University of Alberta

Traffic Routing in Wireless Mesh Networks

By

Juned A. Noonari

Project report submitted to Faculty of Graduate Studies and Research in partial fulfillment of the requirement for the degree of M.Sc. In Internetworking (MINT)

Master of Engineering Project.
Department of Electrical and Computer Engineering,
University of Alberta

Edmonton, Alberta
Fall 2006

Acknowledgements

With utmost gratitude and appreciation I acknowledge the professional help and kind guidance of project supervisor Dr. Ehab S. Elmallah. His persistent effort motivated me to work towards completion of this project enthusiastically and made my way easy. Also my thanks to Dr. Mike H. MacGregor for his continuous effort to help and guide during my 2 year time at University of Alberta, specifically providing with unlimited access at the MINT Lab.

I am thankful to my parents Abdul Sattar and Aishah, my brother Attique and sisters Ambreen, Sheeba and Maria for their constant support and prayers. I like to use this opportunity to thank my uncle Dr. M. Uwais Qarni who provided all his guidance and support during my stay in Edmonton. I am very grateful for Asim for his friendship which made MINT course more pleasurable. I am very grateful for my love and future wife Ishrat who want me to complete this project successfully.

List of Abbreviations

AODV	Ad hoc On Demand Vector
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BS	Base Station
BW	Bandwidth
CBR	Constant Bit Rate
CID	Connection Identifier
CPS	Common Part Sublayer
CRC	Cyclic Redundancy Check
CS	Convergence Sublayer
DCF	Distributed Coordination Fucntion
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DL	Down Link
DSR	Dynamic Source Routing
DSDV	Destination-Sequenced Distance Vector
FDD	Frequency Division Duplexing
FEC	Forward Error Correction
IEEE	Institute of Electrical and Electronic Engineers
IFS	Intermediate Frame Space
MAC	Medium Access Control
MANET	Mobile Ad hoc Network
NLOS	Non Line Of Sight
nrt-VBR	non-real-time Variable Bit Rate
OFDM	Orthogonal Frequcncy Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OLSR	Optimized Link State Routing
OPNET	Optimized Network (Simulation Tool)
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PKM	Privacy Key Management
PS	Privacy Sublayer
PSR	Packet Success Rate
QAM-16	Quadrature Amplitude Modulation 16 level
QAM-64	Quadrature Amplitude Modulation 64 level
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RSA	Ron Shamir Adleman (initial of name who developed RSA algorithm)
RTS/CTS	Request To Send/Clear To Send
rt-VBR	real-time Variable Bit Rate
SA	Security Association
SAID	Security Association Identifier
SDU	Service Data Unit

SFID	Service Flow Identifier
SIFS	Short Intermediate Frame Space
SNMP	System Network Management Protocol
SS	Subscriber Station
TDD	Time Division Duplexing
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TFTP	Trivial File Transfer Protocol
TLV	Time/Length/Value
UL	Up Link
VBR	Variable Bit Rate
Wi-Fi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access,
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network

List of Figures

Abstract

In recent times Wireless Mesh Networks are getting a lot of attention in wireless world. Wireless Mesh Networks are perceived as replacement for wired backbone networks with cheap, easy, fast and flexible deployment. In order to provide wired equivalency in Wireless Mesh Networks still considerable research is required due to its unique requirements.

In first part we introduce basic concepts of Wireless Mesh Networks followed by architecture of Wireless Mesh Networks and its basic types and classes. Second part surveys selected research papers talking about recent areas of interest investigating routing problems and protocols for Wireless Mesh Networks. Third section surveys briefly about recently standardized IEEE 802.16 protocol which is being actively deployed around the world and nearest solution to Wireless Mesh Network in the market as of today.

Additionally in last part, the project conducts OPNET simulation for two Ad-hoc routing protocols, AODV and OLSR, compares their performance and suitability in Wireless Mesh Network. We tried to identify victimized nodes and analyzed for use in WMN router performance in terms of routing protocols used. We found that both protocols perform poorly in WMN and not suitable for WMN.

1 INTRODUCTION

This section provides introduction to Wireless Mesh Networks, why it is important and how it is different from Mobile Ad-hoc Network.

As various wireless networks evolve into the next generation to provide better services, a key technology has emerged recently in shape of Wireless Mesh Network. We will use WMN for Wireless Mesh Network interchangeably in rest of the document.

Wireless Mesh Networks (WMNs) are dynamically self-organized and self-configured, with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity [01].

Wireless Mesh Networks (WMNs) are comprised of two type of nodes [01] [02], mesh routers and mesh clients. Mesh routers form the infrastructure backbone for clients. WMNs are multi-hop Ad-Hoc wireless networks. Compared to conventional Ad-Hoc wireless networks, WMNs contain wireless nodes, which can be either mobile or fixed. Communication in WMNs between two nodes mostly relies on infrastructure. The majority of the traffic is user-to-gateway oriented, whereas in conventional Ad-Hoc

Networks, traffic is mostly user-to-user oriented. Through multi-hop communication, the same coverage area is achieved by mesh routers but with lower transmission power as compared to conventional point to point wireless communication.

The communication between devices in WMNs is Non-Line-of-Sight (NLOS). Therefore, it is anticipated to provide a wide range of coverage. Figure 1.1 shows possible WMN where smaller nodes (clients) are connected with larger nodes (gateway) [03]. The distinctive characteristic of WMN is the dynamic topology, which enables WMNs to be dynamically self-configuring and self-healing. In the case when one path fails, a new path will take over to maintain the network connectivity. Therefore WMNs are highly reliable. Nodes (mesh routers and mesh clients) inside the topology will be able to connect and communicate with each other. Moreover, the gateway/bridge functionalities of mesh routers make it possible for WMNs to be able to interoperate with current existing networks, such as Wi-Fi, WiMax, Cellular Networks, and Wireless Sensor Networks (WSNs). All of these features give WMNs many irresistible attractions,

such as automatic network maintenance, low establishment cost, robust and reliable service coverage.

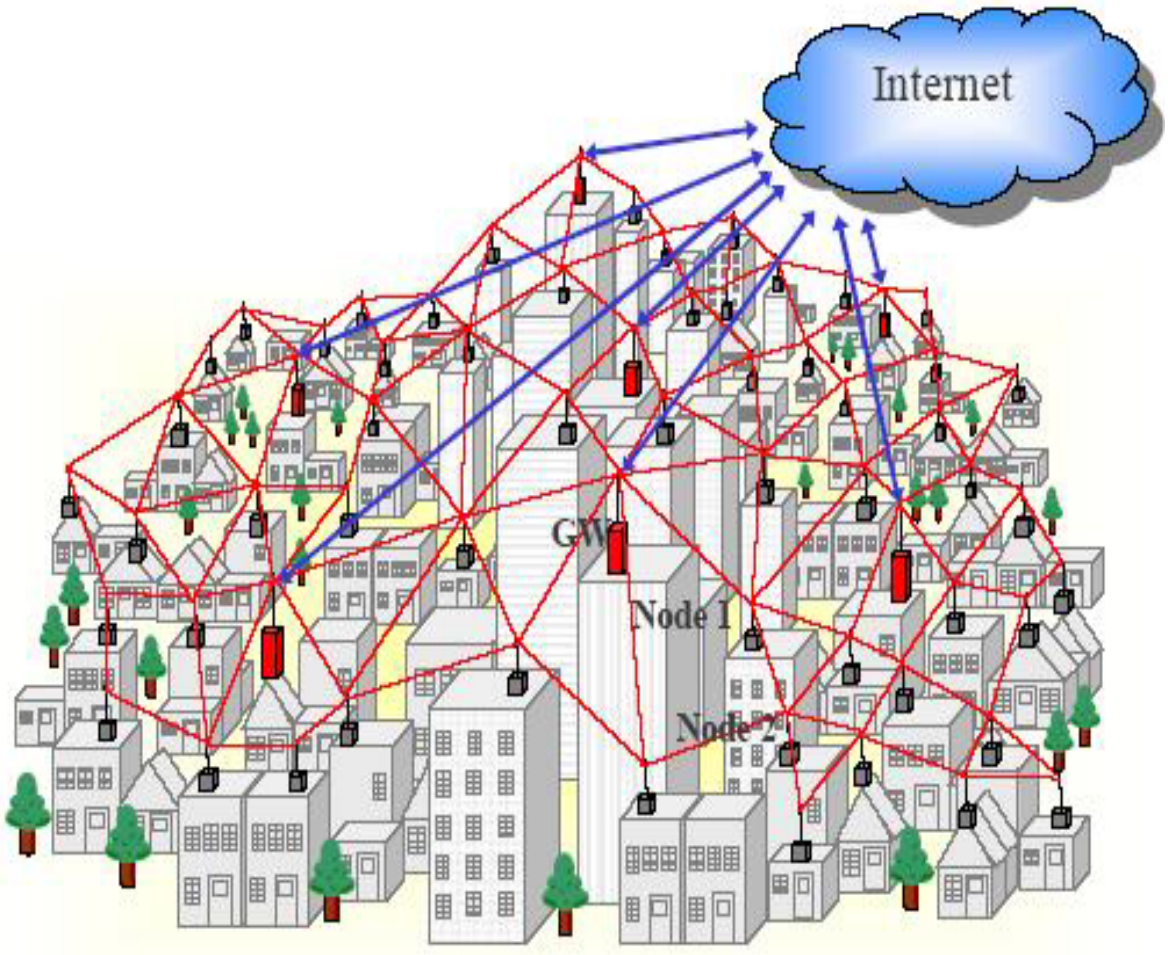

Figure 1.1: Wireless Mesh Network [03]

WMNs will provide services in many areas, such as enterprise, campus, hospital, public surveillance, etc. Numerous applications can be developed using WMN technology. Many companies have already put mesh products on the market. Many WMN deployments are under construction in several cities. For example, a metro-scale Wi-Fi mesh network using ‘Tropos Networks' MetroMesh architecture is being deployed in the City of Chaska, Minnesota. WMNs are expected to be one of the key technologies for wireless networking in the next generation.

2 WMNS ARCHITECTURE

The focus of discussion in this section is types of nodes in Wireless Mesh Networks and classification of WMNs based on architecture.

2.1 Node types in WMN

Nodes in Wireless Mesh Networks are divided into two types [01], namely mesh routers and mesh clients.

2.1.1 Mesh Routers

In order to support mesh networking mesh routers contain additional routing functions besides its capability to work as a gateway/repeater. Mesh routers have multiple wireless interfaces, which can be built on either the same or different wireless access technologies. Examples of mesh routers based on embedded system include PowerPC, or Advanced Risc Machine (ARM). These routers are very compact. Mesh routers can also be built upon usual computers such as laptop or home desk PC

2.1.2 Mesh Clients

Examples of mesh clients include laptop/desktop PC, pocket PC, PDA, IP phone, RFID reader, BACnet controller etc. Mesh clients can also support mesh networking therefore they can work as routers. Mesh clients has simpler hardware and software requirements and usually built with only one wireless interface card. Also mesh clients do not support gateway or bridge functionality.

2.2 Wireless Mesh Network Architecture

The architecture of WMNs can be grouped into three categories [01]: Client Architecture, Infrastructure/Backbone Architecture, and Hybrid Architecture.

