FAULT TOLERANCE WITH MULTI ROUTE AODMV IN WIRELESS MESH NETWORK

Enrol. No. -	112217
Name of Student -	Uday Singh Kushwaha
Name of supervisors -	Prof. Dr. Satya Prakash Ghrera & Dr. Pradeep Kumar Gupta

September-2014

Submitted in partial fulfilment of the Degree of

Master of Technology

DEPARTMENT OF COMPUTER SCIENCE & ENGINNERING

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY UNIVERSITY,

WAKNAGHAT, DISTT: SOLAN (H.P), INDIA

FAULT TOLERANCE WITH MULTI ROUTE AODMV IN WIRELESS MESH NETWORK

Enrol. No. -	112217
Name of Student -	Uday Singh Kushwaha
Name of supervisors -	Prof. Dr. Satya Prakash Ghrera & Dr. Pradeep Kumar Gupta

September-2014

Submitted in partial fulfilment of the Degree of

Master of Technology

DEPARTMENT OF COMPUTER SCIENCE & ENGINNERING

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY UNIVERSITY,
WAKNAGHAT, DISTT: SOLAN (H.P), INDIA

TABLE OF CONTENTS

CERTIFICATE

This is to certify that the work titled **"Fault Tolerance with Multi Route AODMV in Wireless Mesh Network"** submitted by **"Uday Singh Kushwaha"** in partial fulfilment for the award of degree of Master of Technology of Jaypee University of Information Technology University, Waknaghat has been carried out under our supervision. This work has not been submitted partially or wholly to any other University or Institute for the award of this or any other degree or diploma.

Signature of Supervisor: …………………….............
Name of Supervisor: Prof. Dr. Satya Prakash Ghrera
Designation: Head, Dept. of CSE & ICT
Date ……………………..

Signature of Supervisor: …………………….............
Name of Supervisor: Dr. Pradeep Kumar Gupta
Designation: Assistant Professor, Dept. of CSE & ICT
Date ……………………..

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to my advisors Prof. Dr. Satya Prakash Ghrera & Dr. Pradeep Kumar Gupta for their guidance and support. Their extreme energy, creativity and excellent coding skills have always been a constant source of motivation for me. The perfection that he brings to each and every piece of work that he does always inspired me to do things right at first time. He is a great person and one of the best mentors, I always be thankful to them.

I would also like to thank all the faculty members for devoting their time in discussing ideas with me and giving their invaluable feedback. I would like to thank all PhD scholars and Lab staff in JUIT for making our lab such a great place to work. Thanks to all admin staff for supporting me for this thesis work. Special thanks to Mr. Punit and my all friends who always encourage me.

I would like to dedicate this thesis to my amazingly loving and supportive parents who have always been with me, no matter where I am.

Signature of Student: ………………………............
Name of Student: Uday Singh Kushwaha
Roll no: 112217
Date ……………………..

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

One of the main challenges of Wireless Mesh Network is the design of robust routing algorithms that adapt to the frequent and randomly changing network topology and provide various alternate routes from source to destination. According to the connectivity or propagation state, the network topologies are changed dynamically and may fluctuate from time to time. Because of these regular changes of the network topologies, formation and maintenance of the network is to be difficult. The main reason of topology changes is the mobility of nodes. As in WMNs nodes can move freely, the resulting of the topology alteration in the network must be acknowledged to the other nodes so that outdated topology information should be removed or updated. Many reactive and proactive routing protocols have been proposed that is based on single path and multiple paths to solve this problem. Due to the mobility of nodes, single path algorithms are not sufficient for routing thus multipath algorithm is required. Several multipath algorithms have been proposed for this purposed. It maintains various alternate routes to support the ongoing connections, when primary path of route is broken then alternate route is used for sending packets towards the destination and thus lowers the packet drop rate. In cases where no alternate paths are available at any node during failure, route discovery has to restart from source. Since WMNs nodes are either fixed or independent to move in any direction; there may be frequent link breakage. Due to frequent link failure WMNs protocols should have mechanism to repair path locally to reduce latency for route recovery.

The Ad hoc On Demand Multipath Distance Vector (AOMDV) Routing Protocol is one of the most commonly used reactive protocols for multipath routing in Wireless mesh networks. AOMDV performs well, but it does not has local repair capabilities such as it uses backup route for further transmission during the failure but when no back-up route is available it restart route discovery from source to destination that degrades throughput and increases end to end delay. To overcome this problem, we present an AOMDV protocol with local repair capabilities (AOMDV-LR). In this approaches intermediate nodes in the existing paths try to find new path to the destination in the event of link failure and when no alternate route available.

Keywords: Wireless Mesh Networks, Ad-hoc routing, Routing Protocols, Back-up routes, RREQ, RREP, RERR, AOMDV with Local Repair (AOMDV-LR)

CHAPTER 1

INTRODUCTION TO WIRELESS MESH NETWORKS

Introduction
Network architecture
Characteristics
Application scenarios
Critical factors influencing network performance
Capacity of WMNs
Cause of Failure
Required Hardware and Software

INTRODUCTION TO WIRELESS MESH NETWORKS

1.1 Introduction

Wireless mesh networking is a promising communication paradigm for next generation wireless networks. Wireless Mesh Networks (WMNs) include Mesh Clients (MCs) and Mesh Routers (MRs), where MRs form a wireless infrastructure/backbone and supply interconnection with the wired networks to extend the Internet connectivity to the MCs as shown in fig1. Mesh networks are planned/unplanned multi-hop wireless networks [1]. Mesh routers generally have minimal mobility in a mesh network and form the backbone of WMNs. The clients possibly will be either at a halt or mobile and can form self organized ad hoc networks which can uses services by relaying requests to wireless backbone network .This type of network is very attractive in developing countries or in the sparsely populated rural areas where infrastructure is either non- existent or prohibitively expensive. Due to this intrinsic property, WMNs have become the focus of research to increase the coverage range with low cost and easy deployment [2]. WMNs are considered as a superset of traditional mobile ad-hoc networks (MANETs), where the network is comprised of mobile client devices (MESH CLIENTs).

As various wireless networks grow into the next generation to offer better services, wireless mesh networks (WMNs), has emerged recently as a key technology. Each node works not only as a single host but also act as a router that frontward packet on behalf of other nodes that may not be in wireless transmission range of their destinations. WMNs are dynamically self-organized and self-configured network with the nodes in the network involuntarily establishing and maintaining mesh connectivity surrounded by them. This feature brings lots of advantages to WMNs such as easy network maintenance, low up-front cost, robustness, and trustworthy service coverage.

Conventional nodes (e.g., desktops, phones, laptops, PDAs, etc.) are equipped with wireless network interface cards (NICs) that can be connected directly to wireless mesh routers. Nodes that do not contain wireless NICs may also access WMNs through connecting to wireless mesh routers via, for example, Ethernet. Hence, WMNs will truly help the users to be always online anytime anywhere. Additionally, the gateway/bridge functionalities in mesh routers facilitate the incorporation of WMNs with various existing wireless networks such as cellular, wireless sensor, wireless-fidelity (Wi-Fi), and worldwide interoperability for microwave access, WiMedia networks.

WMN is a hopeful wireless technology for various purposes [3], e.g., broadband home networking, neighborhood networks community and, enterprise networking, etc. It is ahead significant attention as an achievable way for cash impecunious Internet service providers (ISPs), carriers, and others to roll out robust and trustworthy wireless broadband service access in a way that needs negligible upfront investments. With the capability of self-organization and self-configuration, WMNs can be planned incrementally, one node at a time, as required. Like additional nodes are installed, the consistency and connectivity for the users increase accordingly.

Installation of WMN is not too difficult task, because all the required components are already available in the form of ad hoc network routing protocols, IEEE 802.11 MAC protocol, wired equivalent privacy (WEP) security, etc. numerous companies have previously realized the potential of this technology and recommend wireless mesh networking products.

1.2. Network architecture [1]:

WMN includes of two types of nodes: mesh routers and mesh clients, wireless mesh router include bonus routing activity to sustain mesh networking with gateway and repeater task as in conventional wireless router. A mesh router is usually outfitted with several wireless interfaces built on either the same or dissimilar wireless access technologies to further enhance the flexibility of mesh networking. A wireless mesh router can attain the same coverage with lower transmission power through multi hop communications with compared to a conventional wireless router. Optionally, the medium access control (MAC) protocol in the mesh router is enhanced with improved scalability in a multi-hop mesh atmosphere. Mesh clients also perform essential functions for mesh networking; hence these can also act as a router. However, gateway or bridge functions do not exist in mesh client. Mesh clients usually have only one wireless interface. The hardware and the software platform for mesh clients can be much simpler than mesh routers. Mesh clients comes under higher variety of devices compared to mesh routers.

The architecture of WMNs can be categorized as follows:

1.2.1. Infrastructure/Backbone WMNs: The architecture as shown in Figure 1.1, where dash lines indicate wireless and solid lines indicate wired links. This type of WMNs includes mesh routers that creates an infrastructure for mesh clients that can be connected to them. The WMN infrastructure/ backbone are built using various types of radio technologies, besides to the mostly used IEEE 802.11 technologies. Mesh routers create a mesh network with self-configuring and self-healing links between themselves. With gateway functionality, mesh routers is connected to the Internet. This approach, also known as infrastructure meshing, offer backbone for conventional clients and facilitate incorporation of WMNs with existing wireless networks, through bridge/gateway functionalities in the mesh routers. Client nodes with ethernet interface are connected to mesh routers by Ethernet links. For client nodes can communicate directly with mesh routers with the same radio technologies as mesh routers. If radio technologies are different, clients have to communicate with the home stations that contain Ethernet connections for mesh routers.

Most commonly Infrastructure/Backbone type WMNs are used. For example, by using infrastructure meshing community and neighborhood networks can be built. The mesh routers can be placed on the roof of houses may be in neighborhoods, which act as an access points for users who are inside the homes and along the streets or roads. Two types of radios are used in the routers; for user communication, and for backbone communication. By using long-range communication techniques including directional antennas the mesh backbone communication may be established.

1.2.2. Client WMNs. Client meshing offers peer-to-peer networks among client devices. In Client WMNs architecture, the actual network to perform routing and configuration functionalities as well as it provides end-user applications to customers are composed by client nodes. Hence, no need of mesh for these types of networks. The basic architecture of client meshing is shown in Figure 1.2. In Client WMNs, a packet deliberated to a destination node in the network hops through several nodes to arrive the destination. Client WMNs are usually formed using single type of radios on all client devices. Moreover, the necessities on end-user devices is increased when compared to infrastructure meshing, as, in Client WMNs, the end-users must perform additional functions such as routing and self configuration.

1.2.3. Hybrid WMNs. These types of architecture are the combination of infrastructure and client meshing as shown in Figure 1.3. Mesh clients access the network through mesh routers as well as directly meshing with other mesh clients. Whereas the infrastructure makes available connectivity to other networks such as the Internet, cellular, Wi-Fi, WiMAX, and sensor networks; the routing capabilities of clients offer enhanced connectivity and coverage inside the WMN.

1.3. Characteristics

Characteristics of Wireless Mesh Networks (WMNs) are explained as follows:

1.3.1. Multi-hop wireless network. An objective of WMNs is to extend the coverage range of current wireless networks without sacrificing the channel capacity. Another goal is to provide non-line-of-sight (NLOS) connectivity between the users without direct line-of-sight (LOS) links. To gather these requirements, the mesh style multi hopping is indispensable, which achieves higher throughput without surrender effective radio range via shorter link distances, less interference among the nodes, and more efficient frequency reuse.

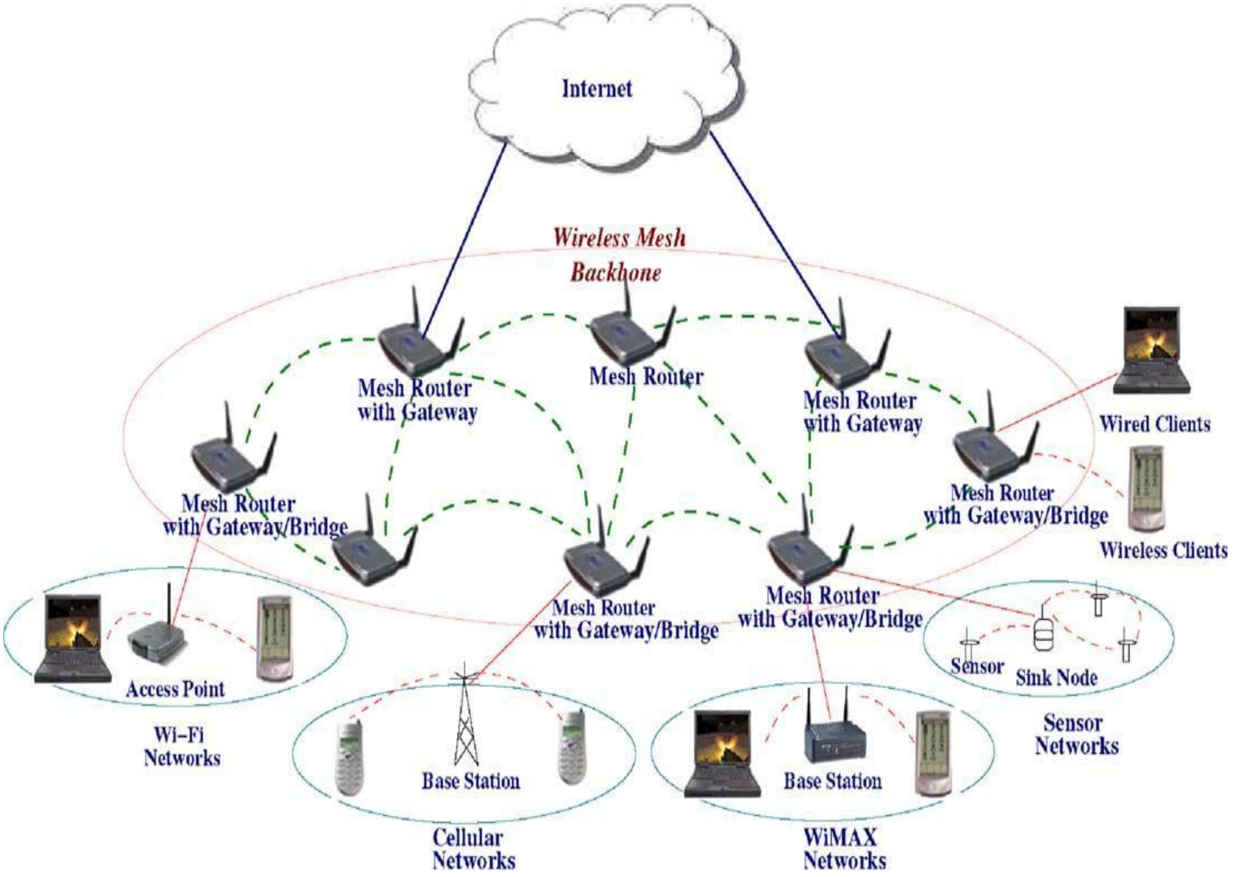


Figure 1.1 Infrastructure/backbone WMNs. [1]

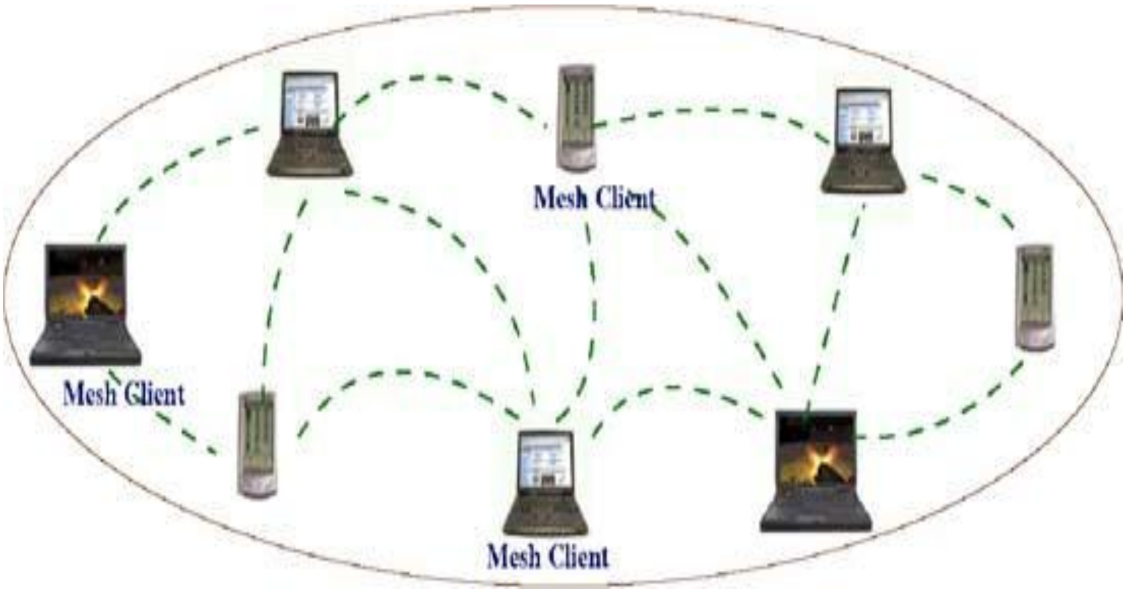


Figure 1.2 Client WMNs.

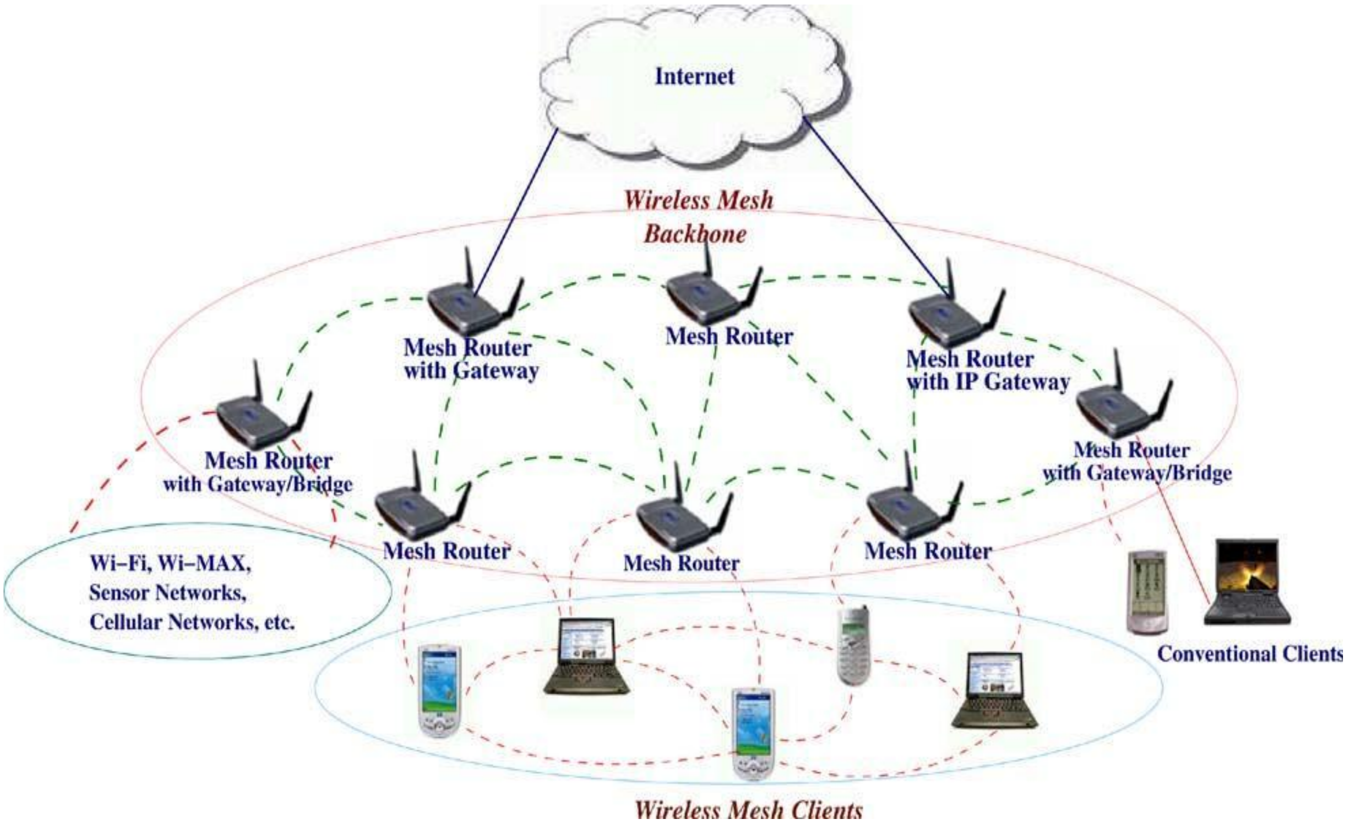

Internet
Wireless Mesh Backbone
Mesh Router with Gateway
Mesh Router
Mesh Router with IP Gateway
Mesh Router with Gateway/Bridge
Mesh Router with Gateway/Bridge
Mesh Router
Mesh Router
Mesh Router
Wi–Fi, Wi–MAX, Sensor Networks, Cellular Networks, etc.
Conventional Clients
Wireless Mesh Clients

Figure 1.3 Hybrid WMNs [1]

1.3.2. Support for ad hoc networking: WMNs offers capability of self-forming, self-healing, and self-organization. It enhances network performance, due to easy deployment and configuration, fault tolerance, and mesh connectivity i.e., multipoint-to-multi-point communications and flexible network architecture. Because of these features, WMNs have low upfront investment requirement, and the network can grow increasingly as needed.

1.3.3. Dependence of power consumption constraints on the type of mesh nodes. Mesh routers usually do not have exact limit on power consumption. However, mesh clients may require power efficient protocols. As an example, a mesh capable sensor needs its communication protocols to be power proficient. Thus, routing protocols or the MAC optimized for mesh routers may not be appropriate for mesh clients such as sensors, because power efficiency is the prime concern for wireless sensor networks.

1.3.4. Mobility dependence on the type of mesh nodes. Mesh clients can be stationary or mobile nodes while mesh routers usually have minimal mobility.

1.3.5. Multiple types of network access. In WMNs, both peer-to-peer (P2P) communications and backhaul access to the Internet are supported. In addition, the incorporation of WMNs with other wireless networks and providing services to end-users of these networks can be consummate through WMNs.

1.3.6. Compatibility and interoperability with existing wireless networks. WMNs built based on IEEE 802.11 technologies [4] must be compatible with IEEE 802.11 standards i.e. support for both mesh capable and conventional Wi-Fi clients. Such WMNs also require being interoperable with other wireless networks such as WiMAX, Zig-Bee, and cellular networks.

Based on their characteristics, in general WMNs are considered as a type of ad-hoc networks because of lack of wired infrastructure that subsist in cellular or Wi-Fi networks through deployment of base stations or access points. While ad hoc networking techniques are requisite by WMNs, the additional capabilities require more sophisticated algorithms and design principles for the apprehension of WMNs. More specifically, instead of being a type of ad-hoc networking, WMNs aim to expand the capabilities of ad hoc networks. Therefore, ad hoc networks can actually be considered as a subset of WMNs. To demonstrate this point, the differences between WMNs and ad hoc networks are summarized below. In this comparison, the hybrid architecture is considered, because it comprises all the advantages of WMNs.

1.3.7. Wireless infrastructure/backbone. WMNs include wireless backbone with mesh routers. The wireless backbone offers large connectivity, large coverage robustness in the wireless domain. On the other hand, the connectivity in ad hoc networks depends on the individual contributions of end-users which may not be trustworthy.

1.3.8. Integration. WMNs support conventional clients that utilize the same radio technologies as a mesh router. It is accomplished through a host routing function presented in mesh routers. WMNs also make possible integration of a variety of existing networks such as Wi-Fi, the Internet, and cellular and sensor networks passing through gateway/bridge functionalities in the mesh routers. Consequently, through the use of the wireless infrastructure, users in a network are provided with services in other networks. The integrated wireless networks through WMNs resemble the Internet backbone, because the physical location of network nodes becomes less important than the capacity and network topology.

1.3.9. Mobility. Since ad hoc networks offer routing using the end-user devices, the network topology and connectivity depend on the movement of users. These oblige additional challenges on routing protocols as well as on network configuration and deployment.

1.3.10. Dedicated routing and configuration. In the ad hoc networks, routing and configuration functionalities for all other nodes are performed by end-users devices. On the other hand, WMNs contain mesh routers for these functionalities. Therefore, the load on end-user devices is significantly reduced, which provides inferior energy consumption. Furthermore, the end-user requirements are limited which reduces the cost of devices that can be used in WMNs.

1.3.11. Multiple radios. Mesh routers can be organized with multiple radios to achieve routing and access functionalities. This enables disjointing of two main types of traffic in the wireless domain. While routing and configuration are executed between mesh routers, the access of network by end users can be carried out on a dissimilar radio. This significantly advances the capacity of the network. Alternatively, in ad hoc networks, these functionalities are executed in the same channel; hence the performance decreases of the network.

1.4. Application scenarios

1.4.1. Broadband home networking. Currently broadband home networking is comprehended through IEEE 802.11 WLANs. An obvious trouble is the location of the access points. Without a site inspection, a home usually has many dead zones lacking service coverage. Solutions based on site inspection not realistic for home networking and also become expensive. Because of Ethernet wiring from access points to backhaul network access modem or hub, installation of multiple access points for home networking is also expensive and not perfect. Furthermore, under two different access points communications between end nodes have to go all the way back to the access hub. Installation of multiple access points is not an efficient solution, mainly for broadband networking. Figure 1.4 depicts the Mesh networking that can solve all these issues related to home networking.

By wireless mesh routers with mesh connectivity the access points should be substituted and set up among them. Consequently, to network faults and link failures the communication among these nodes becomes much more flexible and robust. By adding mesh routers and changing locations of mesh routers dead zones can be also eliminated or involuntarily adjusting power levels of mesh routers. Without going back to the access hub continually communication inside home networks can be realized through mesh networking. Thus, due to backhaul access network congestion can be keep away from network. In this application, wireless mesh routers have no restriction on power consumptions and mobility. Therefore, protocols proposed for mobile ad hoc networks [5] and wireless sensor networks are too cumbersome to achieve satisfactory performance in these applications. In contrast Wi-Fis are not competent of supporting ad hoc multi hop networking. Consequently, WMNs are well-suited for broadband home networking.

