

Joseph P. Macker<sup>a</sup>

macker@itd.nrl.navy.mil

M. Scott Corson<sup>b</sup>

corson@isr.umd.edu

<sup>a</sup> Information Technology Division, Naval Research Laboratory, Washington, DC, USA

<sup>b</sup> Institute for Systems Research, University of Maryland, College Park, MD, USA

*This article provides a snapshot of work underway within the Mobile Ad hoc NETWORKS (MANET) Working Group of the Internet Engineering Task Force (IETF). The article summarizes the proceedings of the last MANET WG meeting, presents some issues currently under discussion on the MANET mailing list (manet@itd.nrl.navy.mil), and gives some rationale behind the architectural design approach being promoted within the group.*

## I. Proceedings of the Chicago Manet WG Meeting

The manet WG held two sessions of two hours each. The presentation and discussion topics covered a number of important mobile routing areas including: existing draft status, implementation progress, new multicast approaches for manet, security design issues for manet, addressing considerations, and several new draft routing proposals. Past WG meetings have held discussions on various simulation tools for the purpose of manet protocol performance analysis. The group made significant recent progress towards a common set of simulation and analysis tools (ns-2 extensions for mobility were briefed Monday, and the code is now publicly available and implementations of several of the proposed draft protocols will soon be included). This progress in the mobile network simulation area is a very encouraging and important result for the group.

Implementations of various manet protocol proposals now exist and status was briefly updated relating to the various Internet Drafts (IDs) at the beginning of the meeting [1, 2, 3, 4, 5]. Subsequently, new proposals and protocol enhancements were presented by various parties. A more “proactive” optimized link state technique with efficient multipoint relaying for flooding control traffic within a manet was presented [6]. Various multicast enhancements were also discussed and a new multicast approach which is independent of any particular manet unicast approach was presented [7]. In addition, several multicast extensions to existing protocols (i.e., TORA [3] and AODV [4]) were outlined by developers. The group is beginning to discuss security issues in the context of manet, and a candidate manet security approach [8] was presented outlining authentication techniques for inclusion in the IMEP protocol. A number of manet protocols now intend to use the IMEP protocol [2], which is a proposed common link status sensing, neighbor discovery, packet aggregation and flexible interface mechanism that is independent of particular routing algorithms.

Open WG discussion took place in addition to presentations and several important topics arose during this segment of the meetings. First, a recommendation to explore alternative address management schemes for manet was presented. Opinions differed on this topic, and it was suggested that more detailed discussion be taken to the mailing list for ongoing exploration. Second, the group generally agreed that a common baseline set of network scenarios, mobility models, and distributed traffic models should be developed to assist

in cross protocol evaluation. Several group members offered to input ideas and guideline proposals in this area. The goal would be to promote future evaluations that cover a broad design space and sufficiently exercise protocol limitations and strengths across protocol families. Third, the importance of an applicability statement was resurfaced by the chairs and several group members to ensure concise communication of a protocol design assumptions and expected limitations. The development of a strawman outline for applicability statement guidance was suggested. The WG plans on developing such a draft applicability statement guideline and working this issue on the mailing list.

In conclusion, progress was evidenced in implementations and the recent release of common simulation extensions for manet. New work was added into the group, including several new protocol drafts and early work on security and multicast for manet. Work remains in defining and reaching consensus on specific manet evaluation scenarios (e.g., mobility models, traffic models) and applicability statement guidance for group use.

The following sections give more details regarding various presentations.

### I.A. CBRP

Mingliang Jiang from the University of Singapore presented the Cluster-Based Routing Protocol (CBRP) [9]. The protocol concept is based upon a well-known clustering algorithm developed at the Naval Research Laboratory and the University of Maryland, and also recently adopted in work at UCLA. The algorithm constructs a set of node clusters, each cluster having a special node designated as the clusterhead, with the property that every non-clusterhead node is directly connected to a clusterhead. The algorithm also builds a tree consisting of clusterheads and nodes (termed gateways) interconnecting the clusterheads of neighboring clusters. The unique design motivation of the proposers of CBRP is to use the shared tree to reduce the overhead of the control packet flooding required by dynamic source routing. In CBRP, while the shared tree is used for more efficient flooding the actual routing of data is performed using a form of dynamic source routing that is similar to the scheme proposed for ad hoc routing from Carnegie Mellon. In CBRP, source routes are constructed from a source through a set of intermediate clusterheads to a destination. Usage of source routing is considered desirable in that it has the ability to make use of end-to-end routes which consist fully or

partially of unidirectional links.

