“Standard” Evaluations *for* Ad Hoc Mobile Networks

The performance of networking protocols is very much dependent upon both the radio that the protocols are run on and the intended application(s) for which the protocol stack is designed and “tuned”. Thus, a network of commercial Wireless LANS with fixed power and no multipath support can not be expected to out perform a network which utilizes advanced radios with adaptive link controls and sophisticated multipath mitigation. Similarly, a network protocol that has been designed to provide maximum throughput on vehicular mounted radios should not be expected to have the same power efficiency as a protocol stack designed specifically to work on low power, lightweight, dismounted radio networks or unattended sensors.

However, there are some attributes of ad hoc mobile networks that are relatively universal and which should be characterized for any protocol stack. These include, for example: time to self configure, time to reconfigure/reroute around a failed node, and time to accomplish a net join. It should be possible to structure a series of evaluations that would characterize the performance of a networking protocol against these key attributes. Further, for specific applications/environments, these evaluations could be be expressed as “challenge problems” by adding the appropriate performance parameters (eg can a network of size x self configure within y seconds).

While it may not be possible to compare network protocols built upon different radios directly, it should be possible to assess the performance of each network as presented against the characteristics of interest and to determine whether the model/simulation predictions correspond well to physical measurements in the experiments. It may then be possible to compare different protocol stacks directly to each other in “virtual” simulation space by running the protocols on a common radio model. However, even here some caution is in order if the protocol stacks were intentionally optimized for different environments.

The GloMo physical experiments and measurements must then 1) characterize the performance of each protocol stack against the critical characteristics and 2) provide sufficient technical detail to enable model validation. For this, a standard set of “tests”/evaluation criteria should be devised to include test set up/configuration, instrumentation, and data reduction methods to be employed.

It is also important to stress the protocols in meaningful ways. We need to learn the conditions under which the protocols could “break down” and what the failure mechanisms are. More importantly, we need to ascertain whether the protocols will be able to support stressing situations that they are likely to encounter, and degrade gracefully and recover quickly when they do break down.

Real time voice traffic carries some specific challenges for mobile wireless networks because of the short packet sizes, the tight delivery delay requirements, and the frequent use of multicast in military applications. The issue is whether the network can support voice while simultaneously handling other required traffic loads. In the Land Warrior Program, the communications system is required to support three simultaneous voice conversations within a squad size unit. So one stressing test may be to look at three simultaneous multicast voice conferences within a ten man squad along with appropriate back ground traffic. Variations could include mobility in restricted environment (ie what happens if there are sudden changes in the network topology).

Another stressor is sheer volume of traffic. At what point does the network overload? What happens at that point? Does the network lock up? Does it lose critical/priority messages? Or does it gracefully degrade – first deferring or dropping lower priority messages, adjusting voice and video data rates, and slowing non critical things down a bit as they stack up in the buffer?

Below are listed candidates for inclusion in "Standard" Evaluations *for* Ad Hoc Mobile Networks:

1) Network Self Organization: Time required for a collection of wireless nodes to automatically organize itself into an ad hoc network capable of routing traffic from any user to any other user or combination of users.
2) Net Join: Time required for an individual node or group of nodes to attach to and become a part of an existing, functioning ad hoc network.
3) Network Self-Healing: Time required for a network to recognize the loss of one or more damaged or otherwise non functioning nodes and route around them.
4) Network Scalability: Network must be capable of Scaling to 10,000 nodes (for this we may be able to examine basic scalability mechanisms at bench, but would have to rely on simulation to actually exercise them.
5) Network support for real time services: Can network support simultaneous multicast voice while also supporting reasonable "background" traffic mix?
6) "Bandwidth on demand"? In additional to nominal background traffic levels associated with situation awareness, voice conversations and other routine services, can an individual node receive or transmit video when needed?
7) QOS routing: Given reasonable traffic mix and loading levels, can network still meet time delay bounds for priority messages and real time services? Can network send priority messages and support priority voice even when it is overloaded with routine traffic levels? Can network support full range of DII services?
8) Robustness/recovery: If network is severely overloaded, or multiple node failures cause network to segment, how long does it take for network to recover when the load is reduced and/or nodes again become functional?
9) Network density: How sensitive to the node density is the network performance? Can the network automatically adapt to work well across a wide range of densities and topologies?
10) Mobility: Can the network readily identify and adapt to changes in topology, particularly those that result from node mobility?

11) Network use of bandwidth: Does network make efficient use of bandwidth? What is the average throughput as a function of raw channel data rate? (This one could be really trick if you have a radio that automatically adapts data rates).
12) Network Security: (I do not know that there is a standard demo that can be run here, but feel that it is important enough that it should be listed. We might come up with several types of attacks like message repeat or flooding (from insider or compromised node) to see if network can continue operations or crashes. Also look at network recovery time.

Other issues for consideration:

- Node Power consumption: Does network have "hot spots that consume batteries, or does routing mechanism consder battery life remaining?
- Asymmetry: Can network function with a mix of mounted and dismounted radios that have different range capabilities and inherently require direct or asymmetric links?
- Can network function with radios that have adaptive link controls? Can it accommodate opportunistic routing?
- Can network support geographic routing?

For each of the Standard Evaluations that we decide upon, we need to develop a more precise definition, set up and measurements scheme. One short example follows:

Network Self Organization

Network self organization is the ability for a group of nodes to automatically "discover " one another, exchange essential routing information and be ready to support network data transfer. However, some networking protocols are "on demand" and are by definition ready immediately (although time to discover initial routes may be higher that time to subsequently route information).

A more meaningful metric may be the time required for a collection of wireless nodes to automatically organize itself into an ad hoc network (capable of routing traffic from any user to any other user or combination of users) and to route either 1) A SITREP from each node member to another designated member (as may be representative of a squad reporting in its location and status to squad leader following a parachute landing); 2) A mulitcast voice to all squad members (as may be the case of squad leader issuing a command or point man issuing a warning); or 3) a single message to another single address (as may be the case in a call fire or sensor to shooter transaction).

To determine time for each of the above three cases, the network topology must first be identified. Again, different topologies are possible, so it may be necessary to test more than one to examine the amount of variation. Six variations are identified:

1) Fully connected (any node can reach any other node in a single hop (ie dense network) – topology stationary
2) Strongly connected (no node is more than two hops away from any other node. All nodes have at least two neighbors. – topology stationary
3) Weakly connected some nodes have only a single neighbor and some nodes may be separated by up to five hops. – topology stationary
4) Start up while mobile with topology changes occuring within strongly connected topology, within weakly connected topology and while transitioning from strongly to weakly connected.

Specific topology laydowns should be agreed upon in advance for each of the above.

Similarly, test messages/packets should be developed in advance.

All networks should be evaluated against the same setups and traffic generation. Physical experiments should be compared with corresponding simulation vignettes. Hopefully results will be very similar. If not, we have a problem with model or test procedure that will need to be resolved. Comparison of test results with simulation results should aid in model validation.