# Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad Hoc Networks

*Luciana Pelusi, Andrea Passarella, and Marco Conti, IIT-CNR*

## ABSTRACT

Opportunistic networks are one of the most interesting evolutions of MANETs. In opportunistic networks, mobile nodes are enabled to communicate with each other even if a route connecting them never exists. Furthermore, nodes are not supposed to possess or acquire any knowledge about the network topology, which (instead) is necessary in traditional MANET routing protocols. Routes are built dynamically, while messages are en route between the sender and the destination(s), and any possible node can opportunistically be used as next hop, provided it is likely to bring the message closer to the final destination. These requirements make opportunistic networks a challenging and promising research field. In this article we survey the most interesting case studies related to opportunistic networking and discuss and organize a taxonomy for the main routing and forwarding approaches in this challenging environment. We finally envision further possible scenarios to make opportunistic networks part of the next-generation Internet.

## INTRODUCTION

During the last few years research on multihop ad hoc networks has focused on a number of application environments. Originally conceived for military applications, and aimed at improving battlefield communications and survivability, multihop ad hoc networks have lately been proposed in many civil scenarios. As far as the application environments of these networks increase, their traditional communication paradigms need adequacy. Two main evolutions of multihop ad hoc networks are envisioned, namely, *mesh networks* and *opportunistic networks*. In this article we focus on Opportunistic Networks.

In opportunistic networking no assumption is made with regard to the existence of a complete path between two nodes wishing to communicate. Source and destination nodes might never be connected to the same network, at the same time. Nevertheless, opportunistic networking techniques allow such nodes to exchange messages between them. Usually this comes at the price of additional delay in messages delivery, since messages are often buffered in the network waiting for a path towards the destination to be available. However, there is a wide range of applications that are able to tolerate this. Actually, this communication paradigm is reminiscent of widespread applications such as e-mailing. Furthermore, allowing nodes to connect and disconnect at will paves the way for a number of novel application scenarios in the field of mobile ad hoc networks. So far, the main focus of research on opportunistic networks has been on routing and forwarding issues, because finding routes towards the desired destination in such disconnected environments is regarded as the most compelling issue.

Several concepts behind opportunistic networks come from the studies on delay-tolerant networks (DTNs) that have been conducted within the Internet Research Task Force and have led to the specification of the DTN architecture (http://www.dtnrg.org/docs/specs). The DTN architecture consists of a network of independent internets each characterized by Internet-like connectivity within, but having only occasional communication opportunities among them. Such communication opportunities can be either scheduled over time or completely random. Independent internets located apart from each other form so-called *DTN regions* and a system of *DTN gateways* is in charge of providing interconnection among them. Hence, in DTNs points of possible disconnections are known and isolated at gateways. Each internet relies on its own protocol stack that best suits the particular infrastructure, communication means, and technologies available in the particular internet's region. The protocols used in the different DTN regions are likely to differ from each other. However, at the DTN nodes, a novel *overlay protocol* is added on top of the traditional transport layers to manage end-to-end data transfers among the DTN regions.

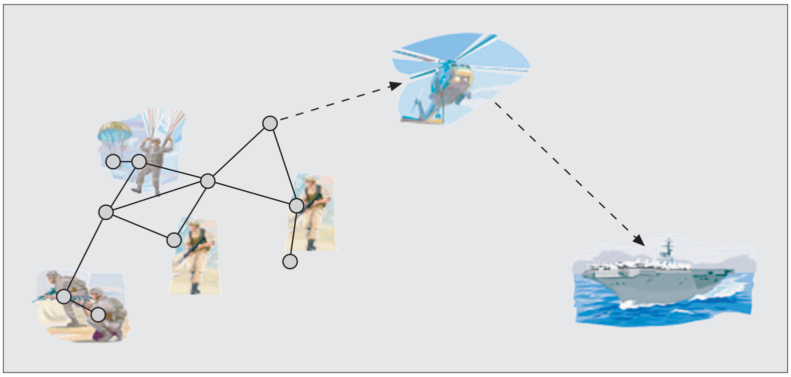
Figure 1 shows an example of DTN connecting the ad hoc network among the soldiers on a battlefield to the LAN on the nearest aircraft

*This work was partially funded by the Information Society Technologies program of the European Commission under the HAGGLE (027918) FET-SAC project.*

carrier. A helicopter is in charge of providing periodic connection between these two internets.[1]

Actually, in the literature there is no commonly agreed-upon terminology nor clear separation of concepts for opportunistic and delay-tolerant networks. The terms "opportunistic networks" and "delay-tolerant networks" are often used interchangeably. In our view, given the above DTN definition, opportunistic networks correspond to a more general concept and include DTNs. While DTNs assume the knowledge of Internet-like topologies, in which some links between gateways could be available just at certain (possibly unspecified) times, in opportunistic networks it is not mandatory to have a priori knowledge about the network topology. Routes in DTNs are typically computed via legacy-Internet techniques by taking into consideration the link unavailability just as another component of link cost. Instead, in opportunistic networks routes are computed at each hop while a packet is forwarded. So, *each node* receiving a message for an eventual destination exploits local knowledge to decide which is the best next hop, among its current neighbors, to reach the eventual packet destination. When no forwarding opportunity exists (e.g., no other nodes are in the transmission range, or the neighbors are evaluated not suitable for that communication), the node stores the message and waits for future contact opportunities with other devices to forward the information. Differently from DTNs, in opportunistic networks each single node acts as a gateway. This makes opportunistic networks a more flexible environment than DTNs, and calls for a more radical revision of legacy routing approaches designed for the Internet or for well-connected MANETs.

