Issues and Imperatives of Adhoc Networks

Bimal H Patel
PG Student, LDCE
Ahmedabad-380015

Parth D Shah
Associate Prof.,CSPIT
Dept of Computer Engg.

Harikrishna B Jethva
Associate Prof., LDCE
Dept of Computer Engg

Nishidh Chavda
Asst. Prof.,CSPIT
Dept of Computer Engg

ABSTRACT
MANET is a self organized, self configurable network having no infrastructure, and in which the mobile nodes move arbitrarily. The mobile nodes can receive and relay packets as a router. Routing is a critical issue and an efficient routing protocol makes the MANET reliable. The provision of quality of service (QoS) guarantees is much more challenging mainly due to node mobility and resource constraints. Security is an essential requirement in mobile ad hoc network (MANETs). Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. 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. Wireless Mobile Ad-hoc networks offer challenges to TCP's congestion control mechanism related to its inability of distinguishing between losses induced by congestion and others types of losses. This article extensively and exclusively studies the issues involved in Adhoc network which can be exploded as further research purpose.

Keywords
MANET, Routing, QoS, Security, TCP

1. INTRODUCTION
In areas in which there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use, wireless mobile users may still be able to communicate through the formation of MANET. Generally there are two distinct approaches of using wireless mobile devices for communicating.

1. Infrastructured (wireless n/w), in which mobile devices communicate with each other through access points [1].
2. Infrastructure less (Ad hoc n/w), in which mobile devices communicate with each other without access points [1].

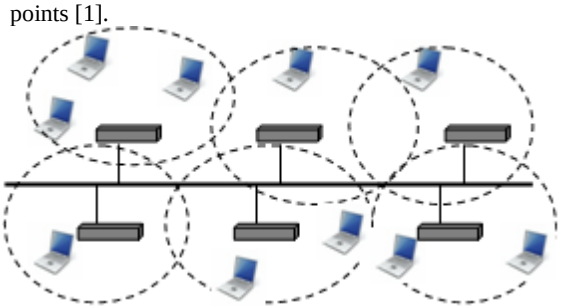

Fig 1: Wireless Network Structures (Infrastructure Networks)

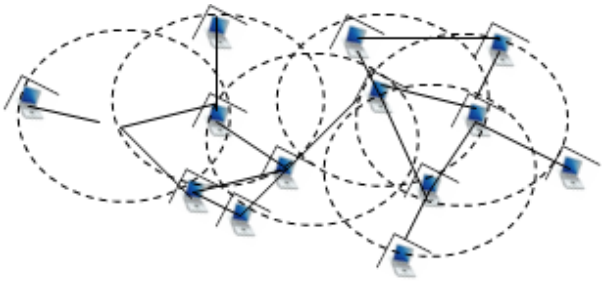

Fig 2: Wireless Network Structures (Infrastructure less Networks)

2. Mobile Adhoc Networks (MANET)
A MANET is a collection of autonomous mobile nodes connected by wireless links that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. The nodes in MANETs intercommunicate through single-hop and multi-hop paths. The intermediate nodes that are on the communication path are acts as routers. Thus the nodes operate both as hosts and as routers.

The MANETs are useful in many application environments that don't need any infrastructure support and where the computing and communications are done in smaller areas. Initially these networks are proposed for military applications such as battlefield communications and disaster recovery, but due to the evolution of the multimedia technology and commercial interest of companies to reach /support the widely civilian applications, it is necessary to provide QoS (Quality of Service) support in MANET like environment.

2.1 Characteristics of MANET
- Autonomous terminal
- Distributed operation
- Multihop routing
- Dynamic network topology
- Fluctuating link capacity
- Light-weight terminals

2.2 Challenges in MANET
- Unicast routing
- Multicast routing
- Dynamic network topology
- Speed
- Frequency of updates or Network overhead
- Scalability
- Mobile agent based routing
- Quality of Service
- Energy efficient/Power aware routing
- Secure routing

The key challenges faced at different layers of MANET are shown in Fig. 3[8]. It represents layered structure and approach to ad hoc networks.

