ENHANCING THE PERFORMANCE OF MOBILE AD HOC NETWORKS WITH INTERNET GATEWAYS

SHIV MEHRA

Bachelor of Engineering in Electronics and Telecommunication Engineering

University of Bombay, India

June, 2000

Submitted in partial fulfillment of requirements for the degree

MASTER OF SCIENCE IN ELCTRICAL ENGINEERING

at the

CLEVELAND STATE UNIVERSITY

December, 2003

ACKNOWLEDGEMENT

I would like to express my sincere indebt ness and gratitude to my thesis advisor Dr. Chansu Yu, for the ingenious commitment, encouragement and highly valuable advice he provided over the entire course of this thesis.

I would also like to thank Dr. Vijay Konangi and Dr. Yongjian Fu for their constant support and advice throughout the work.

I wish thank Kalyan Kalepu, Lubo Song, Nischala Uppala, Sinjae Lee, Sridhar Kalubandi and Wissam Chedid for their encouragement and feedback during the entire course of this thesis.

ABSTRACT

Mobile ad hoc networks allow mobile nodes to communicate with one another without the aid of infrastructure thus forming temporary networks on the fly. For such networks to be operational a special routing protocol has to be designed due to possibility of frequent node mobility. Each node in the network acts like a host as well as a router, thus forwarding data on behalf of other mobile nodes in the network. While such networks are gaining immense popularity, they are prone to scalability issues when the network size (number of nodes) increases, causing the path length between the source and destination to increase linearly. Hence a large number of intermediate nodes are burdened with the forwarding load imposed by other mobile nodes, drastically affecting the performance of ad hoc networks.

In this thesis, a technique to enhance the capacity of ad hoc networks is implemented. The technique exploits the existing infrastructure by placing gateways at fixed locations in the ad hoc network. They are originally placed to provide Internet access to mobile nodes in an ad hoc network, but they can also be utilized to facilitate communication among nodes in the ad hoc network. Those gateways serve as relay nodes, thus taking responsibility of relaying most of the burden (packets) imposed by the mobile nodes in the network. The presence of such gateways is transparent to the mobile nodes and hence the ad hoc routing protocol does not require any complex modification. While it is not surprising that those gateways improve the MANET performance significantly, the main theme of this thesis is to analyze the performance gain quantitatively so that a network designer can decide on the number of gateways as well as the location of gateways in the MANET.

The technique is implemented and simulated based on the Qualnet simulator with Ad hoc On-demand Distance Vector (AODV) protocol as the underlying ad hoc routing protocol. The simulation shows that the capacity of ad hoc networks increases significantly with the introduction of the proposed gateway.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page

CHAPTER I

INTRODUCTION

1.1 Background

Wireless networks consisting of mobile devices coupled with wireless connectivity are becoming an essential part of the future computing environment. Such wireless networks can be broadly classified into two categories according to their dependence on communication infrastructure [35]. Networks in the first category are designed based on the cellular architecture in which nodes communicate via fixed centralized base stations. These base stations control all the transmissions in the network and forward the data to

the intended destinations. Examples of such networks are the cellular phone network and the *Wi-Fi* networks that provide Internet connectivity to mobile users.

A network in the second category consists of mobile devices that use other mobile nodes as routers to route their packets to their intended destination. Such a network is called *Mobile Ad hoc Network (MANET)* [23]. The research on MANETs was initiated by the *Defense Advanced Research Projects Agency (DARPA)* to form a temporary communication network in battlefields and disaster struck areas where the wired infrastructure is unavailable or disrupted [19]. Recently, they have gained immense popularity in the commercial market, and for this reason, the *Internet Engineering Task Force* (IETF) has started a corresponding working group aimed at standardizing IP routing functionality for MANETs [23].

While the deployment and configuration of MANETs can be effortlessly done, a major obstacle is that the location based routing cannot be used due to node mobility and is more critical than in cellular architecture-based networks because not only the source and destination but also the intermediate nodes (acting as routers) are mobile. An intelligent routing protocol must be employed so that each node dynamically finds and maintains routes to destinations. There have been many routing protocols proposed in the literature and three most popular algorithms are *Destination Sequenced Distance Vector (DSDV)* [29], *Dynamic Source Routing (DSR)* [4] and *Ad-hoc On-demand Distance Vector (AODV)* [27].

In addition to the efficient routing, there has been a great demand on providing Internet access to MANET nodes even though the MANET is originally a stand-alone network. This can be achieved by integrating the cellular-architecture based networks

with MANET(s) opening many interesting research issues in such hybrid ad hoc networks. Here base stations or Internet gateways forward data traffic to and from the Internet for mobile nodes in the MANET. Various hybrid networks have been suggested to provide Internet connectivity to MANETs as will be discussed in Chapter III [2,5,11,18,20,33,34]. These hybrid networks can also be considered as an extension of a single-hop cellular network with the multi-hopping techniques. In fact, it is a cost effective solution since less infrastructure is required as nodes are capable of communicating with base stations over multiple hops.

1.2 Thesis Description

In this thesis, we consider the scalability of a MANET. When the number of nodes in the network increases, the burden on intermediate nodes as routers increases and this leads to a significant degradation of per-node throughput as well as more power consumption. This is mainly due to the increased path length between the source and destination. It has been shown that as the number of nodes in the network increases the effective bandwidth of the network drastically decreases as the square root of the number of nodes [13].

This thesis suggests improving the MANET scalability by utilizing the Internet gateway that is originally introduced to provide Internet access to MANETs. These gateways can be used to facilitate communication between MANET nodes. Advantages of such a scheme have been discussed in [6,22,36]. A unique feature of the approach proposed in this thesis is that the nodes in the MANET are not required to know about the presence of such gateways. We call them ***T****ransparent* ***A****d hoc* ***N****etwork* ***G****ateways or*

TANGs. TANGs communicate with one another over high bandwidth wired links thus forming a backbone infrastructure. The main objectives of this thesis are (i) to design an infrastructured MANET based on TANGs and (ii) to evaluate and compare the proposed solution via simulation.

1.3 Thesis Structure

This thesis is organized as follows: Chapter II gives an overview of *Mobile IP* [30] based infrastructured networks and MANETs. It also introduces three important MANET routing protocols: DSDV [29], DSR [4] and AODV [27]. Chapter III discusses the related work pertaining to scalability issues in MANETs. It also gives a brief overview of various techniques providing Internet connectivity to MANETs proposed so far in literature. Chapter IV presents our solution to improve the performance of MANETs based on TANGs. Chapter V gives an overview of the implementation detail of the proposed scheme within the *Qualnet* simulator [31]. This chapter also presents the simulation results and discusses the various inferences made from the obtained results. Chapter VI concludes this thesis.

CHAPTER II

BASIC MOBILE NETWORKS

This chapter gives an overview of two basic mobile networks: Mobile IP based infrastructured networks (Section 2.1) and mobile ad hoc networks (Section 2.2).

2.1 Mobile IP [30]

Mobile IP is a mechanism for maintaining transparent network connectivity to mobile hosts. Mobile IP protocol enables a mobile host to be addressed by the IP address it uses in its home network, regardless of the network to which it is physically attached. Mobile IP introduces the following terminologies.

- *Mobile Node (MN)* is defined a host or a router that changes its point of attachment from one subnet to the other.

- *Home Agent (HA)* is defined as a router on the MN's home network that delivers the data packets destined for the MN to the foreign network where the MN is physically attached.
- *Foreign Agent (FA)* is defined as a router on the MN's visited network that provides routing services to the registered MN. FA broadcasts the *agent advertisement* messages periodically to inform a new MN about the foreign network.

2.1.1 Mobile IP Operation

When a MN moves out of its home network and enters a new foreign network it needs a new address called *care-of address* (COA) to communicate with the Internet. The MN obtains a COA through the FA where it currently resides. Mobile IP defines two messages that are broadcasted to obtain the services of an FA: (i) *agent advertisement* that are broadcasted by the FA as mentioned above and (ii) *agent solicitation* messages that are broadcasted by the MN (in search of an FA). However, if the FA is absent the MN can obtain a COA by different means, for example, through a gateway running the *Dynamic Host Configuration Protocol (DHCP)* [7]. Such an address is called a co-located COA. When an MN receives an *agent advertisement* from the FA, it registers with its HA via the FA giving its current location, identifiable via the COA. Thus the data destined for the MN can be delivered by the HA via the FA. Mobile IP is designed to operate when the FA and the MN are in direct communication range. Thus the FA uses the hardware address for forwarding the packets destined for the MN.

2.2 Mobile Ad Hoc Networks

A mobile ad-hoc network is a collection of mobile nodes that form a temporary network without the aid of fixed communication infrastructure. Since the quality of radio signal degrades with distance the effective transmission range of a node is limited and it makes it necessary for one mobile node to take the assistance of other nodes in forwarding its packets to the destination that is out of its transmission range.

Routing is the most critical design issue in a MANET due to its dynamic nature. The initial approach used for routing was *proactive*, i.e. each mobile node constantly keeps track of routes in the network and this requires the node to exchange control messages at a regular time interval. In a network where bandwidth is not a major constraint, proactive protocols would be preferred since the lead time to start a transmission is less as routes to a destination are available instantly. Section 2.2.1 introduces one such proactive algorithm, called *DSDV (Destination Sequence Distance Vector)* [29]. Later, *reactive* algorithms, where routes are discovered only on demand, have been proposed to alleviate the overhead corresponding to the periodic control messages. *DSR (Dynamic Source Routing)* [4] and *AODV (Ad-hoc On-Demand Distance Vector)* [27] protocol are the well-known reactive algorithms, which will be explained in Section 2.2.2 and 2.2.3 respectively.

2.2.1 Destination Sequence Distance Vector (DSDV) [29]

DSDV is a proactive protocol and is based on the distance vector algorithm used in Internet. Due to the dynamic characteristic of the network the nodes periodically

broadcast routing updates. Each node updates its routing table periodically with routing information to all destinations such as the number of hops to each of the destinations and the next hop node.

DSDV uses sequence numbers, which is initiated by the destination itself, to maintain fresh and loop-free routing paths. When a route to the next hop is broken the node immediately broadcasts the information to its neighbors with the incremented sequence number corresponding to that particular destination. When a mobile node receives new routing information, it checks its routing table to determine if it has a similar kind of information. If the node already has that routing information then it compares the sequence number of the received information to evaluate its freshness. If the sequence number of the information it has is less than that of the received information then it updates its table. If both sequence numbers are the same, the node keeps the information that has the shortest route (or the least number of hops to that destination).

2.2.2 Dynamic Source Routing (DSR) [4]

DSR is a reactive protocol and uses the concept of source routing. It means that the source determines the complete path to the destination that the packets have to traverse, and each packet carries the entire route information in its header. DSR thus permits an intermediate node to cache the routing information in their route cache for their future use.

The DSR discovers routes and maintains routing information by using two main mechanisms: *Route discovery* and *Route maintenance*. *Route discovery* is the process that a source desiring to send data to a destination obtains a route to the destination if it does not have one in its route cache. Route maintenance is the mechanism that the node keeps

track of those routes. When a node finds a link breakage to one of its neighbors while forwarding a packet, it sends a route error message back to the source node. The source as well as all the intermediate nodes updates their route cache by invalidating the routes that contain the broken link. Then, the source node tries to use an alternative route to the destination or invokes a Route discovery for the destination again.

2.2.3 Ad-hoc On-Demand Distance Vector (AODV) [27]

AODV is a combination of DSR and DSDV. It uses the concept of *Route discovery* and *Route maintenance* mechanisms from DSR and uses the concept of sequence numbers, hop-by-hop routing and periodic beacons (i.e. *hello messages*) from DSDV. AODV is an on-demand routing protocol, i.e. routes to the destination are only discovered when required thus avoiding control overhead and consuming less power. AODV uses the sequence number that is generated by the destination for each route entry. The destination sequence number ensures loop freedom and if two similar routes to a destination exist then the node chooses the one with the highest sequence number giving a priority to a more recent route information. AODV uses *Route Request (RREQ)*, *Route Reply (RREP)*, and *Route Error (*RERR*)* messages for route discovery and maintenance. The functioning of AODV is explained below in detail.

Generating and Handling RREQ and RERR

When a source wants to send data to a destination and does not have a route to it, it generates an RREQ packet and broadcasts it. The RREQ uses the following fields in its

packet: *Hop Count*, *RREQ ID*, *Destination IP Address*, *Destination Sequence Number*, *Originator IP Address*, and *Originator Sequence Number*. The hop count is the number of hops from the source to the node handling the RREQ. Thus when a node receives an RREQ, it increments the hop count by one and rebroadcasts the packet to its neighbors. RREQ ID is a number that uniquely identifies the RREQ and is used not to process the same RREQ more than once. Destination sequence number is the greatest sequence number received in the past by the originator for any route towards the destination.