2.2.1 Infrastructure/ Backbone WMNs

Infrastructure/Backbone Architecture contains both mesh routers and mesh clients nodes, as shown in Fig. 2.1. Mesh routers form the infrastructure backbone for clients and bring connectivity to them. Mesh routers perform functions such as routing, as well as self-configuring and self-healing. Moreover, various radio technologies, such as IEEE

802.11, IEEE 802.16, can be used with this type of meshing architecture. Hence, with the built-in gateway/bridge functionality of mesh routers, infrastructure meshing architecture provides an interface for integrating existing wireless networks. Multiple wireless interfaces are enabled in infrastructure/Backbone architecture. Conventional clients that have Ethernet interface can be connected to mesh routers through the Ethernet interface. If the conventional client uses the same radio, then it can directly communicate with mesh routers. Otherwise, the conventional client has to communicate with its Base Station (BS) that is connected to mesh routers via Ethernet interface.

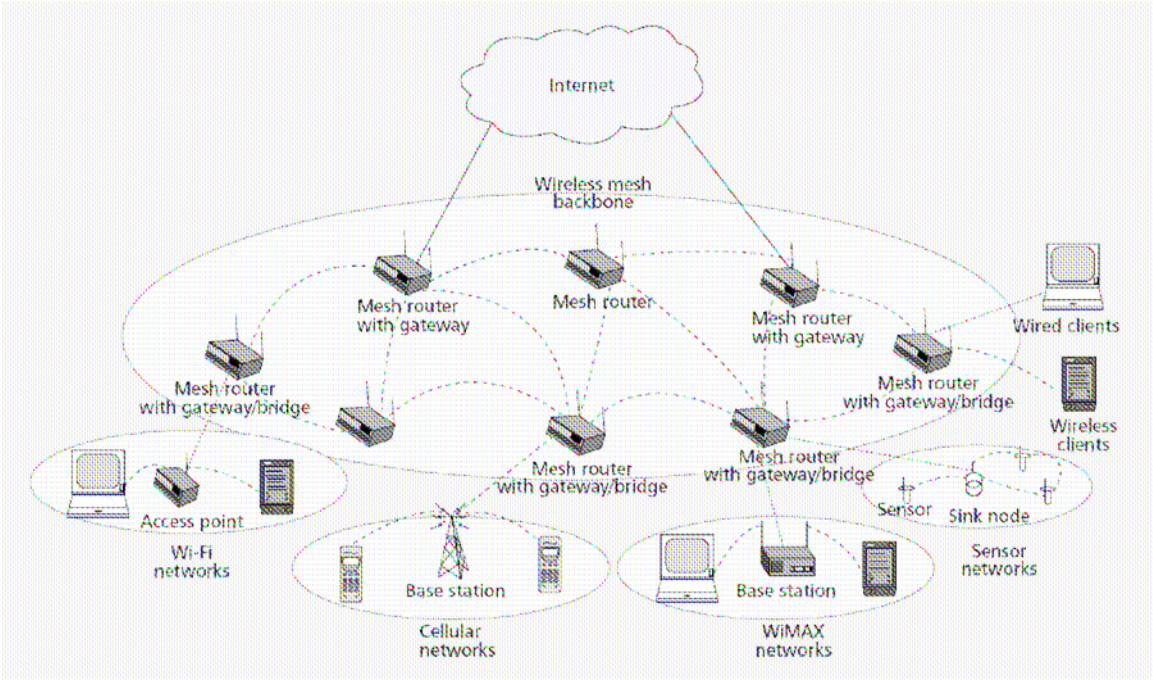

Figure 2.1 Infrastructure/backbone WMN [01]

2.2.2 Client Wireless Mesh Network

Client Architecture only contains client nodes. These client nodes play double roles of network routers and network end-users. No mesh routers are used in this type of networks. Client mesh architecture provides peer-to-peer communications among all the nodes in the network. This type of network is more like a conventional Ad-Hoc network since only one radio technology is usually involved. Special requirements such as software/hardware installation are needed for client nodes in WMNs, since these nodes have to perform the routing functions.

2.2.3 Hybrid Wireless Mesh Network

Hybrid Architecture, as the name suggested, combines the above two types of meshing architecture. In this type of architecture, client nodes communicate with each other via mesh routers, or via peer-to-peer among clients themselves. At the same time, the infrastructure backbone makes the connectivity possible to other existing wireless networks, such as Wi-Fi, WiMax, WPAN and WSNs. This architecture is the model for the future generation networking.

3 OVERVIEW OF SOME RESEARCH WORK

In this section we discuss two selected research papers [04] and [05] in the context of Wireless Mesh Network Routing Protocols.

The requirement of new protocols is triggered due to the special characteristics of WMNs. WMN routing, like other networks, relies on routing metrics. Existing routing protocols use minimum hop counts as a performance metric when selecting routing path. Given the difference between WMNs completely new routing protocols are imperative.

3.1 Cross-Layer Routing in Wireless Mesh Networks

Mesh routers play double roles of forming network backbone as well as forwarding packets. Routing layer should be aware of the local issues of the underlying layers. Thus cross-layer metrics approaches are explored by researchers. [04] proposed a new metric for routing which takes three primitive physical layer parameters: Interference, Packet Success Rate, and Data Rate. The Routing algorithm aims at finding the path with low levels of generated interference, reliability in terms of Packet Success Rate, and highest possible transmission rate.

3.1.1 Cross Layer Approach

We will discuss first 'Cross-Layer Approach' then metrics 'Interference estimation' and then Packet Success Rate estimation'. After that this paper talks about Routing issue in Wireless network and its solutions is discussed. We will touch those topics as primarily organized in original paper.

It is shown in [06] an upper bound on the average traffic carrying capacity λ in wireless multi-hop network is given by

$$\lambda(r) \leq \frac{16AR}{\pi\Delta^2 nLr}$$

A = Total area of network in meter-square

L = Average distance between source-destination pairs

R = Maximum transmission rate in bps

r = Transmission range

n = Number of nodes in network

It is assumed in this equation there is no other transmissions within a distance $(1+\Delta)r$ from a transmitting node. The quantity $\Delta > 0$ models the notion of allowing only weak interference. This equation gives behavior of wireless network. In order to achieve high throughput, one has to maximize the data rate in transmission and to reduce the interference generated by transmitting packets.

Power control policy has direct affect on rate and interference and is a key factor. The power control policy is to set the power depending on the next-hop the transmission aims to reach. The final target is to optimize the parameters of the lower layers on which routing is performed.

Interference and Data Rate are usually used to describe quality of PHY-layer, however these two metrics do not give enough indication about the quality of link. The link on which transmission is done with a limited amount of power may offer low interference and high nominal rate. On the contrary, Packet Success Rate (PSR) estimation at the routing layer along the entire path is able to react to bad channel conditions, by changing completely path in order to reach the same destination.

In order to take place cross-layer approach SIR (signal to interference ratio) information must be propagated from the PHY layer to Routing layer. The transmission parameters, namely power and data rate, have to be propagated from the routing layer down to the physical interface. This can be done by adding side information to the packets.

3.1.2 Interference Estimation

Interference produced by each node is extremely difficult. [04] Shows an alternative approach with a *trend index* function *I(P,N)*, which gives estimation based on local parameters of the transmission level P, and the number N of neighbors reachable with that particular level of power.

Key properties of *I(P,N)* are

- If the number of neighbors N is constant changing the transmission power level from P1 to P2, the smaller the power level, the smaller the interference produced :

$$\forall P_1, P_2 \quad P_1 < P_2 \quad I(P_1, N) < I(P_2, N)$$

- If two nodes are using the same power level P but with different number of neighbors N1 and N2, then the level of interference decreases with the number of neighbors:

$$\forall N_1, N_2 \quad N_1 < N_2 \quad I(P, N_1) < I(P, N_2)$$

These properties are validated by following equation

$$I(P) = \frac{N(P)}{N(P_{max})}\sqrt{\frac{P^2 + P_{max}^2}{2P_{max}^2}},$$

Where $N(P_{max})$ is the number of neighbor nodes reachable with maximal power level P_{max}.

This function is extended to evaluate the interference generated over a network path.

$$I(Path) = \sum_{\forall (i,j) \in Path} I_{i,j}(P_{i,j})$$

$$= \sum_{\forall (i,j) \in Path} \left(\frac{N_{i,j}(P_{i,j})}{N_{i,j}(P_{max})}\sqrt{\frac{P_{i,j}^2 + P_{max}^2}{2P_{max}^2}} \right),$$

where $I_{i,j}$ is the interference produced to send a packet from node *i* to node *j* with power $P_{i,j}$, and $N_{i,j}(P_{i,j})$ is the number of neighbors of the sending node transmitting with power $P_{i,j}$.

3.1.3 Packet Success Rate Estimation (PSR)

[04] uses PSR which has been used in evaluating performance on the basis that it gives better indication of physical channel condition and quality at packet level.

Supposing that the Packet Error Rate PER*(i,j)* is independent over each transmission leg *i* to *j*, one can derive the PSR as

$$PSR(Path) = \prod_{\forall (i,j) \in Path} (1 - PER(i,j)).$$

Packet Error Rate (PER) is typically derived with the hypothesis that errors are uniformly distributed in packet as

$$PER = 1 - (1 - BER)^{L}$$

Where L = packet length

In [07], a new estimator of *PER*, which takes into account the burst structure of errors at output of Viterbi decoders, is presented. Viterbi decoders are nowadays largely used in wireless technologies, like UMTS and 802.11. It is shown in [07] that this result can be used to have precise and reliable estimates of *PSR* at the output of the physical layer.

3.1.4 *Routing Problem in Wireless Network*

Rate, Interference, and *PSR* are used as routing metrics in the effort to find paths that offer: large bandwidth (accordingly with hardware's limits); optimized global performances of the network; reduced interference injected by each packet transmission; reliability. The problem is inherently complex, since three metrics are used. A possible approach might be to mix the metrics in a single one, like for example

$$C(path) = \frac{Interference(path) \cdot PSR(path)}{Rate(path)},$$

Where *C*(*path*) indicates the cost of the path.

The above equation relies on using three metrics to achieve accurate description of network state but at the cost of very complex routing protocol. These metrics are not independent and transmission power has opposite effect on all of these metrics. Cross-layer routing also manages power transmitted, it may optimize path to create more

suitable paths. Also searching for good path in parallel adds another factor of complexity in routing algorithm.

In order to avoid these problems and create optimal routing [04] suggests to split algorithm into two parts that must collaborate with each other and described below and followed by steps to combining both algorithms.

• Power Optimization Strategy

Power optimization strategy involves managing and optimizing power levels locally to communication with neighboring nodes instead of performing globally. In this case global optimum can not be assured however performance is improved.

The steps that each nodes of the network must perform, in order to find the optimal power, are:

Step 1: $\forall j \in \mathcal{N}$, Set $\mathcal{P}_j = \mathcal{P}_{max}$
Step 2: Select $j \in \mathcal{N}$
Step 3: $\mathcal{N} = \mathcal{N} \setminus \{j\}$
Step 4: Find
$\mathcal{P}_j = \{p \in \mathcal{P} | d(p) = \min_{\bar{p} \in \mathcal{P}} d(\bar{p}) \wedge R(p) = R_{max}\}$
Step 5: If $(\mathcal{N} \neq \phi)$ then go to Step 2.

In above algorithm

N is set of nodes that can be reached with maximum power level.

P is set of all available power levels.

Pj is optimal power level to reach neighbor j.

The distance from the optimum is a function of Interference and *PSR*, *d* (*I*(*p*), *PSR*(*p*)), which, in turn, depends on the power level. Thus, the distance can be expressed as function of only the power level *d*(*p*).

