Challenges of Intervehicle *Ad Hoc* Networks

Jeremy J. Blum, Azim Eskandarian, and Lance J. Hoffman

***Abstract*—Intervehicle communication (IVC) networks, a subclass of mobile *ad hoc* networks (MANETs), have no fixed infrastructure and instead rely on the nodes themselves to provide network functionality. However, due to mobility constraints, driver behavior, and high mobility, IVC networks exhibit characteristics that are dramatically different from many generic MANETs. This paper elicits these differences through simulations and mathematical models and then explores the impact of the differences on the IVC communication architecture, including important security implications.**

***Index Terms*—Intelligent transportation systems (ITSs), intervehicle communication (IVC), mobile ad hoc networks (MANETs).**

I. Introduction

In the future, vehicles will likely be equipped with communication capabilities that allow for intervehicle communication (IVC). IVC would perform crucial functions in collision avoidance, road-hazard notification, and coordinated driving systems. IVC networks are an instantiation of a mobile *ad hoc* network (MANET). MANETs have no fixed infrastructure and instead rely on ordinary nodes to perform routing of messages and network management functions.

However, automotive *ad hoc* networks will behave in fundamentally different ways than the models that predominate MANET research. Driver behavior, constraints on mobility, and high speeds create unique characteristics in IVC networks. These characteristics have important implications for design decisions in these networks.

In particular, IVC networks differ from typical MANET models in four key ways. They are characterized by rapid but somewhat predictable topology changes, with frequent fragmentation, a small effective network diameter, and redundancy that is limited temporally and functionally. This paper quantifies these characteristics through simulation and explores their implication for the functionality and security of the IVC network architecture.

II. Related Work

Related work in MANETs has focused on many of the layers of the communications architecture. This section reviews some of the relevant MANET research results from the various architectural layers. However, as shown in Section III, these results have limited applicability for the IVC network.

A. MANET Link Layer

Two issues that have been extensively studied at the link layer are the complementary problems of hidden and exposed nodes, and their effect on throughput [1].

Manuscript received December 1, 2003; revised July 16, 2004 and July 31, 2004. This work was supported in part by Cooperative Agreement DTFH61-99-X-00038 between the U.S. Department of Transportation, Federal Highway Administration, and The George Washington University. The Associate Editor for this paper was F.-Y. Wang.

J. J. Blum and A. Eskandarian are with the Center for Intelligent Systems Research, The George Washington University, Washington, DC 20052 USA (e-mail: blumj@gwu.edu).

L. J. Hoffman is with the Computer Science Department and the Cyber Security Policy and Research Institute, The George Washington University, Washington, DC 20052 USA.

Digital Object Identifier 10.1109/TITS.2004.838218

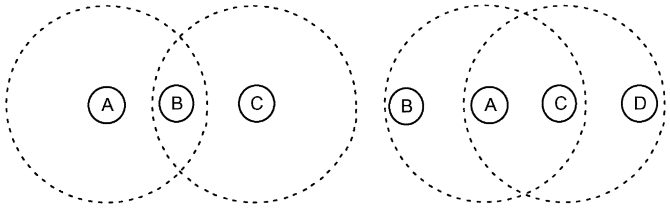

Fig. 1. Hidden and exposed nodes.

Hidden nodes are two nodes that, although they are outside the interference range of one another, share a set of nodes that are within the transmission range of both. As shown in the left-hand side of Fig. 1, nodes A and C are outside the transmission range of each other. If both attempt to transmit at the same time, they will cause a collision at B. Exposed nodes, on the other hand, are nodes that are within interference range of each other. As shown in the right-hand side of Fig. 1, although A and C are within interference range of each other, A could transmit to B and C could transmit to D without causing a collision at either B or D. However, since they are within interference range of each other, only A or C would transmit at a time. The effect of hidden nodes on throughput is handled by request-to-send/clear-to-send (RTS/CTS) handshaking. However, exposed nodes are difficult to address and present one of the most important factors in limiting network throughput.

