Packet Scheduling and Discard Policies for Diffusion Control in Delay and Disruption Tolerant Networks

Diego Passos, Henrique Bueno, Etienne Oliveira and Célio Albuquerque

***Abstract*— A Disruption Tolerant Network (DTN) is characterized by scenarios where end-to-end connectivity is rarely available. Hence, in such networks, the use of existing *ad hoc* routing protocols may result on poor performance, since they rely on the existence of an end-to-end path between the source and destination nodes. This paper proposes a DTN routing strategy called DRAIN. Differently from other proposals based on Epidemic routing, DRAIN considers realistic scenarios where nodes' buffer capacity and link bandwidth are limited. Our performance analysis demonstrates the inefficacy of the Epidemic approach in scenarios under such constraints. However, through a controlled packet diffusion and a quantitative packet deliver estimate, DRAIN is able to present good delivery rates in the same conditions, as well as a lower consumption of network resources.**

***Index Terms*— Delay and Disruption Tolerant Networks, Epidemic Routing, Routing Protocol.**

I. Introduction

PACKET routing is a key topic in computer networks. This problem has already been deeply investigated in *ad hoc* networks and several routing protocols have been proposed, such as OLSR (Optimized Link State Routing) [3], AODV (Ad hoc On-Demand Distance Vector) [12], DSR (Dynamic Source Routing) [7] and many others [5]. All these protocols suppose the existence of an end-to-end path between any two nodes in the network. However, in scenarios where disconnections and high delays are frequent, it can be impracticable to use traditional *ad hoc* routing protocols. Networks with such intermittent connectivity are known as Delay and Disruption Tolerant Networks (DTN).

There are several scenarios where DTN networks can be applied:

- forest parks, where there is no communication infrastructure and data exchange through an *ad hoc* network is difficult because of natural barriers;
- mobile sensor networks, where nodes can be dispersed in a vast region. In this case, nodes can be programmed to periodically turn off themselves to reduce energy consumption, causing network disconnections;
- areas of climatic disaster or under war, where the communication infrastructure has been destroyed and end-to-end connectivity between nodes is not guaranteed because of physical obstacles;
- remote areas, where connections can only be established during short periods of time. These connections can be periodically created according to the movement of ferry nodes [18]. These nodes are responsible for data transfer between remote regions.

In DTNs, a *contact* is established when two nodes share a physical connection or when they are close enough to exchange information. One of the greatest challenges on this kind of network is packet routing. This problem can be mainly addressed in two distinct scenarios: it can be studied considering scenarios where the knowledge of the network state (establishment of contacts and traffic demand) can be predicted at any instant in time, or considering that no contact information is available. The former scenario is known as deterministic, whereas the latter is known as stochastic. Clearly, stochastic scenarios characterize a more complex problem.

One of the main routing protocols for DTN in stochastic scenarios is the Epidemic routing [14]. When two nodes a and b establish a contact, a forwards to b all packets in its transmit buffer, except for those that are already in b, and vice versa. Therefore, as nodes move, contacts are established, packets are diffused and, eventually, their destinations are reached.

The Epidemic routing strategy consumes excessive network resources, compromising its delivery rate in scenarios where nodes' storage capacity and link bandwidth are limited.

There are a number of recent routing protocols proposed for DTN [2], [9], [11], [13], [15], [16], [21], [19]. These protocols, differently from Epidemic routing, exhibit a lower consumption of networks resources, by controlling and restricting packet diffusion in various ways. However, a missing characteristic in all these works is the expected value of the packet delivery rate.

This work proposes the Delivery Rate Aware routing protocol for Intermittent Networks, hereinafter referred to as DRAIN, a packet routing strategy for DTN stochastic scenarios. Furthermore, it considers scenarios where nodes' storage capacity and link bandwidth are limited. In such scenarios, Epidemic routing presents an excessive resource consumption, which can result on low packet delivery rates, as shown in Section IV-C.2. With DRAIN, packet diffusion happens in a controlled way, reducing network resource consumption without losing the focus on reaching a high delivery rate.

To evaluate the performance of the proposal, several experiments were performed using the ns-2 simulator [4]. A module that implements the DRAIN routing strategy as well as DTN characteristics has been developed. To evaluate DRAIN

This work was partially supported by IBGE, CNPq, FAPERJ, and TBE.

Diego Passos, Henrique Bueno, Etienne Oliveira and Célio Albuquerque are with the Instituto de Computação, Universidade Federal Fluminense (UFF), Niterói, RJ, Brazil. E-mail: {dpassos,hbueno,eoliveira,celio}@ic.uff.br.

ISSN 1980-6604/$20.00 © 2008 SBrT/IEEE

results, Epidemic routing and oracle modules were also implemented.

This paper is organized in 5 sections. Section II presents state of the art in DTN routing protocols. Section III presents the DRAIN proposal and its implementation characteristics. Section IV presents the performance evaluation. Finally, Section V presents the conclusions and future work.

II. Related Work

DTN networks face a number of challenges. In [17], authors discuss why conventional internet protocols are not applicable to this type of network. Currently a number of projects that implement DTN have been developed. The SeNDT's (Sensor Networking with Delay Tolerance) [10] project objective is to evaluate the quality of water in lakes and noise pollution on roads. ZebraNet [8] project utilizes wireless sensors in zebras to monitor the animals' typical locations. Information are stored in the sensors until a contact with a base station (or with another zebra sensor) happens.

This work addresses the challenge of DTN routing for which various proposals have been recently investigated [14], [2], [9], [11], [13], [15], [16]. Epidemic routing, introduced in [14], works by distributing application messages among nodes in a network partition. When a node moves towards another partition, packets are diffused. Through these transitive packet exchanges, messages can reach their destinations. A problem with this strategy is the excessive consumption of network resources, since data is replicated each time a contact occurs. Moreover, in limited-resource scenarios (in terms of storage and bandwidth), packet delivery rate could be unsatisfying. This characteristic will be demonstrated in Section IV-C.2.

There are some variations of the Epidemic routing which aim at reducing packet replication through controlled diffusion [2], [9], [11], [13], [15], [16], [21]. In other words, they employ algorithms that decide if a packet should be replicated or not when a contact occurs. Moreover, some proposals consider the use special control packets, known as anti-packets [14], [17], [1], to reduce the number of copies of each message in the network. These anti-packets are diffused through the network when a packet reaches its destination. The anti-packet has the same id of the data packet that reaches the destination and indicates to other network nodes that the data packet has been delivered and its copies can be discarded.

