Enabling Multihop Communication in Spontaneous Wireless Networks

Juan Antonio Cordero, Jiazi Yi, Thomas Clausen, Emmanuel Baccelli

June 21, 2013

Contents

1 Introduction

Since the end of the 20th century, wireless networking is experiencing explosive growth, driven by the popularity of wireless telephony on one hand, and by the development of wireless computer networks on the other hand. Both trends are currently merging into a single attempt: enabling massive wireless Internet access. This phenomenon was inspired by Norman Abramson's pioneer work on packet radio networks [1] in the 1970s, and made possible by the authorization of wireless spectrum use for civil telecommunication purposes, in the 1980s[1]. At first, this deregulation encouraged the democratization of wireless telephony, in the 1990s, thanks to the availability of cheaper, more efficient hardware stemming from Cold War military industry efforts. Since 2000, the introduction of new wireless communication standards using the spectrum authorized for civil use has also fueled the development of wireless computer networks and wireless Internet access.

1.1 Managed Wireless Networks

Wireless Internet access is nowadays mostly provided via link layer technologies such as Wifi (IEEE 802.11 infrastructure mode standards [2]), WiMAX[2] (IEEE 802.16 [3]), UMTS[3] or LTE[4] (3GPP standards [4]), 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: user terminals (hereafter denominated *hosts*) access the Internet through a dedicated, authoritative infrastructure device (hereafter denominated *router*). In that sense user terminals are competing "consumers" of the same networking resource, which consists locally in access to the router granting internetwork (Internet) connectivity. 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.

The basic mechanisms provided by IEEE 802.11 infrastructure mode, WiMAX, UMTS or LTE thus provide communication capabilities over a single wireless hop, between a user terminal and an infrastructure access point. Some extensions of these basic mechanisms provide direct device-to-device communication (as the Wifi ad hoc mode) or even multi-hop wireless communication through relays planned in advance (*e.g.* with LTE or WiMAX). However, these wireless networks all have in common their *managed* nature: they depend entirely on

[1] ISM (Industrial, Scientific, Medical) bands, released in 1985 by US Federal Communications Commission (FCC) for unlicensed use.

[2] Worldwide Interoperability for Microwave Access.

[3] Universal Mobile Telecommunications System.

[4] Long Term Evolution.

an infrastructure planned and deployed in advance, controlled by an operator. This chapter does not focus on such networks.

1.2 Spontaneous Wireless Networks

Although so far not as successful as managed wireless networking, an alternative type of wireless networks has also emerged since 2000: *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 (hereafter, *node*) may behave as a router and a host simultaneously. 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/control from infrastructure devices. Each node 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 solutions to extend and offload managed wireless networks hampered by increasingly heavy smartphone data communications [5]. They can also increase the resilience of the network in scenarios where infrastructure is not usable, due to a disaster, to the military situation or to the political situation, for instance [6]. In addition, spontaneous wireless networking is an effective way to extend the reach of wireless Internet access, without costly additional infrastructure deployment [7].

Popular link layer technologies providing device-to-device communication in spontaneous networks include so far IEEE 802.11 ad hoc mode [2] and IEEE 802.15.4 [8]. However, in order to provide multi-hop communication in spontaneous wireless networks, additional techniques have to be employed on top of such link layer technologies, and that is the subject of this chapter. The focus is put on the use of standard IP protocols to enable multi-hop wireless communications in spontaneous wireless networks – in order for these networks to effectively blend in the Internet, where appropriate.

Handling heterogeneity at layer 3 Since the early days of computer networking and the first steps of today's Internet, the diversity of networking technologies has been handled exclusively at the physical and the link layers (layers 1 and 2 OSI). The internetworking layer (layer 3) has been conceived as a "convergence layer" in which a single protocol (the Internet Protocol, IP) runs unchanged on top of heterogeneous interconnected networks, as it can be observed

in Figure 1 [9].

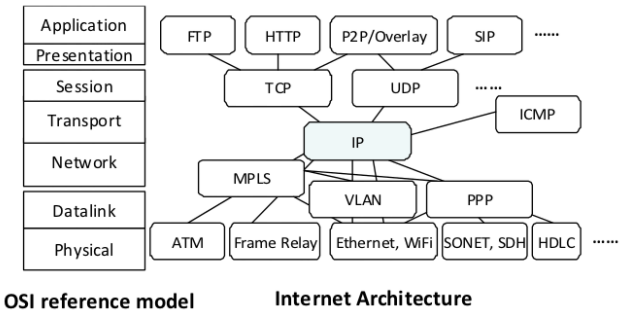

Figure 1: OSI reference model and IP networking architecture [9].

The development of wireless technology entails however substantial changes in the way that networks are usually represented and conceived. Characteristics of spontaneous wireless networks cannot be handled exclusively at lower layers of communication, as they challenge some of the key assumptions of the IP-based networking architecture. They need thus to be taken into account at layer 3. As more flexible wireless networks are deployed and get increasingly interconnected and integrated with other networks –or in the Internet–, the use of IP over these networks need thus to be adapted or reconsidered. The **first contribution** of the chapter is a review of these considerations, as it elaborates on how the IP-based network architecture is challenged by spontaneous wireless networks.

1.3 Mobile Ad hoc and Low-Power Lossy Networks

IP protocols are developed, standardized and maintained by the Internet Engineering Task Force (IETF [10]). Most of the IETF's protocol design and standardization activities have so far focused on two categories of spontaneous wireless networks: Mobile Ad hoc Networks (MANETs) and Low-Power Lossy Networks (LLNs).

Mobile Ad hoc Networks (MANETs) According to the IETF's terminology (defined in RFC 2501 [11]), a MANET consists in a set of "mobile platforms (..) –herein simply referred to as 'nodes'– (..) which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network" [11]. Note that this definition *allows* router mobility, but it is *not restricted* to mobile networks; the term includes all wireless multi-hop ad hoc networks, regardless of whether they are static or not.

Low-Power Lossy Networks (LLNs) According to the IETF's terminology (defined in `draft-ietf-roll-terminology-12`[5] [12]), LLNs are "typically composed of many embedded devices with limited power, memory, and processing resources interconnected by a variety of links, such as IEEE 802.15.4, LowPower WiFi" [12]. LLNs are thus a more specific case of MANETs (as defined in the previous paragraph), in which routers typically operate with constraints on processing power, memory, and energy (battery power). Their interconnections are characterized by high loss rates, low data rates, and link instability. LLNs are comprised of anything from a few dozen to thousands of routers. Supported traffic flows include point-to-point (between devices inside the LLN), point-to-multipoint (from a central control point to a subset of devices inside the LLN), and multipoint-to-point (from devices inside the LLN towards a central control point). Alternative, but similar terminology is employed in `draft-ietf-lwig-terminology` [13], which defines the terms "constrained nodes" and "constrained networks" with various classes of constraints.

Concrete examples of MANETs and LLNs include the following three use cases, selected only for illustrative purposes, to hint at the wide heterogeneity of features, requirements and user expectations that one must address in spontaneous wireless networking.

Vehicular Ad hoc Networks (VANETs) Communication in VANETs is enabled between moving vehicles in urban scenarios or roadways, (possibly) with fixed devices installed in Roadside Units (RSUs) along the road/street. The combination of vehicles and RSUs forms a mobile, highly dynamic ad hoc network. Devices participating in vehicular networks (either inside vehicles or in RSUs) have neither significant energy constraints nor severe computational limitations, but those installed in vehicles are not, in general, cooperative and willing to dedicate resources to others' communication. Research in these networks has typically focused on safety applications, such as distribution along the highway of information about traffic-related events – *e.g.*, jams or accidents [14]. Other purposes could be also considered, such as dissemination of service availability along the highway (gas stations, tolls, accommodation, etc.). As such, a VANET is a category of MANET.

Community Wireless Mesh Networks These are cooperative, non-commercial networking projects in which users join and contribute to the deployment of the network, in particular by sharing resources and allowing the use of their devices as networking relays. Several initiatives have flourished in the last years, such as Spain's *Guifi* [15], mostly deployed over the Eastern coast of Spain (Catalonia and Valencia) but also present in many other parts of the country. Other examples include Germany's *Freifunk* [16] and Austria's *Funkfeuer* [17]. Some

[5] An Internet-Draft in the Last Call for becoming an RFC, at the the time of writing this chapter.

of them cover large geographical areas and contain thousands of nodes[6]. These networks are typically static, most of the links are wireless links operating in free (unlicensed) frequency bands. Their topology and capacity evolve dynamically, in an unplanned manner, subject to events such as the ingress and egress of users, the subsequent availability of new links and resources or the upgrade of a particular networking region. These networks enable free communication among their users, but they can also provide access to the Internet if there are gateways available. As such, a community wireless mesh networks is also a category of MANET.

Wireless Sensor Networks (WSNs) WSNs are collections of sensors intended to measure one or several properties of the environment in which they are deployed. Communication facilities required by such networks need to include, at least, the transmission of collected information from the sensors to a gateway or central server that stores and eventually process it, and the transmission of information (*e.g.*, configuration instructions or measurement schedules) from the server to one or more sensors. There is a broad range of information that may be collected and exchanged through WSNs, some examples including climate studies, bird observation, power monitoring in buildings or tracking of patients' health parameters with body sensors. Properties of a WSN may vary depending on the purposes of the sensor deployment, but there are some usual constraints. Sensors are often battery driven, the lifetime of the sensor is limited by the battery lifetime. Protocols for enabling communication within WSNs must therefore be designed with energy consumption and energy-efficiency in mind. As such, a wireless sensor network is a category of LLN.

Despite their heterogeneity, these use cases – and other applications of spontaneous wireless networks – have common characteristics, including bandwidth scarcity and need for self-organization. These characteristics both require the use of efficient, highly decentralized routing and flooding mechanisms, able to react quickly to topology changes without overloading the network. This chapter thus focuses more specifically on IP protocols that enable routing and flooding in MANETs and LLNs. While plenty of protocols have been proposed in the literature, only few have been effectively implemented, standardized and used in real-world deployments. The **second contribution** of the chapter consists in:

(1) an analysis of the main implications of wireless mesh characteristics on the task of flooding and routing typically implemented in upper-layer protocols; and

(2) a description and discussion of the key mechanisms and operation of the main protocols deployed so far and standardized at the IETF for routing in MANETs, in LLNs and in heterogeneous wired/wireless inter-networks.

[6] *Guifi.net*, for instance, claims 31865 nodes, 20425 of them being "operating nodes" (last query to `http://www.guifi.net` on April 10th, 2013).

1.4 Reader's Guide

Reader is assumed to be familiar with the main concepts of computer networking and the TCP/IP network reference model, whose terminology is used in this chapter. Interested readers are referred to the book of Tanenbaum *et al.* [18] for details; the glossary at the end of the chapter displays standard definitions of the basic networking concepts. Basic knowledge of the Internet Protocol (IP) operation, addressing model, routing and Internet architecture is also preferable, but not necessary. These elements are briefly overviewed in section 2, in order to better highlight the issues that arise with the traditional IP model in spontaneous wireless networks, addressed in section 3. This section describes the conditions under which wireless communication occurs, and examines their impact on the communication performance and the architecture of spontaneous wireless networks. In particular, the section explains the non-suitability of the conventional IP networking model for spontaneous wireless networks, and discusses an alternative model.

The rest of the chapter focuses on the mechanisms and protocols that have been designed to handle flooding and routing in spontaneous wireless networks, paying a particular attention to the efforts deployed at the IETF. Section 4 motivates and presents the mechanisms, and section 5 describes the routing and flooding protocols that have been specifically designed in the IETF to operate on MANETs and LLNs. Section 6 focuses on the problem of extending legacy Internet routing protocols so that they can efficiently operate on hybrid (wired/wireless) inter-networks. Finally, section 7 concludes the chapter.

2 Fundamentals of IP Networking and Internet Routing

This section introduces the main ideas and concepts that are used as a basis for traditional wired Internet. Subection 2.1 presents the key elements of the IP networking model, including addressing, forwarding and the notion of IP link. Subection 2.2 describes the most relevant routing techniques used in the Internet, and subsection 2.3 overviews the Internet routing architecture, based on the notion of Autonomous System. A certain familiarity with the basics of computer networking is assumed, so no details are provided. This section mainly follows the classic manuals of Tanenbaum *et al.* [18], Comer [19] and Perlman [20]. Interested readers are referred to these resources for further explanations.

2.1 The IP Networking Model

The Internet Protocol (IP) defines the key elements enabling communication in an IP network. This section presents the IP addressing mechanism, the notion of IP link and the routing rule used by router in IP networks – the *longest prefix match* criterion.

Addressing In an IP network, every *network interface* is assigned at least one **IP address** that identifies unambiguously the interface in the network. The IP address format varies depending on the protocol version (32 bits for IPv4, 128 bits for IPv6, see Figure 2), but three elements can be distinguished.

- The **host identifier** is the set of bits that identifies the interface in the network.
- The **network prefix** is the set of bits that identifies the network to which the interface is attached.
- The **network mask** allows to obtain the network prefix and the host identifier from the IP address.

Remark The IP address of a network interface is both an *identifier* and a *locator* of the interface: it indicates *who* is (unambiguosly in the internetwork) the attached interface and *where* is it attached (to which network).

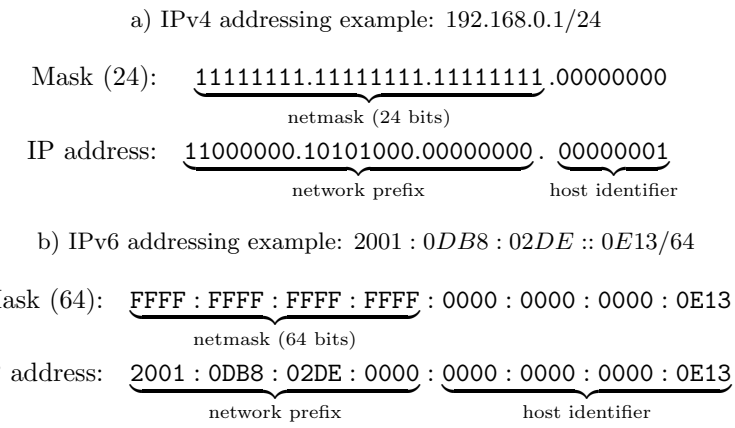

Figure 2: IP address structure, for IPv4 and IPv6.

Based on the information contained in IP addresses from the destination field of the IP header, routers and hosts are able to take decisions upon reception of an IP packet. Trivially, a host receiving an IP packet will accept it only in case that the destination IP address is itself[7] and drop it otherwise. A router

[7] Or the destination address is a broadcast address or a multicast address to which the host has suscribed.

receiving an IP packet over an interface will compare the network prefix of the destination IP address with the prefix of its own interface: if it does not match, it may forward it through another interface, according to the IP forwarding rule (see below). In case of forwarding, the router decreases the *Time-To-Live* field (or *hop-limit* for IPv6), to indicate that the corresponding packet has traversed one (more) router in its path to its destination. This leads to the notion of *IP link* (see Figure 3).

