

EPIDEMIC ROUTING WITH IMMUNITY IN DELAY TOLERANT 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

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

ABSTRACT

In this paper, we modify and extend epidemic routing used in intermittent networks such as Delay Tolerant Networks (DTNs). In particular, we propose to include immunity-based information disseminated in the reverse direction once messages get delivered to their destination. There are many variants of epidemic routing that are intended to result in better resource utilization by reducing the number of copies or through the use of sophisticated forwarding policy. Our focus is to use the information of already delivered messages in an immunity-list that will prevent any future exchange of those messages. Through the use of this technique we expect that the percent of delivered messages at lower delays will be higher because of better buffer and network utilization. Our simulation shows statistically significant performance improvement both in delivery ratio and delay for immunity-based epidemic as compared to the basic epidemic protocol.

I. INTRODUCTION

In this paper, we present a routing protocol that is a variant of the basic epidemic protocol 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. We propose including the information on delivered messages in the form an immunity-list that is exchanged on node encounters so that further exchange of those messages can be prevented. Just as we expect the source message to eventually reach the destination through intermediate node encounters in the basic epidemic protocol, we expect this immunity information to spread in the reverse direction from the destination through the network so that any copies of the delivered message are eliminated from further exchange.

Epidemic routing in 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 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. Percent of delivered messages at lower delays is expected to be higher because of better buffer and network utilization. Our simulation shows such performance improvement in the higher percentage of delivered messages and lower delays as compared to the basic epidemic protocol.

This paper is organized as follows. In Section 2, we provide a background on routing challenges in DTNs and performance aspect of the basic epidemic routing. In Section 3, we provide a brief description of related work and our contribution. In Section 4, we describe the proposed immunity-based epidemic protocol. Simulation setup and results are discussed in detail in Section 5. We conclude the paper in Section 6 with a discussion on future work.

II. BACKGROUND

The primary challenge for routing in DTNs is the dynamic topology of the network due to intermittent connectivity and therefore, the absence of an end-to-end path between source and destination for routing. 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 possible for 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 and 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 or other such rationale 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 reduce 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. RELATED WORK

The basic epidemic protocol we implement in this paper was first discussed in [1]. We adopt some of the same simulation parameters from this study so that we can reproduce their results in large part and compare them with the immunity-based protocol that we propose. Others have proposed variants of the basic epidemic protocol by limiting the number of copies as in [2] or using a forwarding policy based on historic or probabilistic metrics [3] that trade delay for capacity. The limited replication schemes sacrifice delay and try to make up for the deficit in

delivery ratio by better resource utilization. On the other hand, our immunity scheme retains the best feature of Epidemic which is to distribute as many copies as possible before delivery but to rid of the unwanted copies and unnecessary transmissions of the those copies by implementing immunity for delivered messages.

Haas and Small [4] discussed the use of immunity in the context of their infostation model which is more applicable in a sensor network where the message is generally dropped off at a few collection nodes. They study the impact of deleting obsolete information on the network nodes to reduce storage requirements. Their method is based on the use of Markov chains to compare different storage deletion schemes, all variants of the basic immunity concept such as, deleting the message on the delivered node and ignoring any future redundant deliveries, passing that delivered information to other nodes that may or may not carry that message so that they can delete it if they have it.

Another closely related work that is also based on analytical modeling is presented in [5] for the same epidemic and epidemic with immunity algorithms. Both of these works model the delivery delay and buffer occupancies which are relatively easy to obtain from Markov chain modeling as is done in [4] or using ordinary differential equations as in [5] with certain assumptions to reduce the complexity. In either works, simulation is used to collect statistics for their respective model parameters to derive delay and buffer occupancy. For instance, in [5] the simulation implements a number of flows among N nodes and collects statistics on 500 packets to verify the values from their analytical model. Neither of these models gives us an adequate picture of the operational analysis of a conventional network where the immunity-based epidemic protocol is implemented. For instance, what is the marginal improvement in delivery ratio using immunity for a given network environment? Our work here provides some answers to such operational questions. The proposed work relies heavily on simulation of detailed network scenarios implemented in ns2 to provide a comparative analysis of routing with and without immunity for epidemic algorithm. We first introduced the proposed immunity-based epidemic protocol in [6] in a poster presentation and expand on it here with detailed simulation results and analysis.