One way to increase network throughput is to increase the number of nodes in the network. One study with random mobility noted that an increase in network size while holding traffic load constant yields increased throughput [2].

B. MANET Routing Layer

At the routing layer, MANET research has focused on the development of three broad classes of routing protocols, analysis of these approaches under various mobility models, and attempts to manage mobility-related routing issues.

MANET routing protocols, which do not use nodal position data, can be classified as table- or source-driven [3]. Table-driven protocols, DSDV for example, are proactive in the sense that each node attempts to maintain a current representation of the network topology. Source-driven protocols, on the other hand, are reactive in the sense that routes are requested by source nodes only when needed. Table-driven protocols provide lower message latency because routes are immediately available. However, the overhead required to maintain these routes consumes bandwidth and restricts the scalability of these protocols.

Another class of routing protocols uses position-based information for routing decisions [4]. A location service may then be necessary to find the location of a destination node. These protocols also naturally support geocasting, i.e., location-based multicast [5]. In location-based multicast, the set of recipients is defined as nodes located in some target region of space.

A number of mobility models have been used to analyze routing protocols. The most commonly used is the random waypoint model, for example [6]. In this model, nodes move in a random direction for a random amount of time, pause for some period of time, and then choose a different direction.

This random waypoint model conjures up a "a world where people constantly try to pass through walls and cars suddenly leave the roads and drive into rivers" [7, p. 309]. To provide a more realistic model, they devise a graph-based mobility scheme for their analysis of people walking in a city.

Another approach at a more realistic mobility model is scenario-based mobility, which considered scenarios of people moving at a sporting event, in a disaster area, and at a conference [8]. Interestingly, the authors found that the analysis from the random waypoint model corresponded to their scenario-based analysis well.

Mobility presents a number of problems for MANETs, including short-lived paths between nodes and network partitioning. Flow-oriented routing protocol attempts to manage short-lived paths by using nodal mobility information to predict the stability of routes in a source-driven protocol [9]. Epidemic routing attempts to gracefully handle situations in which no path exists between the source and destination nodes [10]. Each node contains a queue of messages to be delivered. When a node encounters another node, the nodes exchange the identifications of messages in their queues. Messages that have not been seen by a node will be exchanged.

C. MANET Security

Because MANETs lack a fixed infrastructure and rely on untrustworthy nodes for the propagation of control and data messages, securing a MANET is very difficult. Research for security controls for MANETs have included secure routing protocols, secure transport protocols, and intrusion-detection systems.

Secure routing proposals have included cryptographic techniques, including hash chains and digital signatures, to ensure the validity of routing messages [11], [12]. By increasing message size, these protocols limit available bandwidth. However, for stable routes, this additional load may not be significant.

Since the transport of messages relies on possibly untrustworthy nodes, not only are routing messages subject to corruption, but data messages also are. Secure message transport (SMT) attempts to address this problem by utilizing the redundancy in the network [11]. SMT cryptographically splits a message into n parts and sends each part over a distinct path. As long as k pieces are received, the message can be decoded. SMT, therefore, requires multiple independent paths between a source and a destination and spare bandwidth.

Intrusion-detection systems for MANETs attempt to identify nodes that are acting maliciously by fabricating, dropping, or altering control or data messages [13], [14]. In these systems, nodes overhear their neighbors' broadcasts in order to ensure that these neighbors are acting appropriately. In order for this eavesdropping technique to be effective, the models assume omnidirectional antennas.

III. Simulation of the IVC Network

In order to assess the applicability of the observations in the related research, an IVC network was simulated. This section describes the packages used to conduct the simulation, the scenarios that were simulated, and the simulation results.

A. Simulation Packages

The simulation of an IVC network was done using two widely used simulation packages. CORSIM was used to generate realistic vehicle mobility data and NS2 was used to generate realistic wireless network behavior.