For example, as is shown in Fig. 2, the woman at the desktop opportunistically transfers, via a Wi-Fi link, a message for a friend to a bus crossing the area, "hoping" that the bus will carry the information closer to the destination. The bus moves through the traffic, then uses its Bluetooth radio to forward the message to the mobile phone of a woman who is disembarking at one of the bus stops. She walks through a nearby park to reach the university. Her cellular phone sends the message to a cyclist passing by. By proceeding in the same way some hops further, the message eventually arrives at the receiver. As is clearly shown in this example, a network connection between the two women never exists but, by opportunistically exploiting contacts among heterogeneous devices, the message is delivered hop-by-hop (hopefully) closer to the destination, and eventually to the destination itself.



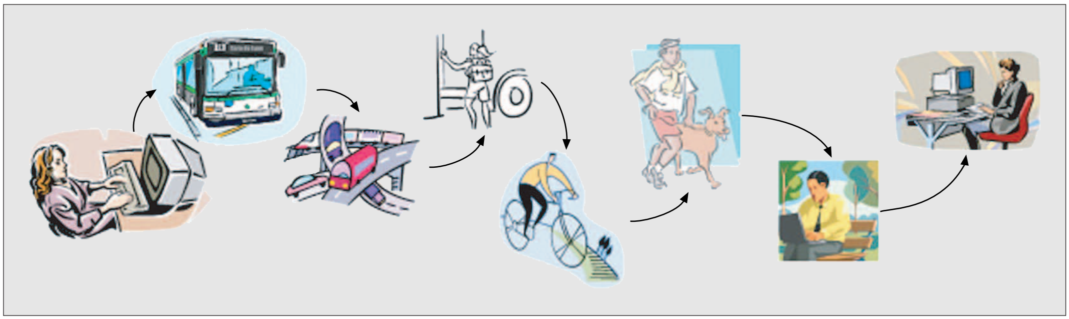
■ **Figure 1.** *An example of a delay-tolerant network.*

Besides allowing nodes that are not connected at the same time to the same network to communicate with each other, opportunistic networks are also a possible way to improve the capacity of multihop ad hoc networks beyond the well-known theoretical limit found by Gupta and Kumar [1]. Actually, Grossglauser and Tse have shown that an opportunistic network in which nodes act as carriers can achieve constant capacity, irrespective of the number of nodes in the network [2].

In this article we provide a survey on the key research approaches to opportunistic networking. We present several case studies in which opportunistic networks have been deployed for real. We discuss the main techniques used for routing and forwarding in opportunistic networks. Finally, we conclude the article by proposing possible future trends of this research area. Due to space limitations, we will be unable to provide very detailed descriptions and examples of the surveyed approaches. The interested reader is referred to [3] for a more thorough discussion.

## Realistic Case Studies

Research on opportunistic networking is devoting particular attention to realistic case studies. One of the basic components of realistic case



■ **Figure 2.** *Opportunistic networking.*

[1] *Since the motion of soldiers on a battlefield is well organized and they proceed in a group, trying not to go too far from each other, temporary disconnections that may arise inside this network are efficiently managed by transport and routing protocols designed for legacy MANETs.*

studies are the mobility models; thus, we present a project that devotes a lot of attention to collecting real mobility traces to be used in the design of efficient forwarding algorithms as well as to perform realistic simulations. Simulations based on real mobility traces are much more dependable for testing than simulations based on generic random mobility models.

Besides looking at realistic mobility models, researchers are also implementing a number of real-application scenarios in opportunistic networks. Such application scenarios are intrinsically opportunistic, in the sense that it is not possible nor advisable to provide a more structured network based on legacy routing approaches. This is the case, for example, with wildlife tracking applications (see ZebraNet [4]) aimed at monitoring wild species in unmanned scenarios. In these scenarios it is important to limit human intervention in order to respect the natural ecosystem, and thus it is necessary to utilize *light* networking. We present examples of such projects. Another example of opportunistic application consists in providing (Internet) connectivity to rural and developing areas where conventional networks do not exist. Deploying traditional (wired or wireless) networks to cover these areas is not cost-effective, whereas opportunistic networks are an affordable solution (e.g., DakNet [5] and SNC [6]). We present examples of such projects subsequently.

The examples referred to hereafter are probably the most well-known opportunistic applications deployed so far. Please refer to [3, section 2.2] for more details.

