Characterizing Mobile Ad Hoc Networks – The MANIAC Challenge Experiment

Vivek Srivastava
Virginia Tech
Arlington, Virginia
vivs@vt.edu

Amr B. Hilal
Virginia Tech
Blacksburg, Virginia
amr.hilal@vt.edu

Michael S. Thompson
Bucknell University
Lewisburg, Pennsylvania
michael.thompson@bucknell.edu

Jawwad N. Chattha
Virginia Tech
Arlington, Virginia
chattha@vt.edu

Allen B. MacKenzie
Virginia Tech
Blacksburg, Virginia
mackenab@vt.edu

Luiz A. DaSilva
Virginia Tech
Arlington, Virginia
ldasilva@vt.edu

ABSTRACT

This paper reports data collected during the first Mobile Ad-hoc Network Interoperability And Cooperation (MANIAC) Challenge, a multi-institution competition that allows us to study issues of interoperability and cooperation in mobile ad hoc networks (MANETs). We characterize network topology and routing. The former includes network connectivity and diameter, node degree distribution, clustering, and frequency of topology changes. The latter includes route length distribution, route asymmetry, frequency of route changes, and packet delivery ratio. Results show a high degree of topology and route changes, even when mobility is low, and a prevalence of asymmetric routes, both of which contradict assumptions commonly made in MANET simulation studies. Our data sets will be made publicly available for use by other researchers.

Categories and Subject Descriptors: C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design - *distributed networks, wireless communication, network topology*.

General Terms: Measurement, Performance, Experimentation

Keywords: Mobile ad hoc networks, cooperation strategies, interoperability, experimental research, network topology, routing

1. INTRODUCTION

Much of the research on mobile ad hoc networks (MANETs) has focused on simulation and testbed studies, while plans for actual deployment of large-scale MANETs remain limited primarily to military and single-vendor public safety deployments of mesh networks. There is uncertainty, in fact, as to whether a large-scale distributed ad hoc network created with hardware and software from many different vendors and controlled by many different administrative entities is even viable. Rather than trying to replicate this scenario in an in-house testbed, we sought to more closely mirror reality by organizing a competition in which we relinquished control of the network and welcomed participation from multiple academic institutions, each of which had the freedom to independently develop their own interoperability and cooperation strategies. Some of the data collected in this experiment, describing network interoperability, topology, and routing in the MANET, are presented in this paper. We hope the lessons learned will be useful in the evolution and, ultimately, deployment of mobile ad hoc networks.

The network characterization presented in this paper focuses on topology and routing. Topology characterization includes network connectivity and diameter, amount of clustering, node degree distribution, and frequency of topology changes. Our study of routing characteristics includes route length distribution, route asymmetry, frequency of route changes, and packet delivery ratio.

We believe this to be the first set of published data on a MANET in which nodes were free to modify their connectivity and routing behavior (unlike in a traditional testbed, where forwarding and routing are under the control of the testbed operator). Results show a high degree of topology and route changes, even when mobility is low, and a prevalence of asymmetric routes, both of which contradict assumptions commonly made in MANET simulation. All our data sets will be made publicly available for use by other researchers.

We start with a description of the experimental set-up in Section 2. Sections 3 and 4 present our results on network topology and routing, respectively. Section 5 summarizes other published experimental results on MANETs, and Section 6 discusses our findings and ongoing work.

2. THE MANIAC CHALLENGE: EXPERIMENTAL DESCRIPTION

All data reported in this paper were collected during the first Mobile Ad-hoc Network Interoperability And Cooperation (MANIAC) Challenge, held in conjunction with IEEE Globecom on November 25-26, 2007 (see Figure 1).

This NSF-funded project established a multi-institution competition in the area of mobile ad hoc networks. The MANIAC Challenge allows us to study issues of interoperability and cooperation in MANETs. In its first year, we focused on the tension between the desire of nodes to limit the number of packets they forward

WiNTECH '08, September 19, 2008, San Francisco, California, USA.

