22nd International Conference on Advanced Information Networking and Applications - Workshops

A Survey of Opportunistic Networks

Chung-Ming Huang, Kun-chan Lan and Chang-Zhou Tsai
Department of Computer Science and Information Engineering,
National Cheng Kung University, Tainan, Taiwan, R.O.C.
E-mail: huangcm@locust.csie.ncku.edu.tw

***Abstract*— We define an opportunistic network as one type of challenged networks where network contacts are intermittent or where link performance is highly variable or extreme. In such a network, there does not exist a complete path from source to destination for most of the time. In addition, the path can be highly unstable and may change or break quickly. Therefore, in order to make communication possible in an opportunistic network, the intermediate nodes may take custody of data during the blackout and forward it when the connectivity resumes. In this paper, we discuss some research challenges in an opportunistic network.**

I. INTRODUCTION

We consider an opportunistic network as a subclass of Delay-Tolerant Network where communication opportunities (contacts) are intermittent, so an end-to-end path between the source and the destination may never exist. The link performance in an opportunistic network is typically highly variable or extreme. Therefore, TCP/IP protocol will break in this kind of environment because an end-to-end path between the source and the destination may only exist for a brief and unpredictable period of time. Long propagation and variable queuing delays might be introduced and many Internet protocols which are designed to assume quick return of acknowledgements and data can fail to work in such networks. One possible solution to resolve the above issues is to exploits node mobility and local forwarding in order to transfer data. Data can be stored and carried by taking advantage of node mobility and then forwarded during opportunistic contacts. Here entire chunks of message are transferred from one storage place to a storage place in another node along a path that is expected to reach the destination.

The applications of opportunistic network is typically used in an environment that is tolerant of long delay and high error rate. For example, Sami Network Connectivity (SNC) Project [1] focuses on establishing Internet communication for Sami population of reindeer herders who live in remote areas. In Zebranet [2], the researchers used a opportunistic network to track the wild zebras.

II. AN OVERVIEW OF OPPORTUNISTIC NETWORKS

A. Architecture

In an opportunistic network, a network is typically separated into several network partitions called regions. Traditional applications are not suitable for this kind of environment because they normally assume that the end-to-end connection must exist from the source to the destination. The opportunistic network enables the devices in different regions to interconnect by operating message in a store-carry-forward fashion. The intermediate nodes implement the store-carry-forward message switching mechanism by overlaying a new protocol layer, called the bundle layer, on top of heterogeneous region-specific lower layers [3], [4], as shown in Figure1. In an opportunistic network, each node is an entity with a bundle layer which can act as a host, a router or a gateway. When the node acts as a router, the bundle layer can store, carry and forward the entire bundles (or bundle fragments) between the nodes in the same region. On the other hand, the bundle layer of gateway is used to transfer messages across different regions, as shown in Figure1. A gateway can forward bundles between two or more regions and may optionally be a host, so it must have persistent storage and support custody transfers.

<table>
<tr><td colspan="2">Application Layer</td></tr>
<tr><td colspan="2">Bundle Layer</td></tr>
<tr><td>Transport
Layer A</td><td>Transport
Layer B</td></tr>
<tr><td>Network
Layer A</td><td>Network
Layer B</td></tr>
<tr><td>Link
Layer A</td><td>Link
Layer B</td></tr>
<tr><td>Physical
Layer A</td><td>Physical
Layer B</td></tr>
</table>

Fig. 1. The protocol stack

B. Challenges

In an opportunistic network, when nodes move away or turn off their power to conserve energy, links may be disrupted or shut down periodically. These events result in intermittent connectivity. When there is no path existing between the source and the destination, the network partition occurs. Therefore, nodes need to communicate with each other via opportunistic contacts through store-carry-forward operation. In this section, we consider two specific challenges in an opportunistic network: the contact opportunity and the node storage.

1) Contact: Due to the node mobility or the dynamics of wireless channel, a node Might make contact with other nodes at an unpredicted time. Since contacts between nodes are hardly predictable, they must be exploited opportunistically for exchanging messages between some nodes that can move between remote fragments of the network. Burns et. al.[5] classified the routing methods for opportunistic network based on characteristics of participants' movement patterns. The patterns are classified according to two independent properties: their inherent structure and their adaptiveness to the demand in the

978-0-7695-3096-3/08 $25.00 © 2008 IEEE
DOI 10.1109/WAINA.2008.292

network. Other approaches proposed message ferries to provide communication service for nodes in the deployment areas [6], [7], [8], [9] In addition, the contact capacity needs to be considered. In other words, how much data can be transferred between two nodes when they are in contact with each other? Hui et. al. [10] define two parameters, contact duration and inter-contact time, that are important parameters in determining the capacity of the an opportunistic network.