Another approach to reduce the impact of flooding messages and also improve the performance is to forward messages only if some condition is met using *Utility-based* or *History-based* routing methods. In [9], [20], [8], nodes maintain a utility value for every other node in the network that is used to decide whether or not messages should be forwarded. However, in this kind of scheme a utility threshold should be determined and, depending on the value, the scheme may present a behavior like the epidemic routing or may increase the delay substantially.

The work presented in [6] uses oracles in DTN routing. Oracles are assumed to have complete knowledge of current and future network connectivity state. Oracles can for instance give information about: when a contact between two nodes will occur, what is the buffer occupation of a node at any time and what is the traffic demand at any moment. Despite generating good results, oracle implementations are not feasible in practice, since they suppose knowledge about mobility patterns and nodes' connectivity.

The Prioritized Epidemic Routing protocol [21] priorizes messages (bundles) for transmission and deletion based upon four inputs: current cost to destination, current cost to source, expiry time and generation time. Internode costs are based on a metric called average availability (AA) which attempts to measure the average fraction of time in the near future that the link will be available for use. Each link's AA is epidemically disseminated to all nodes. The MaxProp [1] and RAPID [19] routing protocols were deployed on a vehicular DTN testbed called UMassDieselNet. This network consists of buses carriyng 802.11b radios and computers that intermittently establish a contact with each other, and covers a 150 square-mile area around Amhest, M.A. MaxProp classifies messages based on a cost (*delivery likelihood*) assigned to each destination, and uses acknowledgments to notify message deliveries. RAPID can optimize a specific routing metric by treating DTN routing as a resource allocation problem. A per-packet utility determines how packets should be replicated. Similarly to the DRAIN proposal, [1] considers that nodes' mobility and traffic demand are unknown and nodes' storage capacity is limited.

Differently from the works presented in this section, DRAIN aims at improving network performance through a quantitative evaluation of the packet delivery rate in scenarios where buffer size and bandwidth are limited.

III. DRAIN Proposal

DRAIN is composed by a set of packet scheduling and discard policies. The idea is to restrict message diffusion scope without losing the objective of increasing packet delivery rate. Basically, the proposal can be divided in three modules:

- a probability attribution module;
- a module to decide which packets should be sent when a contact occurs; and
- a module to choose which packets should be discarded (when needed).

The first item refers to the delivery probability metric used by DRAIN to take its decisions. As the name suggests, this module will infer message delivery probabilities. Later, this information will be used for classifying packets' priorities with respect to the contacts. The probability attribution mechanism will be explained in details in Section III-B.

Another characteristic of the scenarios considered in this work is the fact that link bandwidth is limited, what is a more realistic situation. This means that, when a contact happens, a node may not be able to transfer all packets in its buffer. Hence, a strategy without a packet scheduling policy to choose which packets should be sent when a contact occurs can lose opportunities to send messages, especially when short-time low-bandwidth contacts happen.

This can be verified by taking a simple example. Suppose nodes a and b establish a contact for a period of time sufficient only for node a to send 10 messages. However, it is possible that the eleventh packet on a's buffer is exactly addressed for node b. Therefore, node a will lose an opportunity to send this packet to its final destination.

This example, although simple, illustrates a common DTN situation. Sending opportunities should be taken, since in these networks contacts can be rare. Therefore, a packet scheduling policy is essential. In DRAIN, the set of rules used by the scheduler will be presented in Section III-C.

The last item refers to a set of rules used to decide packets' discard priorities. In the considered scenarios, the size of buffers available to store messages in each node is limited. Therefore, it is possible that, at some moment, a node would have to decide which packets should be kept in the buffer and which should be discarded. A possible approach would be to utilize a FIFO (First In First Out) policy. However, on Section III-D it will be shown that discarding the oldest packet may not be ideal.

A fourth protocol functionality is the utilization of anti-packets. As pointed out on Section II, anti-packets are special control messages of delivery confirmation. Whenever data packets arrive at their destination, this node should generate a correspondent anti-packet and start its diffusion through the network. This mechanism allows copies of data packets already delivered to be removed from the buffers of intermediate nodes faster, releasing network resources. Moreover, in this proposal anti-packets are utilized to infer delivery probability. In Section III-A, the anti-packet format and its usage will be explained in details.

A. *Packet Format*

To implement the mechanisms and policies presented in the following sections, some information needs to be carried into data packets that travel through the network. In this section, the format of the data packets used by the DRAIN proposal is defined.

Figure 1 illustrates the required fields for each data message:

- Source: address or unique identifier of the packet source node;
- Destination: address or unique identifier of the packet destination node;
- Sequence number: communication sequence number between source and destination nodes;
- Hop number: the number of hops that the packet has traveled;
- Payload size;
- the payload itself; and
- Route Vector: a vector storing the route which the packet has traveled.

The three first items (source, destination and sequence number) uniquely identify a packet in the network. The hop count field is initialized with zero when the message is created in the source node and should be increased by each intermediate router. The hop count determines the length of the route vector field and the payload size determines the number of bytes of the following field, which stores the application message. The last field stores a route vector that should be initialized with the identifier of the source node and, as the packet travels, each intermediate node should insert its own identifier. In the worst case, the route vector size grows up to the network size.

The anti-packet format is identical. However, some fields will have a different meaning. The sequence number should be exactly the same as the one contained in the arriving data packet. On the other hand, source and destination fields should be exchanged. This ensures that an intermediate node can identify the data packet associated to that anti-packet. The payload size field should be reset, indicating that this is an anti-packet. Thus, the payload should be null.

Finally, the route vector should be initialized by the anti-packet source node with the same entries of route vector of the correspondent data packet. Differently from what happens with data packets, with anti-packets, this vector will not be changed by intermediate nodes. The reason for this approach will be explained in Section III-B.

