Design And Evaluation Of MANETs Connected To Internet

- Assistant Lecturer: Ahmed Abdulhadi Ahmed[1], ahmedh1333@yahoo.com
- Assistant Lecturer: Haider Galil Al-Qurabi[1], haidergalil@yahoo.com
- Assistant Engineer: Ali Abdulhussien Hassan[1], lia_ali2001@yahoo.com

1. University of Karbala-College of Engineering/Dept. of Electrical and Electronic Eng

Abstract

The Transmission Control Protocol (TCP) was designed to provide reliable end-to-end delivery of data over unreliable networks. In practice, most TCP deployments have been carefully designed in the context of wired networks. Ignoring the properties of wireless ad-hoc networks can lead to TCP implementations with poor performance. A mobile ad-hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies.

In this paper, two MANET (Mobile Ad-hoc NETwork) networks are connected across an IP-Based internet network. The MANET is connected to the IP network through a MANET gateway that is running a MANET routing protocol and an IP routing protocol (or static routing) on one of its interfaces. A MANET gateway is any wireless LAN router that has its MANET Gateway attribute enabled. The MANET routing protocol that used is AODV(Ad-hoc On Demand Distance vector) and the TCP variants that used is Taho, Reno and NewReno and the number of mobile nodes will be 3, 5, and 7 for each scenario that used in the simulation.

After running the simulation, the results showed that the max throughput was in the scenario that has 5 nodes. This means that when increase the number of nodes above 5, the throughput will decrease.

The simulation environment is designed and modeled and the result is collected under the powerful network simulation tool that called OPNET Modeler 14.

Key words: *TCP, MANET, AODV, Taho, Reno, NewReno, IP-Based Network.*

الملخص

في هذا البحث يوجد شبكتان من نوع MANET تربط عن طريق شبكة المعلومات الدولية المعتمدة على الـ IP. شبكة الـ MANET تربط الى الانترنيت بواسطة بوابة الـ MANET و هذه البوابة تشغل بروتوكولات التوجيه و بروتوكولات توجيه العنوانين. و ان نوع بروتوكولات التوجيه الخاصة بالـ MANET هو AODV و ان انواع بروتوكولات الـ TCP المستخدمة هي Taho و NewReno و ان عدد الاجهزة النقالة المستخدمة في هذا البحث كان 3 , 5 , 7 لكل سيناريو.

بعد تشغيل المحاكاة لهذا البحث تبين بأن اكبر مقدار للنواتج كان بالسيناريو الذي يملك 5 من الاجهزة النقالة, و هذا يعني عند زيادة عدد الاجهزة النقالة فوق 5 هذا يؤدي الى تقليل النواتج.

ان بيئة المحاكاة قد صممت و نمذجت و النواتج قد جمعت بواسطة اداة محاكاة الشبكات القوية و يسمى OPNET Modeler 14.

1. Introduction

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad-hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multihop topologies which are likely composed of relatively bandwidth-constrained wireless links. Within the Internet community, routing support for mobile hosts is presently being formulated as "mobile IP" technology. This is a technology to support nomadic host "roaming", where a roaming host may be connected through various means to the Internet other than its well known fixed-address domain space. The host may be directly physically connected to the fixed network on a foreign subnet, or be connected via a wireless link, dial-up line, etc. Supporting this form of host mobility (or nomadicity) requires address management, protocol interoperability enhancements and the like, but core network functions such as hop-by-hop routing still presently rely upon pre- existing routing protocols operating within the fixed network. In contrast, the goal of mobile ad-hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes--which may be combined routers and hosts themselves form the network routing infrastructure in an ad-hoc fashion [1].

Ad-hoc networks are complex distributed systems that consist of wireless mobile or static nodes that can freely and dynamically self-organize. In this way they form arbitrary, and temporary, “ad-hoc” network topologies, allowing devices to seamlessly interconnect in areas with no pre-existing infrastructure. Recently, the protocols such as Bluetooth, IEEE 802.11, and Hyperlan are making possible the deployment of ad-hoc networks for commercial purposes. As a result, considerable research efforts have been made in this new challenging wireless environment [2].

This paper consist of seven sections that describe the overall work done in this paper. Section 2 describes the wireless ad-hoc networks while section 3 explains the ad-hoc routing protocols that are necessary for computers or mobile nodes to communicate with each other. Section 4 describes the performance of TCP protocol over ad-hoc networks and provides the main types of wireless networks. Section 5 shows the way of how connect MANET to IP networks. Section 6 explains the practical part of the paper and the network model that used to test and extract the results from the network settings. Section 7 gives the main conclusions of this paper.

2. Wireless Ad-hoc Networks [4]

A wireless ad-hoc network is a collection of mobile/semi-mobile nodes with no pre-established infrastructure, forming a temporary network. Each of the nodes has a wireless interface and communicates with each other over either radio or infrared. Laptop computers and personal digital assistants that communicate directly with each other are some examples of nodes in an ad-hoc network. Nodes in the ad-hoc network are often mobile, but can also consist of stationary nodes, such as access points to the Internet. Semi mobile nodes can be used to deploy relay points in areas where relay points might be needed temporarily. Figure (1) shows a simple ad-hoc network with three nodes. The outermost nodes are not within transmitter range of each other. However the middle node can be used to forward packets between the outermost nodes. The middle node is acting as a router and the three nodes have formed an ad-hoc network.

