004.

[74] K. Fall, ”A delay-tolerant network architecture for challenged internets,” in Proceedings of ACM SIGCOMM, 2003.

[75] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, H. Weiss, ”Delay-Tolerant Networking Architecture,” IETF Request For Comment RFC 4838, 2007.

[76] The Internet Research Task Force (IRTF), http://irtf.org/

[77] The Delay-Tolerant Networking IRTF Research Group (DTNRG), http://irtf.org/dtnrg

[78] K. Scott, S. Burleigh, ”Bundle Protocol Specification,” IETF Request For Comments, RFC 5050, November 2007.

[79] M. Ramadas, S. Burleigh, S. Farrell, ”Licklider Transmission Protocol,” IETF Request For Comments, RFC 5326, September 2008.

[80] A. Lindgren, A. Doria, E. Davies, S. Grasic, ”Probabilistic Routing Protocol for Intermittently Connected Networks,” IETF Request For Comments, RFC 6693, September 2012.

[81] A. Vahdat, D. Becker, ”Epidemic Routing for Partially Connected Ad Hoc Network,” Duke University Technical Report CS-200006, April 2000.

[82] A. Agarwal, D. Starobinski, T. Little, ”Phase Transition Behavior of Message Propagation in Delay Tolerant Vehicular Ad Hoc Networks”. MCL Technical Report No. 12-12-2008, 2008.

[83] A. Agarwal, D. Starobinski, T. Little, ”Analytical Model for Message Propagation in Delay Tolerant Vehicular Networks”. Proceedings of the Vehicular Technology Conference (VTC). Singapore, 2008.

[84] A. Agarwal, D. Starobinski, T. Little, ”Exploiting Mobility to Achieve Fast Upstream Propagation”. Proceedings of Mobile Networking for Vehicular Environments (MOVE) at IEEE INFOCOM. Anchorage, 2007.

[85] N. Wisitpongphan, F. Bai, P. Mudalige, O. Tonguz, ”On the Routing Problem in Disconnected Vehicular Ad-hoc Networks,” in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), 2007.

[86] Green Communications, www.green-communications.fr

[87] S. Mahfoudh and P. Minet, ”Maximization of energy efficiency in wireless ad hoc and sensor networks with SERENA,” Journal on Mobile Information System, 2009.

[88] B. Blaszczyszyn, A. Laouiti, P. Muhlethaler, and Y. Toor, ”Opportunistic broadcast in vanets (ob-van) using active signaling for relays selection,” in ITS Telecommunications, 2008, Oct. 2008, pp. 384389.

[89] P. Jacquet, B. Mans and G. Rodolakis, ”On space-time Capacity Limits in Mobile and Delay Tolerant Networks,” IEEE INFOCOM, San Diego, 2010.

[90] T. Henderson, P. Spagnolo, J. Kim, ”A Wireless Interface Type for OSPF”, Proceedings of the IEEE Military Communications Conference (MILCOM), pp. 137-145, IEEE ComSoc, Boston, MA (United States), 2003.

[91] Cynthia Dwork, ”Differential Privacy,” in proceedings of International Colloquium on Automata, Languages and Programming (ICALP), pages 112, 2006.

[92] S. Banerjee, N. Hegde, L. Massoulie, ”The Price of Privacy in Untrusted Recommendation Engines”, Arxiv preprint arXiv:1207.3269, 2012.

[93] R. Ogier, P. Spagnolo, ”Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding,” IETF Request For Comments, RFC 5614, August 2009.

[94] T. Henderson, P. Spagnolo: ”Comparison of Proposed OSPF MANET Extensions,” Proceedings of the Military Communications Conference (MILCOM’06). 2006.

[95] V. Mhatre, C. Rosenberg, ”Design Guidelines for Wireless Sensor Networks: Communication, Clustering and Aggregation,” Ad-hoc Networks Journal, Elsevier, 2004.

[96] V. Mhatre, C. Rosenberg, D. Kofman, R. Mazumdar, and N. Shroff, ”A Minimum Cost Heterogeneous Sensor Network with a Lifetime Constraint,” IEEE Transactions on Mobile Computing, Jan. 2004.