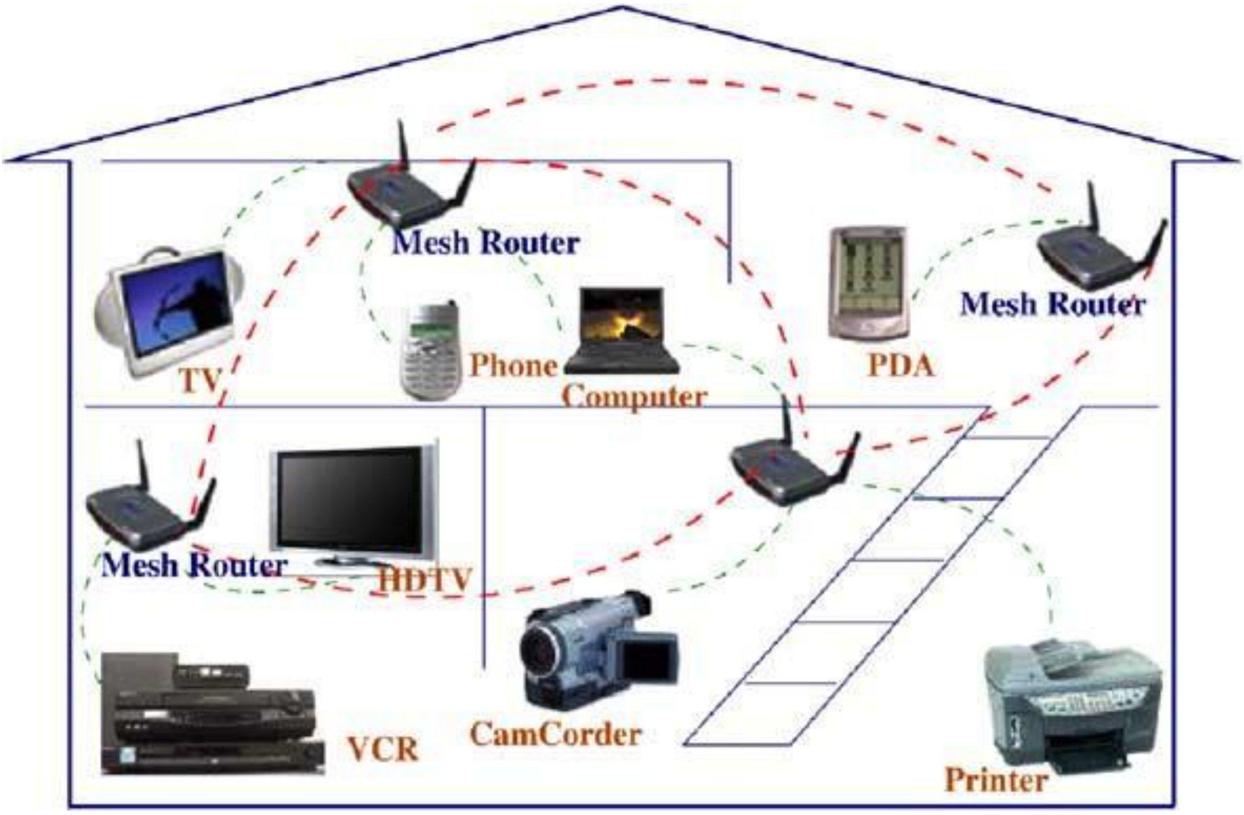


Figure 1.4 WMNs for broadband home networking.

1.4.2. Community and neighborhood networking. Inside a community network, the regular architecture for network access is based on cable or DSL that are connected to the Internet, and the end hop is wireless with connecting a wireless router to a cable or DSL modem. This type of network access has several drawbacks:

- Since all traffic must flow through Internet, it significantly reduces network resource utilization.
- Large percentage of areas in between houses is not covered by wireless services.
- Only single path may be available for individual home to access the Internet or communicate with neighbors.

WMNs eliminate the above disadvantages through more flexible mesh connectivity between homes, as shown in Figure 1.5. WMNs can also permit many applications such as distributed file storage, distributed file access, and video streaming.

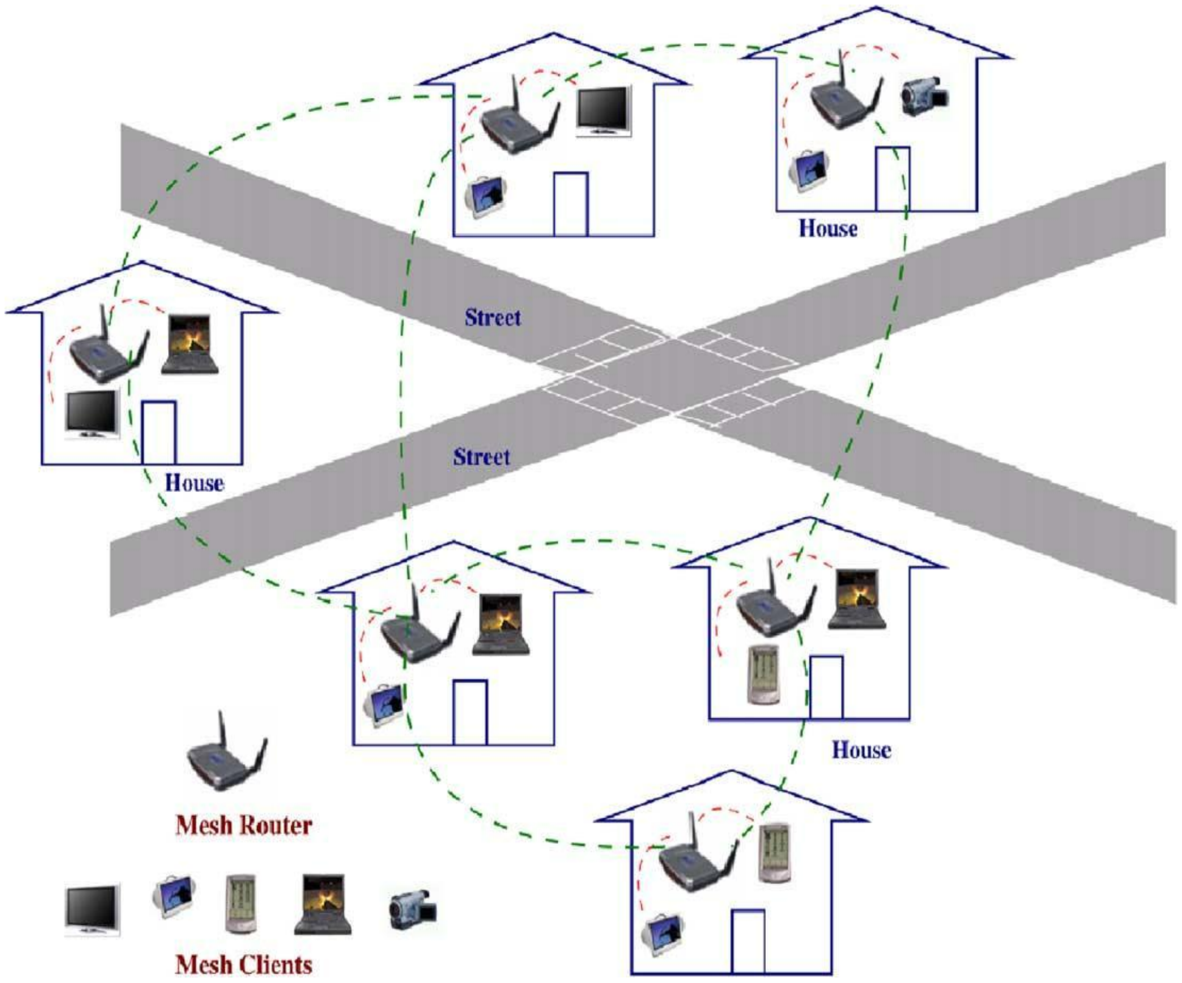


Figure 1.5 WMNs for community networking.

1.4.3. Metropolitan area networks. WMNs in metropolitan area have numerous rewards. The physical layer transmission rate in WMNs is much higher than that in any cellular networks node. For example, an IEEE 802.11g node can transmit at a rate of 54% Mbps. Furthermore, the communication between nodes in WMNs does not rely on a wired backbone. Wireless mesh MAN is a profitable alternative to broadband networking as compared to wired networks (e.g., cable or optical networks) particularly in under developed regions. Wireless mesh MAN covers a potentially much superior area than home, building, enterprise, or community networks, as shown Figure 1.6. Therefore, the requisite on the network scalability by wireless mesh MAN is much higher than that by other applications.

1.4.4. Enterprise networking. This may be a small network within an office or a medium-size network for all offices in a complete building, or a large scale network between offices in multiple buildings. At present, standard IEEE 802.11 wireless networks are commonly used in various offices. Connections between them have to be achieved through wired Ethernet connections, which is the key reason for the expensiveness of enterprise networks. Additionally, adding more backhaul access

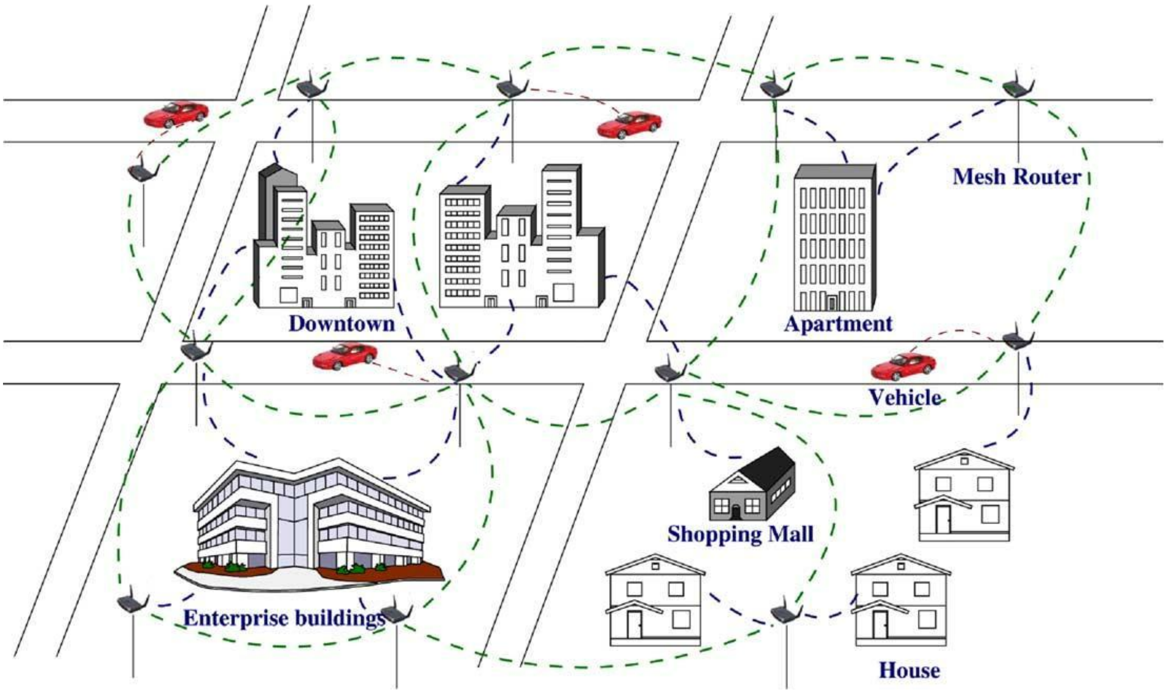


Figure 1.6 WMNs for metropolitan area networks.

Modems only enlarges capacity close by, but does not get better robustness to link failures, network congestion and other troubles of the entire enterprise network. If the access points are substituted by mesh routers, as shown in Figure 1.7, Ethernet wires can be eradicate. Multiple backhaul access modems can be shared by all nodes in the entire network, and hence, advance the robustness and resource utilization of enterprise networks. WMNs can rise easily as the size of enterprise increased. WMNs for enterprise networking are much more complex than at home because more nodes and more complex network topologies are involved. The service model of the enterprise networking may be applied to many other public and commercial service networking scenarios such as hotels, airports, convention centers, shopping malls, sport centers, etc.

1.4.5. Transportation systems. Instead of limiting accesses of IEEE 802.11 or 802.16 to stations and stops, mesh networking technology can expand access into buses and trains etc. Thus, opportune traveler information services, distant monitoring of in vehicle security video and driver communications can be maintained. To permit such mesh networking for a transport system, two key techniques are needed: mobile mesh networks within the vehicle and the high-speed mobile backhaul from a vehicle to the Internet, as shown in Figure 1.8.

1.4.6. Building automation. Under a building, various electric devices including light, elevator, power, air conditioner, etc., require to be controlled and monitored. Presently this job is accomplished through standard wired networks, which are very costly due to the complexity in

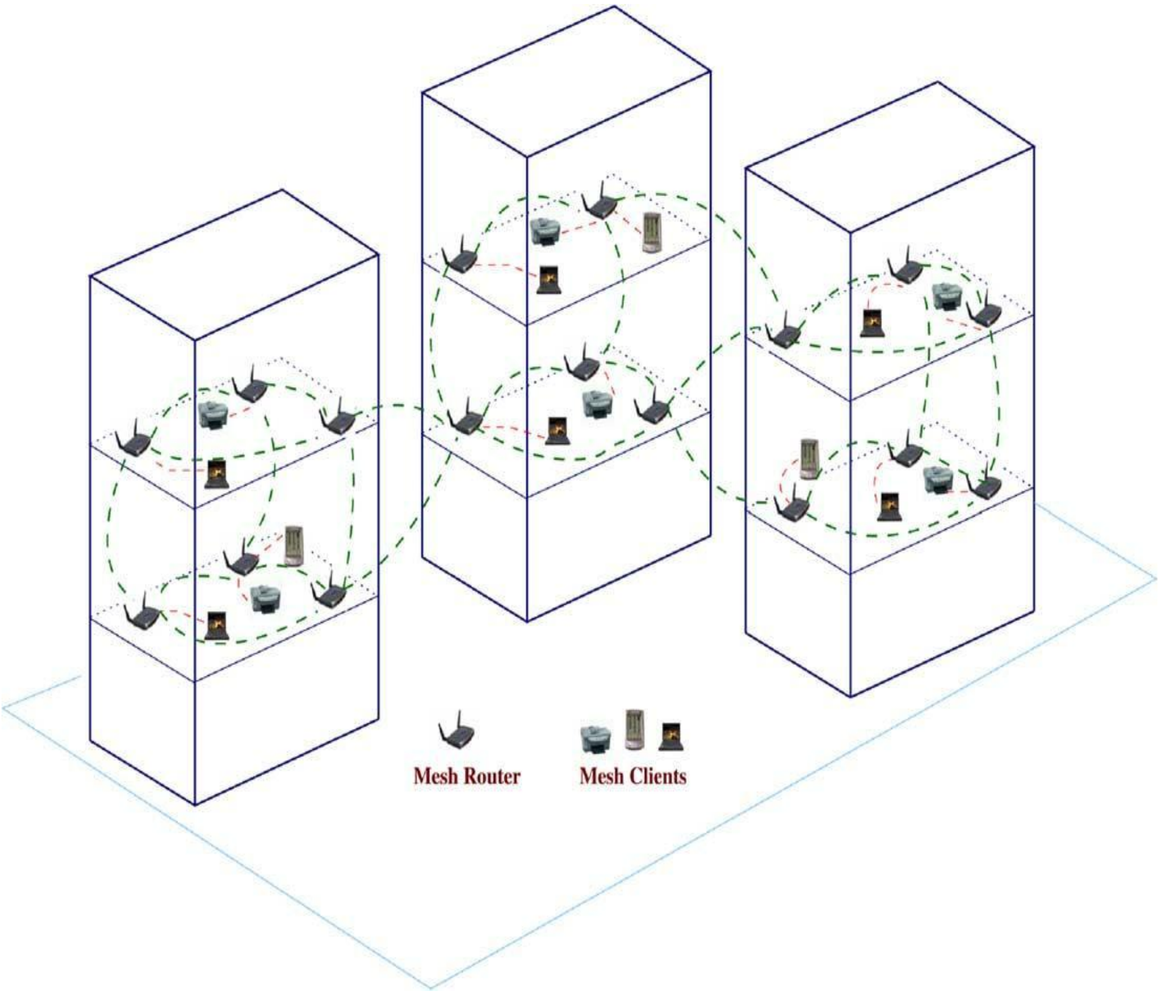


Figure 1.7 WMNs for enterprise networking

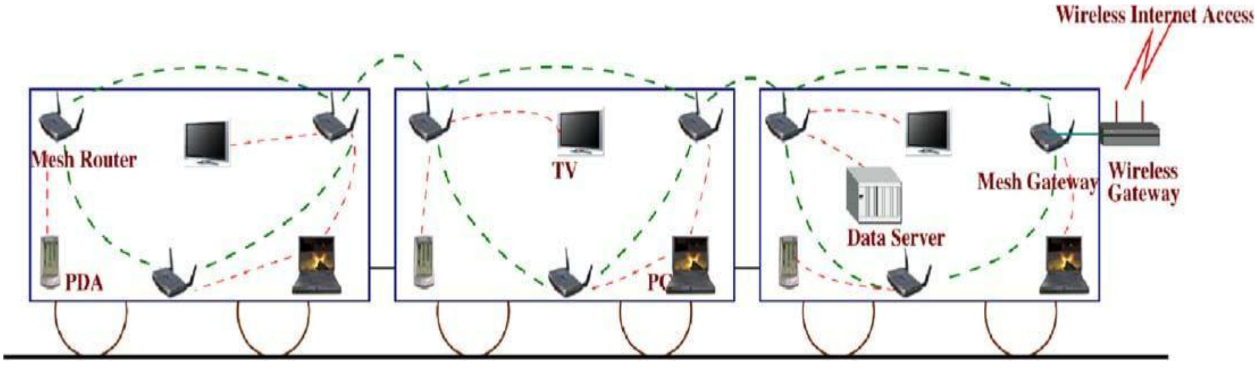


Figure 1.8 WMNs for transportation systems

deployment and preservation of a wired network. Freshly Wi-Fi based networks have been accepted to reduce the cost of wired networks. However, this attempt has not accomplished satisfactory performance yet, since deployment of Wi-Fi s for this application is still quite expensive due to wiring of Ethernet. If access points are replaced by mesh routers, in BACnet (building automation and control networks) as shown in Fig. 1.9, the deployment cost will be considerably reduced. The deployment procedure is also much simpler due to the mesh connectivity between wireless routers.

1.4.7. Security supervision systems. As security is turning out to be a extremely high apprehension, security surveillance system becomes a necessity for enterprise buildings, shopping malls, grocery stores, etc. Consecutively to organize such systems at locations as needed, WMNs are a much more feasible solution than wired networks to connect all devices. Since still images and videos are the chief traffic flowing in the network, this application stress much higher network capacity than other applications.

1.4.8. Health and medical systems. In hospital or medical center, monitoring and diagnosis of data are required to be processed and transmitted from one room to another for various purposes. Data transmission is usually done by broadband, as high resolution medical images and various periodical monitoring information can be easily produced a constant and large volume of data. Traditional wired networks can only offer limited network access to assured fixed medical devices. Wi-Fi support networks must rely on the existence of Ethernet connections, which may basis of high system cost and complexity but without the capability to eliminate dead spots. However, these issues do not be present in WMNs.

Since copious applications can be supported by WMNs, it is infeasible to have an entire list of them. Here, depending on the functions for WMNs, we classify applications of WMNs into numerous classes:

- **Internet access.** Several Internet applications offer significant timely information to people, build life more convenient, and enlarge work efficiency and productivity. For instance, email, search engine such as Google, online actions like chatting, video streaming, eBay, online purchase, etc., have become a requisite part of life. Therefore, people are attracted to subscribe the Internet. In home or small/medium business surroundings, the most trendy network access solution is still DSL or cable modem along with IEEE 802.11 access points. Nonetheless, comparing with this approach, WMNs have many prospective advantages: higher speed, lost cost, and easy installation. Consequently, Internet admission will significantly motivate the development of WMNs.

- **Distributed information storage and sharing within WMNs.** For this type of applications, backhaul access to the Internet is not obligatory. Users of these applications commune within WMNs. A user may desire to store soaring volume data in disks possessed by other users, query/retrieve information located in distributed database servers and download files from other disks based on peer-to-peer networking mechanism. Users inside WMNs may also want to chat,

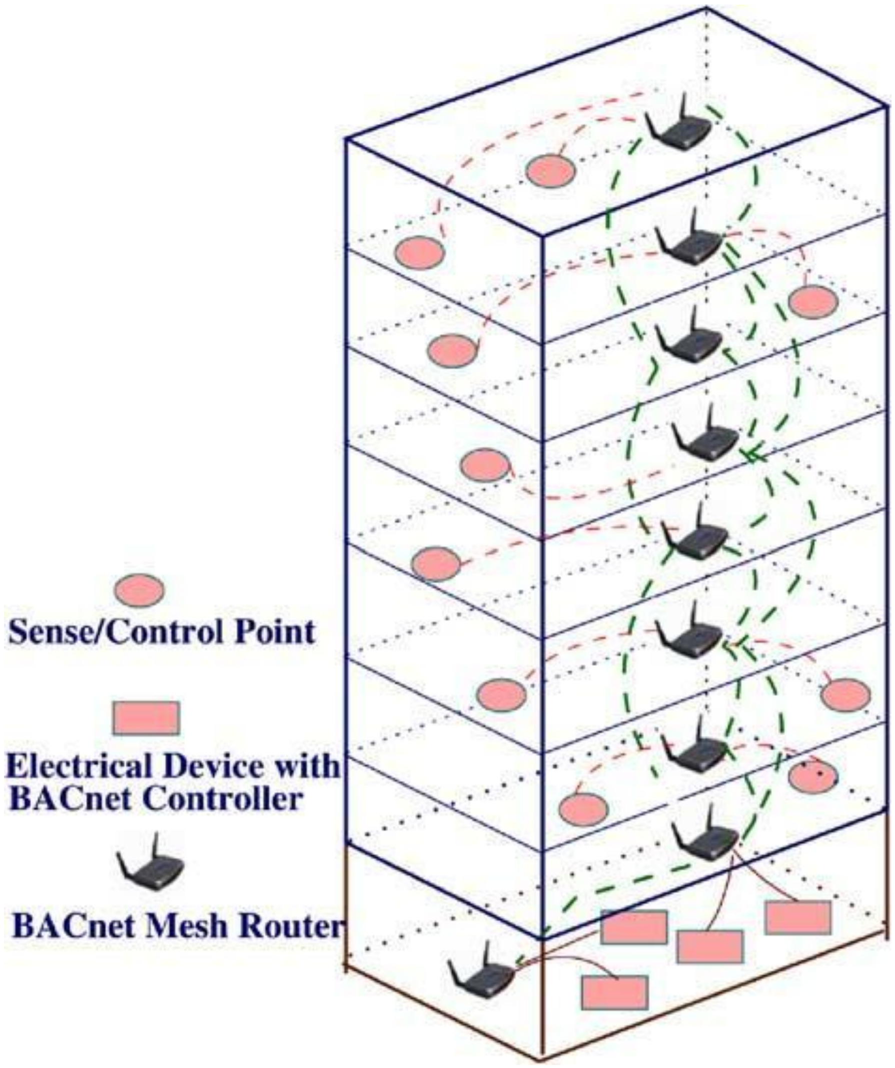


Figure 1.9 WMNs for building automation..

play games with each other and talk on the video phone. To have these applications work at the end users, certain protocols have to exist in the application layer.

• **Information exchange across multiple wireless networks.** Again, this type of applications does not require backhaul access to the Internet. For instance, when a cellular phone communicates to a Wi-Fi phone through WMNs, no Internet is needed. Likewise, a user on a Wi-Fi network may expect to examine the status in different sensors in a wireless sensor network. All these applications must be supported by new procedure/protocol or software in the application layer of the end-users.

Additionally to the above applications, WMNs may also be applied to Spontaneous Networking and Point to point Communications. For example, wireless networks for an vital situation, response team and firefighters do not have knowledge in advance where the network should be deployed. By placing wireless mesh routers in desired locations, a WMN can be speedily established. For a community holding devices with wireless networking capability, (e.g. laptops and PDAs) P2P communication anytime anywhere is a proficient solution for information sharing. WMNs are capable to meet this demand. These applications demonstrate that WMNs are a superset of ad hoc networks, and thus can be accomplished all functions provided by ad hoc networking.

1.5. Critical factors influencing network performance

Before designing, designed and deploying a network all subsequent factors that critically influence its performance need to be considered. For WMNs, the critical factors are summarized as follows:

1.5.1. Radio techniques.

Driven by the hasty progress of semiconductor, RF technologies, and communication theory, wireless radios have undergone a momentous revolution. Currently many approaches have been proposed to augment capacity and flexibility of wireless systems. Typical instances include directional and smart antennas, multi-radio/multi-channel systems and MIMO systems, to date; MIMO has turn into one of the key technologies for IEEE 802.11n, the high speed extension of Wi-Fi. Multiradio chipsets and their expansion platforms are available on the market.

1.5.2. Scalability:

As Multi hop communication is extensive ranging in WMNs. when the size of network augment, the network performance mortify significantly, For multi-hop networking it is well recognized that communication protocols undergo from scalability issue. Transport protocols can be unable to find, it may also possible that routing protocols not be able to discover a consistent routing paths, and MAC protocols may experience remarkable throughput lessening. As an illustrative pattern, current IEEE 802.11 MAC protocol and its derivatives cannot attain a levelheaded throughput seeing that the number of hops increases to 4 or higher. The reason for low scalability is that the end-to-end trustworthiness sharply drops as the degree of the network increases. In WMNs, because of its ad hoc architecture, the centralized multiple access schemes for instance TDMA and CDMA are not easy to employ due to their complexities and a general obligation on timing synchronization for TDMA (and code management for CDMA). When a distributed multihop network is painstaking, truthful timing synchronization within the global network is difficult to achieve. Therefore, distributed multiple access schemes for example CSMA/ CA are more encouraging. However, CSMA/CA has very low frequency spatial reuse competence, which radically limits the scalability of CSMA/CA based multi-hop networks.

1.5.3. Mesh connectivity.

Numerous advantages of WMNs originate from mesh connectivity which is a significant requirement on protocol design, particularly for MAC and routing protocols. Network self organization and topology control algorithms are commonly needed. Topology conscious MAC and routing protocols can considerably improve the performance of WMNs.

1.5.4. Broadband and QoS.

Dissimilar from other ad hoc networks, the majority applications of WMNs are broadband services with different QoS requirements. Therefore, in addition to end-to-end transmission delay and fairness, more performance metrics such as delay jitter, aggregate and per node packet loss ratios and throughput must be measured by communication protocols.

1.5.5. Compatibility and inter-operability.

It is a preferred feature for WMNs to sustain network access for both usual and mesh clients. Therefore, WMNs require being backward compatible with usual client nodes; otherwise, the enthusiasm of deploying WMNs will be significantly compromised. Incorporation of WMNs with other wireless networks requires definite mesh routers to have the capability of interoperation between diverse wireless networks.

1.5.6. Security.

Without a persuasive security solution, WMNs will not be capable to thrive due to lack of incentives by customers to pledge to reliable services. Though numerous security schemes have been proposed for wireless LANs, they are still not ready for WMNs. For example, there is no centralized reliance authority to deal out a public key in a WMN because of the distributed system architecture. The existing security schemes proposed for ad hoc networks may be adopted for WMNs, but numerous issues exist:

- Most security solutions for ad hoc networks are still not older adequate to be practically implemented.
- The network architecture of WMNs is different from a usual ad hoc network, which causes differentiation in security mechanisms.

1.5.7. Ease of use.

Protocols are required to be designed to facilitate the network to be as autonomous as probable, in the sense of power management, self-organization, and dynamic topology control, robust to momentary link failure, and fast user-authentication procedure /network subscription. In addition, network management tools require to be developed to efficiently preserve the operation, configure the parameters of WMNs and monitor the performance. These tools collectively with the autonomous mechanisms in protocols will facilitate hasty deployment of WMNs.

1.6. Capacity of WMNs

The capacity of WMNs is exaggerated by several factors such as network architecture, network node density, network topology, traffic pattern, number of channels used for each node, node mobility and trans-mission power level. A clear understanding of the connection between network capacity and the above issue provide a guideline for protocol architecture design, development, deployment and operation of the network.

Capacity analysis

In the last decade, much research has been accepted out to study the capacity of ad hoc networks which can be adopted to examine the capacity of WMNs.