2) Storage constraint: As described above, to avoid dropping packets, the intermediate nodes are requires to have enough storage to store all messages for an unpredictable period of time until next contact occurs. In other words, the required storage space increases a function of the number of messages in the network. Therefore, The routing and replication strategies must take the storage constraint into consideration. Vahdat and Becker[11] used Epidemic Routing by flooding the network to exploit the best possible delivery delay brought by mobility. This scheme achieves the optimal delay with unlimited relay buffers. However, such a multiple-copy scheme generally incurs significant overhead on storage constraint. Ip et. al.[12] proposed a buffer-management strategy, RRFS-with-RandomDrop, to avoid head-of-line blocking in the FIFO case. They showed that the proposed strategy can reduce the degradation of average delivery delay performance.

III. NETWORK LAYER

In this section, we discuss some routing solutions for an opportunistic network. Based on the number of copies of a message forwarded by the node, we can define two different routing schemes: forwarding-based (single copy) approach and flooding-based (multiple copies) approach. In the forwarding-based approach, there is only one single custodian for each message to help forwarding the message to destination. When the current custodian forwards the copy to an appropriate next-hop neighbor, this neighbors becomes the message's new custodian. The same process is repeated again and again until the message finally reaches its destination. This approach tries to reduce the buffer usages and the number of message transferred in the network. But it may suffer long delays and low delivery ratios. On the other hand, flooding-based approach may generate multiple copies of the same message. Each message can be routed independently for increased efficiency and robustness. This approach achieves lower delays and higher delivery ratio at the cost of a larger buffer space and more message transfers.

A. Forwarding-based approach

In the forwarding-based scheme, based on what type of knowledge nodes use to select the appropriate or the best path to destination node, the prior studies can be classified into three categories: direct-transmission, location-based and estimation-based.

1) Direct-transmission: Spyropoulos et. al. [13] proposed a simple single-copy routing called direct transmission routing. In this approach, after the source node generates a message, the message is hold by the source node until it reaches the destination node. The main advantage of this scheme is that it incurs minimum data transfers for message deliveries. On the other hand, although having minimal overhead, this scheme may incur very long delays for message delivery since the delivery delay for this scheme is unbounded [14].

2) Location-based: In the location-based approach, nodes will choose the neighbors who are closest to the destination to pass the message. LeBrun et al. [15] proposed a method using the motion vector (MoVe) of mobile nodes to predict their future location. The MoVe scheme uses the knowledge of relative velocities of a node and its neighboring nodes to predict the closest distance between two nodes. After the nodes future location are calculated, messages are passed nodes that are moving closer to the destination. As compared to epidemic routing, this approach has less control packet overhead and buffer usage. Leguay et al. [16] presented a strategy that uses a virtual coordinate routing called mobility pattern spaces (MobySpace). The measure of closeness represents the probability that the nodes will come into contact with each other. They showed that this approach consumes less resources than epidemic routing.

3) Knowledge-based: In the knowledge-based approaches, based on certain knowledge about the network, the source and intermediate nodes decide which node to forward the messages as well as whether it should transmit the message immediately or hold the message until it meets a better node. Jain et al. [17] proposed a knowledge-based routing scheme which is the first study in this area. Depending on the amount of knowledge about network topology characteristics and traffic demand, they define four knowledge oracles. Each oracle presents some particular knowledge of network. Based on the available oracles, the authors present a corresponding routing algorithm. The basic idea of their routing algorithms is to apply the traditional shortest path routing techniques to opportunistic network by exploiting the knowledge oracles. At the same time, they use the source routing to forward the message over the shortest path. This scheme formulates the routing in order to minimize the end-to-end delivery latency.

