OPPORTUNISTIC ROUTING IN MOBILE AD HOC NETWORKS

J.Pavithra,
M.Phil Research Scholar,
P.G & Research Department of Computer Science,
Siri PSG Arts and Science College for Women,
Sankari,Tamilnadu,India.

S.Mythili,
Assistant Professor,
P.G & Research Department of Computer Science,
Siri PSG Arts and Science College for Women,
Sankari,Tamilnadu,India.

Abstract: Opportunistic routing for multi-hop wireless ad hoc networks has long been proposed to overcome the decencies of conventional routing. Opportunistic routing mitigates the impact of poor wireless links by exploiting the broadcast nature of wireless transmissions and the path diversity. More precisely, the opportunistic routing decisions are made in an online manner by choosing the next relay based on the actual transmission outcomes as well as a rank ordering.

Keywords: MANET, Opportunistic Routing, Pro active and reactive routing

I.INTRODUCTION

Mobile ad-hoc networks were originally derived from the requirements of military applications. For example, in a battlefield application, where there is no fixed networking infrastructure, soldiers and assets are mobile and they have a need for voice, data, and video communications with each other. Since assets are mobile, traditional IP routing using static routing tables is not suitable for creating networks. Without any fixed networking infrastructure, a MANET has to be created "on the- fly". A MANET is a self-configuring, infrastructure-less network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction and therefore will change its links to other devices frequently. Each node must be willing to participate in forwarding traffic even though the packet is not of its interest. The fact that these networks are self-forming and self-healing facilitates the deployment process and minimizes the need for manual configuration and intervention. MANETs support multi-hop networking to extend coverage and provide redundant paths for increased resilience.

Characteristics of Mobile Ad-hoc Networks

A mobile ad-hoc network has many distinct characteristics, which are mainly due to the fact that it lacks any centralized infrastructures. Additional reasons include:

- Time-varying channel caused by wireless channel propagation: nodes located within the radio range of each other can establish a network connection without any pre-configuration or manual intervention.
- Wireless medium is broadcast in nature; the transmission on one link may interfere with transmissions on other neighboring links.
- Wireless embedded devices are usually constrained by limited resources.

All these limitations make protocol design in MANETs a hard task. In the following, list the main characteristics of MANETs.

- **Self-forming:** Nodes located within the radio range of each other can establish a network connection without any pre-configuration or manual intervention.
- **Self-healing:** Nodes can joint or leave rapidly without affecting the operation of remaining nodes. An important requirement of MANET is its fault tolerance, such that the failure of any node will not significantly degrade performance.
- **No Infrastructure:** In a mobile ad hoc network, mobile nodes form their own network autonomously. All the nodes within the network have the same role. They are both packet source and forwarder. There is no centralized control of network operation.
- **Peer-to-peer communication:** Traditional networks typically support end systems operating in client-server mode. In a MANET environment, mobile nodes can communicate and exchange messages without prior arrangement and without reliance on centralized resources.
- **Highly dynamic network topology:** Mobile nodes are in continuous movement. They move either following certain mobility patterns, or just randomly. The variation of wireless link also changes the connectivity among nodes. The network topology of a MANET is constantly changing over time.
- **Limited resources:** Some or all of the network nodes are suffering from restricted limitation of energy, computation power, memory, etc.
- **Limited bandwidth:** Wireless links have significantly lower capacity than infrastructure-based networks. In addition, the realized throughput of wireless communications - after accounting for the effects of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.
- **Security threats:** Mobile wireless networks are generally more prone to physical security threats than fixed cable networks. The increased possibility of eavesdropping, spoofing, and minimization of denial-of-service type attacks should be carefully considered in a real system deployment.

II. ROUTING IN MOBILE AD-HOC NETWORKS

Packet routing in a mobile ad-hoc network is intrinsically different from routing in wired networks with fixed infrastructures. Due to the infrastructure-less feature, routing in MANETs encounters many challenges that do not exist in wired network routing. For example, one challenge is that, a

MANET node needs to know the reach ability information to its neighbors. However, node mobility and varying of wireless links make the network topology constantly change over time.

Proactive Routing: Proactive routing maintains the route from source to destination all the time by exchanging beaconing messages periodically. Therefore, whenever a sender wants to send packets to a destination, the route information is immediately available in the routing table. The drawbacks are the large amount of controlling overhead, which wastes the scarce network resources. In the following, list some representatives of proactive routing protocols.

