Opportunistic Routing for Disruption Tolerant Networks

Marcello Caleffi*, Luigi Paura*†

*Dipartimento di Ingegneria Elettronica e delle Telecomunicazioni (DIET)
Università degli Studi di Napoli Federico II
Napoli, ITALY
†Laboratorio Nazionale di Comunicazioni Multimediali (CNIT)
Napoli, ITALY
Email: {name.surname}@unina.it

***Abstract*—*Opportunistic networks* represent one of the most interesting evolution of MANET paradigm. Generally speaking, opportunistic networks enable user communication in environments where disconnection and reconnection are likely and link performance is extremely non stationary. In this paper, we propose a routing protocol, based on the *opportunistic routing* paradigm, able to assure connectivity in ad hoc networks characterized by high link dynamic, namely in Disruption Tolerant Networks (DTNs). By means of numerical analysis, a comparison with both traditional and collaborative routing protocols has been state showing that our proposal is able to provide end-to-end connectivity in DTNs, taking advantage by the link dynamic.**

I. Introduction

Since *opportunistic networking* paradigm is a very emerging concept, there is no clear definition commonly agreed in the research community. Nevertheless, the strategies adopted to provide end-to-end connectivity in presence of interference-prone wireless communications and transient network topologies exhibit a common key feature which allows one to distinguish opportunistic networking from traditional ad hoc networking [1].

Usually, ad hoc networking tries to *fortify* the environment [2] so that it behave like a wired network. More in detail, the wireless channel is *reinforced* by means of Automatic Repeat Request (ARQ) or Forward Error Control (FEC) data-link techniques to counteract the time-variant impairment of the wireless propagation, while the transient network topology is *fortified* resorting to multi-path and/or flooding routing techniques.

These approaches are based on two hypotheses. The former is that the network topology is quite dense to assure the presence of a persistent path between each pair of nodes and the latter assures that the wireless propagation conditions are enough stationary to allow a persistent communication among neighbor nodes.

In the last years these assumptions have been relaxed giving rise to the opportunistic networking paradigm, which, rather than counteracts, tries to take advantages by the time-variant nature of the environment to provide end-to-end connectivity in scenarios where traditional networking fails.

Opportunistic networking protocols can be devided in two main classes. The *collaborative routing* protocols exploit the time-variant nature of the network topology to provide connectivity for sparse topologies usually by resorting to a so-called *store-carry-forward* paradigm [3], [4]. Delay Tolerant Networks are a typical application domain for collaborative routing, since they aim to provide connectivity in rural and developing areas where the costs associated with a traditional dense network are no affordable.

The *opportunistic routing* class exploits both the temporal diversity and the broadcast nature of the wireless propagation, usually by resorting to broadcast communications instead of traditional unicast ones, to provide connectivity in presence of hostile wireless propagation conditions. Disruption Tolerant Networks are a typical application domain for opportunistic routing, since they try to provide connectivity to networks characterized by strong shadowing effects as well as intentional interference [5]. In the work [6] the authors suggest to broadcast the packets and to select the next forwarder at the receiver side to take advantage by all the opportunities provided by the wireless propagation. In other words, they exploit spatial diversity, which can assure more resilience to lossy links.

Since such a routing, referred to as *opportunistic routing*, allows several nodes to receive the same packet, the authors single out a sub-set of neighbor nodes, namely a candidate set, allowed to forward the packet to limit the network flooding.

Such a proposal is however unable to exploit all the opportunities offered by the wireless propagation since the candidate set is chosen at the sender side. In fact, if a node, which is very close to the destination, successfully receives the packet, it can not become the next forwarder unless it has been included in the candidate set by the forwarding node. Moreover, to single out the nosed belonging to the candidate set it assumes that a link-quality estimation is available.

To overcome the above drawbacks, we propose a routing

This work is partially supported by the Italian National Project “Wireless multiplatfOrm mimo active access netwoRks for QoS-demanding muLtimedia Delivery” (WORLD) under grant number 2007R989S, and by the Regional project “REmote e COntinuous Monitoring” (RECOM).