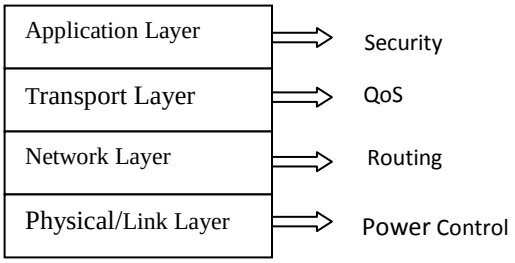

Fig 3: MANET Challenges

2.3 Key issues of MANET

There are several issues and challenges for realization of benefits from Ad-hoc networking. These challenges include:

- Routing
- Security and Reliability
- Quality of Service (QoS) issues
- TCP Variants
- Security Issues
- Simulation and performance issues

3. Routing

Due to frequent changes in topology between any pair of nodes, routing of packets between these nodes becomes a challenging task. The routes among different nodes may potentially contain multiple hops, increasing the complexity of communication in comparison to single hop. Many routing protocols have been developed which support establishing and maintaining multi-hop routes between nodes in MANETs. These routing protocols in MANETs may
be classified into basic 3-groups:

- Pro-active (table-driven) routing
- Reactive (on-demand) routing
- Hybrid (both pro-active and reactive) routing

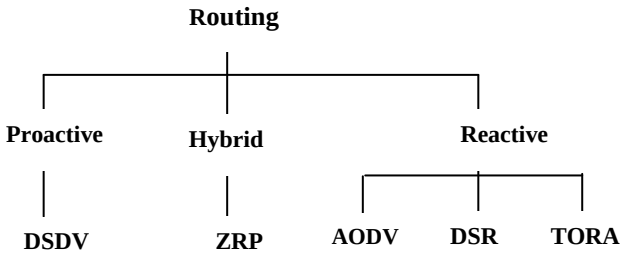

Fig 4: Routing Protocol

Pro-active (table-driven) routing Protocols (RRP)
These routing protocols are similar to and come as a natural extension of the protocols used for the wired networks. In proactive routing, each node advertises their presence by sending an advertisement message on the Ad hoc network side and has one or more tables that contain the latest or fresh lists of destinations and the information of the routes to any node in the network. Each row in the table contains the next hop for reaching to a node/subnet and the cost of that route. There are two kind of table updating process in proactive protocols. These are: -

a) Periodic Update: - Each node periodically broadcasts its table in the network and each node in the network receives that table.
b) Triggered Update: - As soon as a node detects a change in its neighborhood, it broadcasts entries in its routing table that are changed recently.

Examples:
Various table-driven protocols differ in the way the information about change in topology is propagated through all nodes in the network. The examples of this class of ad hoc routing protocols are:

- DSDV (Highly Dynamic Destination-Sequenced Distance Vector routing protocol

Advantages:

- Establish routes in advance.
- Good Connectivity: Always maintain routes from a node to every other node.
- Low or no delay (via frequent broadcasts of current AGs) for route determination.

Disadvantages:

- Bandwidth and power get wasted in the network because of the need to broadcast the routing tables/updates.
- Slow reaction on restructuring and failures.
- As the number of nodes in the MANETs increases, the size of table increases that results high control message overhead.
- Maintain the routes which may never be used.

Summary:
Proactive protocols give the QoS guarantees related to connection set-up, latency, or other real-time requirements. But in this scheme there are overheads in lightly loaded networks.

Reactive (on-demand) routing Protocols (RRP)
These routing protocols take a lazy approach to routing. In this approach the nodes do not maintain or constantly update their route tables with the latest route topology. Instead, when a source node wants to transmits a message (packet), the routes are discovered between a source and a destination by flooding a query into the network. The discovery packet is called the Route Request (RREQ) and the mechanism is called Route Discovery. By receiving the request, destination replies with a Route Reply (RREP) packet. As a result of which, the source dynamically finds the route to destination. Then the actual communication takes place. The discovered route is maintained (in the cache) until the destination becomes inaccessible or until the route is no longer desired.

Advantages:

- It achieves low routing overhead (control message) of communication and scalability since routes are determined on demand.

Disadvantages:

- It increases route discovery delay or latency time in route finding.
- Excessive flooding can lead to network congestion.

Examples of reactive algorithms:
The protocols in this class differ in handling cache routes and in the way route discoveries and route replies are handled.