B. *Probability Attribution*

In this section the metric used by the scheduling and discarding policies will be defined. This metric is based on the message delivery probability for each destination. Each network node should keep a delivery probability estimate for each other node. This estimate will assume an initial value and, as some network events occur, this value can increase or decrease. We also presume that every network node has capacity to store this delivery probability estimate for each other node. Denoting by P_{ab} an estimate of node a about its message delivery probability to node b, the following events and their respective actions can be defined:

- Node a enters the network. In this case, it is necessary to assign some initial value to the P_{ab} estimate for every node b. The best initial value is possibly scenario dependent. Hence, we propose the utilization of a parameter λ, ranging from 0 to 1. Therefore, for each node b on network:
$$P_{ab} \leftarrow \lambda;$$
- Node a receives an anti-packet and verifies that its own identifier is on the *n-th* position of the route vector. That means node a has been successfully used to deliver the message. Therefore, denoting by b the anti-packet source node, the estimate should be increased by de following expression:
$$P_{ab} \leftarrow P_{ab} \cdot (1 - \alpha^n) + \alpha^n.$$
In this expression, α is a configurable parameter that determines the weight of the old estimate. The option

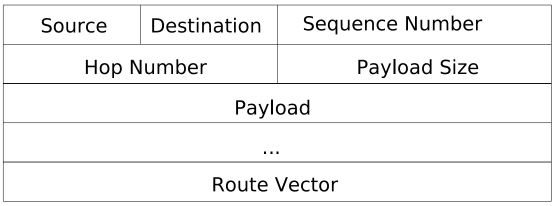


Fig. 1. DRAIN data packet format.

of raising α to the power of n is justified by the fact that the last nodes on a route used to deliver the data packet are, probably, the nodes with higher probability of establishing a contact with destination node and, consequently, with better delivery probability;

- Node a receives an anti-packet and verifies that its identifier is not on the route vector. That means node a was not used on the data packet delivery route. Therefore, denoting by b the anti-packet source node, the estimate should be decreased by the following expression:

$$P_{ab} \leftarrow P_{ab} \cdot (1 - \alpha);$$

- Node a establishes a contact with destination node b. Therefore, even if a does not have packets to deliver, it should increase its estimate (because it has an opportunity to transmit to b):

$$P_{ab} \leftarrow Min\{P_{ab} \cdot (1 + \alpha), 1\};$$

- Node a discards a data packet destined to node b. In this case, since a is discarding a packet without receiving a delivery confirmation, it may suppose that this message did not reach its destination. Hence, it is reasonable that the delivery estimate to node b should be decreased:

$$P_{ab} \leftarrow P_{ab} \cdot (1 - \alpha); and$$

- Node a discards an anti-packet in which the destination field stores node b identifier. Since one of the functions of anti-packets is to indicate to the source of the data packet (in this case, node b) that its message was delivered, it is reasonable to suppose that an anti-packet discard is equivalent to a data packet discard. However, obviously data packets have a bigger importance. Therefore, the decrease applied in this case is:

$$P_{ab} \leftarrow P_{ab} \cdot (1 - \beta),$$

where $\beta < \alpha$.

Clearly, the effects of the presented definitions are dependent on parameters λ, α and β. On Section IV, simulations with different values for these parameters will be presented, allowing an evaluation of DRAIN sensitivity to them.

C. Packet Scheduling Policy

As explained before, the packet scheduling policy proposed in this paper refers to a set of rules that determines nodes actions when a contact occurs. When a contact happens, this policy will determine the transmission priority of each packet in the buffer.

A reasonable first rule is to give priority to packets destined to the current contact. In other words, if node a has a contact with node b, a should initially transmit all packets destined to b. The reason for this is that each opportunity of delibery must be taken, so it is preferable to transmit a duplicate message to its destionation.

After this initial transmission of packets destined to b, it is necessary for nodes to exchange their delivery probability estimates. This exchange is necessary because, through this process, routing data is diffused among nodes. Since in DTNs end-to-end paths are rare, this information can not be diffused efficiently through traditional mechanisms, such as ordinary broadcast algorithms used in *ad hoc* networks, for example.

Once routing data has been exchanged, it is possible to use it to infer the best subset of messages to be sent. Hence, it is necessary to define a value called Accumulated Delivery Probability (ADP). For every message M in the buffer, an Accumulated Delivery Probability will be associated, and initially assigned to 0. Every time the message is replicated to a neighbor its ADP should be updated. This update should follow the rule:

$$ADP_M \leftarrow Min\{ADP_M + P_{bc}, 1\},$$

where c denotes the destination of message M and b denotes the neighbor to which the message is being replicated.

The value ADP_M is an estimate of the probability of message M be delivered to its final destination c, given that it has been replicated to a set of nodes. The objective of ADP is to indicate when to stop replicating the message M, thereby controlling the diffusion scope. So, there is no need to use another mechanism to control packet lifetime, such as TTL (Time To Live) or maximum hop counter.

Hence, it is possible to define new priority classes. Since DRAIN utilizes anti-packets as a resource release mechanism, it is important to diffuse these messages. Therefore, after the previous message exchanges, all anti-packets with Accumulated Delivery Probability lower than ω should be replicated. After that, if there are anti-packets destined to the current contact not yet sent, they should be sent now.

After the transmission of these anti-packets, nodes should start data packet replication. This means that all data packets with Accumulated Delivery Probability lower than 1 should (if possible) be sent. The order of packet transmission in this class tries to maximize the Accumulated Delivery Probability. In other words, packets belonging to this class should be sorted in non-increasing order of the following value:

$$ADP_M + P_{bc},$$

where, again, c denotes the destination of packet M and b denotes its neighbor.

If a contact lasts long enough, all packets from the previous classes can be transmitted. In this case, nodes may utilize the contact time to exchange the remaining anti-packets.

In brief, when a contact occurs, a node should follow the message transmission steps below:

1) Send all data packets destined to the node that established the contact. These packets should be delivered in an Accumulated Delivery Probability non-increasing order;
2) Send routing information. In other words, send the delivery probability estimates;
3) Send all anti-packets with Accumulated Delivery Probability lower than ω.
4) Send all anti-packets destined to the node that established the contact. Again, inside this message class, messages with lower Accumulated Delivery Probability value should be delivered first;

5) Send all data packets with Accumulated Delivery Probability lower than 1. Packets of this group are sorted in a non-increasing order of $ADP_M + P_{bc}$ value; and
6) Finally, send other anti-packets, following again an Accumulated Delivery Probability non-decreasing order.

Although these rules are presented here as phases, the priorities must be evaluated for every packet sent. For instance, if a node is currently sending anti-packets with ADP lower than ω (third rule) and a data packet destined to the node that established the contact arrives (first rule), this new packet has priority and, hence, should be the next to be sent.