## Pocket Switched Networks in the Haggle Project

The Haggle Project (http://www.haggleproject.org) is a four-year project, started in January 2006 and funded by the European Commission in the framework of the FET-SAC initiative (http://cordis.europa.eu/ist/fet/comms-sy.htm). It targets solutions for communication in autonomic/opportunistic networks. In this framework, researchers are studying the properties of Pocket Switched Networks (PSNs), that is, opportunistic networks that can exploit any possible encountered device (e.g., cell phones and PDAs that users carry in their pockets) to forward messages.

The project is putting special emphasis on measuring and modeling pair-wise contacts between devices. Pair-wise contacts between users/devices can be characterized by the means of two parameters: *contact durations* and *intercontact time*s. The duration of a contact is the total time that a tagged couple of mobile nodes are within reach of each other, and thus have the possibility of communicating. An intercontact time is instead the time in between two contact opportunities between the same couple of tagged devices. While the contact duration directly influences the capacity of opportunistic networks because it limits the amount of data that can be transferred between nodes, the intercontact time affects the feasibility of opportunistic networks, and the delay associated with them.

To characterize contact durations and intercontact times occurring in real-world environments, different sets of traces have been collected and analyzed. Some traces have been inferred from the logs collected by the APs of some university campuses. Some others have been directly logged by Bluetooth devices carried by students and researchers in their university and laboratories and, more recently, by the participants to some international conferences.

The analysis of *all* the traces has led to an important result stating that both intercontact times and contact durations are characterized by *heavy-tailed distribution functions* approximately following power laws. This has interesting implications on the delay that each packet is expected to experience throughout the network. Specifically, "naïve" forwarding protocols have been analyzed based on these traces [7]. Such forwarding protocols do not use any information about previous contacts, or nodes' identities, or the context that users are operating in. Instead, they follow statically computed rules that limit the number of replicas of each message, or the number of hops that messages are allowed to travel through. It has been analytically proved that the expected delay of this class of forwarding algorithms is *infinite* under the heavy-tailed intercontact times distribution found in the traces. This is a very important result, as it calls for more evolved forwarding paradigms exploiting knowledge about the users' behavior.

## Wildlife Monitoring: ZebraNet and SWIM

Wildlife monitoring is an interesting application field for opportunistic networks. It focuses on tracking wild species to deeply investigate their behavior and understand the interactions and influences on each other, as well as their reaction to the ecosystem changes caused by human activities. Researchers use opportunistic networks as a reliable, cost-effective, and not intrusive means to monitor large populations roaming in vast areas. Systems for wildlife monitoring generally include special tags with sensing capacity to be carried by the animals under study, and one or more base stations to collect the data from the tags and send them to the destination processing centre. A network protocol is also comprised to percolate the data from the tags towards the base station(s). Base stations can be fixed or mobile, however, in both cases data collection from all the deployed tags is quite challenging. Therefore, it is generally advisable to exploit pair-wise contacts between the animals to let them exchange the information already collected. As a consequence, each animal eventually carries the information collected by its own together with the information collected by the animals it has encountered.

*Wildlife monitoring is an interesting application field for opportunistic networks. It focuses on tracking wild species to deeply investigate their behavior and understand the interactions and influences on each other, as well as their reaction to ecosystem changes.*

ZebraNet [4] is an interdisciplinary ongoing project at Princeton University and its deployment scenario is the vast savanna area of central Kenya under the direction of the Mpala Research Centre (http://www.princeton.edu/~mrm/zebranet.html). The animals to be tracked are zebras wearing special collars. The base station consists of a mobile vehicle for the researchers, which periodically moves around in the savanna and collects data from the zebras encountered. Two alternative protocols have been considered for data collection in ZebraNet. The first one is simple *flooding*, since each collar sends all its data to each encountered neighbor until the data eventually reach the base station. The second one, named *history-based protocol*, proposes that each node selects only one of its neighbors as relay for its data. The selected node is the one with the highest probability to eventually encounter the base station. Each node is thus assigned a hierarchy level (initially zero) that increases each time it encounters the base station, and conversely decreases after not having seen the base station for a certain amount of time. When sending data to a relay node, the neighbor to be selected is the one with the highest hierarchy level. Simulation results show that both forwarding protocols outperform the direct protocol, in which each collar has to directly communicate with the base station to upload data. Moreover, the history-based protocol outperforms flooding in terms of bandwidth and energy consumption. After an initial simulative study, the ZebraNet system has actually been implemented at the Mpala Research Centre, and is currently under test. First results from the real experimentation are already available and have recently been used to define the mobility model used to test some opportunistic forwarding techniques (see [3, section 3.1.2]).