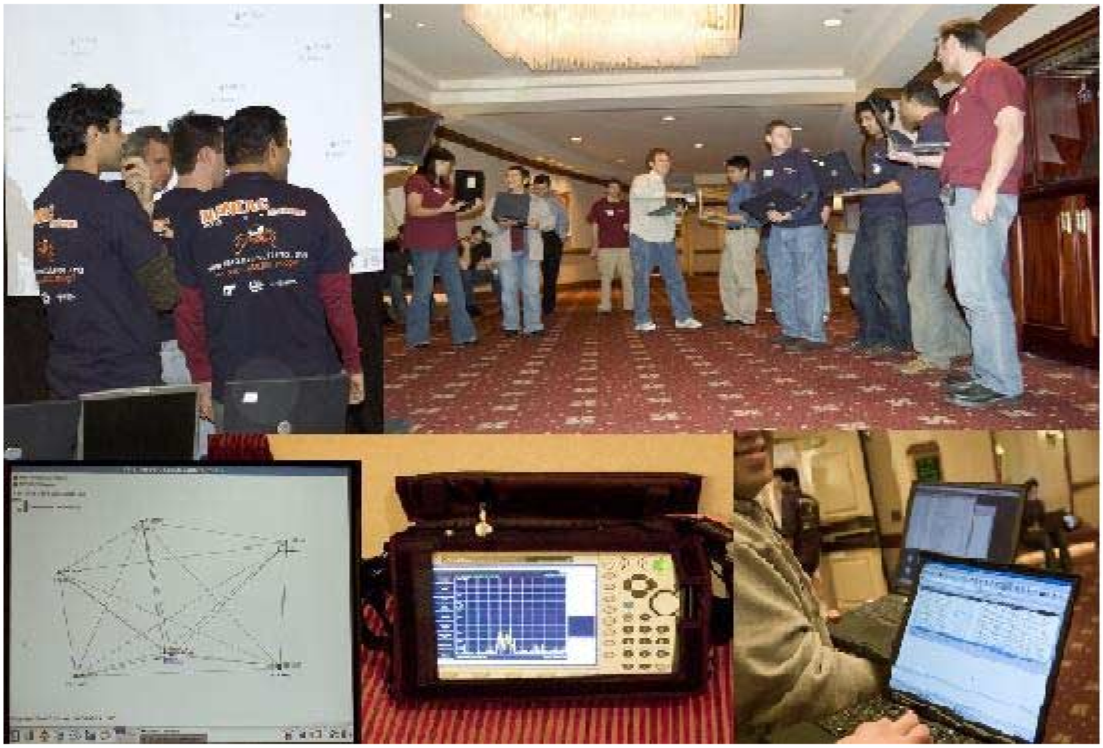

Figure 1 – Pictures from the MANIAC Challenge 2007, showing participating teams and organizers, measurements made with a spectrum analyzer, and one of the topologies captured by the network monitoring tool.

for others (in order to preserve battery life and competitive advantage) and the need for nodes in a MANET to cooperate in order to permit the delivery of packets along multi-hop routes.

The network consisted of 16 laptops equipped with IEEE 802.11b and 802.11g network interface cards (NICs), operating in ad hoc mode. Of these, the authors had direct control over four laptops, which were used to generate real-time and non-real-time UDP traffic to all other nodes in the network. The remaining nodes were operated by teams participating in the competition, with two nodes per team, which included academic institutions such as the University of North Carolina at Charlotte, George Washington University, the University of Puerto Rico at Mayagüez, Auburn University, Bucknell University, and the Technical University of Kosice, in Slovakia. Optimized Link State Routing (OLSR) was used as the routing protocol in the network. We adopted Naval Research Laboratory's (NRL) implementation of OLSR. We chose to run OLSR with default parameter values. For more details on its implementation, please refer to [1]. In addition, a detailed description of the rules of the MANIAC Challenge is available at [2].

We deployed two additional laptops to monitor network traffic and topology. These laptops ran the passive monitoring tool described in [3] and produced a GUI with a picture of the topology, as well as information regarding traffic received and forwarded by each node. A snapshot of the GUI is shown in the lower left-hand corner of Figure 1

All nodes in the network used a common Application Programming Interface (API) designed by us. The two main functions of the API were to facilitate dynamic changes in routing and forwarding decisions by participating teams and to collect traffic and routing data at each node.

