ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 2 ISSUE 1 JANUARY 2012

ADHOC NETWORKS: AN ANALYTICAL OVERVIEW

Tanu Preet Singh

Department of Computer Science & Engineering

Amritsar College of Engineering & Technology, Amritsar

Vikrant Das

Department of Computer Science & Engineering

Amritsar College of Engineering & Technology, Amritsar

Srihthi Maheshwari

Department of Computer Science & Engineering

Amritsar College of Engineering & Technology, Amritsar

ABSTRACT

Mobile Ad Hoc Network (MANET) is a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator also the wireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure.

And it's an autonomous system in which mobile hosts connected by wireless links are free to be dynamic and sometime act as routers at the same time. Despite the technical challenges, the interests of the ad hoc networks increase rapidly in recent years, because they support mobility and are very well suited for many difficult situations, such rescue mission, military, vehicular communications, etc. We discuss in this paper the characteristics of the wireless networks and problems and issues related to them in general. This paper gives the analytic overview of the Adhoc networks.

I. INTRODUCTION

With the widespread rapid development of computers and the wireless communication, the mobile computing has already become the field of computer communications in high-profile link. Since the initial work on the packet radio network (PRNet) in 1972, computer networks have evolved from small-scale initiatives connecting a few geographically separated sites, into a worldwide broadband communication network. Research interest in wireless packet radio networks initially came from the military. Since the mid-1980s, lots of civil applications for wireless ad hoc networks have been studied, such as emergency communication for public services or communication in disaster areas. In the late 1990s, wireless enabled hardware became cheap and omnipresent, and with the foundation of the MANET (mobile ad hoc networks) Working Group, the Internet Engineering Task Force (IETF) started standardization efforts for routing protocols supporting mobile wireless networks [8].

Wireless ad hoc networks are collections of wireless nodes that communicate directly over a common wireless channel. The nodes are equipped with wireless transceiver. They don't need any additional infrastructure, such as base station or wired access point, etc. Therefore, each node doesn't only plays the role of an end system, but also acts as a router, that sends packets to desired nodes [1]. The important thing to remind is that nodes can move freely, so they are battery equipped; devices, to move easily, have to be small, but in this case battery powerful is not so strong. Infact a large battery capacity is obtained with space and space increases devices dimensions therefore this is an issue [2]. The ad hoc are expected to do assignments, which the infrastructure can't do. Ad hoc networks are mostly used by military, rescue mission team, taxi driver. Their works can't rely on an infrastructure's network. As an illustrative example, imagine firefighters put out hazardous fire in a big forest. They have to communicate each other, but establishing a infrastructure or cabling in such area is impossible or too expensive. Adhoc networks are also called ***mesh networks***. The term mesh network accurately describes the structure of the network: All available nodes are aware of all other nodes within range. The entire collection of nodes is interconnected in many different ways, just as a physical mesh is made of many small connections to create a larger fabric [2]. In figure 1, here an ad hoc network links users to a router with access to the Internet. In this example, two users are highlighted, showing two paths through several nodes to

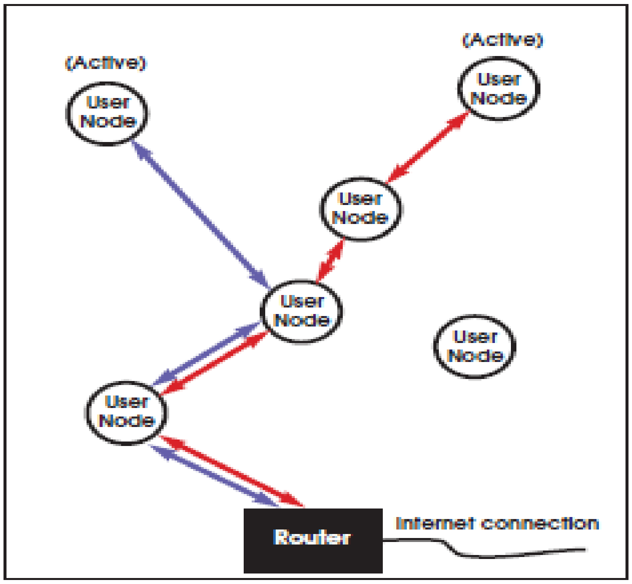


Figure 1: Basic structure of an ad hoc or mesh network, the path form user's node to the destination node is provided by other user's device acting as router.