### **I.B. OLS**

Amir Qayyum from INRIA presented a draft on an Optimized Link State (OLS) algorithm [6]. The approach presented is optimized in the sense that it does not require propagation of full topology knowledge to all nodes, but still guarantees the generation of shortest-path routes to all nodes. The algorithm is intended to run atop IMEP, and to utilize multipoint relaying concepts to disseminate topology information.

### **I.C. AMRoute**

Rajesh Talpade from Bellcore presented a draft on the Ad hoc Multicast Routing Protocol (AMRoute) [7]. The basic concept behind the protocol's design is to have only routers to which multicast hosts are affiliated maintain multicast forwarding tree state. Both senders and receivers are on this bi-directional, shared tree. This is accomplished by tunneling multicast packets between such routers. This has the advantage of being independent of the underlying unicast routing protocol. Another feature of the protocol is that while it is core-based, they are not cores in the traditional sense (e.g. CBT) in that they are not central points for data distribution. These cores assist in member detection and tree formation, and can dynamically migrate among the members nodes. Thus the cores serve a group management functionality, making this an interesting aspect of the protocol.

### **I.D. Carnegie Mellon Simulation Work**

Dave Johnson from CMU presented an overview of work he and several others have been doing in adding mobility extensions to the NS-2 simulation toolkit and simulating particular MANET protocols. The NS-2 simulator is a very desirable software platform to use for several reasons. First of all, it is freely available and can turn most widely available desktop or laptop computers into first-rate simulation platforms. Secondly, it is object-oriented—being written in both OTCL and C++—and can be configured and extended with probably as little pain as is possible given the current state-of-the-art in simulation technology. Thirdly, it comes with a rich set of layered protocol models such as: many flavors of TCP, some multicast protocols and enhanced router queueing. These varied models allow for future detailed studies of various Internet traffic conditions and alternatives over MANETs. CMU's contribution consists of two parts: generic MANET simulation objects such as wireless channel and mobility models, and a first cut at simulating several of the proposed manet routing protocols including DSR, DSDV, AODV and TORA. CMU is planning on making these models available to the rest of the working group. This is a fantastic contribution to the group's efforts.

### **I.E. Sun Microsystems Simulation Work**

Charlie Perkins from Sun briefly presented work he has been involved with on developing MANET simulation technology for the NS-2 simulator. While the motivation is the same as for the CMU work, the two approaches differ in some of the details and level of simulation. For example, the CMU channel

model is possibly being aimed at a highly accurate representation of the signalling environment, whereas the Sun approach is simpler, choosing to model the channel at a coarser level of fidelity. Also, the two efforts have initially developed slightly different mobility models for MANETs. It will be interesting to examine the differing approaches and to develop a set of common simulation models and scenarios for protocol evaluation within the group. Thanks also from the group to all the folks associated with this effort.

### **I.F. LAM**

Scott Corson from the University of Maryland presented a draft on a Lightweight Adaptive Multicast (LAM) protocol [10]. LAM creates and maintains a group-shared forwarding tree for the group. Conceptually, the protocol can be viewed as a fusion of CBT [11] and TORA. The design of the protocol follows the concept of vertically-coupled design to achieve efficiency (low overhead, fast reaction), which is desired in a MANET environment. LAM is specifically built upon TORA, and serves as an integrated component of an IMEP-TORA-LAM manet routing suite. This direct coupling enables LAM to benefit from TORA's mechanisms while reacting to topological changes. Also, during periods of stable topology and constant group membership, the LAM protocol does not introduce additional overhead because it does not require timer-based messaging during its execution.

### **I.G. AODV Multicast**

Charlie Perkins from Sun presented an updated draft of AODV with a new extension to support multicast routing [4]. The extension incorporates the notion of a multicast grouphead, a special node which is the first multicast group member in a connected network portion. The extension reuses the destination sequence number mechanism of unicast AODV to maintain loop freedom, and the grouphead is responsible for initializing and updating the multicast group destination sequence number. While not explicitly identified as such, the grouphead effectively functions as a traditional core (such as in CBT) in that it is a part of the shared, bi-directional multicast data forwarding tree, and is central to the construction and maintenance of the shared tree. Unlike CBT, should the grouphead fail or become partitioned from its previous network portion, AODV specifies a mechanism by which some other node in the network portion will dynamically elect itself as grouphead and form a new tree. AODV also specifies a mechanism by which two previously disconnected trees can merge into a single tree.