[97] S. L. Blond, A. Legout, W. Dabbous, ”Pushing BitTorrent Locality to the Limit,” Computer Networks Journal, Elsevier, 2011.

[98] S. Le Blond, A. Legout, F. Lefessant, W. Dabbous, M. Ali Kaafar, ”Spying the world from your laptop,” in Proceedings of LEET, 2010.

[99] S. Le Blond, P. Manils, C. Abdelberi, M. Kaafar, C. Castelluccia, A. Legout, W. Dabbous, ”One Bad Apple Spoils the Bunch: Exploiting P2P Applications to Trace and Profile Tor Users,” in Proceedings of LEET, 2011.

[100] A. Keranen, J. Ott and T. Karkkainen, ”The ONE Simulator for DTN Protocol Evaluation,” SIMUTools09: 2nd International Conference on Simulation Tools and Techniques. Rome, 2009.

[101] Maple Technical Computing and Simulation, http://www.maplesoft.com/

[102] A. H. Chowdhury, M. Ikram, H.-S. Cha, H. Redwan, S. M. S. Shams, K.-H. Kim, S.-W. Yoo, ”Route-over vs mesh-under routing in 6lowpan,” in Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, IWCMC 09, (New York, NY, USA), pp. 12081212, ACM, 2009.

[103] IEEE 802.11s: Mesh Networking, Extended Service Set (ESS), 2011.

[104] R. Laufer, T. Salonidis, H. Lundgren, and P. L. Guyadec. XPRESS: A cross-layer backpressure architecture for wireless multi-hop networks. In Proc. ACM MobiCom, 2011.

[105] Andrzej Szwabe, Pawel Misiorek, and Przemyslaw Walkowiak. "Delay-Aware NUM System for Wireless Multi-hop Networks". In Proceedings of IEEE European Wireless 2011 (EW2011), pages 530537, Vienna, Austria, April 2011.

Publications

[106] E. Baccelli, M. Townsley, "IP Addressing Model in Ad Hoc Networks," IETF Request For Comments, RFC 5889, September 2010.

[107] E. Baccelli, C. Perkins, "Multi-hop Ad Hoc Wireless Communication," IETF Internet Draft, November 2011.

[108] E. Baccelli, K. Mase, S. Ruffino, S. Singh, "Address Autoconfiguration for MANET: Terminology and Problem Statement," IETF Internet Draft, February 2008.

[109] E. Baccelli, T. Clausen, U. Herberg, C. Perkins, "IP Links in Multihop Ad Hoc Wireless Networks?," Proceedings of the International Conference on Software Telecommunications and Computer Networks (SOFTCOM), Split, Croatia, September 2009.

[110] E. Baccelli, T. Clausen, P. Jacquet, D. Nguyen "OSPF Multipoint Relay (MPR) Extension for Ad Hoc Networks," IETF Request For Comments, RFC 5449, February 2009.

[111] J. A. Cordero, P. Jacquet, E. Baccelli, "Impact of Jitter-based Techniques on Flooding over Wireless Ad hoc Networks: Model and Analysis," in Proceedings of the 31st IEEE International Conference on Computer Communications (INFOCOM), Orlando, USA, March 2012.

[112] E. Baccelli, J.A. Cordero, P. Jacquet, "Optimization of Critical Data Synchronization via Link Overlay RNG in Mobile Ad Hoc Networks," Proceedings of the 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS), San Francisco, USA, November 2010.

[113] E. Baccelli, J.A. Cordero, P. Jacquet, "Using Relative Neighborhood Graphs for Reliable Database Synchronization in MANETs," Proceedings of the Fifth IEEE Workshop on Wireless Mesh Networks (WiMesh) in conjunction with SECON 2010, Boston, USA, June 2010.

[114] E. Baccelli, J.A. Cordero, P. Jacquet, "Multi-Point Relaying Techniques with OSPF on Ad Hoc Networks," Proceedings of the International Conference on Systems and Networks Communications (ICSNC), Porto, Protugal, September 2009.