IP Link Two network interfaces, x and y, are connected to the same *IP link* when they can exchange packets in an IP network without requiring that any router forwards them, that is, when packets sent from one interface are received in the other with the same TTL/hop-limit value. This relationship is denoted as $x \sim_{IP} y$.

- In these conditions, communication is performed in a single *IP hop*.

Remark Let a, b and c be network interfaces. The previous definition implies the following properties of IP links:

- *Symmetry*: $a \sim_{IP} b \iff b \sim_{IP} a$.
- *Transitivity*: $a \sim_{IP} b, b \sim_{IP} c \implies a \sim_{IP} c$.

Note that transitivity does *not* hold in terms of routers. The fact that a router R_1 and a router R_2 are connected to the same link, and R_2 and R_3 are connected to the same link, does not imply that R_1 and R_2 have a link in common: R_2 may be attached to two different links (one connecting with R_1 and another with R_3) by way of two different network interfaces.

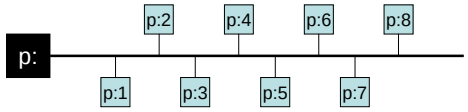

Figure 3: An IP link `p:` with network prefix p. *IP addresses of nodes in this IP link have the structure* `p:i`$/[p]$*, for* $0 < i < 2^{[p]}$.

Forwarding rule When source and destination of a packet do not belong to the same IP link, routers receiving the packet compare the IP address of the destination to the prefixes stored in the routing table, and forward the packet through the network interface corresponding to the prefix showing the *longest prefix match*, this is, the prefix in the routing table for which a bigger number of bits are coincident with those from the network prefix of the IP address of the packet destination.

2.2 Main Routing Techniques

Two types of routing techniques currently dominate [20]: *link-state* routing and *distance-vector* routing (with the variant of *path-vector* routing). The main protocols used historically and currently in the Internet are based on these techniques.

Link-State Routing Routers advertise the status of their links (link-state) to the whole network. Link status may include information about the type of link (broadcast, point-to-point...), the link communication capabilities (one-directional, bi-directional, link cost) or the routers to which communication is available through this link. This way, every router in the network receives the link-state of other routers in the network, maintains information about the whole network topology and is therefore able to locally compute network-wide shortest paths, usually by way of Dijkstra's algorithm [21].

- Some examples of this approach are the Open Shortest Path First (OSPF, RFCs 2328 and 5340 [22, 23]) and the Intermediate System to Intermediate System (IS-IS, RFC 1142 [24]) protocols, as well as the Optimized Link State Routing protocol (OLSR, RFC 3626 [25]).

Distance-Vector Routing A router shares information from its routing table only with its neighbors, indicating *distances* and next hops towards reachable destinations. Neighbor distance is defined according to the current *link metric*, which maps links between routers with estimations of the cost of sending packets through them, represented by scalar values. By receiving the routing tables of all its neighbors, which in turn have been shared with the neighbors of the neighbors, a router is able to identify, for each advertised destination, the neighbor that provides shortest distance and select it as next hop. Distance-vector protocols mostly use the distributed Bellman-Ford algorithm [26, 27] to identify network-wide shortest paths.

- The Routing Information Protocol (RIP, RFCs 1058 [28], 2080 [29] and 2453 [30]) is a prominent example of this family.

Path-vector routing It is based on the same principle as distance-vector routing, a router advertises to its neighbors the paths to all reachable destinations. Each path is described by indicating the routers that are traversed. This way, local distribution of locally maintained paths enables all routers in the network to build routes to all possible destinations.

- The most prominent example of this family of protocols is the Border Gateway Protocol (BGP, RFC 1771 [31]).

The link-state algorithm requires that every single router has storage and computational capacity to compute locally the shortest-path tree of the network,

based on the information received from every other routers, and extract from that tree the next-hop towards every destination in the network. Distance-vector algorithms only require that each router updates the distance-vectors received from their neighbor to infer its own vector of distance vector and select its next-hops.

Due to their computational simplicity, distance-vector protocols were used in the early stages of the Internet. They were gradually replaced by link-state protocols as the ARPANET grew bigger and more complex, due to problems such as the well-known count-to-infinity problem [18] (which appears in the original distance-vector algorithm, but does not appear on path-vector protocols). Poor scalability and slow convergence properties of distance-vector with respect to link-state algorithms were also major reasons to switch from one technique to the other [20].

- The network reaction to a link failure illustrates the differences between link-state and distance-vector algorithms in terms of convergence. In distance-vector algorithms, once a router detects such a failure, it updates the cost of its route towards the lost neighbor and sends the new vector of distances to its neighbors. Neighbors receive this update and *recompute* the cost of the affected route, and then transmit in turn their new vectors. Propagation of topology changes is thus slower than in link-state algorithms, in which a router detecting the failure of the link towards one of its neighbors *floods* an updated topology description which is directly forwarded over the network, without delays caused by route re-computation in intermediate routers [20].

Routing protocols for wired networks used to be *proactive* or table-driven, in which next hop to any possible destination is stored in a table. With the emergence of wireless networks and, more generally, more dynamic networking architectures coping with more scarce (shared) bandwith, *reactive* routing protocols were then designed and deployed, in which routes were only computed upon request (on-demand).

Proactive routing Routers collect and periodically disseminate topology information over the network; this enables them to maintain proactively (*i.e.*, regardless on whether they are used) routes towards all destinations. This way, routers are able to forward packets at any time to any destination in the network.

Reactive routing A router calculates a route to a destination only when it receives packets addressed to that destination and the routing table does not provide a next hop towards it. In this case, the router triggers a *route discovery* process by disseminating a Route Request (RREQ) packet through the network. The route discovery process terminates when the requested destination or another router knowing a valid route towards the destination reply to the requesting router.

- Dynamic Source Routing (DSR, RFC 4728 [32]) or Ad hoc On-Demand Distance Vector (AODV, RFC 3561 [33]), both used in spontaneous wireless networks, are examples of reactive routing protocols.

Proactive maintenance of next hops to every possible destination in the table requires a constant exchange of control traffic in the network, but enables routers to forward packets immediately after receiving them. Reactive protocols adapt the control traffic to the data traffic requirements: when there is no traffic to route, or the traffic follows known paths, a mostly negligible amount of control traffic (very low or even zero, depending on the protocol) is needed. When a router receives packets to be sent to a destination for which no route is known, the router needs to address a route discovery process over the network – such a discovery process is costly in terms of overhead, and leads to significant delays in the forwarding.

Other routing approaches Some other approaches have been explored for routing over spontaneous wireless networks. In some cases, they rely on additional assumptions about properties and capabilities of the involved devices. If nodes' position is available (for instance, by way of GPS), **geographical routing** approaches are possible: in these protocols, a packet is forwarded to the relay getting closer to the final destination. The Greedy Perimeter Stateless Routing (GPSR) protocol [34] was the first protocol exploring this principle.

2.3 The Internet Routing Architecture

In terms of routing, the Internet is organized as a set of interconnected internetworks, denominated *Autonomous Systems* (see Figure 4). The networks in each Autonomous System are under the same administrative control, and are assumed to perform routing inside the AS *autonomously* from the rest of networks in the Internet. The formal definition of an AS is as follows:

Autonomous System "An *Autonomous System (AS)* is a connected group of one or more IP prefixes [internetwork] run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy" [35], the term "routing policy" denoting the way that routing information is exchanged between (but not within) Autonomous Systems. In the interior of an AS, "routers may use one or more interior routing protocols, and sometimes several sets of metrics" [36].

The distinction between routing inside an Autonomous System (intra-AS or intra-domain routing) and routing between different ASes (inter-AS or inter-domain routing) leads to two different types of routing protocols:

(i) *Interior Gateway Protocols* (IGPs), for route discovery and maintenance within an Autonomous System. Intra-domain routing is mostly performed

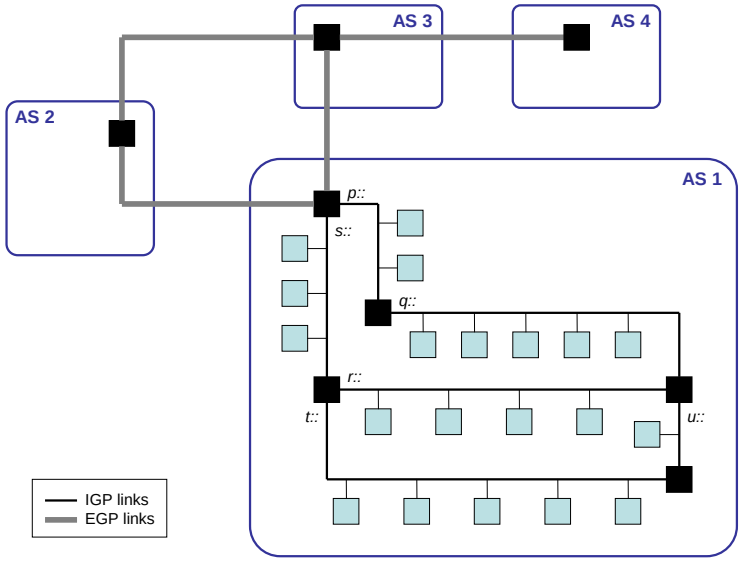

Figure 4: Connection of different Autonomous Systems.

by way of link-state protocols; the most significant link-state routing protocol for TCP/IP networks in the Internet are the Open Shortest Path First protocol (OSPF, [22, 23], described in section 6) and the Integrated IS-IS, an IP variant of the Intermediate Systems to Intermediate Systems (IS-IS) protocol (see [37]).

(ii) *Exterior Gateway Protocols* (EGPs), for route acquisition and information exchange between different Autonomous Systems. The current standard protocol for inter-domain routing is the path-vector Border Gateway Protocol (BGP, [31]).

3 Communication in Spontaneous Wireless Networks

This section describes the basics of communication between wireless devices and presents the main implications for spontaneous wireless networks at layer 3. Physical limitations and derived properties are examined in section 3.1. The implications of these properties in the networking model for spontaneous wireless networks, and in particular the suitability of the IP model, are detailed in section 2.1, is discussed in section 3.2. Finally, section 3.3 describes an IP-compatible networking model for multi hop communication in spontaneous wireless networks.

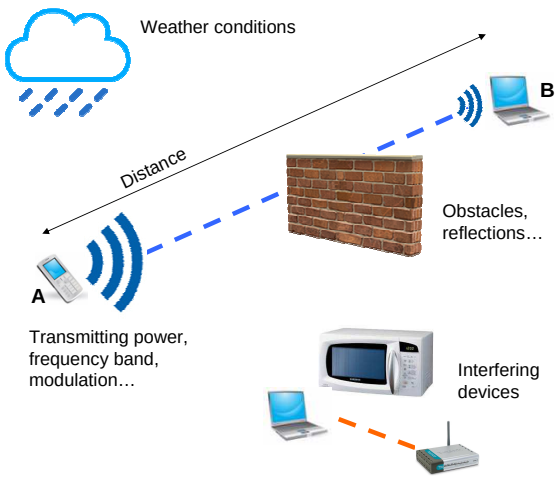

Figure 5: Communication between wireless devices A and B

3.1 Physical Aspects of Wireless Communication

The fact that two wireless devices in a wireless network are able to communicate to each other depends of several factors (see Figure 5), and some of them are not related to any of the involved devices. The most significant factors include:

(i) The distance between two devices.

(ii) The physical properties of the transmitting and receiving antennas: number of transmission/reception antennas, transmission power and antenna directivities.

(iii) Network dynamics: in mobile networks, depending on the relative motion of wireless devices involved in communication, the Doppler frequency shift may have a non-negligible impact.

The modulation and coding schemes used to transmit and receive packets have impact in other physical factors of the transmission, including:

(iv) The characteristics of the wireless medium: signal frequency band, noise power, effect of weather conditions or *interferences* from other devices transmitting in close frequency bands.

(v) The physical topology of the *coverage* area: fading caused by obstacles, reflection and absorption causing multi-path interference and signal loss.

Note that, as some of these factors are time-variant and their impact may change rapidly, *e.g.* (iv), some links (or all of them) may have intermittent availability, even if devices keep static.

Coverage and Interference The concepts of *coverage* and *interference* have been mentioned in the previous list, and are some of the key parameters that define the behavior and impact of a wireless interface in a spontaneous wireless network.

Coverage Area Given a wireless interface A, the *coverage area* of A is the geographical region in which packets transmitted by A can be received and correctly decoded by other interfaces on the same wireless medium as A, when no competing transmission is ongoing. The coverage area of A is denoted by $Cov(A)$.

Interference Area Given a wireless interface A, the *interference area* of A is the geographical region in which interfaces connected to the same wireless medium as A may be unable to receive or correctly decode other packets when there is an ongoing transmission from A. The interference area of A is denoted by $Intf(A)$.

Remark Note that, the coverage area of a wireless networking interface is always contained in the interference area of that interface, that is, $Cov(A) \subseteq Intf(A) \forall A$, as shown in the following and represented in Figure 6.

- Let $T > 1$ be the SINR (Signal-and-Interferece-Noise-Ratio) threshold for receiving and decoding correctly packets from a wireless interface. That means that a transmission (*e.g.*, from A) is received and correctly decoded by the receiver, in absence of competing transmissions, if $\text{SINR}|_{I=0} = \text{SNR} = \frac{S}{N} > T$ and discarded otherwise. As received power decreases quadratically with distance from the transmitter, let $S(d) = \frac{P}{d^2}$. Then, the maximum coverage distance is $d_c = \sqrt{\frac{P}{NT}}$. The maximum distance at which there may be interference (from A), d_i, corresponds to the distance to a receiver B such that another transmitter, C, transmitting with the same power P at any distance $d \leq d_c$ from B, would be unable to send successfully a packet in case of concurrent transmission from A. This is, $T = \text{SINR}|_{N \ll I} = \text{SIR} = \frac{P/d_{BC}^2}{P/d_i^2}$. In the worst case, $d_{BC} = d_c$ and $\frac{P/d_{BC}^2}{P/d_i^2} = \frac{d_i^2}{d_c^2} = T$, and therefore $d_i < d_c$.

Due to the variability of factors having impact on wireless communication, coverage and interference areas of an interface are time-variant and in practice their shapes are significantly more irregular than the circles depicted in Figure 6 [38]. Even within the coverage area at a particular time, when communication is possible, a wireless link is inherently unreliable and prone to transmission errors and packet losses [39], for instance due to interferences from other interfaces in the network or external sources transmitting in the same frequency band.

