The MANIAC Challenge: Exploring MANETs Through Competition

Michael S. Thompson, Amr E. Hilal, Abdallah S. Abdallah, Luiz A. Dasilva, Allen B. Mackenzie

The MANIAC Challenge: Exploring MANETs Through Competition

Michael S. Thompson[1], Amr E. Hilal[2], Abdallah S. Abdallah[2], Luiz A. DaSilva[2], Allen B. MacKenzie[2]
[1]Bucknell University, Lewisburg, PA, USA
[2]Virginia Tech, Blacksburg, VA, USA
michael.thompson@bucknell.edu, (ahilal, yarab, ldasilva, mackenab)@vt.edu

Abstract— **In this paper we discuss the MANIAC Challenge, a cooperative and competitive approach to MANET networking research. Our goal was to create an opportunity for researchers to come together and compete in a MANET-based competition where points were awarded for received traffic and deducted for use of node resources, including packet forwarding. Using software we created, each team built a participation strategy that allowed them to decide how much they would participate in forwarding traffic for other nodes. This exercise turned out to be a resounding success and a wealth of data was gathered about traffic patterns, network behavior, node behavior, and the impact of node participation strategies on the MANET. The major observations of this work are that location and hardware can affect node performance, node participation can affect the larger network in some circumstances, and node mobility patterns can vary based on the goal of the node.**

I. Introduction and Motivation

Mobile ad hoc networks (MANETs) have been a popular research topic for many years. Yet much of the research on 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 applications. 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. The emergence of software-defined radios and, eventually, cognitive radios, may bring efficiencies in the use of spectrum and ultimately yield greater throughput, but the use of such radios in an ad hoc environment also opens new question: How can inter-operability and cooperation among nodes in the network be assured?

Questions linger about how well MANETs will work in the wild, i.e., outside tightly controlled lab environments or military deployments. Are simulation results reported in the literature too optimistic about performance that can be achieved in these networks? Is it feasible to transport real-time traffic, with even modest quality of service (QoS) guarantees, in an ad hoc environment? What are the incentives for a node to perform services (such as routing) for others? We developed and organized the Mobile Ad hoc Networking Interoperability and Cooperation (MANIAC) Challenge, a competition where nodes are programmed and operated by competing teams to form a MANET and carry real- and non-real-time traffic, to address some of these questions.

The impact of node cooperation on the performance of mobile ad hoc networks has been widely discussed and simulated; see for instance published work on resource sharing and reputation schemes [1]–[9], as well as related work on cooperation in peer-to-peer networks [10], [11]. However, the opportunity to observe an uncoordinated ad hoc network (one in which individual decisions are not pre-programmed by some central entity) is rare. The MANIAC Challenge allowed us such an opportunity.

II. The Competition

The MANIAC Challenge is a competition that provides a unique opportunity to study spontaneously-deployed, uncontrolled MANETs, where users make their own decisions regarding tradeoffs between self-interest and common network goals. We view the competition as an educational tool, to encourage students to become engaged in hands-on research in wireless networking, as well as a research experiment, giving us a window into the likely behavior of a MANET of self-interested users whose dynamics we, as researchers, cannot directly control.

During each competition, teams from all over the world came together to form one large MANET. Each team operated two laptops with IEEE 802.11b/g capabilities and was responsible for positioning and moving their own nodes. As the organizers, we operated a set of source nodes, from which we generated multiple real-time and non-real-time data streams to be delivered to each participating node over this MANET. Each team's objective was to ensure the delivery of data streams destined to them while consuming as little energy as possible in forwarding packets for other nodes.

During the competition, our set of source nodes were arranged such that no single team was capable of receiving all data streams without collaboration from nodes from other teams. During the course of the competition itself, the source/destination pairs for streams associated with each team rotated, to "average out" effects unrelated to the teams' strategies (e.g., interference, mobility, presence of physical obstacles) on the delivery of data streams to each team.

Winning teams were declared in two categories: performance and design. The performance winner was determined after an objective evaluation of the performance of the teams during the competition. The objective evaluation was based on: (a) measurements on the traffic flows received, and (b)

measurement of a proxy for energy consumed by each team in forwarding packets. A team was awarded ten (10) points for each received non-real-time packet that belonged to one of their flows (i.e., flows with one of the team's laptops as their intended destination), and ten (10) points for each real-time packet belonging to one of their flows received by a specified deadline. A team lost one (1) point for each packet it forwarded, excluding control traffic. 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. From our point of view, who won the competition is less important than what we were able to learn from the network that emerged during the competition, and hence the latter is the focus of this paper.

The first MANIAC Challenge (denoted MANIAC07) was held in November 2007, in conjunction with IEEE Globecom, and the second (denoted MANIAC09) was held in March 2009, in conjunction with IEEE PerCom. Participants represented academic institutions in Europe, the U.S., and Africa; while most teams comprised graduate students, both competitions counted with at least one all-undergraduate team.