- AODV (Ad-hoc On-demand Distance Vector).
- DSR (Dynamic Source Routing).
- TORA (Temporarily Ordered Routing Algorithm).

Hybrid Routing Protocols (HRP)
This type of protocols combines the advantages of purely proactive and of reactive routing. As the number of nodes increases, hybrid protocols are used to achieve higher performance. The key idea is to use a reactive routing

procedure at the global network level while employing a proactive routing procedure in a node's local neighborhood.

Disadvantage:
The main disadvantages of such algorithms are:

- Advantage depends on amount/number of nodes activated.

Hybrid Routing is a third classification of routing algorithm. Hybrid routing protocols use distance-vectors for more accurate metrics to determine the best paths to destination networks, and report routing information only when there is a change in the
topology of the network. Hybrid routing allows for rapid convergence but requires less processing power and memory as compared to link-state routing.
Examples of hybrid algorithms are

- ZRP (Zone Routing Protocol)

	Proactive	Reactive	Hybrid
Network Organization	Flat/Hierarchical	Flat	Hierarchical
Topology Dissemination	Periodical	On-demand	Both
Route latency	Always available	Available when needed	Both
Mobility Handling	Periodical updates	Routing maintenance	Both
Communication Overhead	High	Low	Medium

Table 1: Characteristics summary of routing protocols [6].

These are some properties of routing protocols that are desirable in MANET:

- **Distributed Operation**
  The protocol should be distributed. It should not be dependent on a centralized controlling node.
- **Loop Free**
  To improve the overall performance, we want the routing protocol to guarantee the routes supplied are loop-free. This avoids any waste of bandwidth or CPU consumption.
- **Demand based Operation**
  To minimize the control overhead in the network and thus not wasting network resources more than necessary, the protocol should be reactive. The protocol should react only when there is a change in the network and that protocol should not periodically broadcast control information.
- **Multiple routes**
  To reduce the number of reaction to topological changes and congestion, multiple routes could be used. If one route has become invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure.

4. Quality of Service Issues

Due to resource constraint and dynamic topology of MANETs, supporting QoS in MANETs is a challenging task. QoS is needed in MANETs, as different applications have different service requirements. The objective to achieve the QoS is that the information carried by the network can be successfully delivered and resources can be better utilized.
The various QoS parameter consideration are as follows:

- **Throughput**: The total bytes received by the destination node per second (Data packets and Overhead).
- **Good put (In terms of Number of Packets)[7]:**
  The ratio of the total number of data packets that are sent from the source to the total number of packets
  that is transmitted within the network to reach the destination.
  Good put (In terms of Packet Size in Bytes):
  The ratio of the total bytes of data that are sent from the source to the total bytes that are transmitted
  within the network to reach the destination.
  Excludes protocol overhead bits as well as retransmitted data packets.
- **Minimum Delay:** Minimum Time taken for the packets to reach the next node.
- **Maximum Delay:** Maximum Time taken for the packets to reach the next node.
- **Packet Delivery Ratio:** Packet Delivery Ratio in this simulation is defined as the ratio between the number of packets sent by constant bit sources (CBR) and number of packets received by CBR sinks at destination.
- **Packet Delivery Ratio** = Σ CBR Packets received / Σ CBR Packets sent It describes the percentage of packets, which reach the destination.
- **Network size:** It determines the number of nodes and size of area that nodes are moving within. Network size basically determines the connectivity. Fewer nodes in the same area mean fewer neighbors to send request to, but also smaller probability of collision.

Some of factors that influence QoS [5] of Wireless Network include:

- **Throughput of Network**
  Represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network.
- **Retransmission Attempts**
  Total number of retransmission attempts by all WLAN MACs in the network until either packet is successfully transmitted or it is discarded as a result of reaching short or long retry limit.
- **Data Dropped**
  Data dropped due to unavailability of access to medium.
- **Medium Access Delay**
  It includes total of queuing and contention delays of the data.

5. TCP Issues

Although TCP provides reliable end-to-end delivery of data over wired networks, several recent studies have indicated that TCP performance degrades significantly in mobile ad hoc networks. This is mainly because TCP considers any packet loss and/or delay as a congestion signal although MANETs encounter several types of losses and delays that are not related to congestion.
Non-congestion losses/delays mainly occur because TCP cannot adapt well to such mobile wireless multi-hop networks.