- **Destination-Sequenced Distance-Vector Protocol :** The destination-sequenced distance-vector protocol (DSDV) [4] is a proactive hop-by-hop distance vector routing protocol, requiring each node to periodically broadcast routing updates. In DSDV, every node in the network maintains a routing table for all possible destinations within the network and the number of hops to each destination. Each entry in the table is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops. Routing table updates are periodically transmitted throughout the network in order to maintain consistency in the table.
- **Global State Routing Protocol :** The global state routing (GSR) [4] is based on the traditional link state algorithm. However, GSR has improved the way information is disseminated in link state approach by restricting the update message among intermediate nodes only. In GSR, each node maintains a link state table based on the up-to-date information received from neighboring nodes, and periodically exchanges its link state information with neighboring nodes only. This has significantly reduced the number of control messages transmitted throughout the network.
- **Optimized Link State Routing Protocol :** The optimized link state routing (OLSR) [5] maintains the network topology information by exchanging link-state messages. OLSR minimizes the size of each control message and the number of rebroadcasting nodes during each route update by employing a new concept called multi-point relaying (MPR) node. During a topology update process, each node selects a set of neighbors to retransmit its packets. This set of nodes is defined as the multi-point relay node. Any node that is not in this MRP node can only read the packet but cannot retransmit it. To select the MPR nodes, each node periodically broadcasts a list of its one hop neighbors using hello messages. From the list of nodes in the hello messages, each node selects a subset of one hop neighbors, which covers all of its two hop neighbors.

Reactive Routing: Reactive routing, or called on-demand routing, protocols were designed to reduce the overheads in proactive routing by maintaining information for active routes only when necessary. This means that routes are determined and maintained for nodes that require sending data to a destination. Route discovery usually occurs by flooding a route request packets through the network. When a node with a route to the destination is reached, a route reply message is sent back to the source node using link reversal if the route request has traveled through bi-directional links or by piggy-backing the route information in a route reply message via flooding.

- **Dynamic Source Routing Protocol :** The dynamic source routing (DSR) [6] protocol uses explicit source routing in which each data packet has in its header a complete list of all intermediate nodes to the destination. DSR is composed of two main mechanisms. In route discovery, a node, which attempts to send a packet to a destination and does not know a route, broadcasts a route request packet. Each node that forwards this packet adds its own address to the header. If the destination received the route request, it sends back a route reply packet containing a copy of the accumulated route along the reverse direction of the path over which the route request packet arrived. Thus, each node forwarding this reply packet is aware of the whole path from the source to the destination. Nodes cache the route information from each packet they overhear. Intermediate nodes may also reply to a route request packet, if it knows a route to the destination (thanks to the cached route information before).
- **Ad-hoc On-demand Distance Vector Protocol :** The ad-hoc on-demand distance vector protocol (AODV) [7] is based on DSDV and DSR protocols. It uses the periodic beaconing messages and sequence numbering procedure of DSDV and a similar route discovery mechanism from DSR. However, there are two major differences between DSR and AODV. The most distinguishing difference is that in DSR, each packet carries a full list of forwarder information, whereas in AODV the packets carry the destination address only. The advantage of AODV is that it is adaptable to dynamic environments. However, nodes may experience large delay during the route setup procedure, and link failures may initiate another route discovery, which introduces extra delays and consumes more bandwidth as the size of network increases.
- **Location-aided Routing Protocol :** The location-aided routing protocol (LAR) [8] is based on flooding algorithm (such as DSR). However, LAR attempts to reduce the routing overheads presented in the traditional flooding algorithm by using location information. This protocol assumes that each node knows its location through a GPS device. Two different LAR schemes were proposed in [9], the first scheme calculates a request zone which defines a boundary where the route request packets can travel to reach the required destination. The second method stores the coordinates of the destination in the route request packets. Both methods limit the control overhead transmitted through the network and hence conserve bandwidth. The disadvantage of this protocol is that it might behave similar to flooding algorithms in highly dynamic environment.

Hybrid Routing: Hybrid routing is a new generation of protocol, which is both proactive and reactive in nature. This routing concept is designed to increase the scalability by allowing nodes with close proximity to work together to form some sort of network backbone to reduce the route discovery overheads. This is mostly achieved by pro-actively maintaining routes to nearby nodes and determining routes to far away nodes using a route discovery strategy. Most hybrid protocols are zone-based, which means that the network is partitioned into a number of zones. Some hybrid protocols separate nodes into trees or clusters. This section describes a number of hybrid protocols.