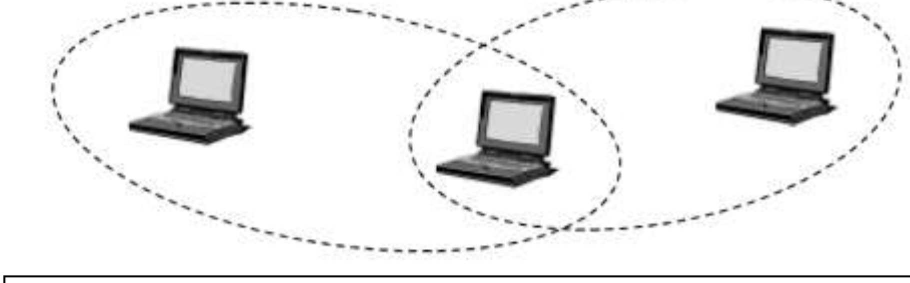

Figure 1: Example of a simple ad-hoc network with three participating nodes.

An ad-hoc network uses no centralized administration. This is to be sure that the network wont collapse just because one of the mobile nodes moves out of transmitter range of the others. Nodes should be able to enter/leave the network as they wish. Because of the limited transmitter range of the nodes, multiple hops may be needed to reach other nodes. Every node wishing to participate in an ad-hoc network must be willing to forward packets for other nodes. Thus every node acts both as a host and as a router. A node can be viewed as an abstract entity consisting of a router and a set of affiliated mobile hosts (Figure 2).

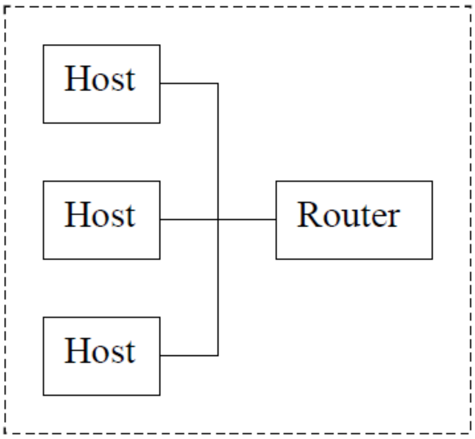

Figure 2: Block diagram of a mobile node acting both as hosts and as router.

A router is an entity, which, among other things runs a routing protocol. A mobile host is simply an IP-addressable host/entity in the traditional sense. Ad-hoc networks are also capable of handling topology changes and malfunctions in nodes. It is fixed through network reconfiguration. For instance, if a node leaves the network and causes link breakages, affected nodes can easily request new routes and the problem will be solved. This will slightly increase the delay, but the network will still be operational. Wireless ad-hoc networks take advantage of the nature of the wireless communication medium. In other words, in a wired network the physical cabling is done a priori restricting the connection topology of the nodes. This restriction is not present in the wireless domain and, provided that two nodes are within transmitter range of each other, an instantaneous link between them may form.

3. Ad-hoc Routing Protocols

Route means the way and protocol is the set of rules through which two or more devices (computers, mobile nodes) are communicating with each others. Routes are multi hop in ad-hoc networks because the propagation range (250 meters in an open field) of wireless radio is limited. Nodes travel freely and randomly in the network and routes are often find connection or disconnection. Establishing strong routes, maintaining and reconstruction in time are the main task for routing protocols. All the above responsibilities are performed by the routing protocol, except generating excessive control message overhead. Data packets send efficiently must be utilized by control packets and be generated only when needed. Routing protocol efficiency in bandwidth and energy consumption could be made by reducing the control overhead [5].

There are several ad-hoc routing protocols such as;

1. **Ad-hoc On Demand Distance vector (AODV) [6]**

   The ad-hoc On-Demand Distance Vector (AODV) routing protocol enables multi-hop routing between participating mobile nodes wishing to establish and maintain an ad-hoc network. AODV is based upon the distance vector algorithm. The difference is that AODV is reactive, as opposed to proactive protocols like DV, i.e. AODV only requests a route when needed and does not require nodes to maintain routes to destinations that are not actively used in communications. As long as the endpoints of a communication connection have valid routes to each other, AODV does not play any role. AODV needs to keep track of the following information for each route table entry:

- Destination IP Address: IP address for the destination node.
- Destination Sequence Number: Sequence number for this destination.
- Hop Count: Number of hops to the destination.
- Next Hop: The neighbor, which has been designated to forward packets to the destination for this route entry.
- Lifetime: The time for which the route is considered valid.
- Active neighbor list: Neighbor nodes that are actively using this route entry.
- Request buffer: Makes sure that a request is only processed once.

The advantage with AODV compared to classical routing protocols like distance vector and link-state is that AODV has greatly reduced the number of routing messages in the network. AODV achieves this by using a reactive approach. This is probably necessary in an ad-hoc network to get reasonably performance when the topology is changing often. AODV is also routing in the more traditional sense compared to for instance source routing based proposals like DSR. The advantage with a more traditional routing protocol in an ad-hoc network is that connections from the ad-hoc network to a wired network like the Internet is most likely easier. The sequence numbers that AODV uses represents the freshness of a route and is increased when something happens in the surrounding area. The sequence prevents loops from being formed, but can however also be the cause for new problems. What happens for instance when the sequence numbers no longer are synchronized in the network? This can happen when the network becomes partitioned, or the sequence numbers wrap around. AODV only support one route for each destination. It should however be fairly easy to modify AODV, so that it supports several routes per destination. Instead of requesting a new route when an old route becomes invalid, the next stored route to that destination could be tried. The probability for that route to still be valid should be rather high.

2. Dynamic Source Routing (DSR)

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad-hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad-hoc network. The use of source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSR to scale automatically to only that needed to react to changes in the routes currently in use [7].

Route discovery: The source starts a route discovery when sending data packet to the destination but have no routing information. To set up a route, the source floods RREQs message with a distinctive request ID. When the destination receives this request message or a node which has destination route information then it transmits RREP message back to the source with route information. Figure 3 shows route discovery of DSR. Node 2 is the initiator and node 9 is the target [5].