Factors Affecting TCP Performance in MANET

In addition to the traditional problems of wireless networking, the mobile multihop ad hoc environment brings more challenges to TCP. The factors are summarized as follows [2]:

- **High Bit Error Rate (BER):** Wireless links are susceptible to high bit error rates due to signal attenuation, Doppler shift and multipath fading. This leads to the loss of TCP data segments or acknowledgments. Hence, the TCP sender will unnecessarily invoke congestion control.
- **Path Asymmetry:** In MANET, path asymmetry may manifest in several forms like bandwidth asymmetry, loss rate asymmetry, and route asymmetry. If the ACKs get bunched up, the sender may transmit data in a burst, which could lead to packet loss on the forward path. Also, disruption of the ACK stream can disrupt window growth and degrade performance to a fraction of the available bandwidth.
- **Route Failures:** The main cause of route failures is node mobility. The route re-establishment duration depends on the underlying routing protocol, mobility patterns of nodes, and traffic characteristics. It is possible that discovering a new route may take significantly longer than the retransmission time out (RTO) at the sender. As a result, the TCP sender will unnecessary invoke congestion control.
- **Network Partitioning:** It is due to node mobility or energy-constrained operation of nodes. If the sender and the receiver of a TCP connection lie in different partitions, all the sender's packets get dropped by the network resulting in the sender invoking congestion control. Frequent disconnections cause a condition called serial timeouts at the TCP sender. This may lead to long idle periods during which the network is connected again, but TCP is still in the back off state.
- **TCP congestion window size:** In MANETs, since the routes change many times during the lifetime of a TCP connection, the relationship between the congestion window size and the tolerable data rate becomes too loose. If the congestion window size is greater than an upper bound, the TCP performance will degrade. Also, reported that, given a specific network topology and flow patterns, there exists an optimal TCP's window size *W* by which TCP achieves the best throughput. But, unfortunately, TCP operates at an average window size that is much larger than *W*; this leads to increased packet loss due to the contention on the wireless channel.
- **Power Scarcity:** Because batteries carried by each mobile node have limited power supply, the life time is limited. Since each node acts as a router as well as an end system, unnecessary retransmissions of TCP segments consume this scarce power resource causing inefficient utilization of available power.
- **Multipath routing:** Some routing protocols maintain multiple routes between source and destination to minimize the frequency of route re-computation. Unfortunately, this sometimes results in a significant number of out-of-sequence packets arriving at the receiver causing the generation of duplicate ACKs which cause the sender to invoke congestion control.
- **Hidden and exposed terminal problem:** Due to the share medium and multi hoping capability the nodes facing the hidden and exposed node problem. Fig: 5 representing the hidden and exposed terminal problem of IEEE 802.11 standard. The circles show the transmission range of A and B, where C is in the transmission range of both A and B. Let A and B both want to transmit data to C, so there will be collision at C, because A and B do not know about the transmission of each other due to hidden node problem [12].

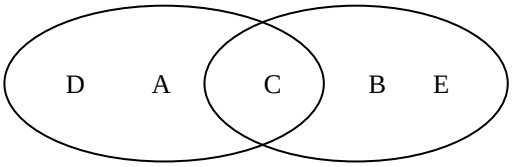

Fig 5: Hidden and Exposed Terminal Problem

Now let that there is a transmission between C and B, while at the same time A wants to transmit data to D, but when A senses the medium, it find that the medium is busy due to C transmission and thus A stops its transmission. Actually in this situation A transmission for D will not going to collide with C transmission, This problem exist in IEEE802.11 standard and known as exposed terminal problem.

- **Out of Order Packet**
  When a receiver receives out of order packets, the receiver transmits duplicate acknowledgement, after receiving three duplicate ACK the sender retransmit the packets and congestion control is activated. But the problem is that congestion control is activated wrongly most of the time, because out-of-order packet occurrence take place due to different reasons such as multipath routing protocol and rout failure and not only due to congestion.