- **Zone Routing Protocol :** In zone routing protocol (ZRP) [10], each node has an associated routing zone, which defines a range, in terms of hops, that each node is required to maintain network connectivity proactively. Therefore, for nodes within the routing zone, routes are immediately available. For nodes located outside the routing zone, routes are determined on-demand, and it can use any on-demand routing protocols to find out a route to the destination. The advantage of this protocol is that it has significantly reduced controlling overheads when compared to a pure proactive protocol. It also reduces the delays associated with pure reactive protocol, by allowing routes to be discovered faster. This is because to determine a route outside the routing zone, ZRP packet only has to travel to a node lying on the boundaries (edges of the routing zone) of the destination.
- **Sharp Hybrid Adaptive Routing Protocol :** The sharp hybrid adaptive routing protocol (SHARP) [10] currently is a joint routing approach of proactive and reactive routing. SHARP is a hybrid routing protocol that finds the optimal mixture of proactive route dissemination and reactive route discovery. It finds the balance point between proactive and reactive routing by adjusting the degree to which route information is propagated proactively versus the degree to which it needs to be discovered reactively. SHARP enables each node to use a different application-specific performance metric to control the adaptation of the routing layer.

III. OPPORTUNISTIC ROUTING DESIGN

The major challenge in opportunistic routing design is to maximize the routing progress of each data transmission towards the destination without producing duplicate transmissions or incurring significant coordination overheads. In order to achieve the potential benefits of opportunistic routing and avoid the abovementioned problems, an effective protocol should implement the following tasks in a distributed fashion:

- **Candidate selection:** All nodes in the network must run an algorithm for selecting and sorting the set of neighboring nodes (candidate list) that can better help in the forwarding process to a given destination. Refer to this algorithm as candidate selection. The aim of the candidate selection algorithm is to guarantee that only the qualified nodes become the candidates and to build the candidate list. In order to accurately build the candidate list, OR protocols require certain metrics to evaluate the network and rank network nodes.
- **Forwarder selection through candidate coordination:** Forwarder selection provides a scheme to select, among all the candidates that have successfully received the packet, only one node that really forwards the packet. Because there is no central controlling node, the forwarder selection process is done through the coordination of multiple candidates. Coordination requires signaling among candidates, and imperfect coordination may cause duplicate packet transmissions.
- **Forwarding responsibility transfer:** This function allows the nodes involved in the forwarding process - the actual forwarder plus the candidates - to become aware of the winner of the selection. The responsibility transfer is the distinguishing feature that differentiates opportunistic routing from flooding. In fact, in both opportunistic routing and flooding, multiple nodes will receive the broadcast transmission from a packet sender. However, unlike in the flooding algorithm, opportunistic routing allows only one node at a time to be in charge of packet forwarding.
- **Duplicate transmission avoidance:** This process is required only in case of imperfect responsibility transfer. If the forwarding responsibility is correctly transferred to the winning forwarder, there is only one node in charge of packet forwarding at any time. In contrast, several packet transmissions occur but only one is innovative, i.e., the one made by the winning forwarder. More effective the duplicate avoidance mechanism is, less network resources will be wasted.

IV.ROUTING METRICS

The general purpose of opportunistic routing is to minimize the expected number of transmissions required to transmit a packet from the source to the destination. The set of candidates that are used by nodes and their priorities have significant impact on routing performance. Therefore, using a good metric to select and prioritize the candidate is a key factor. Candidate can be prioritized based on hop count, geographic distance, expected transmission count (ETX), and expected any-path transmission (EAX) and so on. Utilization of hop count, ETX or EAX needs an underlying routing protocol (either reactive or proactive) to gather such information. Geo-distance requires the availability of location information of nodes. The accuracy of a metric depends on the proper measurement and timely dissemination of such information. Below,describe two metrics of ETX and EAX that have been widely used in the literature.

Expected Transmission Count (ETX) [11] is the average number of transmissions required to reliably send a packet across a link or route including retransmissions. The ETX of a single path route is the sum of the ETX for each link in the route. With the assumption of the packet transmission between nodes i and j with delivery probability pij, the expected transmission count of the link is: **ETX (i; j) = 1 / pij .**

In OR, however, it is necessary to consider the fact that there are some candidates, which can receive the packet. Thus, a packet may travel along any of the potential paths.