the router. If one of the intermediate nodes were to fail (e.g. that user leaves the area), the network will automatically reconfigure itself, locating an alternate path from the user to the router. Typically, all available nodes are also network users, each sharing the total data transfer capacity of the particular hardware and operating protocol being used. [2]

Wireless mobile approaches are very important to make communication between two nodes. Firstly infrastructure wireless networks and secondly infrastructureless wireless networks. [4]

A. Infrastructure Wireless Networks

This architecture allows the wireless station to make a communication between each other and this type relies on the third fixed party and we call it a Base Station that will hand over the offered traffic from the Station to another, the same entity will regulate or organize the allocation of radio resources [4]. When a source node likes to communicate with a destination node, the former notifies the base station.

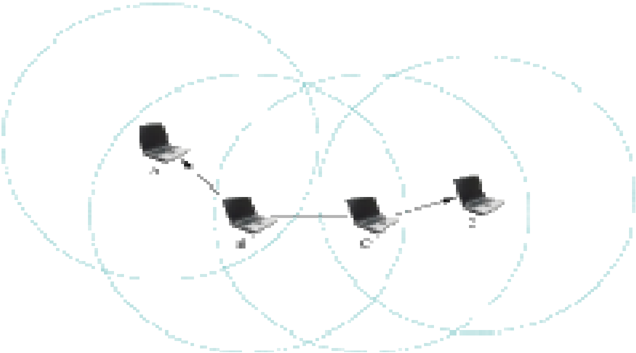
B. Infrastructureless Wireless Networks

In this architecture the nodes communicates with each other without the aid of any centralized administrator .The nodes can dynamically from a network to exchange information without using any existing fixed networks infrastructure [4].

Nowadays, the information technology will be mainly based on wireless technology, the conventional mobile network and cellular are still, in some sense, limited by their need for infrastructure for instance based station, routers and so on. For the Mobile Ad Hoc Network, this final limitation is eliminated, and the Ad Hoc Network are the key in the evolution of wireless network and the Ad Hoc Network are typically composed of equal node which communication over wireless link without any central control. Nodes form the network topology when they are associated to links that connect them. Possible network topologies are flat, tree and cluster based [3]. The ad hoc networks must be less complicated than infrastructure networks. Fundamentals of Adhoc networks which need to be kept in mind while setting up the network are dynamic topologies, bandwidth constraints, energy constraints and network security. Besides these there, hardware (end devices) and the software (routing algorithms), are the integral part of the Adhoc networks. Routing of messages from a source to one or multiple destinations is a fundamental building block for all applications in the domain of ad hoc and sensor networks. In most cases, it only means to divulge information is by routing, either as unicast, any cast, multicast, or broadcast. Whereas there are standard approaches for the latter, it is much more challenging to implement efficient single destination routing, any casting, and multicasting. Energy consumption is an important problem to take care because each device is powered by batteries so their runtime depends on battery capability. Quality of service obtained can be not so high, infact it implies having low battery duration. Energy consumption is measured by the two parameters namely Power Control and Energy Saving. Algorithms now being implemented should take energy consumption to be a major factor while transmitting the data from on node to another.

Figure 2: Shows the neighbors, signal strength, transmission range and the interference regions.

QOS is a guarantee by the network to provide certain performance for a flow in terms of the quantities of bandwidth, delay, jitter, packet loss probability etc. Ad hoc networks make the appear an even more challenging problem than ever before, despite some of re-active routing protocols can be configured to return only paths that comply with certain desired parameters. Bandwidth is seriously limited [6]. Although substantial attempts have been made on research towards design and development of ad hoc network parameters, there is relatively little



understanding of their behavior in terms of the performance by comparing execution times as the system is scaled up [5]. If we can link into a temporary network structure, then the data transmission will be more efficient without the need for large-scale projection equipment that would not have point to point link equipment (such as network line or transmission line). The current wireless LAN technology, Bluetooth is has attracted considerable attention as a development plan. Bluetooth's goal is to enable wireless devices to contact with each other, if the adding the design of Ad Hoc Network (MANET).

II. RELATED WORKS

The term ad hoc comes from Latin and means for this purpose only, so ad hoc networks are created spontaneously by users when they have to communicate each other. An ad hoc network can be made of:

- Nodes connected to each other by wireless nodes;
- Nodes connected to a fixed infrastructure.