6. Security Issues

Securing wireless ad hoc networks is a highly challenging issue. Security problems arise due to dynamic topologies and membership, vulnerable wireless links, roaming in dangerous environment. The physical medium of communication is inherently insecure, so it is important to design aware routing algorithms for MANET. The physical layer should take care of changes in transmission quality, for example by adaptively increasing or decreasing the transmission power. Similarly, the link layer should react to the changes in link error rate, including the use of automatic repeat request. Link layer takes care of the variable bit error rate, the main effect observed by network layer will be a change in effective throughput (bandwidth) and delay.

Various Classification of attack

Roughly there are two main categories always considered as shown in figure 1[9].

- **Passive attacks**
  Those attacks that do not disrupt the normal functionality of MANET while obtaining data exchanged from network
- **Active attacks**
  Those attacks that disrupt the normal functionality of MANET such as doing data interruption, modification or fabrication.

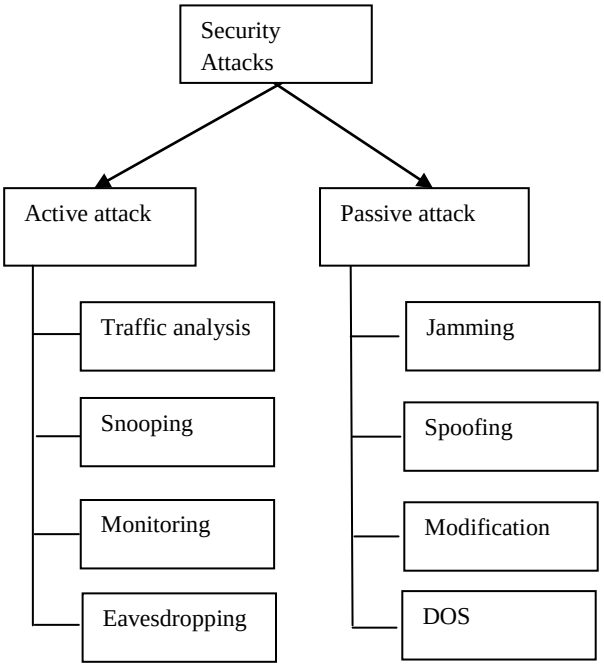

Fig 4: Security Attacks

Other type of classification of attacks is

- External attack: Carried out by nodes that do not belong to the particular domain of the network
- Internal attack: Carried out by the compromised nodes (selfish nodes), which belong to the domain of the network and more secure than external attacks [3].

Characteristics of selfish nodes as follows[4]**:**

- **Do not participate in routing process:** A selfish node drops routing messages or it may modify the Route Request and Reply packets by changing TTL value to smallest possible value.
- **Do not reply or send hello messages:** A selfish node may not respond to hello messages, hence other nodes may not be able to detect its presence when they need it.
- **Intentionally delay the RREQ packet:** A selfish node may delay the RREQ packet up to the maximum upper limit time. It will certainly avoid itself from routing paths.
- **Dropping of data packet:** A selfish nodes may participate in routing messages but may not relay data packets.

7. Simulation and Performance issues

There are two main approaches in system performance evaluation: the first uses measurements; the second is based on a representation of the system behavior via a model [11]. Measurement techniques are applied to real systems, and thus they can be applied only when a real system, or a prototype of it, is available. Using a simulation or analytic model, on the other hand, permits the study of system behavior by varying all its parameters, and considering a large spectrum of network scenarios.

The two current issues are:

- Models of nodes mobility
- Network simulators.

7.1 Mobility models

The ability of ad hoc networks_ protocols to correctly behave in a dynamic environment, where devices position may continuously change, is a key issue. Therefore, modeling users movements is an important aspect in ad hoc network simulation.

This includes among others [10]:

- The definition of the simulated area in which users movements take place, and the rules for modeling users that moves beyond the simulated area;
- The number of nodes in the simulated area, and the allocation of nodes at the simulation start up; and
- The mobility model, itself.

The random waypoint mobility model is the model most commonly used to define the way users move in the simulated area. Recent studies have pointed out problems in the random waypoint model. Two specific types of problems have been identified:

(i) The nodes average speed is decreasing

(ii)The nodes distribution in the simulated area is non-uniform.