A. Implementation: the MANIAC API

Since little of the functionality needed for the competition is normally available to userspace applications, we created a software library, the MANIAC API, that offered the following functionality.

1) Allow users to view packets passing through the networking stack.
2) Allow users to drop, forward, or redirect packets as they passed through the network stack:
   a) Forwarded packets were forwarded using the next hop specified in the routing table; and
   b) Redirected packets were forwarded to a user-specified next hop and ignored the routing table.
3) (MANIAC09 only) Allow the users to sniff packets on the network to passively observe neighboring nodes.
4) Log the packets entering and leaving the API.
5) Log the participant actions (drop, forward, redirect).

The MANIAC API was built for and runs on Linux distributions that include the 2.4 or 2.6 kernel. It relies heavily on the Netfilter library (iptables) [12]. Specifically, it uses the libnfnetlink and libnetfilter_queue libraries. The MANIAC API uses the netfilterqueue to remove packets from the networking stack as they pass through the netfilter subsystem. This functionality was included in MANIAC07 and MANIAC09.

The MANIAC API consisted of one packet queue for MANIAC07 and two packet queues for MANIAC09. Both competitions included a packet queue that removed packets from the kernel networking stack, allowed the participants to examine the packet, and carried out the desired action on the packet (drop, forward, or redirect). The additional queue, added for MANIAC09, contained "sniffed" packets and allowed participants to examine the traffic that was being transmitted by neighboring nodes.

B. Network Traffic

Source nodes operated by us transmitted two types of traffic across the network, real-time and non-real-time. In MANIAC07 the real-time traffic was generated by a real-time media-streaming application and the non-real-time traffic was created by a custom-built traffic generator. Each real-time traffic stream was about 4MB long and each non-real-time traffic stream was about 500KB long.

In MANIAC09 both the real-time and non-real-time traffic streams were generated by our custom-built traffic generator. Both streams were approximately 500KB long and lasted 30 seconds.

We chose to create our own traffic generator because we could not find an open source traffic generator that created real-time traffic and that logged late packets, in addition to dropped packets. [1]

C. Venue Floorplan

Figure 1 shows the floorplan of the Galveston Island Convention Center at the San Luis Resort in Galveston, Texas, the location of MANIAC09. For scaling purposes, the combined Exhibit Hall area is approximately 43,000 sq. ft. Additionally, there is another level above this level that included an open area above the right-most "pre-function" area. The source nodes were placed so that they were as far away from each other as possible, but their exact locations varied slightly during the tests. We adjusted the source node locations during and in between the tests so that each source node could communicate with as few other source nodes as possible. Some of source nodes moved to the upper and lower levels of the building, as well.

The participants and source nodes were allowed to move anywhere in the "pre-function" areas, the "pre-function" area on the second level, and down the hall between the meeting rooms (on the right-hand side). Gray areas were not open to the participants or the source nodes. The competition began with both the participants and the sources nodes in the top right meeting room marked as room 8 in 1. The network was established in this area. Once all of the nodes were connected and ready, the 20-minute timer was started and everyone dispersed. The source nodes moved to their locations and typically stayed there until the end of the competition.

D. Participants and Strategies

In the literature, schemes to stimulate cooperation and mitigate the effect of selfish behavior between nodes in MANETs can be classified into two main classes [8]: virtual currency systems and reputation systems. In virtual currency systems a node receives a virtual payment for serving the network and it uses this virtual currency to pay for neighboring services. Examples of virtual currency systems include Nuglets [2] and Sprite [14]. In reputation systems, a node collects information about other nodes in the network and uses this information to

[1] Please contact the authors if you are interested in this software, as it is open source and publicly available.

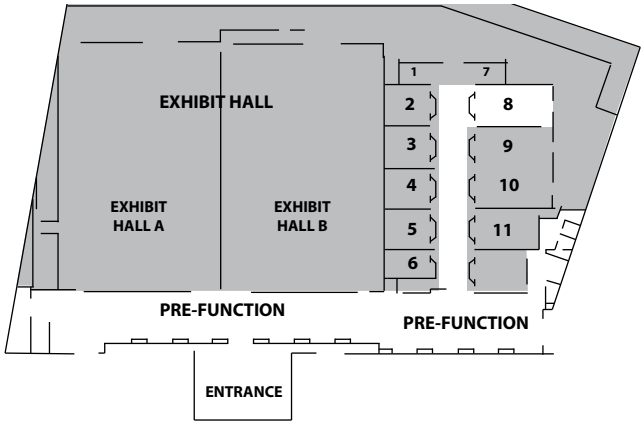

Fig. 1. Galveston Island Convention Center Floorplan [13]

assign a reputation indicator for these nodes. A node's view of another node's reputation determines how the first node will interact with the second. CONFIDANT [15] and CORE [7] are examples of reputation systems.