The important thing to remind is that nodes can move freely, so they are battery equipped; devices, to move easily, have to be small, but in this case battery powerful is not so strong. Infact a large battery capacity is obtained with space and space increases devices dimensions therefore this is an issue. The ad hoc networks can have:

2.1 Fully symmetric environment

When nodes have the same capabilities (in sense of characteristics as energy power) and responsibilities (there is no a central controller).

2.2 Asymmetric environment

Asymmetric capabilities if they have different characteristics such as battery power, transmission range and processing capability; and asymmetric responsibilities when there are classifications in leader and ordinary nodes (a possible example are clusters in which there are clusters heads and ordinary nodes) [3]. Taken a node, all other nodes able to receive its transmission are called neighbors and that region in which nodes can communicate through a wireless link is called transmission range. There is another important region, the interference region, the one in which if a node receives two communications from different sources it is not able to decode them [3].

The Ad hoc networks follow the self-configuring and a self-healing process. The nodes in the network are capable of discovering the other nodes in its range by considering the factors such as the signal strength and the distance of the node. Over the time the network's formation changes as it keeps on updating itself because of the node motion. This leads to network reconfiguration. This behavior is achieved by the identifying the routing protocols and the network topologies. Routing Protocols are of two types namely *Proactive routing protocols (Table Driven) and Reactive routing protocols (On Demand).* Proactive schemes calculate the routes to various nodes in the network. So the nodes can use the route whenever they need it. Reactive scheme will calculate the route, if the nodes need to communicate with a destination node. They will work, if they have to do. Destination Sequenced Distance Vector (DSDV) is an example of proactive scheme. Ad Hoc on Demand Distance Vector (AODV) and Dynamic Source Routing are examples of reactive scheme [1]. The routing protocols need to function as per the need of the environment. In this [4], the author has stressed on the need to design a suitable routing protocol for ad hoc networks especially MANETS. For this the operating environment must consider different aspects which can be classified into two categories namely qualitative aspects and quantitative aspects discussing the performance of the protocols.

2.3 Qualitative Aspects

1. *Distribution operation*: routing cannot rely on one particular node to operate.
2. *Loop freedom*: routing protocols should have consistent characteristics and should be able to avoid the wastage of the bandwidth. With this it is also capable of avoiding the redundancy in the routing table.
3. *Demand based operation*: On demand establishment of the path, avoids burden but causes delay.
4. *Proactive operation*: table driven approach to speed up the path establishment, puts some overhead for table maintenance but saves time.
5. *Security*: must, as it can be interfered with easily.
6. *Sleep period operation*: the routing protocols should be able to accommodate sleep periods without overly adverse consequences [4].

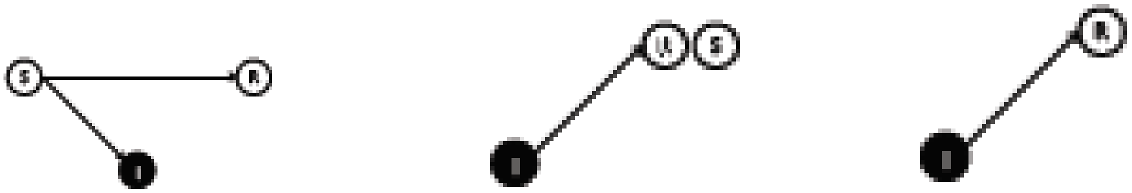
2.4 Quantitative Aspects

1. *End-to-end data throughput and delay*: data transmission rate and delay in the case that every routing protocol must take into account the focus should be how to find the best path [4]?
2. *Route acquisition time: it* tells as to how fast the route to a particular destination is found and established.

3. Percentage out of order delivery: how much of the actual data/packets have been delivered and how many of them were lost on the way causing the miscommunication or erroneous message transfer.

4. *Efficiency*: the simplest method, the smallest control overhead experienced to complete the task and common goal for all routing protocols.

Due to dynamic distributed infrastructure-less nature and lack of centralized monitoring points, the ad hoc networks are vulnerable to various kinds of attacks. There are numerous security problem issues in the ad hoc networks. Unlike wired channel, the wireless channel is accessible to both legitimate network users and malicious attacker. Therefore, the ad hoc networks are susceptible to attacks ranging from passive attacks such as eavesdropping to active attack such as interfering. Especially for MANETs, limited power consumption and computation capabilities due to energy limitation, causes incapability to execute computation-heavy algorithms like public key algorithms. Passive attack means, that the attacker does not send any message. The attacker just listens the channel; therefore, it is almost impossible to detect this attack. In contrast, the active attack modifies, deletes the packets, and injects packets to invalid destination. Active attack can be detected [1].



