

Inter-Domain Traffic Routing in Vehicular Delay Tolerant Networks

Farid Farahmand[§], Ankitkumar N. Patel[‡], Vasco Soares^{††}, Jason P. Jue[‡], and Joel J. P. C. Rodrigues^{††}

[§]Department of Engineering Science, Sonoma State University, Rohnert Park, CA 94928

[‡]Department of Computer Science The University of Texas at Dallas, Richardson, TX 75083

^{††}Instituto de Telecomunicações, NetGNA Group, Portugal

University of Beira Interior, Covilhã, Portugal

email: farid.farahmand@sonoma.edu, vasco.g.soares@ieee.org, apatel@utdallas.edu, jjue@utdallas.edu, joeljr@ieee.org

Abstract—In this paper, we consider the problem of dynamic inter-domain traffic routing between a VDTN and a non-DTN (e.g., Internet). The inter-domain traffic can be classified as inbound and outbound traffic. Our main contribution in this work is the introduction of several fault-tolerant routing algorithms for inbound and outbound traffic. Using simulations, we compare the performance of the proposed algorithms in terms of required resources, packet delivery time, and blocking probability.

Index Terms—Delay-Tolerant Network, Fault-Tolerant, Routing, Transit Networks.

I. INTRODUCTION

In the recent years, numerous studies have been dedicated to investigate Delay (or disruption) Tolerant Networking (DTN) architectures. Such architectures aim to provide more robust networks against long delays, channel disruptions, and limited or intermittent connections [1]. The key feature of DTN architecture is its store-and-forward paradigm, allowing the data to be stored until proper communications between nodes are established and data can be forwarded.

Vehicular-DTN (VDTN), also known as *transient network*, is an emerging class of DTN. The Vehicular DTN architecture exploits moving vehicles, called *mobile nodes*, (e.g., cars, buses, boats) to collect and deliver data between stationary nodes, called *terminals*. Terminal nodes with ISP connection are referred to as *gateways*. The physical interface between the ISP and the gateway can vary depending on the available technology, such as LAN line, satellite, etc.

The general approach of VDTN has been considered for various network environments suffering from intermittent communications and no end-to-end route between source and destination nodes. Consequently, VDTN has been proposed as an alternative solution for environments where little or no communication infrastructure can exist due to hostile surroundings or cost constraints. VDTN is also being studied as a possible low-cost solution to rapidly deploy alternative communication links when existing links (e.g., LAN or satellite links) have partially or fully failed in a particular region following a catastrophic event or a serious security breach [2].

In the past few years, various projects have studied design challenges in VDTN architecture. For example, in [3] the authors report on a successful implementation of a VDTN in a rural area with no communication infrastructure. In [4] the authors focus

on design and mobility patterns of mobile nodes in order to improve network performance. The DieselNet testbed is another attempt to implement VDTN and study its performance [5]. In the Message Ferry project [6] the performance impact of different node interactions in a transient network is studied. In [7] the authors investigate how to ensure reliable message transmission between nodes. Developing real applications such as web search in VDTN has been investigated in [8]. In [9] the authors propose separating data and control planes and transmitting data using free-space optical communication links, while wireless links are used for data control. In [10] the authors consider the impact of adding intermediate relay nodes to the VDTN architecture. Numerous studies have also examined the routing problem in VDTN. An excellent summary of various routing algorithms have been presented in [11]. An introduction to multicasting problem in delay tolerant networking has also been presented in [12]- [15] and a number of routing mechanisms are presented and compared in these studies. In [17] anycast semantics for DTN are analyzed.

With the exception of [14] and [15], in all the studies above, the authors have only focused on the *intra-domain traffic* within the same isolated region. In this paper, we study *inter-domain traffic* routing between a VDTN and a non-VDTN (e.g., Internet). The interconnection between the two networks can be provided by one or more gateways with ISP connections. The inter-domain traffic can be classified as *inbound* and *outbound* traffic. The main objective of this work is investigating a number of fault-tolerant anycast and multicast protocols for routing (1) the received Internet traffic by gateway nodes to the VDTN destination nodes (i.e., inbound traffic); (2) the VDTN traffic to any of the gateway nodes (i.e., outbound traffic). Thus, this work presents three specific contributions: (a) presenting a multicast scheme for inbound traffic; (b) presenting an anycast scheme for outbound traffic; and (c) implementing deflection routing scheme in the VDTN for outbound traffic.