We saw several different ideas of cooperative strategies in MANIAC. The majority of these strategies fall in the class of reputation systems. Teams that employed a reputation scheme used the capabilities of our API to monitor their neighbors and collect information about their cooperative behavior. Then, using different techniques, every team used this information to decide how to interact with neighboring nodes. At the same time, teams tried to come up with packet forwarding strategies that balanced cooperation and selfishness to maximize points. A subset of the strategy approaches from participating teams is described below.

- In 2007, a team from Auburn University proposed a strategy that assumed that the probability of a packet successfully reaching its destination was lower when it had to traverse more hops. So, they decided to drop packets destined to nearby nodes (one or two hops away) and stop these neighbors from gaining points, while they forwarded packets destined to farther nodes because it was not worth harming their reputation by dropping a packet that has a high probability of being dropped later by other nodes.
- The same year, a team from the University of North Carolina Charlotte created a similar, yet less aggressive strategy, where they dealt with packets destined to farther nodes in a slightly different way. A packet was dropped if it was destined to the team's direct neighbor. However, if the packet was destined to a farther destination, they redirect it to the neighbor who received less traffic in the past. They defined traffic of a neighbor as the number of packets forwarded to that neighbor via the current node. Then, they dropped the packet with a probability, p. This probability was adaptively proportional to the ratio of the packets that the team's node forwarded to that neighbor to the total number of packets the team's node forwarded to all of its neighbors.
- In MANIAC09, a team from the Free University of Berlin, Germany, proposed a strategy called "Friendly Clustering" [16]. In this strategy, nodes were categorized into cooperative and non-cooperative sets based on their observed behavior. Nodes maintained their own routing table that was built based on their analysis of the OLSR Hello messages. The routing table stored all neighbors and their respective neighbors. The team used this table to forward packets over different routes than those determined by OLSR. Also, the team members periodically exchanged routing tables and cooperation scores for the other nodes in the network.
- A team from the University of Napoli Federico II, Italy, created a diversity paradigm where each player in the team adopted a different strategy. The first player, called "the free rider," implemented an always-drop strategy. The other player, called "the turncoat," forwarded according to a simple tit-for-tat with forgiveness strategy. The rationale behind this strategy was to enable the free rider to benefit from the teams that do not adopt retaliation-based strategies, while the turncoat established a positive rapport with teams with retaliation-based strategies.
- A team from the Arab Academy for Science and Technology, Egypt, created a strategy called "The Mongoose" [17]. In this strategy, the decision of whether to forward or drop a packet destined to some destination was based on the observed behavior of that destination. However, a node gave an advantage to nodes that were cooperative regardless of their behavior towards other nodes. The strategy calculated and kept three metrics that were used in the forwarding decision process; Anger Level, Randomness Probability, and Reputation Caring Probability. The Anger Level measured how much a node could be angry with others. This was measured for every pair of nodes by calculating the percentage of packets node A forwarded to B with respect to the total number of packets node A was supposed to forward to B. The Randomness Probability was the probability that a node was randomly controlling its traffic paying no attention to another node's reputation. The Reputation Caring Probability was the probability that a node cared about its reputation and punished selfishly behaving nodes. These metrics were used in a polynomial formula optimized for different types of strategies.
- A different approach adopted by some teams in the MANIAC competition relied on restricting the broadcast of the routing protocol control packets. By doing this, a team could include or exclude itself from the routing table of other nodes. The team from the Technical University of Kosice, Slovak Republic, adopted this approach in MANIAC07 and returned with a more advanced version in MANIAC09. Their strategy relied on providing forwarding service for nodes that could only connect to the rest of the nodes through them. The team hid from the rest of the nodes in the network. They from other nodes by capturing, modifying, and resending the

OLSR Hello messages to a set of preselected nodes. Only these nodes could directly send to this team. Similarly, a node continuously checked the status of nodes it already provided service to and if it detected that a node had another way to connect to the network, the team would begin hiding from it.

E. Winning Teams

As we pointed out before, the lessons we learned from this competition are more important than having winners, however, it was important to provide incentives for the teams to participate in the competition. In fact, we consider all of the participating teams, including us, winners because we all acquired a wonderful experience in understanding the potential dynamics of a real MANET. In MANIAC07, the team from the Department of Computer Science at the University of North Carolina at Charlotte won the performance award, while the team from the Department of Computers and Informatics at the Technical University of Kosice won the design award. In MANIAC09, the team from Freie Universitat Berlin in Germany won the performance award, while the team from University of Napoli Federico II in Italy won the design award. For more information and pictures of the competition, please see the competition website at www.maniacchallenge.org.