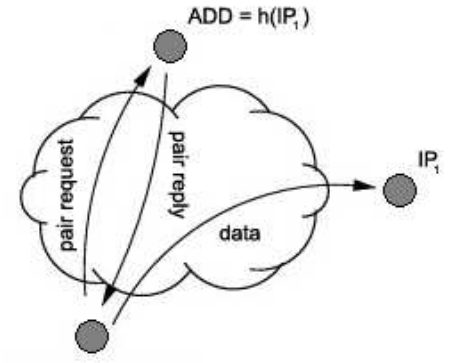

Fig. 1: Location-dependent address discovery

protocol in the context of *Disruption Tolerant Networks* (DTNs), namely for networks characterized by intermittent or disruption-prone connectivity [7]. The proposed protocol extends a location-aware addressing schema, first proposed by [8], to match it with opportunistic routing, building so an distribute procedure for candidate selection able to exploit all the opportunities offered by the wireless propagation.
To evaluate the effectiveness of such a proposal, we have carried out numerical simulations to state a performance comparison with two representative routing protocols in presence of hostile propagation conditions, i.e. in presence of shadow fading, across a wide range of environmental conditions.

II. System architecture

In this section we describe the proposed protocol, namely the Opportunistic DHT-based Routing (ODR) protocol, providing both an operational overview (Sec. II-A) and a detailed functional description (Sec. II-B and Sec. II-C).

A. Overview

As mentioned before, to accomplish the packet routing each forwarder locally broadcasts the packet to all its neighbors, together with an estimate of its distance from the destination. By means of such a distance, the receiving nodes are able to understand if they are potential forwarders, that is if they belong to the candidate set, by comparing their distances with the one stored in the packet header. Clearly, the candidate set is composed by all the neighbors closer than the forwarder to the destination as well as the forwarder.
Each candidate node delays the packet forwarding by an amount of time which depends on its distance estimate from the destination: the more a node is close to the destination, the more the delay is short. A subsequent reception of the same packet from a neighbor closer to the destination allows the node to discard that packet, while a subsequent reception from a farther neighbor gives rise to an acknowledge transmission. This iterative procedure allows that, at each step, the packet has been forwarded by the candidate node closest to the destination.

To limit the overhead due to distance estimation, we exploit a location-aware addressing schema which allows us to group nodes basing on their addresses. This approach lets nodes to estimate their distances from sets of nodes sharing the same address prefix, instead of individually tracking each node.
However, such a procedure requires the availability of a distribute procedure to allow nodes to retrieve the destination addresses before starting a communication. We accomplish this task by resorting to a Distributed Hash Table (DHT) system which exploits a globally known hash function $h(\cdot)$, defined on the IP address space and with values in the location-aware address space.
Every node is part of the DHT system, storing a subset of *pairs* <IP address, location-dependent address> in accordance with the hash function. More in detail, the pair $<ip_1, add_1>$ is stored by the node whose location-dependent address is equal to $h(ip_1)$, namely the *rendezvous-node*. Thus, to find out a location-dependent address a node simply sends a pair request to the rendezvous-node, as shown in Fig. 1. After the reception of the pair reply, the node is able to establish the communication. Clearly, the pair request and reply messages resort to the same data routing procedure illustrated above.

B. Distance estimation

Opportunistic DHT-based Routing (ODR) assigns the location-dependent addresses, namely strings of l bits, to nodes by means of a distribute procedure which resorts to locally broadcasted hello packets. The address allocation procedure guarantees that nodes sharing a common address prefix are close in the physical topology, allowing so us to easily group nodes.
We represent the address space as a *complete binary tree* of $l + 1$ levels, that is as a binary tree in which every vertex has zero or two children and all leaves are at the same level (Fig. 2-a). In the tree structure, each leaf is associated with an address, and a inner vertex of level k, namely a *level-k subtree*, represents a set of leaves (that is a set of peer identifiers) sharing a prefix of $l - k$ bits. For example, with reference to Fig. 2-a, the vertex with the label *01X* is a level-1 subtree and represents the leaves *010* and *011*.
Let us define as *level-k sibling* of a leaf as the level-k subtree which shares the same parent with the level-k subtree the leaf belongs to. Referring to the previous example, the vertex with the label *1XX* is the level-2 sibling of the address *000*.
By means of the sibling concept, nodes can reduce the overhead due to distance state maintaining by a logarithm factor. Each node store a limited-size distance table composed by l entries, one for each sibling, and the k-th section contains the estimated distance with the *nearest* node whose location-dependent address belongs to the level-k sibling.
Clearly, this approach arises a new problem, since the hierarchy related to the sibling concept gives rise to an estimate inaccuracy. In fact, the k-th section stores the estimated distance towards the nearest node whose address belongs to the level-k sibling, i.e. the section stores a lower bound on the distance. We propose a solution to this issue in Sec. II-C.