It is also important to notice that the route vector should be verified before a packet is transmitted. If the identifier of the current contact is already present on the vector, the node should not send the packet, since this would characterize a loop. Therefore, in this situation, another packet must be chosen.

D. Packet Discard Policy

On Section III-C, nodes' actions during a contact were discussed. However, only the aspects referring the order in which messages should be transmitted to neighbors were discussed. In fact, supposing that nodes storage capacity is finite, there should be also priorities to discard messages, because eventually nodes' buffer will be exhausted.

Hence, DRAIN defines the following three discard priority classes (in precedence order):

1) Data packets which associated anti-packet has already been received can obviously be discarded. This discard should happen as soon as the anti-packet is received.
2) If anti-packets occupy more than 10% of the buffer, then anti-packets in excess have discard priority. In this case, discards should be done in non-increasing order of the following greatness:

$$\delta = Hops * t,$$

where $Hops$ denotes the number of hops which the anti-packet copy passed and t represents the amount of time that the message is in the node's buffer. This definition performs a balancing between anti-packets diffusion degree (given by the hops value) and how node's resources are occupied (over time).
3) If still necessary, discard data packets which destination has lower delivery probability (among all estimates from the node). These packets should be discarded in non-increasing order of Accumulated Delivery Probability.

Clearly, this discard policy assigns a lower importance to anti-packets than to data packets. That is reasonable, since anti-packets are just an overhead associated with the proposed mechanisms. On the other hand, data packets are considerably larger than anti-packets. Therefore, even the discard of all anti-packets may not be effective. This justifies the option of not discarding anti-packets if they occupy 10% or less of buffer space.

IV. Performance Evaluation

To evaluate the performance of DRAIN, ns-2 simulations were used. The ns-2 is a natural choice for a network simulator given its wide use and reliability. However, to the present time, ns-2 does not offer official support for DTN simulations. Hence, it was necessary to develop modules to cope with the specific characteristics of DTN, such as the store-carry-forward paradigm. The main goal of this evaluation is to perform a comparison between the DRAIN proposal and the traditional Epidemic routing. Therefore, both Epidemic and DRAIN routing modules have been implemented.

A. Simulation Environment

Usually, DTN scenarios involve wireless links. However, several of the possible DTN scenarios do not involve only wireless links. In the simulation scenarios considered here, the adopted link and physical layers have been simplified to exhibit the following generic characteristics:

- There is no packet loss model. Both the link and physical layers are believed to be completely reliable. Hence, the only reason for a packet to be lost is due to buffer overflow;
- Every node has a fixed transmission rate, which is fully usable by the network layer. In other words, there is no overhead due to the lower layers and the distance between nodes does not interfere with the throughput;
- When there are simultaneous contacts, the available bandwidth is equally divided by each contact. For instance, if the transmission rate is 400 Kbps and the node has 2 simultaneous contacts, the available bandwidth for each contact will be 200 Kbps; and
- A packet cannot not be fragmented. In other words, within a contact a packet has to be completely transmitted, or not transmitted at all.

Even though these assumptions are not completely realistic, they are used for the evaluation of both Epidemic and DRAIN, which guarantees a fair comparison.

B. Simulation Scenarios

The results presented in this section refer to a total of five different (although statistically similar) scenarios. These scenarios model communications in DTN environments such as forest parks and were generated using the parameters shown on Table I. For every node, a random movement is chosen (direction, speed and duration). When the node reaches its destination, another movement is picked. This process is repeated until the end of the simulation time. The traffic distribution is uniformly random. After a short random initial delay (between 0 and 1 second), a pair of nodes is chosen every second and a message is generated to be transmitted between then. Every pair is selected exactly once. Hence, there is a total load of 210 packets on the network. These traffic parameters, as well as the mobility ones, are based on the scenarios evaluated on [14].

Since nodes' messages and movement are randomly chosen, five different scenarios were generated to avoid tendentious results. Table II shows statistical information about the contacts on each scenario. It is worth pointing out that these kind of scenarios (with random mobility patterns) are the worst cases

TABLE I
PARAMETERS USED FOR GENERATING THE EVALUATED SCENARIOS.

Item	Description
Number of Nodes	15
Scenario Dimensions (m)	1 500 x 300
Simulation Duration (s)	2 000
Initial Position	Randomly chosen (uniformly)
Nodes Speed (m/s)	Uniformly distributed in $[10; 20]$
Messages Size (bytes)	1 000
Transmit Rate	Variable
Buffer Size	Variable

for the DRAIN proposal, since the "routes" are not maintained during the simulations. A scenario with better defined mobility patterns, such as scenarios based on cyclic movements or ferry nodes, would be more suitable, because it would allow DRAIN's delivery probability learning process to converge.

TABLE II
STATISTICAL ANALYSIS OF EACH SCENARIO.

Scenario	Number of Contacts	Average Duration (s)	σ
1	2 492	30.21	25.83
2	2 522	29.64	27.69
3	2 408	32.28	30.20
4	2 441	29.65	27.63
5	2 454	31.11	27.85

C. Results

Four series of simulations were performed. The first series has the objective of analyzing the impact and sensitivity of DRAIN parameters. In the second, we intend to show the limitations of the Epidemic routing on scenarios where bandwidth and storage capacity are restricted. In the last two series, the goal is to compare the results from both DRAIN and Epidemic solutions when storage capacity and bandwidth availability (respectively) are varied.

1) Sensitivity to DRAIN Parameters: Before comparing DRAIN and Epidemic routing, it is important to evaluate the impact of varying the parameters defined on DRAIN's proposal. On the simulations presented in this section, the parameter α assumed values ranging from 0.05 to 0.50, in increments of 0.05. For each possible value of α, the parameter β assumed the values of $\alpha/10$, $\alpha/5$ and $\alpha/2$. As for the parameter λ, in this simulations it assumed the values ranging from 0.10 to 0.70, in increments of 0.05. After running some preliminary simulations the parameter ω was set to 0.1.

Nodes bandwidth is set to 10 KB/s, while each buffer comports 10 packets. These values were chosen in order to eliminate bandwidth constrained problem during these simulation series. With a bandwidth of 10 KB/s, a packet length of 1 KB and an average connection duration of approximately 30 seconds, it is possible to transmit 300 packets during each connection opportunity, nevertheless each node can store only 10 packets (packets or anti-packets). As described in Section III-D, the Packet Discard Policy will manage buffer space and discard packets or anti-packets due to the priority classes previously defined.