The goal of the MANIAC API was to give teams the ability to drop, forward, or redirect traffic that was delivered to them to forward onward. This was accomplished with the help of the iptables and netfilter packages available on Linux. Using iptables, one of the Linux firewall packages, to-be-forwarded packets were rerouted into a user-space queue where a team's strategy analyzed each packet and decided whether to forward the packet in accordance with the routing table, drop the packet, or redirect the packet to a different next hop than specified in the routing table.

The API periodically (once per second) stored the routing table at each node into a log. It also logged the number of packets accepted, dropped, and forwarded by each node, the number of non-real-time packets destined to the node that were received, and the number of real-time packets destined to the node that were received within a playback deadline. The real-time traffic mimicked the operation of a stored media player application. After an initial buffering of 20 packets, the receiver expected packets with a playback deadline set according to the inter-departure time of 100 ms. A packet was considered on time if it arrived by the playback time and late if it did not. Packets that never arrived were considered lost, not late. We also used the Distributed Internet Traffic Generator (D-ITG), developed at Universita degli Studico Napoli Federico II, to generate UDP non-real-time packets every 100 ms.

Besides the data collected through the API, during the experiment we had additional nodes collecting Wireshark traces, Observer traces, and Kismet traces, as well as a spectrum analyzer measuring frequency utilization. Wireshark is a network analyzer available through a GNU General Public License. Observer is a software-based network analysis tool capable of collecting layer-2 frames to evaluate 802.11-based WLANs. Kismet is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system. The results presented in this paper originate primarily from data directly collected at network nodes through the API.

Winning teams were declared in two categories: performance and design. The performance winner was determined after an objective evaluation based on: (a) collecting statistics on the traffic flows received, and (b) measuring a proxy for energy consumed by each team in forwarding packets. Packets in each traffic flow were marked as destined to one of the teams in the competition. A team received ten (10) points for each non-real-time packet belonging to one of their flows to reach its intended destination, and ten (10) points for each real-time packet belonging to one of their flows to reach its intended destination by scheduled playback time. A team was deducted one (1) point for each data packet it forwarded, excluding control traffic. The point scheme was arbitrarily selected, with the intent of rewarding a team generously on receipt of its own data while penalizing it slightly for spending energy in forwarding packets for others. The design winner was selected through a qualitative assessment of strategies by the organizers, who observed the competition and attended presentations from participating teams describing their strategies.

Three independent runs of the competition were conducted, each lasting about 20 minutes. To obtain a picture of the network at each time instant, we used the routing log files collected during the competition to generate a topology file for each run. The topology files describe the network at every time instant by listing the path between each pair of nodes. A path from node *x* to node *y* is specified in terms of the node ID of the next hop, and the number of hops to the destination. It is our intention to provide these topology files for public use.

3. NETWORK TOPOLOGY CHARACTERIZATION

The first set of results we present addresses the connectivity properties of a multi-hop ad hoc network of 16 nodes and the stability of routes in this network. These topology results are derived from logs of the routing tables at each node, and are unaffected by cooperation strategies adopted by participating teams (teams had the option of over-riding forwarding decisions but did not alter the routing tables themselves).

3.1 Reachability

Reachability is the ability of a node to reach any other node in the network. One graph-theoretic metric that illustrates reachability is the size of the largest connected component in the network (i.e., the largest connected sub-graph). Figure 2 plots the duration of the experiment run time for which a given largest connected component was observed.

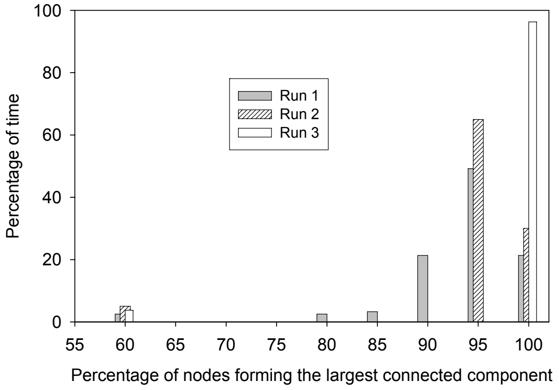

Figure 2. Size of the largest connected component of the topology graph.