Musolesi et al. [18] present the Context-Aware Routing (CAR) protocol that provides an asynchronous communication for message delivery. In an opportunistic network, since the receiver is often not in the same connected network, synchronous delivery of messages is typically not possible. In CAR, if a message cannot be delivered synchronously, the message is sent to a host that has the highest probability of successful delivery and acts as a message carrier. The delivery probability process is based on the evaluation and prediction of context information using Kalman filters. The prediction process is used during temporary disconnection and the process is continued until it is possible to guarantee a certain accuracy. They showed in their simulations that if the buffer size is small, the packet delivery ratio of CAR is better than that of epidemic routing due to that CAR only creates a single copy for each message.

Burgess et al. [19] proposed a protocol called MaxProp for effective routing of messages. A node uses MaxProp to schedule packets transmission to its peers and determines which packets should be deleted when buffer space is almost full. Packets are scheduled based on the path likelihoods to peers according to historical data. In addition, several complementary mechanisms, including acknowledgments, a head-start for new packets, and lists of previous intermediaries are used in this approach. They showed that their approach performs better than the protocols that have access to an oracle [17] that knows the schedule of meetings between peers.

Kun et al. [20] proposed a shortest expected path routing (SEPR) similar to link-state routing to maintain a topology map to each other. SEPR first estimates the link forwarding probability based on history data. When two nodes meet, they exchange the link probability update messages called effective path length (EPL). A smaller EPL value suggests a higher probability of delivery. When a node received a smaller EPL, it will update its local EPL value. EPL is also used in deciding which nodes to forward the messages. Using SEPR protocol, the same message could be forwarded to multiple nodes to increase reliability and to reduce delay.

B. *Flooding-based approach*

In the flooding-based approach, every node broadcasts the received packet to all of its neighbors. However, in an intermittently connected network, some nodes might not be able to receive the broadcast packets due to network partitions. Therefore, each node stores the messages until the messages finally arrive the destination.

1) Epidemic routing: Epidemic routing is first proposed by Vahdat and Becker [11] for forwarding data in an opportunistic network. Epidemic routing utilizes the epidemic algorithm [21] that was originally proposed for synchronizing replicated databases. The epidemic algorithm ensures that a sufficient number of random exchanges of data in the network and guarantees all nodes will eventually receive all messages. The Epidemic Routing is similar to the flooding routing because it tries to send each message to all nodes in the network. For this reason, Epidemic Routing incurs significant demand on both bandwidth and buffer. To reduce such overhead, there are many related paper to make epidemic routing consume fewer resources [22], [5], [23], [19], [20]. To bound the overhead of delivering a message, Spyropoulos et al. [22] proposed a technique called Spray and Wait to control the level of flooding. In the spray phase, there are L number of copies that are initially spread over the network by the source node or other nodes to L distinct relays. In the wait phase, if the destination was not found during the spray phase, each node who has a copy of message will perform direct transmission. Binary spray and wait is a variation of Spray and Wait and produces a better performance. In this approach, the binary spray source node send half of the copies of the message to the new relay node, and keeps the rest to itself. The source node and relay nodes uses repeat this procedure until there is only one copy left. When it is only one copy left, it switches to direct transmission.

2) Estimate/Prediction routing: In Estimate/Prediction routing, nodes do not blindly forward the messages to all or some neighbors. Instead, nodes estimate the probability of each link to destination and use this information to decide whether it should store the packet and wait for a better chance as well as to decide which nodes to forward.

Lindgren et al. [23] proposed a probabilistic routing protocol, called PROPHET (Probabilistic Routing Protocol using History of Encounters and Transitivity). PROPHET estimates a probabilistic metric called delivery predictability. This metric indicates the probability of successfully delivering a message to the destination from the local node. PROPHET operates in a similar way as the Epidemic Routing [11]. When two nodes meet, they exchange summary vectors containing the delivery predictability vector which is based on the delivery predictability information. In theory, if two nodes are often encountered, they have high delivery predictability to each other. On the other hand, if a pair of nodes do not encounter each other in a while, they are intuitively not good forwarders of messages to each other. Hence, the delivery predictability values must age (i.e. be reduced) as the time goes. They showed in their simulation results that the communication overhead of PROPHET is lower than that of Epidemic Routing.