CORSIM is the most widely used microscopic vehicle traffic simulation program in the United States [15]. As a microscopic traffic simulation, it tracks each individual vehicle. The vehicle's mobility is determined by driver behavior, vehicle performance characteristics, and constraints imposed by the roadway geometry and surrounding vehicles.

The network simulator (NS) is a widely used computer network simulator developed by the University of California, Berkeley, and the virtual internetwork testbed (VINT) project [16]. This study used the multihop *ad hoc* wireless extensions provided by the Monarch research group at Carnegie Mellon University, Pittsburgh, PA.

B. Simulation Scenarios

The vehicle simulation simulates traffic on a section of I-880 in Hayward, CA [17]. Data for traffic flows on various dates in 1993 was collected by the Freeway Service Patrol Evaluation Project, University of California, Berkeley. The author modeled the roadway geometry in CORSIM to roughly correspond to the 9.2-mi section of road, with ten exits and ten on-ramps.

Based on traffic data that was collected for March 13, 1993, a scenario was created for this roadway that models average traffic without high-occupancy vehicle (HOV) lanes. In this scenario, 20% of the vehicles were assumed to be equipped with IVC equipment. This high deployment rate was chosen to give a conservative picture of the difficulties that will be encountered in this network. The analysis in the following sections was done with radio ranges ranging from 25–500 ft.

C. Results

The results of these simulations indicate that the IVC network is fundamentally different from the networks studied in other MANET research. The major results of the following sections are as follows.

1) Rapid changes in the IVC network topology are difficult to manage.
2) The IVC network is subject to frequent fragmentation, even at a high rate of IVC deployment.
3) The IVC network has an even smaller effective network diameter under source-generated routing.
4) Unlike the redundancy in other MANETs, the redundancy in IVC networks are severely limited both in time and in function.

1) Rapid Topology Changes: Despite the severe constraints on the movement of vehicles (i.e., they must stay on the roadways), the IVC network experiences very rapid changes in topology. These changes are due to the high relative speed of vehicles, even when moving in the same direction. The direction of vehicle movement, though, has predictive value for the stability of these links.

Fig. 2 shows that the link life is affected by the direction of the vehicles and the radio range. The longer the radio range, the longer the links last. Links between vehicles traveling in opposite directions are very short lived when compared to links between vehicles traveling in the same direction.

A striking result, though, is the extremely limited nature of links, even for vehicles traveling the same direction with long transmission ranges. Even with a long transmission range of 500 ft, these links last approximately 1 min on average. As shown later, the effect of this short time is further exacerbated if a message must traverse several hops.

Unfortunately, as shown in the next sections, the approaches to increasing link life suggested by this analysis have an adverse affect on other desirable attributes. Discarding vehicles traveling in an opposite direction increases network fragmentation. Increasing the radio range has a dramatic adverse affect on network throughput.

2) Frequent Fragmentation: The IVC network will be subject to frequent fragmentation, in which chunks of the network are unable to reach nodes in nearby regions. This analysis is based on the optimistic goal of having IVC in 20% of vehicles. Due to slow introduction and adoption, deployment is likely to be lower for quite some time. With lower and more immediately realizable deployment ratios, the fragmentation would increase.

Fig. 3 shows this fragmentation when all nodes with IVC versus only those nodes traveling in the same direction. The connectivity fell in the checkered regions. Although the connectivity increased as radio range increases, at 500 ft, a node could often reach only 37% of the other nodes on this section of highway. As mentioned earlier, increasing radio range comes at a heavy price. If routes containing nodes traveling in opposite directions are discarded, the connectivity between nodes traveling the same direction is sharply reduced to as little as 16% at the 500-ft transmission range.