The network exhibited a high degree of connectivity, as illustrated in Figure 2. For all three runs, the largest connected component comprised at least 90% of the nodes for at least 95% of the duration of the experiment.

3.2 Clustering and Network Diameter

We next consider the average hop count and the average node clustering coefficient for the network. The clustering coefficient, as defined in [4], represents the degree with which neighbors of a node are connected to one another. Formally, if any node, *k*, has *n* neighbors then the maximum number of edges among those *n* nodes is $n(n-1)/2.$ The clustering coefficient is the fraction of the possible number of edges that actually exist. If there are *l* such actual edges, the clustering coefficient for node *k* is expressed as $C_k = \frac{l}{n(n-1)/2}$. A clustering coefficient near 1 indicates that the node has a densely connected neighborhood.

Table 1 shows the average clustering coefficient, averaged across all nodes and all time instants, for each run of the competition. We also tabulate the average hop count (the average number of hops from each given node to each other node in the network) and notice that the network exhibited a high degree of clustering, with short path lengths.

A random network is a graph-theoretic model that can be thought of as starting with a ring lattice with *n* vertices and *k* edges per vertex and rewiring each edge at random with probability p (p → 1). For random graphs, the clustering coefficient is given by k/n, where *k* is the average node degree for a network of size *n* [4]. For our network comprising of 16 nodes with an average node degree of 7, the clustering coefficient for the equivalent random graph would equal 0.4375. The degree of clustering exhibited by our network was higher than would be expected in a random graph of similar size and node degree.

One of the reasons for such behavior could be the fact that source nodes were placed far apart from each other and teams chose to coalesce together in the center in a way that allowed them to access each of these sources simultaneously through a few hops.

Table 1. Average hop count and clustering coefficient for the network for each run.

Run	1	2	3
Average clustering coefficient	0.569	0.664	0.696
Average hop count	1.207	1.262	1.391

This is also reflected in the distribution of the network diameter as a percentage of time, shown in Figure 3. The maximum hop count was 6, with the network diameter equal to 3 for a majority of the time.

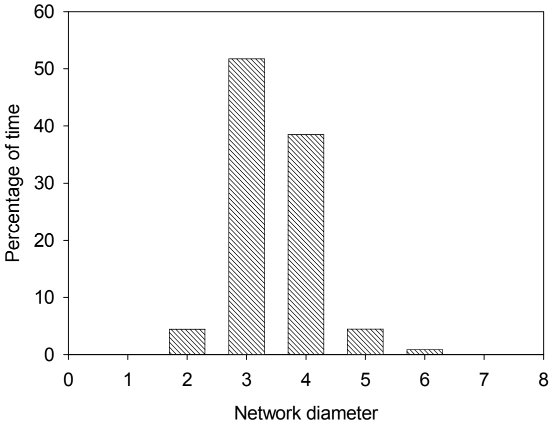

Figure 3. Histogram of network diameter.

3.3 Node Degree Distribution

The distribution of the node degree is shown in Figure 4, with a mean of 7. This means that each node had, on an average, approximately about half of the network as its direct neighbors.

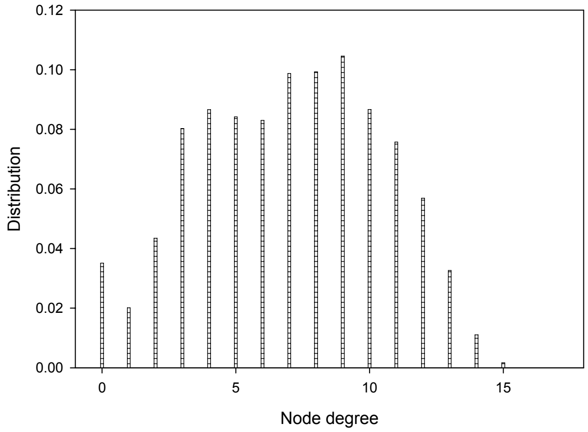

Figure 4. Node degree distribution

3.4 Model of Topology Changes

We also compared our experimental data to a possible model of link connectivity in a wireless ad hoc network. A model of link status (a link is characterized by being up or down) should strive to achieve simplicity and a good fit to experimental results. Modeling wireless links as a two-state Markov chain as shown in Figure 5 can provide a great level of simplicity, yet needs verification. Such a model would imply that the duration of link status (up or down) should conform to a geometric distribution.