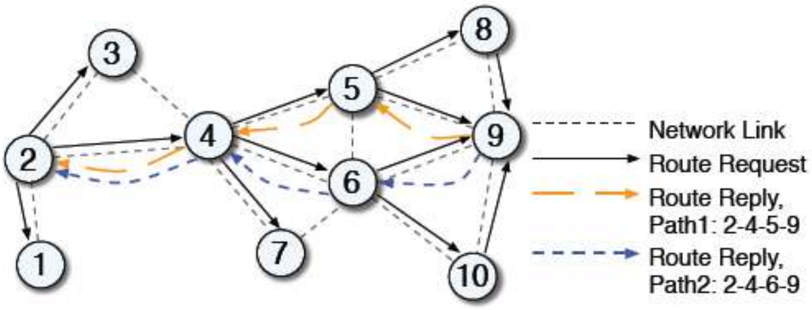

Figure 3: Route discovery for target node

Route Maintenance: In LAN routing the main improvement of DSR is in route maintenance and monitoring in the attendance of mobility. DSR based on the acknowledgments of data packets sent to adjacent nodes to monitors the validity of existing routes. This monitoring is achieved by inactively listening for communication of the adjacent to the next hop or sitting a bit in a packet to ask for open acknowledgment. The RERRs packet is sent to the creative sender to raise a new route discovery stage when a node fails to accept an acknowledgment. Nodes receive a REERs message remove any route entry (from their route cache) which uses the out of order link. When a node has problem transferring packet during that link then REER message is propagated. So this selective transmission reduces control overhead (if no packets pass through a link), it yields a long delay when a packet wants to go through a new link. Node 9 cannot be reached by node 6 anymore and a REER is returned to node 2. DSR main advantages are that it reduce routing overhead and does not need to discover routes to all the nodes in the network. The disadvantage of DSR is low mobility and static networks. Its performance is reduced by high mobility [5].

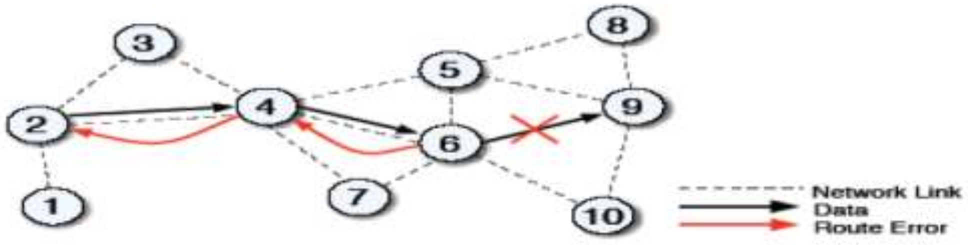

Figure 4: Maintenance for Error Route

3. Temporally-Ordered Routing Algorithm (TORA) [8]

Temporally Ordered Routing Algorithm (TORA) is a distributed routing protocol. The basic underlying algorithm is one in a family referred to as link reversal algorithms. TORA is designed to minimize reaction to topological changes. A key concept in its design is that control messages are typically localized to a very small set of nodes. It guarantees that all routes are loop-free (temporary loops may form), and typically provides multiple routes for any source/destination pair. It provides only the routing mechanism and depends on Internet MANET Encapsulation Protocol for other underlying functions. TORA can be separated into three basic functions: creating routes, maintaining routes, and erasing routes. The creation of routes basically assigns directions to links in an undirected network or portion of the network, building a directed acyclic graph (DAG) rooted at the destination (See Figure 5).

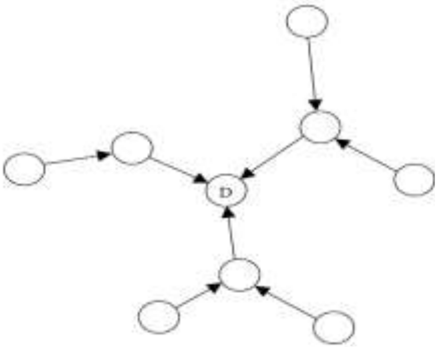

Figure 5: Directed acyclic graph rooted at destination.

4. TCP Performance Over Ad-hoc Networks

The distinguishing feature of wireless networks is that packets (or segments) are transmitted with the presence of wireless links. In wireline networks, two devices can communicate directly only when there is a wired link connecting them. In other words, a device can send messages in a wireless network via the wireless medium, air, to another device provided that the receiver is within the transmission range of the sender. This adds flexibility to how a wireless network is formed and structured. Besides, it supports device mobility. There are two major types of wireless networks, namely, the infrastructured networks and the ad-hoc networks [9].

Infrastructured Networks: An infrastructured network is one with planned, permanent network device installations. It can be set up with a fixed topology, to which a wireless host can connect via a fixed point, known as a base station or an access point. The latter is connected to the backbone network, often via a wired link. Cellular networks and most of the wireless local area networks (WLANs) operate as the static infrastructured networks. All wireless hosts within the transmission coverage of the base station can connect to it and use it to communicate with the backbone network. This means that all communications initiated from or destined to a wireless host have to pass through the base station to which the host connects directly [9,10].