III. Results

The results in this section concentrate on network connectedness and how traffic flowed within the network. Unless otherwise noted, the data in this section is from MANIAC09. The tables included in this section include percentages and actual numbers for logged packets and dropped packets. The logged packet data shows the number of packets that passed through individual nodes, indicating which nodes were in the middle of the network versus those at the periphery. The dropped packet data shows the end result of the participants' strategy. However, to observe a node's behavior, traffic must have been forwarded to the node of interest, meaning that nodes that did not receive much traffic may have had little information from which to develop a strategy.

Each data point is an average of the values from the three competition runs during the MANIAC09 competition. Cells with a number indicate that packets were seen for the address combination even if that cell contains a zero (0). Cells without a number indicate that no traffic with that address combination passed through the logging node's API. This applies to all tables in this section. The row and column labels are a shortened version of the respective node's address. The mapping of node numbers to teams is shown in Table I. Due to problems with participant solutions, some nodes did not log data. These nodes are included for completeness.

Due to limited space, identical columns were combined in some tables. These are noted as such with a column heading that indicates a range. For example, a column header of "51-54" means that columns 51, 52, 53, and 54 are identical and share the data shown in that column.

	Test 1	Test 2	Test 3	Average
MANIAC 07	7.844	7.912	8.352	8.038
MANIAC 09	10.265	8.897	8.044	9.059

TABLE II
Node Degree

Finally, the term "logged" is used throughout this section to refer to an instance when a packet was processed by a node's MANIAC API. A "logging node" is the node that processed a given packet and created a log entry for that packet. The API recorded information about each packet and the action requested by the participant's strategy. This information was used to create all of the tables in this section.

A. Node Degree

Node degree is a common metric for describing a wireless network topology. Node degree is the number of neighboring nodes that a node is connected to; in the case of wireless communications a connection is defined as the ability to communicate bi-directionally. Table II shows the average node degree for MANIAC07 and MANIAC09. These values were calculated by taking the total number of one-hop routes for an instant in time and dividing this number by the number of nodes in the network. The number of nodes in the network varied by the competition and test, between 8 and 15 nodes with an average of approximately 13 nodes for both competitions. Table II shows that the nodes in both competitions were well connected and most nodes could communicate directly with each other.

B. Traffic Flow

This section discusses how the traffic flowed through the network, by relying on the number of packets that were logged by each API instance. This data is organized into two tables, one that groups the packets by the destination address and another that groups the packets by the address of the previous hop.

1) By Destination: Table III shows the number of packets that each node logged, grouped by the destination address of the packet being logged. This information indicates the data flows that occurred in the network as packets flowed to specific hosts. In short, it shows which nodes were in the path of the flow to a given destination host. Non-zero values in a specific row indicate that the corresponding node was a part of the path traveled by a flow. The more non-zero values that a node has, the more integral that node was in moving traffic on the network. Similarly, larger cell values indicate more involvement over time in forwarding or receiving packets to a particular node. More values with larger numbers indicates that a node was a central point in the network for a long period of time. For example, nodes 59 and 62 have a large number of non-zero row values indicating that they were highly involved in forwarding traffic. Conversely, nodes with fewer non-zero

University Name	Strategy Name	Node Numbers
University of Cyprus	FiftySixKei	50, 51
Arab Academy for Science and Technology	Mongoose [17]	52, 53
Free Univeristy of Berlin	Friendly Clustering [16]	54, 55
University of Naples Federico II	Diversity Adaptive Routing	56, 57
University of North Carolina at Charlotte		58, 59
University of Kosice, and Charles University in Prague	Live and Let Live 2009	60, 61
Virginia Tech		62, 63
University of Detroit Mercy	Multi Behavior	64, 65

TABLE I
LIST OF TEAMS PARTICIPATED IN MANIAC 2009 AND THEIR CORRESPONDING NODE NUMBERS

values were less involved in the network and can be considered periphery nodes.

After reviewing this data, we have the following conclusions.

- Most nodes were involved in a small number of flows, specifically 3 or fewer. Additionally, there was little spreading of traffic across the network, as only a few nodes saw traffic from their neighbors.
- As noted, most nodes did not see a majority of the traffic for other nodes. In terms of behavior and node strategy, little information about the behavior of a neighbor makes it difficult to create an appropriate strategy of how to deal with that neighbor. The converse effect could be seen, that a few nodes had a lot of historical knowledge about a small number of nodes in the network, allowing for knowledgable strategy creation.

2) By Previous Hop: Table IV shows the number of packets that were logged by each node, grouped by the packet's previous hop. This information indicates where dataflows came from, as received by a given node. This table should be interpreted the same way as Table III where non-zero values indicate that packets from this previous hop were recorded by a node.

This table provides a picture of where packets were coming from when logged by a node. Specifically, it shows that most nodes spent a lot of time within the transmission range of the source nodes, nodes 21 through 24. This is evident by the fact that almost all of the nodes have a large number of packets from each source – it should be noted that this does not indicate how many of these packets were destined for the logging node.