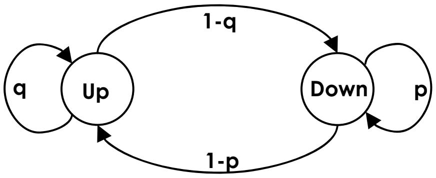

Figure 5. Two-state Markov chain model of link availability.

To test the conformance of the observed wireless link status to a geometric distribution, we considered only links that exhibited change in status more than 20 times during each run. We then applied the chi-square goodness-of-fit test to the data set obtained from each run, and generated histograms, shown in Figures 6 and 7, to visually verify the test result. The hypothesis of a geometric distribution was not confirmed. Data generated during the test and also the histograms show that the first few bins (one or two bins) are the main reason for rejecting the geometric distribution hypothesis. Other bins were close to the expected bin sizes according to the geometric distribution. Based on these observations, we conclude that a two-state Markov chain provides a reasonable, though imperfect, model for wireless link status in an ad hoc network.

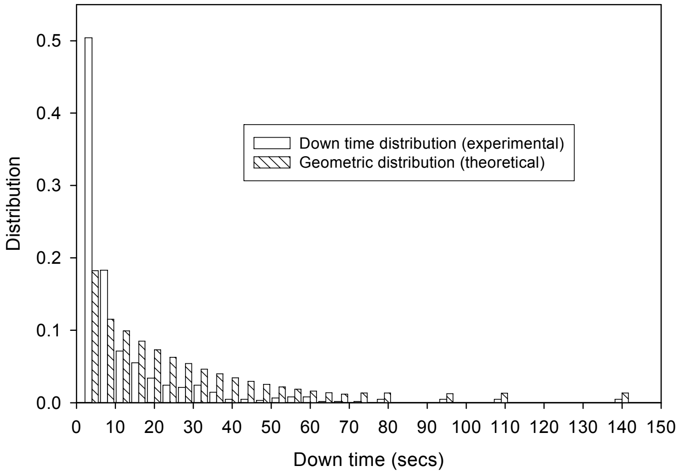

Figure 6. Histogram of link down time (for run 3 of the experiment) compared to the geometric distribution. The other two runs showed a similar trend.

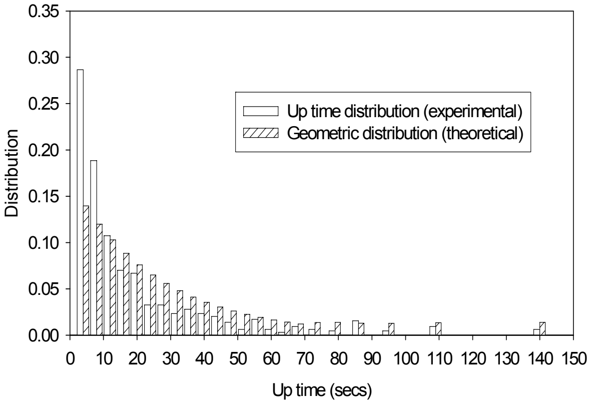

Figure 7. Histogram of link up time (for run 3 of the experiment) compared to the geometric distribution. The other two runs showed a similar trend.

We speculate that the two-state Markovian model provides a considerably better model for link state than a model generated by a conventional simulation mobility model, such as random waypoint. The key problem with mobility-based link state models is that they assume that links only go up and down due to node mobility. Our data clearly demonstrate that link state changes much more often than would be predicted by node mobility alone.

4. ROUTE CHARACTERIZATION

In this section, we characterize route length and discuss the prevalence of asymmetric routes.