In the Shared Wireless Infostation Model (SWIM), whales are the wild species to be monitored [8]. Special tags applied to the whales perform periodic data monitoring. Data is replicated and diffused at each pair-wise contact between whales (similarly to what happens in the flooding protocol of ZebraNet) and finally arrives to special *SWIM stations* that can be fixed (on buoys) or mobile (on seabirds). Hence, both whale-to-whale and whale-to-base-station communications are allowed. From the SWIM stations, data are eventually forwarded onshore for final processing and utilization. No experimental results are actually available to demonstrate the efficiency of the SWIM system on real whales. However, simulation results are quite realistic since the simulation parameters about both the environment and the whales' mobility model have been set according to the observations and studies conducted by biologists on whales' real habits. The simulation results show a not negligible delay for arrival of data at the processing base stations. However, improvements are possible by increasing both the number of whales involved and the number of SWIM stations. Finally, mobile SWIM stations have shown better performance than fixed SWIM stations.

### Opportunistic Networks for Developing Areas

Opportunistic networks can provide intermittent Internet connectivity to rural and developing areas where they typically represent the only affordable way to help bridge the digital divide. One such example is the DakNet Project [5] , which is aimed at realizing a very low-cost asynchronous ICT infrastructure so as to provide connectivity to rural villages in India, where it is not cost-effective to deploy standard Internet access. According to the DakNet project, kiosks are built up in villages and equipped with digital storage and short-range wireless communications. Periodically, mobile access points (MAPs) mounted on buses, motorcycles, or even bicycles pass by the village kiosks and exchange data with them wirelessly. MAPs can upload any sort of request or data stored at the kiosks, and download them to the Internet when passing by an access point (AP) in a nearby town. Similarly, MAPs may download, from the Internet, the requested information and bring it to villages. DakNet has the potential to support Internet/Intranet messaging (e.g., email, audio/video messaging, and mobile e-commerce), distribution of information (e.g., public health announcements, community bulletin boards, news, and music), and collection of information (e.g., environmental sensor information, voting, health records, and census).

*DakNet has the potential to support Internet/Intranet messaging (email, audio/video messaging), distribution of information (public health announcements, community bulletin boards, news, and music), and collection of information (e.g., environmental sensor information, voting, health records, and census).*

Another interesting opportunistic application scenario has been investigated in the framework of the Saami Network Connectivity (SNC) project [6], which aims to provide network connectivity to the nomadic Saami population of the reindeer herders. Saami herders live across the Sápmi region (also known as Lapland) in the northest part of Sweden, Norway, and Finland and move from their villages through the year following the migration of reindeers. Providing network connectivity to the Saami population is a means to protect and defend their habits, culture, and traditions while also supporting their integration into the modern society of their countries. With network connectivity Saami are allowed to continue to live according to their traditions and, at the same time, have much economic sustain through distance work and net-based business. Network-based services can also allow Saami children to receive their education without the need to leave their parents to attend boarding schools. Network connectivity can also give Saami more visibility, and let them have more influence in the political and economical affairs of their country. In its initial stage, the SNC project has only focused on providing email, file transfer, and cached web services to the Saami people. Reindeer herd telemetry is also going to be provided to support the herding activity itself. It should finally be noted that the Saami Network Connectivity (SNC) project focuses on a pure DTN architecture.

## Opportunistic Routing/Forwarding Techniques

In all the above case studies, routing is the most compelling challenge. The design of efficient routing strategies for opportunistic networks is generally a complicated task due to the absence of knowledge about the topological evolution of the network. Routing performance improves when more knowledge about the expected topology of the network can be exploited [9]. Unfortunately, this kind of knowledge is not easily available, and a trade-off must be met between performance and knowledge requirement. Figure 3 shows a possible taxonomy of routing/forwarding[2] algorithms in opportunistic networks. At the bottom of Fig. 3. we list the examples of

*According to the Epidemic Routing protocol, messages diffuse in the network similarly to diseases or viruses, i.e., by means of pair-wise contacts between individuals/nodes. A node is infected by a message when it either generates that message or, alternatively, receives it from another node for forwarding.*

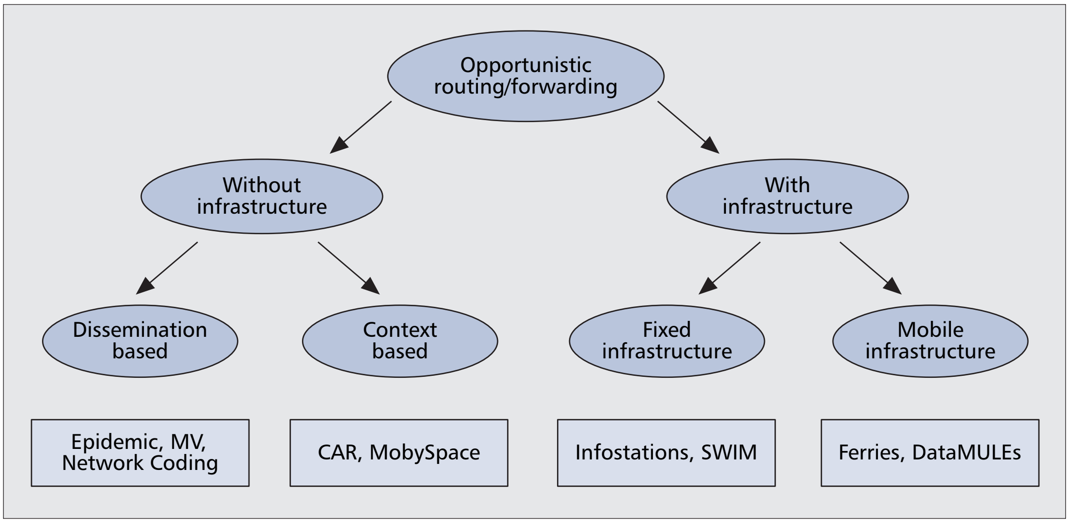


**Figure 3.** *Taxonomy of routing/forwarding techniques for opportunistic networks.*

each class that are mentioned in this article. More details can be found in [3]. Another analysis of routing techniques can also be found in [10].