When a node receives the RREQ packet it checks to see if it is a destination. If not, the node checks its routing table to see if it has a route to the destination. If it does, it checks the destination sequence number in the RREQ packet with the one it has. As in DSDV if the destination sequence number it has is greater than the one in the RREQ then the node sends a RREP to the source stating that it has a route to the destination. A route associated with a higher Destination sequence number is regarded as a fresher route to the destination. If the node does not have a route to the destination or if the node has a route but the sequence number associated with the route is less than that in the RREQ, the node updates its routing table, increments the hop count by one and rebroadcasts the packet to its neighbors. At this point, the node creates a reverse route to the source by recording the address of the neighbor from which it received the RREQ. The reverse route will be used to forward an RREP to the source. When the destination receives the RREQ packet it prepares an RREP packet, increments its current destination sequence number by one and sends the RREP packet to the source through the constructed reverse paths. The source waits for the RREP for a fixed interval of time and retransmits the RREQ if it does not

receive an RREP. If no response is received for a predefined number of times then the source declares the destination is unreachable.

Route Table Management

The route table of a node maintains entries for each destination the node is interacting with or forwarding packets to. Each entry includes the following fields: *Destination IP address, Number of hops*, *Next hop, Destination Sequence Number*, and *Expiration time for the entry*. They help the node to maintain the connectivity of the network. The expiration time associated with the route depends on the size of the MANET and indicates the time after which the particular entry is to be removed. In addition, each node maintains the list of active neighbors so that if a link to one of the active neighbors is broken the node immediately invalidates the entry in the route table and broadcasts an RERR message. This is how AODV reacts to link failures.

Hello Messages

A node broadcasts Hello Messages periodically to maintain connectivity even in the absence of communication. It contains the identity of the sender and sequence number so that its neighbors can update their local connectivity. A node thus assumes a link is broken if it does not receive a Hello message for some predefined amount of time interval from one of its neighbors. It then broadcasts an REER packet to its neighbors regarding the link failure as discussed above.

CHAPTER III

RELATED WORK

As discussed in Chapter I, the main theme of this thesis is to improve the scalability of MANET with the help of Internet gateways. While the original idea of introducing Internet gateways in MANETs is to provide Internet connectivity to MANET nodes, this thesis investigates the possibility of utilizing the Internet gateways to support communication among mobile nodes. In this chapter we introduce and discuss previous works on those two related issues: scalability of MANETs (Section 3.1) and Internet connectivity to MANETs (Section 3.2).

3.1 Scalability of MANETs

When the size of a MANET increases the average distance between the source and destination increases linearly which results in larger delay and drastic decrease in per node capacity. This is mainly due to the large amount of forwarding load imposed on the

intermediate nodes. Random access-based *MAC (Medium Access Control)* protocols, as used in *IEEE 802.11* standard [30], aggravates the situation by increasing the amount of competition a node faces for transmissions as discussed in [21]. Their results show that the end-to-end throughput available to each node degrades as $O(1/\sqrt{n})$, where n is the number of mobile nodes. Another related study showed that the average throughput available to each node is shown to degrade as $O(1/\sqrt{(n\log n)})$ and that $O(1/\sqrt{n})$ is only achievable when the nodes are optimally placed and the range of each transmission is optimally selected [13].

3.1.1 Simple Solutions to Enhance Scalability

According to the aforementioned discussion, the effective bandwidth of a MANET decreases as the number of nodes within the MANET increases. In a large scale MANET, data packets must go through a large number of intermediate nodes before reaching the destination limiting the scalability. In addition to data packets, the overhead induced into the network due to the flooding of control packets (such as RREQ discussed in Chapter II) in the entire network limits the scalability drastically. In the following section, two simple solutions are considered, one for reducing the number of intermediate nodes and the other one for reducing the control overhead.

In [12], the authors exploit the node mobility to improve the average long-term throughput per source-destination pair. They propose that a source node should broadcast its packet to its one-hop neighbors and let one of them deliver the packet to the destination. Since nodes are moving all the time, there is a high probability that at least one relay node gets closer to the destination. This approach does not require any fixed

infrastructure and hence it is cost effective. However the delay incurred due to this approach can be tremendous and hence the solution is limited to high delay tolerant applications. In addition since packets have to be buffered until the destination is close enough, a large buffer size at each node is required. Lastly the performance of this scheme greatly depends on node mobility.

Control overhead is incurred in order to find and maintain the routing paths among nodes. A clustering scheme has been proposed to reduce the control overhead in a large scale MANET [37]. It dynamically builds a hierarchical ad hoc network with backbone nodes, which take care of relaying control packets (possible data packets too) on behalf of other nodes. This scheme breaks a large MANET into a number of small clusters, each with a backbone node and the flooding of the control packets are limited to the backbone nodes. The main advantage of this scheme lies in the selection and maintenance of the backbone nodes as well as overloading on those backbone nodes.

3.2 Internet Access to MANETs

This section gives a brief overview of various techniques for providing Internet connectivity to MANETs proposed so far in literature. Providing Internet connectivity to MANETs requires gateways that act as bridges between the MANET and Internet, since the gateway has to understand the *Internet Protocol (IP)* as well as a MANET routing protocol (e.g. AODV), the routing flow between a MANET node and an Internet node can be drawn as in Figure 3.1.

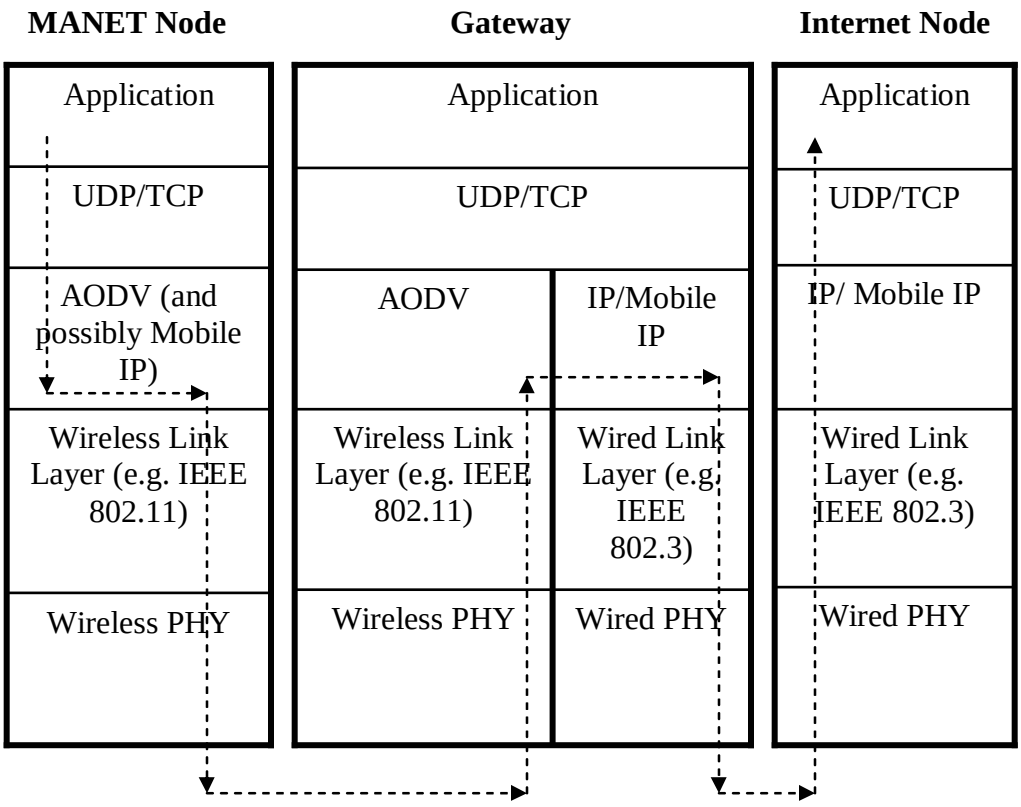


Figure 3.1 Routing flow through the protocol stack between a MANET and Internet node.

An overview of the techniques is provided in Table I. They are generally classified into two groups, depending on whether they use Mobile IP or not to provide Internet access to MANETs. Section 3.2.1 discusses the technique, wherein the Mobile IP Foreign Agent (FA) provides gateway services between the Internet and MANET. In this technique mobile nodes in the MANET, which are running the Mobile IP software as well as the MANET routing protocol are the only nodes that gain access to the Internet. In Figure 3.1, a MANET node runs both AODV and Mobile IP protocol. The gateway is a Mobile IP Foreign Agent and thus this technique utilizes Mobile IP for providing Internet access to MANETs. Section

3.2.2 explains the second technique in which, the Internet Gateway between the MANET and the Internet provides Internet access to all nodes in the ad hoc network. In Figure 3.1, a MANET node runs AODV algorithm only.

Table I Techniques to provide Internet connectivity to MANETs.

Mobile IP Foreign Agent as Gateway Router (Seamless Roaming Supported) (Nodes running both, the Mobile IP software as well as the MANET routing protocol gain Internet access - Section 3.2.1)			
Implementation	Special Features	Routing Protocol	Section
Simulation/Real	Special FA RREP packet is introduced.	Ad Hoc On-Demand Routing Protocol	3.2.1.1 [2]
Simulation in Network Simulator-2 [9]	*MIP*MANET *Cell Switching Algorithm*: This algorithm helps the MN to decide when to switch to a new FA	Ad Hoc On-Demand Routing Protocol	3.2.1.2 [18]
Simulation in Network Simulator-2	*Duplicate Address Detection* [28]: This algorithm helps a node to obtain a unique co-located care-of-address when an FA is not available.	Ad Hoc On-Demand Routing Protocol	3.2.1.3 [34]
Real implementation on OS/2 and AIX	*Implementation of the Route Manager Program*: The route manager coordinates the operations between the MANET routing and Mobile IP to update the nodes routing table.	Modified Version of Routing Information Protocol [14]	3.2.1.4 [20]
Internet Gateway as a Router (Seamless Roaming *Not* Supported) (All Nodes in the MANET gain Internet access - Section 3.2.2)			
Real implementation on Linux / Windows NT	*Cluster Gateway Model*: It is a routing protocol independent gateway acting as a Service Access Point and a FA	Source Initiated Routing Protocol [32]	3.2.2.1 [33]
Real implementation on Free BSD	*Spanning* MANETS *across Heterogeneous Interfaces*: Enables the nodes in the ad hoc network to communicate over different interfaces	Dynamic Source Routing Protocol [4]	3.2.2.2 [5]
Simulation in C++ Protocol Toolkit (CPT) [3] on Sun Ultra II Sparc Workstations	*Implementation of FAMA-NCS* [10] – The Floor acquisition multiple access with non-persistent carrier sensing is implemented as the MAC layer protocol to reduce the control traffic in the network.	Wireless Internet Routing Protocol [25]	3.2.2.3 [11]

Note that the discussion in this chapter is centered on the following three issues that are important to the design of such infrastructured MANETs.

- Naming Convention: The addressing mechanism on the Internet is hierarchical while such an addressing scheme is not viable in ad hoc networks due to dynamic topological changes hence the integration of the two becomes a challenging task.
- Discovery and registration process: This is the process in which, MANET nodes register with the gateway/router to gain access to the Internet.
- Mobile IP (MIP): The industry-standard Mobile IP mechanism [30] can be used for providing Internet access to MANETs.

3.2.1 Mobile IP Foreign Agent as an Internet Gateway

In Figure 3.2 MN1, MN2 and FA are running Mobile IP software as well the MANET routing protocol. The Mobile IP FA acts as gateway and provides Internet service to MN1 and MN2. The MANET routing protocol and Mobile IP have to be modified so that Mobile IP messages can be sent over multiple hops. Thus if MN1 desires to gain access to the Internet it has to first locate a FA and hence it initiates a RREQ as seen in the Figure 3.2. Once MN1 discovers the FA, it sends agent solicitation messages and registers with its HA by following the normal Mobile IP procedures. However the Mobile IP messages have to be routed using the MANET routing protocol. It should be noted that it is possible to have a mobile node that runs the MANET routing protocol only and does not understand the Mobile IP messages. Node N1 in Figure 3.2 is such a node and it cannot gain Internet access even if it wishes to.

The various techniques discussed in this section follow the aforementioned basic concept in providing Internet connectivity to MANETs. The difference among the techniques lies in FA discovery and handoff mechanisms.