All the possible combinations of these values were evaluated in all 5 scenarios, in a total of 390 simulations. Table III shows the obtained results for the best 10 combinations[1]. The first three columns show the values of α, β and λ. The next five columns show the percentage of delivered packets for each scenario, while the last two show the average for all scenarios and standard deviation, respectively. The average value was used to order the table and to define the 10 best combinations.

The six best results use $\lambda = 0.70$ and the three first positions use $\alpha = 0.45$. As for the β parameter, there are 4 occurrences of $\alpha/10$ and three occurrences of the other values. Apparently, the use of a higher initial estimate allows DRAIN to converge faster, making the routing rules more effective. The same seems to be apply to α. With a high value of α, changes on the probabilities' estimates happen faster.

Figure 2 shows the delivery results for all combinations in which λ is 0.70. It is difficult to point out the best value for the parameter β. However, the three curves present a very similar behavior with respect to α. It is also noticeable that changing the value of α causes a higher impact on the delivery than changing β. In conclusion, DRAIN parameters are set to $\alpha = 0.45$, $\beta = 0.225$, $\lambda = 0.7$ and $\omega = 0.1$ in all simulations.

2) Epidemic Limitations: To demonstrate the poor performance of Epidemic routing on environments with bandwidth and storage restrictions, a set of simulations was performed where both available bandwidth and buffer size were simultaneously varied. The bandwidth values ranged from 100 B/s to 1 KB/s, while the storage capacity assumed values between 10 and 400 packets.

The result of these simulations is plotted on the graph of Figure 3. When both bandwidth and storage capacity are widely available, Epidemic routing easily achieves 100% of delivery. If we keep the buffer size fixed on 400 packets and start decreasing the bandwidth, the resulting packet delivery drops exponentially.

[1] The remaining 380 combinations resulted in lower packet delivery

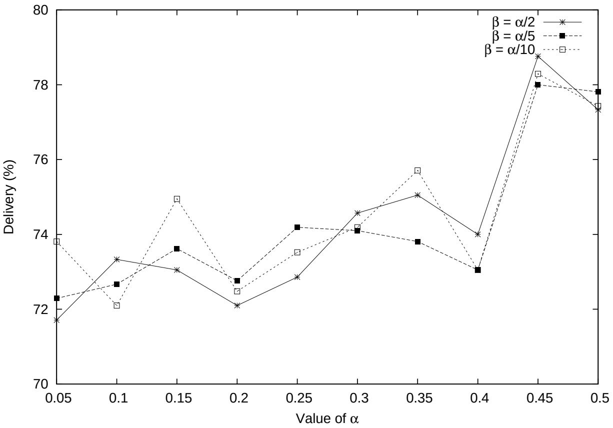


Fig. 2. Delivery in function of the value of α when λ is kept constant in 0.70.

TABLE III
SUMMARY OF PACKET DELIVERY ON EACH SCENARIO WITH EACH COMBINATION OF PARAMETERS.

α	β	λ	**1**	**2**	**3**	**4**	**5**	**Average**	σ
0.45	0.225	0.70	79.05	81.90	80.00	77.62	75.24	78.76	2.25
0.45	0.045	0.70	80.95	79.52	77.14	77.14	76.67	78.29	1.67
0.45	0.090	0.70	80.95	77.14	75.71	77.62	78.57	78.00	1.74
0.50	0.100	0.70	81.90	77.14	76.19	77.14	76.67	77.81	2.08
0.50	0.050	0.70	81.90	76.19	77.14	78.10	73.81	77.43	2.65
0.50	0.250	0.70	76.67	80.95	75.71	74.76	78.57	77.33	2.20
0.45	0.225	0.60	75.71	76.67	71.43	82.38	77.62	76.76	3.52
0.45	0.090	0.60	76.19	74.29	73.33	80.95	79.05	76.76	2.86
0.45	0.045	0.55	77.14	72.86	71.43	76.19	83.81	76.29	4.31
0.45	0.045	0.60	72.38	73.81	74.76	80.95	77.14	75.81	3.00

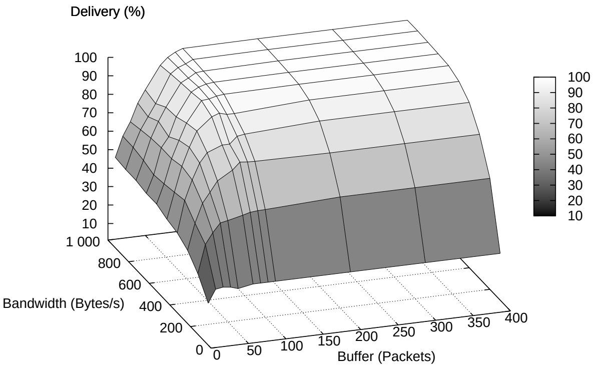


Fig. 3. Epidemic delivery rate in function of bandwidth and buffer size.

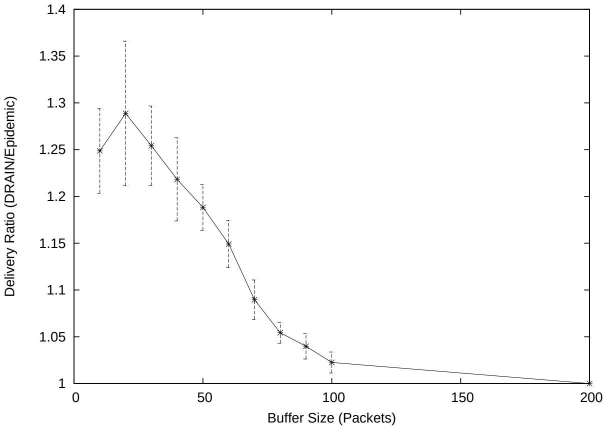


Fig. 4. Ratio of delivery rate between DRAIN and Epidemic routing in function of buffer size.

If, instead, we maintain the bandwidth fixed on 1 KB/s and decrease buffer capacity, the curve stays constant at 100% delivery until the buffer size reaches 100 packets. This happens because, for this scenario, a buffer of 100 packets is relatively large (considering the total amount of 210 packets generated). However, from this point on, if buffer sizes continue to be decreased, the packet delivery drops extremely fast.