[115] C. Adjih, E. Baccelli, T.Clausen, P. Jacquet, R. Rodolakis, "Fish Eye OLSR Scaling Properties," IEEE Journal of Communication and Networks (JCN), Special Issue on Mobile Ad Hoc Wireless Networks, p. 343-351, December 2004.

[116] C. Adjih, E. Baccelli, P. Jacquet, "Link State Routing in Ad Hoc Wireless Networks," Proceedings of MILCOM 2003 - IEEE Military Communications Conference, vol. 22, no. 1, pp. 1274-1279, Boston, USA, Oct. 2003.

[117] E. Baccelli, F. Baker, M. Chandra, T. Henderson, J. Macker, R. White, "Problem Statement for OSPF Extensions for Mobile Ad Hoc Routing," IETF Internet Draft, September 2003.

[118] J. Ahrenholz, T. Henderson, P. Spagnolo, E. Baccelli, T.Clausen, P. Jacquet, "OSPFv2 Wireless Interface Type," IETF Internet Draft, May 2004.

[119] M. Goyal, E. Baccelli, et al., "Improving Convergence Speed and Scalability in OSPF: A Survey," IEEE Communications Surveys and Tutorials, March 2011.

[120] E. Baccelli, J. A. Cordero, P. Jacquet, "OSPF over Multi-Hop Ad Hc Wireless Communications," International Journal of Computer Networks & Communications (IJCNC) Vol.2, No.5, September 2010.

[121] E. Baccelli, T. Clausen, P. Jacquet, D. Nguyen, "Integrating VANETs in the Internet Core with OSPF: the MPR-OSPF Approach," Proceedings of the International Conference on ITS Telecommunications (ITST), Sophia Antipolis, France, June 2007.

[122] J.A. Cordero, E. Baccelli, P. Jacquet, T. Clausen, "Wired/Wireless Compound Networking", in Mobile Ad Hoc Networks: Applications," X. Wang (Ed.), InTech, Chapter 16, pp. 349–374, 2011.

[123] E. Baccelli, P. Jacquet, T. Clausen, "Database Exchanges for Ad-hoc Networks Using Proactive Link State Protocols," in Performance Modelling and Analysis of Heterogeneous Networks, D. Kouvatsos (Ed.), River Publishers, Denmark, Chapter 5, pp. 93–111, 2009.

[124] C. Adjih, E. Baccelli, P. Minet, P. Mhlethaler, T. Plesse, "QoS Support, Security and OSPF Interconnection in a MANET Using OLSR," Journal of Telecommunications and Information Technology (JTIT), issue n2 p. 70-76, June 2008.

[125] Open Source Implementation of RFC5449 and extensions, http://ospfmanet.gforge.inria.fr/

[126] J.A. Cordero, M. Philipp, E. Baccelli, "Routing Across Wired and Wireless Mesh Networks: Experimental Compound Internetworking with OSPF," Proceedings of the 8th International Wireless Communications & Mobile Computing Conference, Limassol, Cyprus, August 2012 (to appear).

[127] M. Goyal, E. Baccelli, M. Philipp, J. Martocci, A. Brandt "Reactive Discovery of Point-to-Point Routes in Low Power and Lossy Networks," IETF Internet Draft, March 2012.

[128] Open Source Implementation of P2P-RPL, http://contiki-p2p-rpl.gforge.inria.fr/

[129] M. Goyal, E. Baccelli, J. Martocci, A. Brandt, "A Mechanism to Measure the Quality of a Point-to-point Route in a Low Power and Lossy Network," IETF Internet Draft, March 2012.

[130] M. Goyal, N. Dejean, D. Barthel, E. Baccelli, J. Martocci, "DIS Modifications," IETF Internet Draft, Spetember 2011.

[131] W. Xie, M. Goyal, H. Hosseini, J. Martocci, Y. Bashir, E. Baccelli, A. Durresi, "Routing Loops in DAG-based Low Power and Lossy Networks," Proceedings of the IEEE Advanced Information Networking and Applications (AINA), Perth, Australia, April 2010.

[132] W. Xie, M. Goyal, H. Hosseini, J. Martocci, Y. Bashir, E. Baccelli, A. Duresi, "A Performance Analysis of Point-to-Point Routing Along a Directed Acyclic Graph in Low Power and Lossy Networks," in proceedings of the 13th International Conference on Network-based Information Systems (NBIS), September 2010.