A first classification is between algorithms designed for completely flat ad hoc networks (*without infrastructure*), and algorithms in which the ad hoc networks exploit some form of infrastructure to opportunistically forward messages (*with infrastructure*). In the former case, approaches can be further divided into *dissemination-based* and *context-based* algorithms. Dissemination-based algorithms are essentially forms of controlled flooding, and differentiate themselves by the policy used to limit flooding. Context-based approaches usually do not adopt flooding schemes, but use knowledge of the context that nodes are operating in to identify the best next hop at each forwarding step. Algorithms that exploit some form of infrastructure can be divided (depending on the type of infrastructure they rely on) into *fixed infrastructure* and *mobile infrastructure*. In both cases the infrastructure is composed by special nodes that are more powerful with respect to the other nodes commonly present in the ad hoc network. They have high storage capacity and hence can collect messages from many nodes passing by, even for a long time. They also have high energy.

Nodes of a fixed infrastructure are located at specific geographical points, whereas nodes of a mobile infrastructure move around in the network following either predetermined known paths or completely random paths.

## Routing Without Infrastructure

***Dissemination-Based Routing*** — Routing techniques based on data dissemination perform delivery of a message to a destination by simply diffusing it all over the network. The heuristic behind this policy is that, since there is no knowledge of a possible path towards the destination nor of an appropriate next-hop node, a message should be sent everywhere. It will eventually reach the destination by passing node by node. Dissemination-based techniques obviously work well in highly mobile networks where contact opportunities, which are needed for data diffusion, are very common. They tend to limit the messages delay, but they are also very resource hungry. Due to the considerable number of transmissions involved, dissemination-based techniques suffer from high contention and may potentially lead to network congestion. To increase the network capacity, the spreading radius of a message is typically limited by imposing a maximum number of relay hops to each message, or even by limiting the total number of message copies present in the network at the same time. When no relaying is further allowed, a node can only send directly to destination when/in case met.

According to the *Epidemic Routing* protocol [11], messages diffuse in the network similarly to diseases or viruses (i.e., by means of pair-wise contacts between individuals/nodes). A node is *infected* by a message when it either generates that message or, alternatively, receives it from another node for forwarding. The infected node stores the message in a local buffer. A node is *susceptible* to infection when it has not yet received the message.[3] A susceptible node becomes infected in case it comes into contact with an infected node (i.e., a node that stores that message) and receives the message from it. An infected node becomes *recovered* (healed from the disease) once having delivered the message to the destination node and, as a result, it also becomes *immune* to the same disease and does not provide relaying to the same message any more. The dissemination process is somehow bounded because each message when generated is assigned a *hop count limit* giving the maximum number of hops that that message is allowed to traverse till the destination. When the

[2] *In opportunistic networks, the concepts of routing and forwarding are mixed together, since routes are actually built while messages are forwarded. In this article we use the terms routing and forwarding interchangeably.*

[3] *The message itself represents the infection/virus.*

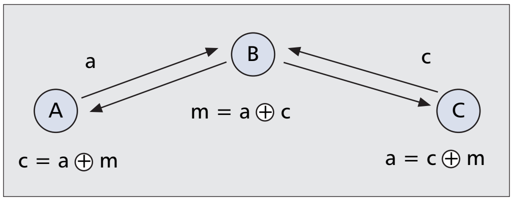


**Figure 4.** *Example of network-coding efficiency.*

hop count limit is one, the message can only be sent directly to the destination node.

The *MV routing* protocol [12] is a further step beyond epidemic routing. Messages are exchanged during pair-wise contacts as in epidemic routing. However, the MV protocol introduces a more sophisticated method to select the messages to forward to an encountered node. Basically, the choice depends on the probability of encountered nodes to successfully deliver messages to their eventual destinations. The delivery probability relies on recent-past observations of both the *meetings* between nodes and the *visits* of nodes to geographical locations. The name *MV* protocol itself comes just from *Meetings* and *Visits*. A similar approach is followed in the PROPHET routing protocol [13].