IV. TRANSPORT LAYER

The existing transport layer protocols, such as TCP, are not suitable for an environment where frequent disruption is a norm and end-to-end paths are typically not available. In [24], authors proposed the Licklider Transmission Protocol (LTP) that provide retransmission-based reliability over links with extremely high latency such as deep space communications. Besides, LTP focuses on the “long-haul” reliable transmission in challenged networks. In an Interplanetary Internet setting, LTP is intended to serve as a reliable “convergence layer” protocol over single hop deep-space RF links. LTP implements ARQ of data transmissions by soliciting selective-acknowledgment reception reports. In order to assure reliable communication, the LTP protocol exploits the procedures of “retransmission” and “accelerated retransmission”. Farrell et al. [25] proposed a generic transport protocol for opportunistic networks by using an extended LTP mechanism [26] to create an end-to-end capable transport protocol called “LTP transport (LTP-T)”. The LTP extension mechanism was originally defined to handle the addition of authentication fields to LTP and allow for the addition of both header and trailer extensions, up to a maximum of 16 (of each). In this work, the authors define a set of extensions of LTP about the transport protocol, i.e., source address, destination address, estimated block size and congestion notification etc.

Since Bundle Protocol [3] requires the services of a “convergence layer adapter (CLA)” to send and receive bundles using an underlying Internet protocol, then in [27] the authors present one such convergence layer adapter that uses the well-known Transmission Control Protocol (TCP). The TCP-based convergence layer (TCPCL) is used to link two bundle nodes. The lifetime of a TCPCL connection will match the lifetime of its underlying TCP connection. In other words, a TCPCL connection is initiated when a bundle node initiates a TCP connection to be established for the purposes of bundle communication. It is terminated either when the TCP connection ends due to one or both nodes actively terminating the TCP connection, or when network errors causes a failure of the TCP connection. In [28], the authors showed that the TCP protocol does not make effective use of available link capacity in a challenged environment like an opportunistic network. , in [29] the authors proposed the use of Saratoga [30] as convergence layer. Saratoga is a rate-based UDP file transfer protocol that can also be used to transfer bundles. The convergence layer is typically running on top of IP since IP is pervasive and supported by many existing link technologies.

V. BUNDLE LAYER

The bundle layer is responsible for storing, carrying and forwarding the data in an opportunistic network. Except from unicast bundle delivery, multicast and anycast delivery approaches are typically used when there are more than one destination.

Protocol	Buffer Management	Estimation of link forwarding probability	Complexity of information exchange or computation for the link state	Reactive or Proactive
Epidemic	Infinite	No	Don't need	Reactive
CAR	Infinite	YES, using Kilman filter	Computation only	Reactive
Spray and wait	Infinite	No	Don't need	Reactive
PROPHET	Infinite	YES, using delivery predictability vector	Exchange and computation	Reactive
MaxProp	Infinite	YES, estimating the delivery likelihood	Exchange and computation	Reactive
Knowledge	Infinite	YES, using oracle based Dijkstra algorithm	Exchange and computation	Reactive
SEPR	YES, remove those packets with smaller EPL	YES,	computation	Reactive
Direction transmission	Infinite	No	Don't need	Reactive
MoVe	Infinite	YES, using motion vector	Exchange and computation	Reactive

TABLE I

THE COMPARISON OF THE ROUTING PROTOCOLS

A. Bundle Delivery Approach

In an opportunistic network, applications utilize nodes to send or receive data that is carried in bundles which can be delivered to a group of nodes. When the group size is greater than one, the delivery semantics may be either anycast or multicast. For anycast delivery, a bundle is delivered to at least one and preferable only one of the members in a group. On the other hand, for multicast delivery, the bundle is intended to be delivered to all members in the same multicast group.

1) Anycast: In [31], authors define an anycast semantics model and proposed a routing metric, called EMDDA (Expected Multi-Destination Delay for Anycast), for anycast. The semantics models allow message senders to explicitly specify the intended receivers of a message. In this study, the anycast routing algorithm is based on the metric EMMA which accurately estimates the delay from a node to the nearest member of the destined anycast group. EMDDA of a node to an anycast group is defined as the minimum value of Practical Expected Delays (PEDs), while PED is the expected delay of taking different paths, from a node to all the destination group members. When a message arrives at a node, but the node is not an intended receiver of the anycast message, the node will calculate its EMDDA to the destination group. The key advantage of using EMDDA is that it can reflect the expected delay between a pair of nodes by taking all possible paths into account instead of only the shortest path.