4.1 Route Length Distribution and Route Symmetry

The mobile ad-hoc environment often causes routes to be asymmetric. Motivated by that, we studied route symmetry, with results illustrated in Figure 8. Routes were investigated up to 7 hops in length. A route from *s* to *d* is said to be symmetric if the route from *d* to *s* traverses the same nodes, but in the opposite order. For example, if the route from a to c is *node_a* to *node_b* to *node_c* and the route from c to a is *node_c* to *node_b* to *node_a*, then we would say that the route from a to c is symmetric (likewise, the route from c to a would also be symmetric). Figure 8 shows that, on the average, nearly 60% of the routes were symmetric. High percentages of asymmetric routes suggest large and fast fluctuations in the routes themselves.

We further investigated how many *x*-hop routes contributed in the total number of symmetric routes. Table 2 shows a breakdown of link characteristics by path length and symmetry.

The first row for each run is the percentage of the total paths of the given length that are symmetric (the remaining percentage for each is asymmetric). The second row for each run shows the distribution of path lengths for all paths. Due to the close physical location of nodes in the network imposed by the size and shape of the venue, it was reasonable to expect that 1-hop links should be the dominant type of links in the network, and these have a high likelihood of being symmetric. We can see a fast degradation in the number of symmetric routes longer than 1-hop, such that we hardly find a symmetric route that is more than 2 hops long. This observation indicates that the common assumption of route symmetry in simulating ad-hoc networks does not hold in practice.

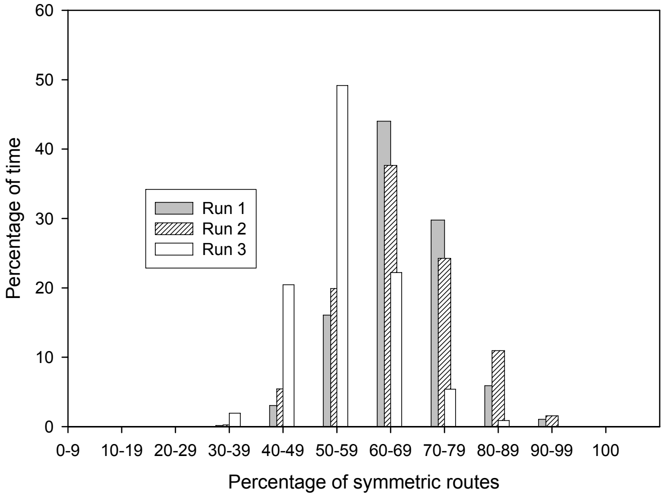

Figure 8. Percentage of symmetric routes.

Table 2. Route length distribution and percentage of symmetric routes

		1-hop	2-hop	3-hop	4-hop	> 4-hop	No route
Run1	Symmetric	92.9%	24.2%	4.2%	0%	0%	65%
	Total	47.4%	27.7%	5%	0.7%	0.1%	19.2%
Run2	Symmetric	88.3%	45.9%	4.5%	0%	0%	41.2%
	Total	47.7%	33.1%	3.7%	0.3%	0%	15.2%
Run3	Symmetric	85.2%	39.5%	10.4%	1%	0%	11%
	Total	44.3%	34.6%	7.7%	0.6%	0%	12.7%

4.2 Route Stability

Inspired by the results obtained from the route symmetry study discussed above, we were interested in finding the reasons for such a high percentage of asymmetric routes. We speculated that asymmetric routes were caused by non-convergence of the routing algorithm due to frequent changes in the topology. In this context, we studied the correlation between topology changes and route changes during the network lifetime as illustrated in Figure 9. The figure presents a scatter plot of the proportion of routes in the network that change versus the proportion of links in the network that change for each time instant. A topology change is defined as the establishment of a new direct link or the teardown of an existing link between two nodes at time t, while a route change is defined as a change in the route between two nodes (detected by a change in gateway or number of hops to the destination).