7.2 Network simulators

Most MANET simulative studies are based on simulation tools. The main advantage of these tools is that they provide libraries containing predefined models for most communication protocols (e.g., 802.11, Ethernet, TCP, etc.). In addition, these tools often provide graphical interfaces that can be used both during the model development phase, and during simulation runs to simplify following dynamic protocol and network behaviors. Popular network simulators used in ad hoc networks include: OPNET [13], NS-2 [14], Glomosim [15] and its commercial version QualNet [16]. Important divergences between the simulators results have been measured. The observed differences are not only quantitative (not the same absolute value), but also qualitative (not the same general behavior) making some past observation of MANET simulation studies an open issue.

8. Discussion and Conclusion

Ad hoc networking is at the center of the evolution towards the 4th generation wireless technology. Its intrinsic flexibility, ease of maintenance, lack of required infrastructure, auto-configuration, self administration capabilities, and significant costs advantages make it a prime candidate for becoming the stalwart technology for personal pervasive communication. In moving forward towards fulfilling this opportunity, the successful addressing of open technical and economical issues will play a critical role in achieving the eventual success and potential of MANET technology. Despite the large volume of research activities and rapid progress made in the MANET technologies in the past few years, almost all research areas (from enabling technologies to applications) still harbor many open issues. This paper reveals important open imperatives which can be used as research purpose.

9. Acknowledgments

The author would like to thank Asst. Prof. Nirav H. Bhatt, Vishal Rathod and Priyanka Patel from U & P U Patel Dept. of Computer Engg., CHARUSAT University for their input and constructive comments on improvements of the paper.

10. References

[1] Anilkumar Sharma, Neha Bhatia, "Behavioural study of MANET routing protocol" IJCEM International Journal of Computational Engineering & Management, Vol. 12, April 2011,pp.100-104.

[2] Z. I. Dafalla, Mayyada Hammoshi "Performance evaluation of Tcp Variants" ATINER's Conference Paper Series COM2012-0046

[3] Matthias Hollick, Jens Schmitt, Christian Seipl, and Ralf Steinmetz "On the Effect of Node Misbehavior in Ad Hoc Networks" IEEE Vol. 6, pp. 3759--3763.

[4] Shailender Gupta, C. K. Nagpal and Charu Singla "Impact Of Selfish Node Concentration In MANET" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April 2011,pp. 29-37.

[5] MukeshKumar, Rahul Rishi, D.K.Madan "Issues And Challenges Of Quality Of Service In Mobile Adhoc Network" International Journal of Computer Science & Engineering Technology (IJCSET) Vol. 1, No. 3,pp. 61-66.

[6] Hongbo Zhou "A Survey on Routing Protocols in MANETs" Technical Report: MSU-CSE-03-08 Mar 28, 2003.

[7] Ankur Lal, Dr.Sipi Dubey, Mr.Bharat Pesswani "Reliability of MANET through the Performance Evaluation of AODV, DSDV, DSR" International Journal of Advanced Research in Computer Science and Software Engineering Vol. 2, No. 5,May 2012,pp. 213-216.

[8] Sunil Taneja, Ashwani Kush "A Survey of Routing Protocols in Mobile Ad Hoc Networks" International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010",pp. 279-285.

[9] Rajni Sharma, Alisha Saini, "A Study of Various Security Attacks and their Countermeasures in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 1 No. 1 December 2011",pp. 01-05.

[10] A. Boukerche, L. Bononi, "Simulation and modeling of wireless, mobile and ad hoc networks, in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking" IEEE Press Wiley, New York, 2003.

[11] J.F. Kurose, H. Mouftah, Computer-aided modeling of computer communication networks, IEEE Journal on Selected Areas in Communications 6 (1) (1988) 130–145.

[12] Md Nazmul, Islam Khan, Rashid Ahmed, Md. Tariq aziz " A survey on TCP Reno, New Reno and Sack over mobile Ad hoc network" International Journal of Distributed and Parallel Systems Vol. 3,No 1,January 2012

[13] Opnet Modeler, http://www.opnet.com/products/ modeler / home.html.

[14] The Network Simulator-ns-2, http:// www. Isi. Edu / nsnam/ns/index.html.

[15] Glomosim, <http://pcl.cs.ucla.edu/projects/glomosim/>

[16] QualNet simulator, http://www.qualnet.com/.