Note that the complexity of this approach is *O*(|N|), *i.e.* proportional to the number of neighbors.

• Route Discovery and Update

In order to discover path [04] proved that cross layer approach to find a path, subject to the metrics interference and PSR is NP-complete, which is same class of problem as in

multi-constraint QoS routing and any approached developed for QoS routing is applicable.

Power optimization is applied to only those links which offer maximum data rate therefore only those links are considered. This has two benefits

-Algorithm is simplified.

-Issues arising with radio interference where low data rate transmitting nodes which throttle network are avoided.

Following is excerpt taken from paper

- **Routing and Power Optimization**

Hence, we combine the two parts,

1. Assume network is stable and nodes have discovered neighbors with the help of neighbor discovery algorithm.
2. Perform power optimization and route discovery algorithms.
3. Now any event can trigger change in metrics of one or more links.
4. Power optimization algorithm is applied to affected links.
5. Step 3 can trigger routing algorithm to re-compute all paths affected by change.

In cross-layer approach step 4 is applied before step 5 which makes computations simple.

3.2 Ripple: A Distributed Medium Access Protocol for Multi-hop Wireless Mesh Networks

This section summarizes the work of [05]. In [05], the authors propose a new MAC protocol called *Ripple* for Wireless Mesh Networks under tree topology. Ripple uses a controlled-access technique to avoid collisions of packets and maximize spatial reuse.

Wireless Mesh Network is intended to operate as wireless backbone infrastructure to replace wired network. Routers in WMN are non mobile and function in fully distributed manner. The nature of WMN is to serve as an access network for clients and communication is multi-hop. Being a fully distributed network without any centralized control packet collision is inevitable hence affecting throughput and performance of WMN. Therefore one of the challenges of WMN is to have new MAC protocol which can coordinate the channel access among neighboring nodes base on limited information exchange.

Use of 802.11 MAC has shown considerable problems in WMN and even with RTS/CTS hidden node and exposed node issues are not solved [08]. RTS/CTS scheduling along a chain can cause serious TCP fairness problems and backoff inefficiencies [09].

There has been several MAC proposals (e.g. MACA-P by Misra, Acharya[10] and DCMA by Raguin [11]) to solve problem such as hidden node, spatial reuse, scheduling fairness etc, but most of the techniques used still adopted a random-access mechanism and suffer from the same backoff inefficiencies and fairness problems that of 802.11 DCF.

3.2.1 *RIPPLE* PROTOCOL

It is proved in [12] that a node in chain topology can attain an optimal utilization of 1/3 by applying spatial-reuse. In [12] it is also predicted if a node can properly schedule its frame transmission interval then data frames can be forwarded hop-by-hop without interfering with other nodes. This is called *ripple phenomenon*. This optimal condition is difficult to realize in WMN due to its distributed nature. Based on these facts authors propose token-passing protocol for nodes in chain and tree topology.

A system model Fig. 3.2.1 is used with following settings:

- Each node is a Wireless Router which can relay other traffic and can generate its own traffic.
- Root node (Parent node/router) is the one connected to internet gateway through wired network (i.e. A1).
- Child node is a router node connected through wireless medium with other routers.
- Cross node is a router which has more than one child nodes e.g. C1.
- Leaf node is a router without any child node.
- Uplink is a transmission of packets from child to parent node.
- Downlink is a transmission of packets from parent node to child.
- Nodes are fixed.
- Uplink and Downlink transmission uses separate high speed wireless channels.
- Transmit time for a data packets is fixed.
- The frame format of RTS, CTS, DATA, and ACK are according to 802.11 MAC.
- Inter-Frame-Spaces of DATA, RTS, CTS and ACK are set to be Short IFS (SIFs).

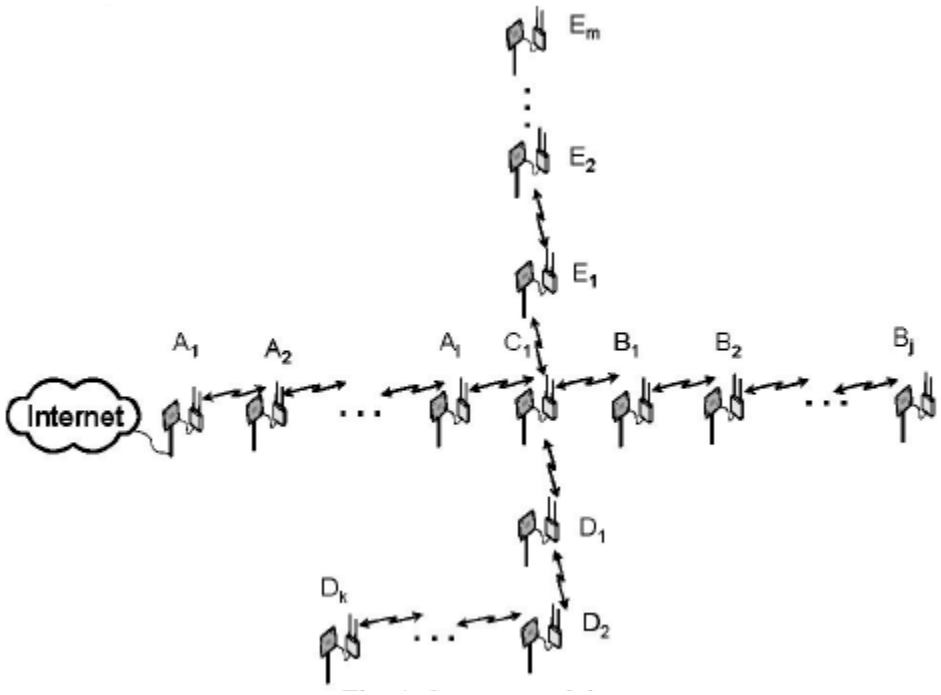

Fig. 3.2.1 System Model [05]

In *Ripple* user information is transported in DATA frames. However a DATA frame without any information is called NULL frame. RTS/CTS frames are defined according to 802.11. Upon receiving a DATA from node replies with ACK frame. If the expected RTS frame is lost or not received then the node which has right to receive a DATA frame will send RTR (Right to receive) frame.

Ripple modifies 802.11 DCF and employs RTS and RTR frames as 'tokens'. A node is allowed to send a DATA frame only if it holds a token.

The format of RTR frame is same as CTS and is used to request a DATA frame from its upstream node. Inter-frame-space of RTR frame is:

$$IFS_{RTR} = SIFS + T_{RTS} + SIFS = 2SIFS + T_{RTS},$$

Where T_{RTS} is the time required by a node to transmit an RTS frame.

The operation of protocol has four states defined in the paper.

- **Transmit (Tx) state:** a node which is ready to send a DATA frame will enter this state.
- **Receive (Rx) state:** a node which is ready to receive a DATA frame will enter this state.
- **Listen state:** a node which is a hidden node or an exposed node or both will enter this state. A node in listen state must keep silence for network-allocation-vector (NAV) and may transmit an RTR token to its upstream node if the channel is sensed clear for IFS_{RTR} after the expiry of NAV.
- **Idle state:** It is a initial state for all nodes, also a node which has been interrupted by unexpected conditions during TX, RX and Listen states will return to this state.

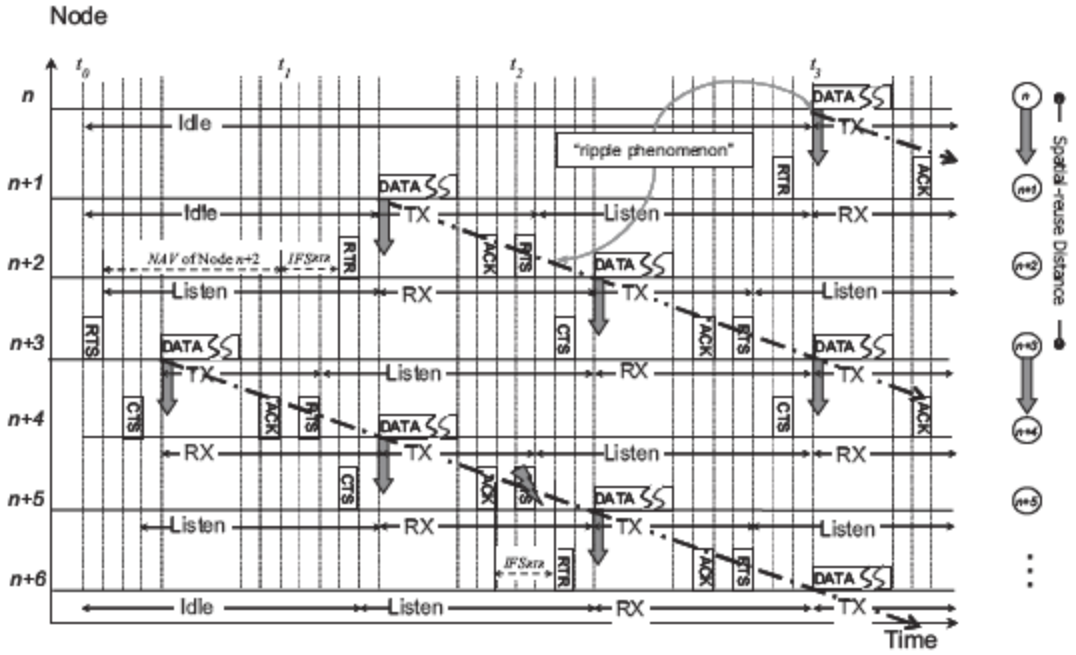

Fig. 3.2.2 State transitions and timing diagram: Downlink transmission [05]

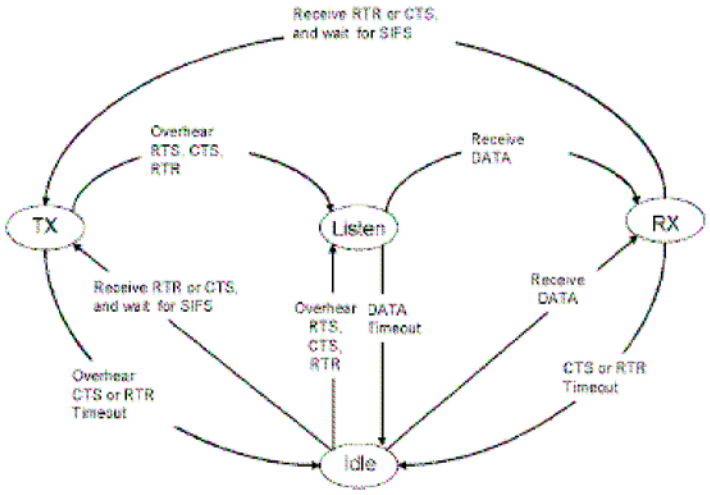

Fig. 3.2.3 Finite state machine: Downlink transmission [05]

Fig. 3.2.2 shows the state transitions and timing diagram for chain of nodes in downlink transmission. State transition are triggered by either transmission or reception of frames. Initially nodes in network use 802.11 DCF to communicate asynchronously among themselves and select *supernode* [13] and then move to Idle mode. Supernode triggers state transitions of other nodes by sending RTS frame to its downstream node. Node *n+3* in Fig. 3.2.2 is elected as supernode at time t_0. Prior to transmission of DATA or NULL frame supernode performs RTS/CTS handshake with downstream nodes (i.e. n+4 node), with RTS token in hand n+4 node can perform handshake with its downstream nodes (child nodes) and send DATA or NULL frame, this process continues hop-by-hop activating the ripple phenomenon. Ripple uses RTS/CTS which prevents hidden node and exposed node problems [14]. By overhearing to RTS and CTS node n+2 and n+5 are forced to enter Listen state at time t_0 and have to remain in this state for NAV duration. A node may use RTR frame to activate a new ripple if its upstream node is in Idle state (e.g Node n+2 at time t_1) or regenerate an interrupted ripple if its upstream node is in TX state (e.g., Node n+5 at time t_2). State transition diagram also shows *Ripple* uses ripple phenomenon such that two nodes distanced from a spatial-reuse distance of three nodes can transmit simultaneously without interference (at time t_3).