2) Multicast: Due to the network partitions and opportunistic contacts, nodes are difficult to maintain a source-rooted multicast tree during the lifetime of a multicast session. The traditional approaches may fail to deliver a message when the link is unstable. In [32], the authors developed several multicast routing algorithms as follows. 1. UBR (Unicast-Based Routing) uses unicast transfer to achieve the multicast service. 2. In STBR (Static Tree-Based Routing), messages are forwarded along a tree in the graph that is rooted at the source and reaches all receivers. Due to that the route is static, the message needs to wait for the next opportunity to be forwarded if a message misses a contact opportunity with a node. This may cause significant increase in the message delay. 3. In DTBR (Dynamic Tree-Based Routing), nodes can determine the next-hop forwarders of a message dynamically based on current available information. 4. BBR (Broadcast-Based Routing) always includes all nodes in the network, so messages are flooded throughout the network. 5. GBR (Group-Based Routing) uses the concept of forwarding group for each message by computing a shortest path tree as in STBR. The group is a set of nodes that are responsible for forwarding the message. Messages are forwarded by flooding within the forwarding group.

In [33], the authors proposed an on-demand situation-aware multicast (OS-multicast) approach. Initially, a source-rooted tree is constructed in the similar way as STBR [32]. When a node receives a bundle, it will dynamically rebuild the tree rooted at itself to all the destinations based on the current network conditions. Their simulation results showed that OS-multicast can achieve smaller delays and better message delivery ratios than DTBR [32].

In [34], the authors propose a context-aware multicast routing (CAMR) scheme where nodes are allowed to use high power transmissions when the node density (which is locally observed) drops below a certain threshold. Each node maintains the contact probabilities using its 2-hop neighbor information. This allows each node to deliver traffic without invoking a route discovery process if all receivers are within its two-hop neighbor. In addition, nodes are allowed to act as message ferries when they discover they are in a very sparse neighborhood. The combined high-power route discovery process and message ferrying features allow CAMR to achieve much higher multicast delivery ratio than DTBR [32] and OS-multicast [33] schemes.

In [35], the authors build a multicast scheme on top of the PROPHET [23], so this scheme is called encounter-based multicast routing (EBMR) scheme. In EBMR, each node selects as many nodes as needed with the highest delivery predictability to each of the multicast receivers. If the next-hop neighbor can not be found, a node will cache the data until a timer expires. When the timer expires, the node simply selects a node with the highest delivery predictability to multicast receivers. In addition, this scheme allows nodes in the boundary region to use directional antenna to find nodes in other regions if they cannot hear any such node using omnidirectional antenna.

VI. APPLICATION LAYER

In an opportunistic network, traditional applications fail to take advantage of the communication opportunities offered by those opportunistic contacts. Hence, even the application is delay-tolerant in nature, the overall application performance can still suffer significantly in a disconnection-prone environment. The well-known paradigms on the Internet is E-mail because this application is delay-tolerant by large and e-mail users are used to wait for hours or days for a reply. However, given that the underlying transport protocol of e-mail (i.e. TCP) is not designed for an opportunistic network, supporting e-mail in such an environment is still quite challenging.

Scott et al.[36] proposed the use of SMTP proxies to hide the disruptions between end users in a challenged network. This proxy is responsible to help the client to perform its work and exchanges the corresponding information to a peer proxy. The peer proxy receives the information and sends it to its SMTP server. The drawback of this proxy-based approach for SMTP protocol is that the proxy has to executes the entire SMTP protocol forwarding the information via the inter-proxy protocol. In [37], the authors describe an architecture to enable mail communication in a heterogeneous environment that combines traditional server-based mail delivery and opportunistic communications for different types of devices. In this architecture, mail messages are sent in bundles into the opportunistic network and carried toward a mail gateway (MWG). The MWG is responsible to forward and receive the mail between the infrastructure network and the opportunistic network. The MWG and corresponding device could implement the Bundle Protocol To eliminate unnecessary process. In addition, each device can be configured with Mail User Agent (MUA) option to send or retrieve mails either through proxy or using separate mail folders.