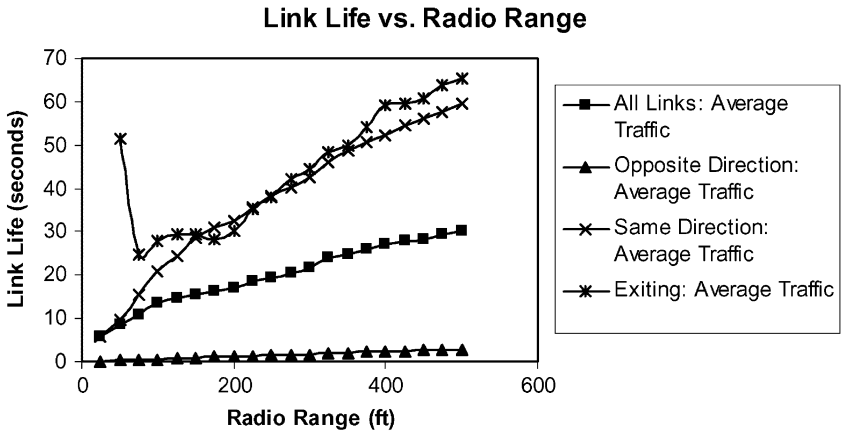

Fig. 2. Link life for various radio ranges.

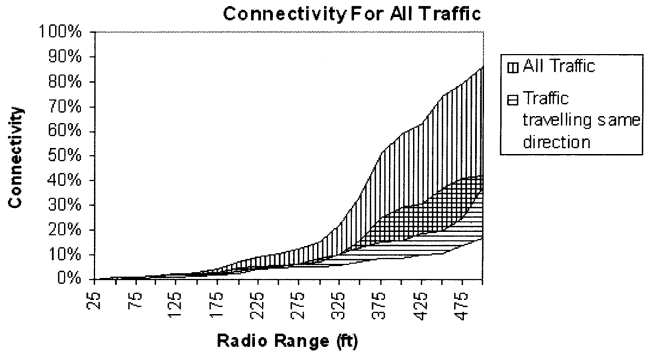

Fig. 3. Network connectivity by radio range.

3) Small Effective Network Diameter: As poor as the nodal connectivity is, the effective network diameter is actually worse. Rapid changes in link connectivity cause many paths to disconnect before they can be utilized.

Proactive routing is only suitable for small networks with limited mobility due to the overhead of maintaining the data on the full network topology at each node. Reactive routing was designed to improve this by initiating route discovery only when a path is needed. However, for IVC, a path may cease to exist almost as quickly as it was discovered.

Fig. 4 shows the expected path lifetime using only nodes traveling in the same direction versus the path setup time for a communication range of 250 ft. In NS, an ftp connection in a wireless network was simulated. There was no other network traffic at the time so, in reality, the response time would actually be worse. As shown in this figure, at approximately nine hops, before the first packet can be acknowledged, the path has disappeared. Furthermore, the precipitous drop in route lifetime indicates that sending even a relatively small message over three or four hops is likely to suffer a route error. Therefore, protocols that find routes before sending messages are likely to perform poorly in IVC networks.

4) Limited Redundancy: The redundancy in MANETs is crucial to providing additional bandwidth and security features. If additional bandwidth is desired, more nodes can be added. Security schemes use independent redundant paths to provide secure message transport. However, in IVC, the redundancy is limited both temporally and functionally.

The limited route lifetime becomes even more acute if multiple routes are needed simultaneously. The effective lifetime of this bundle of routes is the lifetime of shortest lived route. Clearly, this is problematic for schemes whose robustness requires multiple routes.

As noted by earlier research, one of the most critical factors limiting the bandwidth in a generic MANET is the number of exposed nodes. Furthermore, there is a relationship between radio range and the number of exposed nodes. This relationship is quadratic for a completely random mobility model. Because of constraints on movement, the number of exposed nodes for IVC only grows linearly. This linear relationship might present hope for increased throughput in IVC. However, the available transmission medium is also saturated linearly, so the slower growth in the number of exposed nodes does not yield better throughput.