(a) Eavesdropping (passive attack) (b) Modifying (passive attack) (c) Masquerading (active attack)

Figure 5: Security threats

1. *Eavesdropping* (passive), a non-legitimate listening into a transmission between two nodes.
2. *Traffic analysis* (passive), the attacker monitoring the transmission for patterns of communication.
3. *Masquerading* (active), the attacker pretends to be authorized user of a system in order to gain access to it or to gain access to it or to gain greater privileges than they are authorized for.
4. *Replay* (active), the attacker spies' transmissions and retransmits message as the legitimate user.
5. *Message* modification (active), the attacker alters an original message by deleting, adding to, modifying it.
6. *Denial-of-service or interruption* (active), the attacker prevents or prohibits the normal use or management of communications facilities [1].

The principal advantages of an ad hoc network include the following:

1. Independence from central network administration
2. No infrastructure and lower cost.
3. Decentralized and robust.
4. Easy to build and spontaneous infrastructure [1].
5. Self-configuring, nodes are also routers
6. Self-healing through continuous re-configuration
7. Scalable—accommodates the addition of more nodes
8. Flexible—similar to being able to access the Internet from many different locations [2].

III. PROBLEM DEFINITION

There has been considerable research on conserving power in the routing protocol. Most of these researches are focused on controlling the transmission power of the sender network interface. Increasing power consumption and packet storming within ad-hoc network is becoming a core issue for these low power mobile devices [8]. We are aware of the fact that some problems are vendor specific and that, strictly spoken; it is not the task of people performing research at the higher layers of the OSI stack to actually solve hardware problems. However, we feel that a careful choice of research methodology and network architecture can severely reduce the observed problems [7].

The problems we have proposed here deal with routing algorithms and some parameters that can be linked together with them to give out the desired results.

1. How is the link between two nodes affected if we increase the transmission power of the end devices?

We all know that increasing the power and the battery life of the node will surely give out positive results in terms of increased throughput. But the size of the node will simultaneously increase. So how can we keep the size of the node same and still utilize its battery efficiently. Rather than increasing the size of the battery we can increase the transmission power of the sending signals.

2. How can the capacity of the nodes be increased by adding multiple interfaces?

A single node is carrying a single interface that deals totally with the transfer of the packets. It then must experience a greater overhead. As the same interface has to carry out the routing, transmitting and receiving of the messages, it must be constantly be in awake state so as to look out for the incoming messages and outgoing messages. Since the node remains awake all the time it will consume more battery power there by reducing the life of the node. So what happens if we add multiple interfaces to a node and assign them a separate work so they don't interfere in each other and the battery is utilized efficiently?

3. Is the quality of service improved by increasing the power of transmission?
By increasing the transmission power of the node, we are assuming that the throughput of the signal will be good. Increased power of transmission will surely lead to the increased utilization of the battery of the node. But after considering all these factors we are not sure that will the quality of service of the network increase or at least match the minimum standards of a good network.

4. Is hardware compatibility causing the delay in the transmission or hinder it completely?
Many of the issues of the Adhoc networks are due to the mismatch of the hardware provided by them. The performance and the capability of the hardware devices vary greatly when we switch from one vendor to another. These problems can be solved by replacing the hardware. Unfortunately, in a traditional ad hoc network where nodes can join freely, it is wrong to assume that all nodes will react identically to a specific algorithm's action. For example, if a certain algorithm would reduce transmission power of a node to 1 dB/m, the algorithm might operate as expected on hardware from vendor *1* or *2*, but fail to work on hardware from vendor *3* or *4*. If the quality of the hardware cannot be guaranteed, control loops should be provided within algorithms to verify whether a certain action has the desired effect. These effects are very hard to model in a simulator and can only be discovered by putting algorithms to test on real-life test-beds [7].

DSDV is a proactive routing protocol. It is considered as a good algorithm for the transmission in short range. But it has some areas where it still needs to be improved so as to give out the efficient results. DSDV protocol also poses some major questions:

1. Why are sleeping nodes not used?

The routing according to the DSDV protocol occur in four phases namely the Receiving Phase, Transmitting Phase, Idle Phase and the Sleeping Phase. Besides the sleeping phase all other phases consume battery regularly. In the sleep phase the node goes into hibernation and it stops all kinds of transmission processes. The main question is that why is the sleeping phase of the node not utilized effectively. The sleeping phase in the node can be used efficiently for conservation of the battery power.