For a motionless multi hop network, it has been shown that the most favorable transmission power level of a node is reached when the node has six neighboring nodes. With this value, an best possible tradeoff is achieved between the number of hops from source to destination and the channel spatial reuse effectiveness. This result is helpful for infrastructure WMNs with least mobility. When the mobility is a anxiety as in hybrid WMNs, no theoretical results are reported so far. Analytical lower and upper boundaries of network capacity are given in [6]. From the analytical outcomes, it follows that the throughput capacity per node condenses considerably when the node density enhances. A significant implication is derived in [6] as a guideline to advance the capacity of ad hoc networks: A node must communicate with only nearby nodes. To put into practice this idea, two major schemes are suggested in [6]:

- Throughput capacity may be enlarged by deploying relaying nodes.
- Nodes require to be grouped into clusters.

Therefore, communications of a node with any more nodes that is not close by must be conducted through relaying nodes or clusters. On the other hand, these schemes have confines. In the first scheme, a extremely huge number of relaying nodes are required in order to enlarge the throughput by a momentous percent. This will absolutely enlarge the overall cost of a network. In the second scheme, clustering nodes in ad hoc networks or WMNs is not an ideal approach, because it is complicated to handle clusters in a distributed system.

Even so, this implication has goaded other research work such as, where hybrid network architecture is consider to advances the capability of ad hoc networks. In the hybrid architecture, nodes merely communicate with nearby nodes. If they require communicating with nodes with many hops away, base stations or access points are used to relay packets via wired networks. The hybrid architecture may improve capacity of ad hoc networks; however, it can still not be preferential by many applications since wired connections between bases stations do not exist in many ad hoc networks.

By utilizing the node mobility the scheme proposed in [7] enhances the network capability of ad hoc networks. Until the destination node is near to the source node it will not send when a node desires to send packets to another node. Consequently, a node only communicates with its closer nodes via the node mobility. The restriction of this scheme is the obligatory buffer for a node may be infinite and transmission delay may become huge.The evolution in capacity research of ad hoc networks has appreciably driven as analytical approach is given in [6]. Conversely, networking protocols have not been completely captured by the analysis is the restrictions. For example, the uniqueness of ad hoc routing protocols has not been completely captured in the analysis. As another example, power control mechanisms are used to recover the network capacity, and are not measured in the analysis. In any routing protocol, because the routing protocol verify a path according to definite metrics such as the number of hop counts, link quality, etc. the route for packets does not indispensable follow the path along the straight line fragment between the source and destination as given in the analysis.

Accordingly the applicability of the theoretical outcome on practical network architectures still remnants unclear. A close match among the theoretical results in [6] and IEEE 802.11 based ad hoc networks is reported in. On the other hand, this study relies on the supposition that the traffic pattern in a big ad hoc network tends to be local and therefore nodes habitually communicate with nearby nodes. Unless it is deliberately designed so this hypothesis is not always applicable in a network.Most of the existing analytical schemes are based on asymptotic analysis. The upper or lower capacity bounds derived from existing analytical schemes do not reveal the accurate capability of an ad hoc network with a given number of nodes, in particular when the number is tiny. The analysis is simplified by taking benefit of the low mobility characteristic of WMNs. Several analytical schemes are proposed for study the accurate capability of WMNs. However, the analytical model contains three assumptions that are not necessarily applicable.

1.7. CAUSES OF FAILURE

These are the following cause of failure are summarized as:

1. Operator Error
2. Mass Storage Problems
3. Hardware Problems
4. Software Problems
5. Network Problems
6. Denial of Service Attacks
7. Natural Disaster

1.7.1. Operator Error

Operator Errors (OE) are those failures caused directly by human actions. Operator error can be further subdivided into intentional or unintentional errors and as errors that do or do not cause consequential damage. Operator Errors is responsible for over 5% of all system failures [7]. This figure usually varies from enterprise to enterprise based on the intensity of training and other factors such as corporate culture and procedures.This kind of error is useful in exploratory likely types of network system failures. An operator error that affects the network trustworthiness can arise from people’s interaction with networking equipment, physical cables and connectors as well as from actions by other networking devices result from user actions. Other IT devices for instance database servers and e-mail servers can generate broadcast storms and duplication of network addresses due to the deeds of individuals operating the various devices within the network.

1.7.2. Hardware Problems

Category of hardware problems is considered as the major predictor of network failure rates. Networking equipment suppliers have also considered hardware failure as a major source of network failure rates. Approximately 25% of all failures are related to hardware problems such as computer failures [8]. Vendors build severance into their product offerings to advance overall hardware reliability in networking products. A wide range of duplicity options ranging from having no duplication to the full duplication (or more) of equipment and links is always selected and deployed by a network designer. The US Military and Bellcore standards are useful predictors when applied in this slim context. Today, it is general to have individual hardware apparatus of networking equipment have MTBF's ranging. This ranging may be from 80,000 hours to several hundred thousand hours.

There are discrepancies in more than just the selected hardware components in the actual deployment of the networks. The excellence of network planning and design, Excellence of equipment, the communication, the complexity of the implementation, and interoperability of components are the main discrepancies included for the network. To have "five-nine" availability, mission critical networks are designed and are required to gather that performance criteria based on an MTBF assessment. However, other 75% of network failures are included by other four categories of failures and not identified through an MTBF analysis of hardware problems. These other contributors to network breakdown rates must be measured to accurately assess and envisage network availability. MTBF analysis is not a suitable measure for three of these categories.

1.7.3. Software Problems

Nowadays, enterprise networks join large numbers of servers that offer functionality to huge numbers of users using an extremely huge number of software applications. Broadly distributed systems are common in enterprises that are geographically dispersed. The network offers all connectivity among various computer platforms and clients. In systems of such complexity, even with careful monitoring, planning and assessment, it is not easy to forecast the service demands on the network. Failures can arise from inadequate capacity, extreme delays during peak demands well as an appalling failures arising from the loss of a vital component or resource.

By faulty device drivers, subtle differences in protocol implementation and handling, and operating systems error or fault and anomalies network software may be failed. Software problems contribute approximately the same number of failures as hardware problems i.e. approximately 25% and are important to any meaningful reliability analyses [8].

1.7.4. Network Problems

Hardware and Software problems that are directly associated to the Network are included in this category. These may account for more than one third of network failures [8]. To better comprehend the distribution and nature of these types of failures it is useful to consider them in the circumstance of the OSI model. Causes of failures within the lower layers of the model are frequently faulty NIC cards, failures in interface cards in bridges routers and switches, defective cables and connections, beacon failure (Token Ring networks), packet size errors and checksum errors. As Ethernet technologies have enhanced over time, there has been a refuse in the failure rates within the lower layers of the OSI model but, there has been an enhance in the failure rates in the Application Layer as software complexity continues to blow up.

Many of the errors and failures as described here are often localized and not disastrous in nature. Localized failures are very diverse from that defined by the US Military and the Bellcore models which permit for local failures to happen and not be measured a device failure. In understanding the contribution of localized failure to network reliability, it is significant to consider the scale and size of failures that are caused by individual network components. For instance, the failures of a NIC card will not likely results in a Single Point of Failure of the enterprise network. Though, a Core Router failure without suitable redundancy and switchovers can debilitate an entire network.

1.7.5. Denial of Service Attacks

Denials of Service attacks have been a key source of network failures since 2000 [9]. Nowadays they are happening several times a year resulting in service disturbance worldwide. The regularity of this network failure is increasing at an alarming rapidity. From this form of attack only private strongly controlled networks without Internet access are invulnerable by deploying "air-gaps" in the network. Air-gaps can be considered as a physical gap with no connectivity and where data is manually transported among nodes. This scheme is not practical for the vast majority of networks nowadays that rely on Internet connectivity.

An instance of the impact of Denial of Service attacks is the Code Red virus and a more up to date variation, Slammer worm, disrupted millions of computers by unleashing a healthy corresponding Distributed Denial of Service Attack. These attacks resulted in a momentous loss of corporate revenues worldwide. The improved frequency of incidence or threat, and impact of this type of network failure on network disturbance are significant and therefore the Denial of Service Attack category must be incorporated in any valid failure analysis model of an Internet connected enterprise network.

It is probable that even more menacing malicious code will be unleashed to inflict havoc worldwide. Researchers have just postulated how a virus, dubbed the Warhol virus, could dislocate the entire Internet within fifteen minutes. For instance, the Slammer brought Internet service to a halt in India; immobilize a million machines in Korea, disabled automated tellers in the Bank of America, affected universities and a foremost Canadian bank in the course of a few days in 2003.

Worms such as Code Red and Slammer are possibly authored and unleashed by an individual or a tiny number of individuals. An even further worried some threat exists if the malevolent code is part of an information warfare attack. It is well documented that countries such as China have an active expansion program for waging Cyber war.

1.7.6. Failures from disasters

The last category of failure considered is that of disaster scenarios which take place from a wide range of circumstance, many of them environmental and some synthetic. Environmental disasters comprise earthquakes, hurricanes, long-term power outages, floods, tornadoes and fires.

Synthesized disasters can include theft, war and acts of terrorism etc. In some cases there is regional occurrence that may be useful in predicting such an event. On the other hand, in several other cases no previous knowledge or useful means of prediction is probable. Disaster planning has only recently become a high networking priority as the collective mindset of the world has determined on dealing with the threat of widespread violence.

1.8. REQUIRED HARDWARE AND SOFTWARE

This section describes the hardware and software desires for the wireless mesh network.

1.8.1. Hardware Requirements

- **Wireless routers:**
- PC or Laptop with a LAN card
- Power-over-Ethernet adapters
- Omni-directional antennas
- Directional antennas
- Lighting protectors

1.8.2. Software Requirements

- Freifunk firmware version 1.4.5 that can be downloaded from http://download-master.berlin.freifunk.net/ipkg/_g%2bgl

- DD-WRT firmware version 2.3 that can be downloaded from http://www.dd-wrt.com/dd-wrtv2/downloads.php then Select "**stable**" →> select "**dd-wrt.v23 SP2**" →>select "**standard**"→> select "**dd-wrt.v23_wrt54g.bin**"

- Putty.exe it is a Windows SSH client, necessary for any PC/laptop that running Windows and may be downloaded from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html or any other sites according to availability in website on the internet

- Tcpdump: may be downloaded the latest version from http://downloads.openwrt.org/whiterussian/packages

- dot-draw: the latest **olsrd-mod-dot-draw** package may be downloaded from http://downloads.openwrt.org/whiterussian/packages

CHAPTER 2

LITERATURE REVIEW

Routing in Wireless Mesh Networks

Routing protocols applicable to WMNs

Routing protocols in Wireless Mesh Networks

Single-path Routing Protocols for Wireless Mesh Networks

Multipath Routing

Key Aspects in Multi-Path Routing

Protocols for network management

Security in WMNs

LITERATURE REVIEW

2.1. Routing in Wireless Mesh Networks

Routing is the process of moving packets across a network from one host to another by selecting best paths in a network. Since IP has been customary as a network layer protocol for several wireless networks together with WMNs and WMNs are strongly incorporated with the Internet. As compared to wired networks and cellular networks Routing protocols for WMNs are dissimilar from those. Therefore, we concentrate study on routing protocols in this segment.

The routing protocols of ad hoc networks can be applied to WMNs since WMNs share common features with ad hoc networks. For instance, mesh routers of Firetide Networks are based on topology relay that is based on reverse path forwarding (TBRPF) protocol [10], Microsoft mesh networks [11] are developed based on dynamic source routing (DSR) [12,13], and ad hoc on demand distance vector (AODV) routing [14,15] are used by many other companies.

The design of routing protocols for WMNs is an active research area for several reasons even though the availability of several routing protocols for ad hoc networks. Firstly, to advance the performance of routing protocols new performance metrics are required to be exposed and utilized. In addition, existing routing protocols still have limited scalability. Furthermore, as a transparent layer the existing routing protocols care for the underlying MAC protocol. Though, to improve the performance of the routing protocols within WMNs the cross-layer interface must be considered. The necessities of power efficiency and mobility are much different between WMNs and ad hoc networks. Inside a WMN, mesh client nodes usually desire sustain of mobility and a power efficient routing protocol whereas mesh routers in the backbone have least mobility and no restriction on power expenditure.

The routing protocols developed for ad hoc networks may not be appropriate for WMNs due to such dissimilarities.

We believe that a finest routing protocol for WMNs must confine the following features on the basis of the performance of the routing protocols for ad hoc networks and the specific requirements of WMNs:

- **Performance metrics.** To pick the routing path most of the existing routing protocols use least hop count as a performance metric. This has been verified not to be valid in several situations. Suppose a link has bad quality on the least hop count path among two nodes. The throughput between these two nodes will be awfully little if the least hop count is used as the performance metric. Performance metrics associated to link quality are required to resolve this problem, if congestion generated. The least hop count will not be a accurate performance metric either. Usually Round trip time (RTT) is used as an additional performance metric. By considering multiple performance metrics the bottom line is that a routing path be required to be selected.

- **Fault tolerance with link failures**. If a link shatters then the routing protocol must be able to quickly select another path to avoid service disturbance. This should be the main principles to deploy WMNs is to make sure robustness in link failures.

- **Load balancing.** The network resources are shared between many users in WMNs. If any part of a WMN feels network jamming, then a new traffic flows must not be routed through this part. RTT may be impacted by link superiority since performance metrics such as RTT assist to achieve load balancing, but are not always effective.

- **Scalability.** For a very large wireless network setting up a routing path might take a long time, and the end-to-end delay may also become large. Moreover, the node states on the path can change when the path is developed,. Therefore, the scalability of a routing protocol is influential in WMNs.

- **Adaptive Support of Both Mesh Routers and Clients.** A much simpler routing protocol can be designed for mesh routers than existing ad hoc routing protocols by considering the least mobility and no restriction of power consumption in mesh routers,. Nevertheless, for mesh clients, the routing protocol should have the full functions of ad hoc routing protocols. Therefore, it is essential to design an efficient routing protocol for WMNs that may adaptively sustain both mesh routers and mesh clients.

2.2. Routing protocols applicable to WMNs

2.2.1. Routing protocols with various performance metrics

In [16], the impacts of various performance metrics on a routing protocol are deliberated where the LQSR (link quality source routing) is proposed on the basis of Dynamic Source Routing. To choose a routing path according to link quality metrics Link quality source routing is endeavored. The expected transmission count (ETX) [17], per-hop packet pair and per-hop RTT are the three performance metrics that are implemented discretely in LQSR.

Through these three performance metrics the performance of the routing protocol is also compared with the method using the least hop count. ETX attains the best performance For motionless nodes in WMNs, while when nodes are mobile the least hop count method outperforms the three link quality metrics. The cause is that, the ETX metric cannot hurriedly track the transform in the link quality, as the sender moves. This outcome illustrates when mobility is anxious, the link quality metrics used in [16] are still not adequate for WMNs. Routing protocols integrating multiple performance metrics are essential for WMNs and better performance metrics necessitate to be developed.

2.2.2. Multi-radio routing

Since the capacity can be enlarged without modifying the MAC protocol, in WMNs, multi radio per node might be an ideal architecture. A new performance metric, called the weighted cumulative expected transmission time (WCETT) is suggested for the routing protocol. WCETT takes into account both link quality metric and the least hop count. It can attain good tradeoff between delay and throughput since it considers channels with expert quality and channel variety in the same routing protocol.In WMNs, multi channel per radio is an additional alternative to improve the capability of WMNs.

2.2.3. Multi-path routing for load balancing and fault tolerance

To execute better load balancing and to offer high fault tolerance is the main purpose of using multipath routing [18]. Between source and destination several routing paths are selected. Once the routing path is selected packets flow in one of these selected paths. When a failure occurs in ink or in node because of a bad channel eminence or mobility on any power failure, another path can be selected from the set of existing paths. Therefore, without waiting for rediscovery of routing path again from source, the end-to-end delay, throughput, and fault tolerance is improved. Nevertheless, between source and destination the development depends on the accessibility of node disjoint routes.

Complexity is a major shortcoming of multipath routing. WMNs require to be investigated depending on applications whether or not the multipath routing can be used. If the shortest path is taken as the routing performance metric is that multipath routing appears unrealistic. Unless a huge number of shortest paths are selected, load distribution is approximately the same as single shortest path routing [19]. Therefore, with suitable performance metrics how to develop an effective multipath routing protocol is an interesting research topic.

2.2.4. Hierarchical routing

Various hierarchical routing protocols have been proposed in last few years. We describe the general principle of these routing protocols instead of addressing each of them. Hierarchical routing is based on the cluster routing. In this type routing, a certain self organization proposal is employed to collection network nodes into clusters. Every cluster has one or more cluster heads. The cluster head may be situated one or more hops away from the nodes. Some nodes may communicate with more than one cluster and work as a gateway because connectivity among clusters is needed. Routing between clusters and Routing inside a cluster may use different mechanisms. For example, intracluster routing can be on demand whereas intercluster routing can be a proactive protocol.

Hierarchical routing protocols are liable to achieve much improved performance when the node concentration is high, because of shorter average routing path, less overhead, and quicker set up process of routing path. Since a node selected as a cluster head may not essentially have higher processing capability and channel capacity than the other nodes, in WMNs, hierarchical routing in fact may face the implementation difficulty. Unless being deliberately intended so, the cluster head is rehabilitated into a threshold. It proffers a promising technique for scalability.

2.2.5. Geographic routing

Geographic routing algorithms forward packets by only using the position information of the destination node and nodes in the neighborhood as compared to topology based routing algorithms. Thus, changes in topology have a lesser amount of blow on the geographic routing than other routing protocols.

Before time geographic routing algorithms works as single path greedy routing algorithms. As a single path routing, packet forwarding choice is made based on the location information of current forwarding node, the target node and its neighbors. Different greedy routing algorithms vary in the optimization decisive factors that are applied in the forwarding decision. Greedy algorithm is proposed To advance power efficiency, which decrease signaling overhead by eliminates the intervallic hello messages than other greedy routing algorithms. Nevertheless, Delivery is not assured even if a path exists between source and destination is a common problem of all greedy routing algorithms. Keeping the past routing information and fractional flooding can help to assurance delivery. However, these approaches drop the stateless property of single path greedy routing and enlarge communication overhead.

Planar graph based geographic routing algorithms are projected recently in order to keep the stateless property and assurance delivery, though; open issues still linger in these algorithms. For example, the communication overhead is much superior to in the single path greedy routing algorithm in the face routing algorithm. Therefore, as a recovery scheme when the greedy routing algorithm is unsuccessful the face routing algorithm is mostly used.

2.3 Routing protocols in Wireless Mesh Networks

Routing protocols are used to discover and maintain routes between source and destination nodes, in order to forward traffic further from source node to destination node. To carry out well in Wireless Mesh Networks must consider:

- Transmission errors: the fallibility of the wireless means may lead to transmission errors.
- Link and node failures: nodes and links can be failed at any time due to different types of perilous conditions in the environment.
- Incorrect routes: due to node/link failures or additions to the network, routes may befall outdated or based on an incorrect system state.
- Congested nodes or links: due to the topology of the network and the nature of the routing protocols, definite nodes or links may befall congested, which will lead to elevated delay or packet loss.

When considering route formation process, routing protocols can be categorized in three main categories: proactive, reactive and hybrid, as depicted below.

2.3.1 Proactive Routing.

In the proactive routing, each node containing routes to all other nodes/destination in the network. In this type of routing, each node maintain routing table with the possible entries for each destination. Every time when routes are computed, it is piled up in routing table, even when they are not required. Due to the numeral of messages that have to be exchanged to maintain routing information up-to-date it acquires a considerable overhead and bandwidth consumption. Proactive protocols may be unfeasible for large and dynamic networks due to its routing overhead.

2.3.2 Reactive Routing.

Reactive Routing also called on-demand routing. As on demand routing it only compute routes when they are required i.e. when a node wants to send packets, it start route discovery for the desired destination. It requires the transmission of route requests and the wait for replies by a path to the destination for the process of finding an appropriate route towards the destination. This approach is not appropriate for operations that necessitate immediate route availability, due to the delays incurred in this process.

2.3.3 Hybrid routing.

For the hybrid WMNs neither proactive nor reactive protocols present a finest solution. In WMNs has some mobility and thus reactive protocols are most appropriate because route updates are frequent. Proactive routing allows maintaining routes with low overhead as the backbone has compacted mobility.

By merging the best properties of both proactive and reactive protocols hybrid approaches aim at providing an optimal solution. In different parts of the hybrid WMN hybrid routing uses dissimilar routing protocols: reactive protocols for ad hoc zones and proactive protocols in the backbone.

2.4 Single-path Routing Protocols for Wireless Mesh Networks

2.4.1 Proactive Protocols

2.4.1.1 OLSR

We describe some relevant routing protocols used in wireless mesh networks in the subsequently paragraphs. We begin by giving a brief introduction about of OLSR, AODV, and DSR. For expansion of one of these three protocols numerous multipath routing protocols discussed in this report.

Optimized Link State Routing [20] is a proactive protocol that is intended for huge and crowded networks. Communication is supposed to occur frequently in Optimized Link State Routing. To dense the amount of control information sent in the messages and to decrease the number of retransmissions requisite to propagate them OLSR uses two key concepts first one is multipoint relay and second one is multipoint relay selectors.

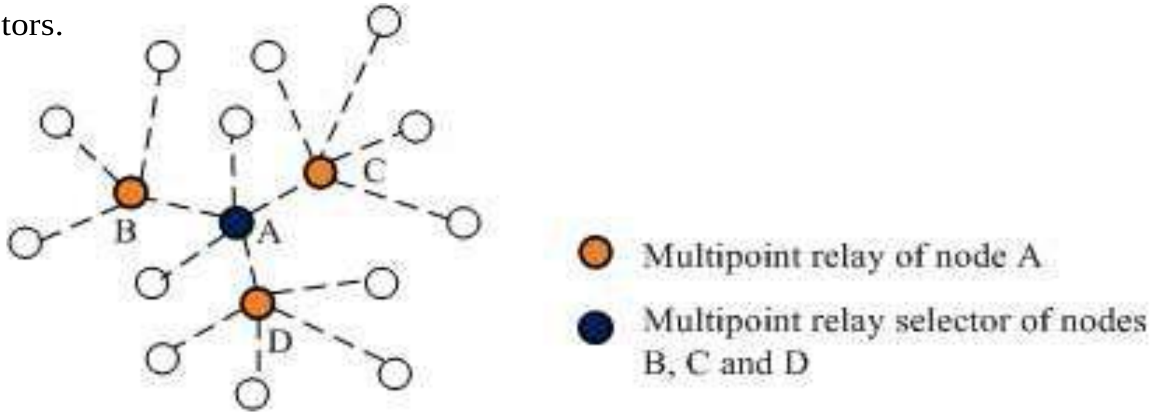

B
A
C
D
Multipoint relay of node A
Multipoint relay selector of nodes B, C and D

Figure 2.1: Multipoint Relays and Multipoint Relay Selectors.

Optimization the flooding of packets and diminishes duplicate retransmissions in the same region is the main principle of MPRs (multipoint relays). As depicted in Figure 2. In this figure each node has several multipoint relays that are chosen among its one hop neighbors in such a behavior that the set covers all the nodes that are two hops away. For example, nodes B, C and D are the multipoint relays of node A. A can arrive at all nodes that are two hops away from it via one of these nodes. Symmetrically, B, C and D will have A in its multipoint relay selector set.

For a node to prefer its multipoint relay selectors, it requires first to detect the set of neighbors with which it has a bidirectional link. This is completed by broadcasting intervallic HELLO messages, to all one hop neighbors. By receiving HELLO messages from an one-hop neighbor N, a node can record the following information about N:

i) The condition of the link to/from N;

ii) A list of the one-hop neighbors that N give access to. Based on this information, a node may select its multipoint relay selectors. The chosen nodes are listed in HELLO messages. While a change is detected in a one or two hop neighborhood this information is refreshed.

Two tables are preserved by OLSR to hold up its operation, first one is the topology table and second one is routing table. From periodic TC (Topology Control) messages, sent by every node in the network the topology table is built with the information acquired. The list of nodes that have chosen the source as a multipoint relay is held by TC message, so a node getting this message has information of two hop links, through the TC sender. Entry about impending destination in the routing table contains the address of a MPR selector established in the TC messag and the address of the last hop to that destination that is the source of the TC message.

Entries of routing table are used to forward traffic towards the network. Topology table is the source of the creation of the routing table, by tracking the associated pairs in a descending order.

2.4.2 Reactive Protocols

2.4.2.1 AODV

Ad hoc On-Demand Distance Vector is a reactive, single path and loop-free distance vector protocol based on hop count. Whenever a source node wishes a route to the destination, it begins the route discovery by flooding the RREQ (Route Request) and then waits for the route reply (RREP) from the destination. If any intermediate node receives the first copy of RREQ and if it knows the destination node, it may unicast a route reply (RREP) to the source node via the reverse path; otherwise, it further re-broadcasts the RREQ packet to its neighbors. The forward path to the destination is established when the source receives the RREP. When any node finds out a link break or successor node failure, the node stars the local repair if the destination is nearby. If the destination is far away it broadcasts the RERR packet to the source. The source then tries to search the route to the destination again if the path is still needed [14, 15].

2.4.2.2 DSR

Likewise AODV, DSR is based on RREQ/RREP packets. However, RREQ collect the addresses of the 'visited' nodes and preserve information regarding the complete path from the source to the destination node, not just the next hop. Every node keeps information in a route cache instead of the routing table [12, 13].

2.5 Multipath Routing

Multipath routing for load balancing and fault tolerance the key point of using multipath routing is to carry out improved load balancing and to offer elevated fault tolerance. Multiple paths are chosen among source and destination. Packets flow in one of these particular paths. When link is out of order on a path because of a dire channel quality or mobility, different path in the set of existing paths may be selected. Therefore, without waiting for setting up a new routing path, throughput, the end-to-end delay, and fault tolerance may be enhanced. On the other hand, the enhancement depends on the availability of node disjoint routes among source and destination. A disadvantage of multipath routing is its complication. Whether or not the multipath routing can be use for WMNs desires to be examined depending on applications. One more problem is that multipath routing is not suitable if the shortest path is picked as the routing performance metric. Unless a huge number of shortest paths are chosen, load distribution is approximately the identical as single shortest path routing. Therefore, how to design an efficient multipath routing protocol with proper performance metrics is an interesting research topic.

Most of the routing protocols that have been proposed for mesh and ad hoc networks are unipath that means only a single route is used between a source and a destination node for the transmission of packets. Uses of numerous good paths to arrive at destinations not just the best path are the main objective of multipath routing. Without magnificent extreme control overhead in maintaining such paths this objective can be achieved. Following benefits can be used by the availability of several paths between a source and a destination.

- Fault tolerance: when there is a failure redundancy in the network or providing backup routes are used [21]. In mesh networks a variety of fault tolerances are introduced at the routing level. To this end, some techniques such as packet salvaging can be applied [22]; if the actual route is out of order it consists modifying the path of a packet.

- Throughput enhancement: enough bandwidth for a connection is not offered by routing with a single path. Since in the mesh network, various links can have inadequate bandwidth. Thus, a better approach to satisfy the bandwidth obligation of some applications to use concurrently multiple paths to route data may be a good. Slighter end-to-end delay is achieved by increasing the throughput and quality of service is improved.

- Load balancing: spreading the traffic along multiple routes can alleviate congestion in some links and bottlenecks since traffic distribution is not identical in all links in the network.

- Error resilience: better error resilience is offered by multipath protocols for distributing traffic (for example, by means of data and error correction codes) over multiple paths. A M-for-N diversity coding scheme is proposed, which consists of using M supplementary links to send traffic, coded in a mode that the system can abide M –1 simultaneous link failures at any time.

- Security: with single path routing protocols, it is easy for an antagonist to instigate routing attacks, but multipath offers attack resilience.