Dissemination-based algorithms also include *network-coding-based routing* [14], which takes an original approach to limit message flooding. Just to give a classical example, let A, B, and C be the only three nodes of a small network (Fig. 4). Let node A generate the information "*a*" and node C generate the information "*c*." Then suppose the information produced needs to be known at all the nodes. Hence, nodes A and C send their information to node B. Then node B, rather than sending two different packets for "*a*" and "*c*," respectively, broadcasts a single packet containing "*a*" xor "*c*." Once "*a*" xor "*c*" is received, both nodes A and C can finally infer the missing information (i.e., node A can infer "*c*" and node C can infer "*a*"). Network coding-based routing outperforms flooding, as it is able to deliver the same information with a fewer number of messages injected into the network.[4] For a more general discussion on network coding, readers can refer to [15].

***Context-based Routing*** — Most of the dissemination-based techniques limit messages' flooding by exploiting knowledge about direct contacts with destination nodes. Context-based routing exploits more information about the context in which nodes are operating so as to identify suitable next hops towards the eventual destinations (e.g., the home address of a user is a valuable piece of context information to decide the next hop). The usefulness of a host as the next hop for a message is hereafter referred to as the *utility* of that host. Context-based routing techniques are generally able to significantly reduce messages' duplication with respect to dissemination-based techniques. On the other hand, context-based techniques tend to increase the delay that each message experiences during delivery. This is due to possible errors and inaccuracies in selecting the best relays. Moreover, utility-based techniques have higher computational costs than dissemination-based techniques. Nodes need to maintain a state in order to keep track of the utility values associated with all the other nodes in the network (i.e., all the possible destination nodes), and hence need storage capacity for both state and messages. Finally, the cost to hold and update the state at each node should also be considered in the overall protocol overhead.

*Context-based routing techniques are generally able to significantly reduce the messages' duplication with respect to dissemination-based techniques. On the other hand, context-based techniques tend to increase the delay that each message experiences during delivery.*

In the Context-Aware Routing (CAR) protocol [16], each node in the network is in charge of producing its own delivery probabilities towards each known destination host. Delivery probabilities are exchanged periodically so that, eventually, each node can compute the best carrier for each destination node. The best carriers are computed based on the nodes' context. The context attributes needed to elect the best carrier are, for example, the residual battery level, the rate of change of connectivity, the probability of being within reach of the destination, and the degree of mobility. When the best carrier receives a message for forwarding, it stores it in a local buffer and eventually forwards it to the destination node when met or, alternatively, to another node with a higher delivery probability. CAR provides a framework for computing next hops in opportunistic networks based on the *multiattribute utility theory* applied to generic context attributes. The simulation results show that CAR is more scalable than epidemic routing, as the protocol overhead is approximately constant regardless of the node buffer size.

In *MobySpace Routing* [17], the nodes' mobility pattern is the context information used for routing. The protocol builds up a high dimensional Euclidean space, named *MobySpace*, where each axis represents a possible contact between a couple of nodes, and the distance along an axis measures the probability of that contact to occur. Two nodes that have similar sets of contacts, and that experience those contacts with similar frequencies, are close in the MobySpace. The best forwarding node for a message is the node that is as close as possible to the destination node in this space. Obviously, in the *virtual contact space* just described, the knowledge of all the axes of the space also requires the knowledge of all the nodes that are circulating in the space. This full knowledge, however, might not be required for successful routing (see [17] for more details).

### ROUTING WITH INFRASTRUCTURE

***Routing Based on Fixed Infrastructure*** — In infrastructure-based routing, a source node wishing to deliver a message generally keeps it until it comes within reach of a base station belonging to the infrastructure, then forwards the message to it. Base stations are generally gateways towards less challenged networks (e.g., they can provide Internet access or be connected to a

[4] *So far, network coding-based routing solutions have been applied only to infrastructureless opportunistic networks. This is the reason why we have included this solution in the infrastructureless section. However, it can be envisioned that in the near future network coding will also be applied to infrastructured opportunistic networks.*

In carrier-based routing, nodes of the infrastructure are mobile data collectors. They move around in the network area, following either pre-determined or arbitrary routes, and gather messages from the nodes they pass by. These special nodes are referred to as carriers, supports, forwarders, MULEs, or even ferries.

LAN). Hence, the goal of an opportunistic routing algorithm is to deliver messages to the gateways, which are supposed to be able to find the eventual destination more easily. Two variations of the protocol are possible. The first one works exactly as described above, and only node-to-base-station communications are allowed. As a result, messages experience fairly high delays. The classic example of this approach is the *Infostation* model [18].

A second version of the protocol allows both node-to-base-station and node-to-node communications. This means that a node wishing to send a message to a destination node delivers the message to the base station directly, if within communication range; otherwise, it delivers the message *opportunistically* to a near node that will eventually forward it to the base station when encountered (routing schemes presented earlier can be used in this phase). Such a protocol has actually been proposed in the Shared Wireless Infostation Model (SWIM) [8].

As results from the above examples, historically, fixed base stations play a passive role in the opportunistic forwarding strategy because simply act as information sinks (e.g., Infostations [18]). However, many benefits can be envisioned by running an opportunistic routing algorithm also at base stations. Base stations, for example, can simply collect the messages sent by the visiting nodes and then wait for the destination nodes to be within reach to forward the stored messages to them. Base stations of a mobile infrastructure (described in the next section) typically play such an active role.