IV. PROPOSED ALGORITHM

In the basic 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 and the associated events are illustrated in Figure 1. Each node

exchanges its message list, *m-list* similar to the summary vector in [1] and the immunity list, *i-list* – both are lists of message-ids. The immunity list contains message ids for those messages that are already delivered to their 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 modified to show receiving messages intended for them as the final destination. This information will be used in future encounters. Figure 1 illustrates how a message moves from source to destination through pairwise encounters of nodes over time. Any attempted exchange of that message in future encounters once it has been delivered is prevented by the information on the i-list as seen from the last event in Figure 1.

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 needs 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 that are also destinations for some messages will update their i-list. Implementing ACKS will speed up the process of distributing the i-list because the sender now can modify its i-list at the same time as the receiving destination node. Both sender and the receiver destination node can then distribute the information on the i-list in future encounters with other nodes. In this paper, we have not implemented the ACKs and limit the modification of the i-list to the receiving destination node only (see Table 1).

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; Add final destination messages to i-list: i-list: $A_i = \{MYL\}$	Note Z's destination is Node B; Add final destination messages to i-list: i-list: $B_i = \{MYZ\}$
New m-list: $A_m = \{WXN\}$	New m-list: $B_m = \{WXN\}$
New i-list: $A_i = \{MYL\}$	New i-list: $B_i = \{MYZ\}$

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; Message Z's destination is Node B;
 After the final exchange, message ids for L and Z are added to the immunity list on Node A and Node B with the final immunity lists on both nodes as being {MYL} and {MYZ} respectively;
 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.

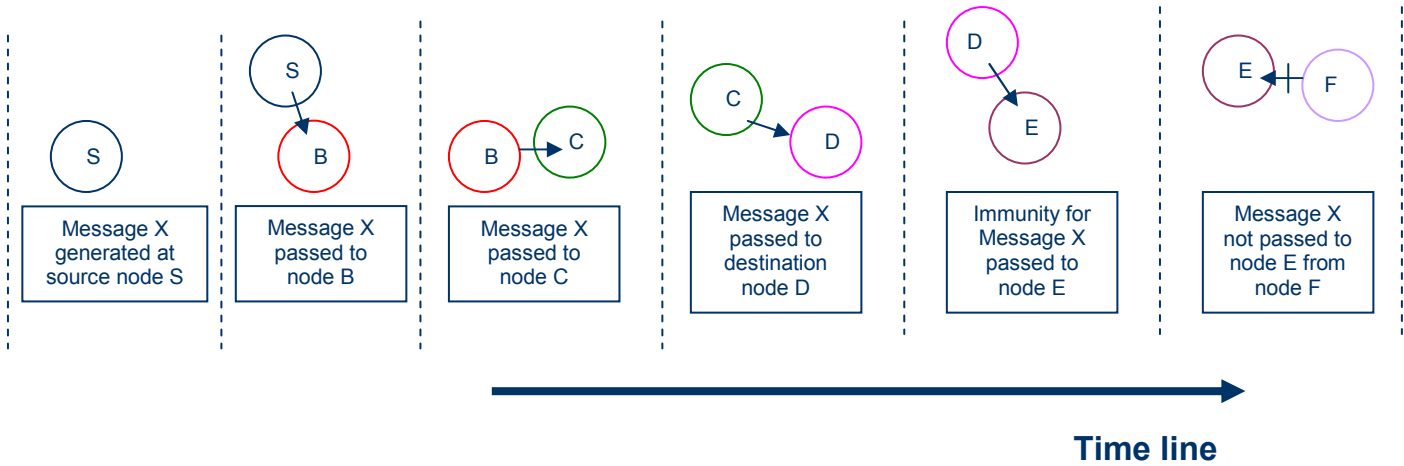


Figure 1. Sequence of events for a single message through pair-wise node encounters

V. SIMULATION

In this section we provide details of our simulation regarding the network environment, performance metrics, and results. The simulation tool we use is ns2. We implement both protocols, epidemic and immunity-based epidemic. The goal is to investigate the traffic flow dynamics in the two scenarios using various performance metrics for different traffic load and buffer capacities on nodes.