### **I.H. Manet Authentication Architecture**

Stu Jacobs from GTE presented a draft on a proposed Manet Authentication Architecture [8]. It is known that wireless links are vulnerable to eavesdropping, replay, spoofing, and other attacks. In the absence of sufficient link-layer security support, some mechanism is required in many contexts to mutually authenticate routers before they begin exchanging network control traffic. The architecture specifies a shared key mechanism based on a keyed-MD5 hash, as well as four levels of public key-based authentication requiring periodic verification via a certificate authority. The default mode is currently no authentication. While the architecture's authentication mechanisms

are logically independent of IMEP or any other routing support protocol, they are presently intended to be implemented in IMEP, requiring the addition of authentication and certificate objects to IMEP. This extended IMEP security functionality ensures that the authentication mechanisms may be used by any network control protocol using the IMEP specification.

## II. Manet Concepts and Architectural Summary

Previous articles in this series have summarized the work underway in the WG, and have detailed various aspects of the network architecture being promoted within the manet WG. Here, for clarity, we first summarize some key concepts of the architecture, and then discuss several aspects of a developing architectural approach.

### II.A. Concepts

As detailed in [12], a MANET consists of mobile platforms—herein simply referred to as “nodes”—which are free to move about arbitrarily. Each node logically consists of a router, one or more hosts and one or more wireless communications devices, see Fig. 1. A MANET is an autonomous system of mobile nodes. The nodes may consist of separate, networked devices (see Fig. 1b), or may be integrated into a single device such as a laptop computer (see Fig. 1c). The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people.

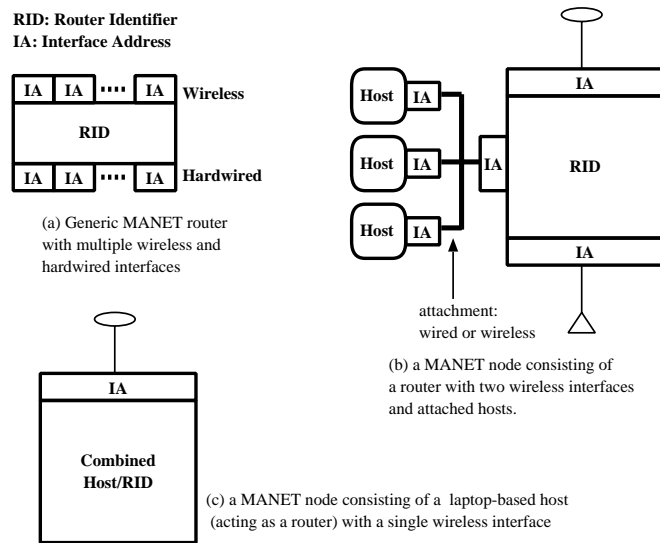


Figure 1: The generic MANET router structure and two possible MANET node configurations.

The nodes are equipped with wireless transmitters and receivers using antennas which may be omnidirectional (broadcast), highly-directional (point-to-point) or some combination thereof. At a given point in time, a wireless connectivity in the form of a random, multihop graph or “ad hoc” network exists between the nodes (see Fig. 2b).

MANETs have several salient characteristics: dynamic topologies; bandwidth-constrained, variable capacity links; potentially energy-constrained routers; and limited physical

security [1]. Additionally, some envisioned networks (e.g. mobile military networks or future commercial networks) may be relatively *large* (e.g. hundreds or possibly thousands of nodes per autonomous system).