3.2 IP Model Issues in Spontaneous Wireless Networks

The properties of wireless medium have severe implications for the characteristics of neighbor relationship at layer 3 (L3) in spontaneous wireless networks.

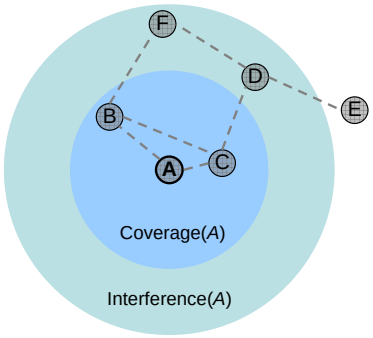

Figure 6: Idealized representation of coverage and interference areas of an interface A.

In contrast to the case of wired IP links, neighbor relationships between wireless interfaces are not necessarily *symmetric* nor *transitive* [40]. This entails some additional effect that are further illustrated in this section: the *hidden node* problem and the *exposed node* problem.

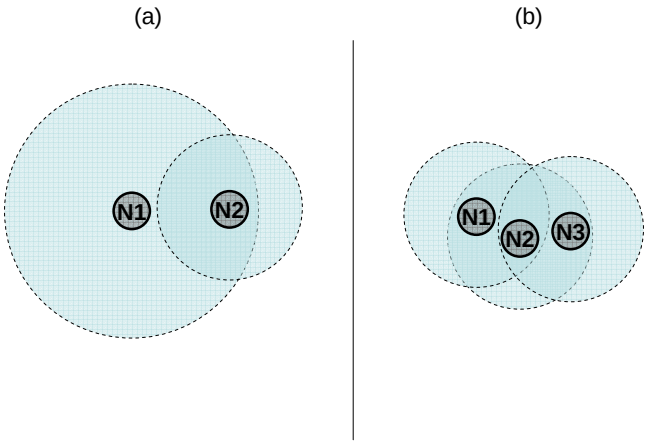

Figure 7: Asymmetry and non-transitivity in neighbor relationships between wireless interfaces.

Non-Symmetric Links Consider the small wireless network in Figure 7.a: for some reason (powerful transmitter, large antenna, ...) the wireless interface of $N1$ has a large enough coverage area that its transmissions can be received by the wireless interface $N2$. The wireless interface of $N2$, on the other hand, has a much smaller coverage radius, such that transmissions from the wireless interface of $N2$ do not arrive at the wireless interface of $N1$. Thus an asymmetric –or more precisely, an unidirectional– connectivity between the wireless interface of

$N1$ and the wireless interface of $N2$ exists: $N2$ sees $N1$ as a neighbor (since the wireless interface $N2$ can receive transmissions from the wireless interface of $N1$), whereas $N1$ does not see $N2$ as a neighbor (since the wireless interface of $N1$ can not receive transmissions from the wireless interface of $N2$). This situation illustrates that neighbor relationships in a wireless network are not necessarily symmetric.

Non-Transitive Links Figure 7.b shows a case of non-transitive links in a 2-hop wireless network. $N1$ and $N2$ are neighbors: the wireless interface of $N1$ is inside the coverage area of $N2$, and therefore $N1$'s transmissions are received at the wireless interface of $N2$ – and viceversa. Observe that the same applies with $N2$ and $N3$: $N2$ and $N3$ are also neighbors. However, direct communication between $N1$ and $N3$ is not possible, as their respective wireless interfaces are outside the coverage area of each other. In a spontaneous wireless network, the fact that $N1$ and $N2$ are neighbors (*i.e.*, can communicate directly) and $N2$ and $N3$ are neighbors as well does not imply that $N1$ and $N3$ are neighbors to each other: neighbor relationship in a spontaneous wireless network is not necessarily transitive.

These two constraints lead to situations that do not occur in traditional IP networks, such as the *hidden node problem* and the *exposed node problem*.

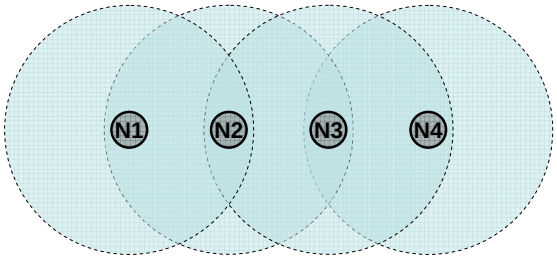

Figure 8: A four-node wireless network, with the (idealized) coverage areas of its nodes.

Hidden Nodes Consider the spontaneous wireless network represented in Figure 8. If $N3$ agrees with its neighbours (N2 and $N4$) that it will, for the moment, have exclusive access to the wireless media via its wireless interface, then $N3$ may go ahead and make a transmission. However, if at the same time $N1$ also transmits over its wireless interface, then the transmissions of the wireless interfaces of $N1$ and $N3$ may appear concurrently at the wireless interface of $N2$ – potentially interfering and causing $N2$ to receive neither of the transmissions. Denoted a *collision*, the possibility and probability of this occurring depends on the L2 (data link layer) mechanisms in place – suffice to observe that such collisions can and do occur when using some common wireless interfaces such as IEEE 802.11. The term *hidden node* originates from

the fact that while the node wishing exclusive access to the wireless media may negotiate this with its direct neighbours (in our case $N2$ and $N4$), nodes out of direct radio range (in our case $N1$) are *hidden* to the node requesting media access and cannot thus participate in the negotiation.

Exposed Nodes This can be considered as the dual problem of the *hidden node* situation described above: an *exposed node* is a node that is prevented to transmit due to the transmission of a neighbor, even when the two transmissions would not be interfer. Consider again the network of Figure 8. In the moment in which $N3$ starts a transmission, after having agreed the exclusive use of the wireless channel with neighbors $N2$ and $N4$, $N2$ is an *exposed node* because it is not able to transmit during the transmission of $N3$, in order to avoid collisions. Note however that not all concurrent transmissions from $N2$ would cause collision with the ongoing transmission from $N2$ to $N4$ – in particular, there are no collisions if destinations do not receive several packets at the same time: a packet transmission from $N3$ to $N4$ and from $N2$ to $N1$ would not cause any collision. The *exposition* of $N2$ to the transmission of $N3$ entails thus a reduction in the available bandwidth.

The hidden and exposed node problems are consequences of the fact that links between wireless interfaces in a spontaneous wireless network are not necessarily symmetric or transitive. These are major differences with the IP networking model (see section 2.1), in which neighbor relationships inside an IP link are assumed to be symmetric and transitive. As these assumptions do not hold necessarily in spontaneous wireless networks, *wireless links in a spontaneous wireless network should not be directly modeled, in general, as IP links* [41].

3.3 An IP-compatible Architectural Model

This section derives from the previously-described observations a general IP-compatible networking model for spontaneous wireless networks [42]. This model enables the compatibility of IP with the characteristics of spontaneous wireless networks, without relying on assumption concerning topology or capabilities of wireless links.

Network View IP operating on a spontaneous wireless network can be conceived in two separate levels, as represented in Figure 9: the level of traditional IP networking, and the level in which wireless interfaces are connected in a spontaneous wireless network.

- The first level (inner white cloud in Figure 9) contains *wireless interfaces* from routers that communicate with each other by way of *wireless links*, and form a spontaneous wireless network with the non-standard properties described throughout this section. Wireless interfaces in this level present *semibroadcast* communication properties (see paragraph below) and are therefore not required to satisfy the conditions of IP links.

- The second level (outer gray cloud in Figure 9) contains the links between routers and hosts, in which the classic IP link model, as described in section 2.1, applies.

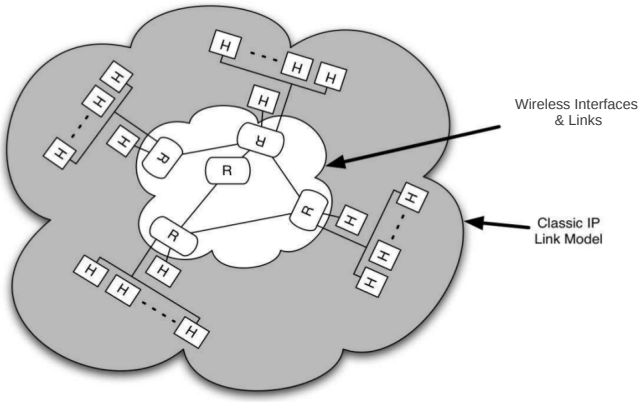

Figure 9: A view of a spontaneous wireless network, following the architecture model described in this section.

Semibroadcast Interfaces As mentioned in section 3.1, packets transmitted by a wireless interface A are simultaneously received by the set of wireless interfaces within the coverage area of A, and can be successfully decoded by all those receiving interfaces for which no other transmission causes interference. In a spontaneous wireless network, this set does not contain in general all interfaces in the network. Moreover, as links are not necessarily symmetric in wireless networks and interface coverage areas have a time-variant, irregular arbitrary shape [38], packets from an interface that has received and correctly decoded packets from A are not guaranteed to be received and correctly decoded by A. Wireless **semibroadcast interfaces** are thus "broadcast-capable interfaces that *may* exhibit asymmetric reachability" (as defined in `draft-ietf-autoconf-manetarch` [43]) and *may* not reach all interfaces in the spontaneous wireless network.

Node Morphology It has been mentioned (see section 1.2) that nodes in a spontaneous wireless network can behave simultaneously as routers and hosts, in contrast to traditional wired computer networks which enforce a clear separation between host and router roles. A first intuition deriving from this observation leads to consider nodes in a spontaneous wireless network as standard hosts with routing capabilities, with an IP subnet prefix assigned to their wireless (semibroadcast) interfaces. This intuition however assumes implicitly that the semibroadcast interface of the router is attached to the IP link over which the

host is configured (and receives its prefix), which is not consistent with the differences between IP links and links between interfaces in spontaneous wireless networks, detailed in section 3.2. Instead, an alternative node model is proposed, which is compatible with the specific characteristics of links between semibroadcast interfaces, and consistent with the two-level network view described above in this subsection. In this model, a node virtually contains *one* router with a wireless interface to interact with the rest of wireless interfaces. As shown throughout this section, links between these wireless interfaces have semibroadcast properties and hence, cannot be configured, in general, as standard IP links in a straightforward manner. A node may also contain one or more hosts: if it does, its hosts belong to the *second level* of the network architecture (see Figure 9). This entails that the links between these hosts and the corresponding router are standard IP links. Figure 10 illustrates the case of a node formed by a router R with a wireless (semibroadcast) interface, and three hosts H_1, H_2 and H_3 connected to R via standard IP links.

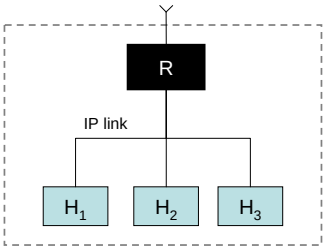

Figure 10: A node model for a spontaneous wireless network.

This implies that, from the point of view of the hosts, and the applications running on these hosts, connectivity is via a classic IP link. Host applications can thus run unaltered over spontaneous wireless networks, as the specificities of wireless semibroadcast communication have no architectural implications over the links through which hosts are connected: they remain architecturally banished to the *first level* depicted in Figure 9, and handled by wireless interfaces of the routers to which hosts are connected. Characteristics of multi-hop wireless communications can however still impact end-to-end performance experienced by hosts – for instance, TCP may not be able to function as expected [44].

With this model, nodes in spontaneous wireless networks can behave simultaneously as hosts (that is, being source or destination of traffic) and as routers (forwarding other's traffic towards its destination), but hosts and routers interface differently with the rest of the network: hosts are connected to a classic IP link, while routers are connected to the spontaneous network by way of a semibroadcast interface over links that cannot be assumed symmetric or transitive, for instance.

Impact on IP Addressing IP addressing model is tied to the notion of IP link, as shown in section 2.1. As the assumptions underlying IP links do not hold in general on links between wireless interfaces, IP links should not be configured by default in spontaneous wireless networks [45]. There are two major implications on not configuring IP links on such a network:

- **Unique Prefixes**. Wireless interfaces must be configured with unique prefixes, *i.e.* such that no two wireless interfaces are configured such that they appear within the same IP subnet. Some common ways to achieve this are:
  - unnumbered interfaces (IPv4) [36];
  - Link-Local Addresses (IPv6);
  - full length prefixes: /128 (IPv6) or /32 (IPv4) prefixes.

  However it is worth noting that prefix lengths shorter than /128 (IPv6) or /32 (IPv4) are possible on the semibroadcast interface, as long as the prefixes are unique to a single wireless interface.
- **Link Local Multicast/Broadcast Scope**. On a wireless interface, a Link Local multicast or broadcast reaches wireless interfaces of neighbor nodes only, regardless of their configured addresses. A Link Local multicast or broadcast on a wireless interface is, thus, a "neighborcast", and is not forwarded nor assumed to be received by all nodes within a spontaneous wireless network.

The principles of the model described in this section have a concrete impact on spontaneous wireless networks operation as described in the remainder of the chapter. On one hand it specifies how IP interfaces should be configured on such networks, and on the other hand it identifies the need for novel protocols and the exact scope of their operation – the *first level* depicted in Figure 9. The following sections will describe techniques and protocols for enabling communication at layer 3 in spontaneous wireless networks, within the scope of the *first level* shown in Figure 9. When needed, assumptions beyond those described in this model will be explicitly detailed in the corresponding protocols.

4 Flooding and Routing in Spontaneous Wireless Networks

As described in section 3, there are important differences in the way that spontaneous wireless networks enable communication between nodes, with respect to the classic fixed/wired networks. These differences have a significant impact in the mechanisms and protocols used in wireless multi-hop scenarios to disseminate information through the network (*flooding*) and find and maintain paths

between pairs of computers in the network (*routing*). This section examines several mechanisms that are used in different routing protocols, discusses the issues and problems that these mechanisms have when operating in spontaneous wireless networks, and describes some techniques to fix or overcome these issues.

Section 4.1 explores the use of neighbor discovery procedures in spontaneous wireless networks. Section 4.2 describes techniques to perform efficient flooding over such networks. Finally, section 4.3 presents the problem of estimating link costs and using them to to identify "good routes" over the network.

4.1 Neighborhood Discovery

In many routing and flooding protocols, routers need to be aware of their own neighborhood. This is particularly important (although not only) in spontaneous wireless networks, in which the neighborhood may change frequently during network operation. Routers acquire knowledge about their neighborhood by way of a **neighborhood discovery** mechanism.

Neighborhood Discovery (ND) is the process whereby each router advertises all the routers to which direct communication is possible (*i.e.*, the routers to which there are network links) about its presence in the network. This way, routers receiving such advertisements from other (neighboring) routers gain insight on their own neighborhood.