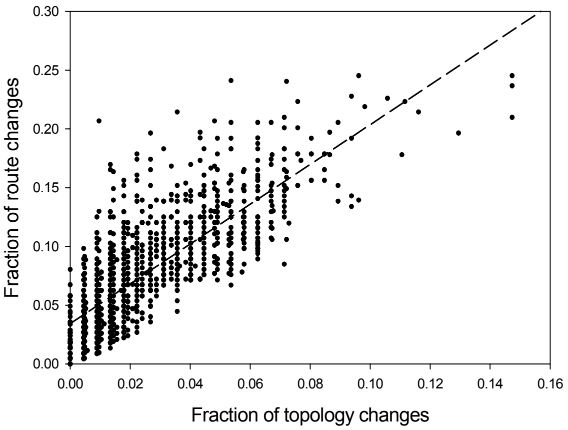

Figure 9. Proportion of route changes versus proportion of topology changes.

We used linear regression to test the relationship between route changes and topology changes, and the fitting line shows an apparent correlation. The regression test was applied to the three runs, with similar results. Link instability can cause the network to have unstable routes and hence an abundance of asymmetric routes may appear.

4.3 Packet delivery ratio

Table 3 indicates the average packet delivery ratio for real- and non-real-time traffic during the three runs. We also indicate in the table the percentage of real-time packets that were delivered within their playback time. The two major reasons for low delivery ratio were the frequent connectivity changes and the packet forwarding strategies employed by each team. As the strategies applied remained essentially unchanged for the three runs, it is likely that the increase in the average packet delivery ratio across the three runs was due to improved connectivity, as indicated by Figure 2.

Table 3. Percentage of real- and non-real time traffic delivered to its destination.

Traffic	Run1	Run2	Run3	Overall
Non-real time	19.45 %	27.91 %	34.20 %	27.18 %
Real-time	22.83 %	23.30 %	33.72 %	26.61 %
Real-time within deadline	21.84 %	22.96%	32.35%	25.72%

5. RELATED WORK

There are a limited number of studies evaluating MANET performance and network characteristics. A major factor in this is the logistical difficulty of working with large MANETs. To create multiple hops, enough space must be available for multiple nodes to lose contact with a subset of the network while maintaining contact with some other portion of the network. Additionally, each node requires an operator to run the software and provide mobility. So, when testing 20 and 30 node networks, 20 and 30 people must be present and cooperate in the execution of the experiment. In the remainder of this section, we will compare our work with other experimental MANET work.

A thorough exploration of experimental work with MANETs is provided in [5]. The authors provide a comprehensive review of experimental MANETs in Section VIB. In addition to reviewing existing efforts, a detailed summary of generalized observations resulting from past experimental research efforts is presented. A few of these, specifically points 1, 5, 10 and 11 were also observed and agreed upon by us. Due to space constraints, the reader is encouraged to consult the paper directly. The remainder of this section covers work not included in [5].

The authors of [6] conducted an experimental MANET study within the context of military communication. This study used 18 heterogeneous nodes to collect performance metrics for the Optimized Link State Routing (OLSR) protocol. Nodes were placed throughout a building and outside the building, emulating an urban or indoor combat scenario. This study investigates the performance of TCP alone and the combination of both TCP and UDP. The metric of interest is throughput of all protocols.

Continuing down in size, researchers from the University of British Columbia and Samsung Electronics created a 10-node MANET for the purpose of comparing the AODV and SAODV protocols [7]. While the purpose of this study was not strictly to collect experimental results, it does present performance data for a MANET test scenario. Metrics of interest for this work were UDP packet delivery, TCP throughput, and overhead.

The final work we reference is from the IIT Institute [8]. This work compares AODV and OLSR in the setting of an 8-node MANET where the network diameter ranges from 2 to 4 hops. This work presents the overhead and delay of the two routing protocols. The experiments in this work are based on two different network topologies; one is a partially connected group of 8 nodes while the other is a “string” topology of 4 nodes. This study uses the ping utility to generate traffic and test for connectivity.

The main conclusion that can be drawn from these works is that performance results are dependent on the scenario of the experiment and since MANETs are versatile these scenarios differ greatly. The results obtained by these works have little application to other scenarios because the underlying network characteristics are too different.