The maximum for vehicles traveling on a given section of highway is a function of the bit rate and the interference radius. Since a vehicle will only transmit data if it hears no transmissions in its interference radius, only one vehicle will transmit within this neighborhood. Consequently, the maximum throughput is given by (1), where $T_{\max}$ is the maximum throughput, B_r is the bit rate, L is the highway length, and R_i is the interference radius.

$$T_{\max} = B_r * L/(2 * R_i). \tag{1}$$

Since the interference radius is proportional to the radio range, increasing the radio range to increase link stability, path life, or network connectivity will decrease the network throughput. Furthermore, since the network throughput is severely limited, adding redundant nodes to the network will not increase bandwidth as it did for other MANETs.

IV. Design Implications

These differences between IVC networks and other MANETs have implications for the design of IVC communications architecture. The IVC physical, link, and network layers must address the limited bandwidth as well as the unstable and fragmented network topology. Security mechanisms in the IVC network must also work within the constraints of the limited bandwidth and cannot rely on the redundancy normally present in MANETs.

A. Physical Layer Implications

One of the most acute challenges that will be faced by the IVC network is the high demand for limited bandwidth. There are two types of safety-critical messages that will likely be transmitted over the network. A-periodic messages will contain information about roadway and environmental hazards and will be transmitted only occasionally, but with a requirement of fast and guaranteed delivery. Periodic messages containing the vehicle position, dynamics, and driver intentions will likely be transmitted at a very high frequency—between 10–20 times per second for each vehicle.

The limited bandwidth in the IVC network can be partially addressed at the physical layer. Different frequency bands could be devoted to the different types of messages, with varying transmission powers for

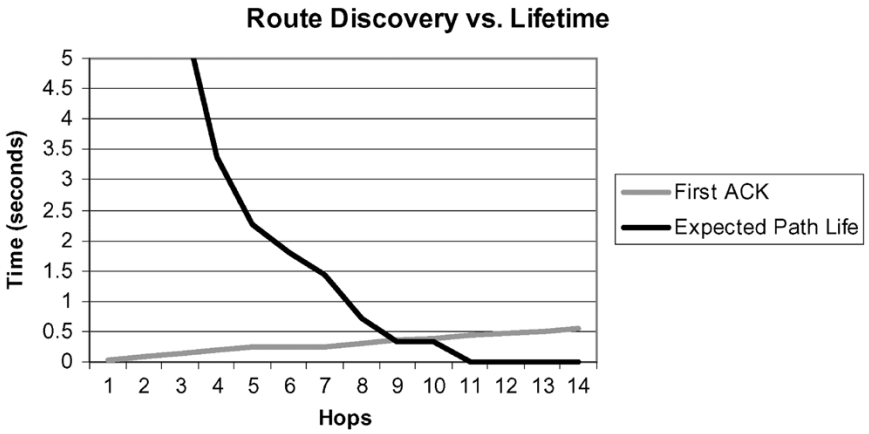

Fig. 4. Route lifetime versus route setup time.

each. For example, one approach uses a combination of low-frequency long-range infrastructure-based communications and high-frequency vehicle–vehicle communication in order to accommodate the varying delivery requirements for each message type [18].

The transmission power can be adaptively lowered to the point where it is just enough so that it is enough to reach a recipient. This reduces the interference range and, thus, linearly increases the network throughput, as seen in (1). Initially, with low levels of IVC equipment deployment, longer transmission ranges have been proposed as a way to realize multihop communication [19].

Another way to reduce the interference range is to use directionalized antennae. In this way, a transmission interferes only with nodes in the direction of the transmission. However, directionalized antennas increase the number of hidden nodes and, as shown later, have an adverse affect on intrusion-detection systems.

B. Link Layer Implications

The link layer must address a number of important issues related to bandwidth utilization. For example, it must address congestion control, latency, throughput, fairness, and scalability with respect to the number of equipped vehicles.