Supporting e-mail in a opportunistic network is quite straightforward since that fits into the characteristics of the opportunistic network very well. However, adding support for Web is much more complicated, because highly interactive application protocols, such as HTTP, are not well suited for this kind of environment. In [36], Scott proposed an implementation of web proxy by extending the World Wide Web Offline Explorer (WWWOFFLE)[38]. The authors split the WWWOFFLE proxy and adding a client and a server side. The client side links to the challenged network and uses bundles to communicate with the server side. The server side has full connectivity to the Internet, so that when the server receives requests from clients, it can use HTTP to retrieve the requested web pages through the Internet. In [39], authors presented a protocol design and a system architecture for delay-tolerant access to web pages. This work uses the bundle protocol to transport the HTTP payloads in network. Furthermore, several scenarios are proposed for retrieving the web contents. First scenario is an end-to-end operation. This scenario requires both client and server to be modified so that bundles can be sent directly to the respective server. Second scenario is a proxy-based operation. Adding proxies t may support a mobile node in content aggregation from one or more origin servers. Finally, in a gateway operation the web clients and web servers communicate with gateway through this protocol. The intermediary gateway are required to covert between HTTP-over-challenged network and HTTP-over-TCP operation. Balasubramanian et al. [40] proposed a system, called Thedu, which uses an Internet proxy to collect search engine result and prefetch result pages. The mobile node can receive the user query through web interface and store it until the mobile node contacts with the proxy. If the connection is broken, the remaining web pages will be downloaded at next contact time. Furthermore, when the proxy awaits connection from a mobile node and has pending response, it downloads the responses and fetches some relevant web pages. In addition, the proxy will prioritize response bundles at next contact time.

VII. CONCLUSION

Opportunistic network is an emerging system that is getting growing interest in networking research community. The opportunistic network places different research challenges on different layers of a protocol stack. In this paper, we provide a quick overview of the state-of-the-art work in providing solutions to various issues in an opportunistic network. This work is aimed to serve as an introductory material to people who is interested in pursuing research in this area.

REFERENCES

[1] A. Lindgren and A. Doria, “Experiences from deploying a real-life dtn system,” *In 2007 4th IEEE Consumer Communications and Networking Conference*, pp. 217–221, 2007.

[2] “The zebranet wildlife tracker,” *http://www.princeton.edu/ mrm/zebranet.html.*

[3] K. Scott and S. Burleigh, “Bundle protocol specification,” *Internet-Draft*, 2007.

[4] J. Segui and E. Jennings, “Delay tolerant networking v bundle protocol simulation,” *in Second IEEE International Conference on Space Mission Challenges for Information Technology*, 2006.

[5] B. Burns, O. Brock, and B. N. Levine, “Mv routing and capacity building in disruption tolerant networks,” *In Proceedings of IEEE INFOCOM*, vol. 1, pp. 398–408, 2005.

[6] W. Zhao, M. Ammar, and 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 ’04*, pp. 187–198, May 2004.

[7] Z. Zhang and Z. Fei, “Route design for multiple ferries in delay tolerant networks,” *In Proceedings of IEEE Wireless Communications and Networking Conference*, pp. 3460–3465, 2007.

[8] Y. Chen, W. Zhao, M. Ammar, and E. Zegura, “Hybrid routing in clustered dtns with message ferrying,” *In Proceedings of the 1st international MobiSys workshop on Mobile opportunistic networking MobiOpp ’07*, pp. 75–82, 2007.

[9] M. M. B. Tariq, M. Ammar, and E. Zegura, “Message ferry route design for sparse ad hoc networks with mobile nodes,” *In Proceedings of the seventh ACM international symposium on Mobile ad hoc networking and computing MobiHoc ’06*, pp. 37–48, May 2006.

[10] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, “Pocket switched networks: Real-world mobility and its consequences for opportunistic forwarding,” *Technical reports published by the University of Cambridge Computer Laboratory*, 2005.

[11] A. Vahdat and D. Becker, “Epidemic routing for partially connected ad hoc networks,” *In Duke University, Technical Report CS-200006*, 2000.

[12] Y.-K. Ip, W.-C. Lau, and O.-C. Yue, “Forwarding and replication strategies for dtn with resource constraints,” *in Proceedings of IEEE Vehicular Technology Conference*, vol. 1, pp. 1260–1264, 2007.

[13] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, “Single-copy routing in intermittently connected mobile networks,” *In 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, pp. 235 – 244, 2004.

[14] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad-hoc wireless networks," *In IEEE/ACM Transactions on Networking*, vol. 10, no. 4, pp. 477–486, 2002.

[15] J. LeBrun, C.-N. Chuah, D. Ghosal, and M. Zhang, "Knowledge-based opportunistic forwarding in vehicular wireless ad hoc networks," *In IEEE Vehicular Technology Conference(VTC)*, pp. 2289–2293, May 2005.