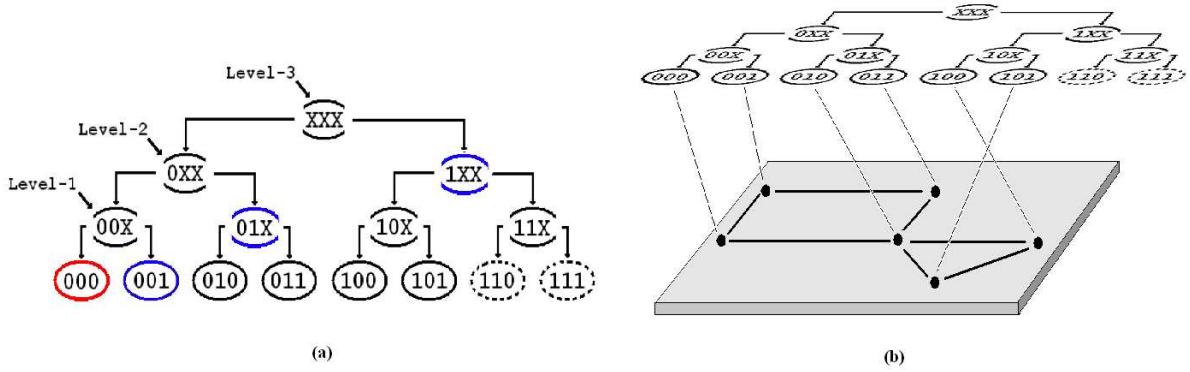

Fig. 2: Relationship between the address space structure and the physical topology

In this paper, we resort to a distance metric, proposed in [9], based on the link-quality. This metric aims to estimate the expected number of packet transmissions (including the retransmissions) required to successfully deliver a packet to the ultimate destination. Clearly, the Opportunistic DHT-based Routing protocol can be easily extended to different metrics.
To estimate the distances, we resort to hello packets and to a moving average filter. Each node locally broadcasts the hellos with an average period τ (one second in our implementation) jittered up to $\pm\tau/k$ for each period, thus we can model the hello reception events as binary independent random variable $x(n) \in \{0, 1\}$. At the time n, the node j evaluates the link quality $q_{i\to j}(n)$ for the packets received by the neighbor i resorting to MA filtering, according to:

$$q_{i\to j}(n) = \sum_{m=0}^{M-1} b(m) x_{i\to j}(n-m) \tag{1}$$

where $b(m)$ are the filter weights.
Since node j broadcasts its estimated link quality $q(i \to j)$ with the hello packets, the neighbor i can retrieve the link quality $q_{i\to j}(n)$ and thus compute the bi-directional link quality $q_{i,j}(n)$ as

$$q_{i,j}(n) = q_{i\to j}(n) \times q_{j\to i}(n) \tag{2}$$

The link quality is thus used to estimate the distance between the nodes *s* and *d* in terms of expected transmission count (ETX) as:

$$d_{s,d}(n) = \sum_{l(i,j)\in R(s,d)} \frac{1}{q_{i,j}(n)} \tag{3}$$

where the $l(i, j)$ are the links belonging to the route $R(s, d)$.

