Performance of Routing Protocols for Mobile Ad-Hoc Networks

Madhavi W. Subbarao
Wireless Communication Technologies Group
National Institute of Standards and Technology
100 Bureau Drive Stop 8920
Gaithersburg, MD, USA 20899-8920
Phone: 301-975-4974 FAX: 301-590-0932 Email: subbarao@nist.gov

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Advances in information technology for these important types of situations are envisioned for future wireless communications. Such network scenarios cannot rely on centralized and organized connectivity, and can be termed as wireless *mobile ad hoc networks* (MANETs). A MANET is an autonomous collection of mobile users (nodes) that communicate over relatively bandwidth-constrained wireless links. Each node is equipped with wireless receivers and transmitters using antennas that may be omni-directional, highly directional, or possibly steerable. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is *decentralized*, where network organization and message delivery must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. Nodes must also contend with the effects of radio communication, including multiuser interference, multipath fading, and shadowing. A MANET may operate in a stand-alone manner, or be connected to a larger network, e.g., the fixed Internet.

The design of network protocols for MANETs is a complex issue. These networks need efficient *distributed* algorithms to determine network organization (connectivity), link scheduling, and routing. An efficient approach is to consider routing algorithms in which network connectivity is determined in the process of establishing routes. Message routing in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as power expended, variable wireless link quality, propagation path loss, fading, multiuser interference, and topological changes, become relevant issues. The network should be able to adaptively alter routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks desire to maintain a *low probability of intercept* and/or a *low probability of detection*. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection (or interception). A lapse in any of these requirements may degrade the performance and dependability of the network.

Various protocols have been recently proposed in the Internet Engineering Task Force (IETF) for executing routing in a MANET: Zone Routing Protocol (ZRP) \cite{HaaPea97}, Ad Hoc On Demand Distance Vector (AODV) Routing \cite{PerRoy98}, Temporally-Ordered Routing Algorithm (TORA) \cite{ParCor98}, Dynamic Source Routing (DSR) Protocol \cite{BroJohMal98}, Cluster Based Routing Protocol (CBRP) \cite{JiaLiTay98}, Ad Hoc

Multicast Routing Protocol (AMRoute) \cite{BomMcaTalLiu98}, Core Extraction Distributed Ad Hoc Routing (CEDAR) \cite{SivSinBha98}, On-Demand Multicast Routing Protocol (ODMRP) \cite{GerPeiLeeChi98}, and Optimized Link State Routing Protocol (OLSRP) \cite{JacMuhQay98}. Other projects are being pursued for mobile wireless networks, such as the Wireless Internet Gateways (WINGS) project \cite{GarFulMadBeyFri97} and the Multimedia Support for Mobile Wireless Networks (MMWN) \cite{RamSte97} and Density and Asymmetry Adaptive Network (DAWN) projects for DARPA's Global Mobile Information Systems (GloMo) program. While these protocols are not designed specifically for MANETs, they may provide enhanced performance and robustness over the proposed MANET routing protocols.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. It is unlikely that a single routing protocol will be optimal for all scenarios. A given protocol will execute efficiently in those networks whose characteristics are in accord with the mechanisms used by the protocol. However, any protocol must efficiently handle several inherent characteristics of MANETs:

- Dynamic topology: Mobility of nodes lends to unpredictable network topology.

- Variable capacity wireless links: Wireless links are bandwidth-constrained. Moreover, since wireless links have lower capacity than hardwired links, traffic congestion is typical rather than atypical. However, as a MANET is often an extension of a fixed network, the same services and demands must be accommodated. These demands will increase as multimedia computing and networking become more mainstream.

- Power constrained operation: Power conservation is *crucial* in mobile wireless systems since these networks typically operate off power-limited sources, which dictate whether a network is operational or not.

- Physical security: Mobile networks are more vulnerable to physical security threats such as eavesdropping and jamming attacks.

The merit of a routing protocol is judged with performance metrics, both qualitative and quantitative. Desirable *qualitative* properties of a MANET routing protocol include the following:

- Distributed: The decentralized nature of a MANET requires that any routing protocol execute in a distributed fashion.

- On demand operation: Since a uniform traffic distribution can not be assumed within the network, the routing algorithm must adapt to the traffic pattern on a demand or need basis, thereby utilizing power and bandwidth resources more efficiently.

- Loop-free: To ensure proper message delivery and efficient network operation, a routing protocol must be loop-free.

- Security: Since MANETs are more vulnerable to physical security threats, provisions for security must be made, e.g., the application of Internet Protocol (IP) security techniques.

- Entering/Departing nodes: A routing protocol should be able to quickly adapt to entering or departing nodes in the network, without having to restructure the entire network.

- Bidirectional/Unidirectional links: Since the condition of a MANET is dynamic, a routing protocol should be able to execute on both bidirectional and unidirectional links.

In this paper, we develop a dynamic power-conscious routing algorithm that incorporates physical layer and link layer statistics. This algorithm

Routing decisions are made based on feedback or information extracted from the received signal.

In this paper, we identify and define meaningful metrics for assessing the performance of MANET protocols. We design and build a unified simulation environment and evaluate the performance of the different protocols proposed in the IETF in different scenarios. Moreover, we identify critical features required for military MANETs and evaluate the protocols in this context.