Authors in [49] [92] have shown that using ETX may give suboptimal selection of candidates and in [95] it was shown that OR in combination with ETX could degrade the performance of the network. Therefore, [160] proposed another metric, which has been widely adopted in OR.

Expected Any-path Transmission (EAX) [12] is an extension of ETX and can capture the expected number of transmissions taking into account the multiple paths that can be used in OR.

V. ROUTING WITH CONGESTION DIVERSITY

In this section, start with our 802.11-compatible design for the congestion awarerouting algorithms BP, E-BP and CDP. Next, summarize the exiting design and our implementation for state of the art protocol Srcr.

Congestion-aware routing

The guiding principle of congestion-aware routing has been congestion avoidance in the network taking into account the queue backlog information t (n) at eachnode n destined for node d at time t and the link qualities W(n; k) between each pair of nodes n; k.BP, E-BP and CDP take routing decisions by exchanging a time-varying congestion aware metric, referred to as the congestion measure. For a set of nodes, denote the congestion measures for destination d at node n as V dX;t(k), where X is the protocol of interest in the set BP, E-BP, CDP. In practice V dX;t(k) is only known at node n via periodic updates received from node k. Let (k) be the latest congestion measure advertised by neighbor k and received at node n. Based on the received congestion-measure (k), each node n in the network updates its routing table. In particular, the routing table determines the next-hop K(n;d)X;t for a packet at node destined for node d. After each successfully acknowledged transmission, the routing responsibility is then transferred to the next hop.

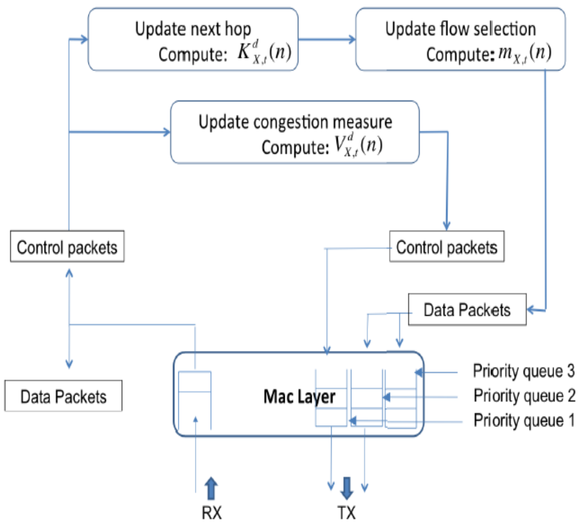


Figure 1: Design of congestion-aware routing algorithms.

The design of these congestion-aware algorithms rely on a routing table at each node to determine the next best hop. The routing table at node *n* consists of a listof neighbors *N*(*n*), a structure consisting of estimated congestion measures *V* (*n*,*d*)*X*,*t*(*k*)for all neighbors *N*(*n*) associated with different destinations, and the best nexthop vector {*K*(*n*,*d*)*X*,*t* }*d*. Node *n* periodically advertises the entries of the its computed congestion measures to its neighbors at intervals of *T* seconds using control packets. Thus, the periodic computation and communication of congestion-measures propagates routing information across the neighbors. The sequence of operations performed areshown in Figure 1.BP, E-BP and CDP have different notions of measuring the effective congestion in the network and thus determining next hop selections.

VI. PERFORMANCE RESULTS

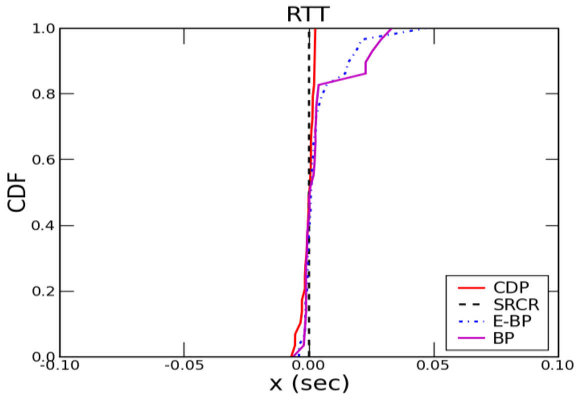
In this section, perform a comparative study of various routing protocols under TCP and UDP traffic. In our comparative analysis, investigate the following performance measures:

1. End-End delay: For M packets, define the mean delay D = 1MPMj=1, where j is the arrival time at the destination and jis the departure time for packet j at the source. For TCP traffic, consider mean delay as mean RoundTrip Time (RTT). are interested in the distribution of per packet delay, e.g.the Cumulative Distribution Function (CDF) of D with respect to the randomchoice of network topology. For illustration purposes, consider a differentialdelay measure which consists of the difference between CDP and the candidate protocol. Specifically, plot the difference Dcandidate DSrcr, where DSrcr is the mean delay for CDP and Dcandiate is the mean delay for the comparative protocol.