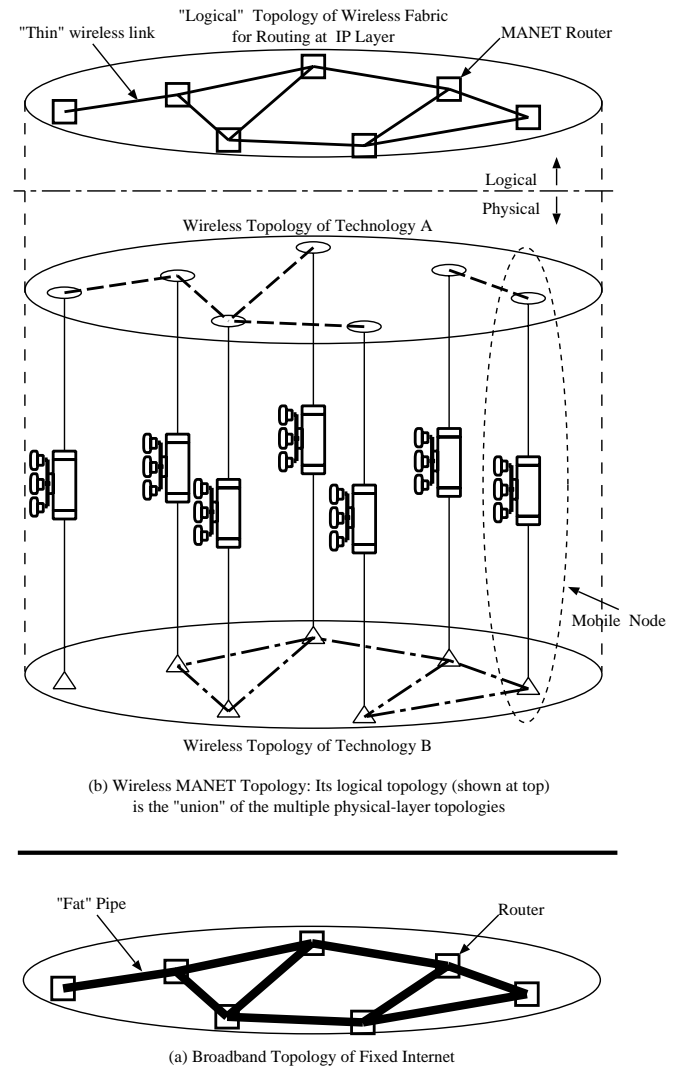


Figure 2: Fixed network and MANET Topologies. Subfigure (b) shows a MANET consisting of two wireless technologies (*A* and *B*), and their logical union which forms the “wireless fabric” for routing at the IP-layer. It is interesting to note here that the topology of a MANET resembles that of the larger, fixed network—only in microcosm; i.e. each mobile node—with its collection of hosts—resembles a subnet, and the routers route information between these “mobile subnets” through the wireless fabric.

When multiple wireless technologies are available in a mobile network, it is technically desirable that routing occur at the IP layer (see Fig. 2b). The figure gives an example network consisting of mobile nodes (e.g. each could be a car or tank), where each node consists of a mobile router with two different wireless devices attached, as well as an attached set of IP-addressable hosts and other devices. In general, the wireless connectivity and, hence, the network topology corresponding to each wireless technology (*A* and *B*) will be different. Thus, adjacent nodes may be connected by one or both technologies. By routing at the IP layer, it is possible to flexibly, efficiently

and robustly forward a packet through the wireless “fabric” consisting of the logical *union* of the topologies of the individual wireless technologies.

For example, in Fig. 2b, a packet may initially be routed via wireless technology *A* for several hops, and then switched to technology *B* on subsequent hops because either more capacity is available there, or because no connectivity exists in technology *A*’s topology. In single-technology (i.e. “subnet-based”) routing, lack of connectivity in topology *A* would either have caused the packet to be dropped, or its restriction to the slower technology *A* would have resulted in higher end-to-end latency. Thus, it can be seen that the ability to dynamically route mixing *both* wireless technologies (by routing through the wireless *fabric*) gives added power and flexibility to the routing and forwarding algorithms, including more robustness to topological changes and potentially higher performance as well. Please refer to [12] for a more detailed discussion.

Support for multi-technology routing is already being evidenced in several proposed protocols [5, 3, 2].

## II.B. Architectural Summary

While the manet WG’s charter is to standardize routing technology for MANETs, this should be done in a fashion cognizant of and in accordance with an overall architecture well-suited for supporting future mobile Internet standards efforts, and of achieving and maintaining interoperability with the current and likely future Internet.

In the following, we discuss the role of manet technology as part of the larger, emerging mobile Internet, and summarize a developing manet architectural concept.

### II.B.1. A Mobile Internet

Conceptually, the emerging “mobile Internet” can be divided into two layers relative to the fixed network—which we term the “mobile host” and “mobile router” layers (depicted in Fig. 3).