2.4.1 Routing Metrics

The route founding segment includes the option of paths among all the offered to forward traffic. If various paths are presented we may wish for to choose a limited number: to use only the one with the most excellent metric or to choose the n best ones. The path valuation and selection according to definite metrics are discussed in this section. Hop count is a widely used metric because it allows speedy path discovery in presence of mobility. On the other hand, in Wireless Mesh Networks, the fixed topology reimbursement from quality-aware routing metrics [23], because radio communication is recurrently unpredictable. Path dependability and link superiority are the performance metrics worn by a significant number of quality aware routing mechanisms. Between two mobile nodes within a definite amount of time we can identify path reliability as the probability of having a successful data transmission [24]. These are the following metrics that may be used to evaluate mesh routing protocols [25]:

- ETX (Expected Transmission Count) is the expected number of transmissions that a node requires to do to successfully transmission of a packet to their neighbor. It is based on the packet delivery ratio with in a definite time interval.

- ML (Minimum Loss): ML defines the route with the nominal probability of end-to-end packet drop.

- ETT (Expected Transmission Time): ETT judge link quality as a utility of the time that a data packet acquires to be effectively transmitted to each neighbor of the node.

- mETX (modified ETX): mETX computes the bit error probability at bit level.

The objective of this metric is to resolve a difficulty related to fast link-quality variation in wireless networks. Metrics that is based on a time window interval does not suffer the link distinction variations or may formulate excess in overhead.

- ENT (Effective Number of Transmissions): ENT dealings the number of succeed retransmissions per link and consider the variation. It is also defined to consider link distinction variations.

- iAWARE approximation the average time, considering aspects similar to medium instability, the medium may be busy because of transmissions from all interfering neighbor, data transmission time, and interferences.

- WCETT (Weighted Cumulative ETT): WCETTshows the interference between the links i.e. inter flow interference that is operated on the same channel. Attenuation of the throughput is a sign of the considered interference.

- MIC (Metric of Interference and Channel-switching): MIC progress Weighted Cumulative ETT, it consider not only interference between the links but also intra flow interference. Channel-switching and Metric of Interference is contested by two main components: the first one confines the potential for the path to interfere with itself and the second one confines the potential for the path to interfere with other paths.

Though there are a lot of metrics may be evaluated for these protocols, and some of them are more complete and complex than others, the mainstream of routing protocols implementations favor metrics with easier designs like ETT or ETX.

The following metrics are most suitable for considering multipath routing protocols:

- Degree of route coupling: between paths in multipath routing it defines the score of interference. In wireless communication it may be identified that the packet transmission is resulted in tainted eminence of a simultaneous communication on a adjacent link. If two routes have links or nodes in common, they may be very much coupled other than this result are occurred even if there is no common links or nodes. In terms of transmission quality low coupling links are the most brilliant which earnings that disjointness among links must be obtained.

- Path correlation: Among two nodes disjoint paths path correlation factor defines the interference of traffic that is related when all the nodes fight for the radio channel and use the analogous radio spectrum. The sum of correlation factor of a set of multiple paths may be definite as the sum of the correlation factor of all couple of paths. Other approaches utilize combinations of a few metrics, particularly in QoS routing, where a subset of paths is chosen only if the joint metric satisfies the QoS necessities.

2.4.2 Proactive Multipath Routing

Proactive multipath routing protocols have two operation phases: network setup and network maintenance.

Network Setup This phase consists of the steps required to construct the routing table desired to forward traffic.

Network Maintenance This phase is accomplished when the routing table has already been created and consists of the steps requisite to maintain and repair the existing routes in face of topology changes.

2.4.2.1 MOLSR

Multipath Optimized Link State Routing Protocol (MOLSR) [28] is a proactive protocol based on OLSR that objective to attain lower delay and packet drop by using multipath routing. As, OLSR use multipoint relays and multipoint relay selectors to limit broadcasts. The function of MOLSR is nearly the same as OLSR, although the network setup phase has some dissimilarity. In this section we explain the differences between these two protocols.

OLSR contain two tables: the topology table and the routing table. The topology table records the organization of the entire network, but does not store any link state factor, so precise routing selection is tough to be made based on this table only. In MOLSR, SNR and Delay are added to the TC (Topology Control) message and these factors, representing the link state between the MPR selector and the TC originator, are also stored in the topology table. The routing table is created based on the topology table and stores two routes to every destination but not more than two. These routes embody the best ones at that moment. A node can select the best route to transmit data, but if it fails the other one may be used without route discovery.

The main differences between OLSR and MOLSR lie in the process to compute the routing table. In MOLSR, more than one route is calculated and two best routes are selected according to the link metrics announced in TC messages. Routes with more than 2 nodes in common are not considered (node disjoint u paths).

2.4.2.2 OLSR-based multipath routing

With reference to multipath proactive routing, there are some link-state protocols based in OLSR. MOLSR [28], as we have seen, computes multiple paths but uses only the best one at each instant. In QOLSR [29] multiple paths are used to persuade definite bandwidth and delay requirements. Such paths have least amount of correlation factor but they are not zone disjoint. Another multipath proactive protocol is MP-OLSR which computes multiple node or link disjoint paths according to various cost functions. All the mentioned solutions use OLSR as base, so its core functionality has two parts: topology information achievement and route computation. To get topology information of the network, nodes use topology sensing and topology discovery. Topology sensing includes link sensing and neighbor recognition and allows each node to gather information about its neighbors, based on the periodic exchange of HELLO messages. Topology detection is based in TC messages and each node gives adequate information to enable routing. Route calculation is performed every time a TC is received. Routes to the entire destinations in the network are computed and saved in the routing table.

However, in MP-OLSR an on-demand scheme is used to avoid the heavy computation of multiple routes to every destination. While the network topology update operation may benefit from the use of multipoint relays, like every node is required to send link-state updates the signaling cost requisite to maintain this information is high, particularly in large and dense networks.

2.5.3 Reactive Multipath Routing

To the best of our acquaintance, most of the multipath routing protocols are reactive. The action of these protocols can be divided into three components: route establishment, route maintenance, and traffic allocation. In the following paragraphs we have a discussion regarding each of these components.

Route Establishment:

During this phase multiple route discoveries is initiated between source node to destination node. Multiple route discoveries are done by folding RREQ (Route Request) with a unique sequence number. To minimize the message cost, nodes discard duplicate route request. New route request are rebroadcasted again and again until they are arrived at the destination node. Destination node in turn, will reply to the RREQ (Route Request) by sending one or multiple route replies (RREP). Because the destination node collects information about numerous existing paths, it may be apply one of the following principles to select the ones to use:

- Minimum cost paths [26]: MCPs illustrates minimum cost of path amongst all the available paths i.e. shortest paths according to the calculation from piggybacked information on the RREQ.

- Non-disjoint paths [27]: A Node Disjoints path shows the path that has common links and nodes that can have nodes and links in common. More simply Non-disjoint routes can be discovered. More disjoint routes can be discovered since no restrictions are mandatory. As, it was uncovered that a network turn out to be more consistent and better amortizes the cost of on demand path discovery over many links, by utilizing rich mesh connectivity, in meanness of using disjoint paths. As the detachment among nodes augment, the probability of detection node and link disjoint routes diminish, as a result non disjoint paths have to be used. However this proposal has also weak spot: it can be more complicated to choose routes that do not interfere with each other since we are considering wireless communication.

- Link disjoint paths: A Link disjoint path shows a path that have no common links but may have common nodes.

- Node disjoints paths: Node disjoints paths shows a path that have no common nodes. In standard, node disjoint routes extend an improved utilize of network resources, since neither nodes nor links are shared between two paths. For fault lenience, node disjoints routes offer the maximum availability, a failure of a node may grounds the failure of several routes since when using link disjoint routes.

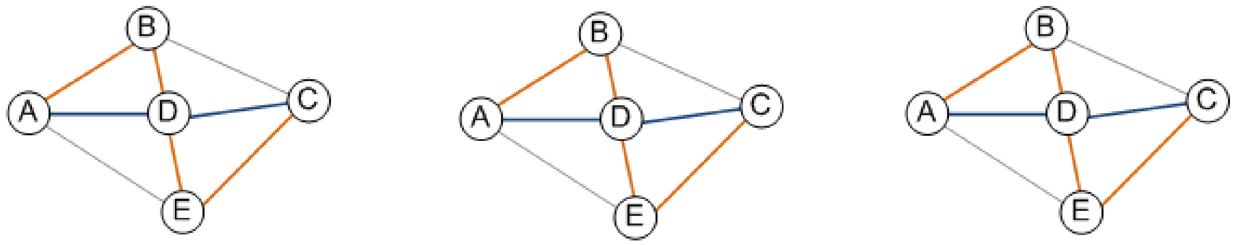
- Zone-disjoint paths: when data communication over one path does not interfere with other paths then the paths are supposed to be zone disjoint, which means that route coupling between the measured paths is zero.

The consequent RREPs have to be sent reverse to the source when the paths have been selected. Due to this reason, about the reverse path information has to be set up all the way through the RREQ forwarding, using either hop-by-hop routing or source routing. Note that several RREQ can reach the destination, and the destination can only reply to a subset of them, according to the norm mentioned above. As an optimization, if an intermediate node accept a RREQ and it has a route to the destination, it may send a RREP with the identified route. On the other hand, in order to let the destination select disjoint or minimum cost paths, sometimes multipath routing protocols have to slow up the reply to RREQ by intermediate nodes [27].

Route Maintenance:

The objective of route maintenance is to legalize existing routes and locate suitable replacements when one of the existing routes becomes fail. There are various ways to maintain routes, from which we highlight two:

- Periodic beacons (HELLO messages): each node periodically transmits a HELLO message to its neighbor. A link connecting the node to the neighbor is presumed busted and sends an error notification to the predecessor nodes affected by the failure, if a node does not receive a HELLO from a neighbor after a certain amount of time, as shown in figure 2.2. Since HELLO messages devour bandwidth that could be enhanced consumption for data traffic, this is not a attractive proposal.



(a) Node disjoint (b) Link disjoint (c) Non-disjoint

Figure 2.2: Multipath Routing Route establishment

- MAC layer acknowledgements: This technique is about the similar, but no additional messages are sent. After a definite number of retries when a node does not receive an ACK for a data packet, those links are assumed to the neighbor to be out of order, and an error notice is sent back.

If any of the previous methods suggests that there is a route breakdown, then it is necessary to rediscover a new route and route rediscovery process must is performed. In the meticulous case of multipath routing, route discovery can be triggered each time only when all the routes have failed or when any of the routes becomes fails. For all scenarios none of the proposals are best, because waiting for all the routes to be unsuccessful previous than performing a route discovery would consequence in a holdup earlier than new routes are available, and reinitiated a route discovery each time a path stop working may earn in superfluous overhead. Any optional technique that can be a compromise among these two marvelous options consists in initiating route detection only while a threshold of n paths stop working. To turn away routes from organism uninvolved as a result of route utilization, immobility becomes significant, if on demand routing protocols have not been browbeaten for a confident amount of time they lean to drop routes.

Traffic Allocation

Once set of paths to the destination is selected by the source node, the selected path is used to send data to the destination. An allocation policy is required to choose the way data is disseminated between the presented paths. There are two germane aspects of an allocation policy: scheduling and granularity. The least unit of information allocated to each path is specified by granularity [24]:

- Per-segment: it forward each segment using a different path after cracking a packet into segments

- Per-packet: distributes the packets from numerous connections among the existing paths.

- Per-connection: It shows allocation traffic for the same connection to a single path.

- Per source-destination pair: Per source-destination pair uses the same path to forward traffic between a certain pair of source and destination nodes

As granularity allows for an enhanced control over the network resources it allows more proficient load balance. At the same time, at the destination granularity per packet or per segment needs reordering.

Paths attained in the route discovery process can be planned using the subsequent approach:

- Round robin: in this approach using a different path a node sends each packet. Because of the possibility of out of order delivery of packets belonging to the same flow this methods suffers from setback. The maintenance of a big buffer is required by TCP and can lead to needless loss due to out of order deliver. As load will be homogeneously distributed it can be used for efficient load balancing.

- Congestion aware: this scheduling to keep away from losses and additional delays scheme proposes to send traffic using non congested links. By the average queue length and improving the performance considerably Congested routes can be calculated.

- Backup path: a source may establish a primary path as well as numerous backup paths to the preferred destination during the route discovery process. In recovering from a failure multipath can be used to decrease the delay, consequently using the backup paths to jump the continuing traffic to these alternative paths, when the primary path stop working as an alternative of shooting down the end to end connection.

- Unequal cost scheme: This scheme proposes to distribute traffic based on link quality and a joint measurement of distance. According to a probability distribution as Boltzmann distribution, path with most excellent metrics is selected [20]. This becomes the most used path, but from time to time other routes may be chosen to forward packets. As all routes are used, they are not separated from routing tables, which prevents route discovery procedures this is the main advantage of this procedure.

- Concurrent delivery: It is referred as sending traffic in more than one path at the same time. This scheme is use may be to enhance throughput.

2.5.3.1 AODV-DM

AODV based Decoupled Multipath [30] suggested an algorithm that defines an shield region around the main path, to avoid interference between neighboring routes, trying to decrease the route coupling problem. Because the latter is designed for single path routing it uses SCTP as an alternative of TCP and SCTP can separately control the traffic rate of each path and cannot acclimatize to the network layer multipath structure.

Route establishment:

The primary path is exposed in the following way: a RREQ message is flooded in the entire network. Each node that receive a RREQ message, stores the information about the sending node in its routing table. From different paths Multiple RREQs may reach at the destination, coming. Firstly by sending a primary route reply (PRREP) the destination responds to the RREQs that have followed the shortest path that is also called main path or primary path. The packet pursues the smallest path; intermediate nodes with the route broadcast the packet to its neighboring nodes, which is considered as “in-region” nodes. The primary path relationship is absolute and an insulating region is established When the PRREP arrives at the source. neighbor’s exterior the insulating region removes the”in-region” nodes from their table to resist future RREPs entering this region.

The destination responds to additional RREQs after waiting a period of time to allow the insulating region to be established. The response packet is known as second route reply (SRREP) and approximately the propagation procedure of this message is same as the PRREP. With the exemption a node getting a broadcast SRREP does not make itself as an “in-region” node. Intermediate nodes shall flood the packet to their neighbors to exterminate themselves from their neighbors’ tables. An “in-region” node throws a route reply rejection packet (RREJ) if it obtains one of these packets, but has no available entry in its routing table to forward the packet. Thus the SRREP sender can endeavor other entries in its table. This procedure is depicted in Figure 2.3.

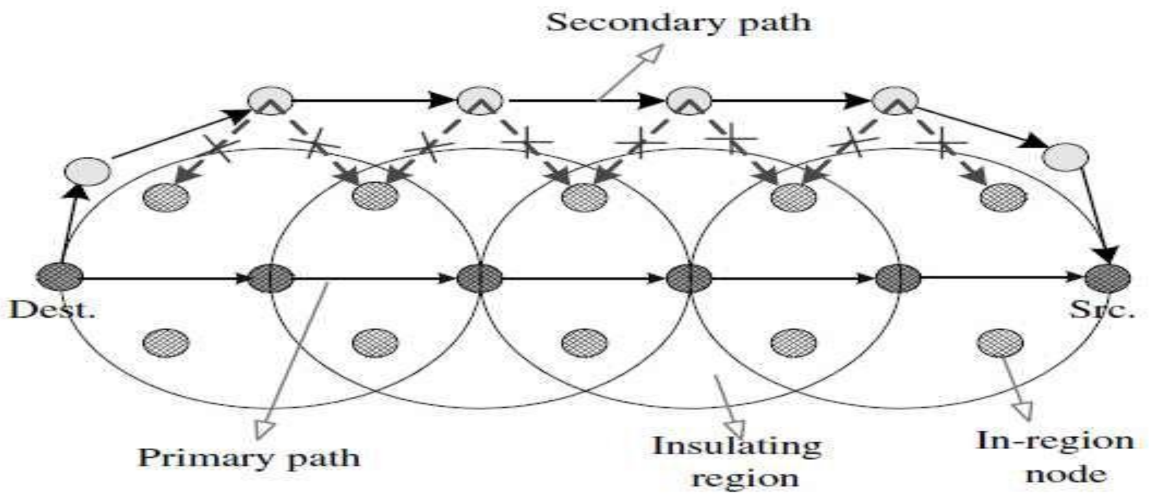


Figure 2.3: AODV-DM illustration [30]

Route maintenance:

Route maintenance is done in the same way as in the base protocol, AODV.

Traffic distribution:

The protocol can use a single path or multiple paths, when the accessible bandwidth between a source/destination pair in not adequate. When multiple paths are used, traffic is scattered concurrently. The decoupled features, and the use of path aware SCTP design, make the protocol appropriate for concurrent data transfer in dense networks; otherwise, the delay can compromise the efficiency of the protocol.

2.5.3.2 AODV-BR

AODV-Backup Routing [21] proposes a backup route mechanism to advances the performance of existing on demand protocols that find out routes through a query/reply procedure.

Route construction:

Route construction is done nearly in the same way as in AODV [15] however multiple paths are formed in the following way. A node appends the neighbor as the next hop to the destination in its alternate route table once a node receives a RREP not directed to itself transmit by a neighbor (if it receives more than one it selects the best). The resulting constitution resembles a fishbone, as depicted in Figure 2.4. The primary path is used until a breakdown occurs.

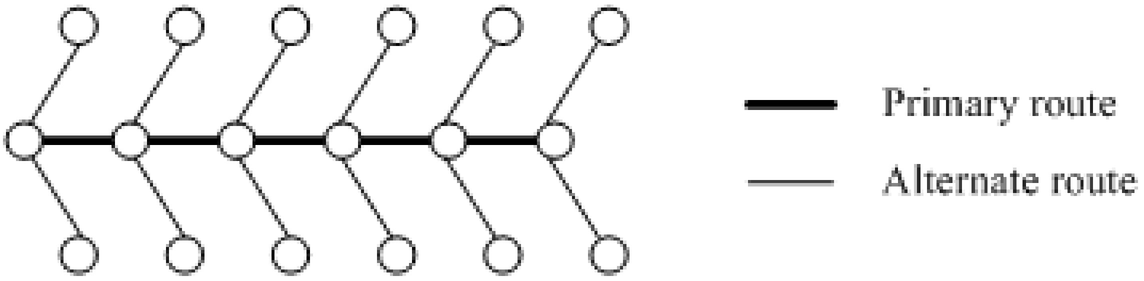


Figure 2.4: Multiple routes forming a fish bone structure [21]

Route maintenance:

Route maintenance is applied when a node detects a link failure or node failure. In this case, the node carries out a one hop data broadcast to its intermediate neighbors, categorizing the packet for alternate routing. Also, the node that notices the failure sends a route error (RERR) packet to the source to start a route rediscovery (sequentially to build a new and optimized path).

Traffic distribution:

For the transmission of packets only one path at a time (the primary path) is used. When it fails, a backup route is used to forward traffic.

AODV-BR was exposed to have improved throughput and protocol efficiency, in mobile scenarios. Furthermore, as the number of data sessions is increased, the protocol becomes less efficient because of collision and contention problems, so it does not perform well under heavy traffic.

2.5.3.3 MP-DSR

The MP-DSR is a DSR based protocol that focuses on path consistency rations. MP-DSR [31] concludes the number of paths required and the lowest path consistency requirement after gathering application path reliability requirements.

Route establishment: The source node sends RREQ messages to the destination node passing through its immediate neighbors with information about the requirements. As this is a source routing protocol, the RREQ message also contains entire visited path and the accumulated path consistency. The intermediate nodes use the information incorporated on the RREQ message to ensure if reliability necessities are still satisfied. If so, the node modernize the accumulated path reliability based on the accessibility of the link just traversed, and message is rebroadcasted to its neighbors or else, the RREQ message is discarded. According to the path reliabilities the destination waits until it receives all the RREQ packets. When all the packets received at the destination it organizes all the arrived packed. Then, according to the reliability required a set of disjoint paths are selected. Passing through each selected path a RREP is sent to the source.

Route maintenance: For each of the following scenarios the route maintenance process is different: when all the routes become fail or when one of the used paths become fails. If all the routes become fail it simply reinitiated the route establishment procedure. The source sends a route ensure messages along the paths to collect the path reliabilities if only one route stop working. The destination replies to the route check messages. The source node collects all the replies, and validates to see if the paths still meet the consistency necessity. If not, route discovery is executed. MP-DSR accumulate QoS uniqueness using local information existing at intermediate nodes, which means widespread knowledge is not obligatory.

Traffic distribution: More than one path traffic is sent if multiple paths are essential to congregate QoS requirements.

2.5.3.4 AOMDV

Ad hoc On-demand Multipath Distance Vector Routing (AOMDV)

The core concept of AOMDV [32] is calculating multiple loop-free paths for each route discovery. With several redundant paths available, the protocol switches routes to an alternate path when a primary path fails. Therefore new route detection is avoided. Route detection is started only when every path to a specific destination stop working. For effectiveness, merely link disjoint paths are calculated so that the paths fail independently of each other.

Note that link disjoint paths are adequate for our intention, as we use multipath routing for sinking routing overheads rather than for load balancing. For the latter, node disjoint paths become more useful, as switching to an alternate route is assured to let alone any congested node. Link disjoint paths, in contrast, may have common nodes. While node disjointness is stricter than link disjointness, we utilize link disjointness in the hope to uncover more alternate routes in the network.

AOMDV Route Discovery

Several changes are essential in the fundamental AODV route detection mechanism to enable calculation of multiple link disjoint routes among source destination pairs. Note that any intermediate node on the route among a source and a destination may also construct such multiple routes to destination, thus making offered a large number of routes between source and destination.

In the route detection process a reverse path is put up backwards to the source via the identical path the RREQ (Route Request) has traversed. If replicas of the RREQ coming via dissimilar paths are mistreated as before, only one reverse path can be produced. To create multiple routes, all replica of the RREQ arriving at a node are evaluated (but not propagated), as each replica defines an alternate route.

However, each of these alternate routes may not be disjoint. For example, more than two replica of RREQ may reach destination, two of which are not via disjoint paths. To differentiate between replicas RREQs that come via disjoint routes reverse routes should be formed only using the former type. The replica of a RREQ reaching destination via node disjoint paths must take different first hops from source.

Were their trajectories to get together again at any node, the replica arriving later in that node will not be propagated further. Therefore, all trajectories of a RREQ among any pair of nodes with distinctive first hops are definite to be disjoint. To find out this, nevertheless, the first hop information requires being included in the RREQ packet as an additional field. Each node memorizes the first hop of each RREQ it has seen with the equivalent source id and broadcast id. A reverse path is forever formed when the first hop is inimitable. Though, as in conventional AODV, only the very first copy of the RREQ is forwarded. Consequently there is no additional routing overhead. All these reverse paths can be used to propagate several RREPs in the direction of the source so that several forward paths can be constructed. All such paths are node disjoint. In the hope of getting link disjoint paths which would be more copious than node disjoint paths, the destination node espouses a "looser" reply strategy. It replies up to k copies of RREQ received via unique neighbors, disrespecting the first hops of these RREQs. Sole neighbors assurance link disjointness in the first hop of the RREP. Away from the first hop, the RREP follows the reverse routes that have been set up already which are node disjoint Each RREP received at an intermediate node takes a dissimilar reverse route when several routes are already available. Because of the "looser" reply policy it is probable for the trajectories of RREPs to cross at an intermediate node.

Sequence Numbers and Loop Freedom Revisited:

If only the destination replies to a RREQ as in the preceding treatment, loops are not probable. This is since RREQs may not loop as only the first received copy is propagated more. This put off any loop in the reverse or forward paths moreover. But are we still free from loops when intermediate nodes select to reply to a RREP? As AODV uses a sequence number based invariant to assure loop freedom. An analogous invariant is maintained in the multipath technique as well. Nonetheless, its design is trickier and desires a to some extent elaborate description.

Contrasting the single path case, dissimilar routes for the identical destination will now have dissimilar hop counts. Nodes must be steady concerning which of these multiple routes it advertises to others. An advertisement takes place when an intermediate node replies to a RREQ, or propagates a RREQ to its neighbors, for example. If two nodes on a route advertise routes such that the advertisement from the upstream node has a slighter hop count, it presents a convinced recipe for loops. To prevent such situations, each node maintains more than one route in general. A route can be constructed through an intermediate node only when the latter advertises it. This is despite of how many routes this node in fact maintains. They institute a strict route advertisement strategy to prevent loops. It is controlled by a field, “advertised hop count” in the routing table entry, which is initialized each time the sequence number of this route entry is updated.

The route list is merely the list of next hops and hop counts consequent to dissimilar paths to the destination. The advertised hop count symbolizes the utmost of the hop counts of each of those several paths so long as a stringent route update rule is followed. This rule is called whenever a node gets a RREQ or RREP packet from a neighbor. As in AODV [49], routes analogous to only the highest recognized sequence number for the destination are preserved. On the other hand, AOMDV allows for several routes for the similar destination sequence number. Several routes can form via any neighbor upon receiving a RREQ or RREP from that neighbour.

The basic structure of a routing table entry in the AOMDV is shown in table 3.1

Route maintenance:

To conserve connectivity information, each node executing AOMDV may use periodic HELLO messages or link-layer feedback is used to sense broken links and nodes that it considers as its immediate neighbors. As in AODV, in case a broken link is sensed, a RERR message is sent to the active neighbors that were using that particular route.

Traffic distribution:

With several redundant available paths, the protocol switches routes to a different path when the path in use becomes fail. Therefore new route detection is avoided. Route detection is initiated merely when all paths to an explicit destination fail. For efficiency, only link disjoint paths are calculated thus that the paths fail independently of each other. Structure of AOMDV routing table is shown in table 2.1.

TABLE 2.1

AOMDV routing table

destination
sequence number
advertised_hopcount
route_List {(nexthop$_1$, hopcount$_{1),}$ (nexthop$_2$, hopcount$_{2),.......}$}
expiration_timeout

2.5.3.1 AOMDV-BU

Ad-hoc On-demand Multipath Distance Vector routing with Backup Route Update Mechanism (AOMDV-BU)

Ad-hoc On-demand Multipath Distance Vector routing with Backup Route Update Mechanism (AOMDV-BU) is an extensive version of AOMDV protocol, which comprise an additional method of backup route update, using a more active route discovery mechanism. The proposed AOMDV-BU performs better than the original AOMDV, reduces both average delay and loss ratio, with the weakness of a larger overhead. AOMDV-BU maintains at least one valid backup path for any route, therefore when the active path breaks down, there is always a backup path waiting. This is attained by revoking route discovery when the number of paths for any route is less than two, while original AOMDV revokes route discovery only when there is no path available to the destination. Backup path can be constructed while the active route is still working by applying this new rule. New nodes that entered in the transmitting range after the last route discovery process could be considered as new neighbours and they may join the discovery of new paths. Thus, backup paths can be discovered and stored in routing table even if the new nodes do not exist at the time of forming the active path. AOMDV-BU algorithm adopts a more active route discover route, which may boost the route overhead [33].

2.6. Key Aspects in Multi-Path Routing

Based on the survey presented, we consider that a well designed routing protocol should concentrate on the following aspects:

- Multiple paths: in an inadequate number, multiple paths should be used in order to ascertain a balance among the number of used paths and unenthusiastic aspects like interferences or overhead.

- Low overhead: as we referred earlier, one of the objectives of routing is to find out and use multiple paths, therefore benefiting from this, but with lower extra overhead.

- Good performance: when multiple paths are used there are additional routes and state to preserve. Sending traffic over the paths in function of its quality is a means of maintaining paths alive. Having methods to supervise routing tables avoiding unnecessary information is also considered necessary to achieve a well designed protocol.