In comparing our proposed routing algorithms, we focused on several performance aspects. First, we examine delay performance and resource efficiency in order to transmit anycast messages to the nearest member of a group of gateways. Second, we consider fault-tolerant ability of the routing algorithms to ensure reliable message delivery as one or more VDTN node failures occur. Fault-tolerant inter-domain traffic routing is an important issue in designing VDTN and we are not aware of any published work in this area. We note that our work is fundamentally different from

[14] and [15] in that we consider a different VDTN architecture and address inter-domain traffic routing when node failure occurs.

The remainder of this paper is structured as follow. In Section II, the network model and assumptions are described. In Section III, we describe the general inter-domain traffic problem. In Section IV, several routing approaches and message deflection policies for inbound and outbound traffic routing are presented. Section IV shows the performance comparison among the proposed heuristic algorithms under different network constraints. Finally, in Section V, we present our concluding remarks.

II. NETWORK MODEL AND ASSUMPTIONS

In our proposed VDTN network, a transportation system is utilized as the transport layer to deliver data. Hence, VDTN consists of vehicles (e.g., trains, buses) along predetermined *routes*. Each route passes along multiple terminals on the transportation system. Two or more routes may intersect at a terminal node.

A unique feature of VDTN architecture is its *bundle layer*. This layer is used as a new layer over the transportation system to aggregate incoming IP data packets into *bundle messages*, or *messages*, and to provide end-to-end message delivery.

In our proposed VDTN architecture, we define two distinct types of nodes: terminal nodes and mobile nodes. Architectural details of these nodes can be found in [16].

Terminal nodes are stationary nodes strategically located to support their surrounding users. Individual end-users are connected to terminal nodes through low-range low-power radio frequency signals, such as the IEEE 802.11 wireless protocol. A key function of a terminal node is to aggregate the incoming IP data packets to create bundle messages. Outgoing IP data packets between a terminal node and its surrounding end-users can be routed using commonly known protocols, such as dynamic source routing (DSR). Another important function of a terminal node is providing store-and-forward capability and acting as an intermediate forwarding node; hence, it can receive messages from mobile nodes and store them until the messages can be uploaded on another mobile node.

Gateway nodes are terminal nodes with ISP connection. Gateways are access points to VDTN. Hence, gateway nodes receive and aggregate the inbound IP packets destined to the same terminal nodes, and create a bundle message with a VDTN destination address. Similarly, gateway nodes receive the outbound bundle messages, extract IP packets and retransmit them toward the appropriate IP node. In the outbound direction, messages which carry inter-domain IP packets can be routed to any gateway node with ISP connection. Hence, an *anycast message* is the one that must be delivered to the *nearest* available member in a group of designated recipients (e.g., gateways) called *anycast group*. Similarly, in the inbound direction, an anycast IP packet can be routed to any gateway in the anycast group.

In the outbound direction, available gateway nodes register with stationary (and/or mobile) VDTN nodes, and the nodes send their inter-domain messages to outbound anycast group. Similarly, the anycast addressing in the inbound direction is essentially assigning a common address (i.e., IP address) to multiple gateways providing the same VDTN service, possibly located at different points in the global network. Thus, IP packets can

be forwarded to the nearest instance of anycast services using underlying routing infrastructure in the Internet.

The connections between gateway nodes and their ISP can be highly unreliable, with random up/down intervals. For example, a gateway node with satellite communications can potentially experience long down times depending on the service and environmental conditions. Furthermore, depending on their location, power line fluctuations, and maintenance schedules, terminal nodes may experience frequent failures. We note that a gateway node can loose its ISP connection, while it is still capable of receiving and forwarding bundle messages.