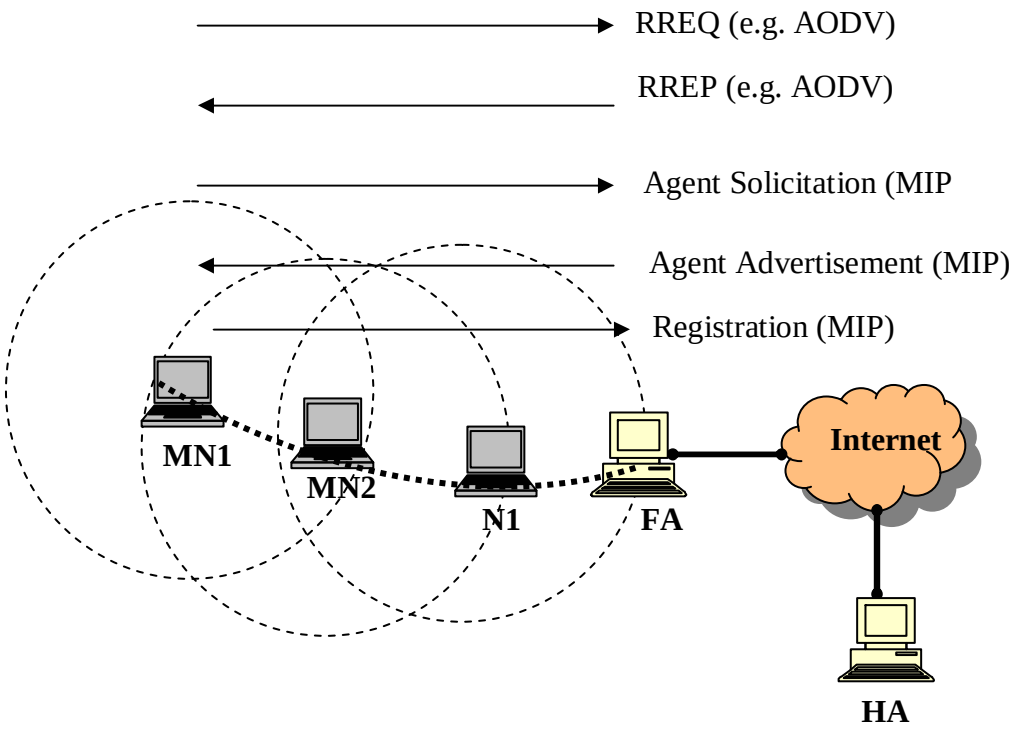


Figure 3.2. Mobile IP FA as a gateway.

3.2.1.1 Global Connectivity for IPv4 MANETs

In [2], the authors assume that the MN gains access to the Internet by obtaining a COA from a Mobile IP FA, which provides the gateway services between the wired Internet and the MANET. The AODV [27] routing protocol, discussed in Chapter II is used for routing within the MANET and for obtaining routes to the FA.

Foreign Agent Discovery and Mobile Node Registration

When an MN desires to access the Internet it prepares an RREQ packet to discover an FA in the MANET. The MN sets the destination IP address as 224.0.0.11 ("All Mobility Agents" i.e. FA and HA multicast group address) in the RREQ and broadcasts it. If the node receiving the RREQ is the FA itself, the FA unicasts a FA-RREP as described below. On receiving the FA-RREP the MN follows the basic Mobile IP procedure to access the Internet. Once the MN has registered with the FA it broadcasts (just once) the FA advertisement on its interface so that other MN's desiring Internet connectivity can register with the FA.

FA-Route Reply

Upon receiving the RREQ, the FA replies with RREP. The authors extend the RREP message discussed in section 2.2.3 to relay additional information regarding the presence of FA's within the MANET. Such an RREP is termed as the FA-RREP and is similar to the normal RREP with an addition of a 'F' bit to it. When the 'F' bit is set, it indicates that the RREP is from the FA. The MN uses this information to distinguish between the RREP from a FA and that from a normal node so as to decide whether the node is on the Internet or in the MANET.

FA-RREP versus RREP

When a MN desires to send packets to a particular destination it first search its routing table to locate an entry that completely matches the IP address of the destination. If found, it should use that route, otherwise, it should try to search for the destination in the

ad hoc network by using normal AODV operation. In this process it is quite possible that the MN would receive the FA-RREP before it receives the normal RREP from the destination, especially if the destination is far from the source when compared to the FA as seen in Figure 3. 3 below. In Figure 3.3 the source S initiates an RREQ but since it is closer to the FA than to the destination, it receives an FA-RREP before the normal RREP from the intended destination D can be received. The source S should not use the route through the FA, but should wait till a normal RREP message is received from node D. If a RREP is not received within the predefined time the MN can assume the node is on the Internet and can route the packets to the FA (assuming it has a route to the FA).

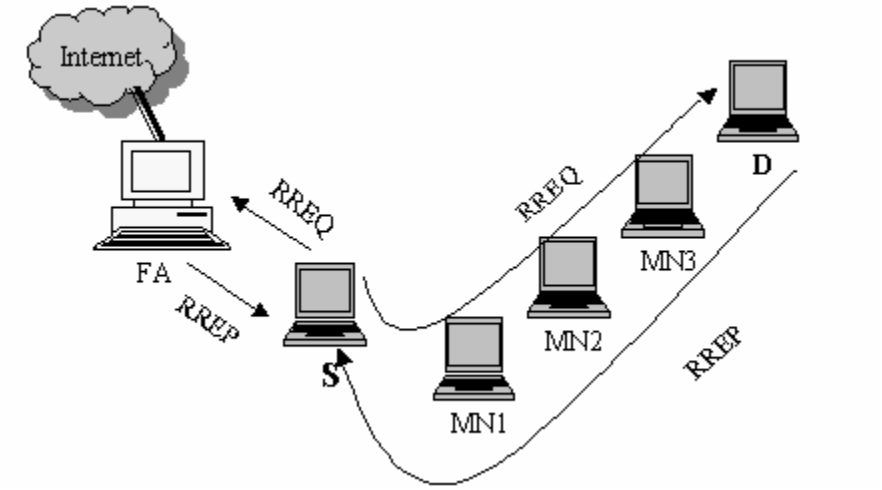


Figure 3.3. Path selection with FA-RREP.

3.2.1.2 MIPMANET- Mobile IP for MANET

In [18], the authors propose the *MIPMANET* protocol that provides Internet access to MANETs with the aid of the Mobile IP FA as the gateway and using the mechanism of *reverse tunneling* [24]. The authors assume that the MN requesting Internet access has a

home address, which is valid on the Internet. The technique is implemented in Network Simulator-2 (ns-2) [9] with AODV as the MANET routing protocol.

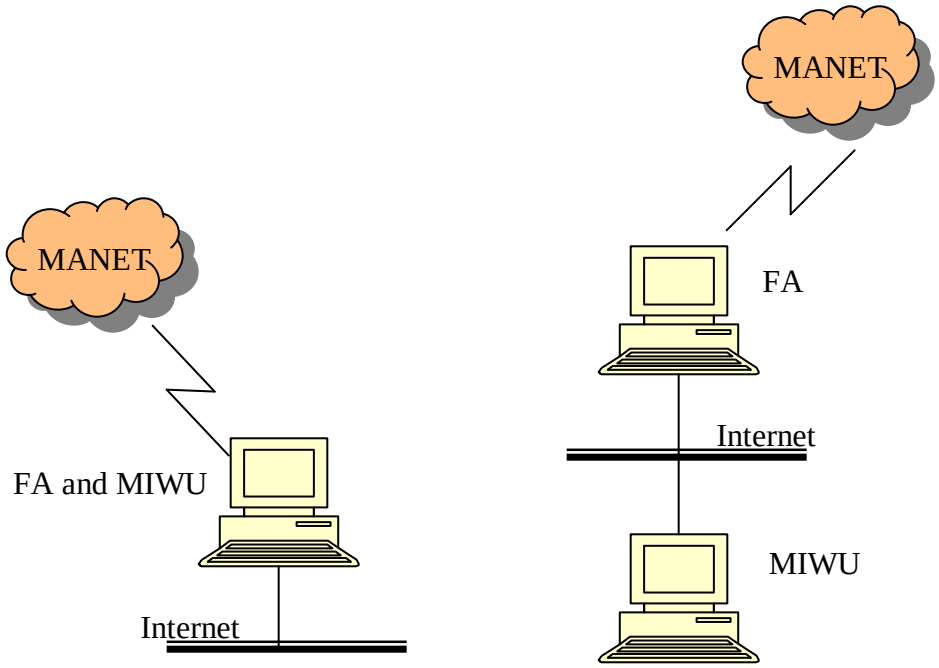
FA Discovery

The FA discovery mechanism in this section is slightly different from that discussed in 3.2.1.1 since there is no special FA-RREP. If the MN does not have a route to the FA it can initiate an agent solicitation message and broadcast it over the MANET. When a FA receives the agent solicitation it can either broadcast the agent advertisement or unicast it to the MN. The approach chosen depends on the number of MN's in the network. If the number of MN's in the network is small the authors propose to unicast the advertisement to the MN since broadcasting would lead to flooding the ad hoc network. But if there are large number of MN's then unicasting advertisement to each MN would be more expensive than broadcasting the advertisements.

Changes to Mobile IP

As mentioned in Section 2.1 the FA and MN communicate with each other using the hardware address instead of the IP address. But when the FA and MN are multiple hops away the hardware address cannot be used and hence the authors propose a separate unit called the *MIPMANET Internetworking Unit* (MIWU), which is inserted between the FA and the MANET. The MIWU is a module that can be loaded on the FA or on a separate host, which is on the same link as the FA as seen in Figure 3.4. It possesses all the MANET routing protocol functionality and the required changes to Mobile IP. From the FA's point of view the MIWU is an MN that is registering with different IP addresses,

but with the same hardware address, thus solving the aforementioned problem of communication between the FA and MN over multiple hops.



(a) MIWU and FA on the same host (b) MIWU and FA on separate hosts

Figure 3.4 MIPMANET internetworking unit

3.2.1.3 Internet Connectivity to Ad hoc Mobile Networks

In [34] the authors propose a technique similar to that discussed in 3.2.1.1 with the exception of a co-located COA if FA is not available. The technique is implemented in the ns-2 with AODV as the MANET routing protocol.

Obtaining a Unique Co-located Care-of-Address

As mentioned in Section 2.1, a MN can acquire a COA either through a FA or through a gateway. Nodes configure their own COAs by using the advertised network prefix. They first choose a random identifier to append to the network prefix. This is the address for which they will perform the *Duplicate Address Detection* (DAD) [28] and is called the requested address. Then, they choose any arbitrary temporary address and prepare an *Address Request* (AREQ) packet that is broadcasted to its neighbors. When the other nodes in the MANET receive the AREQ they first create a reverse route to the temporary address and then check their own IP address with that of the requested address. If there is a match, then that node prepares an *Address Route Reply* (AREP) stating that the requested IP address is already in use and unicasts the AREP on the reverse route to the source node. If the IP address does not match, then the node simply rebroadcasts the AREQ. If the source node does not receive the AREP in a specified amount of time, it assumes that the address is unique and begins to use it, else if it receives an AREP then the node again chooses a random identifier and repeats the entire process.

3.2.1.4 Ad hoc Networking with Mobile IP

The authors of [20] propose a solution by which Mobile IP is integrated with a proactive MANET routing protocol to provide Internet connectivity to all nodes in the MANET. The authors point out that both the Mobile IP and MANET routing protocol modify the nodes routing table. They thus introduced a *route manager* process to coordinate between the two protocols. Thus instead of modifying the routing table directly, both Mobile IP and the MANET routing protocol send their respective route

modification request to the route manager who then decides which modifications will take affect. All nodes in the MANET run both, the Mobile IP as well as the MANET routing protocol. The proactive routing protocol used in this implementation is a modified version of the *Routing Information Protocol (RIP)* [14].

Internetworking between Mobile IP and the MANET routing protocol

Mobile IP was modified to enable unicasting of messages between the FA and the MN over multiple hops. The RIP was modified to pick up agent advertisements/solicitations from the Mobile IP software running on the FA/MN and route them to all the other nodes in the MANET, thus extending the range of the FA to nodes multi-hops away. Both, Mobile IP and modified RIP update the entries in the routing table. If the two processes request a route entry to the same destination via the different gateways then either one of the routes can be entered in the routing table but not both. To resolve this issue the authors have implemented a *route manager* (rtmgrd) program as mentioned earlier, which decides on routes and manages the routing table. The modified RIP has the current-updated topology of the network and hence the routes requested by it are given priority over the routes requested by Mobile IP. Thus Mobile IP as well as the MANET routing protocol is modified to relay their route manipulation request to the rtmgrd.

3.2.2 Internet Gateway as a Router

This section discusses three techniques that have specially designed gateways to provide Internet access to the MANETS. The first technique requires all the MANET nodes to register with the Internet gateways. In the second technique the entire MANET

is considered to be a single IP subnet thus making the task of routing easier. The third technique introduces a gateway, which keeps track of all the topological changes in the network and updates the MANET nodes with the corresponding information.