C. Packet forwarding

The packet forwarding process consists of three steps: the candidate selection, the candidate election and the candidate acknowledgment. To accomplish these steps, each node resorts to two queues. The former, namely the *packet queue*, stores the packets waiting to be forwarded, i.e. the packets for which the node is a candidate forwarder. The latter, namely the *ack queue*, stores for acknowledgment purposes the packets that have not anymore to be forwarded.
The candidate selection ensures that, at each step, only nodes closer than the forwarder to the destination are allowed to re-forward the packet. More in detail, when a node forwards a packet, it stores in the packet header its location-dependent address along with its estimate distance from the destination, and then it locally broadcasts the packet.
A receiving node checks if its overlay distance to the destination, i.e. the length of the address prefix shared by the node address and the destination one, is shorter than the forwarding overlay distance and then checks if its path quality is better than the forwarder one. If both the checks fail, the node does not belong to the candidate set and it stores the packet in its ack queue. Differently, it stores the packet in its packet queue together with a delay time evaluated according to the following relation:

$$delay = \tau * \frac{q_p(r,d)}{q_p(f,d)} * \left[\frac{1}{o_d(r,d) - o_d(f,d) + 1}\right] \tag{4}$$

where τ is the maximum delay time (2 seconds in our implementation), *f* is the forwarding node, *r* is the receiving

destination	path quality	route log
011	1.60	001
00X	3.80	010
1XX	1.25	010

Fig. 3: Node 010 routing table

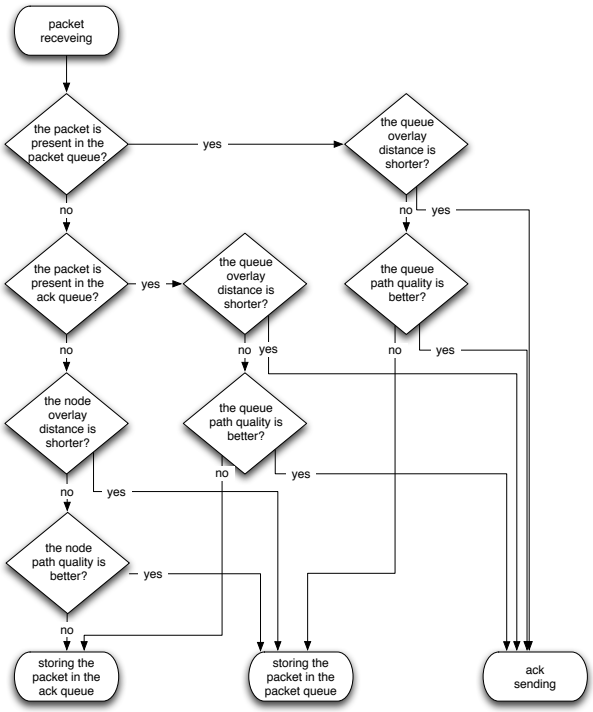

Fig. 4: Packet forwarding process

node, d is the destination one, q_p is the estimated quality and o_d is the overlay distance. By means of this heuristic approach for the delay estimation, we account for the estimate inaccuracy mentioned in Sec. II-B, since the ratio between the estimated qualities ratio is weighted by a factor, i.e. the term in the square brackets in (4) depending on the overlay distances, which measures the size of the clusters of nodes, namely the siblings, to which the qualities refer to.

Thus, the delay times allow nodes to implement a distributed candidate election procedure, by exploiting a TDMA-based scheduling: since the closest node stores in the packet header its distance estimate from the destination and since it is the first that forwards the packet, the other candidates can listen such a packet transmission and therefore give up to the packet forwarding.

Such a strategy does not require explicit acknowledgment for each packet forwarding, although it is not tolerant to to the