Ad-Hoc Networks :An ad-hoc network, such as a packet radio network, is one without a fixed topology. A wireless host can freely communicate with another host directly whenever the receiver is in its transmission coverage. If a wireless host would like to send messages to another host which is not in the coverage region, it will first relay them to a host in its transmission range. The host functions as a relay to forward the messages on its way to the destination. The major advantage of this configuration is flexibility. An ad-hoc network can be built easily, without the need of any preset, fixed infrastructure. In addition, an ad-hoc network is generally more robust than an infrastructured network as it does not have any critical device to maintain the network connectivity. In other words, it is unlikely an ad-hoc network will be partitioned due to the failure of a wireless host, but the malfunction of a base station may partition an infrastructured network, blocking the communication between all wireless hosts connecting to the failed base station and all other hosts in the network. However, there are some drawbacks for ad-hoc networks. First, it is much more difficult and complex to perform routing in ad-hoc networks because of frequent changes in the network topology due to host mobility. Second, it is more difficult to control or coordinate proper operation of an ad-hoc network, since each wireless host may have its own algorithms to perform activities such as time synchronization, power management, and packet scheduling. In an infrastructured network, these algorithms are often implemented in and thus harmonized by the base stations or access points [10].

4.1 Characteristics of Wireless Networks [10]

There are four major characteristics of wireless networks: channel contention, signal fading, mobility, and limited power and energy.

i. ***Channel Contention*** : In a wireless network, signals are broadcast and may interfere with each other. A collision will be sensed and transmissions may fail when there exists concurrent transmissions within the interference range of either sender. Thus, a medium access protocol is needed to coordinate the transmission accesses of the wireless channel so as to achieve a reasonably high channel utilization and goodput.

ii. ***Signal Fading*** : Unlike wired media, signals transmitted over a wireless medium may be distorted or weakened because they are propagated over an open, unprotected, and everchanging medium with irregular boundary. Besides, the same signal may disperse and travel on different paths due to reflection, diffraction, and scattering caused by obstacles before it arrives at the receiver.

iii. ***Mobility:*** Without the constraints imposed by the wired connections among devices, all devices in a wireless network are free to move. To support mobility, an ongoing connection should be kept alive as a user roams around. In an infrastructured network, a handoff occurs when a mobile host moves from the coverage of a base station or access point to that of another one. A protocol is therefore required to ensure seamless transition during a handoff. This includes deciding when a handoff should occur and how data is routed during the handoff process. In some occasions, packets are lost during a handoff.

iv. ***Limited Power and Energy*** : A mobile device is generally handy, small in size, and dedicated to perform a certain set of functions; its power source may not be able to deliver power as much as the one installed in a fixed device. When a device is allowed to move freely, it would generally be hard to receive a continuous supply of power.

4.2 **Problems for TCP [11,12]**

The congestion control mechanisms of TCP have been designed with the assumption that all segment losses are congestive losses. Due to the specific characteristics of wireless networks, TCP suffers poor performance because of noncongestive segment loss (including random loss and burst loss) and packet reordering.

Random Loss — The traditional congestion control measures for TCP has been designed for the wired network environment. The segment loss rate due to bit corruption and link errors is nearly negligible. In other words, almost all segment losses are congestive losses in wired networks. Indeed, the TCP congestion control mechanisms are generally reactive. When the loss of a data segment is inferred, network congestion is postulated. The size of the congestion window is reduced to assist in alleviating the congestion. Unfortunately, in a wireless network, the loss of a data segment does not necessarily correspond to network congestion because it may be dropped due to signal fading. It is typical to have a one percent to two percent random loss rate. With the misinterpretation of the nature of segment loss, the congestion control mechanisms react inappropriately by keeping the sending rate of a TCP connection small and some data segments are retransmitted spuriously. This leads to inferior performance.

Burst Loss — A burst loss event may be initiated by signal fading. Prolonged uncontrollable channel interferences can lead to correlated packet losses. Yet, it generally occurs over a very short duration, leading to a loss of several consecutive segments at a time. In an infrastructured network, all incoming and outgoing communications for a mobile host are routed via the base station it connects to. When it moves away from the coverage area of the base station, it needs to register at another base station in whose coverage area it moves. All subsequent communications are then routed via the new base station and the
handoff process is completed.

Packet Reordering — Packet reordering refers to the network behavior where the receiving order of a flow of packets differs from its sending order. Recent studies show that packet reordering is not a rare event. The presence of persistent and substantial packet reordering violates the inorder or near in-order channel assumption made in the design of some traffic control mechanisms in TCP.

4.3 Variants of TCP

After the introduction of first version of TCP several different flavors exist, the most famous implementation of TCP called Tahoe, Reno, New Reno.

1. **Tahoe:** In the first version of TCP there was no congestion control mechanism. So after observing the congestion collapses 1988 Jacobson introduced several Congestion Control algorithms and this version is called TCP-Tahoe. The congestion control algorithms introduced in this version are: [13]
   a) Slow start
   b) Congestion Avoidance
   c) Fast Retransmit
2. **Reno:** The fast retransmit phase was first introduced in TCP-Tahoe followed by Slow Start. But TCP-Reno also added the algorithm of Fast Recovery, so that Fast Recovery dictates the sender to perform congestion avoidance directly after fast retransmission rather than immediately reducing the data flow using slow start mechanism [13].
3. **New Reno:** TCP Reno recovers only one lost packet during the recovery process. So TCP-New Reno is just adding the capability to TCP Reno to deals with multiple packets losses to recovery in a single transmission window [14].

5. Connecting MANET To IP Network [15]

The characteristics of an ad-hoc network differ substantially from those of the fixed Internet. Connecting an ad-hoc network to the Internet brings up several issues, especially when using an on-demand approach for routing in the ad-hoc network. For a stand-alone ad-hoc network, the issue concerning addressing is to see that each address is only assigned to one node. When the ad-hoc network is connected to the internet it needs IP addresses that are valid on the rest of the Internet as well.