3.2.2.1 Protocol Independent Internet Gateway for MANETs

In [33] the authors propose a special Internet gateway that works together with the MANET routing protocol to provide Internet access for mobile nodes. The proposed gateway functions independently of the underlying MANET routing protocol, thus the MANET nodes need not run any additional software apart from the MANET routing protocol to gain Internet access. Such a gateway is named as the *Cluster Gateway (CG)*. This technique was implemented on a real test bed with Linux and Windows NT machines and the routing protocol used is *Source-Initiated Adaptive Routing Algorithm* (*SARA)* [32].

Services Provided by the Cluster Gateway

The CG provides two services: (i) Service Access Point (SAP) and (ii) Mobile IP Service. In the SAP mode the CG acts as a simple Internet Gateway and performs *Network Address Translation (NAT)* [8] for all outgoing packets from the node in order to assure proper routing to the Internet. In the Mobile IP service mode the CG acts as a normal Mobile IP FA for a MN in the ad hoc network.

Internet Access via CG

The technique proposed in [33] requires every node in the MANET to register with the CG irrespective of their desire to obtain Internet connectivity. This gives CG the capability to determine whether a node is on the Internet or the MANET. Thus the nodes wishing to communicate with other nodes have the option to search the entire MANET for the destination using the MANET routing protocol or "ask" the CG about the location of the nodes (i.e. whether the node is on the Internet or the MANET). When packets are destined for a node in the MANET, since the CG has information about all the nodes in the MANET, they get routed to the CG, which uses the MANET routing protocol to route the packets to the destination.

3.2.2.2 Supporting Hierarchy and Heterogeneous Interfaces in MANETs

In [5] the authors not only introduce a technique to provide a MANET with Internet connectivity but also support for heterogeneous interfaces to achieve internetworking of MANETs. This technique assigns the MANET nodes with an IP addresses from a single IP subnet thus, creating an illusion to the outer world that the ad hoc network is a normal IP subnet. This is in contrast to the technique discussed in 3.2.1.1 where all the MANET nodes may not have the same address. The technique has been implemented practically with DSR as the MANET routing protocol.

Gateway Operation and Discovery

The gateway discovery is quite similar to that discussed in Section 3.2.1.1. Whenever a node wishes to access Internet, it prepares an RREQ as described in DSR [4]. Assuming

that the destination is within the MANET and it has a valid IP address on the Internet, the source node may receive two replies, one from the destination itself (which is presently in the MANET) and the other from the gateway (proxy reply). The gateway uses the reserved *gateway interface index* in the proxy reply and thus the source can differentiate between the gateway RREP and the normal RREP. The node thus uses the normal RREP rather than the gateway RREP if it receives both. However, if the node does not receive the normal RREP it assumes the node is on the Internet. It then sends the packets to the gateway. The gateway on seeing the *gateway interface index* in the header removes it and forwards the packet on the Internet. As mentioned earlier the nodes in the ad hoc network are assigned IP addresses from the same subnet thus packets from the Internet destined for nodes in the ad hoc network can reach the gateway through normal IP routing. Once the gateways receive the packets they use the DSR protocol to forward packets to the required destination.

3.2.2.3 Wireless Internet Gateways (WINGS)

In [11], the authors propose the concept of *Wireless Internet Gateways (WINGS)*, which acts as an IP router that enables connecting the ad hoc networks to the Internet and the corresponding routing protocol called *Wireless Internet Routing Protocol (WIRP)* [25]. This implementation does not support Mobile IP and is solely meant to provide Internet access to nodes in the ad hoc network. In contrast to the previous techniques discussed so far that use the standard IEEE 802.11 [15], this implementation utilizes the *Floor Acquisition Multiple Access with Non- persistent Carrier Sensing (FAMA-NCS)*

[10] as the underlying MAC protocol. The main motivation of using FAMA-NCS is that it interacts with WIRP and reduces the control traffic in the network.

WIRP and WING Operation

WIRP is a proactive protocol and hence each WING is aware of the topology of the network. They thus (WINGS) keep updating their neighbors the topology of the entire network i.e. provide the neighbor routes to all the other nodes in the network. In order to achieve this, the functionality of WIRP can be divided into the following three modules: Reliable transmission of update, neighbor discovery mechanism and its path-finding algorithm. The first component is responsible for updating the neighbors of each WING about the overall network topology. The second component causes WINGS to check connectivity with their neighbors with the aid of hello messages (similar to that discussed in Section 2.2.3) and the FAMA-NCS. The third component is responsible for finding the shortest path to the nodes in the network, which is based on the one in [25].

CHAPTER IV

TRANSPARENT AD HOC NETWORK GATEWAY

Chapter III introduced two techniques to enhance the MANET scalability exploiting mobility [12] and backbone nodes [37]. However, both techniques require radical modifications to the underlying MANET routing protocol. Chapter III also gave a brief overview of how MANETs can be integrated with the fixed infrastructure with the aid of Internet gateways thus aiming at providing Internet connectivity to MANETs. This thesis exploits this concept of infrastructured MANETs (i.e. introducing Internet gateways in MANETs) to enhance the overall performance of MANETs. To achieve this goal this chapter introduces a special gateway called ***T****ransparent* ***A****d hoc* ***N****etwork* ***G****ateway (TANG)*, which acts as a relay node and collectively forms a backbone network similar to that discussed in [37]. AODV is the MANET routing protocol used in this study. Section 4.1 introduces TANG and gives a brief explanation on the structure of TANG. The operation of TANG and its advantages are discussed in Section 4.2 and 4.3 respectively.

4.1 Transparent Ad hoc Network Gateway (TANG)

As discussed in section 3.1 a MANET has inherent scalability problem. Recently, some researchers analytically showed that it could be improved drastically by introducing infrastructured nodes into the MANET [6,22]. In this section TANGs are proposed for that purpose. A large scale MANET is divided into equal sized cells and each cell includes a TANG as seen in Figure 4.1. However such a division of the MANET into cells is completely transparent to the MANET nodes as they are not aware of the presence of these gateways in the MANET. Since the primary goal of TANG is to enhance the performance of the MANET, this thesis makes the following assumptions regarding TANG:

- The TANGs are assumed to have no power constraints.
- The bandwidth of the link over which the TANGs communicate with one another is assumed to be ideally infinite.
- The TANGs are considered to be static nodes i.e. no mobility.
- The TANGs are assumed to behave as relay nodes in the transmission of packets (data and control) and not as sinks or sources.

Implementation of TANG in a MANET does not require any modification to the underlying MANET routing protocol as mentioned earlier. The introduction of TANG into a MANET, divides the MANET into two different subnets as seen in Figure 4.1. A pure MANET resides on subnet 1 and the MANET nodes communicate with one another via their wireless interface. On subnet 2 the TANGs form a wired network thus forming a backbone network, as indicated by the solid lines in Figure 4.1. The communication

between the MANET nodes can take place via TANG or via the normal multi-hop links. However, it should be noted that TANGs operate the MANET routing protocol on both subnets as opposed to the Internet gateways (discussed in the Chapter III and seen in Figure 3.1), which uses the MANET routing protocol on one subnet and the IP protocol on the other subnet. Due to this there is no complexity concerning TANG and they can be considered normal MANET nodes with the exception of having two interfaces[1].

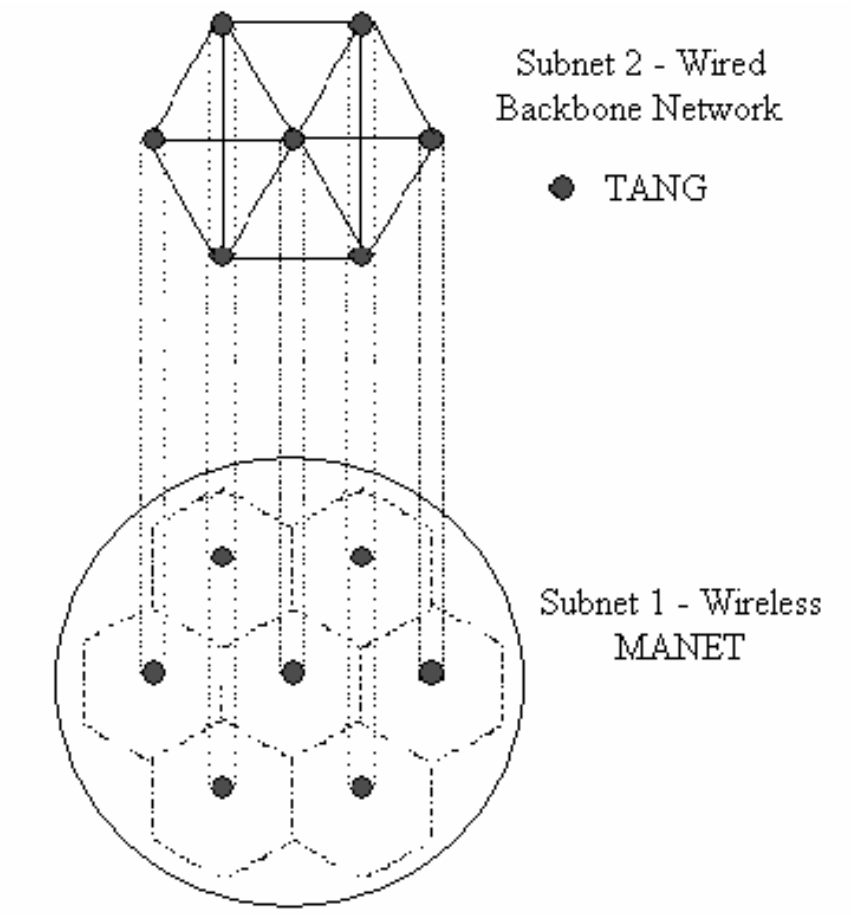


Figure 4.1. The concept of TANGs in a MANET.

[1] As mentioned earlier the routing protocol used in this implementation is AODV. This implementation of AODV follows the specification of AODV Internet Draft 9 [27]. As per this draft AODV should be able to handle multiple interfaces.

4.2 TANG *Operation*

Whenever the TANG receives an RREQ it first checks to see if it has a route for the originator of the RREQ. If not, it generates an entry in its route table, which has all the necessary information as discussed in Section 2.2.3. Along with this information it also makes a note (in its route table) of the interface on which the RREQ was received. Thus when a TANG receives an RREP for the originator of the RREQ, it will be aware of the interface on which the message is to be forwarded.

In Figure 4.2 a source node S wishing to communicate with destination node D would ideally flood the control packets in the MANET and thus one of the probable paths could be S-1-2-3-4-5-6-7-8-D (path1). Those eight nodes between the source and the destination would have to take the burden of forwarding the data packets sent by S. An alternative shorter path could be achieved with the installation of TANGs within the MANET at fixed locations. The TANGs (node C, E and G) form a backbone network designated as Subnet 2 in Figure 4.2. Thus the RREQ from the source S is received by nearest TANG (node C) and it broadcasts the request on its other interface so that the other TANGs (nodes E and G) can receive the request. Both TANGs ‘E’ and ‘G’ in turn broadcast the request and destination D would respond on receiving the request. The path now becomes S-A-B-C-E-F-D (Path 2). By the introduction of TANGs, only three mobile nodes (A, B and F) are burdened by the forwarding load of S as opposed to eight nodes (if Path 1 was used). In addition, the source node is unaware of the TANGs even though its packets are routed via them.

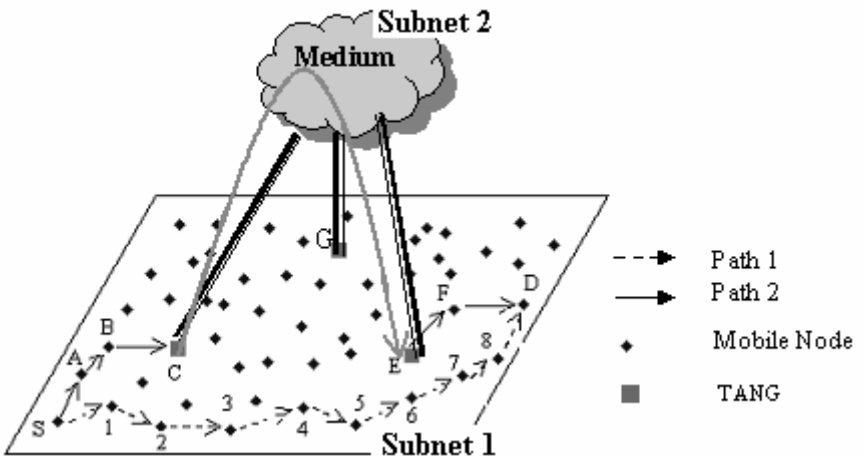


Figure 4.2. Functioning of TANG.