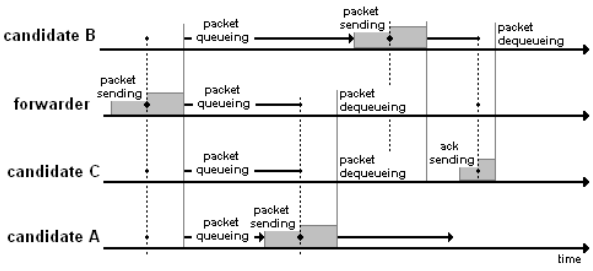

Fig. 5: Typical ODR packet forwarding

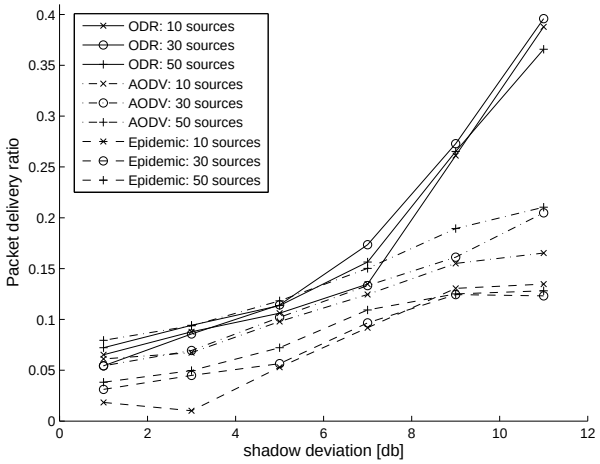

Fig. 6: Packet delivery ratio for different data loads

hidden terminal problem, as illustrated in Fig. 5, where the candidate *B* is unable to listen for the packet forwarding of *A*, and thus it forwards the packet as well. In such a case, it is necessary to resort to explicit acknowledgment, namely *C* stores the packet sent by *A* in the ack queue and thus, it is able to acknowledge to *B* that the packet was successfully received by a node (*A*) closer to destination.

Fig. 4 gives a detailed description of the whole forwarding process resorting to a flow chart representation.

III. Performance analysis

To evaluate the performance of the proposed protocol, we have implemented it as a routing agent on the widely adopted network simulator ns-2 [10] version 2.33 using the wireless extension developed by the CMU Monarch project [11].

We have compared the performances achieved by our protocol with those of two representative routing protocols, namely the Ad Hoc On Demand Distance Vector (AODV) [12] and the Epidemic Routing [13]. The former is a traditional ad hoc routing protocol based on persistent unicast communications among neighbor nodes. The latter exploits the *store-carry-forward* paradigm and it has been proposed to provide connectivity for Delay Tolerant Networks.

A. Experimental setup

Usually, performance analyses for both traditional and opportunistic networking adopt a deterministic radio propagation model which is clearly unrealistic in the case of Disruption Tolerant Networks. Therefore, we consider a propagation model, the *Shadowing* one, which accounts for the long-term fading effects by means of a zero-mean Gaussian variable $N(0, \sigma)$. According to it, the received mean power $P_{dB}(d)$ at distance d is:

$$P_{dB}(d) = P_{dB}(d_0) - \log \beta(d/d_0) + N(0, \sigma) \qquad (5)$$

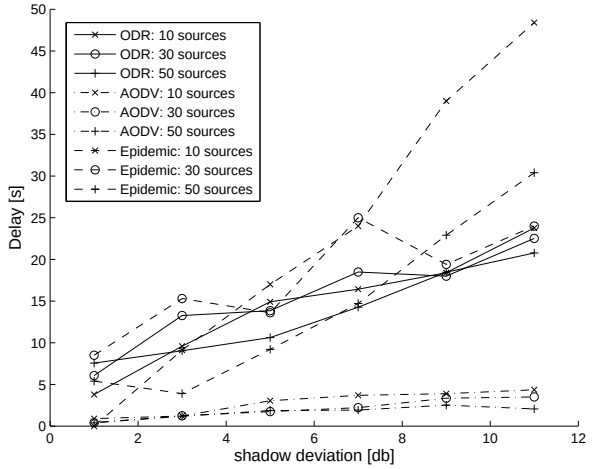

Fig. 7: Delay for different data loads

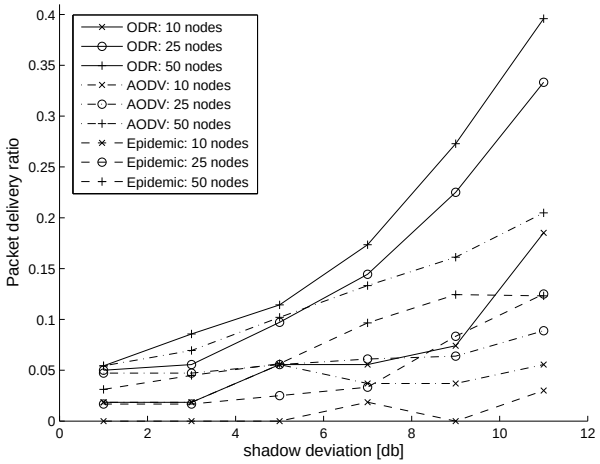

Fig. 8: Packet delivery ratio for different density values

where $P_{dB}(d_0)$ is the received mean power at the first meter, β is the path-loss exponent and σ is the shadow deviation, both empirically determined for a certain environment. In our performance analysis, we set β to 3.8 to model a shadowed urban area, and we vary σ from 1.0 to 11.0dB in order to assess the behavior of the analyzed protocols under a wide range of variability levels of the propagation conditions. Moreover, we set the values of the parameters of the data link layer to simulate an IEEE 802.11b Orinoco network interface [14] with long preamble, CCK11 modulation and two-handshake mechanism, resulting in a transmission range of roughly 35 meters and in a nominal transmission rate of 11 Mbps.

The duration of each experiment is 3000 seconds and the nodes move in accordance with the *random way-point* model [15] with no pause time and at a steady speed over a rectangular $750 * 175\ m^2$ flat area.

After the initial 1000 seconds, a certain fraction of nodes starts to generate data traffic, since the initial period is used to assure that the routing protocols reach a steady state. Each node involved in the traffic generation sends packets of 1000 bytes to each other node in the network, deferring the subsequent transmissions of 1 second. The adopted data traffic allows us to assess the protocol performances under infrequent and concurrent transmissions, as it happens in the case of emergency message dissemination.

B. Numerical results

Since we are primarily concerned with Disruption Tolerant Networks, the performance comparison aims to evaluate the impact of the link dynamic for sparse networks in several environmental conditions. In fact, taking into account both the transmission range and the node density, the mean node connectivity degree is lower than 1 for all the considered scenarios. This value is reasonable to assure the presence of network partitions [16].

The first set of experiments (Fig. 6 and Fig. 7) refers to a scenario with 50 nodes and a node speed equals to $0.01\ m/s$ and a growing number of nodes which generate data traffic.

As regards to the average packet delivery ratio (Fig. 6), the results show that the performances of all the analyzed protocols improve as the shadow deviation increases.

It is worthily to note that these surprising behavior is reasonable, also if unintuitive. In fact, the physical layer model of ns-2 accounts only for the effects of the long-term fading over the packet power (5), neglecting so the effects of information corruption due to fading as well. For such a reason, the fading introduces a time-diversity, which is exploited by the routing protocols to provide end-to-end connectivity.

More in detail, the proposed protocol outperforms the other one as the variability of the wireless propagation grows, providing so an effectively end-to-end connectivity (a delivery ratio equals to 0.4 can satisfy the requirements of several not real-time applications). Moreover, the same figure shows that the performances of all the compared protocols are substantially unaffected by the increase of data load, implying so that we have modeled a sustainable data traffic.

Fig. 7 shows the average packet delay vs. the shadow deviation. Clearly, both the Opportunistic DHT-based Routing and the Epidemic Routing protocols suffer of higher delay times with respect to AODV. The results of Epidemic Routing are expected, since it resorts to the store-carry-forward paradigm, i.e. the forwarder stores the packet until it moves near the destination. As regard to ODR, the delays measure both the time needed to retrieve the location-dependent address and the time for data packet forwarding, i.e. each delay measures the amount of time needed to route three packets.

In the second set of experiments the number of the nodes in the network grows and the node speed is equal to $0.01\ m/s$. Fig. 8 shows the average packet delivery ratio vs. the shadow deviation: clearly, all the protocol performances decreases as the network becomes more sparse and the AODV performs

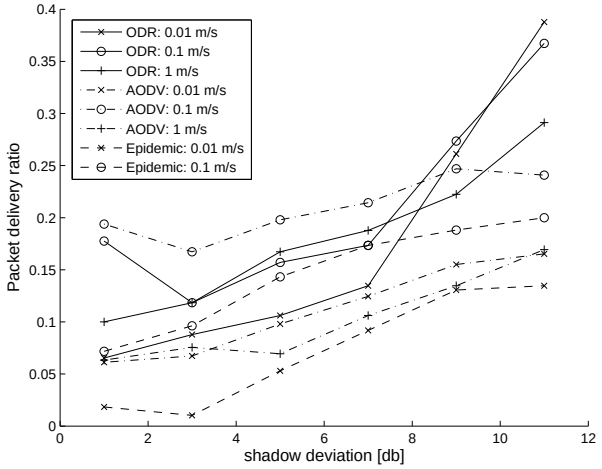

Fig. 9: Packet delivery ratio for different speed values

worst, since it is designed for dense ad hoc networks. The Opportunistic DHT-based Routing outperforms both Epidemic and AODV in all the considered environments, achieving the best performances for the higher values of shadow deviation as well.