2. Overhead: most routing information never used.

The main problem of the proactive routing protocols is that there is an un-necessary overhead of maintaining the routing information of those nodes which are not taking part in the transmission of the packets or which have been idle from a long time.

3. It only considers hop count as metric but is not considering efficiency (processing speed) of nodes.

In the above figure , if node A needs to send a packet to node B, it has two route alternatives, firstly it can send from route 1 which has less number of intermediate nodes a, hence less hops but the performance of the nodes is poor with low processing speed. Secondly, it can send via

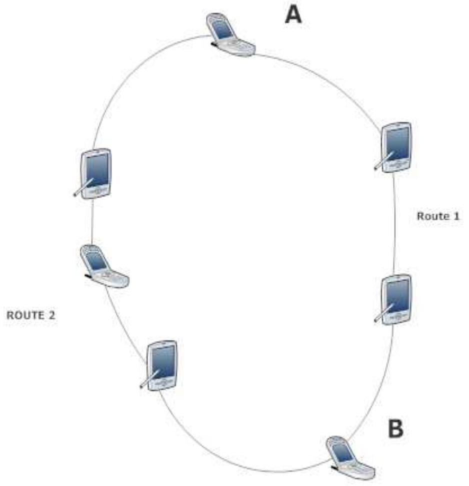


Figure 6: Different routes from two nodes.

route 2 which has comparatively more number of hops but the processing speed of the nodes is much more than those of route 1.Though with more hops but the second route can send the data packet easily and reliably.

4. It is also not considering the status (free/busy) of internal nodes.
During the routing of packets the status of the node should be considered. Of the node is already in a transmitting process then the source node should find an alternate path to send the data and apply the techniques of load balancing.

IV. PROPOSED MODELS/SUGGESTIONS

A Heterogeneous Hierarchical Architecture

It is inherent to the nature of wireless ad hoc networks that low-quality nodes will sooner or later join the network. Wireless systems will always be more unreliable than their wired counterparts, and therefore, algorithms must be able to detect anomalies and react accordingly.

Firstly, transmission power should be chosen wisely: neither too low nor too high. While in a static set-up, transmission power can be set manually by trial and error; there is need for automatic tuning in dynamic environments. Cross layer protocols might provide a way to implement these control loops. Secondly, because of interference and hardware related issues, the choice for a specific channel has an impact on the wireless link quality. Problems occur at various layers of the protocol stack when wireless links break due to changing channel conditions or failing hardware. Thirdly, it was shown that small devices with multiple interfaces suffer from self-generated interference. In order to overcome this problem we should focus our research on an architecture which takes this fact into consideration. An algorithm which presupposes a complete separation between multiple interfaces at end-user nodes will most likely never be able to achieve its claimed results when used in real systems. In a heterogeneous architecture, devices have distinct capabilities and technologies. In a wireless mesh network (WMN), two types of nodes are distinguished: mesh routers and mesh clients. Mesh routers hold superior properties concerning processing power, interfaces, available power and memory, enabling them to perform more complex functions. In addition, they have limited mobility compared to the clients, resulting in a wireless mesh backbone. Mesh routers can be added or removed at any time and act as gateways to other networks such as the Internet. In a *hybrid* WMN, mesh clients can connect to the backbone network either directly, or by using a multi hop path through other clients. Some benefits of heterogeneous hierarchical networks have been described in the past, such as an increase in coverage, or the (theoretical) ease of set-up. However, we believe that there are more reasons why hierarchical heterogeneous architectures can help to realize robust wireless networks, and that a conscientious choice of networking architecture can help certain assumptions that are invalid for homogeneous wireless networks become valid. The mesh routers in the backbone can and should have multiple interfaces: they can be bigger in size and antennas can adequately be separated, thereby reducing the interference problems. Additionally, they have an “unlimited” power supply as they are most likely connected to a host system with plenty of power such as a building or a truck. Faulty hardware may be used within a cooperative wireless network, resulting in decreased performance and satisfaction for the end-users. In a traditional ad hoc network, even if one user invests in high-quality hardware, he can still experience bad performance if the person he is connecting through uses faulty hardware. In a heterogeneous architecture, end users can, e.g., connect to a mesh backbone which is constructed with hardware of better quality. The nodes which are higher in the hierarchy can be more expensive, as less nodes of higher hierarchy are needed.