4.3 Advantages of TANG

The time required to do the network-wide search for a destination reduces drastically as the RREQ*s* are forwarded over the backbone link. This leads to a prompt response from the destination reducing the end-to-end delay drastically. Moreover due to the reduced path length between the source-destination the per-node throughput and the overall capacity of the MANETs increases tremendously. In a pure MANET if a source does not receive a RREP in a specified time period, the node floods the network with *duplicate* RREQs, which can be a frequent phenomenon in a large-scale MANET. This can exorbitantly affect the per-node throughput.

Node mobility in a MANET leads to link failures causing heavy data loss and triggering RERRs. Such broadcast packets (RERRs and duplicate RREQ) flood the network affecting the performance of MANETs. But in case of infrastructured MANETs with TANGs most of the routing is done via the backbone network and hence avoiding the aforementioned problems. It should however be noted that whenever the TANG

receives a broadcast message like an RREQ from the originator, the TANG is supposed to re-broadcast the message on all its interfaces except the interface on which it has received the RREQ.

Chapter V

Simulation Results and Discussion

This chapter introduces the simulation setup to evaluate the performance of the proposed infrastructured MANET using TANGs. The simulation is based on the *Qualnet Simulator* [31], which is the commercial version of *GloMoSim network simulator* [1]. A brief overview of the Qualnet simulator is given in Section 5.1. Section 5.2 discusses the simulation setup to simulate pure MANET and infrastructured MANET with TANGs. The simulation results are presented in Section 5.3 and 5.4 and emphasize on the following issues:

- Performance of infrastructured MANET as compared to pure MANET under heavy and light network load (Section 5.3).
- Relationship between the number of gateways in the network and the performance of the network (Section 5.3).

- Scalability of an infrastructured MANET with TANGs as compared to a pure MANET (Section 5.4).

According to the results presented in Section 5.3 and 5.4, the capacity of infrastructured MANET with TANGs is significantly better than that of a pure MANET.

5.1 Qualnet

5.1.1 What is Qualnet?

Qualnet is a discrete event simulator that can be used to create and animate a wide variety of experiments, graphically analyze results obtained from these experiments and even add new protocols to the simulator. Qualnet can be divided into six components, which are summarized in Table II below.

Simulations in Qualnet can be conducted either in the Qualnet Simulator or the Qualnet Animator. The Qualnet Simulator requires a configuration file in which various configuration and simulation parameters can be defined e.g. simulation time, number of nodes for which the simulation is to be conducted, terrain area, type of routing protocol to be used etc. The Qualnet Animator can be used to set the configuration parameters via the graphical interface instead of defining them in a configuration file. After the simulation is completed the simulator generates a statistics file and using the Qualnet Analyzer one can get a wide range of graphs to analyze the obtained results. Interested readers can find an elaborate explanation of all the listed components of Table II in [31].

Table II. Components of Qualnet.

Components	Function
Qualnet Animator	Conducts the design and animation of simulation experiments.
Qualnet Simulator	A network simulator tool.
Qualnet Analyzer	Produces graphs from statistics generated by the simulation experiments.
Qualnet Designer	Designing and incorporating new protocols in Qualnet.
Qualnet Tracer	Packet tracing tool.
Qualnet Importer	Network data collection tool.

5.1.2 Conducting Simulations in Qualnet

The simulations can be conducted by invoking the simulator through the command line or by using the graphical toolbar of the animator as mentioned earlier. The snapshot in the Figure 4.3 shows a MANET simulation scenario in the Qualnet Animator. The circles in the snapshot indicate the radio broadcasts range of the mobile nodes and the arrows signify the successful data packet transmission.

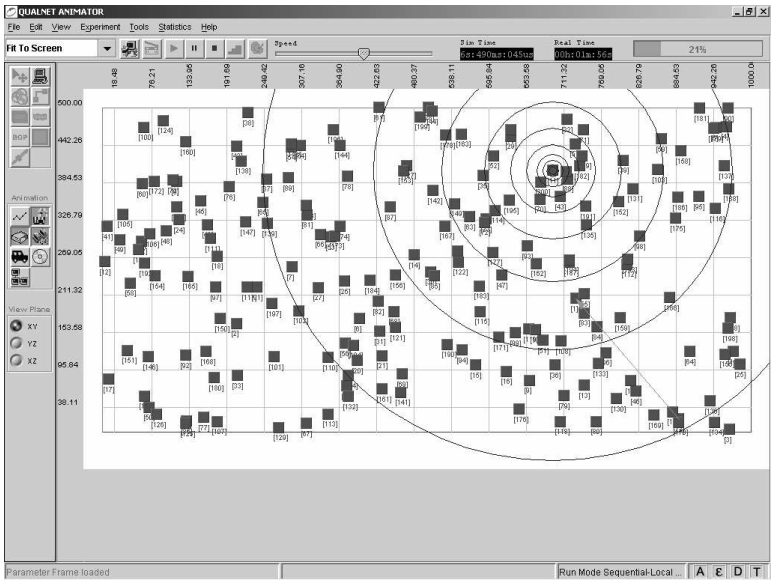


Figure 5.1. Snapshot of a MANET simulation.

5.2 Simulation Setup

As discussed above, the simulation study investigates the effectiveness of TANGs under various scenarios determined by the factors such as traffic intensity, node mobility, the number of TANGs and the number of nodes. This section discusses these simulation factors as well as performance metrics used in this thesis to assess the performance of a MANET.

Scenario

The baseline scenario consists of 100 mobile nodes randomly distributed over a rectangular area of 2200m x 600m. To see the effects of number of nodes, it is varied to 100, 200 and 500 nodes in an area of 2200m x 600m, 3200m x 900m and 5000m x 1000m respectively.

Movement Model

The mobility model used in this study is the *Random Waypoint Model* [17]. As per this model, a mobile node remains stationary for a specified pause time, after which it begins to move with a randomly chosen speed towards a randomly chosen destination within the defined topology. The node repeats the same procedure until the simulation ends. The random speed is chosen to be a value, which is uniformly distributed between a defined minimum and maximum value. The pause time and the speed used in this study are shown in this section in Table III.

Communication Model

The communication model is determined by four factors: number of sources, packet size, packet rate and the communication type. This study uses the *CBR (Constant Bit Rate)* communication type, which uses *UDP (User Datagram Protocol)* as its transport protocol. In Section 5.3, 40 sources are used to generate network traffic with a packet rate of 2 and 4 packets/sec (light and heavy network load respectively). In section 5.4, 20 CBR sources are chosen with a packet rate of 4 packets/sec. The packet size of 512 bytes was used throughout the simulation.

TANG Placement

Figure 5.2 shows the placement of 8 TANGs in a MANET. The entire area is logically divided into equal sized cells and a TANG is placed at the center of each cell. It should however be noted that the transmission range of the TANGs may not necessarily cover the entire cell, thus nodes within a particular cell could communicate via the TANG in that cell by reaching it over multi-hops or a single-hop.

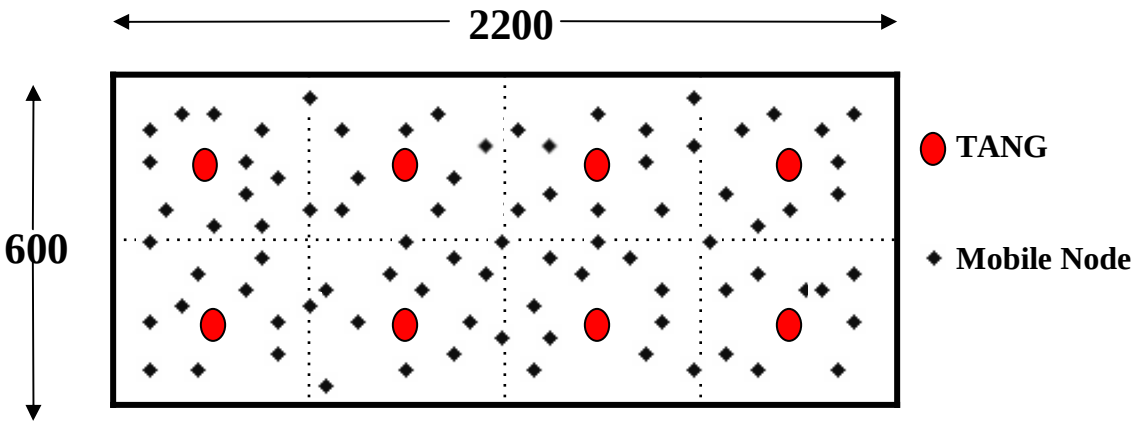


Figure 5.2. Placement of 8 TANGs in a MANET of area 2200 x 600m.

The simulation for infrastructured MANETs uses 2,6,8 and 10 TANGs with 100 mobile nodes in Section 5.3. In Section 5.4 the number of TANGs are chosen to be $\sqrt{n}$ where n is the number of nodes in the network [22].

General Simulation Parameters

Table III summarizes all the parameters that are general to all the simulations conducted in this study.

Table III. General simulation parameters.

Parameters	Values	
Radio Characteristics		
Transmission Range	250 meters	
Wireless Bandwidth	2 Mbits/sec	
Wired Characteristics		
Wired Bandwidth	100 Mbits/sec	
Number of TANGs	2,6,8 and 10 TANGs in network with 100 nodes (Section 5.3)	10,14 and 22 in a network with 100, 200 and 500 nodes respectively (Section 5.4)
Communication Model		
Traffic Type	Constant Bit Rate	
Packet Size	512 bytes	
Packet Rate	2 packets/sec and 4 packets/sec for light and heavy network load respectively (Section 5.3)	4 packets/sec (Section 5.4)
Number of Sources	40 sources (Section 5.3)	20 sources (Section 5.4)
Mobility Pattern		
Speed	0 m/s – 15 m/s	
Pause Time	0s, 100s, 200s, 300s and 400s	
Simulation Parameters		
Simulation Time	400 seconds	
Number of Nodes and network area	100 nodes in an area 2200 x 600m	100,200 and 500 nodes in an area of 2200 x 600m, 3200 x 900m and 5000 x 1000m respectively
Routing and MAC Protocols		
Routing Protocol	AODV	
MAC Protocol	802.11	

Performance Metrics

The following are the performance metrics used to evaluate the performance of a infrastructured MANET and a pure MANETs.

- Throughput – It is defined as the amount of data successfully delivered from the source to the destination in a given period of time.
- End-to-End Delay – This is defined as the time required for a packet to travel from source to destination.
- Packet Delivery Ratio – It is defined as the ratio of total data packets received at the destinations to those generated by the sources.

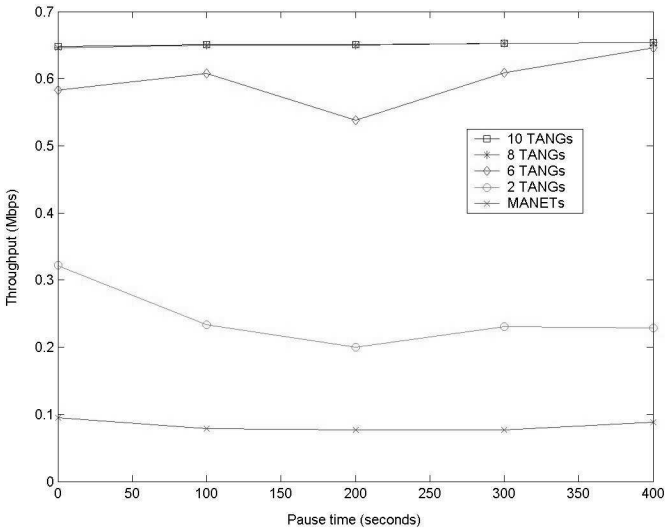
In order to understand the main causes of performance degradation, the routing-related control overhead associated with the AODV routing protocol is measured. Thus, the number of duplicate RREQ packets generated, the number of RERR packets initiated and number of data packets lost due to broken links were used in the performance evaluation.

5.3 Varying Mobility and Fixed Number of Nodes

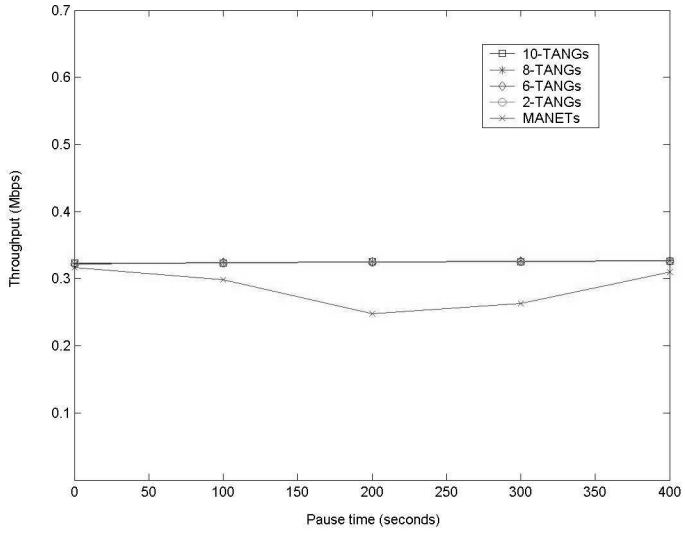
This section shows the results for all the performance metrics discussed in section 5.2. As mentioned earlier, the network consists of 100 nodes and the comparison of a pure MANET with infrastructured MANET with 2,6,8 and 10 TANGs is presented. Each data point is an average of 10 runs to remove the random measurement error.