As we restrict both bandwidth and storage simultaneously, Epidemic delivery rate easily gets below 50%. In the extreme case, when buffer size reaches 10 packets and bandwidth is limited to 100 B/s, Epidemic routing is able to deliver only 19% of the packets. The graph also shows that the performance of Epidemic routing suffers more when bandwidth is restricted than when storage capacity is limited.

3) Impact of Limited Buffer Capacity: In this series, nodes buffer capacity has been varied from 10 to 400 packets. As stated in Section IV-B, the total number of data packets generated is 210. Hence, for the Epidemic routing, a 400 packet buffer is virtually infinity. However, this may not be true for the DRAIN routing, since for every delivered data packet a corresponding anti-packet is injected into the network. During this simulations, all nodes from Epidemic and DRAIN routing protocols were configured to use a bandwidth of 10 KB/s.

Figure 4 shows the ratio of packets delivered with the DRAIN and Epidemic routing. The results are based on the average of the five scenarios and the bars show the 95% confidence interval. Clearly, the delivery rate with DRAIN was not inferior for any scenario or buffer size. Specially when buffer size is less than 50 packets, DRAIN achieved an improvement of more than 20% on average. Moreover, the graph shows a tendency of increase in the percentage difference between DRAIN and Epidemic routing with the decrease of buffer size. Furthermore, DRAIN routing achieved 100% of packet delivery for every scenario when buffer size was equal to or higher than 30 packets. As for the Epidemic routing, for a buffer size of 30 packets, it only achieved 80% of packets delivery.

Table IV summarizes the packet discard statistics for each scenario. The last column shows the difference between the number of packets discarded with DRAIN and Epidemic routing. When buffer size is 400 packets, Epidemic routing does not discard any packets and, therefore, this difference is 0. Once again, this happens because, for the Epidemic routing, a 400 packets buffer is infinity.

However, for buffer sizes equal to or less than 200 packets (i.e., when the buffer is not infinity for the Epidemic routing), the Epidemic strategy causes a considerable higher number of discards. This shows that, although DRAIN's discard policy has a higher computational cost, it must be used considerably less times, when compared with the Epidemic policy. If we take buffer size equals to 50, for instance, the Epidemic

TABLE IV

SUMMARY OF PACKET DISCARD ON EACH SCENARIO IN FUNCTION OF STORAGE CAPACITY.

Scen.	Buffer Size	DRAIN	Epidemic	Difference
1	10	1 834	47 349	45 515
1	20	2 866	80 046	77 180
1	50	503	105 118	104 615
1	100	0	111 110	111 110
1	200	0	3 200	3 200
2	10	3 526	44 500	40 974
2	20	2 460	74 933	72 473
2	50	613	104 076	103 463
2	100	1	108 692	108 691
2	200	0	3 099	3 099
3	10	1 953	46 912	44 959
3	20	1 505	77 061	75 556
3	50	484	104 382	103 898
3	100	1	107 872	107 871
3	200	0	3 043	3 043
4	10	2 152	46 773	44 621
4	20	1 051	77 208	76 157
4	50	464	106 188	105 724
4	100	0	108 356	108 356
4	200	0	3 136	3 136
5	10	2 817	45 370	42 553
5	20	4 567	80 083	75 516
5	50	881	103 633	102 752
5	100	53	107 985	107 932
5	200	0	3 232	3 232

routing discarded more than 100 times the number of packets discarded by DRAIN in any scenario.

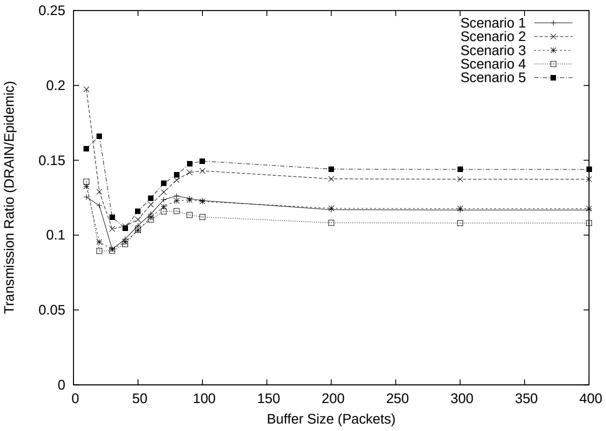


Fig. 5. Ratio of number of transmissions between DRAIN and Epidemic routing in function of buffer size.

Figure 5 shows a similar metric: the ratio of transmissions. Each series in the graph represents the ratio between the number of transmissions with DRAIN and Epidemic routing in a different scenario. Once again, it is clear that the number of transmissions with the Epidemic routing is considerably higher than with DRAIN. The number of transmissions with DRAIN is at least 80% lower, when compared with the Epidemic routing. For most of the cases, the number of transmissions with DRAIN is between 85% and 90% less than with Epidemic.

This metric can be quite important, because the power consumption of the nodes is proportional to the number of transmissions. Hence, for scenarios where energy is a constraint, DRAIN routing would be a better choice from this point of view.

4) Impact of Limited Link Bandwidth: In the third series of simulations, the buffer size has been kept constant in 200 packets, while the bandwidth varied from 100 B/s to 20 KB/s. Although anti-packets consume bandwidth, the received anti-packets are not considered for the delivery rate calculation. All the other parameters have been kept with the same values from the previous series.

The graph on Figure 6 shows the ratio between the delivery rate from DRAIN and Epidemic routing. For values of bandwidth higher than 900 B/s, this ratio was always constant in 1, that is, both Epidemic and DRAIN delivered all packets. Nevertheless, the results show that, when bandwidth becomes a constraint, the performance difference between DRAIN and Epidemic is even more accentuated. When the available bandwidth is 200 B/s, DRAIN is able to deliver more than 1.5 times the number of packets delivered by the Epidemic routing in all scenarios.

If the bandwidth drops to 100 B/s (the lowest value used), DRAIN achieves more than 3 times the Epidemic delivery rate, again on all scenarios. In fact, with this bandwidth, while DRAIN delivers more than 95% of the packets, Epidemic routing cannot reach 30% of delivery rate. This shows the inefficacy of the Epidemic routing when bandwidth is a limiting factor.