Fig. 3.2.3 shows finite state diagram for downlink transmission. In RX state node inherits token and is eligible for DATA transmission. When node is ready to send DATA it enters TX state. After finishing DATA transmission node scans channel and enters Listen state during NAV when it overhears RTS,CTS or RTR frame. Upon expiration of NAV, for clear channel sensed for IFS_{RTR} the node may reply CTS for RTS frame or automatically transmit and RTR frame to upstream node. The node enters RX state when it begins to receive a DATA frame. With any exception in TX, RX, and Listen states, the node should move to Idle state.

The performance of each node (except child nodes of cross ndoes) in *Ripple* under error-free channel is derived in the paper and following exerpt describes it.

"Denote $p_{i,j}$ as the state transition probability from state I to state j and P_i as the state probability of a tagged node, where $i,j \in \{TX,RX,Listen,Idle\}$, respectively. In error free channel, $p_{TX,Idle}=p_{RX,Idle}=p_{Listen,Idle}=0$ and $p_{TX,Listen}=p_{Listen,RX}=p_{RX,TX}=1$. Thus, it can be shown that $P_{TX}=P_{RX}=P_{Listen}=1/3$. In other words, a node attains the optimal utilization of 1/3 under spatial-reuse and each node has an equal chance to access the wireless channel."

Through simulations writers compared throughput with various nodes and loads and verified when more than 3 nodes are used 802.11 DCF attains a low throughput of much less than 1/3 spatial-reuse, however through *Ripple* system was able to attain optimal throughput and it was irrelevant of chain length.

Still there is more research is required to verify system under noisy conditions before this protocol is fully realized.

4 OVERVIEW OF IEEE 802.16 STANDARD

In this section we will discuss IEEE 802.16 standard also known as WiMax. We will give brief introduction of the standard and why it is important followed by technical overview of standard itself. MAC and PHY layer of IEEE 802.16 will also be discussed.

[16],[17],[18],[19] and [20] were used to prepare IEEE 802.16 survey.

4.1 INTRODUCTION

Growth of wireless media and its usage gained popularity through 802.11 WLAN and widely deployed around the world. The limitation of 802.11 is data rate and range. There was demand of new wireless technology which can potentially and effectively replace wired backbone and backhaul systems, making growth of network rapid, easy and cost effective. This leads researcher to come up with new standard 802.16 WirelessMAN^{TM} Air Interface for Broadband Wireless Access (also known as WiMax).

Below is brief description of IEEE 802.16

- IEEE 802.16 (2001)
  - Air Interface for Fixed Broadband Wireless Access System MAC and PHY Specifications for 10 – 66 GHZ (LoS)
  - One PHY: Single Carrier
  - Connection-oriented, TDM/TDMA MAC, QoS, Privacy
- IEEE 802.16a (January 2003)
  - Amendment to 802.16, MAC Modifications and Additional PHY Specifications for 2 – 11 GHz (NLoS)
  - Three PHYs: OFDM, OFDMA, Single Carrier
  - Additional MAC functions: OFDM and OFDMA PHY support, Mesh topology support, ARQ
- IEEE 802.16d (July 2004)
  - Combines both IEEE 802.16 and 802.16a

- Some modifications to the MAC and PHY

- IEEE 802.16e (2005)
  - Amendment to 802.16-2004
  - MAC Modifications for limited mobility

WiMax is designed for Metropolitan Area Networks with range of more than 50 Km and can support data rates of more than 70 Mbps (shared). It can also be used in Mesh Mode creating mesh network with increased range. WiMax consists mainly of Base Station (BS) and Subscriber Station (SS) much like cellular networks and support point-to-multipoint and mesh topology. BS to SS link is usually a microwave link. 802.16 standard defines protocol independent core for ATM, IP and Ethernet, with robust QoS features (such as CBR, rt-VBR, nrt-VBR, BE) to give enough flexibility for service provider to support various layer 2 and layer 3 services. Security model in 802.16 is very strong and threats learned from 802.11 are rectified by using PKM protocol and RSA public key encryption algorithm (PKCS#1).

IEEE 802.16 referenced model is shown below

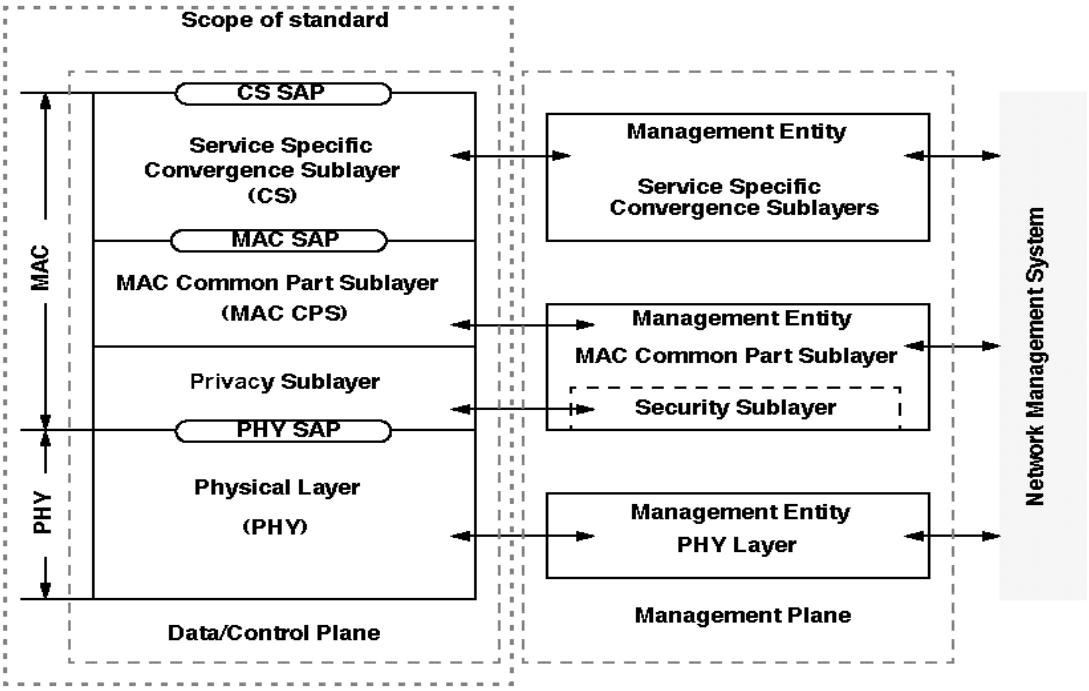

Fig 4.1 802.16 Reference Model [20]

4.2 IEEE 802.16 PHYSICAL LAYER DETAILS

4.2.1 Adaptive Burst Profiles

80.16 standard defines adaptive burst profiles using single-carrier modulation. Coding schemes for these profiles are selected and adjusted on individual basis from Subscriber Stations. Error correction is achieved through FEC Reed-Solomon GF(256) which is combined with an inner block convolution code for robust transmission of data. 802.16 has capability of using QPSK, 16 QAM, 64 QAM to support various burst profiles.

802.16 has frames of 0.5, 1, or 2 ms and divided into physical slots. At physical layer the physical frame has UL (uplink) and DL (downlink) sub frame. PHY can carry UL and DL frame either with TDD or FDD. In TDD same frequency is used however in FDD UL and DL are transmitted on different frequencies.

4.2.2 Duplex Schemes

802.16 can support two types of duplex schemes i.e. Time Division Duplex and Frequency Division Duplex. In Downlink Transmission Subscriber Stations (SS) are associated with a specific burst and in Uplink transmission a variable time slot is allotted to SS. In TDD downlink and uplink transmission share the same RF channel on the other hand FDD DL and UL transmission is carried out on different RF channels. SSs in TDD do not support full duplex to make it low cost. In FDD support of half duplex is incorporated.

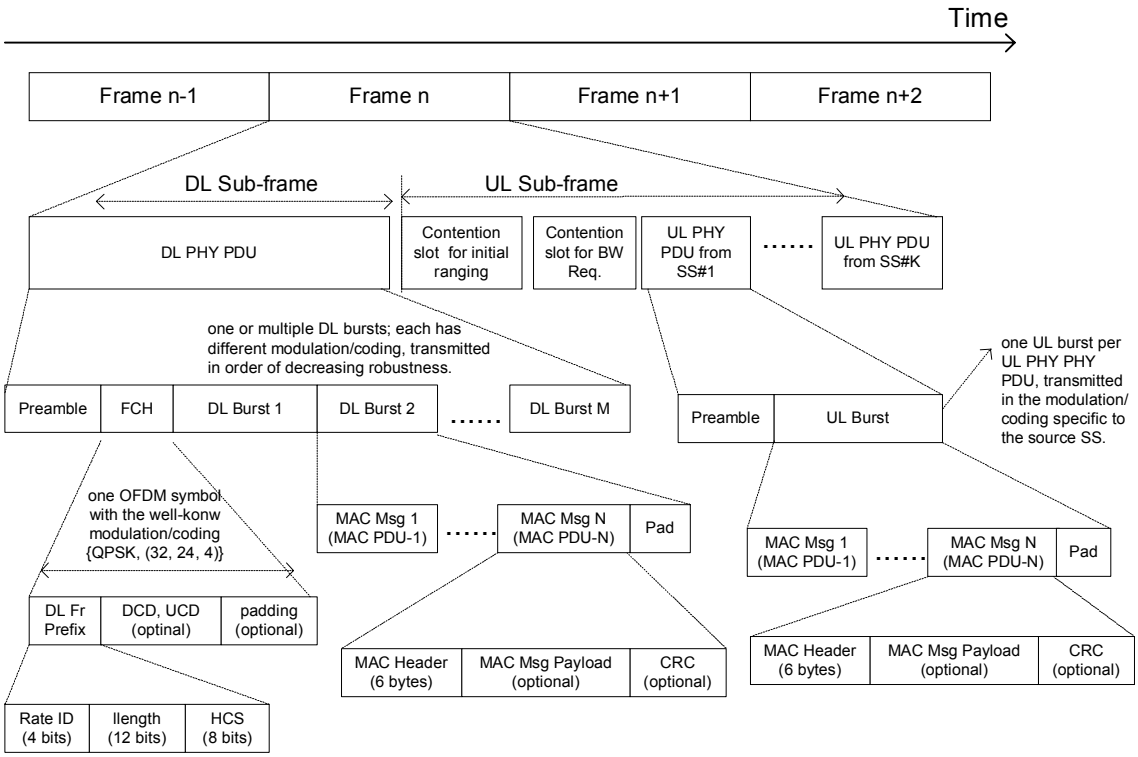

Figure 4.2.1 OFDM PHY TDD Frame Structure [20]