- Low degree of route coupling: as in wireless medium interferences between different channel shares a conditional factor in transmissions, in an finest protocol, these interferences must be diminished.

2.7. Protocols for network management

Several management functions are required to maintain the suitable operation of WMNs.

2.7.1. Mobility management

Mobility management consists of two significant tasks: handoff management and location management. Location management deals with location registration and call delivery, while handoff management is deal with for handoff initiation, data flow control for call handoff and new connection generation. The mobility management mechanism developed for cellular or mobile IP networks might be useful for WMNs. Nevertheless, the centralized mechanism is normally not applicable on WMNs which are based on distributed and ad hoc architecture. Therefore, distributed mobility management is ideal solutions for WMNs. Mobility management mechanism of ad hoc networks are mainly comprised of two types: hierarchical mobility management and distributed.

These mechanisms may not achieve well for WMNs because of the specific features of WMNs. More particularly, the backbone of WMNs does not have tall mobility as mobile nodes in ad hoc networks, but connections among all mesh routers are wireless. Mesh clients may continually roam across different mesh routers. These features also turn into the mobility management mechanism for cellular networks ineffective for WMNs. As a result, new mobility management mechanism needs to be developed for WMNs.

Location service is a preferred feature in WMNs. Location information may increase the performance of MAC and routing protocols. It may help to develop promising location associated applications.

2.7.2. Power management

The objective of power management for WMNs diverges. Typically, mesh routers do not have a restriction on power consumption; power management aims to manage connectivity, interference, spectrum spatial recycle, and topology. If a single channel is used in each network node then the interference between the nodes directly impacts the spectrum spatial recycle factor. Sinking transmission power level reduces the interference and enhances the spectrum spatial reuse efficiency. Nonetheless, more hidden nodes may reason of performance degradation in MAC protocols. Therefore, power management mechanisms are closely coupled with MAC protocols. Furthermore, as connectivity affects performance of a routing protocol, power management is also decisive for the network layer.

In distinction to mesh routers, mesh clients may be expecting protocols to be power efficient. For instance, power efficiency is the major anxiety for a number of mesh clients are IP phones or even sensors. Therefore, in WMNs, it is quite probable that some applications need power management to optimize both power efficiency and connectivity, which consequences in a complicated problem.

2.7.3. Network monitoring

In a network management protocol several functions are performed. Particularly in the mesh routers the statistics in the MIB (management information base) of mesh nodes; require to be reported to one or numerous servers to incessantly monitor the network performance of the entire network. On the server, in the performance monitoring software data processing algorithms examine these statistical data and discover potential aberration. The server reacts to take responses in case any irregular symptom is sensed for example triggering an alarm. Data processing algorithms can also achieve several other functions for example network topology monitoring Based on the statistical information gathered from MIB. Because of mobility in mesh clients or probable failures in some mesh routers the network topology of WMNs is not forever fixed. Therefore, for WMNs monitoring the network topology is a preferred feature.

The effectiveness of these algorithms needs to be enhanced for a large scale mesh network since a few network management protocols have been designed for ad hoc networks. Additionally, to facilitate accurately detect irregular operation of WMNs, efficient data processing algorithms are required. Moreover, how to hastily find out network topology is still an open problem.

2.8. Security in WMNs

Security is forever a serious step to organize and manage WMNs. Virtual private networking (VPN) is probable over wireless LANs. With standard key encryption scheme it can be implemented for tunneling for example to provide protected virtual paths along the shared networks IPSec is used.

For wireless LANs security in terms of authentication as well as authorization is not a big apprehension; a few wireless LAN commercial system implementations offer authentication, authorization, and accounting (AAA) services via gateways or straight over the wireless LAN access point to be careful of this concern. Authentication, authorization, and accounting are usually performed through a centralized server such as RADIUS (remote authentication dial in user service). Conversely, in WMNs the centralized algorithm is not scalable. WMNs still not have efficient and scalable security solutions similar to mobile ad hoc networks. Since their security is easier to be compromised due to: dynamic transformation of network topology, susceptibility of channels and nodes in the shared wireless medium, and nonexistence of infrastructure. In and for DSR and AODV, correspondingly the attacks can advertise routing updates. Different type of attacks is packet forwarding, i.e., the attacker cannot alter routing tables. The packets on the routing path that is not steady with the routing algorithms may be lead to a diverse destination. Furthermore, can impersonate a genuine node and sneak into the network, and does not follow the required stipulation of routing algorithms. Various malevolent nodes may create wormhole and shortcut the usual flows between legitimate nodes.

Similar types of attacks as in routing algorithms may also take place in MAC protocols. For instance, the backoff technique and NAV for virtual carrier sense of IEEE 802.11 MAC may be distorted by some attacking nodes, which reason the network to be forever congested by these malevolent nodes.

Attackers may sneak into the network by misusing the cryptographic primitives. In a cryptographic protocol, the exchange of information between users occurs recurrently. The users utilize a fair exchange protocol which depends on a trusted third party. Conversely, this trusted party is not accessible in WMNs caused by lack of infrastructure. Therefore, another exchange algorithm called rational exchange. Rational exchange ensures that a mischievous party cannot gain anything from misconduct, and therefore, will not have any incentives to behave badly.

The key management is one of the most important jobs for network security. Nonetheless, the key management for WMNs becomes much more complicated, since there is no server to manage security keys, central authority, or trusted third party. Key management in WMNs requires to be performed in a dispersed way. A self organization algorithm was projected into dispense and supervise the security keys. In self organizing key management system, certificates are stored and distributed through users themselves. When the public keys of two users require to be verified, they first merge the local certificate repositories and then find the suitable certificate manacles inside the merged repositories that may pass this corroboration.

To improve security of WMNs, two strategies require to be adopted. Either to embed security procedure into network protocols for example secure routing algorithm and MAC protocols or response systems to sense attacks or to develop security monitoring, monitor service commotion, and react quickly to attacks. To date, several secure protocols have been projected. Nonetheless, their role of defending attacks is awfully limited, since procedure positioned in a single protocol layer cannot resolve troubles in other layers. Nonetheless, security attacks in a network may come concurrently from dissimilar protocol layers. Therefore, a multi protocol layer security mechanism is preferred for network protocols.

CHAPTER 3

PROPOSED ROUTING PROTOCOL

PROPOSED ROUTING PROTOCOL

According to the connectivity or propagation state in Wireless Mesh Networks, the network topologies are changed dynamically and may fluctuate from time to time. Because of these regular changes of the network topologies, formation and maintenance of the network is to be difficult. The main reason of topology changes is the mobility of nodes. As in WMNs nodes can move freely, the resulting of the topology alteration in the network must be acknowledged to the other nodes so that outdated topology information should be removed or updated. Many reactive and proactive routing protocols have been proposed that is based on single path and multiple paths to solve this problem. Due to the mobility of nodes, single path algorithms are not sufficient for routing.

Several multipath algorithms have been proposed for this purposed. It maintains various alternate routes to support the ongoing connections, when primary path of route is broken then alternate route is used for sending packets towards the destination and thus lowers the packet drop rate. In cases where no alternate paths are available at any node during failure, route discovery has to restart from source. Since WMNs nodes are either fixed or independent to move in any direction; there may be frequent link breakage. Due to frequent link failure WMNs protocols should have mechanism to repair path locally to reduce latency for route recovery.

Our proposed protocol is based on AOMDV routing algorithm with local repair capability i.e. Ad hoc on Demand Distance Vector Routing with Local Repair (AOMDV-LR). The Ad hoc AOMDV-LR is multipath routing protocol is intended for efficient local route repair. Numerous configuration parameters used by AOMDV-LR are based on AODV and AOMDV. It discovers the route only when requisite i.e., on demand or need basis. AOMDV-LR nodes use different types of message like RREQ (route request), RREP (route reply), RERR (route error), and HELLO messages to communicate among each other. Among these, RREQ (route request) and RREP (route reply) messages are used for route discovery.

When a node required a route to the destination node, the originating node broadcasts a RREQ message towards its neighboring nodes, which broadcast the message towards their neighbors, and the process, is continuing till destination node get this RREQ. A RREQ message is begun with time to live (TTL) and a specified hop number by the originating node. RREQ receiving node can send RREP message with entire route information to the originating rote if any or multiple route is found in its cache. When the destination node receive a RREQ that is intended for it, replies a RREP message to the originating node. The destination node is supposed to be unreachable and the messages queued for this destination are thrown out if the TTL values in the RREQ have reached a definite threshold and still no RREP messages have been received. Each node in the Wireless Mesh network maintain a monotonically increasing sequence number and the protocol guarantee that the node only update routes with fresher ones by using sequence numbers. It guarantees loop-freedom for all routes to the destination in the network. Nodes along with the path can update entries of their routing table with the latest destination sequence number. RREQ and RREP messages include this latest destination sequence number during route discovery.

AOMDV-LR uses proactive and reactive both approaches within local area to decrease the route discovery delay in the network. As a proactive protocol it finds another route from its routing table and as a reactive protocol it search route on-demand basis when no alternate route is found. The node is supposed to be no longer available in the network, if a node has not received any message from some outgoing nodes for a specified period of time. If any node senses that next node has become unavailable then precursor node attempts to repair the broken node itself or tries to find another route to the destination when no alternate route is available, instead of sending REER message to the source as shown flowchart in figure 3.1.

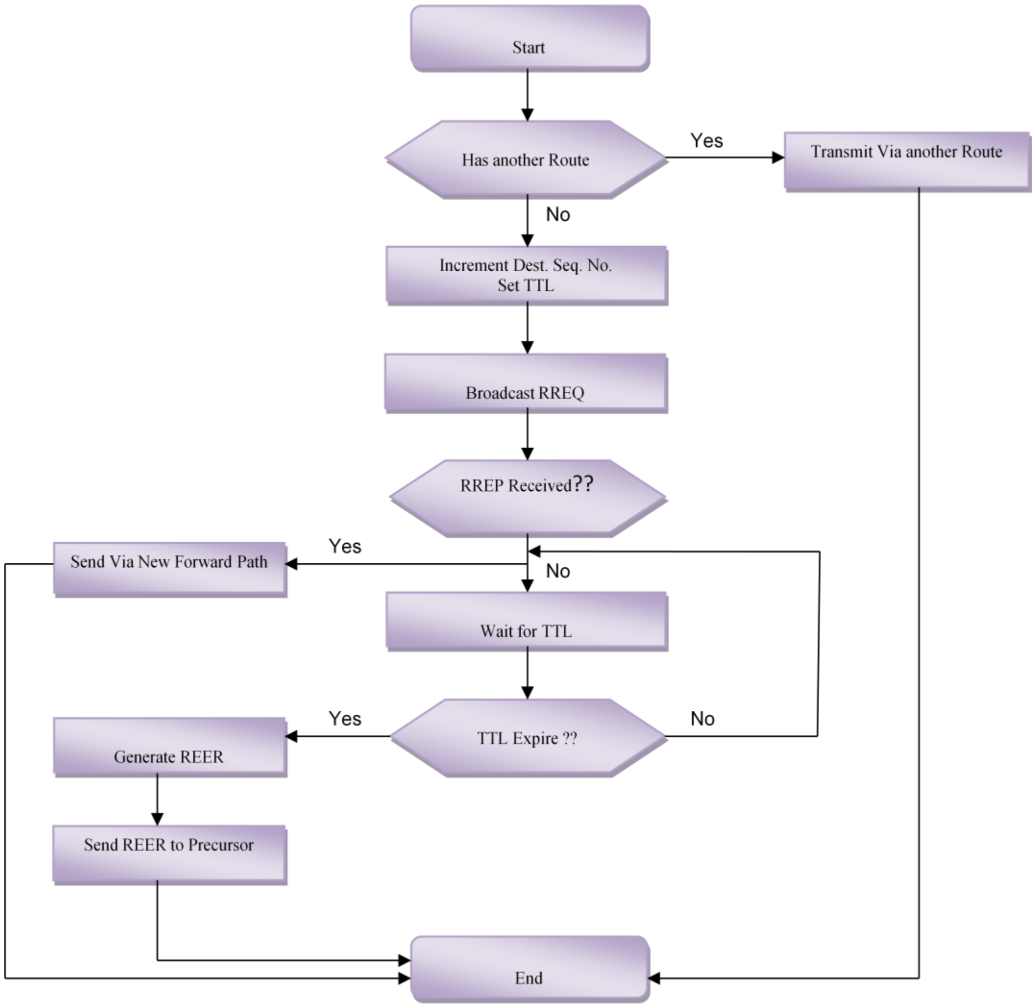


Figure 3.1 Flow chart for local repair in AOMDVLR

If the precursor node attempts to repair the broken node itself, fewer number of data packets will be lost and the route may be re-establish with a lower overhead. Also, the source node is not at all worried with another Route Discovery procedure.Local Repair is not expected to show much advantage for smaller routes, but for larger routes, especially with 10 or more than 10 hops, Local Repair is awfully beneficial. This is because in larger routes, there are more probability to breakage of links and if the intermediary nodes always carry on sending Route Error message to the source which in turn carry on initiating Route Discovery, vast number of control message are devoted and the performance will deteriorate.

Local Repair makes the precursor node of the break to effort a repair of the route. This is done through broadcasting a RREQ (Route Request) with a time to live (TTL) set to the last known distance of the destination plus an increment value. This TTL value is used with a supposition that the destination is not likely to be distant away from where it was before the break.

This precursor node increments the sequence number of the destination in its RREQ message by 1 before broadcasting it. This avoids the nodes further precursor of this node from respond to the RREQ. Thus, this mechanism prevents loop construction. End-to-end delay is improved because loss can be recovered within the neighboring nodes instead of original source node. This approach gets better consistency in term of packet release ratio as compared with AOMDV. Note that this RREQ broadcast by intermediate node is done only once. If no node replies to this broadcast within a specified TTL, the intermediate node simply sends a RERR back to the originating node by listing all the destinations which have become unreachable due to the break.

According to above scenarios AOMDV-LR follows this algorithm:

Step 1: Proactive Multipath routing: have one active and multi alternate routes for one destination in its routing table at each node as shown as table 4.1.

Step 2: In figure 3.2, a node or link goes down in the active route i.e. C-E link. If intermediate node C has other sub routes to destination D in its routing table, it will select the sub route with the least hop count and send packet via this route.

TABLE 3.1

Routing Table for Node B

DESTINATION	DEST. SEQ. NO	NEXT HOP	HOP COUNT	PRIORITY NOTICE
D	2	C	2	ACTIVE ROUTE
D	2	K	3	SUB ROUTE

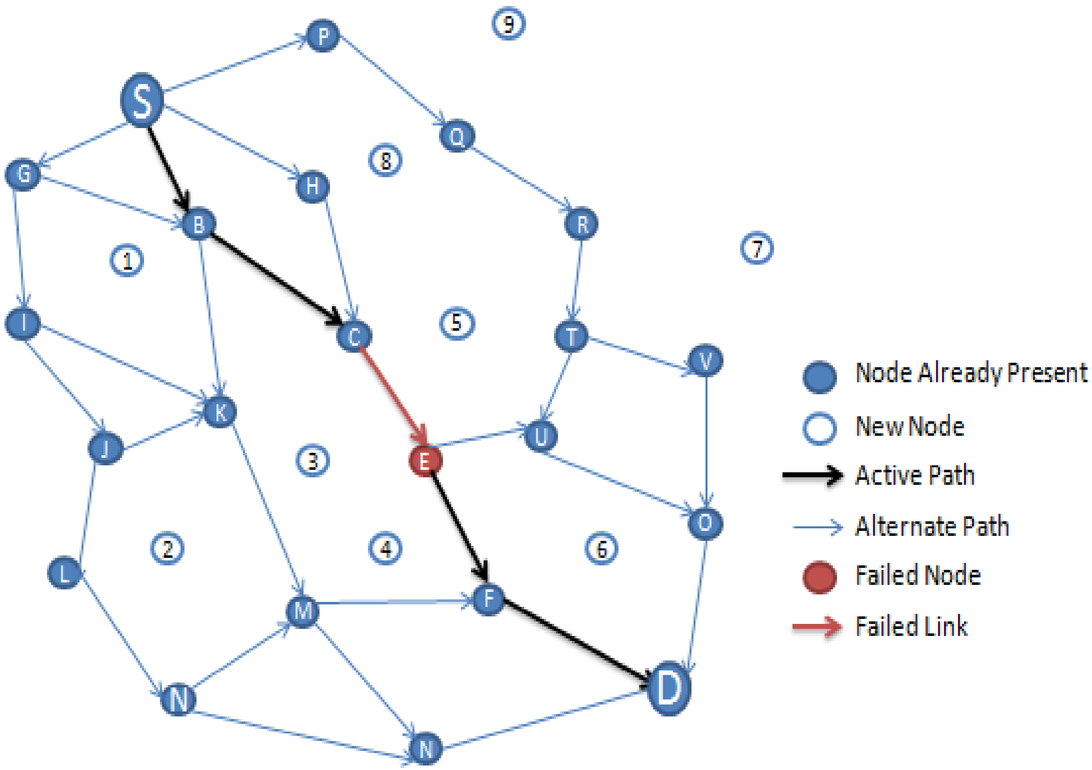


Figure 3.2: Node or link break in the active route

But if it has no sub-route to destination D, node C does not send any RERR message to the source. Instead, it attempt to reach destination node D via another hop. It investigates again to reach to node D by sending a RREQ message to its neighbor only by incrementing sequence number of the destination by 1 before to prevent loop construction. And when it finds any node along its new path node 5 and starts sending packets via node 5 to D (1) as in figure 3.3.

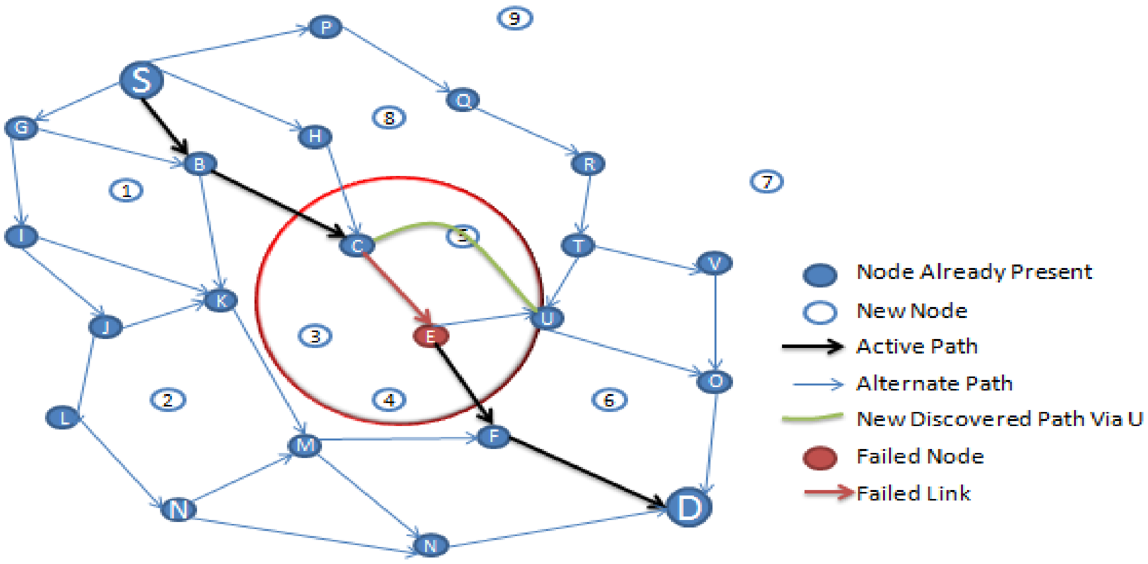


Figure 3.3 Local repair by intermediate route

Step 3: If the node C could not investigate a new path to destination D, it will send out a RERR packet to the source node S via its precursor node B. If the routing table of node B has another sub-route to destination D, B will select a new sub-route to D according to step-2. If B does not found any sub route to D it again send RERR to its precursor node and this process is repeated till source S if no alternate path is found in the precursors node. Intermediate node will send further packets via these new / old sub-route if found. If source S had only one route to destination D, it will restart route discovery for this destination as in figure 3.4.

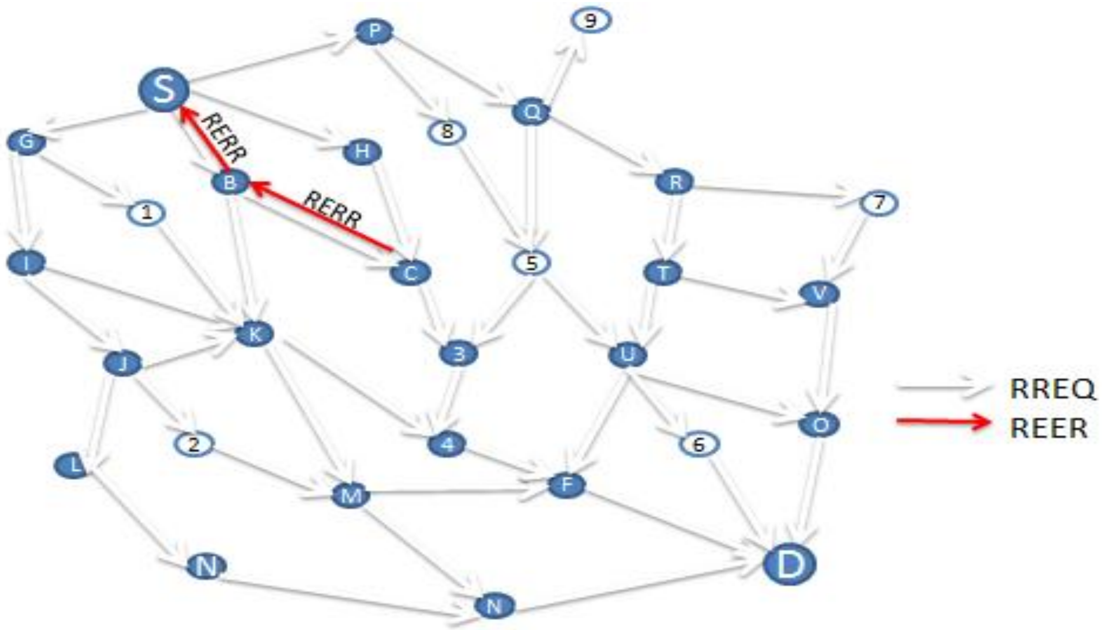


Figure 3.4 Source restart route discovery after receiving RERR

CHAPTER 4

SIMULATION RESULTS AND PERFORMANCE ANALYSIS

Simulation

Scenario files generation in ns2

TCL file specifications

Simulation Screenshots

Performance metric

Results and Performance analysis

SIMULATION RESULTS AND PERFORMANCE ANALYSIS

4.1. Simulation

For the simulation and evaluation of the performance of the AOMDVLR NS-2 simulator and outcome is used to compare with the original AOMDV protocol. The NS-2 is developed at UC Berkeley which is a discrete event driven simulator. We have used Red Hat Linux environment with version NS-2.34 of network simulator. NS-2 is appropriate for designing new protocols, comparing dissimilar protocols and traffic evaluation. It is an object oriented simulation written in C++, where OTcl interpreter is a frontend. The error-free wireless channel model is selected in the simulations in order to isolate the effects of node mobility. The simulations with varying nodes are performed in a square field of dimensions 2000m×2000m. The nodes are initially placed uniformly at random in the field. For the simulation of node movements the random waypoint mobility model is used. Pause time is always set to zero. Several CBR/UDP connections is consisted by several traffic pattern between randomly chosen source destination pairs. Data packets have a fixed size of 512 bytes in all the experiments, and the simulation time is 1000 seconds. Each data point in the plots is an average of five such runs with different number of nodes. Identical traffic and mobility scenarios are used across all protocol variations. All the summarized simulation parameter for the proposed protocol AOMDVLR and existing protocol AOMDV are given as in table 4.1.

Table 4.1: Simulation Parameter for AOMDV-LR and AOMDV

S.No.	**Parameters**	**Values**
1	Area Size	2000m X 2000m
2	Number of Nodes	5-25
3	Node mobility speed	0.9v to 1.1v.
4	Propagation range	250m
5	Mobility model	Random way point
6	Data rate	5Kbps
7	Simulation time	1000s
8	Pause Time	0
9	No. of experiments	5 times

4.2 Scenario files generation in ns2

In our case, we have generated several scenario files to compute the performance of our protocols. It has been recommended that the average number of neighbor nodes should be maintained among 6-8 for healthier performance and scalability. The area within which these nodes are allowed to navigate is referred to the room size or simply area. This is described by the length and breadth of the enclosed space within which the nodes can move freely. We design our scenarios for different number of nodes ranging from 5 to 25.

4.3 TCL file specifications

The individual aspects of the scenario implementation as described in the TCL file are listed as table 4.2:

Table 4.2 TCL file specifications

Channel	Wireless Channel
Network Interface type	Wireless
Propagation Model	Two ray ground
MAC layer	802.11
Buffer type	FIFO
Size of the buffer	50 packets
Antenna type	Omni directional
Bandwidth of each node	1MHz
Packet size	512 bytes

The TCL file when executed for a particular scenario produces two new files of the type 'trace' and 'nam'. These two files hold the information about the implementation of the protocol described in the tcl on the specified scenario file. Individual particulars like the number of sent and received packets, packet loss, packet delivery ratio etc can all be extracted from these two files.