5.3.1 Throughput

The throughput obtained for different pause times and from different scenarios of a heavily loaded network is shown in Figure 5.3(a). As seen in the graph the throughput (~0.65 Mbps) achieved from infrastructured MANETs with 8 and 10 TANGs is almost 6.5 times greater than that achieved by a pure MANET (~0.09 Mbps). Even with 2 TANGs the throughput (0.2 –0.32 Mbps) achieved is twice as much as that obtained by a pure MANET. The main reason for such low throughput in a pure MANET is, for a highly loaded network there are many transmissions and hence the nodes are burdened with forwarding the data and routing information of other mobile nodes thus decreasing the throughput drastically. But in case of infrastructured MANETs due to the backbone infrastructure the intermediate nodes are relieved of this burden and hence enhancing the throughput tremendously.



(a) Heavy network load.



(b) Light network load.

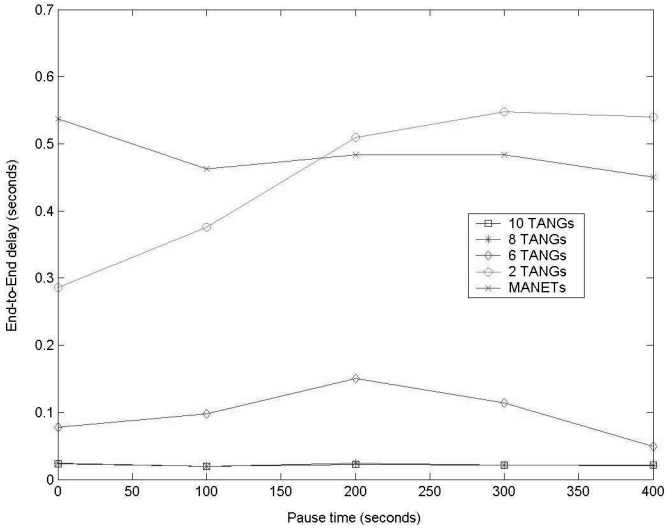
Figure 5.3. Throughput graph.

When the network load is light, in Figure 5.3(b), it can be seen that the throughput is constant for infrastructured MANETs irrespective of the number of TANGs introduced into the MANET. One important observation is that at moderate mobility (200s –300s) the performance of MANETs is degrades as seen in Figure 5.3 (a) and (b). As noted in [17] and [16] with low mobility the nodes get clustered, which leads to congestion in the network thus degrading the performance drastically.

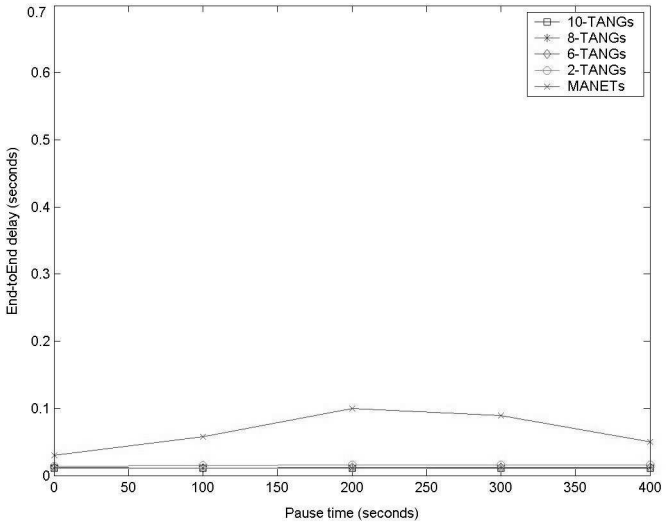
5.3.2 End-to-End Delay

Figure 5.4 (a) and (b) show the end-to-end delay comparison under heavy and light network load respectively. As seen in the Figure 5.4 (a) the delay for a infrastructured MANET with 8and 10 TANGs is almost 20 times less than that achieved by a pure

MANET and a infrastructured MANET with 2 TANGs (except at low pause times). Figure 5.4 (b) shows that the delay for infrastructured MANETs is constant as compared to that achieved by the pure MANET.



(a) Heavy Network Load.

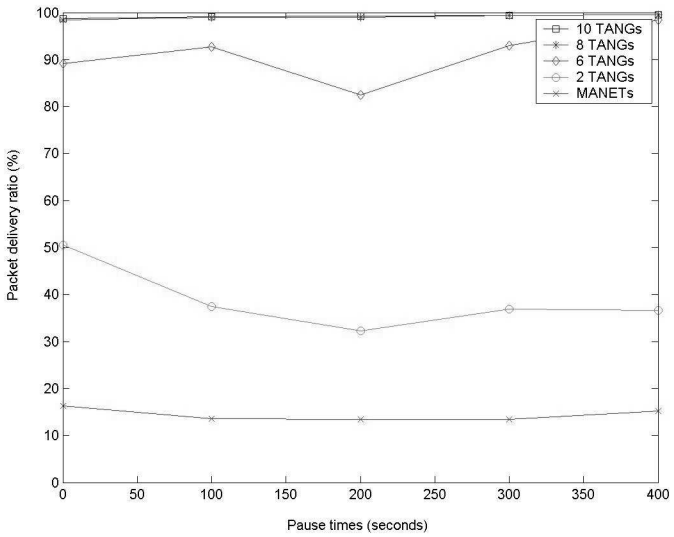


(b) Light network load.

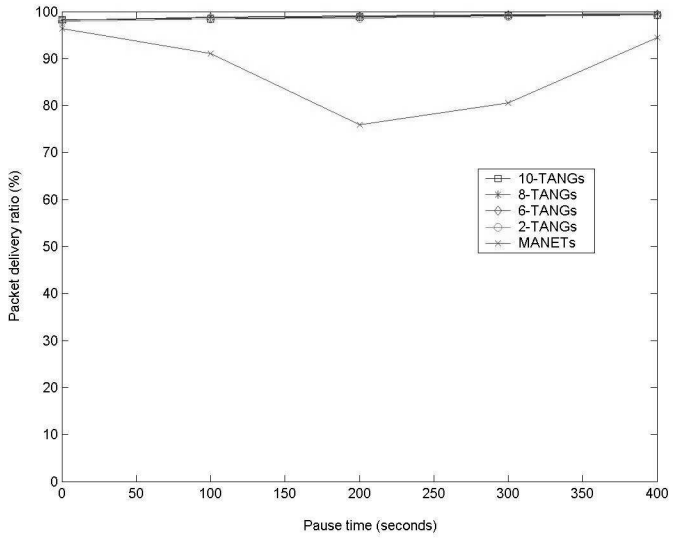
Figure 5.4 End-to-End delay graph.

5.3.3 Packet Delivery Ratio

For a heavily loaded network the infrastructured MANETs with 8 and 10 TANGs (Figure 5.5 (a) delivers almost 98% of the packets for lower pause times and almost 100% for higher pause times thus performing more than 5 times better than pure MANETs. The delivery ratio is less than 20 percent for a pure MANET indicating how a MANET fails completely under heavy network load. However as seen in the Figure 5.5 (a) infrastructured MANETs with 2 TANGs still perform twice as much as compared to pure MANETs. In case of a lightly loaded network the packet delivery ratio of infrastructured MANETs is constant (average 99%) irrespective of pause time as seen in the Figure 5.5 (b). While for a pure MANET the packet delivery ratio degrades by almost 20% for moderate pause times (200s and 300s).



(a) Heavy network load.



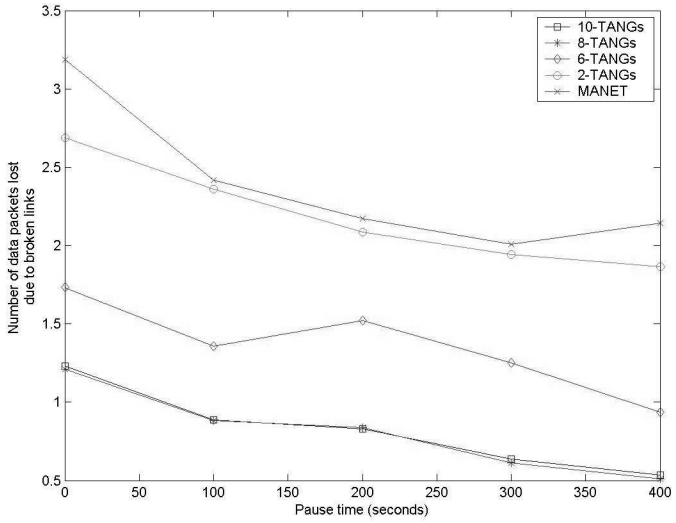
(b) Light network load.

Figure 5.5. Packet delivery ratio.

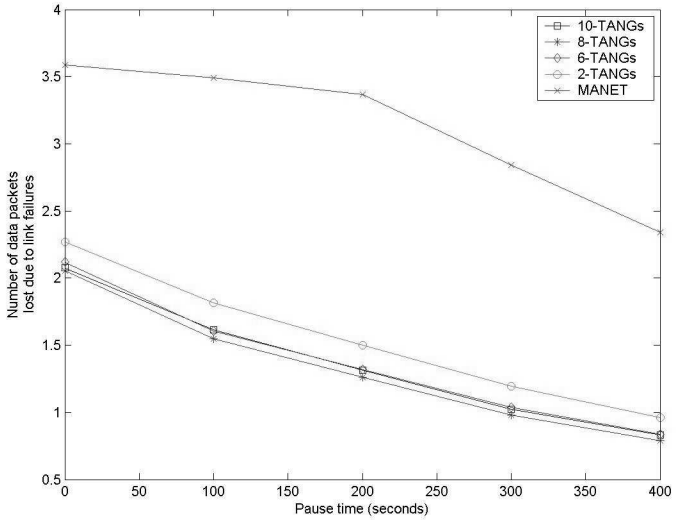
5.3.4 Data Loss, Initiated RERR and Duplicate RREQ

As seen in Figure 5.5(a) the packet delivery ratio in MANETs is very low especially at high mobility and this is mainly caused by a lot of link failures. This section shows the corresponding traffic overhead per data packet originally transmitted from source nodes. It is noted that the number of data packets generated during the simulation is 32,000 and 16,000 for heavy and light load respectively[*]. (40 sources x 4 or 2 packets/sec x 400 simulation seconds/2. The last divisor (2) is introduced because those 40 sources start their data transmission at any random instance between 0 and 400 seconds.)

[*] If there are 5 intermediate forwarding nodes on the average, total data packets transmitted amount to 160,000 and 80,000 packets respectively.



(a) Heavy network load.

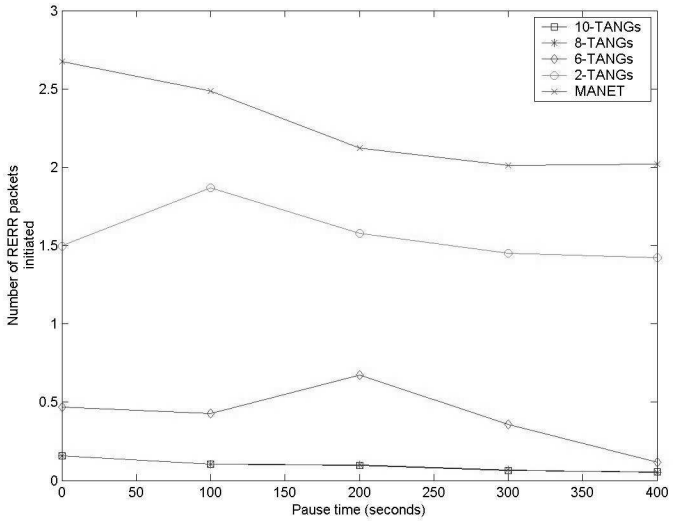


(b) Light network load.