5.1 IP Routing

Addressing on the Internet is hierarchical with IP addresses divided into a network ID and a host ID as depicted in Figure 6. All hosts on a certain network use the same network ID. In this way, each IP address is mapped to a physical location that can be derived by looking at the network ID of the IP address. This also means that an Internet host does not have to keep track of routes to every other Internet host. Instead, routing information can be aggregated; one entry in the routing table can handle all hosts that share the same network ID. To make better use of the address space yet another level of hierarchy is used; a network can be divided into subnetworks. The host ID is then divided into a subnet ID and a host ID as shown in Figure 7. Instead of having 2 hosts in a single network, the address space can be divided into 2 subnets with 2 hosts in each subnet. This extra level of hierarchy is only visible within the network, a host in another network can still use one route to reach all subnets that use the same network ID.

The number of networks in the Internet is quite substantial and it is not always necessary to keep track of them all, since they only have limited interconnections. Because most networks are leaf networks, default routes are widely used.

In principle, IP routing works as follows;

1. Look for an entry in the routing table that matches the complete destination IP address. If found, use that route.
2. Look for an entry in the routing table that matches just the network ID of the destination IP address. If found, use that route.
3. Look for a default entry in the routing table. If found use that route. Otherwise consider the destination unreachable.

The ability to use one route to an entire network instead of having one route per host and the ability to use a default route are two powerful features of IP routing.

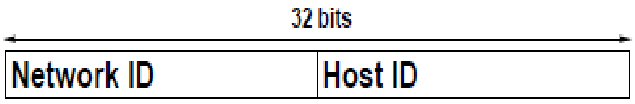

Figure 6 An IP Address

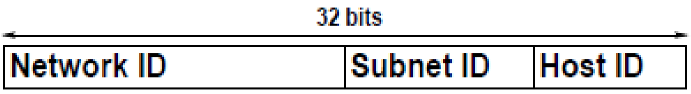

Figure 7 An IP Address with Subnet ID

5.2 MANET Routing in IP Network

In order to make ad-hoc network to be routable from the Internet just as any other Internet network, network should be assigned with an ID and make sure that the nodes in the ad-hoc network use it.

In such a scenario it is the IP multihop communication within the ad-hoc network that distinguishes it from regular Internet networks. Nodes in the ad-hoc network cannot expect to have link-layer connectivity with all other nodes in the ad-hoc network as in regular Internet networks. In order to reach the default gateway between the ad-hoc network and the fixed Internet, nodes must use IP layer routing.

The traditional view of ad-hoc networks is as autonomous systems of mobile IP nodes. As such, the ad-hoc network should be able to operate without any centralized configuration. Also, from an ad-hoc point of view, any set of nodes should be able to form an ad-hoc network regardless of which addresses they use and without having to use any particular network ID. This implies that one no longer can decide if a node belongs to that particular network by looking at the network ID.

In a stand-alone ad-hoc network without the hierarchy that the network ID creates there is no meaning in a default route, since either the recipient is reachable within the ad-hoc network or it is not reachable at all. As a result of this, routing in ad-hoc networks is typically performed using host routes only. This is the case for both AODV and DSR for example; neither of them uses network- nor default routes. AODV and DSR search their routing tables in the following manner:

1. Look for an entry in the routing table that matches the complete destination IP address. If found, use that route.
2. Try to find a host route within the ad-hoc network by using the route discovery mechanisms. If found, use that route. Otherwise consider the destination unreachable.

5.2 Reaching the Internet from a MANET

Host routing by ad-hoc nodes, should still be feasible when we connect an ad-hoc network where on-demand routing is used with the fixed Internet since routing information is only kept for destinations with which an ad-hoc node is currently communicating. If the ad-hoc network is connected to the Internet there has to be at least one node that resides on the border between the ad-hoc network and the rest of the Internet. This node will be referred to as the Internet gateway.

If the ad-hoc network has a network ID assigned to it (that all nodes within the ad-hoc network use), then the ad-hoc nodes could probably store default- and network routes in their routing table and use almost the same kind of lookup mechanism that ordinary IP routing does.

For destinations in other networks, i.e., destinations whose network ID differs from the ad-hoc network’s, the lookup mechanism of ordinary IP routing could probably be used. For destinations located within the ad-hoc network, i.e., destinations that use the same network ID as the node itself the lookup mechanism has to be modified. Instead of sending packets for these destinations directly to the connected interface a host route has to be used. If such a route does not exist the route discovery mechanism has to be invoked to find a host route within the ad-hoc network. The node may not decide to use a default route since that route probably would lead out on the Internet.

6. Simulation Roadmap

The design model of the project is shown in figure 8. In this figure there are 3 sections. The first section contains 3 mobile nodes (this number will be changed for each scenario), and these mobiles connected to router gateway that connect these nodes to the Internet. The second section contains

IP-based internet network and it is intermediate network between network in section one and network in section three. Section three contains two servers that provide the services to mobile nodes in section one. These services are file transfer protocol application (FTP) and web browsing application (HTTP). The simulation roadmap contains three scenarios, each scenario has its ah-hoc routing protocol (AODV), specific number of mobile nodes (3, 5, 7), but each scenario will divided into sub-scenarios in order to change the type of TCP variants (Taho, Reno, NewReno).

1. **Three Nodes Scenario**
   In this scenario, there are 3 mobile nodes and each has the AODV ad-hoc routing protocol. The TCP variants will be changed from in sub-scenarios into Taho, Reno and NewReno.
2. **Five Nodes Scenario**
   In this scenario, there are 5 mobile nodes and each has the AODV ad-hoc routing protocol. The TCP variants will be changed from in sub-scenarios into Taho, Reno and NewReno.
3. **Seven Nodes Scenario**
   In this scenario, there are 7 mobile nodes and each has the AODV ad-hoc routing protocol. The TCP variants will be changed from in sub-scenarios into Taho, Reno and NewReno.