Mobile nodes are mounted on vehicles (e.g., buses) and act as store-carry-forward devices. It is assumed that message exchange between mobile nodes is not possible due to the short and infrequent *contact times* among mobile nodes (i.e., the time intervals during which the mobile nodes are within communication range) and the low data-rate that would be achieved. When a message is exchanged between a mobile and terminal node the receiver assumes *message custody* and will be in charge of appropriate and timely delivery of the message. In this paper we assume messages can be discarded and require retransmission when, for example, intermediate nodes are not available messages are expired. In our architecture, we also assume that mobile nodes are capable of message deflection. That is, if an intermediate node or the intended gateway node has failed, the mobile node can reroute the message according to some deflection policy, described later.

Another important function of mobile nodes is disseminating network status information between the terminal nodes. Status information includes performance metrics such as up/down times, average message delivery time between nodes, and buffer occupancy rate. Clearly, due to inherent message delay throughout the VDTN, node status information may not reflect the latest network condition.

III. PROBLEM DESCRIPTION

A vehicular delay tolerant network can be modeled by a directed graph $G_1(V_1, E_1)$. V_1 and E_1 represent the set of nodes and the set of directed links, respectively. V_1 includes the set of terminal nodes where the traffic can be originated and terminated, V_1^t . G_1 can be interconnected with other network graphs, say $G_2(V_2, E_2)$, via sets of gateway nodes, V_1^g and V_2^g , where $V_1^g \subseteq V_1$, $V_2^g \subseteq V_2$, and $V_1^g = V_2^g = V^g$. Clearly, $V_1^g \cup V_1^t \subseteq V_1$ and $V_2^g \cup V_2^t \subseteq V_2$. We assume Node g is an instance of an anycast service node V^g . We also assume the two graphs are *independent* and do not share any routing information with one another.

The inbound traffic is defined by node pair (s, d) , where $s \in V_2^t$ and $d \in V_1^t$. In case of outbound traffic, $s \in V_1^t$ and $d \in V_2^t$. The path between s and d consists of multiple directed links in VDTN and non-VDTN graphs, e.g., l_1 and l_2 . For example, for outbound traffic, a directed link l_1 exists when mobile nodes connects s to $g \in V^g$. A directed link l_2 , on the other hand, connects g to d on G_2 . This is depicted on Fig. 1(a) and (b). The node pairs (s, g) and (g, d) define the anycast traffic with g representing the nearest member in the anycast group, V^g .

We now define the general problem of routing anycast messages in VDTN. Given two independent networks interconnected by two or more gateway nodes, the anycast problem aims at finding the path with minimum delivery time among all deliverable links.

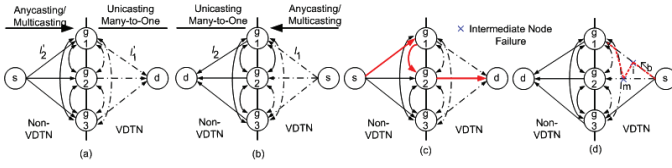


Fig. 1. A VDTN graph representing the (a) inbound routing and (b) outbound routing; (c) example of message passing in the inbound direction; (d) example of outbound message deflection in VDTN.

Minimizing the message delivery time in outbound direction between node pair (s, d) located on two separate networks, G_1 and G_2 , can be represented as follow: $\min D(s, d) = \min D_{G_1}(s, g) + \min D_{G_2}(g, d)$.

In the above expression, $g \in V^g, s \in V_1, d \in V_2$ and $\min D(i, j)$ denotes the minimum path delay between node pair (i, j) . If G_1 and G_2 represent a VDTN and a non-DTN network, respectively, since the total delay in VDTN is much larger, the expression above will be reduced to $\min D(s, d) = \min D_{G_1}(s, g)$.

IV. ROUTING HEURISTIC ALGORITHMS

As we mentioned before, the problem of supporting inter-domain traffic with multiple gateways connecting two heterogeneous domains can be divided into inbound and outbound traffic routing problems. In either case, the routing algorithm must address two basic operations: *gateway routing* and *message deflection*. In inter-domain traffic, gateway routing is based on multicasting or anycasting. Message deflection is referred to the mechanism in which the bundle message must be forwarded to another node when the intended intermediate node or gateway node are not operational. Such decisions may be made depending on the network status. We assume that VDTN nodes are stateful and network status is communicated between terminals via mobile nodes. However, due to inherently long delays in VDTN, status messages are not communicated in real-time and only long term statistical information may be available.