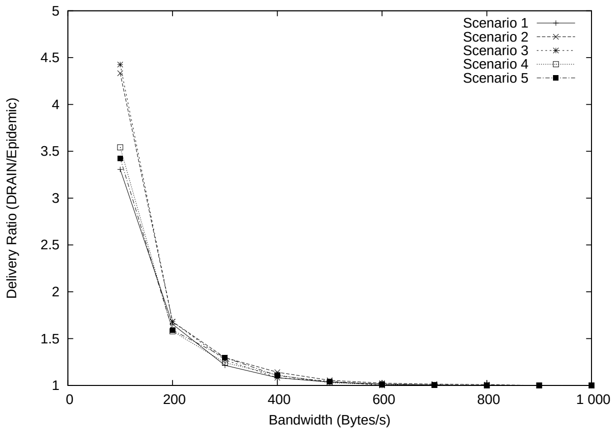


Fig. 6. Ratio of delivery rate between DRAIN and Epidemic routing in function of buffer size.

As for the packet discard statistics, Table V shows that, in this case, the difference between DRAIN and Epidemic routing is not as impressive (in terms of absolute values) as when buffer space is restricted. With low bandwidth, both routing strategies are unable to send many packets on each contact, and therefore no discards happen. Also, as seen on Table IV, the buffer size of 200 packets leads to low packets loss (or no packet loss, in the case of DRAIN).

However, there is a clear increasing tendency of this difference as the available bandwidth increases. While DRAIN

TABLE V

SUMMARY OF PACKET DISCARD ON EACH SCENARIO IN FUNCTION OF BANDWIDTH.

Scen.	Bandwidth	DRAIN	Epidemic	Difference
1	100	0	0	0
1	1000	0	218	218
1	5 000	0	2 006	2 006
1	10 000	0	3 200	3 200
1	20 000	0	7 293	7 293
2	100	0	0	0
2	1000	0	243	243
2	5 000	0	1 794	1 794
2	10 000	0	3 099	3 099
2	20 000	0	6 782	6 782
3	100	0	0	0
3	1000	0	161	161
3	5 000	0	1 812	1 812
3	10 000	0	3 043	3 043
3	20 000	0	7 586	7 586
4	100	0	0	0
4	1000	0	175	175
4	5 000	0	1 950	1 950
4	10 000	0	3 136	3 136
4	20 000	0	7 989	7 989
5	100	0	0	0
5	1000	0	144	144
5	5 000	0	2 078	2 078
5	10 000	0	3 232	3 232
5	20 000	0	7 694	7 694

remains with no packet discards as more bandwidth becomes available, the Epidemic routing has the chance of sending more unnecessary packets, increasing the probability of buffer overflows.

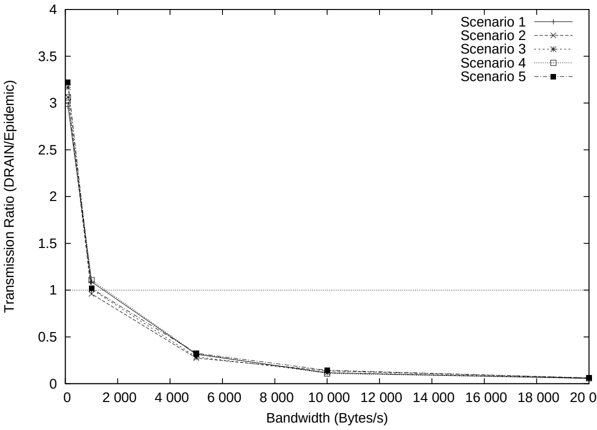


Fig. 7. Ratio of number of transmissions between DRAIN and Epidemic routing in function of buffer size.

Figure 7 shows the ratio between the number of transmitted packets with both DRAIN and Epidemic routing. All scenarios presented a very similar behavior. When the bandwidth is limited, the number of packets transmitted with DRAIN is considerably higher. With nodes bandwidth set to 100 B/s, for instance, DRAIN transmits more than 3 times the number of transmitted packets by the Epidemic routing. However, as the bandwidth availability grows, this ratio drops exponentially. The explanation is that with lower bandwidth DRAIN can send more packets than the Epidemic routing. This happens due to the existence of the anti-packets. These packets tend to be smaller than regular data packets and, thus, they demand less bandwidth to be transmitted. On the other hand, when more bandwidth becomes available, the Epidemic routing is able to send a larger number of packets on each contact. Since the Epidemic routing does not control its diffusion, the ratio tends to drop.

V. CONCLUSIONS

This paper proposed a new routing strategy for Delay and Disruption Tolerant Networks called DRAIN. The objective of DRAIN is to perform packet routing in scenarios where nodes' storage capacity and link bandwidth are limited. The main focus was to reduce network resource consumption while still reaching a high delivery rate. This work also presented arguments and simulation results to explain and demonstrate the inefficacy of Epidemic routing on environments where resources are restricted.

Differently from other works, this strategy uses a quantitative evaluation of delivery probability. Hence, good routes can be chosen through the association of probabilities with network events. This allows nodes to choose whether or not they should transmit a packet and which packets should be sent in a given contact based on historical data. Using this approach, nodes may avoid wasting bandwidth and buffer space sending or receiving unnecessary packets, thereby improving network resource utilization. With a better use of resources, an improvement on other metrics, such as the delivery rate, was obtained.

Three series of simulations were executed to measure the performance of DRAIN. The first one evaluated DRAIN parameters, allowing us to understand how they affect the convergence from the probability estimates. The second series evaluated DRAIN and Epidemic strategies in scenarios where storage capacity is limited. Results showed that DRAIN presented considerable performance improvement, when compared to Epidemic routing. In the third series, DRAIN and Epidemic strategies were compared on scenarios where bandwidth is a constraint factor. Once again, DRAIN obtained better delivery results on all evaluated cases.

It was also noticeable that the percentage difference between DRAIN and Epidemic routing delivery rates increases as both storage capacity and bandwidth restrictions grow. When the buffer size is restricted, simulations results showed a 20% improvement with DRAIN. On the other hand, when the constraint is bandwidth, DRAIN delivery rates were more than 3 times better. It is important to notice that DRAIN was evaluated using random scenarios, which are not the best cases for the proposal. In scenarios with cyclical mobility patterns or ferry nodes, DRAIN would probably present even better results.