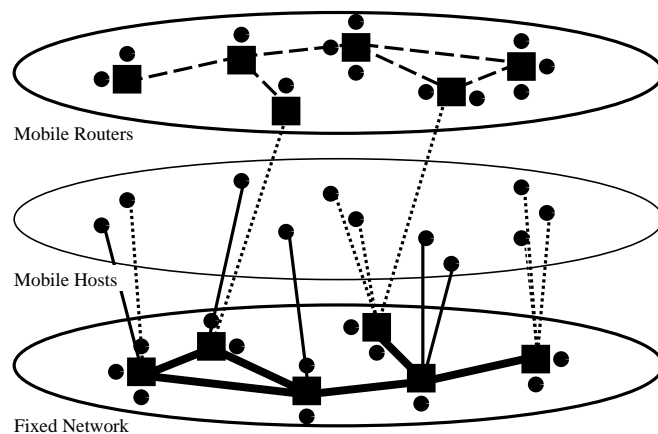


Figure 3: The emerging “mobile Internet”—the Mobile Host and Mobile Router layers—and its relationship with the traditional fixed network.

The mobile host layer consists of hosts temporarily attached to routers on the fixed network, termed “fixed routers” (this paradigm is supported by approaches such as mobile IP and DHCP). These hosts are logically “one hop” from a fixed

router, and their connections may be wired or wireless. Principle functions handled by this layer are location and address management relative to the fixed network. This functionality requires routing support from the fixed network infrastructure.

The mobile router layer consists of mobile routers and mobile hosts, with each mobile host permanently or temporarily affiliated with a mobile router<sup>1</sup>. The mobile router layer need not require routing support from the fixed network, as it forms a mobile infrastructure *parallel* to the fixed infrastructure. Conceptually, one can view the mobile router layer as an alternative to the fixed network layer, albeit a relatively undesirable one for some communications due to its relatively low capacity. Because of this, it is envisioned that, in the near term, the mobile router layer will operate as a “stub” network from the perspective of the fixed network, carrying only traffic that is either sourced or destined for a host in the mobile router layer<sup>2</sup>. Also, while the mobile router layer can be viewed *logically* as a unified network parallel to the fixed network, in the near term, it will likely be partitioned into separate autonomous systems of mobile routers. It remains to be seen whether future technology advances allow removal of these restrictions, permitting creation of a *globally-unified* wireless network carrying *transit* Internet traffic in parallel with the fixed network.

From the manet perspective, a host in the mobile router layer may be in one of two states relative to the fixed network: “disconnected” or “greater than one hop” from the fixed network. When disconnected, the MANET in which the host resides forms an autonomous system *independent* of the fixed network. When connected, at least one mobile MANET router is between the mobile host and a fixed router (the fixed router forming a gateway to the fixed network). In the special case where a mobile device is *both* a MANET router and mobile host, the hop between the router and host is only virtual. This hop (or connection) between a mobile host and a MANET router may be wired or wireless, whereas the connections between MANET routers are generally assumed to be wireless.

In the context of this two-layer conceptualization, the role of the manet WG is to develop routing standards for the mobile router layer. While the WG is not chartered to develop protocols for manet/fixed network interoperability, it should consider the implications of its approach on future interoperability efforts.

## II.C. Architectural Approach

The mobile router layer consists of mobile routing infrastructure. The purpose of a manet architecture is to structure the mobile infrastructure, fixing some of its aspects while leaving others flexible, permitting these to be developed as needed over time. The goal of our approach is to specify an architecture which gives future designers maximum *flexibility* in designing MANET control protocols (i.e. policies). Aspects of the infrastructure identified thus far for inclusion in the architecture include addressing and router authentication.

<sup>1</sup>In some cases this distinction is only logical, as a single device may be both a mobile host and a mobile router.

<sup>2</sup>Operation as a full-fledged “transit” network would require carrying traffic with both source and destination addresses outside the mobile router layer. This mode of operation significantly increases operational complexity and is considered infeasible in the near term.

### II.C.1. Addressing

A sufficient addressing architecture appears to be one which supports the following requirements:

1. *interoperability* via adherence to the IP addressing architecture;
2. *simultaneous use of multiple wireless technologies* (support for routing through the wireless fabric); and
3. the presence of *multiple hosts per router*.

These requirements can be realized by an addressing architecture that specifies:

- identifying router and host interfaces with IP addresses (satisfies requirement 1);
- identifying a router with a separate Router ID (RID) (permits requirement 2); and
- one (*or more*) interfaces per router (permits requirement 3).

This approach essentially says to duplicate the practice already followed in parts of the fixed network (e.g. [14]), as this practice appears to be sufficient for building a mobile routing infrastructure as well.