In the following paragraphs we first focus on gateway routing for inbound traffic and then we discuss outbound traffic routing. Finally, we elaborate on different message deflection policies.

A. Inbound Traffic Routing

In the inbound direction, the source is connected to the Internet and the destination node is a VDTN terminal node. We consider two routing schemes to transmit IP packets to the gateways: multicast routing and anycast routing. On the other hand, a message containing inter-traffic IP packets, can be routed to VDTN destination nodes from a single or multiple gateways. We refer to such routing approaches as unicasting or many-to-one-casting, respectively. In the following paragraphs we only focus on multicast/many-to-one routing and anycast/unicast routing approaches; we note that regardless of the way the message is routed in VDTN, different message deflection policies can be implemented when a node failure occurs:

- *Multicast/many-to-one routing (MUL-MTO)*: In this routing approach all gateways receive the packets intended for a terminal node. Thus, each gateway creates a bundle message

and independently forwards it toward the destination terminal. Consequently, the destination terminal receives multiple copies of each message, requiring to accept one and discard the rest. Referring to Fig. 1 (a), $s \rightarrow \{g1 \wedge g2 \wedge g3\} \rightarrow d$ will be an example of an inbound multicast/many-to-one routing.

- *Anycast/unicast routing (ANY-UNI)*: In anycast routing the nearest gateway to the source receives the IP packets and after aggregation and creating one or more messages, the gateway will forward the messages to the destination terminal node. In Fig. 1 (a), path $s \rightarrow g2 \in \{g1, g2, g3\} \rightarrow d$ will be an example of inbound anycast/unicast routing.

Regardless of the routing mechanism, before a message is passed on to a mobile node, it is necessary to check and make sure the node has sufficient buffering capacity. If not, the message delivery must be deferred to the next mobile node arrival along the designated route.

It must be noted that gateways can communicate with one another on the non-VDTN level in order to exchange status information and IP packets. For example, referring to Fig. 1 (c), assume node $g1$ receives IP packets and stores them until link $g1 \rightarrow d$ becomes available. Meanwhile, if $g2 \rightarrow d$ becomes available, Node $g2$ advertises the status of its links to the entire anycast group, e.i., other gateways. By calculating and comparing the shortest paths between $g1 \rightarrow d$ and $g2 \rightarrow d$, $g1$ decides whether to hand the packets to $g2$ or not. If Node $g2$ accepts such transaction, it will receive the IP packets, recreate the message, and become responsible for delivering the message to the next VDTN hop. We refer to such exchange as *message passing* between gateways.

B. Outbound Traffic Routing

Message routing in the outbound direction can also be based on anycasting or multicasting. Hence, various routing combinations can be considered. Our focus in this subsection, however, is anycast message routing in VDTN. We introduce two anycast routing heuristic algorithms for VDTN. These algorithms differ in the way they assign a gateway node address to the message when node failure occurs.

1) *Hard assignment*: In this case, the VDTN source node assigns one of the anycast group members (e.g., gateway) g to the inter-domain messages according to some cost function (e.g., minimum delivery time) based on the latest available status information, as described in Section II. Hence, the message is scheduled to be delivered by a specific mobile node. When the link becomes available (e.g., the specified mobile node arrives), its capacity must be checked for sufficient storage availability. If the mobile node is unable to pick up the message, message delivery is delayed until the next mobile node with the same route arrives. Otherwise, the message is passed on and its custody is given to the mobile node.

At the time of handing the message to an intermediate node, m , it is possible that m is not available due to lack of sufficient storage or hardware failure. In this case, the mobile node evaluates other possible paths to the assigned gateway g according to the message deflection policy. The mobile node will discard the message if no other path exists to the gateway or the gateway is experiencing hardware failure. A potential issue with HA is the

possibility of message *looping* in the network due to unpredictable node failures. A simple approach to limit message looping is to impose an upper bound on the number of hops a message can visit.