1-hop and 2-hop neighborhood Depending on the information advertised by ND messages, receiving routers learn different aspects about their neighborhood. If messages only advertise the presence of the originating router, the receiving router will acquire information about the routers that maintain links to itself. If links are bi-directional (as IP links in standard IP networks), this is sufficient for enabling bi-directional communication between routers: a router receiving a ND message from a neighbor can exchange packets in both directions with it. This is the case of traditional neighbor discovery protocols for Internet, such as the *Neighbor Discovery Protocol* (NDP) for IPv6 [46], which assumes that all the links are bi-directional and is used to actively keep track of which neighbors are reachable.

In spontaneous wireless networks, bi-directional communication availability cannot be inferred from the reception of an ND advertisement, given the fact that asymmetric links are possible (section 3.2). This is taken into account in ND protocols for spontaneous wireless networks. In these protocols, ND advertisements (typically denominated **Hello messages**), contain not only the id of the originating router, but also the list of its current neighbors (*i.e.*, routers from which the originating router has received Hello messages). This enables every router in the network to detect the (1-hop) neighbors with which bi-directional communication is possible, and identify the routers that belong to its 2-hop neighborhood – that is, the set of routers that are 2-hop neighbors or "neighbors of its neighbors".

- **Example** Assume that router A receives a Hello from a neighbor B, in which B indicates to have recently received a Hello from A; then A learns that link A-B is symmetric. As B lists identifiers of all its 1-hop neighbors in its Hello, A learns its 2-hop neighbors through this process.

Together with 1-hop neighbors, additional information may be included in Hello messages – in particular, the cost of the links towards the listed neighbors, when metrics other than hop-count (see section 4.3) is used. Exchange of Hello messages is typically done periodically, although some events may trigger non-periodic Hellos (*e.g.*, changes in the topology).

The *Mobile Ad Hoc Network Neighborhood Discovery Protocol* (NHDP, RFC 6130) [47] is the main ND protocol for spontaneous wireless networks. It is used as auxiliary protocol by other routing protocols that need neighborhood information to take their decisions, such as OLSRv2 (see section 5.1). In NHDP, Hello messages are exchanged periodically and they contain the id of the originating router and the list of its 1-hop neighbors. The IETF also standardized an optimization of NDP for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). This optimization, specified in RFC 6775, adapts the operation of NDP to the lossy conditions of communications and the low-power device constraints of LoWPANs. This is done, for instance, by avoiding unsollicited messages (such as periodic router announcements), reducing the use of multicast for address resolution, limiting the duplicate address detection checks, or enabling better compression algorithms [48].

Other routing protocols include their own Hello mechanism. This is the case of AODV [33] (see section 5.2) or OSPF and its MANET extensions [49, 50, 51] (see section 6.2). In the last case, some approches have been explored in order to avoid redundant notifications and hence reduce control traffic by only reporting changes in the neighborhood occurred since the last Hello transmission: this principle leads to the *incremental Hellos* mechanism used in the Overlapping Relays extension of OSPF (OR/SP [51]) and the *differential Hellos* mechanism used in the MANET Designated Routers extension of OSPF (OSPF-MDR [50]). However, experiments show that the potential benefits (mostly, saved amount of traffic) of these two mechanisms are not significant, in particular when compared with the additional complexity they introduce in the corresponding protocols [52].

4.2 Flooding

Flooding is the process through which information originated in one router is disseminated across the network, so that it can be received by every other router in the network.

The most obvious procedure to perform flooding from a router in a conventional IP network consists of the **pure flooding** procedure:

1. The source router sends the message through all its network interfaces.

2. Every router that receives the message *for the first time* retransmits it over all the network interfaces *except the one over which it was received*.

The fact that each router retransmits only *once* ensures that the process terminates in a finite number of steps. The fact that *all* routers receiving the message retransmit it ensures that the message is received –if there are no packet losses– by every router in the network at least once.

In a spontaneous wireless network, as routers communicate with *all* their wireless neighbors by way of a *single* wireless interface (see section 3), the straightforward usage of this mechanism implies that the source router broadcasts the message to be flooded and the neighboring routers rebroadcast it over the same interface it was received. It is known [53] that such a naive approach is not efficient and does not scale in a wireless multi-hop scenario. Three reasons can be highlighted:

a) excessive retransmissions that reduce the available bandwidth,

b) systematic packet collisions due to concurrent transmissions of wireless interfaces (partly) sharing the same wireless channel, and

c) duplicate packets reception due to the fact that the packet is received and retransmitted over the same interface (and, therefore, transmitted twice in the intersection between the coverage area of the sender and the receiver interface).

Remark Although the three effects are closely inter-related, and all are due to the bandwidth scarcity and the semi-broadcast properties of wireless communication detailed in section 3, it is important to point out that they constitute *different* effects; solving one of them does not necessarily solve the others.

Excessive Number of Retransmissions and Efficient Flooding In a spontaneous wireless network, a single transmission from a wireless interface is received by the wireless interfaces of all the neighbors within its coverage area. If all routers retransmit the same message as they receive it, this is likely to cause a significant number of *redundant transmissions* – *i.e.*, transmissions that do not bring new information for *any* of the interfaces receiving them.

Consider the situation in Figure 11, in which node A (in the center) floods a message to all its neighbors, and they in turn retransmit the same message so that it is received by all the 2-hop neighbors of A. In theory, every 2-hop neighbor has received the message – possibly several times. The redundant retransmissions do not bring new information, but increase the probability of collisions. This effect becomes more relevant in a context of bandwidth scarcity and high network router density.

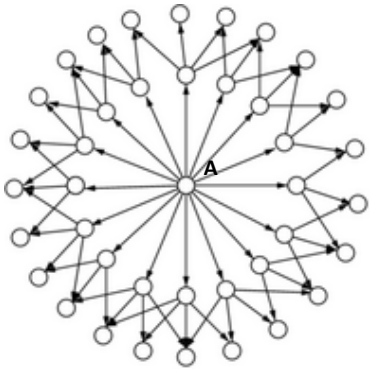

Figure 11: Classical flooding in spontaneous wireless networks.

Efficient flooding techniques explore different strategies to reduce the number of flooding retransmissions (and therefore, to decrease the amount of traffic overhead involved), while preserving as much as possible the ability of the flooding procedure to reach all (or most of) the routers in the spontaneous wireless network.

For every efficient routing technique, a set of the routers that receive a message (typically, not all of them) are allowed to retransmit it. If efficient flooding reaches all routers in the network, the set of routers allowed to retransmit a message is a *Dominating Set* (DS) in the network graph. As only one router originates and originally sends the message, and every other forwarding router has previously received it via flooding, the set of routers and the wireless links between them usually form a **Connected Dominating Set** (CDS). Given a graph $G = (V, E)$ representing a spontaneous wireless network, where V is the set of vertices (representing network routers) and E is the set of edges (representing network links), a Connected Dominating Set of G is a subset of vertices $D \subseteq V$ with two properties:

1. *Connection.* D induces a connected subgraph of G, that is, any node in D can reach any other node in D by a path that stays entirely within D.

$$\forall x, y \in V, \quad \exists p = (x, p_1, p_2, ..., p_n, y) \subseteq D \wedge x\bar{p}_1, p_1\bar{p}_2, ..., p_n\bar{y} \in E$$

2. *Domination.* D is a dominating set of G, meaning that every vertex in G either belongs to D or is adjacent to a vertex in D.

$$\forall v \in V, \qquad v \in D \vee (\exists w \in D : u\bar{w} \in E)$$

Figure 12 displays an example of Connected Dominating Set over a network graph.

The notion of CDS is useful for efficient flooding purposes: several efficient flooding techniques rely on the construction and maintenance of Connected

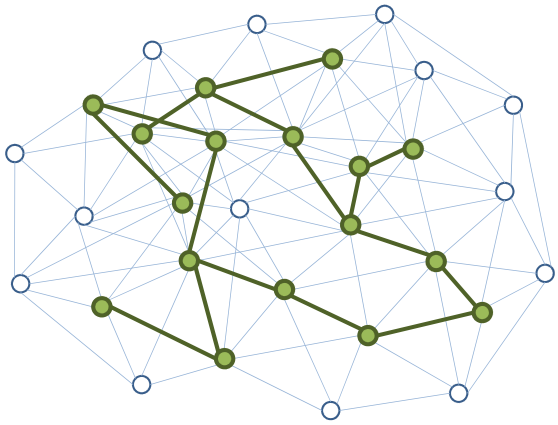

Figure 12: Example of CDS (thick edges) over a network graph of 30 nodes (light edges represent communication between nodes).

Dominating Sets of forwarding nodes, over which packets are flooded through the network. One of the main techniques based on this principle is the *Multi-Point Relaying* (MPR) technique.

- **Multi-Point Relays** [54] is an algorithm through which a node selects a subset of its 1-hop neighbors (*multi-point relays*) such that each 2-hop neighbor is reachable through (at least) one of the selected 1-hop neighbors (*MPR coverage criterion*). MPR selection requires that the selecting node knows the 2-hop neighbors that will be covered by its MPRs. By using MPR, the retransmission of flooding traffic can be significantly reduced, as shown in Figure 13, compared to classical flooding in Figure 11.

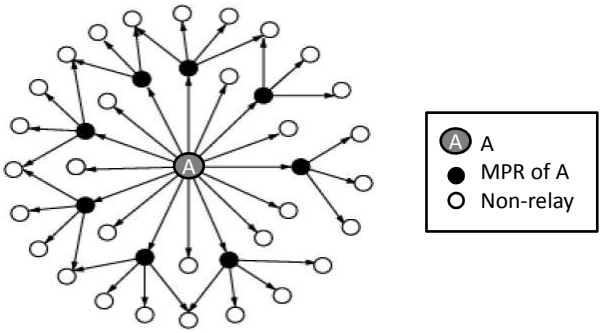

Figure 13: Efficient flooding with Multi-Point Relays.

Remark Note that the MPR coverage criterion does not guarantee by itself that the set of nodes selected as MPRs form a Connected Dominating

Set [55]. The set of MPRs is by definition a dominating set, as every node is either a MPR for a neighbor, or is adjacent to its own MPR. As the heuristic for MPR selection is relative to the source, however, the subgraph resulting from MPRs and the MPR links (links connecting nodes with their relays) between them *is not necessarily connected*. This can be easily fixed by adding an arbitrary router and all its links to the subgraph, as proved in Cordero (2010) [55].

Multipoint relays of a router can be used to perform efficient flooding, but the principle can be used for performing other networking operations. The MPR selection algorithm can be slightly modified so that the overlay that includes all links between routers and its (modified) multi-point relays is sufficient to compute shortest paths over the underlying network [55]. This result has been exploited in some extensions of OSPF for MANETs, as shown in section 6.

Systematic Packet Collisions and Jittering Techniques Consider the spontaneous wireless network of Figure 14, in which router A floods a message through the network. The broadcast transmission of A is received at the same time by B and C, which retransmit the message towards E and D (in the case of B) and D and F (in the case of C). Then, concurrent retransmissions from B and C cause a systematic packet collision from D's perspective.

Remark In this example, the collision could not be detected with any CSMA[8] layer 2 mechanism neither by B nor by E, due to the fact that B and E are not neighbors to each other. B is a *hidden node* for E (and vice versa).

Remark Note that this problem cannot be addressed only by way of *efficient flooding* approaches: none of the retransmissions by B and E are redundant, so none of them could be avoided without leaving nodes uncovered (C if B does not retransmit, F if E does not retransmit).

The fact that flooded messages are forwarded simultaneously by wireless interfaces receiving them through the same wireless shared medium may cause packet collisions during the flooding procedure (depending on the network topology at the time of flooding). Unlike other packet transmissions for which the collision probability may vary depending on the traffic pattern, these flooding collisions are *systematic* and will occur, for a given network topology and flooding algorithm, any time that the source node floods a new message (in the example, any time A floods a message).

This effect could be alleviated by allowing routers to wait a random amount

[8]Carrier Sense Multiple Access. CSMA is a medium access control (MAC) protocol for wireless networks in which nodes sense the medium before transmitting, and only transmit if the sensed medium is idle, that is, if the node does not detect any ongoing transmission within its reception range. See *e.g.* Tanenbaum *et al.* [18] for reference.

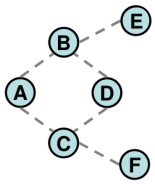

Figure 14: An example of spontaneous wireless network. *(Broken lines denote direct communication)*

of time (denominated **jitter**) before retrasmitting a flooded message, in order to reduce the probability of concurrent transmissions by neighboring wireless interfaces. This technique is known as **jittering**, and has been standardized by the IETF in RFC 5148 [56]. The recommendation from RFC 5148 is that delays are selected following an uniform distribution between 0 and a maximum jitter value, MAX_JITTER. Figure 15 illustrates the effect of jittering techniques in the network example of Figure 14. In the example, node A is flooding a packet to all the other nodes. When node B and C receive the packet from A, instead of retransmitting the packet immediately, they wait a random delay. In this way, simultaneous transmission of B and C (which can cause collision at D in this case) can be avoided.

Although jittering can be theorically implemented at different layers of the

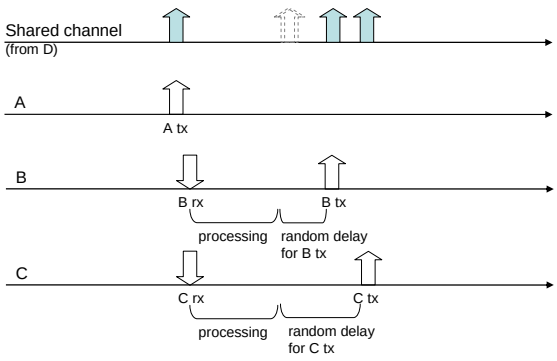

Figure 15: Use of jitter for flooding. Node A is flooding a packet in a network. Node B and C wait a random delay before the packet is retransmitted. The dashed overlapping arrows represent the packet collision that would occur if no jitter were used.

protocol stack, it has been shown that its use in layers upper than L3 brings little benefit [57]. As the problem of systematic collisions affects every L3 routing protocol using wireless flooding, jittering techniques can be implemented by

different protocols. The addition of random delays in flooded packets impacts differently in proactive and reactive protocols, given the different use of flooding in both routing strategies. Other jittering effects are due to the specifities of the techniques employed in each case. In proactive protocols where jitter is used (as described in RFC 5148 [56], which recommends to introduce random delays and piggyback all pending messages when a transmission is scheduled), such as OLSR or the OSPF extensions for MANETs, jittering leads to longer LSA messages – this may cause additional packet collisions, if jitter values are not configured properly [58, 59]. In reactive protocols such as AODV, where jitter is used for Route Request (RREQ) flooding, the addition of random delays may lead to suboptimal path selections, which can be minimized by adapting the random distribution used for determining jitter values [60, 61].