After running these scenarios, the result displayed in a comparison fashion as shown in figures 9, 10, 11, 12, 13, 14. This figures showed that the throughput is maximum in scenario 2, where the number of mobile nodes is 5. The throughput decreases in scenario 3, where the number of mobile nodes is 7. So in order to get the maximum throughput, the number of mobiles nodes should not exceed specific number (5).

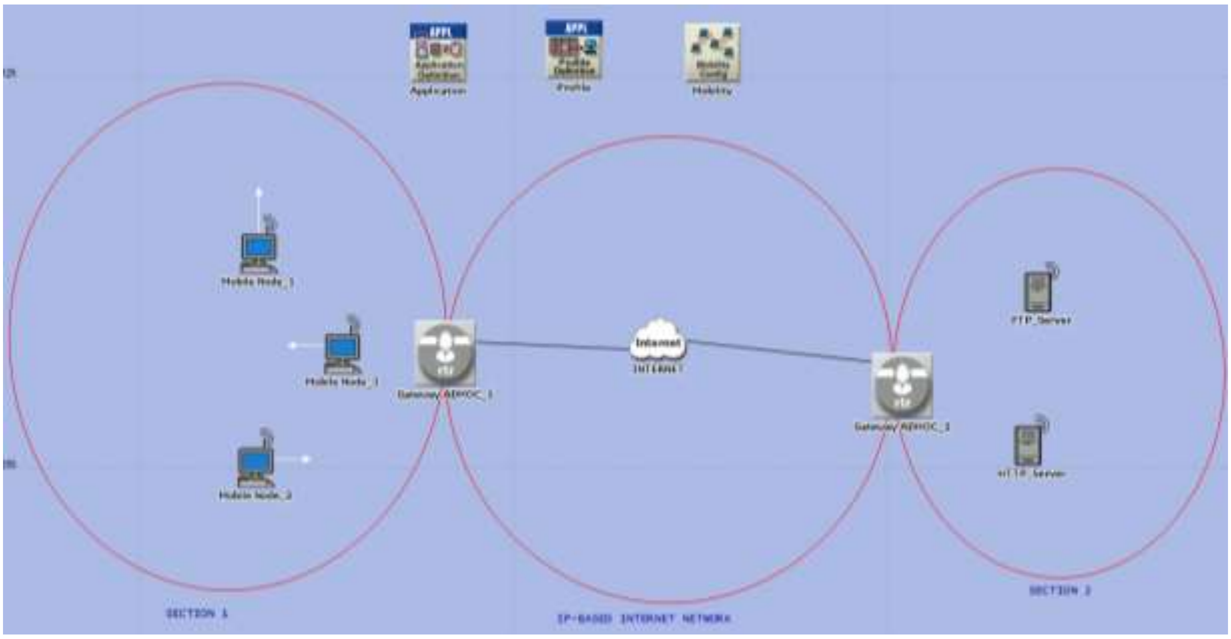

Figure 8 Simulation Design

7. Conclusions

This paper presented the state-of-the-art of TCP over mobile ad-hoc networks (MANETs). The principal problem of TCP in this MANET environment is clearly its inability to distinguish between losses induced by network congestion and others types of losses. TCP assumes that losses caused by routing failures, by network partitions, and by high bit error rates.

This paper also described the steps required to connect the MANET to the IP-Based internet network. This is doing by using MANET router gateway that had the ability to connect MANET to the IP network through running a MANET routing protocol and an IP routing protocol (or static routing) on one of its interfaces.

After running the simulation model, the results show that throughput is important parameters and the throughput will decrease if the number of the mobile nodes increased above the 5 nodes. So in order to get maximum throughput, the number of wireless nodes should not exceed 5 mobile nodes.

8. Suggestions for Future Works

In order to improve the work in this paper, one can add wired connected servers to the IP-Based internet network. This connection could be Ethernet or serial connection. One can run another ad-hoc routing protocol, such as DSR or TORA and notice the difference between them and AODV.

9. References

[1] S. Corson and J. Macker, *"Mobile Ad-hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations"***,** RFC 2501**,** January 1999.

[2] H. Ahmed et al., *"A Survey of TCP over ad-hoc Networks"*, IEEE Communications Surveys, Vol 7, NO. 3, Third Quarter 2005.

[3] J. Postel. *"Transmission Control Protocol,"* RFC 793, Sep. 1981.

[4] Tony Larsson, Nicklas Hedman, *"Routing Protocols in Wireless Ad-hoc Networks -A Simulation Study"*, Master's thesis in Computer Science and Engineering, Luleå University of Technology, 1999.

[5] Muhammad Ijaz, " *Transmission Control Protocol (TCP) Performance Evaluation in MANET* ", MSc. Thesis, Blekinge Institute of Technology ,March 2009.

[6] Charles E. Perkins, "Ad-hoc On-Demand Distance Vector (AODV) Routing", Mobile Ad-Hoc Networking Working Group, Internet Draft, Nokia Research Center 17 February 2003.

[7] David B. Johnson, "The Dynamic Source Routing Protocol for Mobile Ad-Hoc Networks (DSR)", IETF MANET Working Group, Internet Draft, 19 July 2004.

[8] V. Park, *" Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification"*, IETF MANET Working Group, Internet Draft, 20 July 2001.

[9] J. H. Schiller, *Mobile Communications, 2nd ed.*, Addison-Wesley, 2003.

[10] KA-Cheong Leung and Victor O. K. LI, "Transmission Control Protocol (TCP) in Wireless Networks: Issues, Approaches, and Challenges": IEEE Communication Surveys, 4th Quarter, 2006, Vol. 8, No. 4, pages 64-79.