2) *Soft assignment*: The main difference between Soft assignment (SA) and HA is that in SA if the gateway is not available at the time of message arrival, the mobile node will calculate the routes to all anycast group members and determine an alternative gateway for the message according to the message deflection policy. The main advantage of SA over HA is that it considers paths to all other gateway nodes prior to discarding the message. Our motivation in proposing SA, is to study VDTN performance with a simple architectural modification.

In the next subsection, we describe the message deflection policy in the context of anycast routing problem for inter-domain traffic in VDTN. We note that in general, message deflection can be implemented for both outbound and inbound traffic. However, in this work we focus on outbound traffic deflection. For simplicity, we only consider terminal node failures.

C. Message Deflection Policy (MDP)

Upon detecting an unavailable node (intermediate or gateway), the mobile node calculates all possible routes from any terminal node along its path to the intended gateway node according to some cost function. Fig. 1 (d) shows how the outbound message is deflected when the intermediate nodes along paths $\Upsilon(s, g_1)$ and $\Upsilon(s, g_2)$ become unavailable and the message must be deflected from the original path. We consider two cost objectives for message deflection:

- *Minimizing total delivery time (TDT)*: The mobile node calculates the minimum path delay from any other reachable node along its path and the intended gateway and delivers the message to the appropriate next hop. For example, in Fig. 1(d), when Node i becomes unavailable, mobile node b calculates Node m on its path as the next hop.
- *Minimizing path failure probability (PFP)*: The mobile node calculates an alternative route with the highest probability of delivery from any other reachable node along its path to the intended gateway. Recall that each terminal node receives information about down/up times of other nodes in the network. Thus, the probability of hardware failure for a node m at any given time t , $P_m(t)$, can be calculated over a discrete window size W ranging from $t - W$ to t by summing all down periods and dividing it by W . Hence, the node failure probability due to hardware failure (e.g., power fluctuation) along the path, $\Upsilon(i, j)$, connecting node pair (i, j) , at any given time t , can be computed by $P_{i,j}(t) = 1 - \prod_{m \in \Upsilon(i,j), m \neq i} (1 - P_m(t))$.

V. PERFORMANCE ANALYSIS

This section compares the performance of the aforementioned anycast and multicast routing algorithms for inter-domain traffic. VDTN graphs, as defined in Section III, are randomly generated by uniformly distributing N nodes in a $20 \times 20 \text{ km}^2$ geographical area. The probability of establishing a link between a node pair is uniform. The network connectivity is given by *connectivity factor* (K), indicating the percentage ratio of established links over the

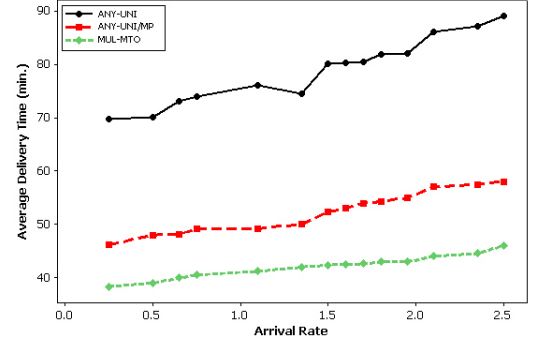


Fig. 2. Average message delivery time.

number of links in a fully connected network (i.e., $N(N-1)/2$). For each topology as many as $\lceil N/5 \rceil$ nodes were selected to perform as gateway nodes. The number of generated network topologies is sufficient to guarantee a confidence interval of 15% or better at 90% confidence level.

In our study, we only consider inter-domain traffic requests, which are dynamically generated. We assume the traffic is uniformly distributed among all terminal and gateway node pairs. Furthermore, the mobile node buffers are limited and their schedules are fixed and known to all VDTN nodes. We assume that the requests arrive to the network with Poisson distribution with arrival rate λ .

In addition, for simplicity, we assume that all stationary nodes have the same probability of hardware failure, P , and the failure time of the node is Geometrically distributed with probability $P=0.05$. In this work, we assume node hardware failure does not impact messages that are already stored the node, since messages are saved in secondary memory devices.