Every node in network can interleave between sleep mode and idle mode. Sleeping condition of a node is the condition that every node in the network knows that the node is in sleep mode but that node will interleave between sleep mode and idle mode, during that sleeping condition without revealing to the network. A node can go to sleep mode when it will only receive control packet for some fixed amount of time. The time may not same for each node in the network that is every node will take a random amount of time. When a node ready to go to sleep node it will transmit a control message indicating its address. When all other nodes receive that message they will update their routing table by setting a flag for that node. After a node going to sleep mode it will periodically wake up to idle mode but it will not revel this information to the network. When a node is in sleeping condition and receives a sleep mode message of another node it will just update the table for that node but will not wake up. When a node gets a request to wake up message (RW) then it will reveal that it is wake up by sending a wake up message containing its routing table information to its neighbors. It will remain in wake up state during data packet forwarding or receiving.

Sending and Receiving

When a node is in sleeping condition and wants to transmit data to another node which is in wake up state then first it will wake up and broadcast wake up message along with current routing table information. When its neighbors get wake up message they will also wake up and also update its table and then according to current table information sender will send data packet. When a node wants to send data to another node that is in sleeping condition then it will first broadcast RW message by Flooding. When any sleeping node receive that RW message will wake up and communicate as usually.

Besides this, the routing tables contain information of the nodes which were not active for over a long period of time. So maintaining their information and sending this information over and over again in the form of “full dumps” or to the new node entering the networks is the shear wastage of bandwidth, memory and the battery life of the source and the intermediate nodes. Instead the nodes in the network should be integrated with a clock that will monitor the status of the node. If the node has been inactive or has been in the idle state for a while then the state of the node should automatically be changed into the sleep state. While going in the sleep state it should broadcast the message containing its status, to all the other nodes in the network. Then in the routing table of the nodes should be updated and flag corresponding to the status of that node should be set to 1. Whenever a “full dump” is sent to a new node in the network, it should contain only the IDs of the sleeping nodes with their flag set to 1. When the sleeping node wakes up it will send its information in the form of incremental dump. In this way the size of the routing table can be reduced.

Table 1: DSDV routing table

Destination	NextHop	Metric	Sequence number	Install	Flags	Stable_data
MH_1	MH_2	2	S406_MH_1	T001_MH_4		Ptr1_MH_1
MH_2	MH_2	1	S128_MH_2	T001_MH_4		Ptr1_MH_2
MH_3	MH_2	2	S564_MH_3	T001_MH_4		Ptr1_MH_3
MH_4	MH_4	0	S710_MH_4	T001_MH_4		Ptr1_MH_4
MH_5	MH_6	2	S392_MH_5	T002_MH_4		Ptr1_MH_5
MH_6	MH_6	1	S076_MH_6	T001_MH_4		Ptr1_MH_6
MH_7	MH_6	2	S128_MH_7	T002_MH_4		Ptr1_MH_7
MH_8	MH_6	3	S050_MH_8	T002_MH_4		Ptr1_MH_8

While routing the nodes consider the hop count as the parameter/metric to route packets. But as explained above (theoretically) the nodes can send data easily and efficiently when they have good processing speed. The sent will also be reliable and the overall network performance can be improved. In general the structure of the routing table is as shown in the figure above. There should be a standard set according to which the processors can be manufactured. The standards should be as level 1, level 2, and level 3 and so on.

The sequence number in here is represented as S406_MH$_1$ where S406 is the ID of the device and MH$_1$ is the destination. To consider processing speed as a metric, it should be tagged along the sequence number, for example the sequence number S406_MH$_1$ can be changed to S406_MH$_1$_2 where 2 at the end tell the processing speed according to a predefined standard. This can help the source node to identify and select the route efficiently.

V. RESULTS

In this paper we challenged various scenarios in which the Adhoc networks work. The problems of the Adhoc networks in general were discussed. Hardware issues caused the problems can be easily removed by the cooperation among various vendors. Putting up multiple interfaces could lead to increased capacity of the nodes and argued that, in contrast to what is believed in many research papers, adjusting transmission power is not a measure of freedom but a necessity. Improvement of various transmission parameters can lead to the efficient delivery of packets. The overhead in the DSDV protocol is reduced as it need not transmit the whole routing table over and over again. The required information is given and the rest is received in the form of the incremental dumps.