Duplicate Packets and Detection Techniques The reception of duplicate packets is a common situation in wireless flooding, due to the fact that flooded messages are retransmitted by forwarding nodes over the same wireless interface in which they were received. Consider the situation of Figure 16: router *N2* is retransmitting a broadcast packet received from router *N1* on the same interface as the one over which it was received, so as to ensure receipt also by router *N3*, causing router *N1* to receive the packet a second time.

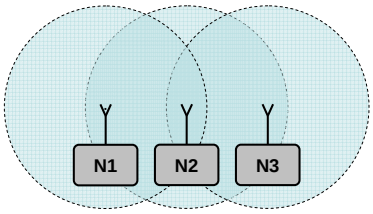

Figure 16: The need for duplicate detection: retransmission over the same interface as a packet was received.

Depending of the protocol and the use it makes of flooding and of flooded packets, the way to detect duplicate packets might be different. In link-state routing protocols such as OLSR or OSPF, for instance, flooded messages are link-state advertisements (LSAs) that are stored locally before being retransmitted, in case they bring fresh topology information; in this case, a duplicate LSA can be easily recognized by checking whether the LSA is already installed in the local Link-State Database (LSDB). If flooded messages are not stored locally, the protocol needs to store state for every forwarded message in order to detect a duplicate – this is, for instance, the strategy of the Simplified Multicast Forwarding (SMF) protocol [62]. In case a received message was already received and forwarded, it is dropped.

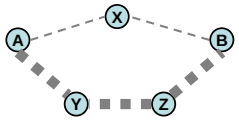

Figure 17: An example of different link metric. $A\bar{X}$, $X\bar{B}$ are unreliable links; $A\bar{Y}$, $Y\bar{Z}$, $Z\bar{B}$ are reliable links.

4.3 Link Metrics

Metrics are used to evaluate the cost of a link or a path (set of links), so that a routing protocol is able to determine whether a path or a link should be preferred over another.

The simplest link metric is the **hop-count**: a link has metric 1 if it is available, 0 otherwise. Typically, in the early versions of routing protocols for spontaneous wireless networks (e.g., AODV, OLSRv1 for mobile ad hoc networks), only the hop-count metric is used. This way, the metric or cost for a path is equal to the number of hops involved.

When a route between two hosts is being calculated under the hop-count metric, paths with less number of hops are preferred to paths with more number of hops. However, using only minimum hop routes in spontaneous wireless networks may result in suboptimal routing in practice, as the minimum-hop routes are not necessarily the best ones [63, 64].

Figure 17 give an example showing the limit of hop-count metric. The minimum hop route from node A to B is $\{A, X, B\}$. However, the links $A\bar{X}$ and $X\bar{B}$ are poor with high loss rate (but still able to deliver packets), and $A\bar{Y}$, $Y\bar{Z}$, $Z\bar{B}$ are reliable links. In this case, $\{A, Y, Z, B\}$ is preferred to the route with minimum hop count.

Because of the limitation of hop-count metric, new metrics need to be defined. The link metrics used in spontaneous wireless network are expected to have following properties [65]:

- **Dimensionless**. The metric may correspond to specific physical information, but this knowledge is not used by the routing protocol.
- **Additiveness**. The metric of a route is the sum of the metrics of the links forming that route. It also requires a metric where a low value of a link metric indicates a "good" link a high value of a link metric indicates a "bad" link.
- **Directionality**. The metric from a router A to router B does not need be the same as the metric from B to A. This is a direct consequence of the fact that wireless links are not bi-directional.

The kind of metric used in a network depends on the link/physical layer protocol used, the type of information that is available from lower layers, the application requirements, etc. Some examples of link metric include delay, packet loss probability (Expected Transmission Count, ETX [66], that estimates the average number of transmissions before success over a link), queue length (at the receiver) or data rates (Expected Data Rate, EDR [67]; this metric is not additive, thus a mapping that inverts its ordering must be applied).

5 IETF Routing Protocols for Spontaneous Wireless Networks

Since the late 1990s, in parallel with the emergence and deployment of new and more flexible networking technologies, the IETF has embarked upon a path of designing, developing and standardizing new routing protocols and flooding mechanisms. These protocols and mechanisms are designed for networks with increasingly more fragile and low-capacity links, with less pre-determined connectivity properties and with increasingly constrained router resources.

Most of the IETF protocol design and standardization activity has focused on protocols designed for Mobile Ad hoc Networks (MANETs) and Low-Power Lossy Networks (LLNs), both defined in section 1.3. This section presents the main flooding and routing protocols designed and standardized by the IETF for these types of networks in the last years: OLSRv1 and OLSRv2, RPL, AODV and LOADng.

Routing in MANETs: OLSR and AODV IETF activities targeting MANETs have converged on the development of two protocols, each one representative of one of the two main routing families (see section 2.2): reactive and proactive routing.

IETF design and standardization work in the reactive routing realm for mobile ad hoc networks first led to the Ad-hoc On-demand Distance Vector protocol (AODV) [33]; the efforts in proactive routing, in turn, led to the Optimized Link State Routing (OLSR) [25]. A distance vector protocol, AODV operates in an *on-demand* fashion, acquiring and maintaining routes only while needed for carrying data, by way of *Route Request-Route Reply* exchanges. A link state protocol, OLSR is based on periodic control messages exchanges, and each router proactively maintaining a routing table with entries for all destinations in the network. OLSR provides low delays in forwarding and has a predictable, constant control overhead – at the expense of requiring memory in each router for maintaining complete network topology. AODV limits the memory required for routing state to that for actively used routes – at the expense of delays for the *Route Request-Route Reply* exchange to take place, and control overhead dependent on data flows.

Based on the operational experience acquired through AODV and OLSRv1, the IETF is currently designing and developing successors for OLSR and AODV. In the first case, the IETF community involved in OLSR has standardized OLSR version 2 (OLSRv2) [68] and its related components (packet format [69] [70], NHDP [47]). Work on AODV version 2 [71] has started, as AODV derivative flourished: IEEE 802.11s [72], which is based on AODV, and the G3-PLC standard [73], published in 2011, which specifies the use of the *6LoWPAN Ad hoc Routing Protocol* (LOAD, specified in `draft-daniel-6lowpan-adhoc-routing`) [74] at the MAC layer, for providing layer 2 routing for utility (electricity) metering networks.

Routing in LLNs: RPL and LOADng LLNs can be regarded as a subset of MANETs, but with more stringent constraints in terms of device CPU and memory limitations, and work over more fragile links. Concerning LLNs, two protocols can be highlighted: RPL and LOADng. The IETF explored the problems of routing and adaptation of IPv6 for operation over the IEEE 802.15.4 MAC protocol, accommodating characteristics of that MAC layer, and with a careful eye on resource constrained devices (memory, CPU, energy, ...). Two initial approaches to such routing were explored: *mesh-under* and *route-over*. Both approaches entail different additional assumptions on the (link) characteristics of the addressed spontaneous wireless network, not present in the general networking model described in section 3.3.

1. The *mesh-under* approach performs L2.5 multi-hop routing, that is, provides routing in an adaptation layer between 802.15.4 (MAC layer, L2) and IP (network layer, L3). This L2.5 routing enables the underlying mesh-routed multi-hop topology to be presented at the network layer as a single broadcast domain.

2. The *route-over* approach, in contrast, exposes the underlying multi-hop topology to the IP layer, whereupon IP routing would build multi-hop connectivity.

The IETF efforts on routing over 802.15.4 initially led to LOAD [74], a derivative of AODV adapted for L2-addresses and mesh-under routing, and with some simplifications over AODV (*e.g.,* removal of intermediate node replies and sequence numbers). However, 6LoWPAN was addressing other issues regarding adapting IPv6 for IEEE 802.15.4, such as IP packet header compression, and efforts to solve routing issues were suspended. In parallel with these efforts, the IETF has also specified the "Routing Protocol for Low-power lossy networks" (RPL), designed to support 6LoWPAN networks in a route-over configuration [75, 76].

However, reasons for using a simplified reactive approach instead of RPL have emerged, including better support for bi-directional data flows such as a request/reply of a meter reading [77], as well as algorithmic and code complex-

ity reasons [78]. These observations led on one hand to a renewed interest in AODV-derived protocols for specific scenarios, resulting in LOADng [79] [80] and AODVv2 [71], while on the other hand leading to the development of an extension of RPL to support reactive path discovery (P2P-RPL [81]).

5.1 Optimized Link State Routing Protocol (OLSR)

OLSR is developed for mobile ad hoc networks, and operates as a table driven, proactive protocol, i.e., it exchanges topology information with other routers in the network regularly. The key concept used in the protocol is that of multipoint relays (MPRs, described in section 4.2), selected nodes which forward broadcast messages during the flooding process. This efficient flooding technique substantially reduces the message overhead as compared to a classical flooding mechanism.

OLSR version 1 was standardized in RFC 3626 [25]. The work continues as OLSR version 2 (OLSRv2 [68]), which retains the same basic algorithms as its predecessor, however offers various improvements, *e.g.* a modular and flexible architecture allowing extensions, such as security, to be developed as add-ons to the basic protocol.

Every router running OLSR in the network generates two types of messages: *Hellos* and *Topology Control* (TC) messages. Information collected through exchange of these messages allows routers to perform the three basic processes of OLSR: Neighborhood Discovery, Link State Advertisements and Routing Set Calculation. Because OLSR (version 1) and OLSRv2 shares the same basic mechanisms, the text below applies to both protocols.

Neighborhood Discovery OLSR routers discover their neighborhood by exchanging Hello messages with their 1-hop neighbors, as explained in section 4.1. These Hello messages can be generated proactively at a regular interval or as a response to a change in the router itself. In OLSR, a Hello message contains the local interface address(es), and its 1-hop neighbor addresses. With the broadcast of Hello messages to the router's 1-hop neighbor, the router is able to get the topology information in two hops.

Link State Advertisements Link State Advertisement is the process where by the determined link state information is advertised through the network. For OLSR, this process is optimized by MPR flooding. MPR selection is encoded in outgoing Hellos.

Routers may express, in their Hello messages, their "willingness" (integer between 1 "will never" and 7 "will always") to be selected as MPR, which is taken into consideration for the MPR calculation. This is useful, for example, when an OLSRv2 network is *managed*, meaning that its topology is known or

predictable. The set of routers having selected a given router as MPR is the MPR-selector-set of that router. Each router must advertise, at least, all links between itself and its MPR-selector-set, in order to allow all routers to calculate shortest paths.

Such link state advertisements are carried in Topology Control (TC) messages. TC messages are broadcast by each node to the whole network to build the intra-forwarding database needed for routing packets. A TC message is sent by a node in the network to declare a set of links, which must include at least the links to all nodes of its MPR Selector set, *i.e.*, the neighbors which have selected the sender node as a MPR. TC messages are received by all nodes in the network, by way of the MPR flooding process described above. With the broadcast of TC messages to the whole network, the node is able to get the topology information that is more than two hops away. TCs are sent periodically, however certain events may trigger non-periodic TCs.

Routing Set Calculation The Routing Set of a router is populated with Routing Tuples that represent paths from that router to all destinations in the network. These paths are calculated based on the Network Topology Graph, which is constructed from information in the Information Bases, obtained via Hello and TC message exchange.

Changes to the Routing Set do not require any messages to be transmitted. The state of the Routing Set should, however, be reflected in the IP routing table by adding and removing entries from that routing table as appropriate. Only appropriate Routing Tuples (in particular only those that represent local links or paths to routable addresses) need to be reflected in the IP routing table.

OLSR does not mandate which algorithm to be used for path calculation, as along as the shortest paths for all destinations from all local OLSR interfaces can be obtained using Network Topology Graph. One example is Dijkstra's algorithm [21].

5.2 Ad Hoc On-Demand Distance-Vector Protocol (AODV)

The Ad hoc On-Demand Distance Vector (AODV) [33] protocol enables dynamic, self-starting, multi-hop routing between participating mobile routers wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication.

Compared to pro-active protocols like OLSR, AODV is more suitable under following constraints:

- Few concurrent traffic flows in the network (i.e., traffic flows only between few sources and destinations);

- Little data traffic overall, and therefore the traffic load from periodic signaling (for proactive protocols) is greater than the traffic load from flooding RREQs (for reactive protocols);
- State requirements on the router are very stringent, i.e., it is beneficial to store only few routes on a router.

AODV was initially standardized as an experimental RFC in 2003 [33]. Derivatives of AODV include 802.11s (with HWMP [72]) and LOADng [79]. In the following of this section, the basic mechanisms of AODV, *Route Discovery* and *Route Maintenance* are explained. Then a main derivative work of AODV, called LOADng, is also introduced. Note that at the time of writing, work on AODVv2 [71] has just started, and thus we will not elaborate further on AODVv2 in this chapter.

Route Discovery The route discovery process is initiated when a source router needs a route to a destination router and it does not have a route in its routing table. The source router floods the network with a RREQ packet specifying the destination for which the route is requested. When the destination router, or an intermediate router with sufficiently up-to-date information about the requested destination, receive the RREQ packet, they generate a Route Reply (RREP) packet, which is sent back to the source along the reverse path. Each router along the reverse path sets up a forward pointer to the router it received the RREP from. This sets up a forward path from the source to the destination.

Route Maintenance When a router detects a broken link while attempting to forward a packet to the next hop, it generates a RERR packet that is sent to all sources using the broken link. The RERR packet erases all routes using the link along the way. If a source receives a RERR packet and a route to the destination is still required, it initiates a new route discovery process.

5.2.1 Lightweight On-demand Ad hoc Distance-Vector (LOADng)

The *Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation* (LOADng) [79] is derived from AODV. Compared to AODV [33], it has more concise and flexible message format, and simplified message processing, which makes it more adapted to networks with constrained devices, such as sensor networks. It is also used for ITU Standard G. 9956 [73].

Compared to AODV, LOADng has both simplifications and extensions to be more suitable to LLNs:

- Only the destination is permitted to respond to an RREQ; intermediate LOADng Routers are explicitly prohibited from responding to RREQs, even if they may have active routes to the sought destination. This also

eliminates Gratuitous RREPs while ensuring loop freedom, so that the protocol complexity can be greatly reduced.