It is assumed that mobile nodes (e.g., buses) in the VDTN move at a speed of 40 km/hr and have a transmission range of 10 m . Also, the average time spent by a message along each given link (including the waiting time and transport time) is known in advance. Unless otherwise indicated, the following assumptions are made: $N = 15$, $K = 14$. Transmission bandwidth is assumed to be unlimited. We also assume that message bundle fragmentation is not allowed.

We first examine the proposed inbound routing algorithms, namely, ANY-UNI and MUL-MTO routing mechanisms. Fig. 2 shows that multicast routing offers considerably shorter average message delivery time. This figure also suggests that message passing can significantly improve average message delivery time in ANY-UNI. Further simulation results, not shown here, indicate that as the number of gateway nodes increases, message passing between gateways can further improve the average message delivery time.

We now examine the results obtained for outbound traffic using HA and SA. First, we only consider the TDT deflection policy and assume terminal nodes have limited buffer capacity. Fig. 3 (a) and (b) show message blocking probability and average delivery time, respectively. As expected, HA results in higher blocking probability and lower average delivery time. Recall that message blocking can occur due to limited storage, hardware failure, exceeding maximum allowable hop count, or finding no path to

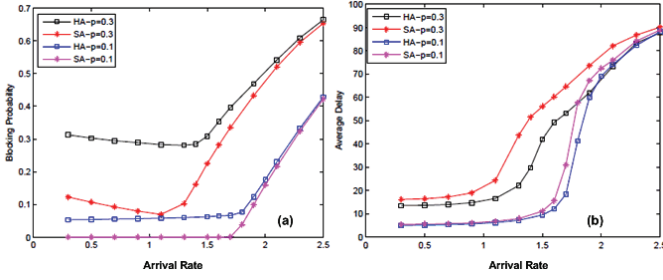


Fig. 3. Outbound routing using HA and SA for $P = 0.1, 0.3$: (a) blocking probability v.s λ ; (b) average delivery time in minutes v.s λ .

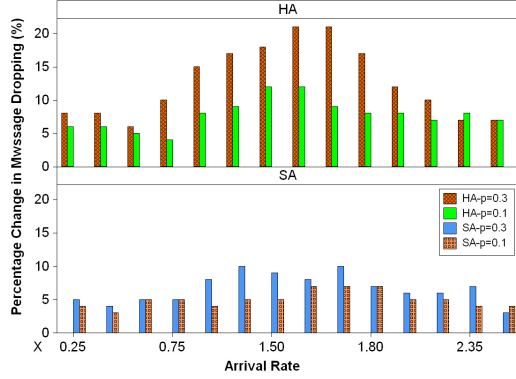


Fig. 4. Percentage change in HA/SA message dropping probability when PFP message deflection policy is utilized instead of TDT. Positive change indicates improvement.

the gateway node.

In contrast to HA, SA routing algorithm considers all available gateways for delivery, thus, resulting in lower overall message dropping. Fig. 3 (a) and (b) also suggest that as node hardware failure probability increases and nodes become less reliable, the difference between HA and SA becomes more significant at low arrival rates. Our results show that as the arrival rate increases, the difference between HA and SA performance becomes less significant.

Our results (not shown here) also indicate that as the arrival rate becomes larger, the mobile node buffer size becomes dominant. Consequently, the terminal buffer requirement becomes less important. In fact, when the node probability of failure is high ($P = 0.3$), SA requires higher total buffer requirement compared to HA. This is because, on average, using SA routing, messages will travel more hops.

Fig. 4 shows the percentage improvement in HA message blocking probability when PFP message deflection policy is utilized in place of TDT as node failure occurs. Note that we only consider the outbound traffic. This figure suggests that at moderate arrival rates, PFP can significantly improve average message delivery time, particularly, if the node failure probability is high (e.g., $P = 0.3$). This is because PFP attempts to select the alternative path to the intended gateway with the minimum probability of failure. Note that as the arrival rate increases, the performance of TDT and PFP becomes almost the same.