***Routing Based on Mobile Infrastructure (Carrier-Based Routing)*** — In carrier-based routing, nodes of the infrastructure are mobile data collectors. They move around in the network area, following either predetermined or arbitrary routes, and gather messages from the nodes they pass by. These special nodes are referred to as *carriers*, *supports*, *forwarders*, *MULEs*, or even *ferries*. They can be the only entities responsible for messages delivery, when only node-to-carrier communications are allowed, or they can simply help increasing connectivity in sparse networks and guaranteeing that also isolated nodes can be reached. In the latter case, delivery of messages is accomplished both by carriers and ordinary nodes, and both node-to-node and node-to-carrier communication types are allowed.

The *data-MULE system* [19] focuses on data retrieval from sparse wireless sensor networks. It consists of a three-tier architecture:

- The lower level is occupied by the sensor nodes that periodically perform data sampling from the surrounding environment.
- The middle level consists of mobile agents, named MULEs, which move around in the area covered by sensors to gather their data.
- The upper level consists of a set of wired APs and data repositories which receive information from the MULEs. They are connected to a central data warehouse where the data received is stored and processed.

In the *message-ferrying approach* [20], extra mobile nodes are opportunistically exploited to offer a message relaying service. These nodes are named *message ferries* and move around in the network where they collect messages from source nodes. Message collection may happen in two ways:

- *Node-initiated message ferrying*: the ferry node moves around following a predefined and known path. Each node in the network has knowledge of the paths followed by active ferries, and moves to meet ferries when it has data to deliver.
- *Ferry-initiated message ferrying*: the ferry node, again, moves around following a predefined, default path. Any source node wishing to deliver messages sends a ServiceRequest to the ferry (via a long-range radio signal), which also includes its current position. After having received the request from the source node, the ferry changes its trajectory to meet up with the source node.

## Concluding Remarks and Future Trends

At the top level of our taxonomy, we have divided routing techniques for opportunistic networks between algorithms that do exploit some form of infrastructure and algorithms that do not. Actually, the vast majority of studies in the literature follow this distinction. We believe that a very interesting area still to be investigated is how to design multitier opportunistic networks. In this sense, the data MULEs and message-ferrying architectures are the most promising approaches. They are susceptible to various improvements but have the potential to be utilized as bases for more general and global architectures. For example, in the data MULEs approach, lower-level nodes exploit the higher level and more capable mobile devices (the MULEs), which, in turn, exploit a further infrastructure level, (i.e., the APs). However, routing algorithms exploited at each layer are pretty trivial or do not exist at all. Instead, we can envision a multitier *fully opportunistic* network. In such a network, each level of the infrastructure is an opportunistic network in which nodes may exploit routing algorithms to communicate among themselves, and may rely on the upper levels of the infrastructure to reach nodes that are too far away. For example, a low level can consist of devices such as PDAs, or smart phones. An opportunistic routing algorithm can make those devices able to communicate with each other. To reach nodes too far away for such routing to be effective, a higher level consisting, for example, of a "city-bus network" might be used. In this scenario, buses will act similarly to MULEs. However, multihopping will be used also at this level of the network via a (possibly different) opportunistic routing algorithm. This will enable connection among different clouds of the lower-tier devices just by relying on the city-bus network. Clearly, the city-bus network might exploit further infrastructure levels such as a mesh network formed by APs, or even access the Internet through standard Wi-Fi APs.

Designing such an opportunistic multitier network is one of the most interesting challenges that can currently be envisaged. Once designed and developed, such a network might actually represent a fundamental building block for the next-generation Internet.

Designing such an opportunistic multi-tier network is one of the most interesting challenges that can currently be envisaged. Once designed and developed, such a network might actually represent a fundamental building block for the Next-Generation Internet.

## REFERENCES

[1] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," *IEEE Trans. Info. Theory*, vol. 46, Mar. 2000, pp. 388–404.

[2] M. Grossglauser and D. N. C. Tse, "Mobility Increases the Capacity of Ad-Hoc Wireless Networks," *IEEE/ACM Trans. Net.*, vol. 10, no. 4, Aug. 2002.

[3] L. Pelusi, A. Passarella, and M. Conti, "Beyond MANETs: Dissertation on Opportunistic Networking," IIT-CNR Tech. Rep., May 2006, online available at http://bruno1.iit.cnr.it/~bruno/techreport.html

[4] P. Juang *et al.*, "Energy-Efficient Computing for Wildlife Tracking: Design Trade-Offs and Early Experiences with ZebraNet," *ACM SIGPLAN Notices*, vol. 37, 2002, pp. 96–107.

[5] A. Pentland, R. Fletcher, and A. Hasson, "DakNet: Rethinking Connectivity in Developing Nations," IEEE Computer, vol. 37, no. 1, Jan. 2004, pp. 78–83.

[6] A. Doria, M. Uden, and D. P. Pandey, "Providing Connectivity to the Saami Nomadic Community," *Proc. 2nd Int'l. Conf. Open Collaborative Design for Sustainable Innovation (dyd 02)*, Bangalore, India, Dec. 2002.