This table also shows that nodes 62 and 64 received packets that were forwarded by the majority of the nodes in the network, while most nodes in the network did not receive forwarded traffic from nodes 50 through 61, 63, and 65. This indicates that nodes 62 and 64 were actively involved in forwarding traffic through the network. Examining the raw data, we could not find a correlation between the node degree and the forwarding count, so we assume that these nodes were simply in a location that lent itself to being a center point of the network.

After reviewing this data, we draw the following conclusions.

- Most of the packets traversed a one-hop path. While all nodes received a large amount of traffic directly from the source nodes most of these packets were not forwarded by these nodes. We assume that they either dropped these packets or the packets were destined for that host. Data later in this paper indicates that it was likely the latter and the nodes were well placed to receive their own packets.
- Since most of the nodes did not forward much traffic, for whatever reasons, it is difficult to externally observe the behavior of their strategies. We were disappointed by this and desired to see the strategies having more of an impact on traffic flow.

C. Traffic Dropping

This section concentrates on the behavior of the participants' strategies. Specifically, we show data regarding how many packets were dropped, correlated to the destination and the previous sender of the packet. These two characteristics are likely to be the major factors used to categorize packet that are being forwarded. These are the major factors because participants were interested in helping or hindering specific nodes based on observed behavior and the destination address and previous sender's address are about the only information that is useful in this context. Since we, the organizers, generated all of the traffic, the source address was likely of little interest to the participants.

As noted in Section III-B.2, many of the nodes did not receive traffic from a majority of the nodes in the network. This is actually a good thing because it allows us to observe how nodes behaved towards nodes that they were both familiar and unfamiliar with. Our metrics of interest in this context are the number and percentage of packets that a node drops. Again, this data will be presented grouped by packet destination address and the previous sender of the packet. We feel these two attributes are the most interesting to participants for the reasons previously mentioned.

1) Based on the Destination: Table V shows the percentage of packets that were dropped by each node, grouped by the packet's destination address. This percentage is based off of the total number of packets that the dropping node received

	50	51	52	53	54	55	56	57	58	59	60-61	62	63	64	65
50	20367	90	0	0	0	0	240	0	0	0	0	0	0	0	0
51	0	7794	0	0	0	0	0	0	0	0	0	0	0	0	0
52	0	0	1791	0	0	0	0	0	0	0	0	0	0	0	0
53															
54	0	1179	0	0	26400	0	0	0	558	0	0	0	0	621	0
55	0	0	0	513	0	18711	0	0	0	321	0	1350	993	204	0
56	0	588	0	0	0	0	7158	0	726	0	0	0	0	0	0
57	0	2190	123	0	774	378	0	24549	414	0	0	0	0	0	0
58	0	0	0	0	1233	0	0	0	0	372	0	0	0	0	0
59	0	3222	2517	501	0	642	1317	3579	945	25407	0	0	693	0	0
60															
61															
62	5277	4551	4137	1119	108	822	1746	915	4833	3141	0	25635	1089	2403	0
63	0	126	0	0	0	0	0	0	0	0	0	0	4446	0	0
64	0	0	0	0	0	0	0	597	0	0	0	0	0	4683	0
65	1353	1293	0	381	0	0	0	0	6	0	0	1371	768	1143	12429

TABLE III

THE TOTAL PACKETS LOGGED BY EACH NODE'S API ORGANIZED BY PACKET DESTINATION. ROWS ARE THE LOGGING NODE AND COLUMNS ARE THE PACKET'S DESTINATION ADDRESS.

	21	22	23	24	50	51-54	55	56-57	58	59-61	62	63	64	65
50	9	5385	7440	1728	0	0	0	0	0	0	5271	0	864	0
51	0	51	4887	0	57	0	0	0	0	0	2799	0	0	0
52	1005	0	741	0	0	0	0	0	0	0	45	0	0	0
53														
54	4905	9258	8907	3404	0	0	0	0	0	0	582	0	1702	0
55	6702	7665	4308	2036	0	0	0	0	0	0	159	0	1018	204
56	0	0	4374	1864	225	0	0	0	0	0	1077	0	932	0
57	4086	11430	4419	5452	0	0	150	0	0	0	165	0	2726	0
58	1161	0	0	296	0	0	0	0	0	0	0	0	148	0
59	4413	12375	10068	5748	0	0	0	0	807	0	2529	9	2874	0
60														
61														
62	10221	13401	4542	17608	0	0	777	0	0	0	0	0	8804	0
63	0	0	1014	1598	0	0	0	0	0	0	1035	0	799	0
64	789	4491	0	0	0	0	0	0	0	0	0	0	0	0
65	2718	5394	3684	3488	0	0	0	0	0	0	321	1395	1744	0

TABLE IV

THE TOTAL PACKETS LOGGED BY EACH NODE'S API ORGANIZED BY THE ADDRESS OF THE PREVIOUS HOP. ROWS ARE THE LOGGING NODE AND COLUMNS ARE THE PREVIOUS HOP.

destined to a specific address. The column indices are the destination address of the packet being logged and the row indices are the address of the logging node. A zero data value means that a node did not drop any packets destined for the specified node, while a blank cell indicates that no traffic destined to that (row) node was received. Zero values indicate that no traffic was dropped while values of 100 indicate that all traffic was dropped.