4.4. Simulation Screenshots:

The sample screen shot of a scenario of 25 mobile nodes is shown in the following screenshot

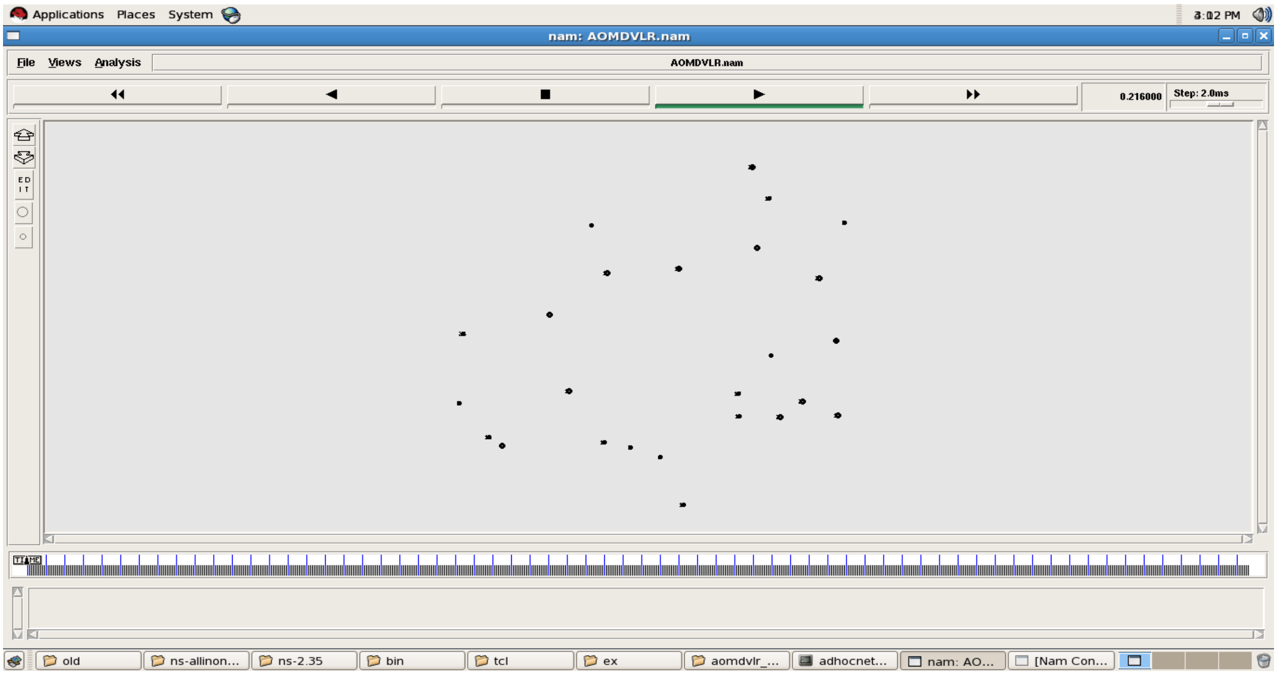


Figure 4.1(a) Screen shot of execution of nam file

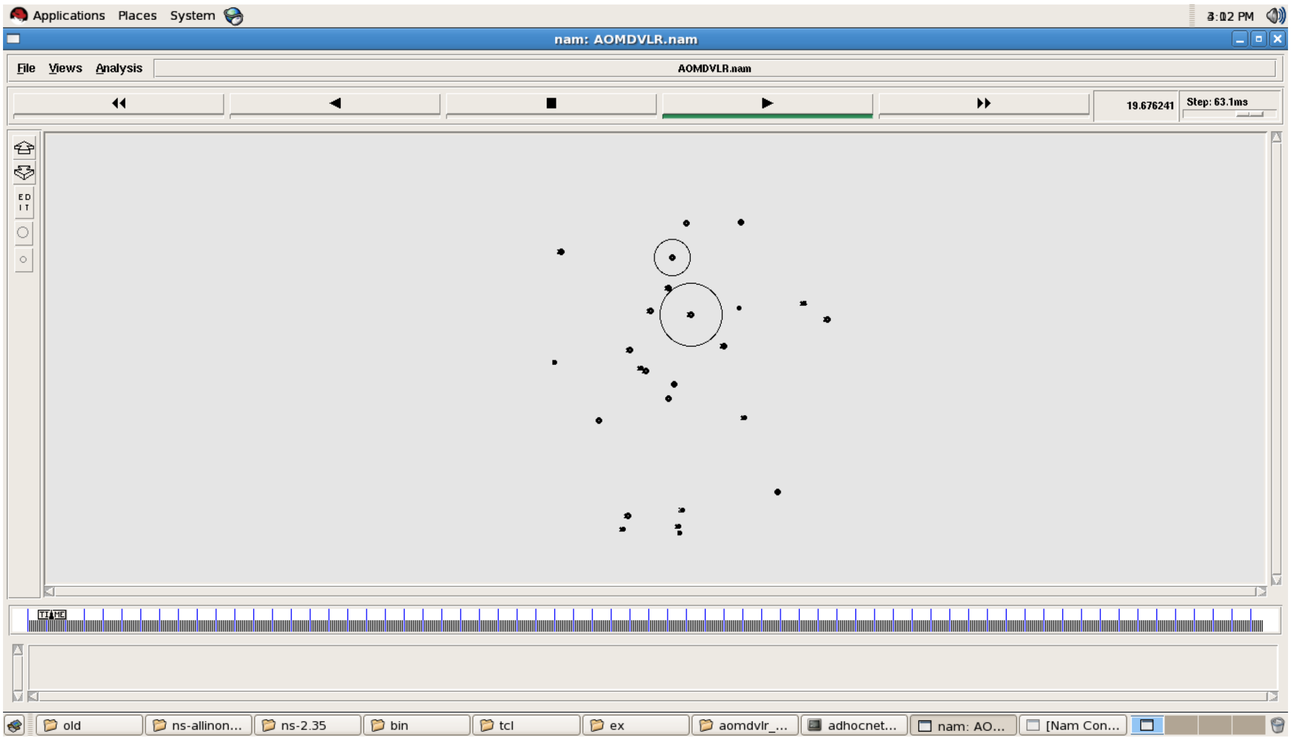


Figure 4.1(b) Screen shot of execution of nam file

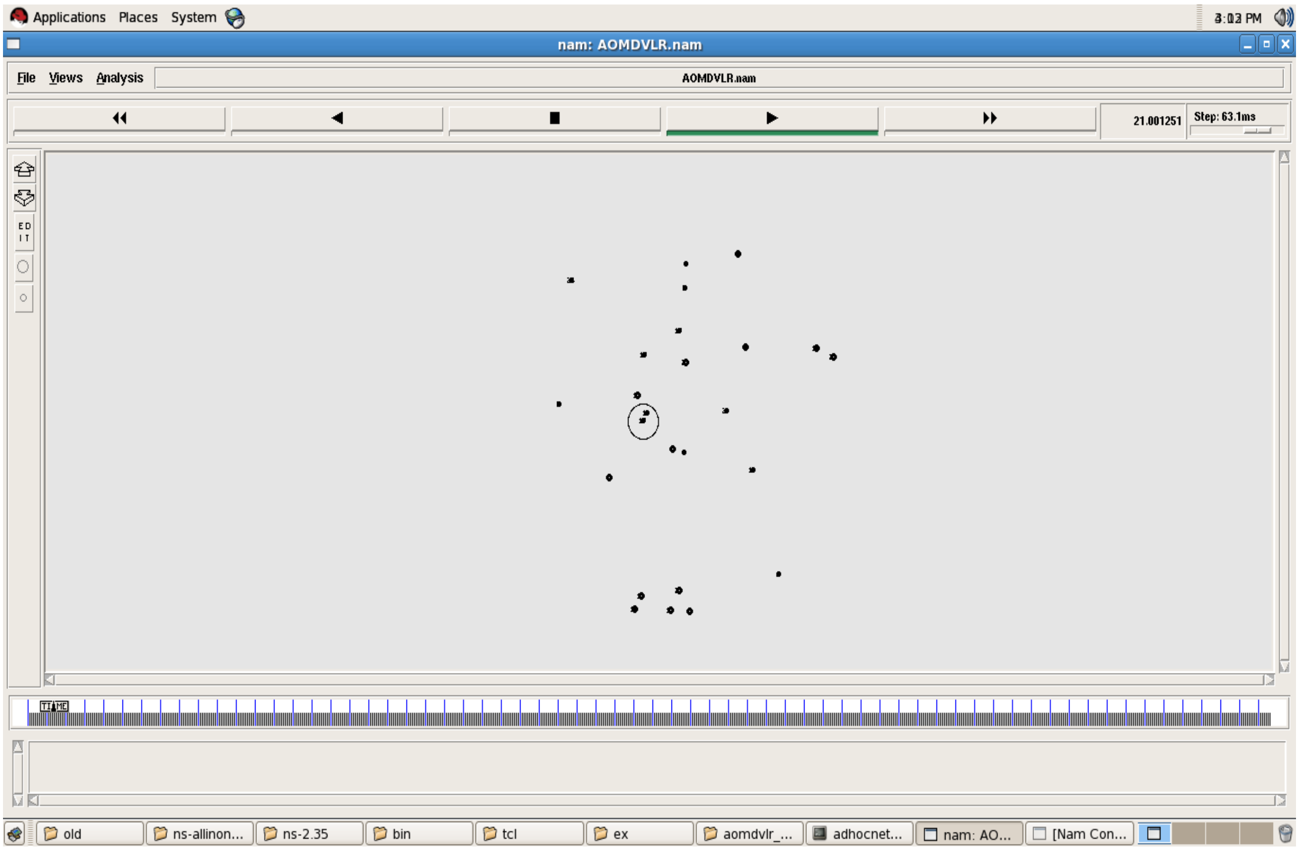


Figure 4.1(c) Screen shot of execution of nam file

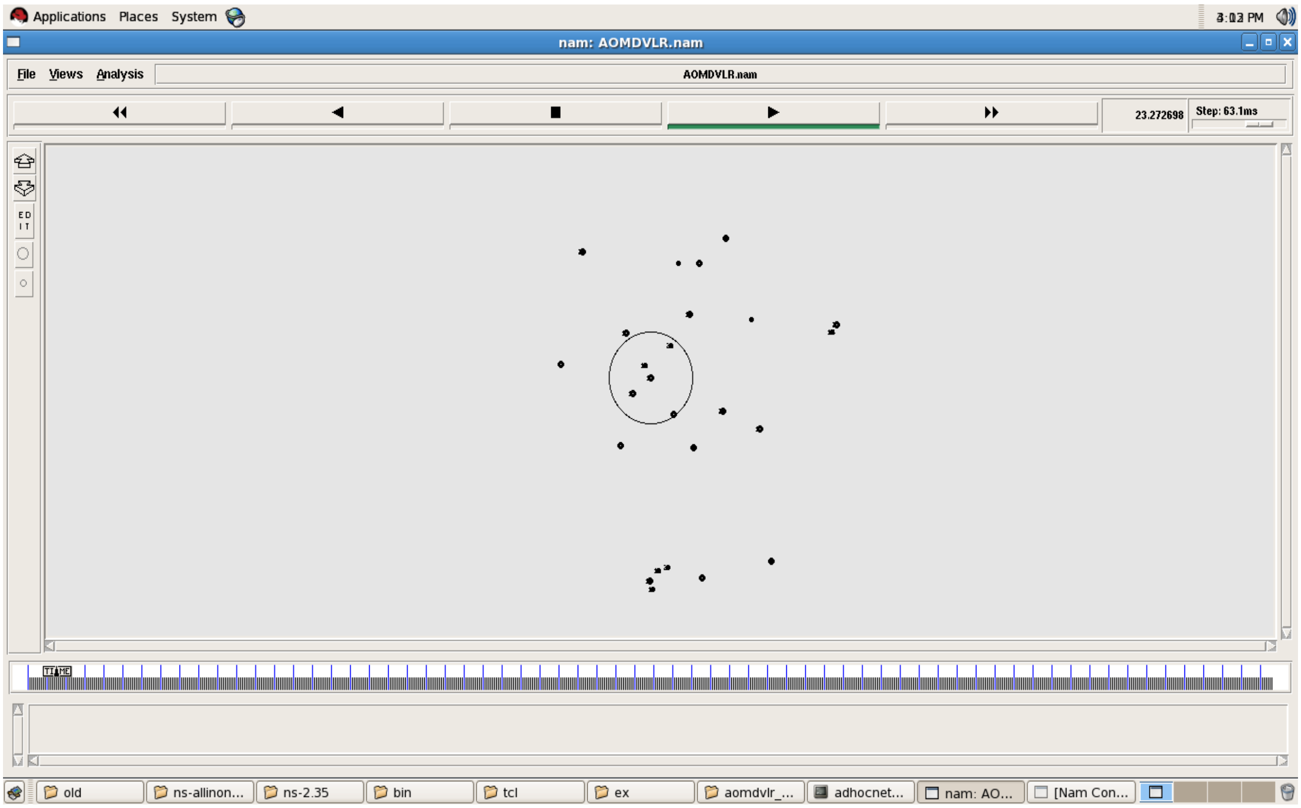


Figure 4.1(d) Screen shot of execution of nam file

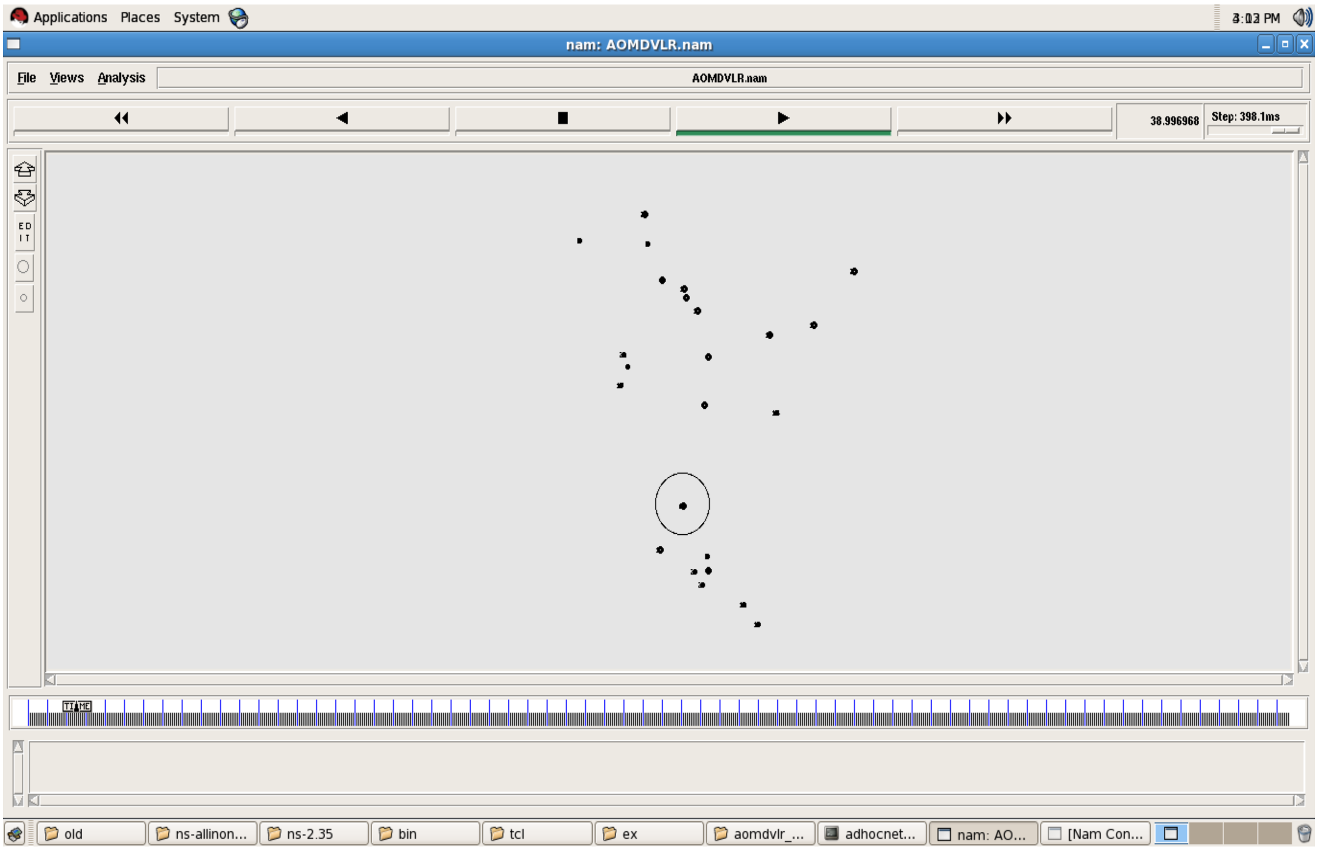


Figure 4.1(e) Screen shot of execution of nam file

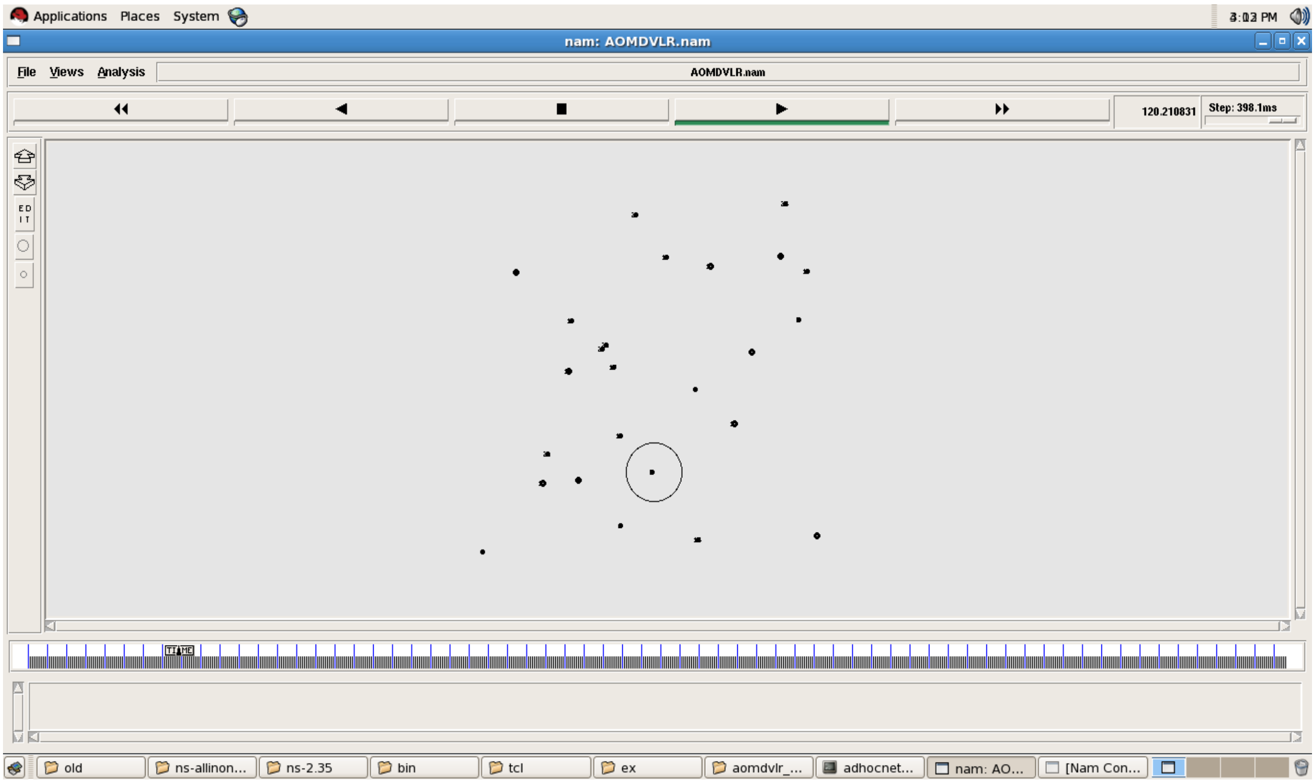


Figure 4.1(f) Screen shot of execution of nam file

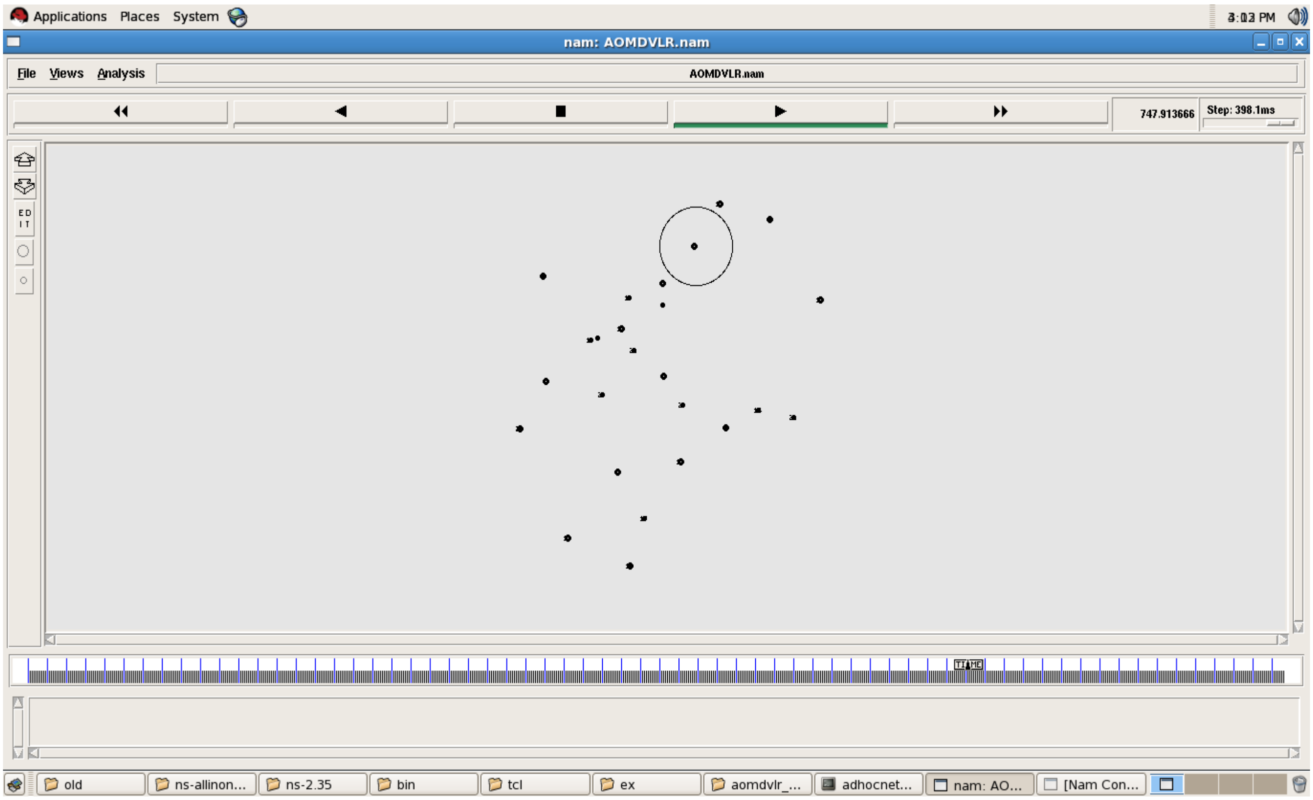


Figure 4.1(g) Screen shot of execution of nam file

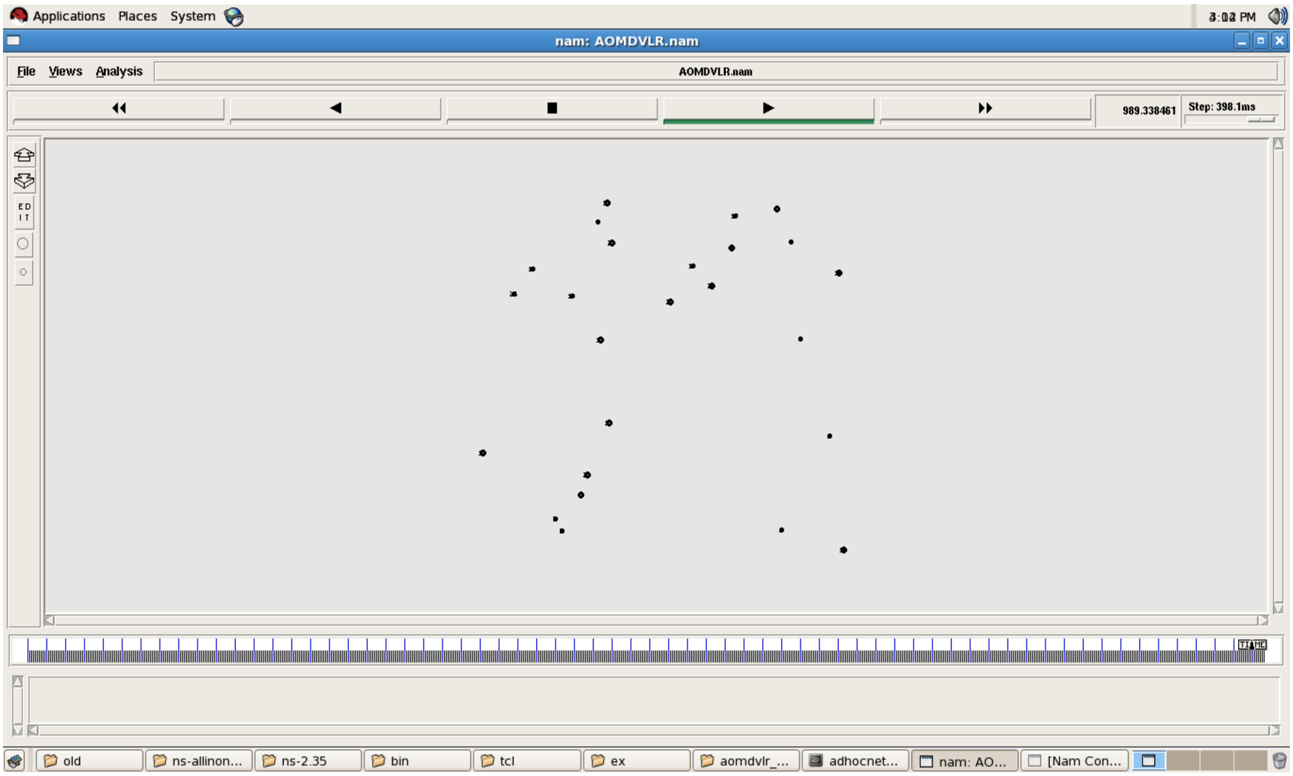
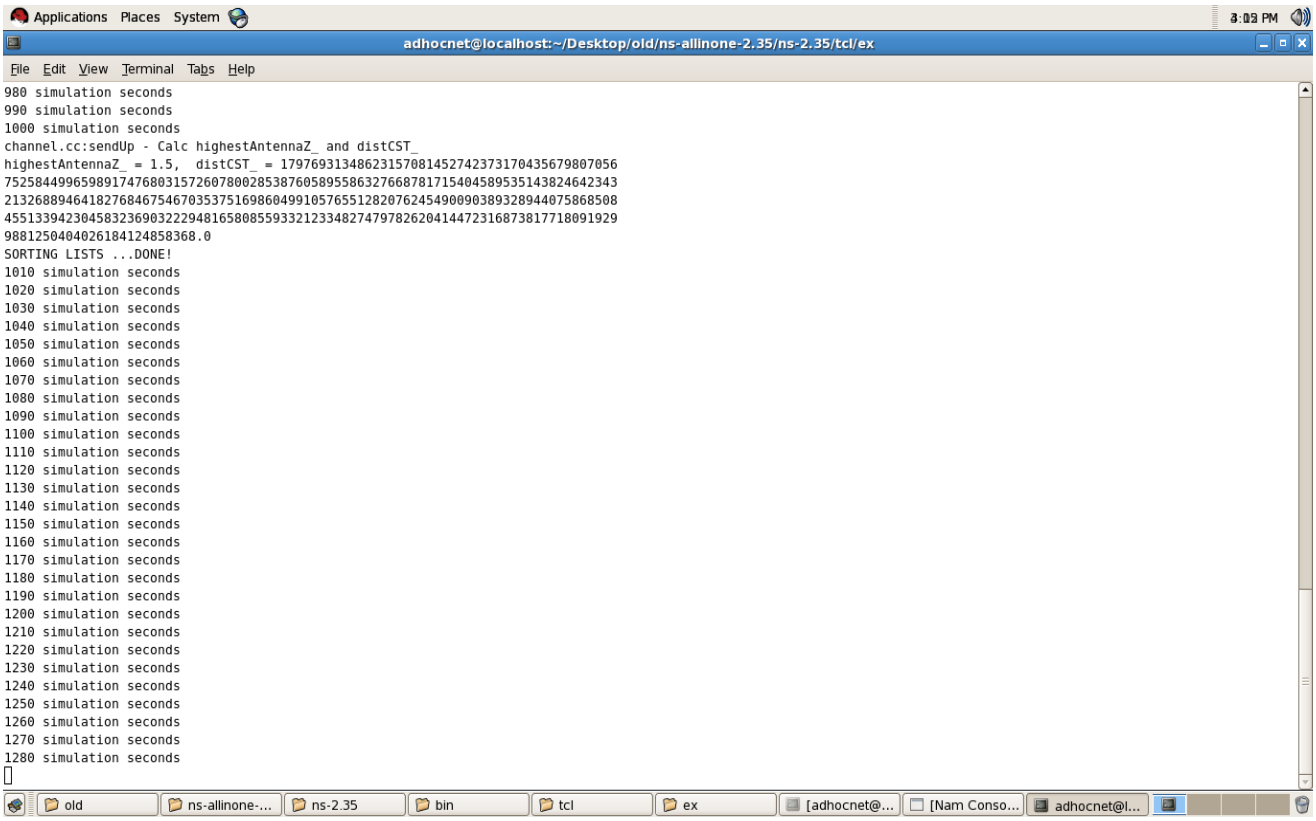
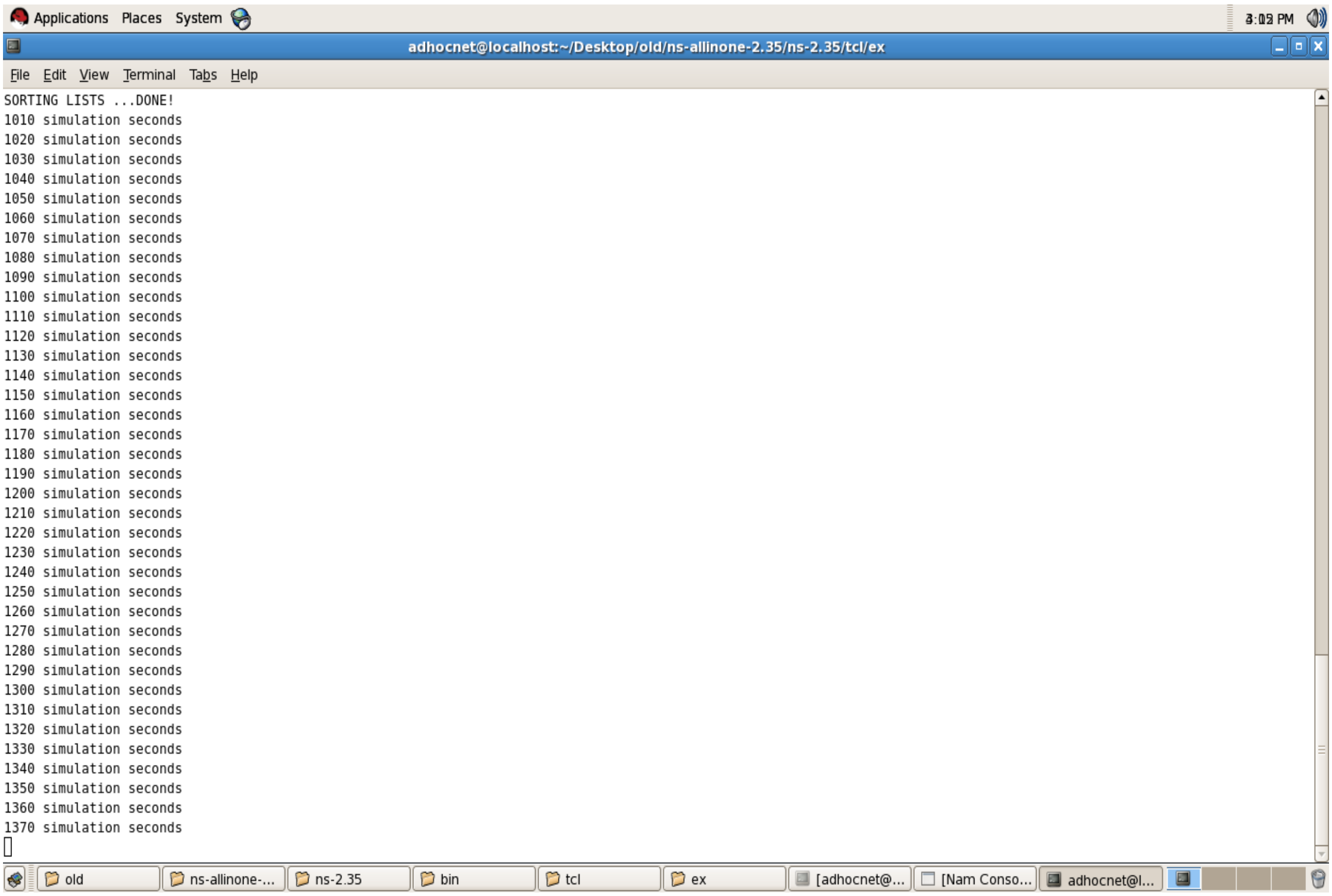


