

Immunity-based Epidemic Routing in Intermittent Networks

Padma Mundur

Institute for Advanced Computer
Studies
University of Maryland
College Park, MD 20742
pmundur@umiacs.umd.edu

Matthew Seligman

Laboratory for Telecommunications
Sciences
8080 Greenmead Road
College Park, MD 20742
seligman@ltsnet.net

Jin Na Lee

Department of Electrical and
Computer Engineering
University of Maryland
College Park, MD 20742
jn1114@gmail.com

ABSTRACT – In this research, we propose to modify and extend epidemic routing used in intermittent networks. In particular, we propose to include immunity-based information disseminated in the reverse once messages get delivered to their destination. The goal is to design a more efficient routing protocol in terms of resource utilization. The idea is to analyze and evaluate the network performance using an immunity scheme in the context of epidemic routing and its variants. The reverse dissemination of such information requires minimal resources and the tradeoff in timely purging of delivered messages can be significant. We are using ns2 to implement a detailed simulation of the proposed immunity-based epidemic routing.

Keywords – Routing Protocols, Intermittent Networks, Partitioned Mobile ad hoc Networks, Delay Tolerant Networks

I. INTRODUCTION

In this poster proposal, we present details of work-in-progress on routing issues in an intermittent network like Delay Tolerant Networks (DTN) or Mobile Ad Hoc Networks (MANET) with partitions. Epidemic routing is a simple routing protocol used in such networks where mobility forms an integral part of the routing solution. In particular, we are focusing on implementing immunity-based reverse messaging in the context of epidemic routing and evaluating its performance effectiveness in increasing delivery ratio, decreasing delay and in-network storage requirements. The main contribution of this work is in developing a routing protocol with detailed performance evaluation using simulation and analytical modeling.

Epidemic routing at its simplest form will continue to exchange messages even well after the message is delivered to its destination. The algorithm results in every new node in contact that does not already possess the message receiving the message; with all nodes in the topology eventually receiving a copy. Several improvements are suggested for better resource utilization such as limits on the number of copies per

message or exchanging the message with only a subset of the nodes that satisfy some criteria such as number of visits to the destination node in the recent past. In this proposed work, we will investigate the impact of immunity concept which will prevent needless copying of the message once it gets delivered to its destination. Such immunity-based routing will have impact on storage utilization, delivery ratio, and delay. The algorithm is described in detail in the following sections.

II. BACKGROUND

The primary challenge for routing in DTNs is the dynamic topology of the network due to intermittent connectivity. DTN topology may consist of static and mobile nodes. The links between pairs of static nodes could be up or down, for instance through intentional duty cycling to conserve resources. If mobile nodes are involved, network topology changes as nodes move. In such a situation the link connectivity between pairs of nodes is brought about when they come into range of each other. Therefore, mobility causes intermittent connectivity. This by itself is not a problem if we can detect synchronous multi-hop paths between a source and a destination as we do in MANETs. In a DTN however, that is not the case because there is no assumption regarding node density to enable multi-hop paths.

The extent of topology knowledge is critical to the design of a routing algorithm. At one extreme, opportunistic contact between pairs of nodes is the only way for possible eventual delivery of data. Much of routing decision needs to be made using minimal topology knowledge, the extent of which could be that each node can detect only its neighbors and is unaware of the number and location of other nodes in the topology. At the other extreme, scheduled contact between nodes of known topology may lead to a possible asynchronous path between nodes for an eventual delivery. The challenge is to design routing algorithms that will

maximize delivery ratio and minimize delay where possible. The epidemic routing-based algorithms make the most use of opportunistic contact. For these algorithms the required topology knowledge is minimal. Uncontrolled mobility is an essential feature giving rise to opportunistic contact between mobile nodes.

With minimal or no topology knowledge the simplest delivery scheme is to copy the message to each node that the source and its relays come in contact with – this is the basic idea behind epidemic routing. This will result in a maximum of $(n-1)$ copies in a network of size n nodes, more if we allow multiple copies to exist within the same node. As is evident, this strategy consumes the most resources in a generally resource deprived network environment. Despite having a high per packet delivery probability and the lowest delay, the non-scalable nature of this solution demands limitations on replication. Variants of epidemic routing adopt limited replication trading delay for capacity. One of the following two strategies is used to limit replication in the existing algorithms: 1) fix the number of copies per message and disperse on contact with distinct relay nodes; 2) use historical encounter-based metrics to decide whether to copy the message on contact. These ideas are discussed in detail in the current literature. However, the concept of immunity as a technique to cut down the number of copies within the network for better resource utilization has not been given much attention. We focus on that aspect in this work.

III. PROPOSED ALGORITHM

In an epidemic routing algorithm the communication on node encounters is as follows: each node on encounter will exchange summary vectors of the messages they have. Comparing the two vectors, each node will determine the messages it does not have and send a request for those messages to the other node. This simple communication protocol needs to be modified to accommodate the immunity message exchange. The details of such a communication pattern are given in Table 1. Each node exchanges its message list, *m-list* and the immunity list, *i-list*. The immunity list contains message ids for those messages that are already delivered to its destination. Using the two lists, the individual nodes compile and exchange the message list they want from the other node. After receiving the payload, both nodes modify their m-list and i-list. At the end of a successful exchange, both nodes will have the same set of messages and their immunity lists match both of which will be used in a future encounter.