- A LOADng Router does not maintain a precursor list, thus when forwarding of a data packet to the recorded next hop on the route to the destination fails, an RERR is sent only to the originator of that data packet. The rationale for this simplification is an assumption that few overlapping routes are in use concurrently in a given network.
- Optimized flooding is supported, reducing the overhead incurred by RREQ generation and flooding. If no optimized flooding operation is specified for a given deployment, classical flooding is used by default.
- Different address lengths are supported – from full 16 bytes IPv6 addresses over 6 bytes MAC addresses and 4 bytes IPv4 addresses to shorter 1 and 2 bytes addresses such as RFC 4944 [82]. The only requirement is, that within a given routing domain, all addresses are of the same address length.
- Control messages are carried by way of the Generalized MANET Packet/Message Format [69].
- Using RFC 5444 [69], control messages can include TLV (Type-Length-Value) elements, permitting protocol extensions to be developed.
- LOADng supports routing using arbitrary additive metrics, which can be specified as extensions to this protocol.

5.3 Routing Protocol for LLNs (RPL)

RPL – the *Routing Protocol for Low Power and Lossy Networks* [75] – is an IPv6 routing protocol designed and standardized by the ROLL Working Group in the IETF. It is is intended to be the IPv6 protocol for LLNs and sensor networks, applicable in all kinds of deployments and applications of LLNs.

DODAG Construction The basic construct in RPL is a "Destination Oriented Directed Acyclic Graph" (DODAG), depicted in Figure 18 . In a converged LLN, each RPL router has identified a stable set of parents, each of which is a potential next-hop on a path towards the "root" of the DODAG, as well as a preferred parent. Each router, which is part of a DODAG (i.e. has selected parents) will emit DODAG Information Object (DIO) messages, using link-local multicast, indicating its respective rank in the DODAG (i.e. distance to the DODAG root according to some metric(s), in the simplest form hop-count). Upon having received a (number of such) DIO messages, a router will calculate its own rank such that it is greater than the rank of each of its parents, select a preferred parent and then itself start emitting DIO messages. The emission of DIO message is controlled by *Trickle* Algorithm [83], to reduce the flooding overhead.

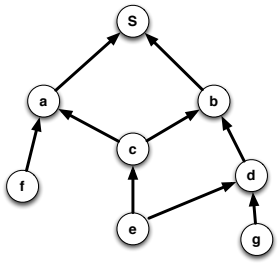

Figure 18: RPL Basic Construct: DODAGs

The DODAG formation thus starts at the DODAG root (initially, the only router which is part of a DODAG), and spreads gradually to cover the whole LLN as DIOs are received, parents and preferred parents are selected and further routers participate in the DODAG. The DODAG root also includes, in DIO messages, a DODAG Configuration Object, describing common configuration attributes for all RPL routers in that network - including their mode of operation, timer characteristics etc. RPL routers in a DODAG include a verbatim copy of the last received DODAG Configuration Object in their DIO messages, permitting also such configuration parameters propagating through the network.

A Distance Vector protocol, RPL restricts the ability for a router to change rank. A router can freely assume a smaller rank than previously advertised (i.e. logically move closer to the root) if it discovers a parent advertising a lower rank, and must then disregard all previous parents of higher ranks. The ability for a router to assume a greater rank (i.e. logically move farther from the root) than previously advertised is restricted, to avoid count-to-infinity problems. The root can trigger "global recalculation" of the DODAG by increasing a sequence number, DODAG version, in DIO messages.

The DODAG so constructed is used for installing routes: the "preferred parent" of an RPL router can serve as a default route towards the root, or the root can embed in its DIO messages the destination prefixes, included by DIOs generated by RPL routers through the LLN, to which connectivity is provided by the root. Thus, RPL by way of DIO generation provides "upward routes" or "multipoint-to-point routes" from the sensors inside the LLN and towards the root.

"Downward routes", i.e., the routes from root to sensor nodes, are enabled by having sensors issue Destination Advertisement Object (DAO) messages, propagating as unicast via parents towards the DODAG root. These describe which prefixes belong to, and can be reached via, which RPL router. In a network, all RPL routers must operate in either of storing-mode or non-storing-mode, specified by way of a "Mode of Operation" (MOP) flag in the DODAG Configuration

Object from the root. Depending on the MOP, DAO messages are forwarded differently towards the root:

- In *non-storing-mode*, an RPL router originates DAO messages, advertising one or more of its parents, and unicast it to the DODAG root. Once the root has received DAOs from an RPL router, and from all routers on the path between it and the root, it can use source routing for reaching advertised destinations inside the LLN.
- In *storing-mode*, each RPL router on the path between the originator of a DAO and the root records a route to the prefixes advertised in the DAO, as well as the next-hop towards these (the router, from which the DAO was received), then forwards the DAO to its preferred parent.

"Point-to-point routes", for communication between devices inside the LLN and where neither of the communicating devices are the DODAG root, are as default supported by having the source sensor transmit via its default route to the DODAG root (i.e., using the upward routes) which will then, depending on the "Mode of Operation" for the DODAG, either add a source-route to the received data for reaching the destination sensor (downward routes in non-storing-mode) or simply use hop-by-hop routing (downward routes in storing-mode). In the case of storing-mode, if the source and the destination for a point-to-point communication share a common ancestor other than the DODAG root, a downward route may be available (and used) before reaching the DODAG root. Both of these modes stretch the route by important factors, and lead to significantly longer paths compared to the shortest P2P paths available in the network [84]. To address this issue, an extension of RPL called RPL-P2P [81] is currently developed by the IETF. P2P-RPL defines a new mode of operation which provides RPL with a reactive approach to discover better paths on demand between an arbitrary source and destination, without having to go through the root or the first common ancestor of this source and destination.

While RPL has been specified as *Proposed Standard* in IETF, its applicability and performance in LLNs are not yet fully understood [85]. The following lists some limitations and concerns that have emerged concerning basic RPL mechanisms.

Requirement of DODAG Root In RPL, the DODAG Root has both a special responsibility and is subject to special requirements. The DODAG Root is responsible for determining and maintaining the configuration parameters for the DODAG, and for initiating DIO emissions. The DODAG Root is also responsible (in both storing and non-storing mode) for being able to, when downward routes are supported, maintain sufficient topological information to be able to construct routes to all destinations in the network.

In a given deployment, selected RPL Routers can be provisioned with the required energy, memory and computational resources so as to serve as DODAG

Roots, and be administratively configured as such - with the remainder of the RPL Routers in the network being of typically lesser capacity. In storing mode, the DODAG root needs to keep a routing entry for all RPL Routers in the RPL instance. In non-storing mode, the resource requirements on the DODAG Root are likely much higher than in storing mode, as the DODAG Root needs to store a network graph containing complete routes to all destinations in the RPL instance, in order to calculate the routing table (whereas in storing mode, only the next hop for each destination in the RPL instance needs to be stored, and aggregation may be used to further reduce the resource requirements).

Data Traffic Flows RPL makes a-priori assumptions of data traffic types, and explicitly defines three such traffic types:

1. sensor-to-root data traffic (multipoint-to-point), which is predominant,
2. root-to-sensor data traffic (point-to-multipoint), which is rare, and
3. sensor-to-sensor (point-to-point) data traffic, which is extremely rare.

RPL is suited for networks where sensor-to-root traffic is dominant, by distribution of DIO messages and building of a collection tree. The one way traffic from the sensor to the root can be forwarded through the preferred parent.

However, the data traffic characteristics, assumed by RPL, do not represent a universal distribution of traffic types in LLNs. There are scenarios where sensor-to-sensor traffic is a more common occurrence, e.g., in Building Automation scenarios. In addition, there are scenarios, where all traffic is bi-directional. For example, the IETF protocol for use in constrained environments, CoAP [86, 87], makes use of acknowledgments to control packet loss and ensure that packets are received by the packet destination. In the four message types defined for CoAP: confirmable, acknowledgement, reset and non-confirmable, the first three are dedicated for sending/acknowledgement cycle.

The DAO Mechanisms: Downward and Point-to-Point Routes In RPL, the "mode of operation" stipulates that either downward routes are not supported (MOP=0), or that they are supported by way of either storing or non-storing mode. In case downward routes are supported, RPL does not provide any mechanism for discriminating between which routes should or should not be maintained. In particular, in order to calculate routes to a given destination, all intermediaries between the DODAG Root and that destination must themselves be reachable effectively rendering downward routes in RPL an "all-or-none" situation.

The basic mechanisms in RPL force the choice between requiring all RPL Routers to have sufficient memory to store route entries for all destinations (storing mode) or suffer increased risk of fragmentation, and thus loss of data packets, while consuming network capacity by way of source routing through

the DODAG Root (non-storing mode).

In addition, RPL does not explicitly specify how the DAO message are sent, which are used to build "downward" routes from root to sensors. This would make the different implementations unlikely to be interoperable.

6 Routing in Wired/Wireless Internetworks with OSPF

Protocols reviewed in section 5 have been specifically designed for spontaneous wireless networks. However, the increasing deployment of wireless technologies and the integration of different sorts of flexible networks with the Internet is leading to more complex inter-networks, neither purely wired networks nor purely spontaneous wireless networks, resulting from the interconnection of wireless mesh networks with fixed, wired networking infrastructure, inside Internet's Autonomous Systems. Figure 19 shows schematically a *compound Autonomous System*, in which fixed and wireless mesh networks are interconnected in the same routing domain.

In these scenarios, a classic IGP (in IP networks, typically OSPF) is used

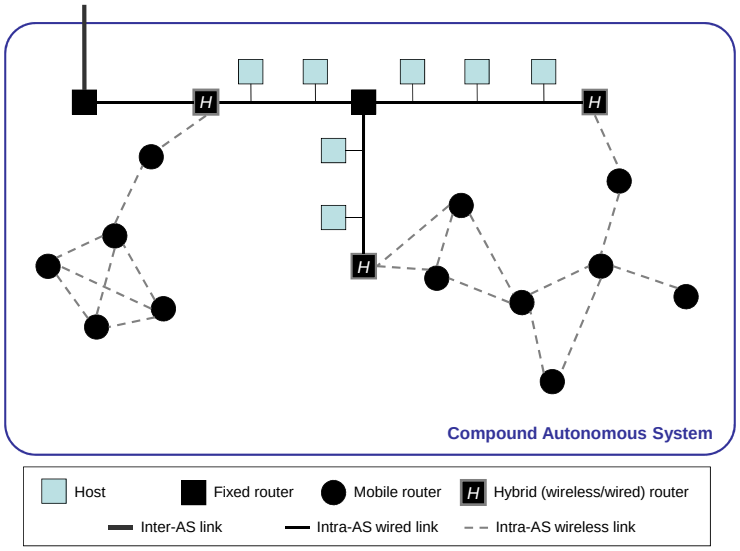

Figure 19: A compound Autonomous System.

for routing in the fixed network inside the AS. Rather than using an additional protocol for routing in the wireless mesh network inside the AS, it makes sense to explore approaches *extending* the protocol already used in the AS, so that it can take into consideration the issues described in section 3, run efficiently over

wireless dynamic networks, handle the heterogeneity of the hybrid internetwork and thus perform routing over the whole compound AS. Extension for hybrid internetworks of a protocol already in use can significantly reduce the transition costs (technical implementation, engineer training...), as only minor changes, or no changes at all, will be needed in the networks using the original protocol. It may be also benefial in terms of networking management complexity and routing performance, as a single (extended) routing protocol is more bearable than several protocols running in different parts of the internetwork. In the latter case, route distribution between different protocols operating at wireless and wired networks needs to be performed in specific *hybrid routers* (see Figure 19); this adds another layer of networking complexity and is likely to cause routing suboptimality. The advantages of extending a protocol in use come, however, at the expense of increasing the complexity and narrowing the space for optimization in the extended protocol, which needs to cope efficiently with a broader range of networking scenarios.

This section reviews the IETF extensions of the Open Shortest Path First (OSPF) protocol for MANETs. Section 6.1 shortly reviews the basics of OSPF, the main IGP for IP networks and a major representative of the link-state routing family, and indicates the reasons that prevent OSPF to be used "as-is" in wireless multi-hop ad hoc networks. Section 6.2 describes the main elements of the three extensions for MANETs standardized by the IETF: Multi-Point Relays (MPR-OSPF, specified in RFC 5449), MANET Designated Routers (OSPF-MDR, specified in RFC 5614) and Overlapping Relays (OR/SP, specified in RFC 5820).

6.1 Open Shortest Path First Protocol (OSPF)

OSPF [22, 23] is a link-state routing protocol for IP networks. Each router maintains a local **Link State Database** (LSDB), representing the full network topology. The protocol ensures that each router has the same LSDB and, thus, the exact same view of the network topology. Paths to every possible destination are derived from the **Shortest Path Tree** (SPT) that every router computes, by way of Dijkstra's algorithm [21].

Routers acquire information about their 2-hop (bi-directional) neighborhood and advertise their own presence and their 1-hop neighbors by periodically exchanging **Hello** messages with all their neighbors, in the way described in section 4.1.

Topology information is also disseminated through the network by way of **Link State Advertisements** (LSAs). Each such LSA lists mainly the current adjacencies of the router which generated the LSA. The local LSDB stored by a router contains the most recent LSAs received from every other router in the network.

Each router synchronizes its LSDB with a subset of its bidirectional neighbors. Synchronization between two neighboring routers is performed on a master-slave basis, by exchanging summaries of all LSAs in their LSDB, and then allowing each router to request retransmission of missing or locally outdated link-state advertisements. Links between a router and its synchronized neighbors are called **adjacencies**. The set of adjancencies is expected to form a network-wide connected backbone, connecting all routers in the network, in order to ensure paths can be computed correctly.

Finally, routers also acquire remote topology information by receiving LSAs. LSAs are flooded through the entire network in reliable fashion (explicit acknowledgements and retransmissions) via the backbone formed by adjacencies. Thus, any router which has formed adjacencies must advertise this periodically by way of constructing an LSA and performing LSA flooding.

$$\text{SPT links} \subset \text{Adjacent links} \subset \text{Bi-directional links} \tag{1}$$

Remote topology information is then used for the construction of the Shortest Path Tree: each router computes the shortest paths based on the information contained in the set of received LSAs.

This operation implies that OSPF exchanges control traffic and performs routing according to two principles:

1. Data traffic is routed to the corresponding destination through links contained in the Shortest Path Tree.
2. Data and control and traffic (LSAs and acknowledgements) is sent over adjacent (synchronized) links.

Interface Types Rules for flooding and adjacency handling vary for the different *interface types* supported by OSPF. Four main interface types are specified in RFC 2328 [22]:

- *Point-to-point interfaces* are those connected to point-to-point links. Such a link only permits communicating with a single (neighboring) interface.
- *Broadcast interfaces* participate in a broadcast link, in which any interface can directly communicate with any other interface. A classic example of broadcast link is Ethernet.
- *Non-Broadcast Multiple Access (NBMA) interfaces*, for non-broadcast networks (*i.e.*, networks supporting more than two routers, but without broadcast capability) in which each pair of interfaces can communicate directly. This interface type may be used with X.25 and ATM networks with Switched Virtual Circuits (SVC).