At first glance, the most noticeable attribute of this table is how sparse it is. This reiterates the observation that most nodes only saw traffic from a small subset of nodes in the whole network. After further inspection, it is evident that most of the values are either 0 or 100, indicating that most of the nodes took and "all or nothing" approach to forwarding traffic from neighboring nodes.

Only nodes 55 and 62 had drop percentages other than 0% and 100%. Of these two, node 62 is the most "interesting" with drop percentages that varied from 0% to 83%. This node was one of the nodes from the team that we, the organizers, fielded. This node employed a strict tit-for-tat strategy. It should also be noted that the two nodes on this team were not eligible to win the competition and actually did obtain the most points was the quantitative portion of the competition. We included this team in the competition to test how well two separate strategies would fair against other strategies. One node on the team employed a tit-for-tat strategy and the other simply forwarded every packet it was asked to forward. These nodes did not optimize their location to be in the range of as many sources as possible, like the rest of the participant nodes.

Table III alone does not completely depict how many packets were actually acted upon and thus only shows part of the impact of individual nodes. By observing the total traffic that each node received, in Table V, it is possible to calculate exactly how many packets were dropped or forwarded by each node. This is accomplished by multiplying the drop percentage in Table III by the total packets in Table V. The resulting value is the number of packets that were dropped by a host matching the destination address and logging node pair. Together these two tables accurately depict the impact that individual nodes had on individual neighbors and the network as a whole.

We have drawn the following conclusions from this data.

- Almost all of the participant strategies showed an "all or nothing" behavior, forwarding all packets destined for a host or none of the packets destined for a host. We were surprised by this behavior and expected more variable forwarding behavior.
- Participant strategies used the destination address of a packet to make decisions about how to act on a packet. This is a hypothesis, but we feel it is valid given the all or nothing behavior of the strategies. Had the participants used other information to make decisions, we think that these numbers would be between 0 and 100 instead of at 0 and 100.
- Again, the limited involvement of most nodes in the network means that nodes had limited information about how to deal with neighboring nodes.

Node	Drop Pct
50	0
51	0
52	0
53	0
54	75
55	73.259
56	66.667
57	83.333
58	50
59	77.778
60	0
61	0
62	26.802
63	0
64	50
65	75
Average	54.799

TABLE VII
THE AVERAGE DROP PERCENTAGE FOR EACH NODE AND THE AVERAGE FOR ALL NODES.

2) Based on the Previous Hop: Table VI shows the percentage of dropped packets grouped by the packet's previous sender. This percentage is based on the total number of packets that the logging node received from each previous sender. The column indices are the previous sender's address and the row indices are the address of the logging node. A zero data value means that a node did not drop any packets from the specific previous sender and a blank cell indicates that no traffic immediately from that (row) node was received. Zero values indicate that no traffic was dropped while values of 100 indicate that all traffic was dropped.

The values in this table vary from 0% to 100%. This data, compared with the data in Table V, leads us to believe that nodes used the destination address to make drop/forward decisions because of the variance in this table in contrast to and the striking "all or nothing" values in Table V. If both tables varied as much as this table, we would not have come to this conclusion.

Like the other tables, this data supports our assertion that nodes processed only a small subset of the streams flowing through the network.

D. Global Impact of Strategies

Given the data from the previous sections, this section discusses the impact the strategies had on the observed traffic flows. Table VII shows the average drop percentage for each node. Overall, the nodes have an average drop percentage about of 55%. If all of the traffic in the network passed equally through all of the nodes in the network, the loss should be around 50%.

	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
50	0	0					0									
51		0														
52			0													
53																
54		100			0				100						100	
55				100		0				100			39.5	100	100	
56		100					0		100							
57		100	100		100	100		0	100							
58					100					0						
59		100	100	100		100	100	100	0	0				100		
60																
61																
62	0	0	0	0	83.3	0	38.1	81.9	38.2	31.7			0	0	75.0	
63		0												0		
64								100							0	
65	100	100		100					100				100	100	0	0

TABLE V

THE PERCENTAGE OF PACKETS THAT WERE DROPPED BY EACH NODE, GROUP BY THE DESTINATION ADDRESS OF THE PACKET. ROWS ARE THE LOGGING NODE AND COLUMNS ARE THE DESTINATION ADDRESS.