An alternative communication pattern is to involve only one node in the computation part of this exchange using *push-pull* logic. For example, Node A in Table 1 can compute messages it wants from Node B and also the messages it need to push to Node B. For this push-pull logic, Node A will request the *m* and *i* list from Node B. As payload, it will send the messages Node B requires and also a request for its own messages. On receiving the actual messages, the nodes can update their i-list. In this research, we will evaluate several such alternative proposals.

TABLE 1: Communication protocol on node encounters:

Node A	Node B
Messages: m-list: $A_m = \{WXYZ\}$	m-list: $B_m = \{XLMN\}$
Immunity: i-list: $A_i = \{M\}$	i-list: $B_i = \{Y\}$
Send and receive m-list and i-list; merge i-lists: $A_i = \{MY\}$	Send and receive m-list, i-list; merge i-lists: $B_i = \{MY\}$
Find messages to request from Node B: Step1: $A_r' = B_m - A_i = \{XLN\}$ (remove immunity messages from B_m); Step2: r-list $A_r = A_r' - A_m = \{LN\}$ (remove common messages)	Find messages to request from Node A: Step1: $B_r' = A_m - B_i = \{WXZ\}$ (remove immunity messages from A_m); Step2: $B_r = B_r' - B_m = \{WZ\}$ (remove common messages)
Request and receive new messages: $\{LN\}$; Send ACKs (optional)	Request and receive new messages: $\{WZ\}$; Send ACKs (optional)
Note L's destination is Node A; Note Z's destination is Node B. Add final destination messages to i-list (wait for ACKs before doing this): i-list: $A_i = \{MYLZ\}$	Note Z's destination is Node B; Note L's destination is Node A. Add final destination messages to i-list(wait for ACKs before doing this): i-list: $B_i = \{MYLZ\}$
New m-list: $A_m = \{WXN\}$	New m-list: $B_m = \{WXN\}$
New i-list: $A_i = \{MYLZ\}$	New i-list: $B_i = \{MYLZ\}$

Notation: for Node A (mirrors for Node B)

Message list, *m-list*: A_m

Immunity list, *i-list*: A_i

Message Request list (excludes immunity): A_r

Message Request list (excludes immunity and common messages), *r-list*: A_r

Summary of the interaction for the example above:

Node A has message X in common with Node B;

Node A does not want message M which Node B has and Node B does not want message Y which Node A has – this information comes from the immunity list each node has;

New messages for Node A from Node B are L and N found by comparing the message summary vectors and the immunity lists;

New messages for Node B from Node A are W and Z;

Message L's destination is Node A and Node B knows it; Message Z's destination is Node B and Node A knows it;

After the final exchange and after receiving ACKs, message ids for LZ are added to the immunity list on Node A and Node B with the final immunity lists on both nodes as being {MYLZ};

Message N is added to Node A with its new message list becoming {WXN} and W is added to Node B and its new message list the same as Node A's, for further transmission.

IV. SIMULATION

We are using the network simulation tool ns2 to implement the immunity-based epidemic routing protocol. The two specific scenarios of interest are proposed as follows:

1. Sensor networks with known repositories as destinations: in this scenario the traffic flow is from individual sensor nodes toward the repositories for all messages.

2. Conventional networks: in this scenario, we could have sources sending messages to randomly picked destinations.

The goal is to investigate the traffic flow dynamics in the two scenarios using various performance metrics. The delivery ratio and the delay are two metrics that are used to analyze the performance of the proposed routing algorithm.

With the immunity-based algorithm, we also want to quantify the network lifetime of a message once it is delivered to its destination and anti-packet information is disseminated. This will have implications on storage utilization in storage constrained networks, delivery ratio and the delay. The average number of copies within the network per message is another metric used to evaluate the effectiveness of immunity-based epidemic exchange.

The topology, node density, and the mobility pattern will govern connection opportunity and connection duration between nodes. If a randomized mobility pattern is used, analytical evaluation is possible in addition to a simulation analysis and we will work on

that. Associated with network related parameters, we have message related parameters such as TTL for both messages and their immunity packets to facilitate purging message lists for undeliverable messages and immunity lists for messages no longer in the network. Investigating an appropriate method to assign values for TTL is part of this work.

V. RELATED WORK AND CONTRIBUTION

The proposed work will have the following contribution: a new routing protocol based on the concept of immunity for epidemic routing in DTNs; a detailed performance evaluation using metrics such as delivery ratio, delay, lifetime per message before and after delivery with an analysis of the impact of topological factors such as node density, connection opportunities, connection duration on performance metrics.

Haas and Small [1] discussed the use of immunity in the context of their infostation model. They study the impact of deleting obsolete information on the networks nodes to reduce storage requirements. Their method is based on the use of Markov chains to compare five different storage deletion schemes. Other than this work, we are not aware of other works on this topic. Our proposed work relies heavily on simulation of detailed network scenarios to provide a comparative analysis of routing with and without immunity.

VI. REFERENCES

[1] Z. Haas and T. Small, A new networking model for biological applications of ad hoc sensor networks, IEEE/ACM Transactions on Networking, Vol. 14, Issue 1, February 2006.