The 802.11 Distributed Coordination Function has been proposed for use for the IVC link layer [20]. Unfortunately, given the high demand for bandwidth, this approach is likely to result in a large number of collisions. Explicit allocation of timeslots, frequencies, or codes is problematic because of the highly dynamic topology of the IVC network. When vehicles encounter congestion, the number of vehicles within radio range sharply increases, necessitating a reallocation of the codes. High relative velocities also contribute to a need for reallocation.

In other MANETs, the addition of nodes provided additional bandwidth and exposed nodes are a primary factor in limiting bandwidth. Due to constraints on mobility, in an IVC network, the limit on available bandwidth is reached more quickly. Adding additional nodes will not increase bandwidth. Furthermore, the slower growth in the number of exposed nodes with respect to radio range fails to represent this situation.

Congestion control at this layer must organize access to the limited media in an equitable and efficient manner. Safety-critical messages must have guarantees on their delivery. This guarantee could be provided through the separation in time or space of these transmissions. For example, time slots or spectrum could be reserved. Alternatively, additional radio operating on a different frequency could be added to completely separate these messages. This additional radio would allow for the simultaneous transmission and reception of safety-critical messages.

One approach to distributed reservation scheme extends the R-ALOHA protocol [21]. In this protocol, vehicles rely on their neighbors to determine if their request for a slot has succeeded. However, given the volatility of neighbor sets under vehicular mobility, it is unclear if this approach will yield an unacceptably high number of collisions.

Other decentralized schemes that avoid collisions altogether allocate time slots based on the location of the vehicles [22], [23]. The roadway is discretized into cells such that only one vehicle may occupy a cell at a time. Each cell is associated with a time slot or channel that is assigned in such a way to prevent collisions while promoting special reuse.

C. Routing Layer Implications

The IVC routing layer must efficiently handle rapid topology changes and a fragmented network. Current MANET routing protocols fail to fully address these specific needs.

Neither proactive nor reactive routing protocols are suitable for the IVC network. Proactive protocols will be overwhelmed by the extremely rapid rate of change in the topology. Reactive protocols are problematic in that they attempt to discover a route before sending a message. Unfortunately, the routes discovered have an expected lifetime that precludes all but the routing of the shortest of messages.

The alternative then is to use location-based routing. Briesemeister *et al.* argue that this should be used because messages will likely be delivered to vehicles in a zone of relevance for a given message [24]. More importantly, it is shown here that is no other feasible way to deliver messages. There is a problem with zone-of-relevance approach is that it may be difficult to discern the location of vehicles that are interested in a message. So, for more generic delivery protocol, a location service or equivalent mechanism is needed for vehicles to obtain location data used for routing decisions.

However, location-based routing, in and of itself, does not address the frequent fragmentation of the network. For this, IVC routing will need to utilize other means, such as epidemic routing protocols and hybrid communication strategies. Epidemic routing protocols require the prioritization of messages in the transmission queue; this prioritization should reflect the time- and distance-varying importance of the IVC messages [25], [26]. The reliable transmission of messages to distant vehicles may also require out-of-band means; for example, via cellular network.

Specific adaptations of location-based routing for IVCs propose the routing of packets along the road network [27]. Due to the constraints on vehicle movement imposed by the roadway, greedy location-based forwarding algorithms may result in suboptimal routes.

D. Security Implications

Security mechanisms developed for other MANETs have limited applicability for the IVC network. The need for additional bandwidth, reliance of nodal overhearing, and redundancy requirements render them largely unsuitable.

Wireless media is particularly susceptible to denial-of-service attacks, including resource exhaustion and jamming. The protocols should be developed so that deliberate resource-exhaustion attacks can be detected easily. The mitigation of jamming threats with spread-spectrum techniques heightens scalability issues due to its increased bandwidth requirements.

Current MANET intrusion-detection systems will not work if directionalized antennas are used. The intrusion-detection techniques rely on eavesdropping on both upstream and downstream messages. Using directionalized antennas will prevent the nodal overhearing of downstream messages. One approach to utilize these systems would be to deploy a network of fixed receivers on the roadside. However, this involves overcoming the barrier of significant infrastructure investment.