Additionally, we found, that little work has been done to characterize or group MANET usage scenarios. One goal of the MANIAC project is to analyze the underlying network behavior and present results that give insight into what is going on at the routing and topology levels when nodes have the freedom to make their own forwarding and routing decisions. This freedom adds an additional dimension of variability to an already dynamic platform. Additionally, this freedom invalidates certain assumptions about cooperation in MANETs and creates a feasible area of investigation. We feel this is feasible because cooperation directly affects a node's lifetime and performance by consuming resources. If desired, it would be good to be able to turn off or reduce cooperation to save resources.

6. CONCLUSIONS

This paper presents data describing network topology and performance collected from a heterogeneous ad hoc network created during the MANIAC Challenge, an inter-university competition. Our topology results, including measures of reachability, clustering, node degree, and network diameter measures, demonstrate that our observed network was highly connected and clustered, with a relatively low diameter. Given these facts, which suggest a relatively benign operating environment, it is somewhat surprising that our measures of route stability and symmetry demonstrate that the operational network experiences an extraordinary amount of "churn." Routes, especially those longer than one hop, are highly asymmetric and change rapidly. These observations support the conclusion that routing proactively in a real ad hoc network is extremely difficult. This dynamicism casts serious doubts on ad hoc networking work that builds on simulation models in which links are made and broken in a more controlled, systematic environment. The frantic pace of topology changes in our network suggests that the vast majority of topology changes were caused by factors other than node mobility, which contradicts the assumptions of many simulation models.

Despite the high connectivity, our results also demonstrate extremely poor network performance, with just over one quarter of data packets successfully delivered to their destinations. While part of this poor performance may reflect the fact that teams were incentivized to behave selfishly in the competition environment, we note that this selfishness seems unlikely to completely explain the poor performance as more than 40% of the routes in the network were single-hop routes, on which no packet forwarding was required. This abysmal performance may highlight the insufficiency of the IEEE 802.11 protocol family as a foundation for ad hoc networking research, and the lack of a readily available alternative suggests other difficulties in creating real-world ad hoc networks.

We are currently working to deepen our understanding of the results of the 2007 MANIAC Challenge through more detailed analytical techniques and to package and disseminate the raw data that we collected so that other researchers may examine it as well. At the same time, we are preparing for a second round of competition at the 2009 MANIAC Challenge; interested researchers are invited to visit the MANIAC Challenge website at www.maniacchallenge.org for more information.

7. ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under Grant No. NSF-0519825.

We gratefully acknowledge the contributions of Dr. Kerry Wood, Dr. George Hadjichristofi, Dr. Mohamed Tamer Refaei, and Mr. Hanif Kazemi to software development and testing for the MANIAC Challenge. We are also indebted to all the teams of students and faculty who participated in this experiment.

8. REFERENCES

[1] J. Macker and R. Lee, "http://cs.itd.nrl.navy.mil/work/olsr/," August 2007.

[2] L. A. DaSilva and A. B. MacKenzie, "www.maniacchallenge.org," August 2006.

[3] H. Kazemi, *et al.*, "MMAN – A Monitor for Mobile Ad Hoc Networks: Design, Implementation and Experimental Evaluation," *The Third ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH 2008)*, September 2008.

[4] D. H. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature,* vol. 393, pp. 440-442, June 1998.

[5] W. Kiess and M. Mauve, "A survey on real-world implementations of mobile ad-hoc networks," *Ad Hoc Networks,* vol. 5, pp. 324-339, April 2007.

[6] T. Plesse*, et al.*, "OLSR Performance Measurement in a Military Mobile Ad-hoc Network," *Ad Hoc Networks,* vol. 3, pp. 575-588, September 2005.

[7] Y. Lin*, et al.*, "Experimental comparisons between SAODV and AODV routing protocols," *1st ACM workshop on Wireless Multimedia Networking and Performance Modeling* Ocotber 2005, pp. 113-122.

[8] E. Borgia, "Experimental evaluation of ad hoc routing protocols," *3rd IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom '05)*, March 2005, pp. 232-236.