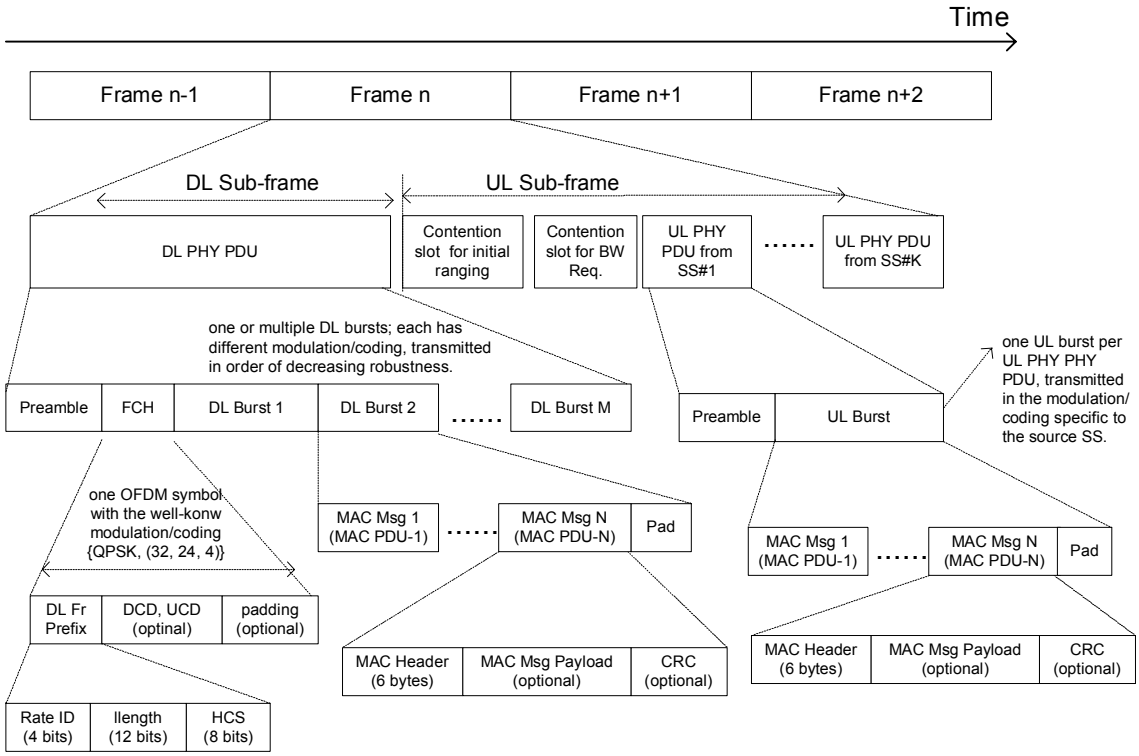

Figure 4.2.2 OFDM PHY FDD Frame Structure [20]

4.3 IEEE 802.16 MAC LAYER DETAILS

4.3.1 MAC Addressing and Identifiers

802.16 comprises of mainly two parts which are Subscriber Station and Base Station. SS is identified through unique 48 bit MAC address. Base Station has 48 bit base station ID (not a MAC address) and 24 bit operator's ID. Different types of connections are identified with 16 bit CID (connection identifier) which is used in MAC PDUs. Also addressing contains service flow id SFID which is 32 bit long and for security purposes 16 bit Security Association ID is used.

4.3.2 Service-Specific Convergence Sublayers

IEEE defines two Service-specific convergence sublayers to support 802.16 MAC mapping from different type of services from higher layers. These are

- ATM Convergence Sublayer (ATM CS)
- Packet Convergence Sublayer

ATM CS maps ATM services and Packet CS maps IPv4, IPv6, Ethernet and VLAN. The primary function of CS is to classify Service Data Units to the proper MAC, enable bandwidth allocation, and retain QoS. In addition to these functions CS can also perform payload header suppression and construction.

4.3.3 MAC Common Part Sublayer (MAC CPS)

The MAC PDU is the data unit of MAC CPS and exchanged between on uplink and downlink between BS and SSs. It consists of fixed length MAC header, a variable-length payload and an optional cyclic redundancy check (CRC). MAC PDUs are divided into three types:

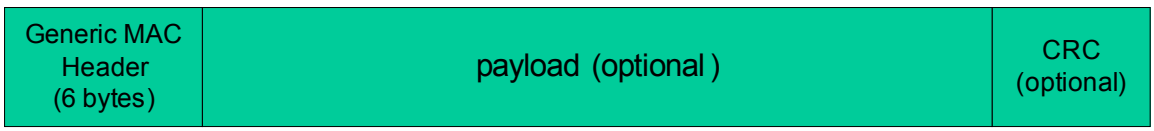

Figure 4.3.1 MAC PDU [20]

- DATA MAC PDUs
- Management MAC PDUs
- Bandwidth (BW) request PDU

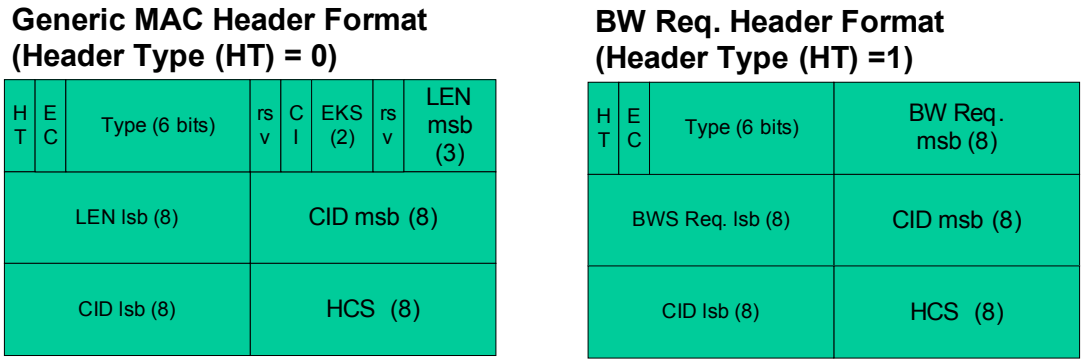

Figure 4.3.2 MAC Headers (a) Generic (b) BW Req. Header [20]

For DATA and Management MAC PDU the HT field is set to 0 (zero). Payload are MAC SDU from upper layer in DATA MAC PDU and it is transmitted on connection. Management MAC PDU payload has MAC Management messages or IP packets encapsulated in MAC CS PDUs, these PDUs are transmitted on management connections. BW req. PDU has HT=1 and transmitted without payload.

Encapsulation of packets is shown in below figure 4.3.3

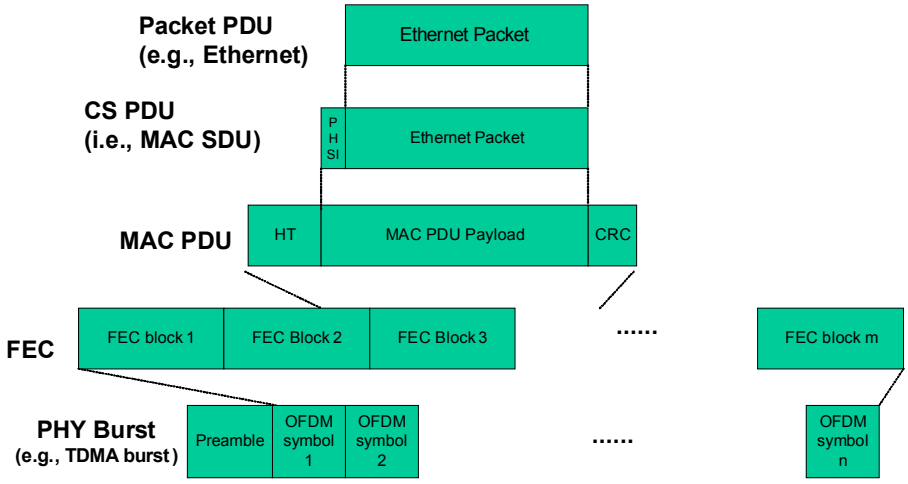

Figure 4.3.3 Packet encapsulation [20]

When a SS enters network it is assigned three management connections in each direction. First one is Basic Connection, used for transfer of short and time-urgent MAC management messages and RLC (radio link control) messages. Secondly there is Primary Management Connections which has longer and more delay tolerant MAC management messages such as for authentication and connection setup. Last and third one is Secondary Management Connection which is used to transfer standard based management messages e.g. DHCP, SNMP, TFTP etc. Basic and Primary Management has MAC management messages as MAC PDU payload whereas Secondary Management connection has IP packet based CS PDU as MAC PDU payload.

802.16 has defined 41 MAC management messages and uses TLV (type/length/value) format and can be sent on basic connections, primary mgmt connections, broadcast connections and initial ranging connections.

Different types of packet are formatted into MAC SDU from corresponding CS and then formatted according MAC PDU format. MAC SDUs possibly fragmented and/or packed (fragmentation and packing) before transmission into air. Fragmentation is the process in which MAC SDU is divided into one or more MAC SDU segments. Packing is process of packing multiple MAC SDUs into a single MAC PDU, both processes are shown below:

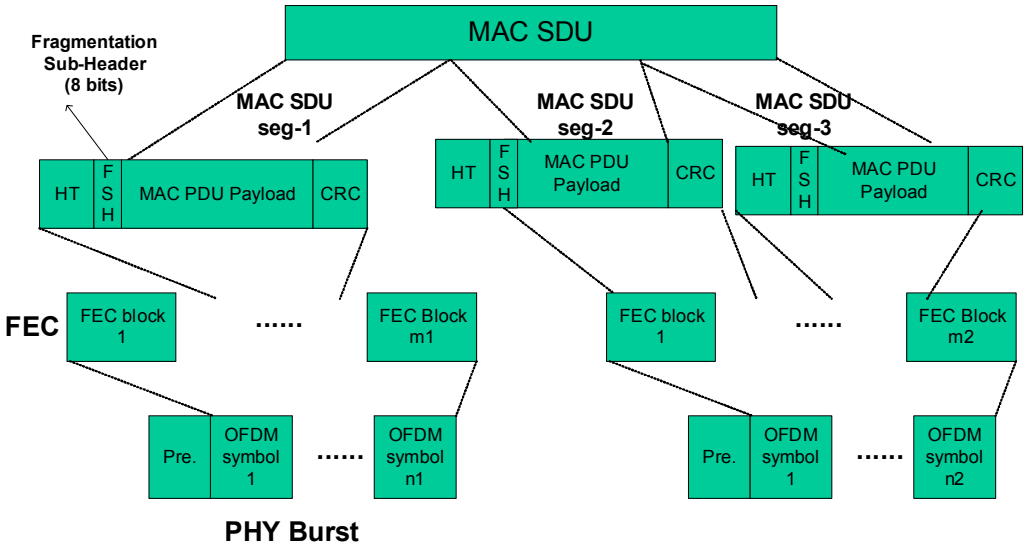

Figure 4.3.4 Fragmentation

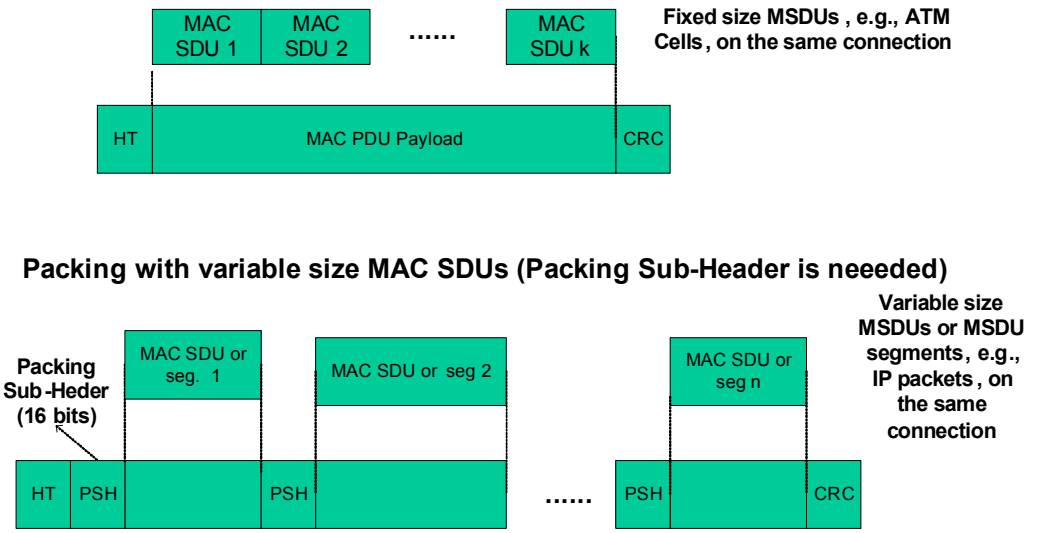

Figure 4.3.5 Packing [20]

After possible fragmentation and packing MAC PDUs are transmitted in PHY burst with FEC blocks.