[16] J. Leguay, T. Friedman, and V. Conan, "Dtn routing in a mobility pattern space," *In Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, pp. 276–283, 2005.

[17] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," *In Proceedings of ACM SIGCOMM*, vol. 34, pp. 145–158, 2004.

[18] M. Musolesi, S. Hailes, and C. Mascolo, "Adaptive routing for intermittently connected mobile ad hoc networks," *In IEEE WoWMoM 2005*, pp. 183–189, 2005.

[19] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," *In Proceedings of IEEE INFOCOM 2006*, pp. 1–11, 2006.

[20] K. Tan, Q. Zhang, and W. Zhu, "Shortest path routing in partially connected ad hoc networks," *In Proceedings of IEEE Globecom 2003*, vol. 2, pp. 1038–1042, 2003.

[21] A. A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry, "Epidemic algorithms for replicated database maintenance," *In Proceedings of the Sixth Symposium on Principles of Distributed Computing*, pp. 1–12, 1987.

[22] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: An efficient routing scheme for intermittently connected mobile networks," *In Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking WDTN '05*, pp. 252–259, 2005.

[23] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," *In ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 7, no. 3, pp. 19–20, 2003.

[24] M. Ramadas, S. Burleigh, and S. Farrell, "Licklider transmission protocol - specification," *Internet-draf*, 2007.

[25] S. Farrell and V. Cahill, "Ltp-t: A generic delay tolerant transport protocol," *Technical reports published by the University of Dublin*, 2005.

[26] S. Farrell, M. Ramadas, and S. Burleigh, "Licklider transmission protocol - extensions," *Internet-draf*, 2007.

[27] M. Demmer and J. Ott, "Delay tolerant networking tcp convergence layer protocol," *Internet-draf*, 2006.

[28] L. Wood, C. Peoples, G. Parr, B. Scotney, and A. Moore, "Tcps protocol radius:the distance where timers prevent communication," *In Proceeding of IWSSC'07*, 2007.

[29] L. Wood, W. M. Eddy, W. Ivancic, J. McKim, and C. Jackson, "Saratoga: a delay-tolerant networking convergence layer with efficient link utilization," *In Proceeding of IWSSC'07*, 2007.

[30] L. Wood, J. McKim, W. Eddy, W. Ivancic, and C. Jackson, "Saratoga: A convergence layer for delay tolerant networking," *Internet-draf*, 2007.

[31] Y. Gong, Y. Xiong, Q. Zhang, Z. Zhang, W. Wang, and Z. Xu, "Anycast routing in delay tolerant networks," *In IEEE GLOBECOM*, pp. 1–5, 2006.

[32] W. Zhao, M. Ammar, and E. Zegura, "Multicasting in delay tolerant networks: Semantic models and routing algorithms," *in Proceeding of Sigcomm Workshop in DTN*, pp. 268–275, 2005.

[33] Q. Ye, L. Cheng, M. C. Chuah, and B. D. Davison, "Os-multicast: On-demand situation-aware multicasting in disruption tolerant networks," *in Proceedings of IEEE VTC*, vol. 1, pp. 96–100, May 2006.

[34] P. Yang and M. C. Chuah, "Context-aware multicast routing scheme for disruption tolerant networks," *in Proceedings of ACM international workshop on PE-WASUN '06*, pp. 66–73, 2006.

[35] M. Chuah and Y. Xi, "An encounter-based multicast scheme for disruption tolerant networks," *Technical reports published by the University of LEHIGH*, 2007.

[36] K. Scott, "Disruption tolerant networking proxies for on-the-move tactical networks," *in IEEE MILCOM 2005.*, vol. 5, pp. 3226–3231, 2005.

[37] T. Hyyrylainen, T. Karkkainen, and C. Luo, "Opportunistic email distribution and access in challenged heterogeneous environments," *In Proceedings of the second workshop on Challenged networks CHANTS*, pp. 97–100, 2007.

[38] http://www.gedanken.demon.co.uk/wwwoffle/.

[39] J. Ott and D. Kutscher, "Bundling the web: Http over dtn," *In Proceeding of WNEPT2006*, 2006.

[40] A. Balasubramanian, Y. Zhou, W. B. Croft, B. N. Levine, and A. Venkataramani, "Web search from a bus," *In Proceedings of the second workshop on Challenged networks CHANTS CHANTS '07*, pp. 59–66, 2007.