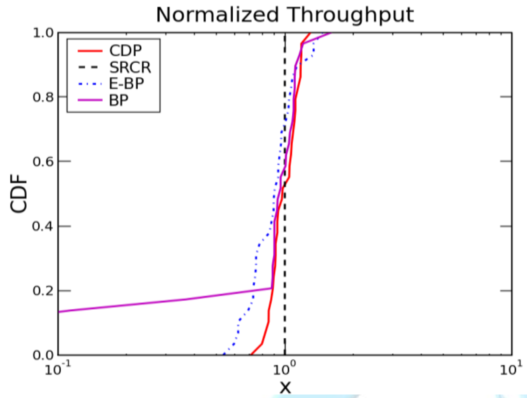
2. Throughput ratio: The throughput is the number of bytes received at the destinationfor the duration of the experiment. Again when investigating the CDP performancewith respect to the network topology, use the normalized throughputratio as a measure of performance, where the normalized throughput ratio is definedas the ratio between the throughput of the candidate protocol versus the Srcr.

VII. EXPERIMENTS WITH TCP

In this section, study the performance of congestion-aware routing algorithmsfor TCP used for reliable communications. Report the comparative performance ofthe candidate routing protocols (relative to Srcr) under reliable transfer control algorithms TCP-Veno [18] by selecting a configuration of two TCP flows with randomlyselected source and destination pairs. do not expect to see significant improvementfor congestion-aware routing protocols with respect to Srcr when the sources of trafficare TCP. The first reason for the insignificant performance gain is that the current implementationsof TCP are non-aggressive. TCP tries to avoid congestion in the networkand thus makes the congestion routing insensitive to congestion routing. Secondly, TCPis known to have performance degradation with respect to the packet reordering. (Figure 2 shows that BP, E-BP and CDP suffer from the reordering of packets introduced bythe dynamic route selection.)



(a) Differential RTT



(b) Normalized throughput

Figure 3: Performance for TCP traffic

Given the above considerations, the best can hope is that the proposed congestionaware routing does not degrade the performance. show that this is the casefor CDP and E-BP. Figures 3(a) and 3(b) compare the CDF of the Round Trip Time

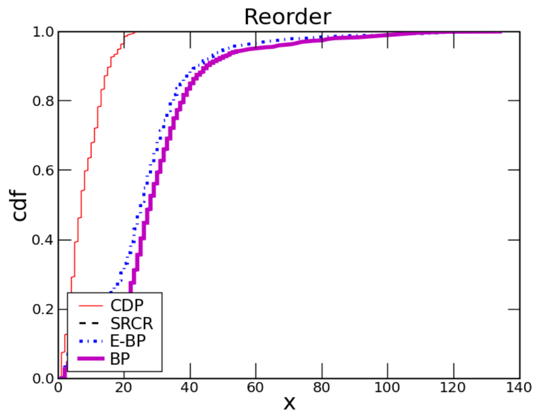


Figure 4: CDF of reordering

(RTT) and the normalized throughput for multi-hop flows for CDP, Srcr, BP and E-BP. These set of experiments show that CDP and E-BP exhibit a comparable performance with Srcr for TCP flows. For multi-hop flows, the performance of TCP for BP suffersfrom the loops and "dead ends", resulting in timeouts and very low throughput for routeswith multiple hops.Next, dissect and study the more interesting case of UDP traffic.

VII.CONCLUSIONS

A number of assumptions are imposed on the optimality of AdaptOR. AdaptOR is designed for a static network. An important area for future research is to extend AdaptOR algorithm for mobiles networks. However, the generalization to the networks with inter-channel interference follows directly from. The price of this generalization is shown to be the centralization of the routing/scheduling globally across the network or a constant factor performance loss of the distributed variants. In the future, we are interested in generalizing D-ORCD for joint routing and scheduling optimizations as well as considering system level implications. Incorporating throughput optimal CSMA-based MAC scheduler with congestion aware routing is also a promising area of research.