IEEE 802.16 MAC QoS uses service flow QoS scheduling, dynamic service establishment and two phase activation model (admit first, then activate), to provide better QoS. Service flow is identified through 32 bit SFID (Service Flow ID). Service flow is classified into three types:

Provisioned: When service is only provisioned but not accepted/admitted into system or active, it is controlled by network management system.

Admitted: Allocated service resources are reserved by BS but not active.

Active: BS is committed with the required resources.

80.16 has support for following class of services at MAC CPS.

- UGS: Unsolicited Grant Services
- rtPS: Real-time Polling Services
- nrtPS: Non-real-time Polling Services
- BE: Best Effort

IEEE 802.16 MAC classifies two SS according to their ability to accept bandwidth grants either for SS or for a connection. BW grant requests allow the BS uplink scheduling algorithm to properly consider QoS when allocating bandwidth. BW request messages are sent through BW request header either in contention based BW request slot or a regular UL (uplink) allocation of the SS.

MAC CPS performs *Ranging* (process of acquiring physical parameters, time slots to enable SS to communication with BS). When SS joins a network *initial ranging* is performed, and later to maintain good connection and RF link *periodic ranging* is performed.

MAC uses ARQ based on sliding window protocol to maintain flow control. It has 11 bit sequence no. and uses CRC-32 to check for data errors. This is an optional feature of 802.16.

4.4 Privacy Sublayer (PS)

Privacy Sublayer provides security over the air transmission. Security is provided at the bottom of the MAC protocol's internal layering. SS obtains authorization key and traffic keying material from the BS using PKM protocol. The key management protocol uses X.509 digital certificates, the RSA public-key encryption algorithm between SS and BS.

Security Associations used in 802.16 are of three types: Primary SA which is established during initial registration, Static SA is provisioned within BS and Dynamic SA created dynamically. SAs are identified by 16-bit SAID.

802.16 uses 56-bit DES running in the CBC (cipher block chaining) mode. To reduce the number of computations during normal operation the transmission encryption keys are exchanged using 3DES with a key exchange key derived from the authorization key.

5 Simulation Models and Results

In this section we intend to briefly discuss two types of routing protocols (reactive and proactive), simulation tool OPNET Modeler, its modules which will be used in building up simulations for WMN. Later in the section we will go through project scenarios for WMN where above mentioned protocols will be used and obtain results. At the end will discuss results obtained and conclude discussion.

The intent of the simulation is route traffic between WMN routers and compares two MANET (Mobile Ad hoc Network) routing protocols AODV and OLSR and identify victimized routers creating traffic throughput bottlenecks in the Wireless Mesh Network.

5.1 Routing Protocols

Two types of routing protocols are considered to be used in WMN, first is 'Reactive' and second is 'Proactive'. Combination of both is also used and called 'Hybrid' protocols.

The reactive protocol does not find route till it is required [15], hence no periodic route updates are passed. Reactive protocols are also known as 'on-demand' protocols and find route by flooding. These protocols are power and bandwidth efficient but at the cost of latency in route discovery and not suitable for real time traffic. Examples are AODV, DSR etc.

Proactive protocols are based on periodic exchange of control messages and maintain routing table [15]. They pass local neighborhood information and topological network map to evaluate routes. These protocols can provide route information immediately without any latency but at the cost of bandwidth. Examples of proactive protocols are DSDV, OLSR etc.

For simulation purposes one reactive protocol AODV (Ad hoc On Demand Distance Vector) and one proactive protocol OLSR (Optimized Link State Routing) are used.

5.2 Simulation Tool OPNET Modeler 11.5

OPNET Modeler 11.5 Educational version is used to create simulations for AODV and OLSR. Modeling problem in OPNET are solved by building a network in Network Model, Node Model and Process Model and results are analyzed. Each model is edited in network, node or process editor respectively. Hierarchical relationship is shown in Figure 5.2.1.

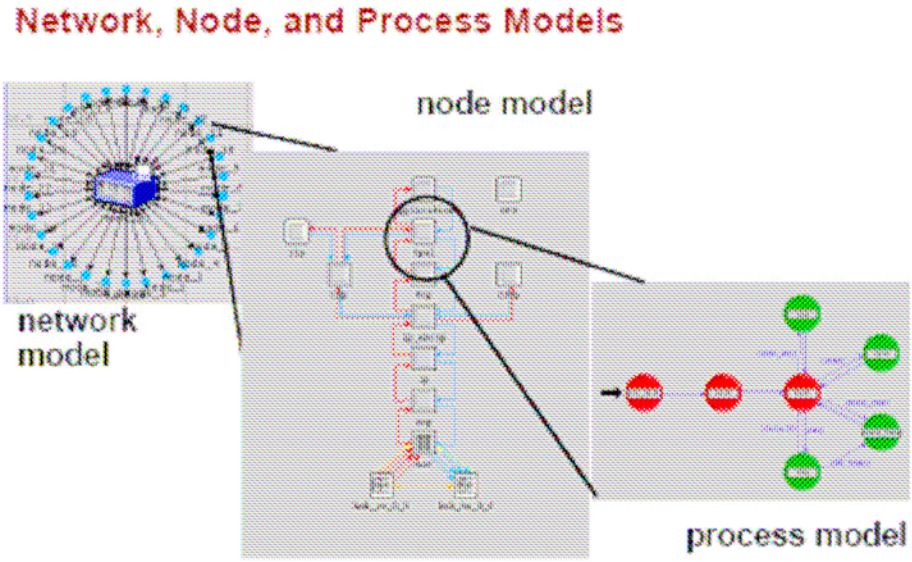

Figure 5.2.1 Network, Node, and Process Models [21]

The work flow [21] to create network model in OPNET is shown below:

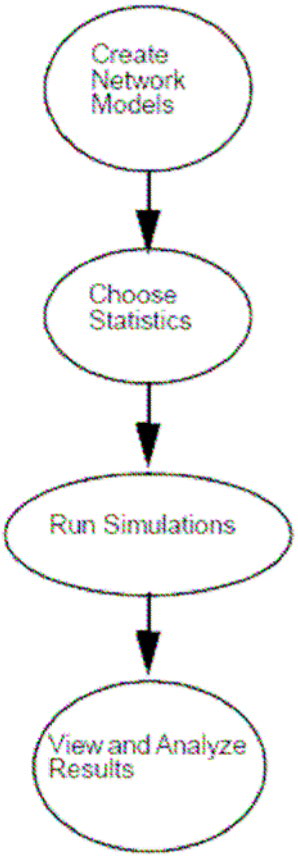

Figure 5.2.2 Steps to create and run simulation around project editor [21]

5.2.1 OPNET EDITORS

OPNET has many types of editor [21] to create projects and build scenarios and collect statistics, brief introduction to those editors is given as under:

- **Project Editor**: From this editor one can build a network model using models from standard library, choose statistics about the network, run simulations and view results.
- **Node Editor**: The Node Editor lets you define the behavior of each network object. Behavior is defined using different modules, each of which models some internal aspect of node behavior such as data creation, data storage, etc. Modules are connected through packet streams or statistic wires. A network object is typically made up of multiple modules that define its behavior.

- **Process Model Editor**: The Process Editor lets you create process models, which control the underlying functionality of the node models created in the Node Editor. Process models are represented by finite state machines (FSMs), and are created with icons that represent **states** and lines that represent **transitions** between states. Operations performed in each state or for a transition are described in embedded C or C++ code blocks.

5.2.2 OPNET Node Models [21]

- MANET station: MANET station models have a raw traffic generator over IP. If application traffic such as HTTP, FTP, etc. are not important and also TCP needs to be omitted, then these station models can be used. They can be used to generate raw packets at a configured rate. MANET station support IEEE 802.11 a/b/g standard. **At the moment OPNET has no support for IEEE 802.16 (WiMax).**

- Wireless LAN Server: In client-server architecture, a workstation connects to server for traffic exchange. The "wlan_server" model can be configured to run any MANET routing protocol and route data packets between a client and server.

- Receiver Group Configuration: The "Receiver Group" Configuration node is used to limit the communication range to a user defined threshold. Under "Receiver Selection Parameters/Selection Parameters", distance or channel match criteria can be supplied in order to restrict communication range. Transmitters use these threshold values to compute the set of possible receivers.
- Application Configuration Module: It is used to create common application (email, file transfer etc) or customized application.
- Profile Configuration Module: A profile is applied to a workstation or server or LAN. It specifies the application used by particular group of users.