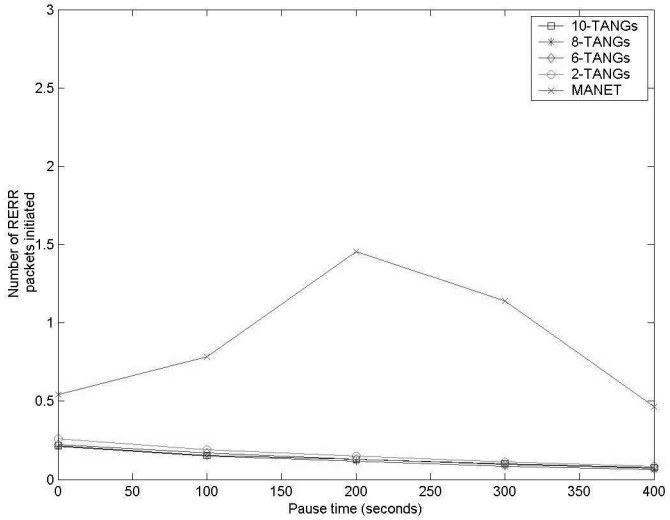
Figure 5.6. Data lost due to link failures.

Figure 5.6 (a) and (b) show the amount of data lost due to broken links for a heavily and lightly loaded network respectively. It can be seen that infrastructured MANETs with 8 and 10 TANGs (Figure 5.6 (a)) perform approximately 3 times better

than the pure MANET for lower pause times (high mobility) and approximately 4 times better for higher pause times for a network with heavy load. As seen in Figure 5.6 (b), for a lightly loaded network infrastructured MANETs loose 2 times less the number of data packets when compared to pure MANETs irrespective of the pause time.



(a) Heavy network load.

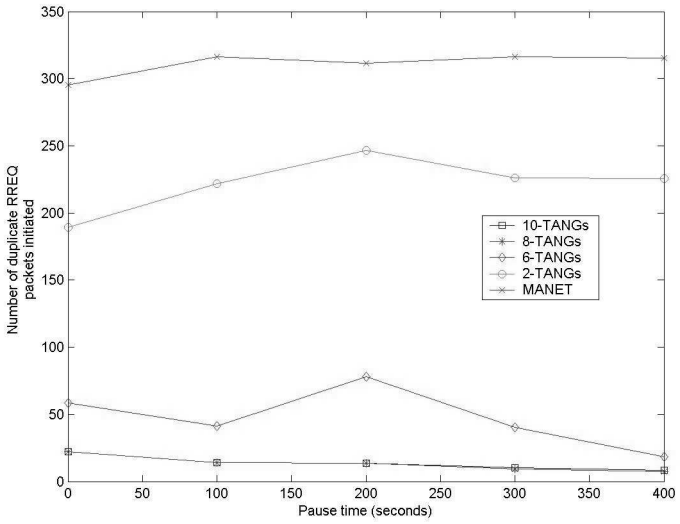


(b) Light network load.

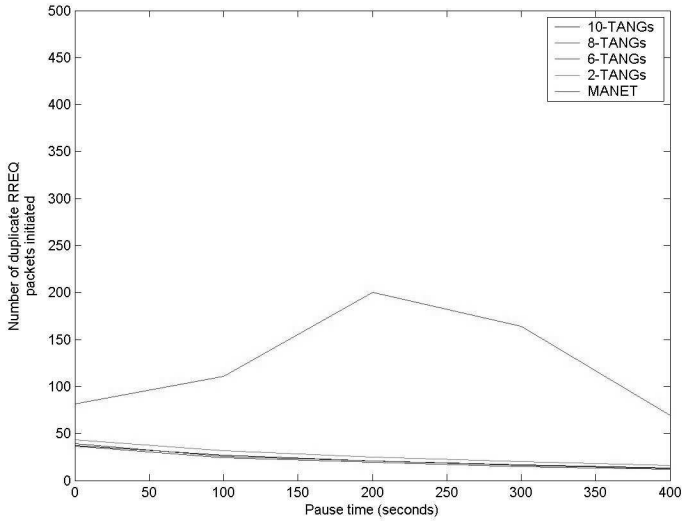
Figure 5.7. Number of initiated RERR packets.

In case of MANETs when the load in the network increases the data packet lost due to link failures is large as seen in Figure 5.6 (a) and (b) a result of which the number of RERR messages initiated by a MANET is approximately 15 times more for infrastructured MANETs with 8 and 10 TANGs irrespective of the pause time as seen in Figure 5.7 (a) for a heavily loaded network.The number of RERR packets generated by infrastructured MANETs is negligible less when compared to the pure MANET for moderate pause times (200s) for a lightly loaded network (Figure 5.7 (b)).

When the network load is heavy the sources generate a large volume of duplicate RREQ packets due to link failures. In Figure 5.8 (a) it can been seen that the number of duplicate RREQs generated in infrastructured MANETs with 6,8 and 10 TANGs is negligible when compared to pure MANETs. Infrastructured MANETs with 2 TANGs initiates twice less than the number of duplicate RREQs when compared to those initiated by MANETs for a heavily loaded network. In case of light loaded network (Figure 5.8 (b)) infrastructured MANETs perform approximately 7 times better than pure MANETs for moderate pause times (200s) and roughly 3 times better for lower and higher pause times.



(a) Heavy network load.



(b) Light network load.

Figure 5.8. Number of duplicate RREQ packets initiated.

5.4 Scalability

This part of the simulation study presents results, which prove that the scalability of infrastructured MANETs is substantially better than that of pure MANETs. The simulations were conducted for a MANET and an infrastructured MANET with network size of 100, 200 and 500 nodes. Section 5.4.1 shows results comparing an infrastructured MANET and a pure MANETs with no mobility involved, while section 5.4.2 presents results comparing infrastructured MANETs (consisting of 100,200 and 500 nodes) with mobility. Each data point is an average of 10 runs.

5.4.1 Scalability Infrastructured MANETs versus MANETs with No Mobility

As seen in the Figure 5.9 the throughput of infrastructured MANETs is constant even as the number of nodes in the network increases as opposed to that of pure MANETs. When the number of nodes is less the throughput of an infrastructured MANET and a pure MANET is comparable but with increasing number of nodes the performance of MANETs drastically reduces by almost 50%, which is less than what was expected from the previous analysis study ((1 – (1/$\sqrt{2}$)) or 30% reduction).

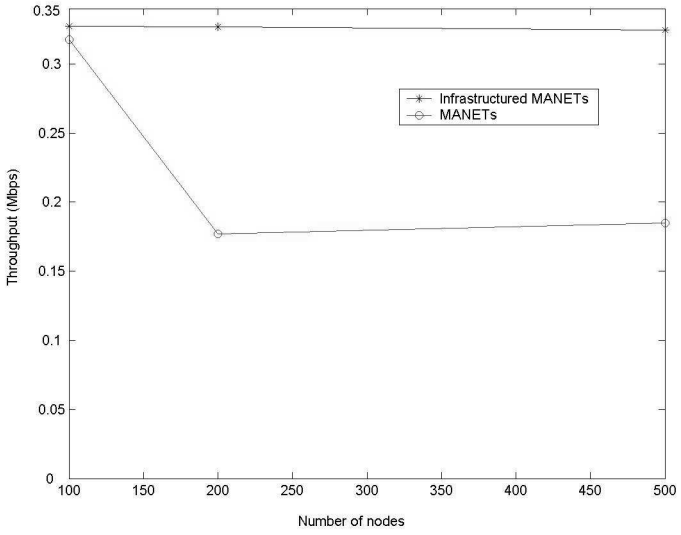


Figure 5.9. Throughput graph – No mobility.

Figure 5.10 shows how the delay in MANETs increases as the number of nodes increases. As discussed by Li et al [21] the path length increases drastically in MANETs as the network size increases leading to large delays. Therefore the delay of an infrastructured MANET is 30 times less for 200 nodes and more than 57 times less for 500 nodes when compared to a pure MANET. Figure 5.11 shows the packet delivery

ratio for infrastructured MANETs is almost constant at approximately 99% irrespective of the number of nodes, but for pure MANETs it decreases with the number of nodes and is approximately 45% less than infrastructured MANETs.

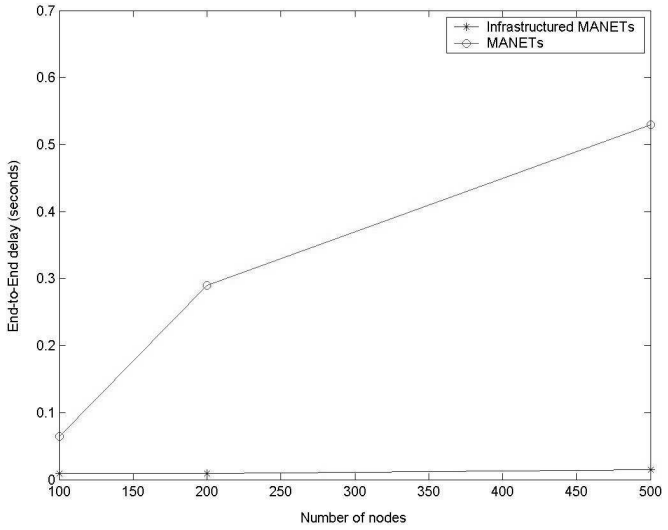


Figure 5.10. End-to-End delay graph – No mobility.

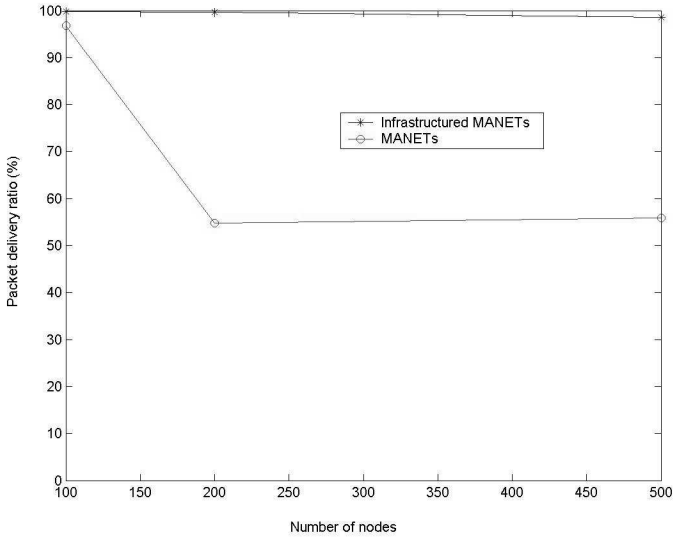


Figure 5.11 Packet delivery ratio – No mobility.

5.4.2 Scalability of Infrastructured MANETs with Varying Mobility

In this section mobility is added to the model described above. As seen in Figure 5.12 the throughput of an infrastructured MANET almost constant, ranging between 0.320 – 0.328 Mbps irrespective of the pause time and number of nodes thus proving good scalability for an infrastructured MANET.

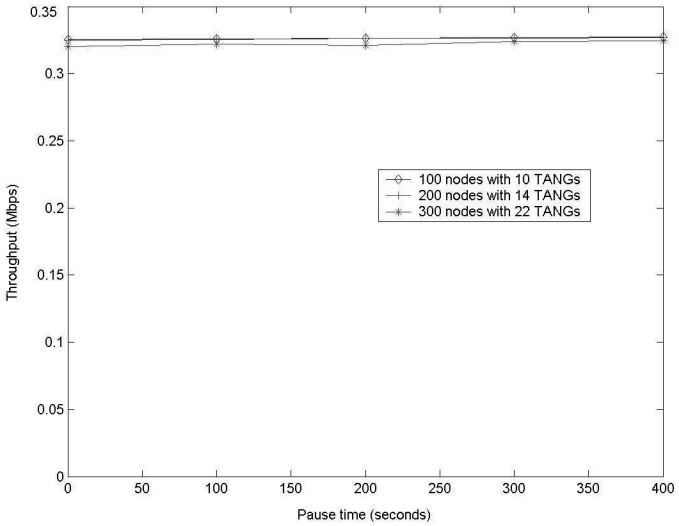


Figure 5.12. Throughput graph-Scalability

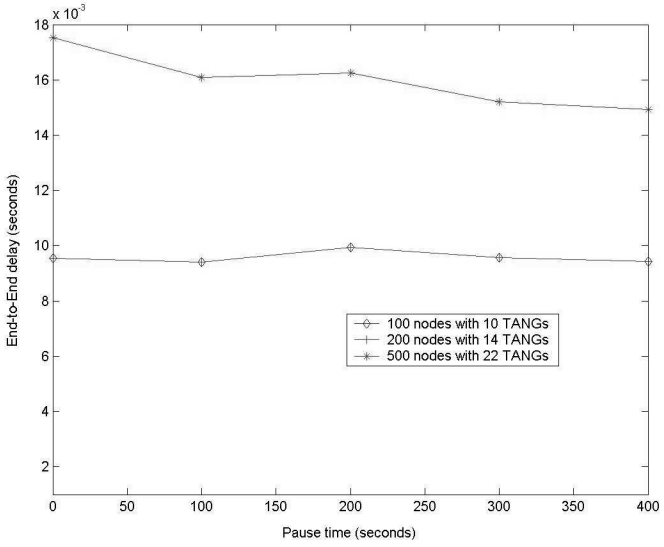


Figure 5.13. End-to-End delay graph-Scalability.