The sleeping nodes are included into networks and managed efficiently. The routing information about the sleeping node is reduced to a great extent. The route selection by the source node can be done efficiently as it can select between the routes which have less hops or which have greater processing speed. The battery life of the nodes can be saved by automatically changing there state from idle to sleep state and broadcasting the information about its state.

VI. FUTURE WORKS

Mobility in the wireless networks is very popular now days. Many peoples in the street walk and are using small devices like PDA, laptops, or phone to communicate, listening to music, write SMS, exchanging data with other people near them, etc. Routing algorithms are the main challenge. There is still a great deal of work to be done to improve these protocols, the overheads in them, the efficient path finding techniques and removing the unnecessary flooding of the network again and again. Since the nodes are mobile, link between nodes are not symmetric, and the topology are always changed, the routing algorithms used in wired network must be modified or must be invented. The ad hoc networks still have to deal with wireless problems, such as security and higher error rate. Especially MANETs have to consider their power supply, since they are not supported with fixed power supply. It is an important task to extend these results for networks as there are several other measures for network capacity such as transport capacity, information theoretic capacity, and capacity of cooperative nodes.

VII. REFERENCES

[1] Martinus Dipobagio, "An Overview on Ad Hoc Networks"

[2] Gary Breed," Wireless Ad Hoc Networks: Basic Concepts", 2007 Summit Technical Media, pp. 44-46

[3] "Wireless ad hoc networks"

[4] Saleh Ali K.Al-Omari1, Putra Sumari2,"An Overview of Mobile Ad hoc Networks for the Existing Protocols and Applications", International journal on application of graph theory in wireless Adhoc sensor networks, Vol 2 No. 1, March 2010.

[5] M. Shahaya Sheela, A. Sivanantha Raja and V.R. Sarma Dhulipala, "Parametric Analysis of Mobile Ad- Hoc network Environment", International Journal of Computer Applications, Volume 9 No. 9, November 2010.

[6] K. Rajesh Kumar and Dr. S. Radhakrishna,"A Secure Routing Protocol for Mobile Adhoc Network"

[7] Stefan Bouckaert, Dries Naudts, Ingrid Moerman, and Piet Demeester,"Making ad hoc networking a reality: problems and solutions", Journal of Telecommunications and Information Technology, January 2008.

[8] Nayan Ranjan Paul, Laxminath Tripathy and Pradipta Kumar Mishra, "Analysis and Improvement of DSDV Protocol", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011

[9] K. Tamizarasu and M. Rajaram ,"Analysis of AODV Routing Protocol for Minimized Routing Delay in Ad Hoc Networks", International Journal on Computer Science and Engineering (IJCSE).

[10] http://www.cs.unibo.it/bison/progress/adhoc.shtml

[11] http://computer.howstuffworks.com/mote3.html

[12] http://www.adhocnets.org/2010/index.html

[13] Muazzam Ali Khan Khattak, Khalid Iqbal, Prof Dr. Sikandar Hayat Khiyal," Challenging Ad-Hoc Networks under Reliable & Unreliable Transport with Variable Node Density", Journal of Theoretical and Applied Information Technology, 2008

[14] Hossein Pishro-Nik and Faramarz Fekri ,"Analysis of Wireless Ad-Hoc and Sensor Networks in Finite Regime"

[15] Mihaela Cardei and Jie Wu ,“Energy-Efficient Coverage Problems in Wireless Ad Hoc Sensor Networks”, 2007

[16] Shobha.K.R and Dr.K.Rajanikanth, “Adaptive AODV Routing Protocol for Mobile Adhoc Networks”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.1, March 2011

[17] Padmini Misra, “Routing Protocols for Ad Hoc Mobile Wireless Networks”, Routing Protocols for Ad Hoc Mobile Wireless Networks, 2007

[18] http://www.cis.ohio-state.edu/~misra

[19] F. L. LEWIS, “Wireless Sensor Networks”, Smart Environments: Technologies, Protocols, and Applications, 2004

[20] Vijayalakshmi, M. Avinash Patel and Linganagouda Kulkarni, “Qos Parameter Analysis on AODV and DSDV Protocols In A Wireless Network”, Indian Journal of Computer Science and Engineering Vol. 1 No. 4 283-294