5.2.3 Configuring AODV, OLSR and WLAN in OPNET

OPNET has support for various routing protocols using WLAN 802.11 technology. These parameters and selection of routing protocols along with its attributes is done by selecting node attributes in OPNET. Screen shot of MANET workstation and selection option is given in below given figures:

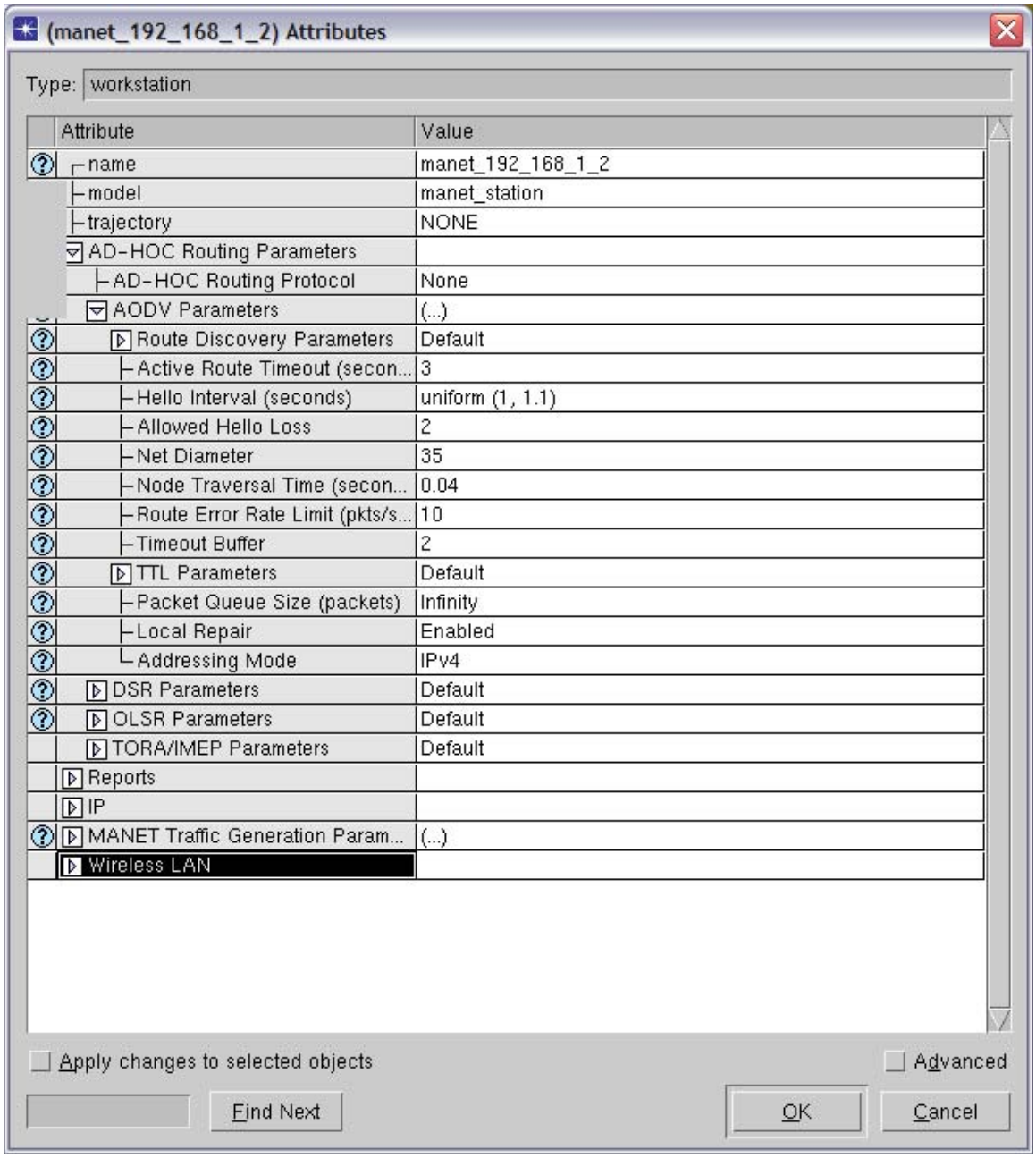

Figure 5.2.1 AODV parameters

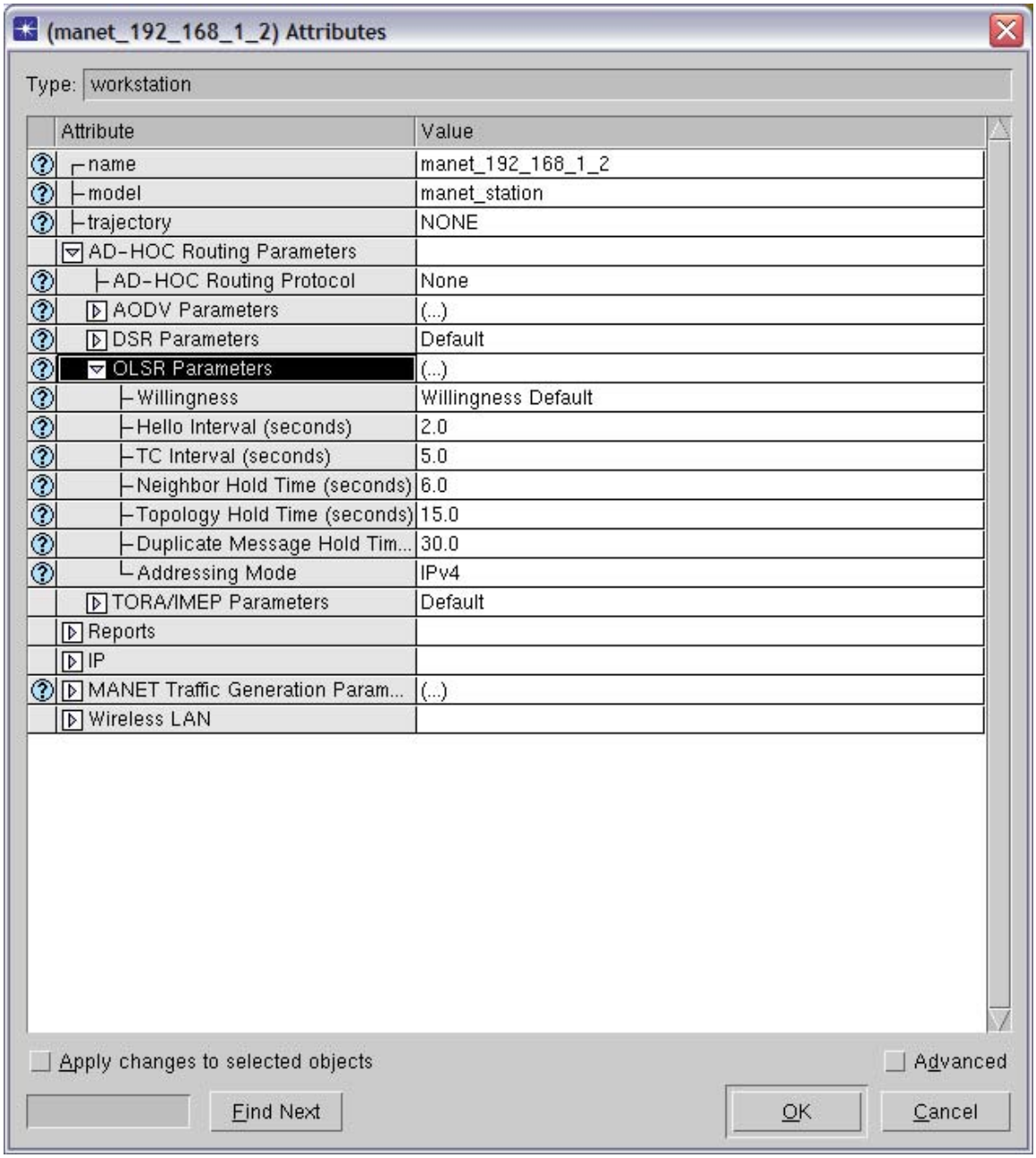

Figure 5.2.2 OLSR parameters

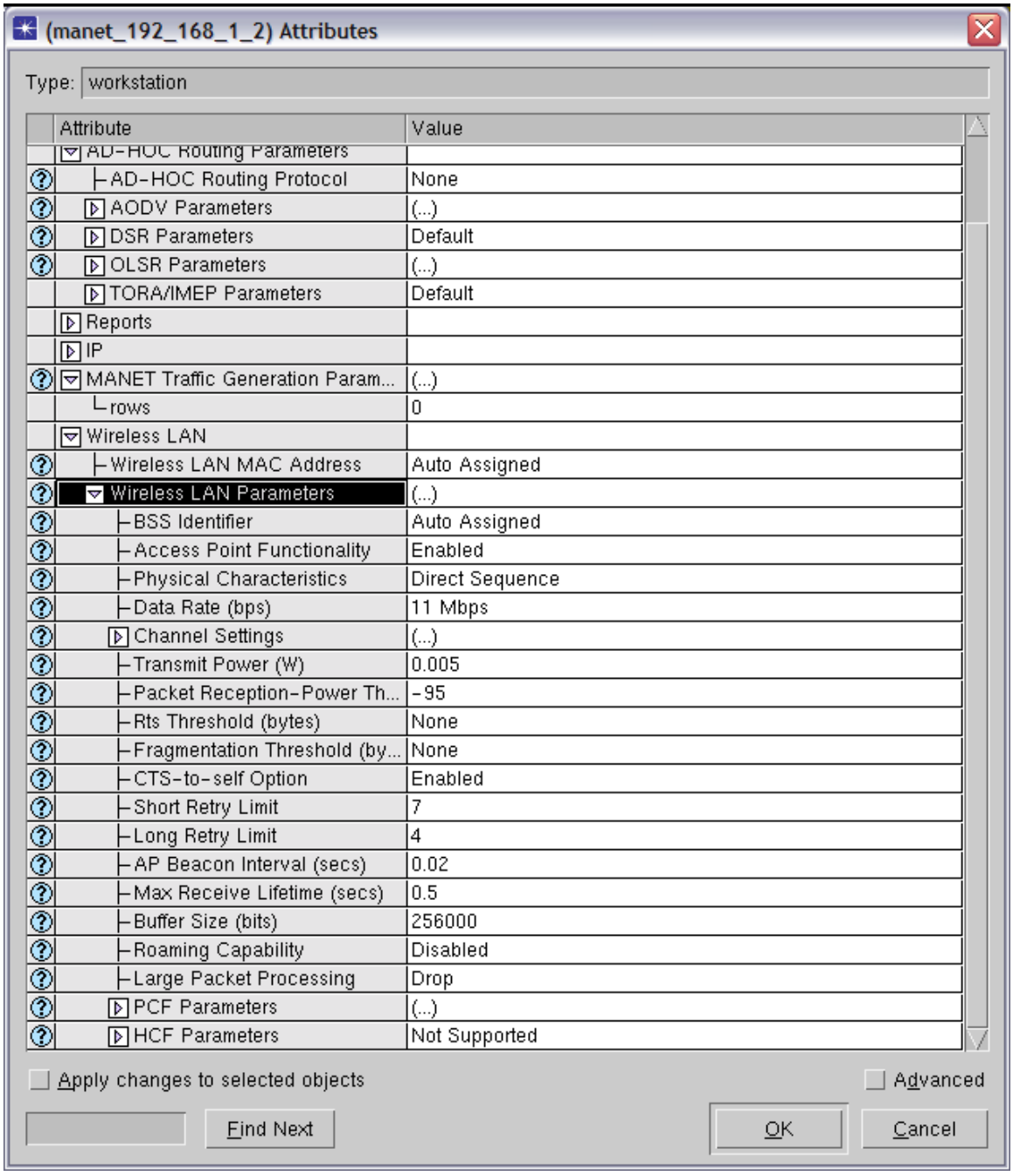

Figure 5.2.3 WLAN parameters

5.2.4 Choosing Statistics for AODV, OLSR and WLAN in OPNET

OPNET has flexibility of choosing different statistics for both AODV and OLSR in addition to WLAN statistics. These statistics are selected either be selecting individual MANET station or also we can set global statistics to view and analyze results after the simulation. OPNET has option of either selecting from the list of standard statistics or customizing results and reporting specific results according to requirement of project. Following figure shows standard list of statistics that can be obtained in OPNET.