In the third set of experiments, we analyze the node mobility effects. More in detail, we simulate a network with 50 nodes and 10 traffic sources and the results are presented in Fig. 8. Both ODR and Epidemic Routing perform worse than AODV as the node speed increases, since AODV is able to exploit a moderate mobility to achieve better performances. We do not present the results for Epidemic Routing in the case of speed value equals to $1\ m/s$ since in such a case the delivery ratios are very small since such a protocol needs bidirectional unicast communications which become unavailable in case of sparse networks with high mobility.

Finally, as regards to routing overhead, the numerical results, not presented for the sake of brevity, shows that Opportunistic DHT-based Routing exhibits the worse performances with respect to both AODV and Epidemic Routing.

IV. Conclusion

The paper proposes a routing protocol for Disruption Tolerant Networks (DTNs). Resorting to the opportunistic routing paradigm and to a location-dependent addressing schema, the proposal is able to provide an end-to-end connectivity for DTN scenarios across different environmental conditions in presence of light data traffic.

Currently, we are working to reduce the routing overhead, which is mainly due to the hidden terminal effects, by improving both the candidate selection and the candidate acknowledgment procedures. Moreover, we plain to adopt a more realistic physical layer model to account also for the effects of information corruption on the protocol performances.

Acknowledgment

The authors would like to thank ...

References

[1] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks," *Communications Magazine, IEEE*, vol. 44, no. 11, pp. 134–141, November 2006.

[2] H. Zhu and K. Lu, "Resilient opportunistic forwarding: Issues and challenges," *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pp. 1–7, Oct. 2007.

[3] A. S. Pentland, R. Fletcher, and A. Hasson, "Daknet: Rethinking connectivity in developing nations," *Computer*, vol. 37, no. 1, pp. 78–83, 2004.

[4] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet," in *ASPLOS-X: Proceedings of the 10th international conference on Architectural support for programming languages and operating systems*, vol. 37, no. 10, October 2002, pp. 96–107.

[5] S. Farrell, V. Cahill, D. Geraghty, I. Humphreys, and P. McDonald, "When tcp breaks: Delay- and disruption- tolerant networking," *Internet Computing, IEEE*, vol. 10, no. 4, pp. 72–78, July-Aug. 2006.

[6] S. Biswas and R. Morris, "Exor: opportunistic multi-hop routing for wireless networks," *SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 4, pp. 133–144, 2005.

[7] M. Brunner, L. Eggert, K. Fall, J. Ott, and L. Wolf, "Dagstuhl seminar on disruption tolerant networking," *SIGCOMM Comput. Commun. Rev.*, vol. 35, no. 3, pp. 69–72, 2005.

[8] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Dart: dynamic address routing for scalable ad hoc and mesh networks," *IEEE/ACM Transactions on Networking*, vol. 15, no. 1, pp. 119–132, 2007.

[9] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," *Wireless Networkks*, vol. 11, no. 4, pp. 419–434, 2005.

[10] T. V. Project, "The ns manual (formerly ns notes and documentation)."

[11] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in *MobiCom '98: Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, 1998, pp. 85–97.

[12] C. Perkins and E. Royer, "Ad hoc on-demand distance vector routing," in *2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp. 90–100.

[13] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," April 2000.

[14] Proxim, "Orinoco 11b client pc card specification," 2004.

[15] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless Communications and Mobile Computing*, vol. 2, no. 5, pp. 483–502, 2002.

[16] C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in *MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, 2002, pp. 80–91.

[17] V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in *INFOCOM '97: Proceedings of the INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution*, 1997, p. 1405.