Note that this approach does not specify *how* IP addresses are assigned to interfaces (on host or routers), or *what* the RID is and *how* it is assigned. This is a separable issue, although one which is related to routing. The intent is that the RID not be visible outside the network layer—it is only to be used internally by the routing algorithms.

Policies and protocols for RID and IP address assignment will be developed on an as-needed basis. These policies should reflect the nature of a MANET domain, just as the routing policy should reflect the nature of the domain. It is the view here that policies should be dynamic (i.e. varying from domain to domain), but core elements of the infrastructure such as the addressing architecture should be uniform throughout the mobile infrastructure. This uniformity facilitates interoperability between policies and with the fixed network.

### II.C.2. Router Authentication

Recent work has begun on developing approaches for MANET router authentication [8]. The architectural aspect of this work consists of determining which aspects of the problem are independent of any particular routing policy, and independent of any particular authentication policy. Work thus far has determined that authentication (and in some cases certificate) object exchanges are necessary, and that an additional mechanism is required for coordinating these exchanges over multiple hops *without* using information provided by a routing protocol. The approach put forth in [8] is fragmentary, and much work remains to be done.

### II.D. Protocol Design

While preservation of protocol design *flexibility* is the goal of the manet architectural approach, *efficiency*—in terms of either *bandwidth* or *energy* usage—is the principle goal of behind MANET protocol design. This approach differs somewhat from the design approach prevalent in the fixed network, largely because the resource constraints *differ* in the

two environments. In the fixed network, the principle constraints are *processing* and *storage* capacity within the routers themselves—not bandwidth or energy as in MANETs. The net effect on MANET protocol design is a shift from vertically-decoupled protocol layers with intensive horizontal peer-to-peer communication (in the fixed network) to more vertically-coupled protocol layers with minimal horizontal communication. This issue is examined in more detail in [13].

Usage of this design approach is already being evidenced in the case of multicast routing protocol design, where a close coupling between unicast and multicast routing functionality is being proposed [4, 10], and in the case of neighbor sensing and other mechanisms, where several proposed protocols [3, 6, 8] are designed to utilize IMEP for various functions.

## III. Conclusions

From the preceding, it is clear that there are many issues facing the MANET WG. Its charter is to develop IP routing technology, but this should be done with an eye towards developing an architecture well-suited for supporting the future standards efforts, and of achieving interoperability with the current and likely future Internet.

## References

- [1] M. S. Corson and J. Macker. “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”. *Internet Draft (work in progress)*, 9/98.
- [2] M. S. Corson, S. Papademetriou, P. Papadopoulos, V. Park, and A. Qayyum. “An Internet MANET Encapsulation Protocol (IMEP) Specification”. *Internet Draft (work in progress)*, 9/98.
- [3] V. Park and M. S. Corson. “Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification”. *Internet Draft (work in progress)*, 9/98.
- [4] C. Perkins and E. Royer. “Ad Hoc On Demand Distance Vector (AODV) Routing”. *Internet Draft (work in progress)*, 8/98.
- [5] J. Broch, D. Johnson, and D. Maltz. “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks”. *Internet Draft (work in progress)*, 3/98.
- [6] P. Jaquet, P. Muhlethaler, and A. Qayyum. “Optimized Link State Routing Protocol”. *Internet Draft (work in progress)*, 8/98.
- [7] E. Bommaiah, M. Liu, A. McAuley, and R. Talpade. “AM-Route: Ad hoc Multicast Routing Protocol”. *Internet Draft (work in progress)*, 8/98.
- [8] S. Jacobs and M. S. Corson. “MANET Authentication Architecture”. *Internet Draft (work in progress)*, 8/98.
- [9] M. Jiang, J. Li, and Y. Tay. “Cluster Based Routing Protocol (CBRP) Functional Specification”. *Internet Draft (work in progress)*, 8/98.
- [10] L. Ji and M. S. Corson. “LAM: Lightweight Adaptive Multicast Protocol”. *Internet Draft (work in progress)*, 8/98.
- [11] A. Ballardie. “Core Based Trees (CBT) Multicast Routing Architecture”. *Internet RFC 2201*, 9/97.
- [12] J. Macker and M. S. Corson. “Mobile Ad Hoc Networking and the IETF”. *ACM Mobile Computing and Communications Review*, 2(1).
- [13] J. Macker and M. S. Corson. “Mobile Ad Hoc Networking and the IETF”. *ACM Mobile Computing and Communications Review*, 2(3).
- [14] J. Moy. “OSPF Version 2”. *Internet RFC 2328*, 4/98.