VI. CONCLUSIONS

we considered the problem of dynamic inter-domain traffic routing in vehicular delay tolerant networks (VDTN). For inbound inter-domain traffic we compared anycast and multicast routing in terms of message delivery and buffer requirement. We showed that message passing between gateways can improve average message delivery time in VDTN. We also introduced two message deflection routing algorithms and showed that under different failure scenarios, these algorithms can significantly improve network performance.

ACKNOWLEDGMENTS

This work was supported in part by the Instituto de Telecomunicações, Next Generation Networks and Applications Group (NetGNA), Covilhã Delegation, Portugal in the framework of the VDTN@Lab Project.

REFERENCES

- [1] DARPA ATO, "Disruption Tolerant Networking," <http://www.darpa.mil/ato/solicit/DTN>.
- [2] F. Farahmand, "Applications of Vehicular Delay Tolerant Networks," Central Connecticut State University, Technical Report, 2008.
- [3] A. Pentland, R. Fletcher, and A. Hasson, "Daknet: Rethinking connectivity in developing nations," *IEEE Computer*, Vol. 37, No. 1, pp. 7883, 2004.
- [4] A. Seth, D. Krocker, M. Zaharia, S. Guo, S. Keshav, "Low-cost communication for rural internet kiosks using mechanical backhaul," *Proceedings of the 12th annual international conference*, 2006.
- [5] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks," In *Proc. IEEE INFOCOM*, April 2006.
- [6] W. Zhao and M. H. Ammar, "Message ferrying: proactive routing in highly-partitioned wireless ad hoc networks," In *proceedings of the IEEE Workshop on Future Trends in Distributed Computing Systems*, Puerto Rico, May 2003.
- [7] K. Fall, W. Hong, and S. Madden, "Custody transfer for reliable delivery in delay tolerant networks," Technical Report, Intel Research, Berkeley, IRB-TR-03-030, 2003.
- [8] A. Balasubramanian, Y. Zhou, W. B. Croft, B. N. Levine, Aruna Venkataramani, "Web search from a bus," *Proceedings of the second ACM workshop on Challenged networks*, September 14-14, 2007, Montreal, Quebec, Canada.
- [9] R.A. Nichols, D.J. Tebben, A. Dwivedi, "Delay Tolerant Networking for free-space optical communication systems," *Sarnoff Symposium, 2007 IEEE* Volume , Issue , April 30 2007-May 2 2007 Page(s):1 - 5
- [10] F. Farahmand, et al., "Vehicular Wireless Burst Switching Network: Enhancing Rural Connectivity," The 3rd IEEE Workshop on Automotive Networking and Applications (AutoNet 2008) Co-located with *IEEE GLOBECOM* 2008.
- [11] Z. Zhang, "Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges," *IEEE Communications Surveys and Tutorials*, Vol. 8, No. 1, pp. 24-37, 2006.
- [12] W. Zhao, M. Ammar, E. Zegura, "Multicasting in delay tolerant networks: semantic models and routing algorithms," *Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, p.268-275, August 26-26, 2005, Philadelphia, Pennsylvania, USA.
- [13] Q. Ye, L. Cheng, M. Chuah, and B. Davison, "OS-multicast: On-demand Situation-aware Multicasting in Disruption Tolerant Networks", *Proceedings of IEEE 63rd VTC*, Vol. 1, pp. 96-100, Melbourne, Australia, May 2006.
- [14] Q. Ye, L. Cheng, M. Chuah, B. Davison, "SHIM: A Scalable Hierarchical Interdomain Multicast Approach for Disruption Tolerant Networks", *IEEE International Wireless Communications and Mobile Computing Workshop (IWCMC)*, Oct, 2007.
- [15] H. Samuel, W. Zhuang, and B. Preiss, "DTN based dominating set routing for MANET in heterogeneous wireless networking," *ACM Mobile Networks and Applications (MONET)*, vol. 14, no. 2, pp. 154-164, April 2009.
- [16] F. Farahmand, et al., "Node Placement in Vehicular Wire Delay-Tolerant Networks," *IEEE Globecom*, New Orleans, LA, USA, 2008.
- [17] Y. Gong et al., "Anycast routing in delay tolerant networks", *IEEE GLOBECOM*, November 2006.