The delay (Figure 5.13) almost doubles for 500 nodes at lower pause times and is relatively high for higher pause times too when compared to 100 and 200 nodes, but is still acceptable.

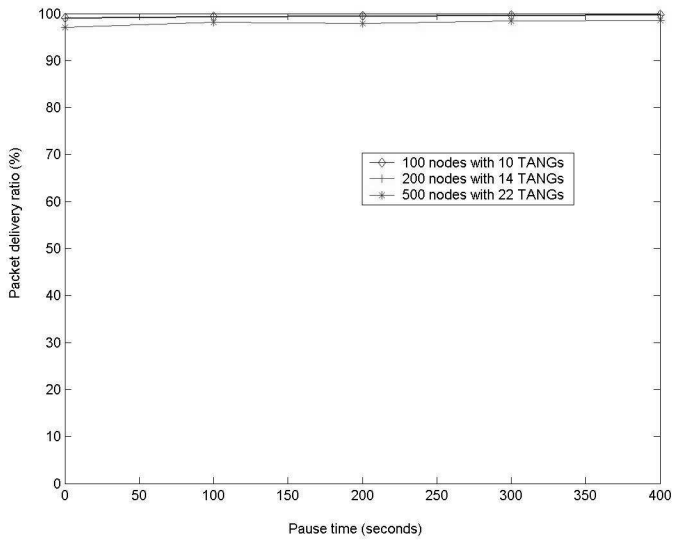


Figure 5.14. Packet delivery ratio graph-Scalability.

The packet delivery ratio for an infrastructured MANET range between 97 – 98% for 500 nodes and between 99 - 100% for 100 and 200 nodes irrespective of pause time as seen in the Figure 5.14, thus indicating good scalability.

CHAPTER VI

CONCLUSIONS

This thesis motivates the use of an infrastructured MANET as opposed to a pure MANET in order to achieve scalable network performance. A special static gateway called TANG is proposed that improves the overall performance of the network drastically. The TANGs use their short-range wireless radios to communicate with the MANET nodes and use their large bandwidth wired links to communicate among themselves, thus forming an ideally infinite backbone infrastructure. They thus take most of the responsibility in forwarding packets (data as well as routing packets). This relieves the intermediate nodes from the burden of routing, hence increasing the per node throughput drastically.

The simulation of an infrastructured MANET under heavy network congestion showed that per node throughput improves tremendously when compared to a pure

MANET. Moreover since the communication is local, the delay is almost negligible while the packet delivery ratio is very high for an infrastructured MANET with TANGs when compared to that achieved by a pure MANET. A pure MANET seems to perform quite satisfactory under light network load. This observation verifies the results of [6]. The simulations also show that at high network load due to immense competition in accessing the medium, collisions in the network increases thus a lot of link failures causes data packets to be lost in pure MANETs. This leads to broadcast of RERR and duplicate RREQ messages, which flood the network and affect the overall performance of the network.

The simulations also showed that the performance of pure MANETs degrades almost linearly with an increase in the number of nodes in the network. But in case of an infrastructured MANET the performance remains almost constant even when the number of nodes is increased. This shows that the scalability of an infrastructured MANET is far superior to that of a pure MANET. The reason for such improved performance comes form the fact that TANGs break large scale MANETs into small *virtual* MANETs and hence the communication becomes *local* (over multi-hops). In addition, the source and destination that are far apart, take advantage of the backbone networks, drastically reducing the delay.

It is evident from the results that the TANGs are not bottlenecks even when the network congestion is high. The main reason is because the nodes in the MANET are not aware of the presence of the TANGs and hence do not unicast their requests to them, thus using the shortest path to the destination, which may not necessarily be through the TANG.

Based on this study it can be concluded that introducing 8 TANGs in a MANET consisting of 100 nodes in an area of 2200 x 600m can significantly improve the scalability of a MANET and that adding more TANGs to the network does not contribute significantly. In summary, the three main issues discussed in Chapter 5 were studied and from the simulation results it can be concluded that an infrastructured MANET with TANGs increase the overall performance of the MANET immensely without requiring any modification to the underlying protocol.

BIBLIOGRAPHY

[1] L. Bajaj, M. Takai, R. Ahuja, K. Tang, R. Bagrodia and M. Gerla "GloMoSim: A Scalable Network Simulation Environment," Technical Report, UCLA Computer Science Department – 990027, 1998.

[2] E. Belding-Royer, Y. Sun and C.E. Perkins "Global Connectivity for IPv4 Mobile Ad hoc Networks," *IETF Internet Draft*, draft-royer-MANET-globalv4-00.txt, November 2001 (Work in Progress).

[3] D. Beyer, B. Nguyen "The C++ Protocol Toolkit: Overview," *Rooftop communications Technical Manual*, December 1995.

[4] J. Broch, D.B. Johnson and D. Maltz "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," IETF Internet Draft, draft-ietf-manet-dsr-01.txt, December 1998 (Work in progress).

[5] J. Broch, D. Maltz and D. Johnson "Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks," *In Proceedings of I-SPAN*, June 1999.

[6] O. Dousse, P. Thiran and M. Hasler “Connectivity in ad hoc and hybrid networks,” *In Proceedings of IEEE INFOCOM*, 2002.

[7] R. Droms “Dynamic Host Configuration Protocol”, RFC 2131, March 1997.

[8] K. Egevang and P. Francis “The IP Network Address Translator (NAT),” RFC 1631, May 1994.

[9] K. Fall and K. Varadhan Ns Manual. The VINIT Project. http://www.isi.edu/nsnam/ns/doc/.

[10] C.L. Fullmer and J.J. Garcia-Luna-Aceves “Floor acquisition multiple access (FAMA) for packet radio networks,” *In SIGCOMM*, pages 262-273, Cambridge, MA, 1995.

[11] J.J. Garcia-Luna-Aceves, C.L. Fullmer, E. Madruga, D. Beyer and T. Frivold “Wireless Internet Gateways (WINGS),” *In Proceedings of MILCOM'97*, October 1997.

[12] M. Grossglauser and D. Tse “Mobility Increases the Capacity of Ad-hoc Wireless Networks,” *In Proceedings of IEEE INFOCOM*, pages 1360-1369, 2001.

[13] P. Gupta and P.R. Kumar “The Capacity of Wireless Networks,” *IEEE Transactions on Information Theory*, Vol. 46, No. 2, pages 388-404, March 2000.

[14] C. Hedrick “Routing Information Protocol,” IETF RFC 1058, June 1988.

[15] IEEE Computer Society LAN MAN Standards Committee. “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” *IEEE Standard 802.11*, New York, NY, 1997.

[16] P. Johansson, T. Larsson, N. Hedman and B. Mielczarek “Routing protocols for mobile ad-hoc networks – a comparative performance analysis,” *In Proceedings*

of the 5th International Conference on Mobile Computing and Networking (ACM MOBICOM '99), pages 195-206,August 1999.

[17] D.B. Johnson and D. Maltz. "Dynamic Source Routing in Ad-Hoc Wireless Networks," *In Proceedings of Mobile Computing*, edited by T. Imielinski and H. Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[18] U. Jonsson, F. Alriksson, T. Larsson, P. Johansson and G. Maguire "MIPMANET - mobile IP for mobile ad-hoc networks," *In Proceedings of Workshop on Mobile Ad Hoc Networking (MobiHOC'00)*, Boston, MA, August 2000.

[19] J. Jubin and J.D. Tornow "The DARPA Packet Radio Network Protocols," *In Proceedings of the IEEE*, pages 21-32, Vol. 75, No. 1, January 1987.

[20] H. Lei and C.E. Perkins "Ad Hoc Networking with Mobile IP," *In Proceedings of EPMCC*, 1997.

[21] J. Li, C. Blake, D.S.J. De Couto, H.I. Lee and R. Morris "Capacity of ad hoc wireless networks," *MOBICOM*, pages 61–69, 2001.

[22] B. Liu, Z. Liu and D. Towsley "On the Capacity of Hybrid Wireless Networks". *In Proceedings of IEEE Infocom'03*, San Francisco, CA, April, 2003.

[23] MANET Working Group within the Internet Engineering Task Force (IETF) Webpage, http://www.ietf.org/html.charters/manet-charter.html.

[24] G. Montenegro, ed. "Reverse Tunneling for Mobile IP, revised," RFC 3024, January 2001.

[25] S. Murthy and J.J. Garcia-Luna-Aceves "An Efficient Routing Protocol for Wireless Networks," *ACM Mobile Networks and Applications Journal*, Special issue on Routing in Mobile Communication Networks, Vol. 1, No. 2, 1996.

[26] C.E. Perkins, E. Belding-Royer, S. Das and M. Marina "Performance of two on-demand Routing Protocols for Ad-hoc Networks," *In Proceedings of IEEE Personal Communications*, pages 16-28, February 2001.

[27] C.E. Perkins, E. Belding-Royer and S. Das "Ad Hoc On Demand Distance Vector (AODV) Routing," *IETF Internet draft*, draft-ietf-manet-aodv-13.txt, February 2003 (Work in Progress).

[28] C.E. Perkins, J.T. Malinen, R. Wakikawa, E. Belding-Royer and Y. Sun "Ad hoc Address Autoconfiguration," *IETF Internet Draft*, draft-ietf-manet-autoconf-01.txt, November 2001 (Work in Progress).

[29] C.E. Perkins and P. Bhagwat "Highly Dynamic Destination Sequenced Distance-Vector Routing for Mobile Computers," *In Proceedings of the SIGCOMM Conference on Communication Architecture, Protocols and Appilcations*, pages 234-244, August 1994.

[30] C.E. Perkins, ed., "IP Mobility Support," *IETF Request For Comments*, 2002.

[31] "*QualNet User's Manual, version 3.6,"* Scalable Network Technologies, Inc. 2003.

[32] R. Ramanujan , S. Takkella, J. Bonney and K. Thurber "Source-Initiated Adaptive Routing Algorithm (SARA) for Autonomous Wireless Local Area Networks," *In Proceedings of the 23rd IEEE Conference on Computer Networks*, October 1998.

[33] A. Striegel, R. Ramanujan and J. Bonney "A Protocol Independent Internet Gateway for Ad Hoc Wireless Networks," *In Proceedings of Local Computer Networks (LCN) 2001*, Tampa, FL, November 2001.

[34] Y. Sun, E. Belding-Royer and C.E. Perkins "Internet Connectivity for Ad hoc Mobile Networks," *International Journal of Wireless Information Networks special issues on Mobile Ad hoc Networks*, Vol. 9, No. 2, April 2002.

[35] S. Toumpis and A. Goldsmith "Ad hoc network capacity," *Conference Record of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers*, pages 1265 -1269 vol.2, 2000.

[36] Y. Tseng, C. Shen and W. Chen "Integrating Mobile IP with Ad Hoc Networks," *IEEE Computer* Vol. 36, No. 5, pages 48-55, 2003.

[37] K. Xu and M. Gerla "A heterogeneous routing protocol based on a new stable clustering scheme," *In Proceedings of MILCOM*, Anaheim, CA, October 2002.

ACRONYMS

AODV	Ad hoc On-Demand Distance Vector
AREP	Address REPly
AREQ	Address REQuest
CG	Cluster Gateway
COA	Care-Of-Address
DAD	Duplicate Address Detection
DARPA	Defense Advanced Research Projects Agency
DHCP	Dynamic Host Configuration Protocol
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
FA	Foreign Agent
FAMA-NCS	Floor Acquisition Multiple Access with Non-persistent Carrier Sensing
HA	Home Agent
IEEE	Institute of Electrical and Electronics Engineers

IP	Internet Protocol
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
MIP	Mobile IP
MIPMANET	Mobile IP for Mobile Ad hoc Networks
MIWU	MIPMANET Internetworking Unit
MN	Mobile Node
NAT	Network Address Translation
ns-2	Network Simulator-2
PHY	PHYsical
RERR	Route ERRor
RIP	Routing Information Protocol
RREP	Route REPly
RREQ	Route REQuest
SAP	Service Access Point
SARA	Source-Initiated Adaptive Routing Algorithm
TANG	Transparent Ad hoc Network Gateway
TCP	Transport Control Protocol
UDP	User Datagram Protocol
Wi-Fi	Wireless Fidelity
WINGS	Wireless Internet Gateways
WIRP	Wireless Internet Routing Protocol