[7] A. Chaintreau *et al.*, "Impact of Human Mobility on the Design of Opportunistic Forwarding Algorithms," *Proc. 25th IEEE INFOCOM 2006*, Barcelona, Spain, Apr. 23–29, 2006.

[8] T. Small and Z. J. Haas, "The Shared Wireless Infostation Model — A New Ad Hoc Networking Paradigm (or Where There is a Whale, there is a Way)," *Proc. 4th ACM Int'l. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc 2003)*, Annapolis, MD, June 1–3, 2003.

[9] J. Sushant, K. Fall, and R. Patra, "Routing in a Delay Tolerant Network," *Proc. SIGCOMM '04*, Aug. 2004.

[10] Z. Zhang, "Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks: Overview and Challenges," *IEEE Commun. Surveys*, vol. 8, no.1, 1st Quarter 2006.

[11] A. Vahdat and D. Becker, "Epidemic Routing for Partially Connected Ad Hoc Networks," Tech. Rep. CS-2000-06, Department of Computer Science, Duke University, Durham, NC, 2000.

[12] B. Burns, O. Brock, and B. N. Levine, "MV Routing and Capacity Building in Disruption Tolerant Networks," *Proc. IEEE INFOCOM 2005*, Miami, FL, Mar. 2005.

[13] A. Lindgren, A. Doria, and O. Schelèn, "Probabilistic Routing in Intermittently Connected Networks," *Mobile Computing and Commun. Review*, vol. 7, no. 3, July, 2003.

[14] J. Widmer and J.-Y. Le Boudec, "Network Coding for Efficient Communication in Extreme Networks," *Proc. ACM SIGCOMM 2005 Wksp. Delay Tolerant Networks*, Philadelphia, PA, Aug. 22–26, 2005.

[15] L. Pelusi, A. Passarella, and M. Conti, "Encoding over the Network: Techniques and Challenges," IIT-CNR Tech. Rep., June 2006, online available at http://bruno1.iit.cnr.it/~bruno/techreport.html

[16] M. Musolesi, S. Hailes, and C. Mascolo, "Adaptive Routing for Intermittently Connected Mobile Ad Hoc Networks," *Proc. 6th IEEE Int'l. Symp. World of Wireless, Mobile and Multimedia Networks (WoWMoM 2005)*, Taormina-Giardini Naxos, Italy, June 13–16, 2005.

[17] J. Leguay, T. Friedman, and V. Conan, "Evaluating Mobility Pattern Space Routing for DTNs," *Proc. IEEE Infocom 2006*, Barcelona, Spain, Apr. 2006.

[18] D. Goodman *et al.*, "INFOSTATIONS: A New System Model for Data and Messaging Services," *IEEE VTC'97*, vol. 2, May 1997, pp. 969–73.

[19] S. Jain et al., "Exploiting Mobility for Energy Efficient Data Collection in Wireless Sensor Networks," *ACM/Kluwer Mobile Networks and Applications (MONET)*, vol. 11, no. 3, June 2006, pp. 327–39.

[20] W. Zhao, M. Ammar, and E. Zegura, "A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks," *Proc. 5th ACM Int'l. Symp. Mobile Ad Hoc Networking and Computing (Mobihoc)*, ACM Press, May, 2004, pp. 187–98.

## BIOGRAPHIES

LUCIANA PELUSI (Luciana.Pelusi@iit.cnr.it) received a Laurea degree in computer engineering from the University of Pisa, Italy, in 2003. She is a Ph.D. student at the Institute for Informatics and Telematics of the Italian National Research Council (IIT-CNR) in Pisa. Her research interests are in the area of pervasive systems and include multimedia networking, energy-efficient protocols for ad hoc and sensor networks, and opportunistic networking.

ANDREA PASSARELLA (Andrea.Passarella@iit.cnr.it) is with IIT-CNR, Italy. Previously, he was a researcher at the Computer Laboratory, Cambridge, United Kingdom. He holds a Ph.D. degree in computer engineering from Pisa University, Italy. He is working on opportunistic, ad hoc, mesh and sensor networks, specifically on p2p systems, multicasting, transport protocols, and energy management. He was TPC Member of IEEE PerCom and WoWMoM, and TPC Vice-Chair for ACM REALMAN, and IEEE MDC. He is an Associate Technical Editor for *IEEE Communications Magazine*.

MARCO CONTI (Marco.Conti@iit.cnr.it) is a research director at IIT-CNR. He published more than 180 research papers and two books: *Metropolitan Area Networks* (Springer, 1997) and *Mobile Ad Hoc Networking* (IEEE-Wiley, 2004). He served as TPC chair of several conferences including, IFIP-TC6 Networking 2002, IEEE WoWMoM 2005 and PerCom 2006, and ACM MobiHoc 2006. He is Associate Editor of *Pervasive and Mobile Computing* (Elsevier), and Area Editor for *IEEE Transactions on Mobile Computing* and *Ad Hoc Networks*.