Network Model is based on conventional networks where each node acts as a source for generating the message and directing it to a randomly picked destination. The time interval between message generation on a node is modeled after exponential distribution. Mobility model is based on Random Waypoint (RWP) model. The same mobility pattern is used for comparing both basic epidemic and immunity protocols in a given scenario. The simulation results are valid for that reason despite the objections to RWP model in the research community. The total simulation time is 4000 seconds – traffic load shown on graphs in the number of messages generated (such as 500 or 1000 messages) is during the overall simulation time but they are generated using a Poisson distribution within the simulation. Other parameters related to network environment are given in Table 2. Most of the values used in this simulation for instance hop count at 4 or radio range at 50m are shown to give reasonable performance (above 60% delivery ratio) in the original epidemic implementation at [1] which is the reason we adopt those numbers here.

Table 2. Simulation Model Parameters

Number of nodes	50
Coverage area	1500m X 300m
Radio range	50m
Node speed	0-20 m/sec Uniform Distr.
Message length	1 KB
Hop count limit	4
Simulation time	4000 sec
Traffic load range	500 – 1000 messages
Buffer capacity range	1% to 10% of traffic load

A. Performance Metrics

Delivery ratio (DR) and the delay are two metrics that are used to analyze the performance of the proposed routing algorithm. The delivery ratio is defined as the ratio of the total number of delivered messages to the total number of messages generated during simulation time. The delay metric refers to average delay in seconds per message taking into consideration all delivered messages to their destination. Redundant deliveries for the same message are possible and are discounted in computing either the DR or the delay.

B. Performance Results

Figures 2 and 3 show the performance of epidemic and immunity-based epidemic protocols for varying buffer

capacities. On the x-axis, the buffer size is indicated as a percentage of the fixed traffic load in the number of messages. On the y-axis, the DR is plotted corresponding to each buffer capacity level. The widest gap in performance between the two protocols occurs between 2 - 4%. The performance conforms to expectation except at about 1% the marginal improvement with immunity is in fact higher for a 1000 message workload as compared to 500 which may seem counter-intuitive. But that can be explained by noting the increase in buffer capacity at 1% of 1000 messages which is 10 messages buffer capacity, twice as much as the 1% capacity at 500 messages workload. The results also indicate that about 10% buffer capacity is enough to achieve nearly 100% DR for both protocols. The relative advantage of the immunity-based protocol is seen through the buffer capacity range for workloads, 500 and 1000 messages.

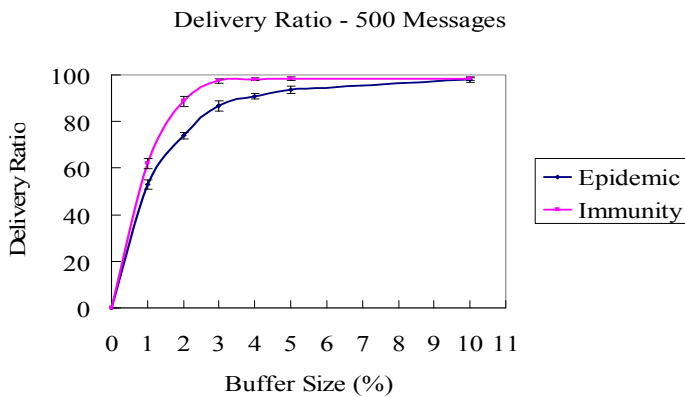


Figure 2. Delivery ratio for varying buffer capacities and fixed traffic load 500 messages

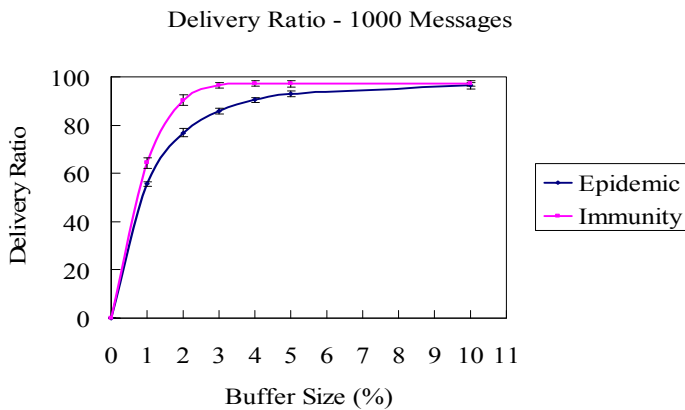


Figure 3. Delivery ratio for varying buffer capacities and fixed traffic load 1000 messages

In Figure 4, the results indicate that the relative performance improvement with the immunity-based protocol is maintained through the varying load. In fact, for the given network size in terms of number of nodes, and their mobility pattern, the most operational advantage is realized between loads of about 250 to 1000 messages.