- *Point-to-multipoint interfaces*, for those non-broadcast networks in which direct communication between any pair of interface is not guaranteed. This may be the case, for instance, in Frame Relay networks using only Permanent Virtual Circuits (PVC), if not every pair of routers have a PVC between them.

OSPF only provides support for the two first interface types. In the NBMA and point-to-multipoint cases, OSPF *emulates* the behavior of a broadcast link and point-to-point links, repectively. For NBMA networks, LSA flooding and LSDB synchronization are handled by way of **Designated Routers** (DRs). A Designated Router (as well as a Backup Designated Router, BDR, expected to become DR in case of DR's failure) is elected from among routers whose interfaces are connected to the same link. DRs (and BDRs) form adjacencies with all the routers connected to the same link, and the Designated Router becomes responsible for flooding of LSAs, originated by routers on that link. A router point-to-multipoint link, in turn, is handled as a set of independent point-to-point links, one per neighboring router with which direct communication is available.

6.2 MANET Extensions: A Wireless Interface for OSPF

Standard interface types for non-broadcast networks (point-to-multipoint and NBMA) are not adapted for operation in a wireless multi-hop ad hoc network. As discussed in section 3.2, routers in a wireless multi-hop network may not agree on which routers are connected to a given link. This implies that the DR-based mechanisms of NBMA cannot be directly used in wireless multi-hop ad hoc networks. DR election may be inconsistent between different routers, causing flooding to disfunction and, possibly even preventing the protocol from converging. The use of the point-to-point interface, in turn, does not scale in these dynamic networks: point-to-point emulation for every pair of interfaces directly reachable to each other causes an excessive control traffic overhead, even for relatively small networks, as shown experimentally in Henderson *et al.* [88]. This fact has led the research and industrial OSPF community to develop a new interface type to support the characteristics of wireless multi-hop ad hoc networks.

This new interface type needs to optimize the operation of (1) describing local topology in LSAs, (2) performing LSA flooding and (3) establishing and maintaining adjacencies in the context of wireless communication. Different approaches have been explored at the IETF, which have led to three different extensions of OSPF, consisting of three different interfaces for wireless multi-hop networks (or MANETs, in IETF's terminology).

Multi-Point Relays MPR-OSPF [49] use Multi-Point Relays (MPR [54], see section 4.2) to optimize topology description, LSA flooding and LSDB synchronization. Nodes select MPRs from among their bidirectional neighbors in order

to provide 2-hop coverage, and use them to disseminate their LSAs. A router becomes adjacent to both neighbors which it has selected as multi-point relays (MPRs) and neighbors which have selected the router as their multi-point relay (MPR selectors). Each router advertises in its LSAs its own MPRs and MPR selectors; consequently, the Shortest Path Tree is constructed over the set of adjacencies.

Overlapping Relays & Smart Peering The Overlapping Relays / Smart Peering (OR/SP) extension of OSPF [51] floods LSAs via MPR as in MPR-OSPF, where the multi-point relays selected among the adjacent (synchronized) neighbors of the electing router. Adjacencies are selected following the Smart Peering (SP) rule, in which a neighbor becomes adjacent if it is not already reachable through the computing router's current Shortest Path Tree. The SP criterion reduces dramatically the number of synchronized links in the network. LSAs list adjacent neighbors, and may also list additional bidirectional neighbors (so-called *unsynchronized adjacencies*). The SPT is thus constructed over adjacencies and a subset of bidirectional neighbors.

MANET Designated Routers OSPF-MDR [50] relies on two Connected Dominating Sets (CDS): the MANET Designated Routers (MDR) backbone and the Backup MDRs (BMDR) backbone. Both extend the standard OSPF (for NBMA networks) notions of "Designated Routers" and "Backup Designated Routers" to MANETs. This implies that routers behave differently depending on their role. MDRs are the only nodes allowed to flood LSAs. Every non-MDR router becomes adjacent at least to the closest MDR, and MDRs must become adjacent to other MDRs. LSAs list a configurable subset of links of the originator, which must at least include the adjacent neighbors. The SPT is thus constructed over adjacencies and a subset of bidirectional neighbors.

Compatibility with the OSPF routing philosophy detailed in section 6.1 varies significantly depending on the considered OSPF extension. MPR-OSPF is designed to preserve the two principles in OSPF routing: shortest, synchronized paths for data traffic and synchronized links for control traffic. Under the Overlapping Relays extension, data traffic paths are synchronized, but they are not necessarily optimal, as routers only synchronize a small fraction of their available links. Although providing several configuration parameters to tune the protocol's performance, the MANET Designated Routers (OSPF-MDR) also try to minimize the control traffic by reducing the number of synchronized links, even when this may lead to path suboptimality for data traffic.

Preserving OSPF routing principles Performed experiments suggest that extensions providing (theoretical) shortest paths for data traffic achieve a better performance than those neglecting shortest paths or allowing suboptimal routing in a wireless multi-hop network [52, 89]. Further analysis showed that preserving the second principle (all traffic is sent over synchronized links) in

OSPF over mobile ad hoc networks, in the way that MPR-OSPF does, requires a significant amount of overhead due to the LSDB exchange between routers becoming *adjacent* (synchronized), and does not bring substantial benefit, due to short lifetime of several synchronized links in a wireless multi-hop dynamic network [90].

Why maintain LSDB synchronization in Extended OSPF ? LSDB synchronization between two routers proves useful in classic (wired) Internet internetworks, but is an expensive operation to perform in a dynamic (wireless multi-hop or mobile ad hoc) network. This is the reason why other link-state protocols such as OLSR, designed specifically for wireless mesh and mobile ad hoc networks, does not provide any mechanism for synchronizing the LSDBs of neighboring routers: topology information is only disseminated through the network by way of LSA flooding (see section 5.1). In the case of extended OSPF, there are two reasons for maintaining the notion of LSDB synchronization:

1. **OSPF backwards compatibility**. In standard OSPF [22, 23], the notion of *adjacency* is essential in the protocol's architecture and the router's operation, regardless of the specific types used for running OSPF in the router's interfaces.

2. **Routing in heterogeneous internetworks**. Unlike OLSR, extended OSPF is expected to run over hybrid internetworks (or compound Autonomous Systems, see Figure 19), that is, internetworks in which wired networks handled by standard OSPF interface types coexist and are interconnected with wireless multi-hop networks using the adapted wireless interface of (extended) OSPF. In these scenarios, in which some nodes (with wireless interfaces) are exposed to frequent disconnections from the network (meaning that their LSDBs may be no longer updated for a while) and others maintain stable links with their neighbors (those with wired interfaces), the fact that every router is expected to synchronize its LSDB with *at least* one of its neighbors provides an upper bound for the maximum time that a router A (in the wireless region of the internetwork) stays *disconnected* (that is, unaware of its local topology) from another router B (in the wired region of the internetwork) after missing an LSA flooded by router B. This becomes an issue as the time between consecutive LSA flooding processes from B is typically high – as wired links are stable and thus require less frequent updates about their state than wireless ones.

Further Extensions: adapted LSDB synchronization, MPR+SP and SLOT-OSPF In this context, some additional approaches can be explored beyond the three standardized extensions of OSPF. Clausen *et al.* [91], for example, propose a LSDB synchronization process based on the periodic broadcasting of *signatures* of the LSDB by every router to its neighborhood. These signatures allow neighbors of the originator to detect topology inconsistencies with its own LSDB, and request unicast retransmission of the corresponding

LSAs. This turns the standard OSPF synchronization mechanism, based on a router-to-router LSDB exchange, to a router-to-neighborhood mechanism that takes advantage from the semibroadcast nature of communication in a wireless multi-hop network.

Without modifying the standard OSPF adjacency-forming process, LSDB synchronization can be kept, but the number of adjacencies per router should be reduced as much as possible, given the high cost of synchronization in terms of overhead and its small benefit in a dynamic network, with short-lived links. Data traffic should be sent over shortest paths (that is, optimal paths over the network, according to the available LSDB information and the metric in use), but these paths do not need to be synchronized. This leads to combine in the same OSPF extension the mechanisms to provide shortest paths (MPR selection for topology description) and the mechanisms reducing the most the number of adjacencies to be established per router (*e.g.*, the Smart Peering rule used in the Overlapping Relays extension). The resulting extension, denominated MPR+SP, presents a better routing performance than extensions MPR-OSPF and OR/SP in which it is based, as shown in Cordero *et al.* [90]. Similarly, extension SLOT-OSPF [92] using the Relative Neighbor Graph (RNG [93]) for establishing adjacencies and MPR selection for computing shortest paths, also achieves better results in terms of delivery ratio and control traffic overhead than the standard extension to which it compares. In both cases (MPR+SP and SLOT-OSPF) shortest path computation, for which a comprehensive view of the network topology (with most of the links) is required, is splitted from the adjacency-forming criterion, which aims to reduce as much as possible the number of LSDB synchronizations to be performed. This split enables a further optimization of the protocol routing performance.

7 Conclusion: Integrating Spantaneous Wireless Networks in the IP Architecture

This chapter reviewed recent trends towards more collaborative network layer paradigms, accommodating spontaneous wireless networks. The thread followed throughout the chapter is the compatibility, in practice, with standard IP protocols currently at work in today's Internet. Indeed, absent such compatibility, slim are the chances that a given solution would actually be deployed 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. This chapter thus focused on standards developed by the IETF, which are relevant for spontaneous wireless networks.

In principle, spontaneous wireless networking is IP-disruptive: the way in which communication is performed in spontaneous wireless networks challenges some of the fundamental assumptions underlying traditional computer networking and the legacy IP networking architecture. The first part of this chapter has focused on identifying and discussing the impact of spontaneous wireless networking paradigms on layer 3, and has studied an alternative architectural model that could integrate spontaneous wireless networks in the IP networking architecture.

Due to their harsh characteristics, spontaneous wireless networks cannot be efficiently managed by standard protocols at layer 3 and above. In particular, legacy routing and flooding mechanisms are unsuitable to efficiently track low bandwidth, asymmetric, time-variant and lossy communication channels, between devices that may be mobile and thus create even more instability in the network topology. The second part of this chapter reviews various advanced techniques have been recently developed in order to accommodate these demanding characteristics: efficient flooding, non-trivial link metrics, neighborhood discovery, jittering techniques, duplicate detection mechanisms. These techniques are employed by several routing protocols developed by the IETF, mainly targeting Mobile Ad Hoc Networks (MANETs) and Low-Power Lossy Networks (LLNs), two categories of spontaneous wireless networks.

Taking a step back, it is perhaps worthy to observe that there are essentially four categories of solutions to deal with IP-disruptive characteristics [94]:

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 [95], 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.

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. Most of the efforts that are mentioned in this chapter fall in this category. There are however limits to what one can achieve when taking this approach: it is unlikely that one can achieve game-changing innovation if one is allowed to replace only a single, small part

of the whole system. 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 new system that performs significantly better, thanks to new protocols that can leverage cross-layer information to better cope with IP-disruptive lower layers. One example of such an approach is the XPRESS cross-layer stack [96], which collapses transport, network, and MAC layers and uses backpressure to provide better performance in wireless mesh networks. Cross-layer approaches are probably the most disruptive type of approaches, as their 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. Essentially, such an approach considers the Internet as a black box providing a service equivalent to a cable connecting source(s) and destination(s), and provides novel mechanisms efficiently using this cable to cope with IP-disruptive characteristics. One example of such construction is the experimental Delay Tolerant Networking (DTN) architecture developed by the Internet Research Task Force (IRTF) [97] [98] [99], including a specific routing protocol targeting DTNs [100].

It can be anticipated that innovative networking paradigms will continue to appear in the future, providing improvements at the price of IP-disruptive characteristics. However, in order to deploy or advance towards these new paradigms, one of the above approaches will have to be employed.

References

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

[2] "The IEEE Standards Association, 802.11." ONLINE: http://standards.ieee.org/about/get/802/802.11.html.

[3] "The IEEE Standards Association, 802.16." ONLINE: http://ieee802.org/16/.

[4] "3GPP Telecommunications Standards Body." ONLINE: http://www.3gpp.org.

[5] "Customers Angered as iPhones Overload AT&T." The New York Times, September 2009.

[6] "The Commotion Wireless Project." ONLINE: https://code.commotionwireless.net/projects/commotion.

[7] "One Laptop Per Child." ONLINE: http://one.laptop.org.

[8] "IEEE Standards Association, 802.15.4." ONLINE: http://www.ieee802.org/15/pub/TG4.html.

[9] M. Kohno, "Perspective on Future Internet Routing." Asia Future Internet Hong Kong Workshop, February 2011.

[10] "The Internet Engineering Task Force (IETF)." ONLINE: http://www.ietf.org.

[11] M. S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations." Informational RFC 2501, January 1999.

[12] J. Vasseur, "Terminology in Low power And Lossy Networks." Internet Draft, draft-ietf-roll-terminology-12, work in progress, March 2013.

[13] C. Bormann, M. Ersue, and A. Keranen, "Terminology for Constrained Node Networks." Internet Draft, draft-ietf-lwig-terminology-04, work in progress, April 2013.

[14] R. Stanica, E. Chaput, and A.-L. Beylot, "Broadcast communication in vehicular ad-hoc network safety applications," in *Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC 2011)*, (Las Vegas, NV, USA), January 2011.

[15] "Barcelona Wireless Community Network." ONLINE: http://www.guifi.net.

[16] "The Freifunk Wireless Community Networks." ONLINE: http://www.freifunk.net.

[17] "Austrian Wireless Community Network." ONLINE: http://www.funkfeuer.at.

[18] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks, 5th Edition*. Prentice Hall, 2011.

[19] D. E. Comer, *Internetworking with TCP/IP (Vol. 1): Principles, protocols and architecture, 4th Edition*. Prentice Hall, 2000.

[20] R. Perlman, *Interconnections (2nd Edition): bridges, routers, switches, and internetworking protocols*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2000.

[21] E. Dijkstra, "A note in two problems in connection with graphs," *Numerische Mathematik, no. 1*, 1959.

[22] J. Moy, "OSPF Version 2." ST RFC 2328, April 1998.

[23] R. Coltun, D. Ferguson, J. Moy, and A. e. Linden, "OSPF for IPv6." ST RFC 5340, July 2008.

[24] D. R. Oran, "OSI IS-IS Intra-domain Routing Protocol." RFC 1142, February 1990.

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

[26] R. Bellman, "On a routing problem," *Quarterly of Applied Mathematics, no. 16, vol. 1, pp. 87-90*, 1958.

[27] L. R. J. Ford, "Network flow theory," *RAND Corporation, paper P-923*, 1956.