[11] J. Bennett, C. Partridge, and N. Shectman, *"Packet Reordering is Not Pathological Network Behavior*," *IEEE/ACM Trans.Net.*, vol. 7, no. 6, Dec. 1999.

[12] H. Velayos and G. Karlsson, *"Techniques to Reduce IEEE 802.11b MAC Layer Handover Time," Proc. IEEE ICC 2004*, vol.7, Paris, France, 20–24 June 2004.

[13] M. Allman, V. Paxson, and W. Stevens*, "TCP Congestion Control,"* Request for Comments, RFC 2581, Network Working Group, Internet Engineering Task Force, Apr. 1999.

[14] S. Floyd and T. Henderson, *"The NewReno Modification to TCP's Fast Recovery Algorithm,"* Request for Comments, RFC 2582, Network Working Group, Internet Engineering Task Force, April 1999.

[15] Fredrik Alriksson, *"MIP MANET Mobile IP for Mobile Ad-Hoc Networks"*,MSc. Thesis, Stockholm, 1999.

List of Observations

AODV	Ad-hoc On Demand Distance vector
DSR	Dynamic Source Routing
FTP	File Transfer Protocol
HTTP	Hepertext Transfer Protocol
IP	Internet Protocol
LAN	Local Area Network
MANET	Mobile Ad-hoc Network
RERRs	Route Errors
RREQs	Route Requests
RREP	Route Reply
TCP	Transmission Control Protocol
TORA	Temporally-Ordered Routing Algorithm

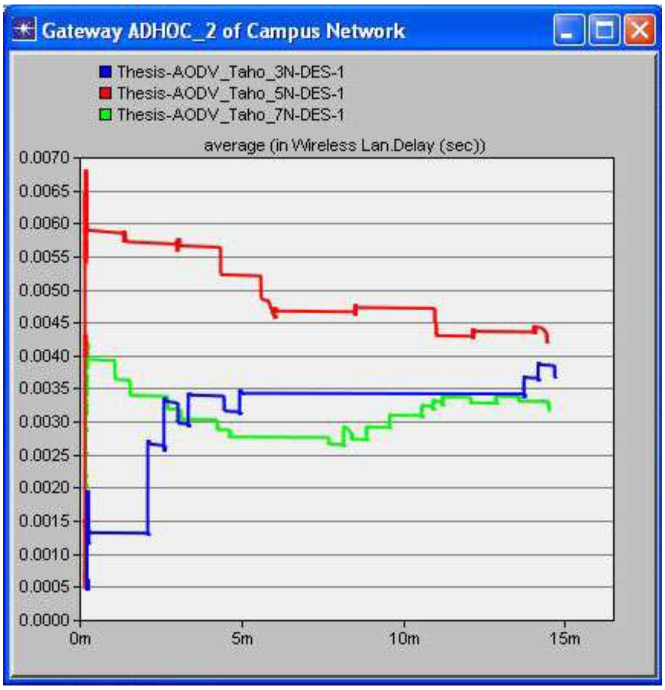

Figure 9 Average Delay (sec) Comparison between 3, 5, 7 Mobile Nodes in Taho TCP Variant

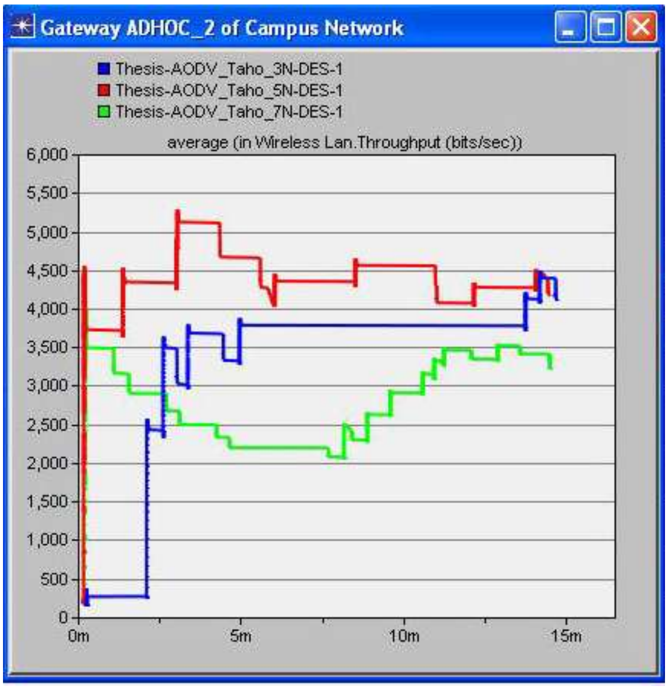

Figure 10 Average Throughput (bits/sec) Comparison between 3, 5, 7 Mobile Nodes in Taho TCP Variant

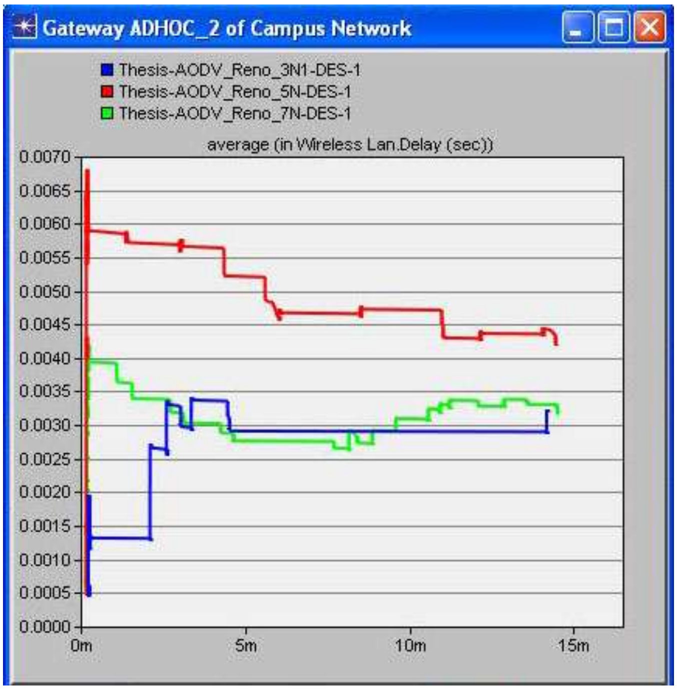

Figure11 Average Delay (sec) Comparison between 3, 5, 7 Mobile Nodes in Reno TCP Variant