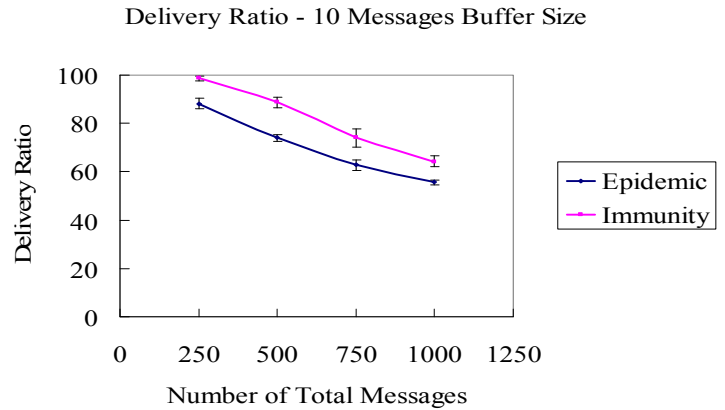


Figure 4. Delivery ratio for varying traffic load and fixed buffer capacity at 10 messages

In Figures 5-8, cumulative delay distribution for delivered messages is shown for scenarios of varying buffer capacities and traffic load. The percent of message delivered plotted on the y-axis is the ratio of the number of delivered messages to the total number of messages generated – therefore, each performance curve levels off at their maximum achievable DR. In the graphs presented, the cut-off shown is 500 seconds but a small percentage of messages in both protocols are delivered at longer than 500 seconds delay.

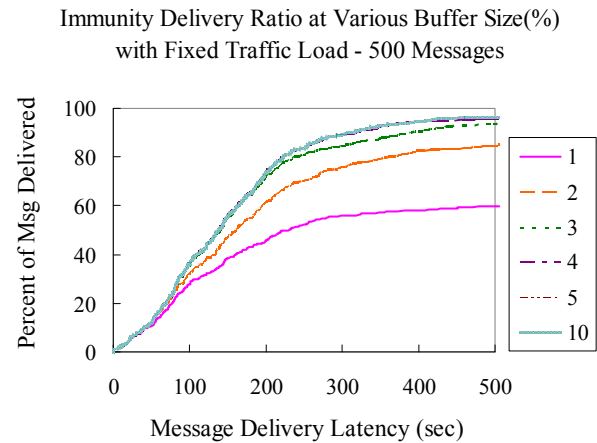


Figure 5. Immunity delay distribution for varying buffer sizes

The results follow the intuition that for lower workloads and higher buffer capacities, the percent of messages delivered with lower delay is higher for the immunity-based protocol. For instance, in Figure 5 with the immunity-based protocol more than 80 percent of delivered messages have 500 seconds or lower delay at 2% buffer capacity whereas for the epidemic protocol without immunity (see Figure 6), the percent delivered barely crosses 60% for the same delay. Similar explanation holds for the difference in performance between the two

protocols for varying traffic load as seen from Figures 7 and 8.