Figure 4.1(h) Screen shot of execution of nam file


Applications Places System
3:03 PM
adhocnet@localhost:~/Desktop/old/ns-allinone-2.35/ns-2.35/tcl/ex
File Edit View Terminal Tabs Help
old
ns-allinone-...
ns-2.35
bin
tcl
ex
[adhocnet@...
[Nam Conso...
adhocnet@l...

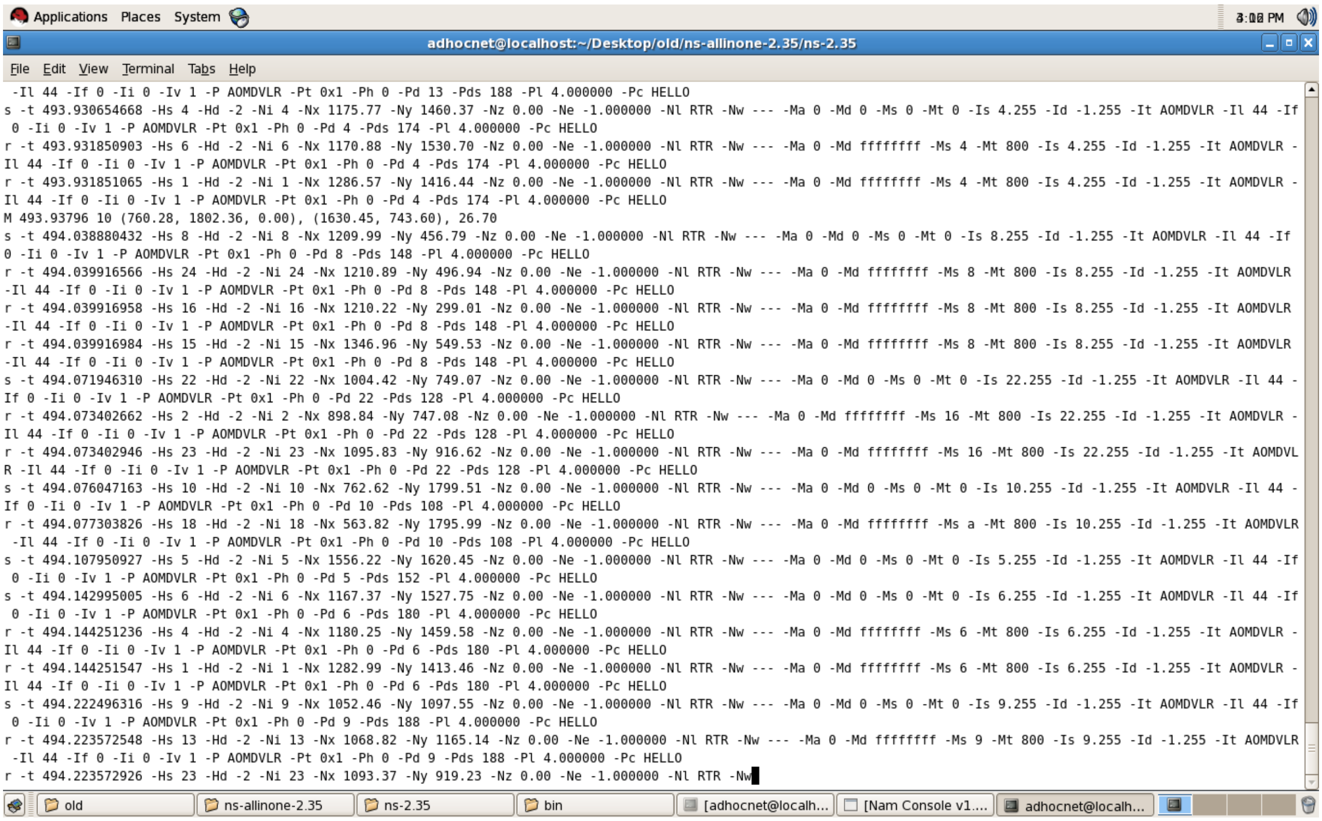
```
980 simulation seconds
990 simulation seconds
1000 simulation seconds
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 179769313486231570814527423731704356798070567525844996598917476803157260780028538760589558632766878171540458953514382464234321326889464182768467546703537516986049910576551282076245490090389328944075868508455133942304583236903222948165808559332123348274797826204144723168738177180919299881250404026184124858368.0
SORTING LISTS ...DONE!
1010 simulation seconds
1020 simulation seconds
1030 simulation seconds
1040 simulation seconds
1050 simulation seconds
1060 simulation seconds
1070 simulation seconds
1080 simulation seconds
1090 simulation seconds
1100 simulation seconds
1110 simulation seconds
1120 simulation seconds
1130 simulation seconds
1140 simulation seconds
1150 simulation seconds
1160 simulation seconds
1170 simulation seconds
1180 simulation seconds
1190 simulation seconds
1200 simulation seconds
1210 simulation seconds
1220 simulation seconds
1230 simulation seconds
1240 simulation seconds
1250 simulation seconds
1260 simulation seconds
1270 simulation seconds
1280 simulation seconds
```

Figure 4.2(a) Screen shot of simulation second


Applications Places System
3:03 PM
adhocnet@localhost:~/Desktop/old/ns-allinone-2.35/ns-2.35/tcl/ex
File Edit View Terminal Tabs Help
old
ns-allinone-...
ns-2.35
bin
tcl
ex
[adhocnet@...
[Nam Conso...
adhocnet@l...

```
SORTING LISTS ...DONE!
1010 simulation seconds
1020 simulation seconds
1030 simulation seconds
1040 simulation seconds
1050 simulation seconds
1060 simulation seconds
1070 simulation seconds
1080 simulation seconds
1090 simulation seconds
1100 simulation seconds
1110 simulation seconds
1120 simulation seconds
1130 simulation seconds
1140 simulation seconds
1150 simulation seconds
1160 simulation seconds
1170 simulation seconds
1180 simulation seconds
1190 simulation seconds
1200 simulation seconds
1210 simulation seconds
1220 simulation seconds
1230 simulation seconds
1240 simulation seconds
1250 simulation seconds
1260 simulation seconds
1270 simulation seconds
1280 simulation seconds
1290 simulation seconds
1300 simulation seconds
1310 simulation seconds
1320 simulation seconds
1330 simulation seconds
1340 simulation seconds
1350 simulation seconds
1360 simulation seconds
1370 simulation seconds
```

Figure 4.2(b) Screen shot of simulation second



```
 -Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 13 -Pds 188 -Pl 4.000000 -Pc HELLO
s -t 493.930654668 -Hs 4 -Hd -2 -Ni 4 -Nx 1175.77 -Ny 1460.37 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 4.255 -Id -1.255 -It AOMDVLR -Il 44 -If
 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 4 -Pds 174 -Pl 4.000000 -Pc HELLO
r -t 493.931850903 -Hs 6 -Hd -2 -Ni 6 -Nx 1170.88 -Ny 1530.70 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms 4 -Mt 800 -Is 4.255 -Id -1.255 -It AOMDVLR -
Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 4 -Pds 174 -Pl 4.000000 -Pc HELLO
r -t 493.931851065 -Hs 1 -Hd -2 -Ni 1 -Nx 1286.57 -Ny 1416.44 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms 4 -Mt 800 -Is 4.255 -Id -1.255 -It AOMDVLR -
Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 4 -Pds 174 -Pl 4.000000 -Pc HELLO
M 493.93796 10 (760.28, 1802.36, 0.00), (1630.45, 743.60), 26.70
s -t 494.038880432 -Hs 8 -Hd -2 -Ni 8 -Nx 1209.99 -Ny 456.79 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 8.255 -Id -1.255 -It AOMDVLR -Il 44 -If
0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 8 -Pds 148 -Pl 4.000000 -Pc HELLO
r -t 494.039916566 -Hs 24 -Hd -2 -Ni 24 -Nx 1210.89 -Ny 496.94 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms 8 -Mt 800 -Is 8.255 -Id -1.255 -It AOMDVLR
-Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 8 -Pds 148 -Pl 4.000000 -Pc HELLO
r -t 494.039916958 -Hs 16 -Hd -2 -Ni 16 -Nx 1210.22 -Ny 299.01 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms 8 -Mt 800 -Is 8.255 -Id -1.255 -It AOMDVLR
-Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 8 -Pds 148 -Pl 4.000000 -Pc HELLO
r -t 494.039916984 -Hs 15 -Hd -2 -Ni 15 -Nx 1346.96 -Ny 549.53 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms 8 -Mt 800 -Is 8.255 -Id -1.255 -It AOMDVLR
-Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 8 -Pds 148 -Pl 4.000000 -Pc HELLO
s -t 494.071946310 -Hs 22 -Hd -2 -Ni 22 -Nx 1004.42 -Ny 749.07 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 22.255 -Id -1.255 -It AOMDVLR -Il 44 -
If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 22 -Pds 128 -Pl 4.000000 -Pc HELLO
r -t 494.073402662 -Hs 2 -Hd -2 -Ni 2 -Nx 898.84 -Ny 747.08 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms 16 -Mt 800 -Is 22.255 -Id -1.255 -It AOMDVLR -
Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 22 -Pds 128 -Pl 4.000000 -Pc HELLO
r -t 494.073402946 -Hs 23 -Hd -2 -Ni 23 -Nx 1095.83 -Ny 916.62 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms 16 -Mt 800 -Is 22.255 -Id -1.255 -It AOMDVL
R -Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 22 -Pds 128 -Pl 4.000000 -Pc HELLO
s -t 494.076047163 -Hs 10 -Hd -2 -Ni 10 -Nx 762.62 -Ny 1799.51 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 10.255 -Id -1.255 -It AOMDVLR -Il 44 -
If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 10 -Pds 108 -Pl 4.000000 -Pc HELLO
r -t 494.077303826 -Hs 18 -Hd -2 -Ni 18 -Nx 563.82 -Ny 1795.99 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms a -Mt 800 -Is 10.255 -Id -1.255 -It AOMDVLR
 -Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 10 -Pds 108 -Pl 4.000000 -Pc HELLO
s -t 494.107950927 -Hs 5 -Hd -2 -Ni 5 -Nx 1556.22 -Ny 1620.45 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 5.255 -Id -1.255 -It AOMDVLR -Il 44 -If
 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 5 -Pds 152 -Pl 4.000000 -Pc HELLO
s -t 494.142995005 -Hs 6 -Hd -2 -Ni 6 -Nx 1167.37 -Ny 1527.75 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 6.255 -Id -1.255 -It AOMDVLR -Il 44 -If
 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 6 -Pds 180 -Pl 4.000000 -Pc HELLO
r -t 494.144251236 -Hs 4 -Hd -2 -Ni 4 -Nx 1180.25 -Ny 1459.58 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms 6 -Mt 800 -Is 6.255 -Id -1.255 -It AOMDVLR -
Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 6 -Pds 180 -Pl 4.000000 -Pc HELLO
r -t 494.144251547 -Hs 1 -Hd -2 -Ni 1 -Nx 1282.99 -Ny 1413.46 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms 6 -Mt 800 -Is 6.255 -Id -1.255 -It AOMDVLR -
Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 6 -Pds 180 -Pl 4.000000 -Pc HELLO
s -t 494.222496316 -Hs 9 -Hd -2 -Ni 9 -Nx 1052.46 -Ny 1097.55 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 9.255 -Id -1.255 -It AOMDVLR -Il 44 -If
 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 9 -Pds 188 -Pl 4.000000 -Pc HELLO
r -t 494.223572548 -Hs 13 -Hd -2 -Ni 13 -Nx 1068.82 -Ny 1165.14 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma 0 -Md ffffffff -Ms 9 -Mt 800 -Is 9.255 -Id -1.255 -It AOMDVLR
 -Il 44 -If 0 -Ii 0 -Iv 1 -P AOMDVLR -Pt 0x1 -Ph 0 -Pd 9 -Pds 188 -Pl 4.000000 -Pc HELLO
r -t 494.223572926 -Hs 23 -Hd -2 -Ni 23 -Nx 1093.37 -Ny 919.23 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw
```

Figure 4.3 Screen shot of execution of trace file

4.5. Performance metric

In Multipath traffic environment with node mobility following metric are chosen to compare the performance of routing protocol.

ROUTING OVERHEAD: It is the total number of routing packets or control packets generated during the simulation by routing protocol. The entire packets sent or forwarded at network layer is consider routing overhead.

$$\mathrm{RO} = \sum_{i=1}^{n} \mathrm{Cs}_i + \sum_{i=1}^{n} \mathrm{Cf}_i \qquad (1)$$

Where RO is routing overhead, Cs_i is control packet sent and Cf_i is control packet forwarded

PACKET LOSS RATIO**:** Packet loss ratio is the difference between number of data packet sent and data packet receive in the network.

$$\mathrm{PLR} = \frac{\sum_{i=1}^{n} \mathrm{Ds}_i - \sum_{i=1}^{n} \mathrm{Dr}_i}{\sum_{i=1}^{n} \mathrm{Ds}_i} * 100 \qquad (2)$$

Where PLR is packet loss ratio, Ds_i is data packet sent and Dr_i is data packet received

PACKET DELIVERY RATIO: Packet delivery ratio (PDR) is defined as the percentage of the ratio between the number of packets sent by sources and the number of received packets at destination. This performance evaluation parameter measures reliability, effectiveness and efficiency of a protocol.

$$\mathrm{PDR} = \frac{\sum_{i=1}^{n} \mathrm{Dr}_i}{\sum_{i=1}^{n} \mathrm{Ds}_i} * 100 \qquad (3)$$

Where PDR is packet delivery ratio, $\mathrm{Ds}_i$is data packet sent and Dr_i is data packet received.

4.6. Results and Performance analysis

In the simulated scenario the number of CBR/UDP connections is varied while the mean speed is fixed at 5 m/s and the offered load at 160 kb/s. For a constant mean node speed and constant offered load, increasing the number of connections will spread the same amount of traffic among several connections. This will stress the protocol, as it requires a routing protocol to maintain routes between more numbers of source-destination pairs. Moreover, each route discovery will become more expensive because of the smaller amount of traffic over each connection. Figure 4.4 demonstrates how protocol routing overhead varies with varying number of nodes. The general trend observed from the figure, AOMDVLR gave result better than AOMDV. It is observed that, the routing overhead of AOMDVLR is lower than AOMDV for all varied connection. As the number of nodes increases the performance gain by local repair becomes more significant. This shows that the AOMDVLR performs better as compared to AOMDV in all possible number of nodes.

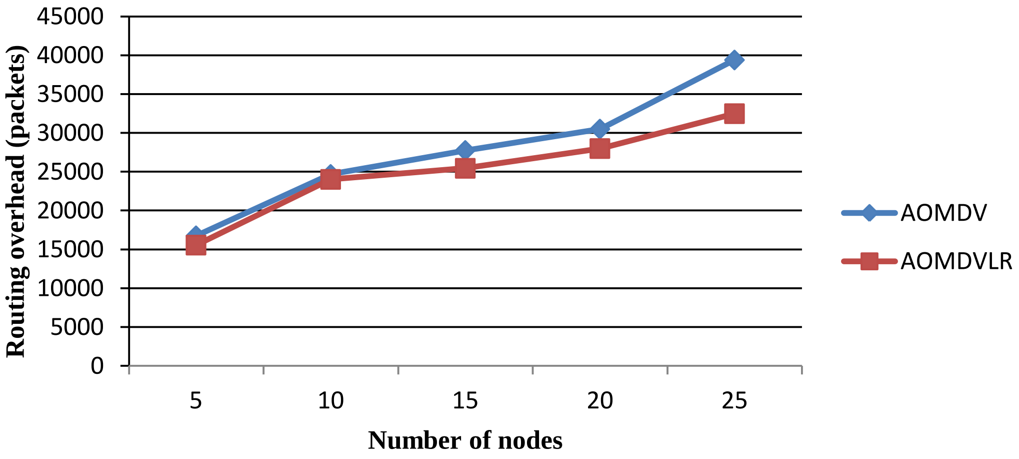


Figure 4.4 Routing overhead in varied connections

Now we can analyze the Figure-4.5. It shows that, packet loss ratio for AOMDVLR decreases as the number of nodes increased. It can be concluded that the packet loss ratio of AOMDV-LR is comparatively better than AOMDV which is highly real time requirement.

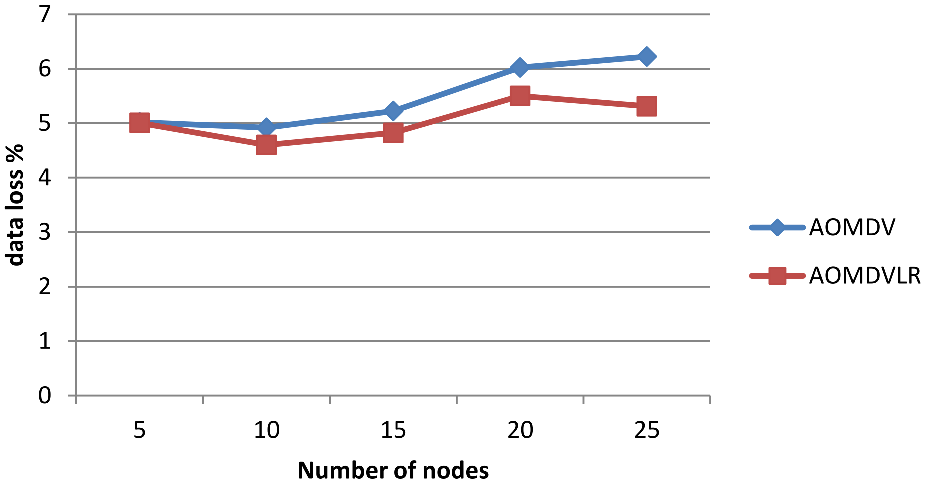


Figure 4.5 Packet loss ratio in varied connections

It is maximized the Packet Delivery ratio of proposed routing protocol due to local route repair of AOMDV. From Figure-4.6 it is observed that, AOMDVLR performance in terms of Packet Delivery ratio is better than AOMDV in different connections.

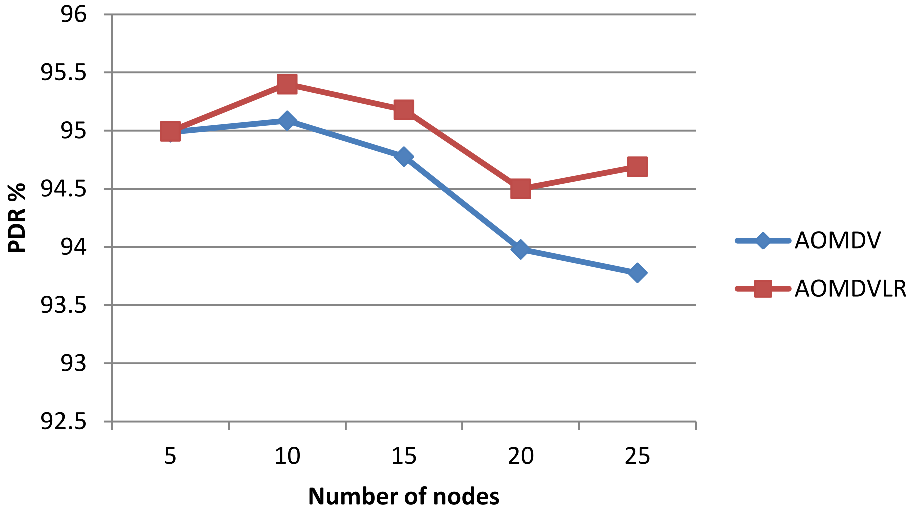
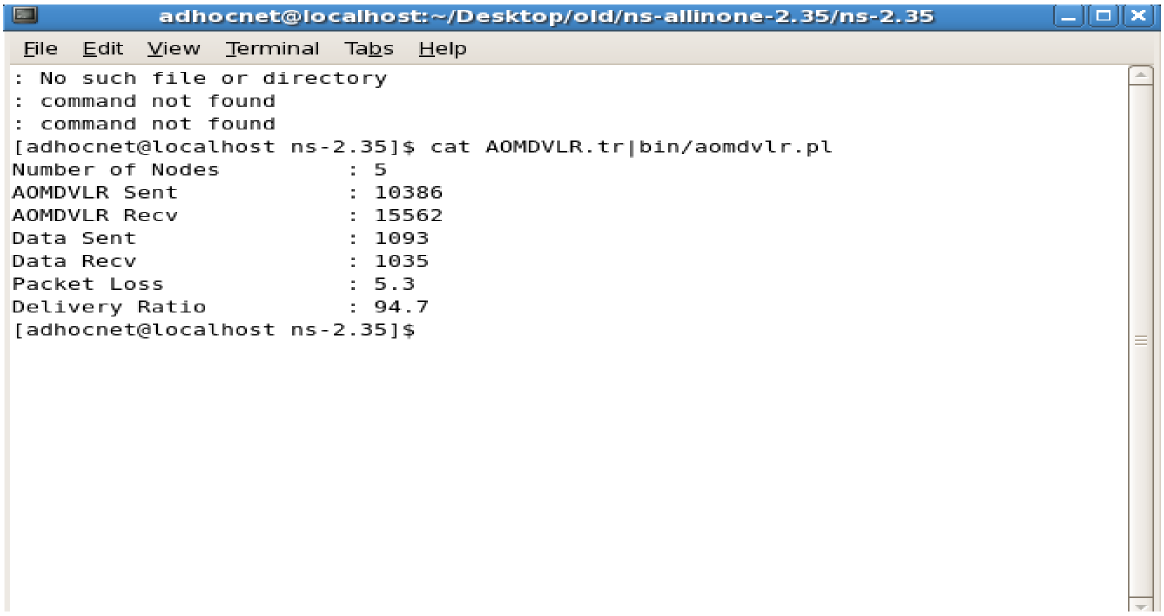


Figure 4.6 Packet delivery Ratio in varied connections

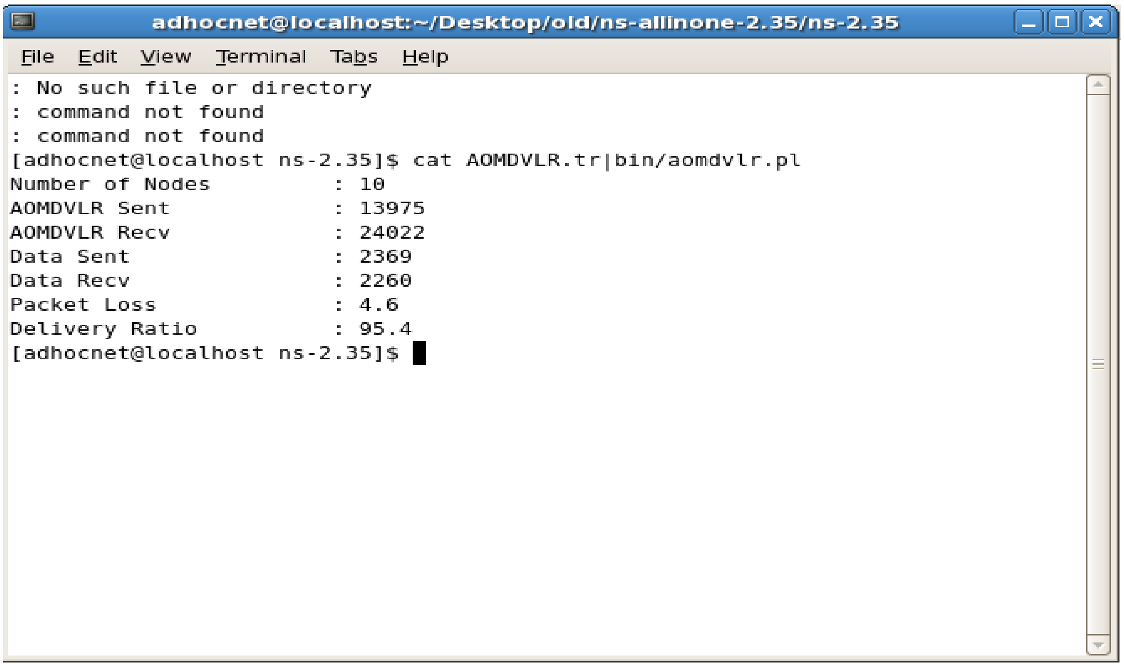
From all these scenario sets, it can be concluded that the AOMDVLR protocol can successfully calculate route and forward data packets in Wireless Mesh Networks scenarios better than the original AOMDV in the aspects of Routing Overhead, Packet Delivery Ratio and packet loss ratio.