Future work includes a more complete evaluation of the estimates convergence and parameters sensibility, such as α, β, λ and ω, in scenarios showing ferries, college campus, VANETs (Vehicular Ad-hoc NETworks) with inter-vehicular communications (or Car-to-Car, C2C) and vehicle-roadside communications (or Car-to-Infrastructure, C2I), and with large networks. Both topics can be more deeply investigated, in order to allow scenario specific optimizations or a good generic configuration of DRAIN. The computational cost of DRAIN's priority rules also deserves further investigation, since they might become expensive as the number of packets increases. Still in this line, a possibility is to perform an individual evaluation of each one of DRAIN's rules and mechanisms. This way, it might be possible propose a less computationally expensive set of rules, but still achieving a good delivery rate.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, B. N. Levine, Maxprop: Routing for vehicle-based disruption-tolerant networks, in: Proceedings of IEEE Infocom, 2006.

[2] B. Burns, O. Brock, B. N. Levine, MV routing and capacity building in disruption tolerant networks, in: Proceedings of IEEE Infocom, 2005.

[3] T. Clausen, P. Jacquet, Optimized link state routing protocol (OLSR), RFC Experimental 3626, Internet Engineering Task Force (Oct. 2003).

[4] K. Fall, K. Varadhan, The ns manual, Tech. rep., UC Berkeley, LBL, USC/ISI, and Xerox PARC, available at http://www.isi.edu/nsnam/ns/ns-documentation.html (Apr. 2002).

[5] X. Hong, K. Xu, M. Gerla, Scalable routing protocols for mobile ad hoc networks, IEEE Network 16 (4) (2002) 11–21.

[6] S. Jain, K. Fall, R. Patra, Routing in a delay tolerant network, in: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM), 2004.

[7] D. B. Johnson, D. A. Maltz, Dynamic source routing in ad hoc wireless networks, in: Mobile Computing, Springer US, 1996, pp. 153–181.

[8] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, D. Rubenstein, Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet, SIGPLAN Not. 37 (10) (2002) 96–107.

[9] A. Lindgren, A. Doria, O. Schelén, Probabilistic routing in intermittently connected networks, SIGMOBILE Mob. Comput. Commun. Rev. 7 (3) (2003) 19–20.

[10] P. McDonald, D. Geraghty, I. Humphreys, S. Farrell, V. Cahill, Sensor network with delay tolerance (SeNDT), in: Proceedings of 16th International Conference on Computer Communications and Networks (ICCCN), 2007.

[11] M. Musolesi, S. Hailes, C. Mascolo, Adaptive routing for intermittently connected mobile ad hoc networks, in: Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM), 2005.

[12] C. E. Perkins, E. M. Belding-Royer, S. R. Das, Ad hoc on-demand distance vector (AODV) routing, RFC Experimental 3561, Internet Engineering Task Force (Jul. 2003).

[13] K. Tan, Q. Zhang, W. Zhu, Shortest path routing in partially connected ad hoc networks, in: IEEE Global Telecommunications Conference (GLOBECOM), 2003.

[14] A. Vahdat, D. Becker, Epidemic routing for partially connected ad hoc networks, Tech. Rep. CS-200006, Duke University (April 2000).

[15] Y. Wang, S. Jain, M. Martonosi, K. Fall, Erasure-coding based routing for opportunistic networks, in: Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking (WDTN), 2005.

[16] J. Widmer, J.-Y. L. Boudec, Network coding for efficient communication in extreme networks, in: Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking (WDTN), 2005.

[17] Z. Zhang, Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges, IEEE Communications Surveys & Tutorials 8 (1) (2006) 24–37.

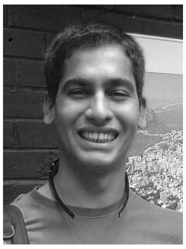
[18] W. Zhao, M. Ammar, E. Zegura, A message ferrying approach for data delivery in sparse mobile ad hoc networks, in: Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc), 2004.

[19] A. Balasubramanian, B. Levine, A. Venkataramani, DTN Routing as a Resource Allocation Problem, in: Proceedings ACM SIGCOMM, August, 2007.

[20] T. Spyropoulos, K. Psounis, C. Raghavendra, Single-copy routing in intermittently connected mobile networks, in: Proceeding of the IEEE Conf. Sensor and Ad Hoc Communications and Networks (SECON), 2004.

[21] R. Ramanathan, R. Hansen, P. Basu, R. Rosales-Hain, R. Krishnan, Prioritized epidemic routing for opportunistic networks, in: Proceedings of the 1st international MobiSys workshop on Mobile opportunistic networking - MobiOpp'07, 2007.

Diego Passos Diego Passos received the B.S. degree in computer science from Fluminense Federal University (UFF), Rio de Janeiro, Brazil, in 2007. Currently, he is a M.S. student at UFF. His major research interests are multihop wireless networks and wireless routing.



Henrique Bueno Henrique Bueno is a Systems Analyst at Petrobras and a M.Sc. candidate in the Department of Computer Science at Universidade Federal Fluminense (UFF). He also received a B.S. degree in Computer Science from UFF in 2006. Current research interests include middleware technologies for grid computing and service oriented architecture (SOA).

Etienne Oliveira Etienne C. R. de Oliveira received data processing degree from Anglo-American University in 1989, and M.Sc. degree in computer science from Fluminense Federal University (UFF), in 2006. Since 1986 he has been a researcher at Brazilian Institute of Geography and Statistics, and since 1998 he has been a professor at Unigranrio University. Currently, he is a D.Sc. student at Fluminense Federal University (UFF). His major research interests are delay-tolerant networks, multihop wireless networks, sensor networks, and wireless routing.

Célio Albuquerque Célio Albuquerque (S'94-M'00) received the B.S. and M.S. degrees in electrical and electronics engineering from Universidade Federal do Rio de Janeiro, Brazil, in 1993 and 1995, and the M.S. and Ph.D. degrees in information and computer science from the University of California at Irvine in 1997 and 2000, respectively. From 2000 to 2003, he served as the networking architect for Magis Networks, designing high-speed wireless medium access control. Since 2004 he has been an Associate Professor at the Computer Science Department of Universidade Federal Fluminense, Brazil. His research interests include Internet architectures and protocols, wireless networks, multicast and multimedia services, and traffic control mechanisms.