[28] C. Hedrick, "Routing Information Protocol." RFC 1058, June 1988.

[29] G. S. Malkin and R. E. Minnear, "RIPng for IPv6." ST RFC 2080, January 1997.

[30] G. S. Malkin, "RIP Version 2." ST RFC 2453, November 1998.

[31] Y. Rekhter and T. Li, "A Border Gateway Protocol 4 (BGP-4)." ST RFC 1771, March 1995.

[32] D. B. Johnson, D. A. Maltz, and Y.-C. Hi, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad hoc Networks for IPv4." Experimental RFC 4728, February 2007.

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

[34] B. Karp and H. T. Kung, "Gpsr: Gredy perimeter stateless routing for wireless networks," in *Proceedings of the MobiCom'2000*, (Boston, MA, USA), August 2000.

[35] J. Hawkinson and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)." BCP RFC 1930, March 1996.

[36] F. Baker, "Requirements for IP Version 4 Routers." ST RFC 1812, June 1995.

[37] R. Callon, "Use of OSI IS-IS for Routing in TCP/IP and Dual Environments." RFC 1195, December 1990.

[38] D. Kotz, C. Newport, and C. Elliott, "The Mistaken Axioms of Wireless-Network Research." Technical Report TR2003-467, July 2003.

[39] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[40] E. Baccelli and C. Perkins, "Multi-hop Ad Hoc Wireless Communication." Internet Draft, draft-baccelli-manet-multihop-communication-01, work in progress, May 2012.

[41] E. Baccelli, T. H. Clausen, U. Herberg, and C. E. Perkins, "Ip links in multihop ad hoc wireless networks ?," in *Proceedings of the 17th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, (Croatia), p. 5, September 2009.

[42] T. Clausen, "A MANET Architectural Model." Inria Research Report n. 6145, January 2007.

[43] I. Chakeres, J. Macker, and T. Clausen, "Mobile Ad hoc Network Architecture," November 2007. Internet Draft, draft-ietf-autoconf-manetarch-07, work in progress.

[44] M. Gerla, K. Tang, and R. Bagrodia, "Tcp performance in wireless multihop networks," *Proceedings of the IEEE WMCSA Conference, pp. 41-50*, 1999.

[45] E. Baccelli and M. Townsley, "IP Addressing Model in Ad Hoc Networks." Informational RFC 5889, September 2010.

[46] T. Narten, E. Nordman, W. A. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)." ST RFC 4861, September 2007.

[47] T. Clausen, C. Dearlove, and J. Dean, "Mobile Ad Hoc Network Neighborhood Discovery Protocol." Std. Track RFC 6130, April 2010.

[48] Z. Shelby, S. Chakrabarti, E. Nordmark, and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)." ST RFC 6775, November 2012.

[49] E. Baccelli, P. Jacquet, D. Nguyen, and T. Clausen, "OSPF Multipoint Relay (MPR) Extension for Ad Hoc Networks." Experimental RFC 5449, February 2009.

[50] R. Ogier and P. Spagnolo, "Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding." Experimental RFC 5614, August 2009.

[51] A. Roy and M. W. Chandra, "Extensions to OSPF to Support Mobile Ad Hoc Networking." Experimental RFC 5820, March 2010.

[52] E. Baccelli, J. A. Cordero, and P. Jacquet, "Ospf over multi-hop ad hoc wireless communications," *International Journal of Computer Networks and Communications (IJCNC), vol. 2, num. 5*, September 2010.

[53] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," Proceedings of ACM MobiCom'99, Seattle, USA, 1999.

[54] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint relaying for flooding broadcast messages in mobile wireless networks," Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'2002), Big Island (Hawaii), USA, April 2002.

[55] J. A. Cordero, "Mpr-based pruning techniques for shortest path tree computation," in *Proceedings of the 18th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, (Split, Croatia), p. 5, September 2010.

[56] T. Clausen, C. Dearlove, and B. Adamson, "Jitter Considerations in MANETs." IETF Inf. RFC 5148, February 2008.

[57] R. Friedman, D. Hay, and G. Kliot, "Jittering Broadcast Transmissions in MANETs: Quantification and Implementation Strategies," tech. rep., Department of Computer Science, Technion, 2009.

[58] J. A. Cordero, P. Jacquet, and E. Baccelli, "Impact of jitter-based techniques on flooding over wireless ad hoc networks: Model and analysis," Proceedings of the 31st IEEE International Conference on Computer Communications (INFOCOM 2012), Orlando, USA, 2012.

[59] J. Cordero, "A probabilistic study of the delay caused by jittering in wireless flooding," *Wireless Personal Communications*, pp. 1–25, 2013.

[60] J. Yi, J. A. Cordero, and T. Clausen, "Jitter Considerations in On-Demand Route Discovery for Mobile Ad Hoc Networks," Proceedings of the 16th International Conference on Network-Based Information Systems (NBiS'2013), Gwanju, South Korea (to appear), September 2013.

[61] J. A. Cordero, J. Yi, and T. Clausen, "Optimization of Jitter Configuration for Reactive Route Discovery in Wireless Mesh Networks," Proceedings of the 11th International Symposium on Modeling and Optimization in Mobile, Ad hoc and Wireless Networks (WiOpt 2013), Tsakuba City of Science, Japan (to appear), May 2013.

[62] J. Macker, "Simplified Multicast Forwarding." Experimental RFC 6621, May 2012.

[63] D. S. J. D. Couto, D. Aguayo, B. A. Chambers, and R. Morris, "Performance of multihop wireless networks: Shortest path is not enough," *ACM SIGCOMM Computer Communication Review, vol. 33, issue 1, pp. 83-88*, January 2003.

[64] Z. Wang and J. Crowcroft, "Bandwidth-delay based routing algorithms," Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM'95), November 1995.

[65] C. Dearlove, T. Clausen, and P. Jacquet, "Link Metrics for the Mobile Ad Hoc Network (MANET) Routing Protocol OLSRv2 - Rationale," April 2013. Internet Draft, draft-ietf-manet-olsrv2-metrics-rationale-03, work in progress.

[66] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom)*, (San Diego, California, USA), p. 8, Sep 2003.

[67] J. C. Park and S. K. Kasera, "Expected data rate: An accurate high-throughput path metric for multi-hop wireless routing," in *Proceedings of the Second Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON 2005)*, (Santa Clara, CA, USA), September 2005.

[68] T. Clausen, C. Dearlove, and P. Jacquet, "The Optimized Link State Routing Protocol version 2." Internet Draft, draft-ietf-manet-olsrv2-11, work in progress, April 2010.

[69] T. Clausen, C. Dearlove, J. Dean, and C. Adjih, "Generalized MANET Packet/Message Format." Std. Track RFC 5444, February 2009.

[70] T. Clausen and C. Dearlove, "Representing Multi-Value Time in MANETs." IETF Std. Track RFC 5497, February 2009.

[71] C. Perkins, S. Ratliff, and J. Dowdell, "Dynamic manet on-demand (aodvv2) routing," March 2013. IETF Internet Draft, draft-ietf-manet-aodvv2-00.

[72] G. Hiertz, S. Max, R. Zhao, D. Denteneer, and L. Berlemann, "Principles of ieee 802.11s," in *Proceedings of WiMAN in conjunction with the 16th ICCCN*, (Honolulu, Hawaii, USA), p. 6, Aug 2007.

[73] "ITU-T G.9956: Narrow-Band OFDM power line communication transceivers - Data link layer specification," November 2011.

[74] K. Kim, S. D. Park, G. Montenegro, S. Yoo, and N. Kushalnagar, "6LoWPAN Ad Hoc On-Demand Distance Vector Routing," June 2007. Internet Draft, work in progress, draft-daniel-6lowpan-load-adhoc-routing-03.

[75] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, and J. Vasseur, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks," March 2012. IETF RFC 6550.

[76] J. Vasseur, N. Agarwal, J. Hui, Z. Shelby, P. Bertrand, and C. Chauvenet, "RPL: The IP routing protocol designed for low power and lossy networks." IPSO Working Paper n. 7, April 2011.

[77] U. Herberg and T. Clausen, "A comparative performance study of the routing protocols load and rpl with bi-directional traffic in low-power and lossy networks (lln)," Proceedings of the 8th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN), October 2011.

[78] T. Clausen, U. Herberg, and M. Philipp, "A critical evaluation of the "ipv6 routing protocol for low power and lossy networks"," Proceedings of the 5th IEEE International Conference on Wireless & Mobile Computing, Networking & Communication (WiMob), October 2011.

[79] T. Clausen, A. C. de Verdiere, J. Yi, A. Niktash, Y. Igarashi, H. Satoh, and U. Herberg, "The lln on-demand ad hoc distance-vector routing protocol - next generation," October 2011. Internet Draft, work in progress, draft-clausen-lln-loadng.

[80] T. Clausen, A. Camacho, J. Yi, A. C. de Verdiere, Y. Igarashi, H. Satoh, and Y. Morii, "Experience with the loadng routing protocol for llns," October 2011. Internet Draft, work in progress, draft-lavenu-lln-loadng-interoperability-report.

[81] M. Goyal, E. Baccelli, M. Philipp, A. Brant, and J. Martocci, "Reactive discovery of point-to-point routes in low power and lossy networks," March 2013. IETF Internet Draft, draft-ietf-roll-p2p-rpl-17.

[82] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," September 2007. Standards Track RFC 4944.

[83] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "The Trickle Algorithm." IETF Std. Track RFC 6206, January 2011.

[84] W. Xie, M. Goyal, H. Hosseini, J. Martocci, Y. Bashir, E. Baccelli, and A. Durresi, "A performance analysis of point-to-point routing along a directed acyclic graph in low power and lossy networks," in *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, pp. 111–116, 2010.

[85] T. Clausen, A. Colin de Verdiere, J. Yi, U. Herberg, and Y. Igarashi, "Observations of RPL: IPv6 Routing Protocol for Low power and Lossy Networks," February 2013. Internet Draft, work in progress, draft-clausen-lln-rpl-experiences-06, work in progress.

[86] Z. Shelby, K. Hartke, and C. Bormann, "Constrained Application Protocol (CoAP)." Internet Draft, draft-ietf-core-coap-14, work in progress, March 2013.

[87] W. Colitti, K. Steenhaut, and N. De Caro, "Integrating wireless sensor networks with the web," Proceedings of the Proceedings of the IEEE Workshop on Internet of Things Technology and Architectures, 2011.

[88] T. R. Henderson, P. Spagnolo, and J. K. Kim, "A wireless interface type for ospf," Proceedings of the Military Communications Conference (MILCOM'03), Seattle, WA, USA, October 2003.

[89] E. Baccelli, J. A. Cordero, and P. Jacquet, "Multi-hop relaying techniques with ospf on ad hoc networks," in *Proceedings of the 4th IEEE International Conference on Sensor Networks and Communications (ICSNC)*, (Porto, Portugal), September 2009.

[90] J. A. Cordero, T. Clausen, and E. Baccelli, "Mpr+sp: Towards a unified mpr-based manet extension for ospf," Proceedings of the 44th Annual Hawaii International Conference on System Sciences (HICSS'2002), Garden Island (Hawaii), USA, January 2011.

[91] T. Clausen, E. Baccelli, and P. Jacquet, "Ospf-style database exchange and reliable synchronization in the optimized link-state routing protocol," Proceedings of the 1st IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON'2004), Santa Clara (CA), USA, October 2014.

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

[93] G. T. Toussaint, "The relative neighborhood graph of a finite planar set," *Pattern Recognition, vol. 12, no. 4*, pp. 261–268, 1980.

[94] E. Baccelli, "IP-Disruptive Wireless Networking: Integration in the Internet," Habilitation Thesis, Université Pierre et Marie Curie Sorbonne, December 2012.

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

[96] R. Laufer, T. Salonidis, H. Lundgren, and P. LeGuyadec, "XPRESS: A Cross-layer Backpressure Architecture for Wireless Multi-hop Networks," *ACM MobiCom*, September 2011.

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

[98] K. Scott and S. Burleigh, "Bundle Protocol Specification," November 2007. Experimental RFC 5050.

[99] M. Ramadas, S. Burleigh, and S. Farrell, "Licklider Transmission Protocol," September 2008. Experimental RFC 5326.

[100] A. Lindgren, A. Doria, E. Davies, and S. Grasic, "Probabilistic Routing Protocol for Intermittently Connected Networks," September 2012. Experimental RFC 6693.

Glossary

Autonomous System "An *Autonomous System (AS)* is a connected group of one or more IP prefixes [internetwork] run by one or more network operators which has a SINGLE and CLEARLY DEFINED routing policy" [35], the term "routing policy" denoting the way that routing information is exchanged between (but not within) Autonomous Systems. In the interior of an AS, "routers may use one or more interior routing protocols, and sometimes several sets of metrics" [36].

Computer network A *computer network* is a set of network links and the computers (hosts and routers) attached to any of these links.

End system See *host*.

Host A *host* (or *end system*) is a node in the network able to be source or final destination or network traffic, but is not able to forward packets from one link to another.

Intermediate system See *router*.

IP link Two network interfaces, x and y, are connected to the same *IP link* when they can exchange packets in an IP network without requiring that any router forwards them, that is, when packets sent from one interface are received in the other with the same TTL/hop-limit value. This relationship is denoted as $x \sim_{IP} y$.

Link metric Under a routing protocol, a *link metric* is a map that matches every link in the network with an estimation of the cost of sending packets over that link. The most trivial and most widely used link metric in wireless multi-hop networks is **hop-count**: all available links are assigned a value 1. Examples of other link metrics are the Expected Transmission Count (ETX) [66], based on packet loss probability; the Expected Data Rate (EDR) or other estimations based on delay or available bandwidth.

Neighbor Two nodes are *neighbors* if they can directly communicate. More generally, two nodes are *i-hop neighbors* if they can communicate in i hops.

Network interface A *network interface* of a node is a device that provides access from that node to a network link through an underlying physical communication channel.

Network link between nodes There is a *link* between two nodes A and B, denoted by $A \longrightarrow B$, if and only if A is able to transmit data to B and B is able to receive such data, without intervention of any other node. Nodes are connected to these network links by way of network interfaces.

Router A *router* (or *intermediate system*) is a node that is able to forward packets from one network link to another. Routers take forwarding decisions based on the information they store in the local routing table.

Routing protocol A *routing protocol* is a set of procedures performed over the network in order to collect routes and maintain the routing tables of the routers in the network. These procedures enable nodes to transmit and successfully deliver packets to desired destinations in the network.

Routing table The *routing table of a router* is a local database that maps a destination in the network to the network interface through which a packet sent to that destination should be forwarded. Information in a routing table is collected and distributed by way of a routing protocol.