	21	22	23	24	50	51 54	55	56-57	58	59-61	62	63	64	65
50	0	0	0	0							0		0	
51		0	0		0						0			
52	0		0								0			
53														
54	0	6.7	6.2	12.0							96.9		12.0	
55	12.7	0	23.0	16.7							0		16.7	100
56			16.5	21.0	0						0		21.0	
57	6.9	23.5	9.3	5.9			0				0		5.9	
58	67.9			100									100	
59	100	22.1	29.5	19.3					0		26.3	100	19.3	
60														
61														
62	17.6	4.7	16.5	11.2			0						11.2	
63			0	0							0		0	
64	75.6	0												
65	0	46.3	39.5	17.6							89.7	0	17.6	

TABLE VI

THE PERCENTAGE OF PACKETS THAT WERE DROPPED BY EACH NODE, GROUP BY THE PREVIOUS HOP'S ADDRESS. ROWS ARE THE LOGGING NODE AND COLUMNS ARE THE PREVIOUS FORWARDING NODE.

However, Table VIII shows that the actual average global drop rate is just over 20% for all tests. The actual drop values in this table show that a subset of the nodes, those not in the high drop percentage group, forwarded most of the traffic in the network. The key point of this section is that regardless of how each node actually behaved, the global behavior was more significantly affected by the nodes that were actually in the data path between a source and destination.

IV. LESSONS LEARNED

This section details specific lessons that we learned during this project. These are presented in no particular order.

A. Competitions are effective research tools.

First and foremost, the MANIAC Challenge was a success in multiple ways. First, it facilitated a medium-sized, heterogeneous MANET that worked well in the face of packet dropping and route manipulation. Second, it brought together

Version	Test	Accept Count	Drop Count	Drop Pct
2	1	69030	11914	17.259
2	2	64710	19129	29.561
2	3	64933	12120	18.665
2	Avg.	66224.333	14387.667	21.726

TABLE VIII
AVERAGE NUMBER OF ACCEPT AND DROP ACTIONS AND THE GLOBAL DROP PERCENTAGE.

researchers from all of the world who would have, likely, never been in the same place at the same time. Next, the collection of ideas for strategies extended well beyond what we could have devised on our own and showed how diverse such approaches can be. Finally, it created a wealth of experimental MANET behavior data for the research community we have made this data publicly available in the CRAWDAD Project [18].

B. Heterogeneous MANETs can exist with minimal effort.

While the logistics of creating and configuring the MANETs for the MANIAC Challenge were challenging, the actual communication between nodes in the network was almost flawless. We found few if any problems related to incompatibility between nodes. This leads us to believe that MANET standardization has come a long way and is mature enough to facilitate studies like this. The heterogeneous aspect of the MANIAC Challenge was not a challenge at all.

C. Location and hardware play a large role in communication ability.

In the first competition, the winning team had more traffic pass through its nodes than any other team. It is likely that the team's nodes' communication ability was better than the other nodes in the competition. We observed a similar run away victory in the second competition from a participant that worked hard to place himself in the "middle" of the network. Both of these winners had large amounts of the network traffic pass through them during the competition. Tangential to this is that in order for a forwarding strategy to have an effect on the network, traffic must be forwarded by that node, requiring it to be in a physical location that causes the routing protocols to send traffic to it. A good location can play a major role in the participation level of a node.

D. Nodes were nomadic and moved to maximize their connectivity.

In both competitions, participants paid close attention to how they where connected to the network and moved to maximize their connectivity with our source nodes. They did this by monitoring their routing table and moving slowly while watching carefully for the results of their movement. Most moved at the beginning of the competition, but settled down when they found a location that gave them reasonable connectivity with the most source nodes possible. This is interesting because it suggests there may be situations when nodes in a MANET move to maximize their communication ability. This is contrary to other movement models with no purpose or a purpose unrelated to communication ability. In some cases, communication may be the main concern. For example, notice how often people move about buildings trying to find a better mobile phone signal so they can use the phone.

E. Data flows traverse a small subset of the total set of routes.

We observed that packet flows through a network traverse only a small subset of the nodes in the network. When neighbor behavior observations are of interest, it is difficult to make such observations if traffic is nowhere near the node wishing to observe it. This lessens the possible impact of neighbor observation-based operations, such as reputation-based strategies.

We also noted that some nodes may become "core" nodes and end up forwarding a large percentage of the total traffic traversing the network. This bottleneck has been noted previously in MANET routing research. Our observations further confirm this, even in a fairly well-connected network with a high node-degree. In the context of forwarding strategies, this means that a single node can have a drastic effect on the network and can disrupt network traffic if it chooses to reduce its level of participation.

F. Node drop behavior varied little over time.

From Table V we observed that most nodes had drop rates of either 0% or 100%. From this we can summarize that most nodes did not vary their behavior over time. Regarding the participant strategies, we expected to see more variance over time of node behavior. This may be a result of strategies not seeing enough traffic to begin assessing the reputation of neighboring nodes. This would likely be a result of short lived traffic streams or the small amount of multi-hop traffic.