Epidemic Delivery Ratio at Various Buffer Size(%)
with Fixed Traffic Load - 500 Messages

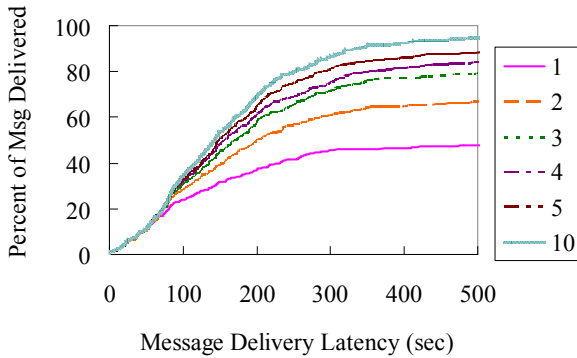


Figure 6. Epidemic delay distribution for varying buffers

Immunity Delivery Ratio Varying Traffic Load
at Fixed Buffer Size - 10 Messages

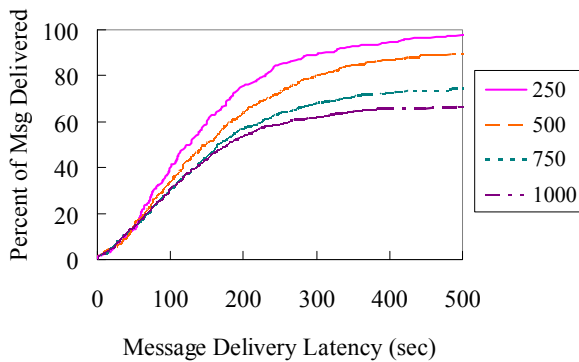


Figure 7. Immunity delay distribution for varying traffic

Epidemic Delivery Ratio Varying Traffic Load
at Fixed Buffer Size - 10 Messages

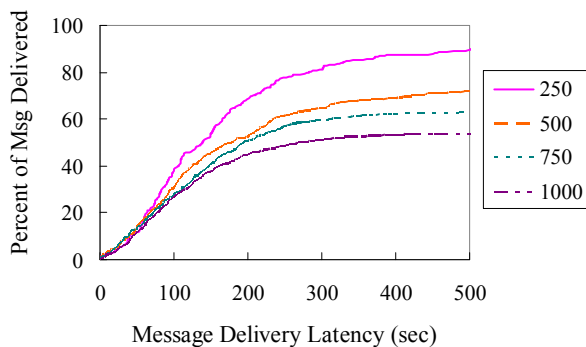


Figure 8. Epidemic delay distribution for varying traffic

In Figures 5 and 6, the bottom curve shows the performance for 1% buffer capacity and the top curve is for 10% with other capacities in between in consecutive order. Similar description goes for Figures 7 and 8, where the bottom curve shows the performance for the highest workload at 1000 messages and the top curve for 250 messages with others in between in consecutive order.

The head-to-head comparison between the two protocols is shown in Figures 9 and 10. In Figure 9, the delay performance of Immunity at 2% buffer capacity closely matches that of the Epidemic at 5% buffer capacity. The bottom curve indicates performance for Epidemic at 2% and the top curve for Immunity at 5%. In Figure 10, the delay performance of Immunity at workload 1000 messages closely matches that of Epidemic at 500 messages. The bottom curve shows performance for Epidemic at 1000 messages with the top curve showing performance for Immunity at 500 messages.