The above result is evaluated from simulation of a new protocol AOMDVLR as shown in following screenshots:


adhocnet@localhost:~/Desktop/old/ns-allinone-2.35/ns-2.35
File Edit View Terminal Tabs Help

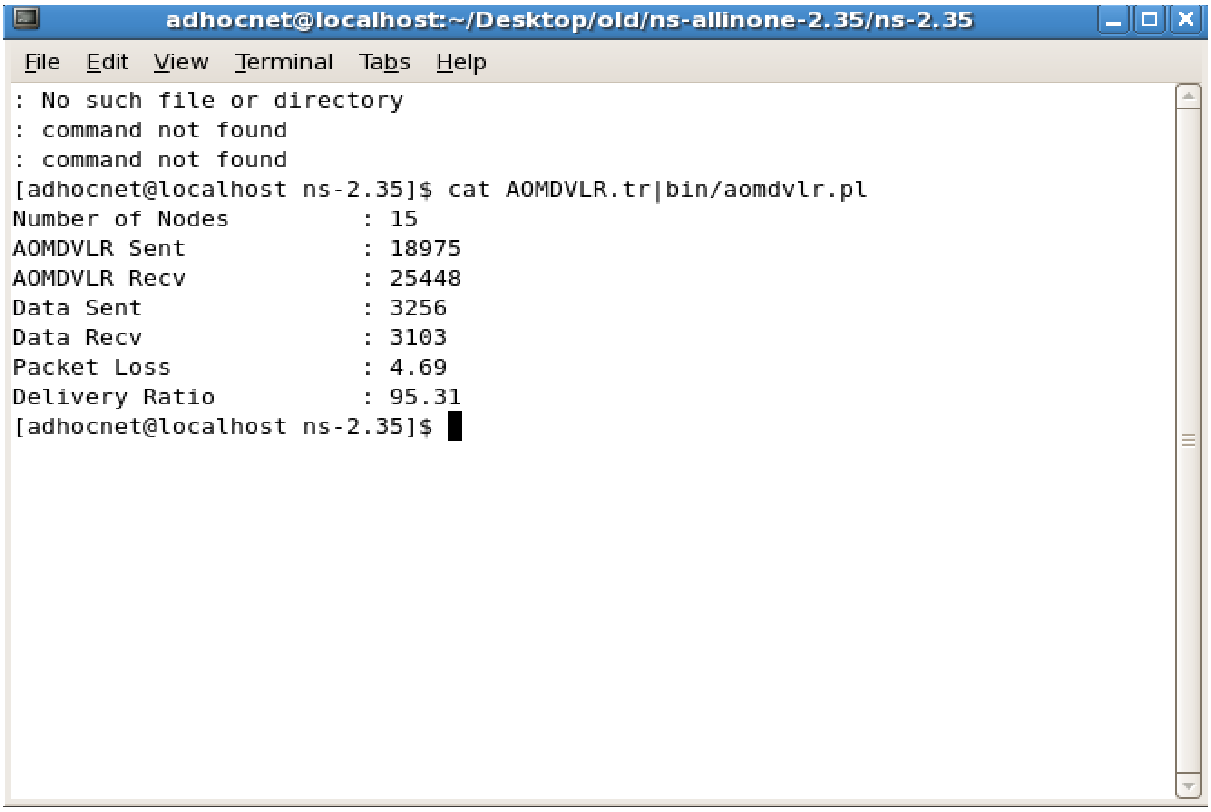
```
: No such file or directory
: command not found
: command not found
[adhocnet@localhost ns-2.35]$ cat AOMDVLR.tr|bin/aomdvlr.pl
Number of Nodes          : 5
AOMDVLR Sent             : 10386
AOMDVLR Recv             : 15562
Data Sent                : 1093
Data Recv                : 1035
Packet Loss              : 5.3
Delivery Ratio           : 94.7
[adhocnet@localhost ns-2.35]$
```

Figure 4.7 (a) Outcome with 5 nodes


adhocnet@localhost:~/Desktop/old/ns-allinone-2.35/ns-2.35
File Edit View Terminal Tabs Help

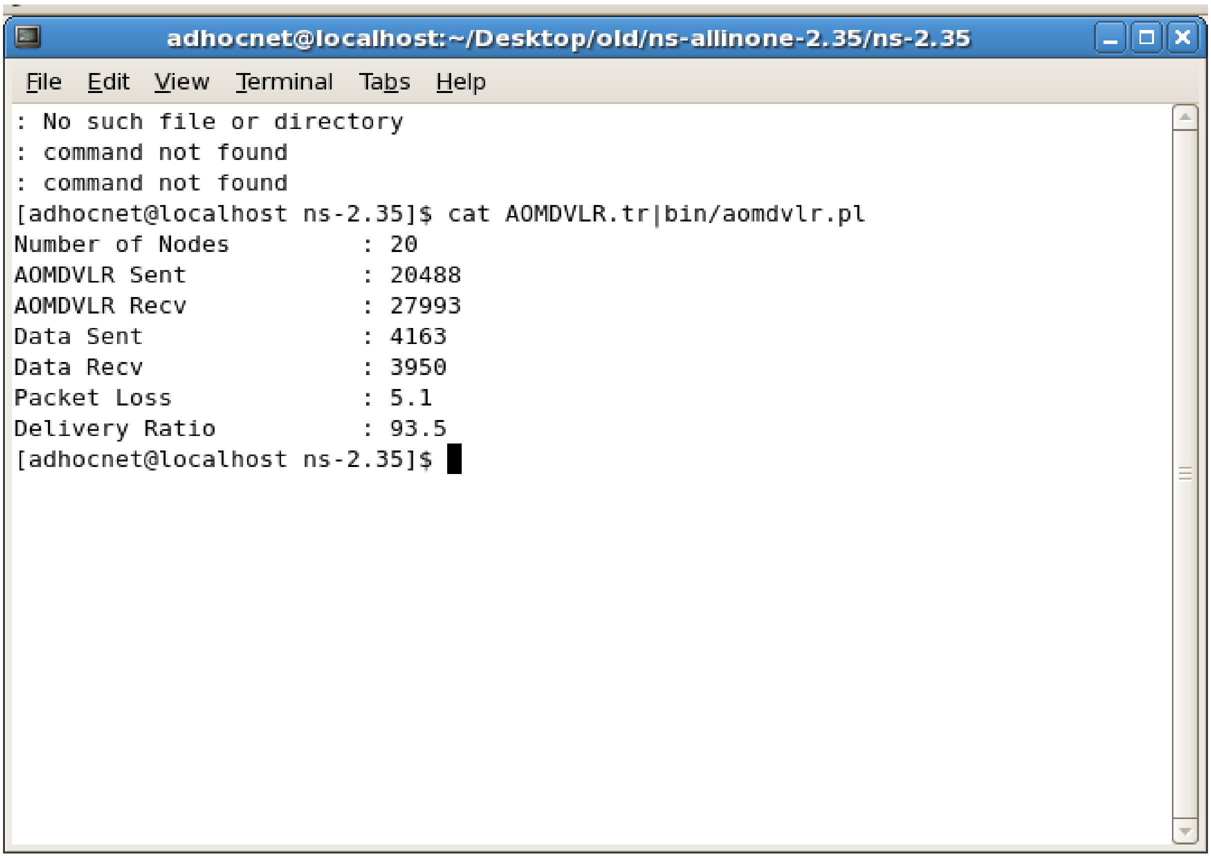
```
: No such file or directory
: command not found
: command not found
[adhocnet@localhost ns-2.35]$ cat AOMDVLR.tr|bin/aomdvlr.pl
Number of Nodes          : 10
AOMDVLR Sent             : 13975
AOMDVLR Recv             : 24022
Data Sent                : 2369
Data Recv                : 2260
Packet Loss              : 4.6
Delivery Ratio           : 95.4
[adhocnet@localhost ns-2.35]$
```

Figure 4.7 (b) Outcome with 10 nodes


adhocnet@localhost:~/Desktop/old/ns-allinone-2.35/ns-2.35
File Edit View Terminal Tabs Help

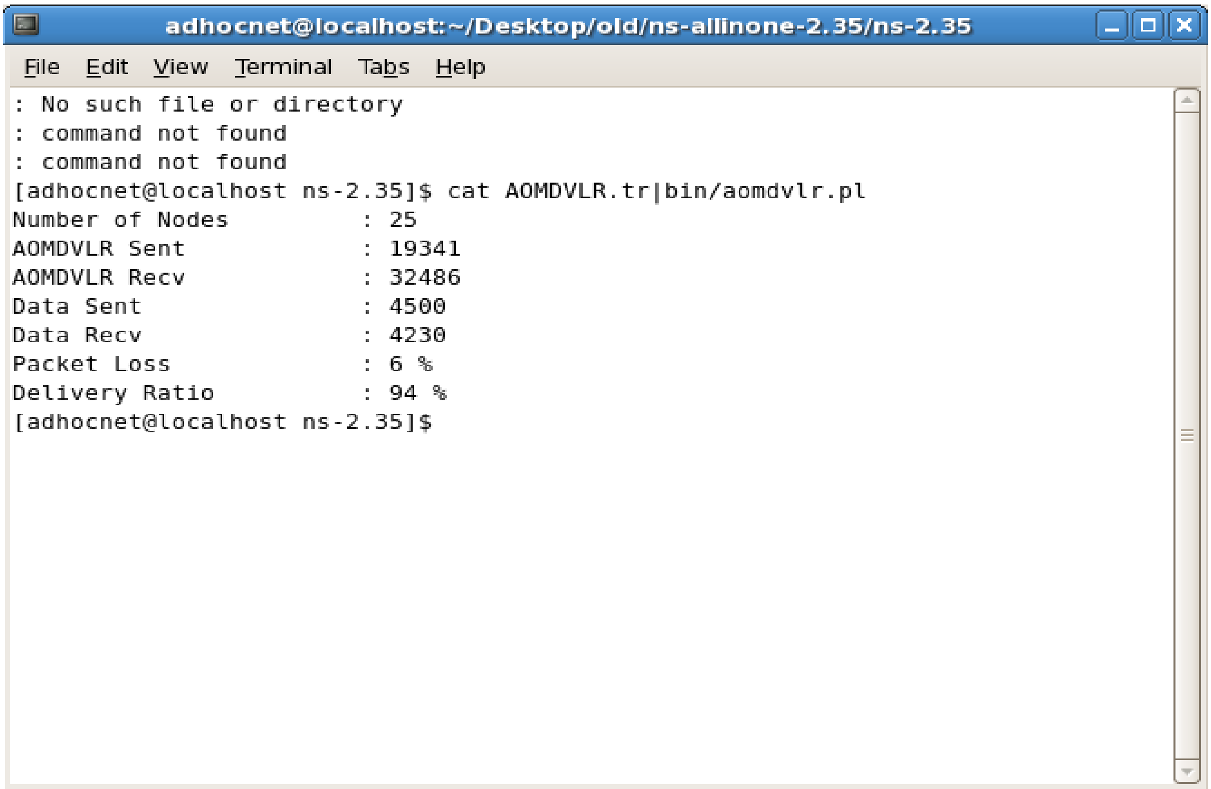
```
: No such file or directory
: command not found
: command not found
[adhocnet@localhost ns-2.35]$ cat AOMDVLR.tr|bin/aomdvlr.pl
Number of Nodes          : 15
AOMDVLR Sent             : 18975
AOMDVLR Recv             : 25448
Data Sent                : 3256
Data Recv                : 3103
Packet Loss              : 4.69
Delivery Ratio           : 95.31
[adhocnet@localhost ns-2.35]$
```

Figure 4.7(c) Outcome with 15 nodes


adhocnet@localhost:~/Desktop/old/ns-allinone-2.35/ns-2.35
File Edit View Terminal Tabs Help

```
: No such file or directory
: command not found
: command not found
[adhocnet@localhost ns-2.35]$ cat AOMDVLR.tr|bin/aomdvlr.pl
Number of Nodes          : 20
AOMDVLR Sent             : 20488
AOMDVLR Recv             : 27993
Data Sent                : 4163
Data Recv                : 3950
Packet Loss              : 5.1
Delivery Ratio           : 93.5
[adhocnet@localhost ns-2.35]$
```

Figure 4.7(d) Outcome with 20 nodes



adhocnet@localhost:~/Desktop/old/ns-allinone-2.35/ns-2.35
File Edit View Terminal Tabs Help

```
: No such file or directory
: command not found
: command not found
[adhocnet@localhost ns-2.35]$ cat AOMDVLR.tr|bin/aomdvlr.pl
Number of Nodes          : 25
AOMDVLR Sent             : 19341
AOMDVLR Recv             : 32486
Data Sent                : 4500
Data Recv                : 4230
Packet Loss              : 6 %
Delivery Ratio           : 94 %
[adhocnet@localhost ns-2.35]$
```

Figure 4.7(e) Outcome with 25 nodes

CHAPTER 5

CONCLUSION AND FUTURE WORK

CONCLUSION AND FUTURE WORK

In this thesis, the performance of original Ad Hoc on Demand Multipath Distance Vector routing (AOMDV) , a multipath routing algorithm that provide multiple path to the destination and the proposed Ad Hoc on Demand Multipath Distance Vector routing with local repair (AOMDVLR), which includes an additional mechanism of local repair in AOMDV, are analyzed. AOMDV select an alternate path when primary path become fail due to either link failure or node failure. But when no alternate path available it restart route discovery from source that may increase time to rediscover route from source to destination. However, AOMDVLR provide local repair to the nodes that are participating in the routing as intermediate nodes. A failure detected node start local repair at their own end to provide alternate route by selecting existing neighbors and new neighbors. Since in AOMDVLR, source does not bothered about route reestablishment, it reduces time to rediscover route from source to destination.

For evaluation of the performance of the new protocol AOMDVLR, NS-2 simulator is used, in comparison with the original AOMDV. To evaluate the performance of proposed protocol various simulation environments are used with different number of nodes. Using a more active route discovery mechanism and local repair, the proposed AOMDVLR performs better than the original AOMDV in the aspects of Routing Overhead, Packet Delivery Ratio and packet loss ratio. Proposed protocol AOMDVLR reduces routing overhead and packet loss ratio and increases packet delivery ratio in comparison of existing protocol AOMDV.

For future work, the buffer may be used in the intermediates node to decrease the packet loss value with local repair needs to be analyzed and carefully selected, buffer may be implemented in the intermediate nodes that will store received packet when any failure is detected and after recovery of route by using local repair all the stored packet may be transmitted on the basis of store and forward technique. Hardware test bed experiments will also be implemented for more extensive and thorough performance evaluation.

REFERENCES

[1] Akyildiz, Ian F., Xudong Wang, and Weilin Wang. "Wireless mesh networks: a survey." Computer networks 47, no. 4 (2005): 445-487.

[2] Bicket, John, Daniel Aguayo, Sanjit Biswas, and Robert Morris. "Architecture and evaluation of an unplanned 802.11 b mesh network." In Proceedings of the 11th annual international conference on Mobile computing and networking, pp. 31-42. ACM, 2005.

[3] Mesh Networking Forum, “Building the business case for implementation of wireless mesh networks,” Mesh Net-working Forum 2004, San Francisco, CA, October 2004.

[4] Garg, Sohan, and Ram Kumar. "A WIRELESS MESH NETWORK: ARCHITECTURE, ISSUES, APPLICATIONS."

[5] Chlamtac, Imrich, Marco Conti, and Jennifer J-N. Liu. "Mobile ad hoc networking: imperatives and challenges." Ad Hoc Networks 1, no. 1 (2003): 13-64.

[6] Gupta, Piyush, and Panganmala R. Kumar. "The capacity of wireless networks." Information Theory, IEEE Transactions on 46, no. 2 (2000): 388-404.

[7] Grossglauser, Matthias, and David Tse. "Mobility increases the capacity of ad-hoc wireless networks." In INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 3, pp. 1360-1369. IEEE, 2001.

[8] Hudyma, Robert, and Deborah I. Fels. "Causes of failure in IT telecommunications networks." Proceedings of SCI, Florida (2004): 35-38.

[9] Staniford, Stuart, Vern Paxson, and Nicholas Weaver. "How to Own the Internet in Your Spare Time." In USENIX Security Symposium, pp. 149-167. 2002.

[10] Ogier, Richard, Fred Templin, and Mark Lewis. Topology dissemination based on reverse-path forwarding (TBRPF). IETF RFC 3684, February, 2004.

[11] Navda, Vishnu, Anand Kashyap, and Samir R. Das. "Design and evaluation of imesh: an infrastructure-mode wireless mesh network." In World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a, pp. 164-170. IEEE, 2005.

[12] Johnson, David B. "The dynamic source routing protocol for mobile ad hoc networks." draft-ietf-manet-dsr-09. txt (2003).

[13] Das, Samir R., Elizabeth M. Belding-Royer, and Charles E. Perkins. "Ad hoc on-demand distance vector (AODV) routing." (2003).

[14] Draves, Richard, Jitendra Padhye, and Brian Zill. "Comparison of routing metrics for static multi-hop wireless networks." In ACM SIGCOMM Computer Communication Review, vol. 34, no. 4, pp. 133-144. ACM, 2004.

[15] De Couto, Douglas SJ, Daniel Aguayo, John Bicket, and Robert Morris. "A high-throughput path metric for multi-hop wireless routing." Wireless Networks 11, no. 4 (2005): 419-434.

[16] Mueller, Stephen, Rose P. Tsang, and Dipak Ghosal. "Multipath routing in mobile ad hoc networks: Issues and challenges." In Performance tools and applications to networked systems, pp. 209-234. Springer Berlin Heidelberg, 2004.

[17] Ganjali, Yashar, and Abtin Keshavarzian. "Load balancing in ad hoc networks: single-path routing vs. multi-path routing." In INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, vol. 2, pp. 1120-1125. IEEE, 2004.

[18] Jacquet, Philippe, Paul Muhlethaler, Thomas Clausen, Anis Laouiti, Amir Qayyum, and Laurent Viennot. "Optimized link state routing protocol for ad hoc networks." In Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International, pp. 62-68. IEEE, 2001.

[19] Perkins, Charles E., and Elizabeth M. Royer. "Ad-hoc on-demand distance vector routing." In Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on, pp. 90-100. IEEE, 1999.

[20] Johnson, David B., and David A. Maltz. "Dynamic source routing in ad hoc wireless networks." In Mobile computing, pp. 153-181. Springer US, 1996.

[21] Lee, Sung-Ju, and Mario Gerla. "AODV-BR: Backup routing in ad hoc networks." In Wireless Communications and Networking Confernce, 2000. WCNC. 2000 IEEE, vol. 3, pp. 1311-1316. IEEE, 2000.

[22] Nasipuri, Asis, and Samir R. Das. "On-demand multipath routing for mobile ad hoc networks." In Computer Communications and Networks, 1999. Proceedings. Eight International Conference on, pp. 64-70. IEEE, 1999.

[23] Koksal, Can Emre, and Hari Balakrishnan. "Quality-aware routing metrics for time-varying wireless mesh networks." Selected Areas in Communications, IEEE Journal on 24, no. 11 (2006): 1984-1994.

[24] Tsai, Jack, and Tim Moors. "A review of multipath routing protocols: From wireless ad hoc to mesh networks." In ACoRN early career researcher workshop on wireless multihop networking, vol. 30. 2006.

[25] Nasipuri, Asis, and Samir R. Das. "On-demand multipath routing for mobile ad hoc networks." In Computer Communications and Networks, 1999. Proceedings. Eight International Conference on, pp. 64-70. IEEE, 1999.

[26] Campista, Miguel Elias M., Pedro Miguel Esposito, Igor M. Moraes, Luís Henrique Maciel Kosmalski Costa, Otto Carlos Muniz Bandeira Duarte, Diego G. Passos, CélioVinicius N. de Albuquerque, Débora Christina M. Saade, and Marcelo G. Rubinstein. "Routing metrics and protocols for wireless mesh networks." Network, IEEE 22, no. 1 (2008): 6-12.

[27] Mueller, Stephen, Rose P. Tsang, and Dipak Ghosal. "Multipath routing in mobile ad hoc networks: Issues and challenges." In Performance tools and applications to networked systems, pp. 209-234. Springer Berlin Heidelberg, 2004.

[28] Xuekang, Sun, Gu Wanyi, Xiao Xingquan, Xu Baocheng, and Guo Zhigang. "Node discovery algorithm based multipath olsr routing protocol." In Information Engineering, 2009. ICIE'09. WASE International Conference on, vol. 2, pp. 139-142. IEEE, 2009.

[29] Badis, Hakim, and Khaldoun Al Agha. "QOLSR, QoS routing for ad hoc wireless networks using OLSR." European Transactions on Telecommunications 16, no. 5 (2005): 427-442.

[30] Hu, Xuhui, and Myung J. Lee. "An efficient multipath structure for concurrent data transport in wireless mesh networks." Computer Communications 30, no. 17 (2007): 3358-3367.

[31] Leung, Roy, Jilei Liu, Edmond Poon, A-LC Chan, and Baochun Li. "MP-DSR: a QoS-aware multi-path dynamic source routing protocol for wireless ad-hoc networks." In Local Computer Networks, 2001. Proceedings. LCN 2001. 26th Annual IEEE Conference on, pp. 132-141. IEEE, 2001.

[32] Marina, Mahesh K., and Samir R. Das. "On-demand multipath distance vector routing in ad hoc networks." In Network Protocols, 2001. Ninth International Conference on, pp. 14-23. IEEE, 2001.

[33] Chen, Zhenyu, Lin Guan, Xingang Wang, and Xunli Fan. "Ad hoc On-demand Multipath Distance Vector routing with Backup Route Update Mechanism." In High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on, pp. 908-913. IEEE, 2012.

PUBLICATIONS

- Uday Singh Kushwaha, S.P. Ghrera, P. K. Gupta. "Performance Evaluation of AOMDV Routing Algorithm with Local Repair for Wireless Mesh Networks" Indersicence in International Journal of Electronic Security and Digital Forensics (IJESDF) 2014 (Communicated)

- Uday Singh Kushwaha, P. K. Gupta. " AOMDV Routing Algorithm for Wireless Mesh Networks with Local Repair (AOMDV-LR)" *Proc. of IEEE 15th* International Conference on Communication and Signal Processing - ICCSP' 15, 2014, pp. 1513-1517.

CURRICULUM VITA

UDAY SINGH KUSHWAHA
241/1 Village Post Bahuribandh
Distt. Rewa (M.P.) 486001
Email ID: udaysingh.jec@gmail.com
Mb: 9827294243

Career Objective: To pursue a challenging career and be part of a progressive organization that gives scope to enhance my knowledge, skills and to reach the pinnacle in the computing and research field with sheer determination, dedication and hard work.

Work Experience: (5 Years)

- Joined as a Lecturer in the Department of Computer Science and Engineering at Jaypee Polytechnic and Training Centre Rewa, from 03rd Jan 2012 to till date.
- Worked as a Lecturer in the Department of Computer Science and Engineering at Jaypee University of Information Technology, Waknaghat Distt Solan (H.P.) from 02nd Jan 2010 to 02nd Jan 2012.
- Worked as a Lecturer in the Department of Computer Science and Engineering at Govt. Women's Polytechnic College, Jabalpur from 28-07-2009 to19-12-2009 (One Semester).

Academic Profile:

- Pursuing Master of Technology in Computer Science , Jaypee University of Information Technology
- Graduation Bachelor of Engineering in Information Technology, Govt. Jabalpur Engineering College with 69.28% in 2009
- Diploma in Computer Science and Engineering, Samrat Ashok Technological Institute Polytechnic College with 64.86% in 2006
- High School Exam from M.P. Board with 79.40% in 2003

Technical Skills:

Programming languages:	C, C++, JAVA
Operating System:	Windows, Linux, Dos

Field of interest:

Computer Architecture, Operating System, Data Structure, DBMS, Object Oriented Technology, Computer Network and Network Security.

Projects and Trainings:

- 45 days vocational training from West Central Railway Jabalpur
- 15 days vocational training from P.H.E. Vidisha

B.Tech (Project)

- Cryptography – Digital watermarking based secure authentication for image – as a major project in the B.E. final year.
- Employee salary management (software for the pay slip of employee) - as a mini project in B.E. 6th semester.

M.Tech (Thesis)

- Fault Tolerance with Multi Route AODMV in Wireless Mesh Network – pursing as a thesis of the M.Tech Final year under the guidance **Prof. Dr. Satya Prakash Ghrera, Professor, Brig (Retd.) and Head, Dept. of CSE and Dr. Pradeep Kumar Gupta Assistant Professor** (Senior Grade), Department of Computer Science and Information Communication Technology, Jaypee University of Information Technology, Solan, Himachal Pradesh, INDIA.

Publication:

- Uday Singh Kushwaha, P. K. Gupta. “AOMDV Routing Algorithm for Wireless Mesh Networks with Local Repair (AOMDV-LR)" *Proc. of IEEE 15th* International Conference on Communication and Signal Processing - ICCSP' 15, 2014, pp. 1513-1517.
- Uday Singh Kushwaha, S.P. Ghrera, P. K. Gupta. "Performance Evaluation of AOMDV Routing Algorithm with Local Repair for Wireless Mesh Networks" Indersicence in International Journal of Electronic Security and Digital Forensics (IJESDF) 2014 (Communicated)

Conference / Workshop Attended

- Attended IEEE International Conference on Image Processing (ICIIP-2011) Organized by the Department of Computer Science and Engineering and Information Communication Technology, Jaypee University of Information Technology, Waknaghat, Himachal Pradesh

- Attended IEEE International Conference on Image Processing (ICIIP-2014) Organized by the Department of Computer Science and Engineering and Information Communication Technology, Jaypee University of Information Technology, Waknaghat, Himachal Pradesh
- Attended Two weeks ISTE-Workshop on DBMS conducting by IIT Bombay
- Attended Three days IEEE sponsored 3-days workshop on wireless network simulation using NS2.
- Attended two weeks ISTE- Workshop on Computer Programming conducting by IIT Bombay
- Attended two weeks ISTE- Workshop on Computer Networking conducting by IIT Bombay

Extra Cocurricular Activities:

- Acting as an Examiner (Internal and External) in RGPV and JUIT, JUET University.
- Acting as an Examiner in many central Evaluations work in RGPV, JUIT and JUET University
- Act as volunteer in International Conference on Image Information Processing 2014 held at Jaypee University College of Information Technology.
- Qualified Graduate Aptitude Test for Engineering(GATE-2011)
- Attended training programme on Entrepreneur and Carrier Planning & Department at Govt. Jabalpur Engineering College, Jabalpur.

Personal Profile

Date of Birth	: 08th Dec 1987
Father's Name	: Mr. Jayram Kushwaha
Father's Occupation	: Govt. Service
Sex / Marital Status	: Male / Unmarried
Nationality	: Indian
Languages Known	: Hindi & English

I certify that the information given above is true, complete and correct to the best of my knowledge and belief.

Date: -

Uday Singh Kushwaha