Secure message-transport techniques require the utilization of multiple routes. This is problematic due to the limited temporal availability of routes. Moreover, in addition to limiting the ability to employ spread-spectrum techniques, limited bandwidth also limits the availability of redundant paths for security purposes.

This limited bandwidth also restricts the frequent use of cryptographic techniques, including digital signatures and the distribution of public key certificates and certificate revocation lists, which increase message size. Increasing the size of periodic messages in other MANETs is a more readily acceptable technique, since routes and associations between nodes are more stable. However, in the IVC network, where routes and nodal associations are short lived, this tradeoff of bandwidth for security may not be satisfactory.

V. Conclusion and Future Work

In conclusion, the IVC network exhibits very different characteristics from other MANETs. Specifically, the constraints on vehicle movements, varying driver behavior, and high mobility cause rapid topology changes, frequent fragmentation of the network, a small effective network diameter, and limited utility from network redundancy. These changes have implications for the IVC architecture at the physical, link, network, and application layers. At these layers, adjustments must be made to effectively use the limited bandwidth and efficiently function in the rapidly changing network.

Future analysis, which the authors intend to perform, will examine the IVC network under a variety of traffic and roadway situations. Furthermore, the authors intend to tightly couple CORSIM and NS2 together to allow the content of IVC messages to alter driver behavior. The ultimate goal will be to use this analysis to design effective and secure protocols for the IVC network.

Acknowledgment

The authors would like to thank the students and faculty members at the University of California, Berkeley, for making available the NS simulator and the students and faculty members of the Monarch Project, Carnegie Mellon University, Pittsburgh, PA, for their *ad hoc* network extensions to NS. The authors would also like to thank G. McHale of the Federal Highway Administration for his assistance in using the CORSIM simulator. Finally, they would like to acknowledge the assistance of the Partners for Advanced Transit and Highways (PATH) program at the University of California for making available the traffic-flow data used in this paper.

References

[1] S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC protocol work well in multihop wireless *ad hoc* networks?," *IEEE Commun. Mag.*, vol. 39, pp. 130–137, Mar. 2001.

[2] D. D. Perkins, H. D. Hughes, and C. B. Owen, "Factors affecting the performance of *ad hoc* networks," presented at the IEEE Int. Conf. Communications, New York, 2002.

[3] E. M. Royer and C.-K. Toh, "A review of current routing protocols for *ad hoc* mobile wireless networks," *IEEE Pers. Commun.*, vol. 6, pp. 46–55, Apr. 1999.

[4] M. Mauve, J. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *IEEE Network*, vol. 15, pp. 30–39, Jan./Feb. 2001.

[5] Y.-B. Ko and N. H. Vaidya, "GeoTORA: A protocol for geocasting in mobile *ad hoc* networks," presented at the International Conf. Network Protocols, Osaka, Japan, Nov. 2000.

[6] S. R. Das, R. Castañeda, and J. Yan, "Simulation-based performance evaluation of routing protocols for mobile *ad hoc* networks," *Mobile Networks Applicat.*, vol. 5, pp. 179–189, 2000.

[7] J. Tian, J. Hähner, C. Becker, I. Stepanov, and K. Rothermel, "Graph-based mobility model for mobile *ad hoc* network simulation," presented at the 35th Annual Simulation Symp., San Diego, CA, Apr. 2002.

[8] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark, "Scenario-based performance analysis for routing protocols for mobile *ad-hoc* networks," presented at the Annu. Int. Conf. Mobile Computing and Networking, Seattle, WA, Aug. 1999.

[9] W. Su, S.-J. Lee, and M. Gerla, "Mobility prediction and routing in *ad hoc* wireless networks," *Int. J. Network Manag.*, vol. 11, pp. 3–30, 2001.