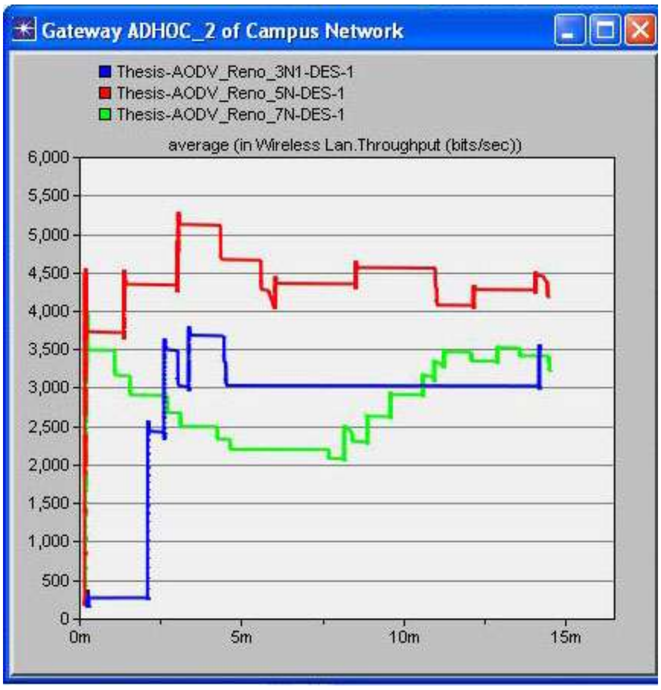

Figure 12 Average Throughput (bits/sec) Comparison between 3, 5, 7 Mobile Nodes in Reno TCP Variant

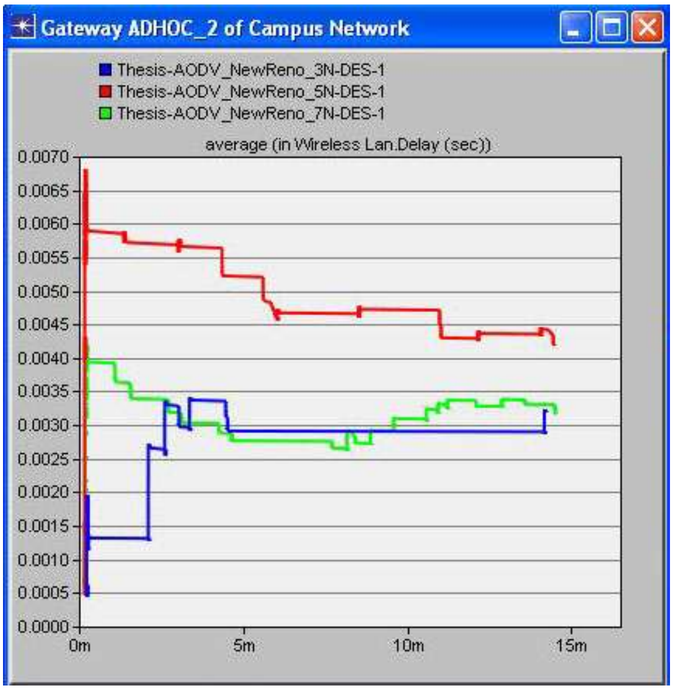

Figure 13 Average Delay (sec) Comparison between 3, 5, 7 Mobile Nodes in NewReno TCP Variant

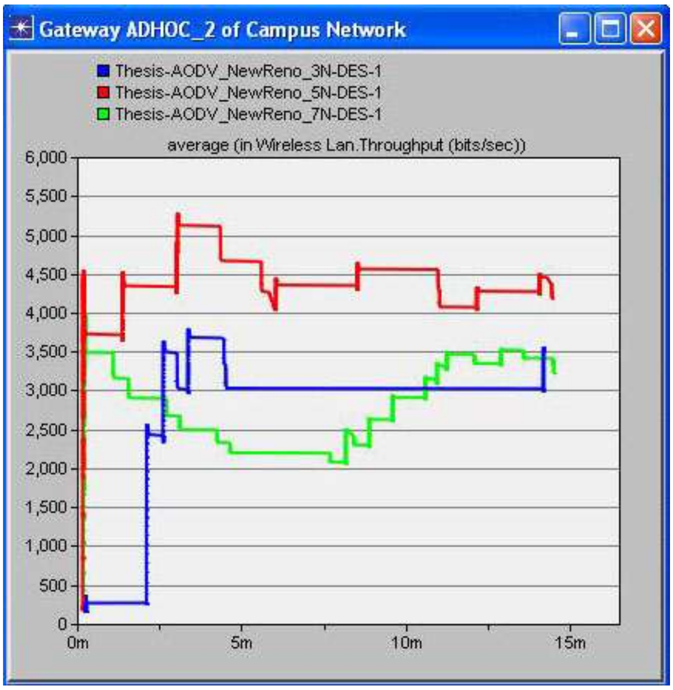

Figure 14 Average Throughput (bits/sec) Comparison between 3, 5, 7 Mobile Nodes in NewReno TCP Variant