G. Participation strategies do affect the larger network.

Given the observations of this work, we conclude that participation strategies can have an effect on the network as a whole, but the level of effect varies based on other factors, including the location of the node in the network. Nodes on the periphery of the network can have "drop all" strategies, but the impact is minimal if if no traffic is routed to them. Conversely, nodes in the middle of a MANET, whether it be by choice or by chance, can have a drastic effect on the reliability of the network.

V. SUMMARY AND CLOSING THOUGHTS

In this paper, we presented some of the results of the MANIAC Challenge, a unique MANET research project structured around the premise of a competition. We discussed the premise and logistics of the competition, including the motivation, software, and venue. Next, we discussed some of the strategies that were employed by participants in the competition. Finally, the remainder of the paper presented and discussed results in the areas of traffic flow and the effects of participant strategies.

In the broader sense, we used the network created by the competition to study how experimental MANETs move and

change over time and how local participation strategies can affect global network performance. We observed traffic flows through the network and noted that only a subset of the nodes in the network will ever see specific traffic flows. We found that node location and physical hardware capabilities play a significant role in overall network performance. These considerations were more crucial than specific forwarding strategies adopted by the participant nodes.

We found the competition context to be an excellent way of getting others involved in hands-on experimental wireless network research. In addition, we found the competition scenario created a unique experimental MANET testbed from which to gather network behavior data.

ACKNOWLEDGEMENTS

We would like to thank all of the MANIAC participants over the years and the many folks at Virginia Tech and Bucknell who have contributed to the MANIAC Challenge project.

REFERENCES

[1] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *MobiHoc '02: 3rd ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM, 2002, pp. 226–236.

[2] L. Buttyán and J.-P. Hubaux, "Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks," Swiss Federal Institute of Technology, Lausanne, Switzerland,, Tech. Rep. DSC /2001/001, January 2001.

[3] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," *Performance Evaluation*, vol. 57, no. 4, pp. 427 – 439, 2004, selected Papers from the First Workshop on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (Wi Opt'2003).

[4] P. Dewan, P. Dasgupta, and A. Bhattacharya, "On using reputations in ad hoc networks to counter malicious nodes," in *ICPADS*, 2004, pp. 665–672.

[5] M. Felegyhazi, M. Félegyházi, L. Buttyan, and J.-P. Hubaux, "Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks - the static case," in *PWC 2003 Personal Wireless Communications*, 2003, pp. 23–25.

[6] J. Liu and V. Issarny, "Enhanced reputation mechanism for mobile ad hoc networks," in *2nd International conference on Trust Management*, 2004, pp. 48–62.

[7] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *6th Joint Working Conference on Communications and Multimedia Security*, 2001, pp. 107–121.

[8] V. S. Pavan, V. Srinivasan, P. Nuggehalli, C. F. Chiasserini, and R. R. Rao, "Cooperation in wireless ad hoc networks," in *IEEE Infocom*, 2003, pp. 808–817.

[9] A. Urpi, M. Bonuccelli, and S. Giodano, "Modelling cooperation in mobile ad hoc networks: A formal description of selfishness," in *Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, 2003, pp. 3–5.

[10] I. M. P. Golle, K. Leyton-Brown and M. Lillibridge, "Incentives for sharing in peer-topeer networks," in *2nd International Workshop on Electronic Commerce*, Novermber 2001.

[11] K. Lai, M. Feldman, I. Stoica, and J. Chuang, "Incentives for cooperation in peer-to-peer networks," Workshop on Economics of Peer-to-Peer Systems, Berkeley, CA, June 2003.

[12] Netfilter.org packet filtering project. http://www.netfilter.org/.

[13] Galveston island convention center at the san luis resert - floorplans and specifications. http://www.galvestonislandconventioncenter.com/floorplans/.

[14] S. Zhong, J. Chen, and R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *IEEE INFOCOM*, 2002, pp. 1987–1997.

[15] S. Buchegger and J. yves Le Boudec, "Performance analysis of the confidant protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks," in *IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing*, 2002, pp. 226–236.

[16] F. Juraschek, H. Will, M. G, and J. Schiller, "Friendly clustering - the winning strategy of the maniac challenge 2009," in *Fourth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH) - Demosession*, Beijing, China, 21 September 2009.

[17] A. AbdelRahman, M. El-Nasr, and O. Ismail, "A novel forwarding/dropping decision engine for wireless multi-hop ad-hoc networks," in *5th International Conference on Collaborative Computing*, November 2009, pp. 1 –5.

[18] Crawdad project - maniac competition data. http://crawdad.cs.dartmouth.edu/meta.php?name=vt/maniac.