[10] A. Vahdat and D. Becker, "Epidemic routing for partially-connected *ad hoc* networks," Tech. Rep. CS-200 006, Duke Univ., Durham, NC, Apr. 2000.

[11] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," presented at the SCS Communication Networks and Distributed Systems Modeling and Simulation Conf., San Antonio, TX, Jan. 2002.

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for *ad hoc* networks," presented at the Working Session Security *ad hoc* Networks, Lausanne, Switzerland, 2002.

[13] Y. Zhang and W. Lee, "Intrusion detection in wireless *ad-hoc* networks," presented at the Annu. Int. Conf. Mobile Computing and Networking, Boston, MA, Aug. 2000.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," presented at the Annu. Int. Conf. Mobile Computing and Networking, Boston, MA, Aug. 2000.

[15] L. E. Owen, Y. Zhang, L. Rao, and G. McHale, "Traffic flow simulation using CORSIM," presented at the 2000 Winter Simulation Conf., Orlando, FL, Dec. 2000.

[16] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless *ad hoc* network routing protocols," presented at the 4th Annu. ACM/IEEE Int. Conf. Mobile Computing and Networking, Dallas, TX, 1998.

[17] K. Petty, *FSP 1.1: The Analysis Software for the FSP Project*. Berkeley: Univ. California Press, 1994.

[18] K. A. Redmill, M. P. Fitz, S. Nakabayashi, T. Ohyama, F. Ozguner, U. Ozguner, O. Takeshita, K. Tokuda, and W. Zhu, "An incident warning system with dual frequency communications capability," presented at the IEEE Intelligent Vehicles Symp., Columbus, OH, June 2003.

[19] A. Ebner, H. Rohling, L. Wischoff, R. Halfmann, and M. Lott, "Performance of UTRA TDD *ad hoc* and IEEE 802.11b in vehicular environments," presented at the 57th IEEE Vehicular Technology Conf., Jeju, South Korea, Apr. 2003.

[20] J. Zhu and S. Roy, "MAC for dedicated short range communications in intelligent transport system," *IEEE Commun. Mag.*, vol. 41, pp. 60–67, Jan. 2003.

[21] F. Borgonovo, A. Capone, M. Cesana, and L. Fratta, "ADHOC: A new, flexible and reliable MAC architecture for *ad-hoc* networks," presented at the Wireless Communications and Networking Conf., Mar. 2003.

[22] S. V. Bana and P. Varaiya, "Space division multiple access (SDMA) for robust *ad hoc* vehicle communication networks," presented at the IEEE Int. Conf. Intelligent Transportation Systems, Oakland, CA, Aug. 2001.

[23] S. Katragadda, G. Murthy, R. Rao, M. Kumar, and R. Sachin, "A decentralized location-based channel access protocol for inter-vehicle communication," presented at the 57th IEEE Vehicular Technology Conf., Jeju, South Korea, Apr. 2003.

[24] L. Briesemeister, L. Schafers, and G. Hommel, "Disseminating messages among highly mobile hosts based on inter-vehicle communication," presented at the IEEE Intelligent Vehicles Symp., Dearborn, MI, Oct. 2000.

[25] B. Xu, A. Ouksel, and O. Wolfson, "Opportunistic resource exchange in inter-vehicle *ad-hoc* networks," presented at the IEEE Int. Conf. Mobile Data Management, Berkeley, CA, Jan. 2004.

[26] L. Wischhof, A. Ebner, H. Rohling, M. Lott, and R. Halfmann, "Adaptive broadcast for travel and traffic information distribution based on inter-vehicle communication," presented at the IEEE Intelligent Vehicles Symp., Columbus, OH, June 2003.

[27] J. Tian, L. Han, K. Rothermel, and C. Cseh, "Spatially aware packet routing for mobile *ad hoc* inter-vehicle radio networks," presented at the Intelligent Transportation Systems Conf., Shanghai, China, Oct. 2003.