VIII.REFERENCES

[1]. Kevin Fall. A delay-tolerant network architecture for challenged internets. In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM '03, pages 27–34, New York, NY, USA, 2003. ACM.

[2]. S. Yousefi, M.S. Mousavi, and M. Fathy. Vehicular ad hoc networks (vanets): Challenges and perspectives. In ITS Telecommunications Proceedings, 2006 6th International Conference on, pages 761–766, June 2006.

[3]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. Comput. Netw., 38(4):393–422, March 2002.

[4]. I.T. Almalkawi, M. Guerrero Zapata, J.N. Al-Karaki, and J. Morillo-Pozo. Wireless Multimedia Sensor Networks: Current Trends and Future Directions. Sensors, 10(7):6662–6717, 2010.

[5]. Personal area networks. http://en.wikipedia.org/wiki/Personal area network.

[6]. S. Morgenthaler, T. Braun, Zhongliang Zhao, T. Staub, and M. Anwander. Uavnet: A mobile wireless mesh network using unmanned aerial vehicles. In Globecom Workshops (GC Wkshps), 2012 IEEE, pages 1603–1608, Dec 2012.

[7]. Denis Ros´ario, Zhongliang Zhao, Torsten Braun, Eduardo Cerqueira, and Aldri Santos. Opportunistic routing for multi-flow video dissemination over flying ad-hoc networks. In World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium and Workshops on a, June 2014.

[8]. Charles E Perkins and Elizabeth M Royer. Ad-hoc on-demand distance vector routing. In Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on, pages 90–100. IEEE, 1999.

[9]. Zygmunt J Haas, Marc R Pearlman, and Prince Samar. The zone routing protocol (zrp) for ad hoc networks. draft-ietf-manet-zone-zrp-04. txt, 2002.

[10]. Venugopalan Ramasubramanian, Zygmunt J. Haas, and Emin G¨un Sirer. Sharp: A hybrid adaptive routing protocol for mobile ad hoc networks. In Proceedings of the 4th ACM International

Symposium on Mobile Ad Hoc Networking &Amp; Computing, MobiHoc '03, pages 303–314, New York, NY, USA, 2003. ACM.

[11]. Brad Karp and H. T. Kung. Gpsr: greedy perimeter stateless routing for wireless networks. In 6th annual international conference on Mobile computing and networking, pages 243–254, New York, NY, USA, 2000.

[12]. Ya Xu, John Heidemann, and Deborah Estrin. Geography-informed energy conservation for ad hoc routing. In Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, MobiCom '01, pages 70–84, New York, NY, USA, 2001. ACM.

[13]. Yan Yu, Ramesh Govindan, and Deborah Estrin. Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks. Technical report, Technical report ucla/csd-tr-01-0023, UCLA Computer Science Department, 2001.

[14]. Charles E Perkins and Pravin Bhagwat. Highly dynamic destinationsequenced distance-vector routing (dsdv) for mobile computers. In ACM SIGCOMM Computer Communication Review, volume 24, pages 234–244. ACM, 1994.

[15]. Tsu-Wei Chen and Mario Gerla. Global state routing: A new routing scheme for ad-hoc wireless networks. In Communications, 1998. ICC 98. Conference Record. 1998 IEEE International Conference on, volume 1, pages 171– 175. IEEE, 1998.

[16]. Thomas Clausen, Philippe Jacquet, C´edric Adjih, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, Laurent Viennot, et al. Optimized link state routing protocol (olsr). 2003.

[17]. David B Johnson, David A Maltz, Josh Broch, et al. Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 5:139–172, 2001.

[18]. Gregory D Abowd, Anind K Dey, Peter J Brown, Nigel Davies, Mark Smith, and Pete Steggles. Towards a better understanding of context and context-awareness. In Handheld and ubiquitous computing, pages 304–307. Springer, 1999.

[19]. Daniel Aguayo, John Bicket, Sanjit Biswas, Glenn Judd, and Robert Morris. Link-level measurements from an 802.11 b mesh network. ACM SIGCOMM Computer Communication Review, 34(4):121–132, 2004.

[20]. Rudolf Ahlswede, Ning Cai, S-YR Li, and Raymond W Yeung. Network information flow. Information Theory, IEEE Transactions on, 46(4):1204– 1216, 2000.