[133] E. Baccelli, M. Philipp, M. Goyal, "The P2P-RPL Routing Protocol for IPv6 Sensor Networks: Testbed Experiments," Proceedings of the IEEE International Conference on Software Telecommunications and Computer Networks (SOFTCOM), Split, Croatia, September 2011.

[134] C. Adjih, E. Baccelli, P. Jacquet, P. Minet, M. Philipp and G. Wittenburg, "Deployment Experience with Low Power Lossy Wireless Sensor Networks," in the Proceedings of the 1st IAB Workshop on Interconnecting Smart Objects with the Internet, March 2011.

[135] E. Baccelli, J. Schiller, "Towards Scalable MANETs," Proceedings of the IEEE International Conference on ITS Telecommunications (ITST), Phuket, Thailand, October 2008.

[136] E. Baccelli, T. Zahn, J. Schiller, "DHT-OLSR," INRIA Research Report RR-6194, May 2007.

[137] E. Baccelli, "OLSR Scaling with Hierarchical Routing and Dynamic Tree Clustering," Proceedings of the IASTED International Conference on Networks and Communication Systems (NCS), Chiang Mai, Thailand, March 2006.

[138] A. Szwabe, A. Nowak, E. Baccelli, J. Yi, B. Parrein. ”Multi-path for Optimized Link State Routing Protocol version 2,” IETF Internet Draft, 2011.

[139] A. Szwabe, P. Misiorek, M. Urbanski, and E. Baccelli, ”OLSRv2 Backpressure Traffic Engineering Extension”, IETF Internet Draft, 2011.

[140] E. Baccelli, P. Jacquet, B. Mans, G. Rodolakis, ”Information Propagation Speed in Bidirectional Vehicular Delay Tolerant Networks,” Proceedings of the 30th IEEE International Conference on Computer Communications (INFOCOM), Shangai, China, April 2011.

[141] E. Baccelli, P. Jacquet, B. Mans, R. Rodolakis, ”Highway Vehicular Delay Tolerant Networks: Information Propagation Speed Properties,” in IEEE Transactions on Information Theory (ISSN-0018-9448), March 2012.

[142] E. Baccelli, T. Clausen, R. Wakikawa, ”IPv6 Operation for WAVE, Wireless Access in Vehicular Environments,” Proceedings of the 2nd IEEE Vehicular Networking Conference (VNC), Jersey City, USA, November 2010.

[143] E. Baccelli, L. Gerhold, C. Guettier, J. Schiller, T. C. Schmidt, G. Sella , U. Meissen, A. Voisard, M. Waehlisch, G. Wittenburg, ”SAFEST: A Framework for Early Security Triggers in Public Spaces,” in proceedings of the French Interdisciplinary Workshop on Global Security (WISG), Troyes, France, January 2012.

[144] G. Paschos, E. Baccelli, P. Jacquet, A. Szwabe, P. Misiorek, A. Schmidt, ”Final Report on Theoretical Advances of Optimization-based Modeling and Achievable Performance Limits for Wireless Networks,” OPNEX Project Deliverable D1.3, November 2010.

[145] K. Choumas, S. Keranidis, T. Korakis, I. Koutsopoulos, L. Tassiulas, F. Juraschek, M. Gunes, E. Baccelli, P. Misiorek, A. Szwabe, T. Salonidis, H. Lundgren, ”Optimization driven Multi-Hop Network Design and Experimentation: The Approach of the FP7 Project OPNEX,” in IEEE Communications Magazine, Radio Communications Series, to appear in 2012.

[146] E. Baccelli, P. Jacquet, B. Mans, R. Rodolakis, ”Multi-lane Vehicle-to-Vehicle Networks with Time-Varying Radio Ranges: Information Propagation Speed Properties,” INRIA Research Report RR-8037, August 2012.

[147] J.A. Cordero, E. Baccelli, T. Clausen, ”MPR+SP: Towards a Unified MPR-based MANET Extension for OSPF,” INRIA Research Report RR-7319, May 2010.