Delivery Ratio at Various Buffer Size(%)
with Fixed Traffic Load - 500 Messages

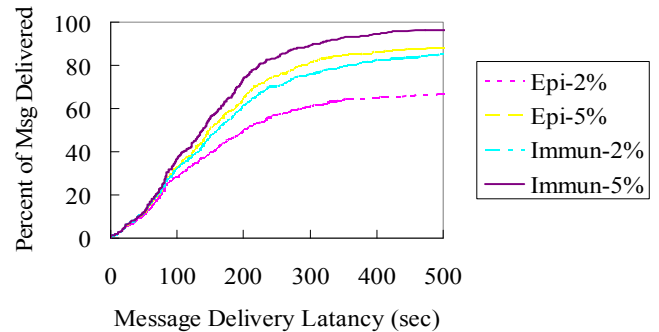


Figure 9. Immunity v. Epidemic delay distribution – varying buffer size

Delivery Ratio Varying Traffic Load
at Fixed Buffer Size - 10 Messages

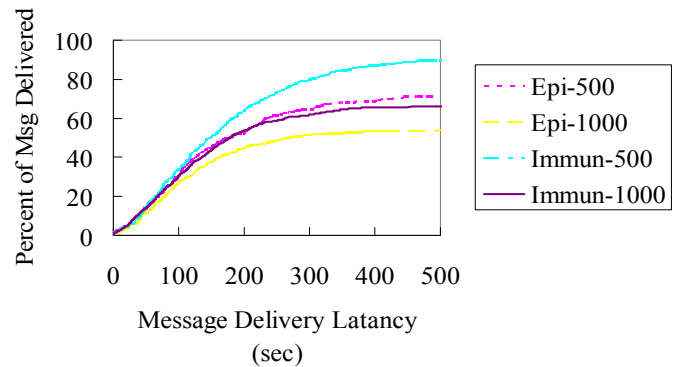


Figure 10 Immunity v. Epidemic delay distribution – varying traffic load

C. Summary of Results

All results discussed are average performance of their respective metrics collected over multiple runs of the simulation with statistically significant performance margins within 95% confidence intervals.

- Immunity protocol results about 15% increase in delivery ratio over Epidemic for the given network environment;
- About less than 5% buffer size results in more than 90% delivery ratio for the immunity protocol and close to that for the epidemic protocol;
- Immunity advantage is seen over a wide range of traffic load;
- Higher percent of messages delivered with lower latency under immunity protocols as seen from the delay distribution graphs. This applies to both situations of varying working loads and buffer capacities;
- The delay performance of Epidemic can be achieved at less than half the buffer capacity with Immunity for a fixed workload. The delay performance of Immunity at twice the workload is about the same as Epidemic for a given buffer size.

VI. CONCLUSION AND FUTURE WORK

In this work, we proposed an improvement over epidemic routing protocol that uses the idea of maintaining a list of delivered messages on each node, called the immunity list. On exchanging the immunity lists between two nodes, further dissemination of those messages is prevented in future node encounters. This is expected to increase the number of delivered messages due to improved buffer and network utilization. The performance improvement noted in the simulation verifies that claim. We have shown that a higher percentage of the total workload is delivered at lower delay under immunity-based protocol. The relative operational advantage with the immunity protocol holds for varying traffic load and buffer capacities. More than 90% of the maximum deliverable messages under each scenario experience 200 seconds or less delay under immunity-based protocol, resulting in about 30% improvement over the basic epidemic protocol.

The performance improvement we show is dependent on the number of nodes, radio range, buffer and hop count restrictions. It is possible *on average* in an ideal situation between the basic epidemic and the immunity-based epidemic protocols to have higher performance, sometimes as much as 25% based on a uniform distribution of copies and immunity information within the network. A rigorous sensitivity analysis using different network sizes, mobility

patterns will show the range of performance for both protocols. 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 these aspects in our future work.

The significance of the current work is that the immunity-based protocol retains the best feature of Epidemic namely, to distribute as many copies of the message as possible *before* delivery but rids of the unwanted copies and unnecessary transmissions by eliminating copies *after* delivery. To study the network dynamics before and after delivery, we have collected statistics on the average number of transmissions and message drops due to buffer overflow, and average number of copies per message. The network behavior in terms of these metrics shows that Immunity scheme retains more copies per message within the network before delivery than Epidemic and that in turn translates to better performance in delivery ratio. More copies per message is the result of better network and buffer utilization due to an accumulated advantage of getting rid of unnecessary transmissions and unwanted copies. In a future publication, we will present results related to network flow dynamics under our immunity-based protocol.

VII. REFERENCES

- [1] A. Vahdat, and D.Becker. Epidemic Routing for Partially Connected Ad Hoc Networks. *Technical Report CS-200006*, Duke University, 2000.
- [2] T. Spyropoulos, K. Psounis, and C. Raghavendra. Spray and Wait: Efficient Routing in Intermittently Connected Mobile Networks. *ACM SIGCOMM Workshop on Delay Tolerant Networks (WDTN)*, August 2005.
- [3] A. Lindgren, A. Doria, and O. Schelen. Probabilistic Routing in Intermittently Connected Networks. *SIGMOBILE Mobile Computing and Communications Review*, Vol. 7, No. 3, 2003.
- [4] 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.
- [5] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, Performance Modeling of Epidemic Routing, *Preprint submitted to Elsevier*, September 2007.
- [6] P. Mundur, M. Seligman, and J. (Ginnah) Lee, Immunity-based Epidemic Routing in Intermittent Networks, Poster presentation, *SECON*, June 2008.