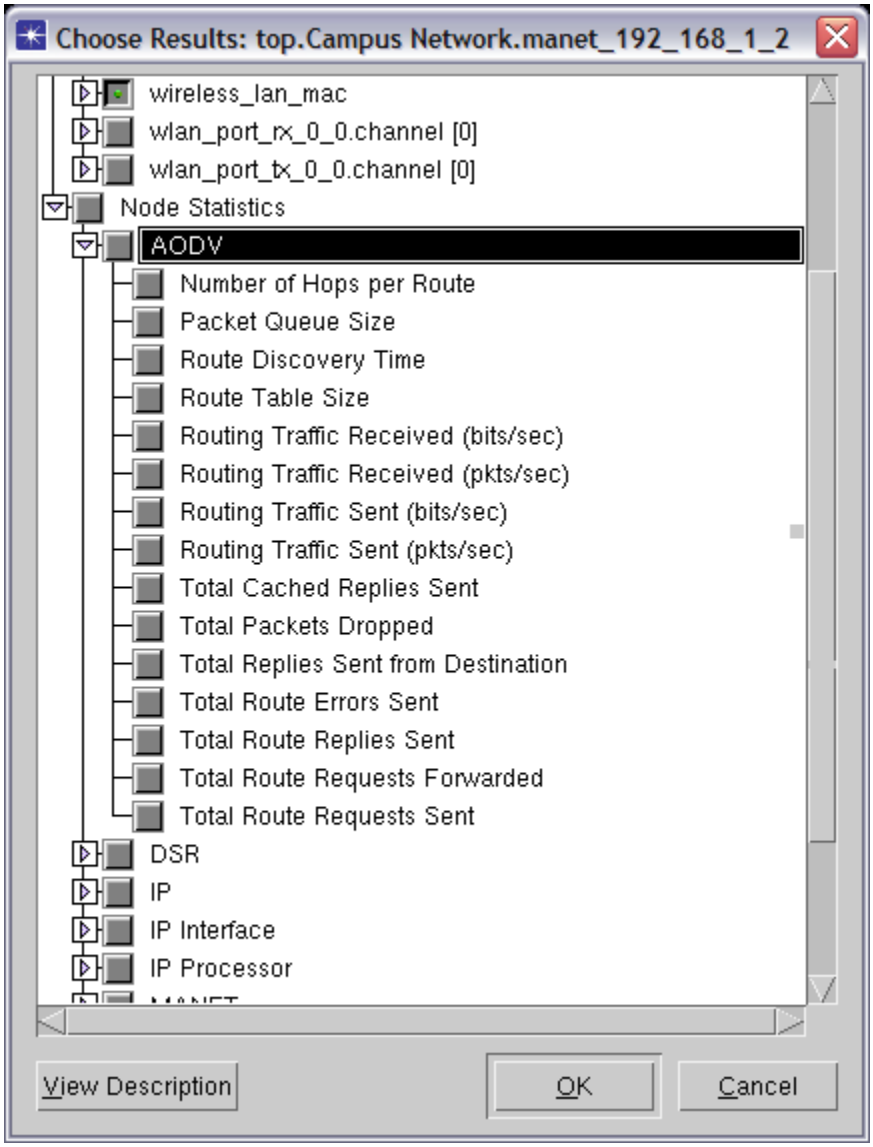

Figure 5.2.4 AODV statistics

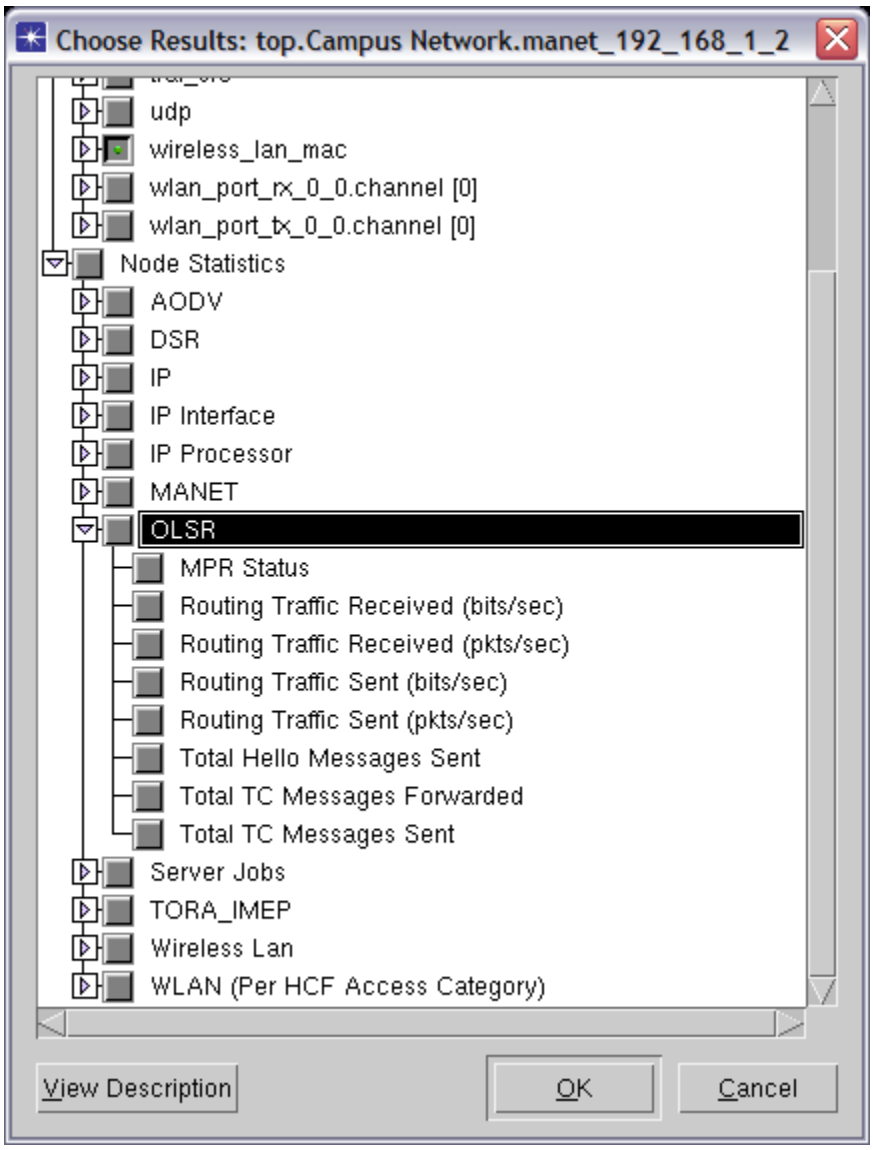

Figure 5.2.5 OLSR statistics

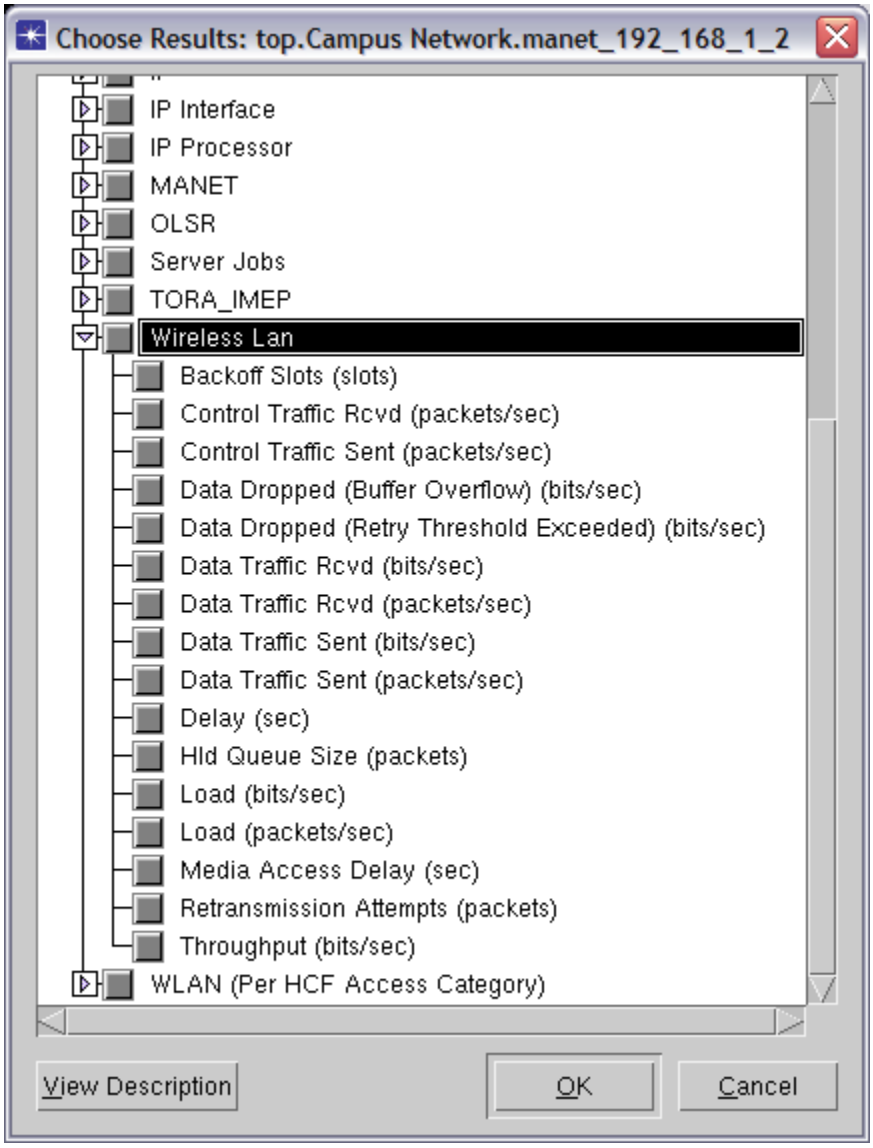

Figure 5.2.6 WLAN statistics

5.3 Experimental Setup

5.3.1 Methodology

In OPNET under single project two scenarios are created. We are using MANET workstation due to its support for both AODV and OLSR routing protocols. MANET workstations represent WMN backbone routers. WMN routers are randomly placed over

a medium size network of 2000x2000 square meter area and suitably configured with IP addresses to forward IP traffic.

We have configured some WMN routers to generate traffic of 200 Kbps and others are not generating any traffic but participating in network and can forward traffic as in multi hop communication networks. WMN nodes are placed randomly without any pre plan to create true randomization and shows growth of network based on demand. WMN routers will generate traffic by setting up traffic generation parameters in Wireless LAN. Technology supported by OPNET is 802.11 (as of today OPNET Modeler does not support 802.16 standard). One MANET workstation is designated as GW where all other traffic routers are sending traffic.

This setup typically represents ISP (Internet Service Providers) design where backbone WMN routers are at the edge level and responsible for not only forwarding traffic by other WMN routers but also forward traffic received by its end clients.

To enhance performance one can tune up setting parameters of WMN routers by changing values for Tx range, Rx sensitivity, RTS/CTS threshold etc.

Details of parameters of WMN routers, GW, statistics obtained and top level diagram and scenario diagrams are given in *Appendix A*

5.3.2 Assumptions

- Single radios at single channel are operating.
- APs have similar transmission properties.
- The medium access is performed according to CSMA/CA protocol with RTS/CTS mechanism
- Propagation and transmission delays are negligible.
- We will ignore the Capacity of router at this stage and consider all WMNR router have same capacity

5.4 Output of Experiment

Results of simulation for both scenarios show very low generation of traffic 200 Kbps results in huge packet loss due to buffer overflow and retry thresholds. Diagrams clearly show although most of the routers perform poorly with both AODV and OLSR but problem of BOF is higher with AODV at individual router levels (nodes). Also low traffic generation causes significant amount of data dropped due to Retry Threshold attempts.

Overall average performance is slightly better in OLSR. When tried higher number of routers in simulation it was observed the amount of data dropped and number of victimized nodes increases rapidly. Table 1 and Table 2 presents node wise details (also refer to appendix A).

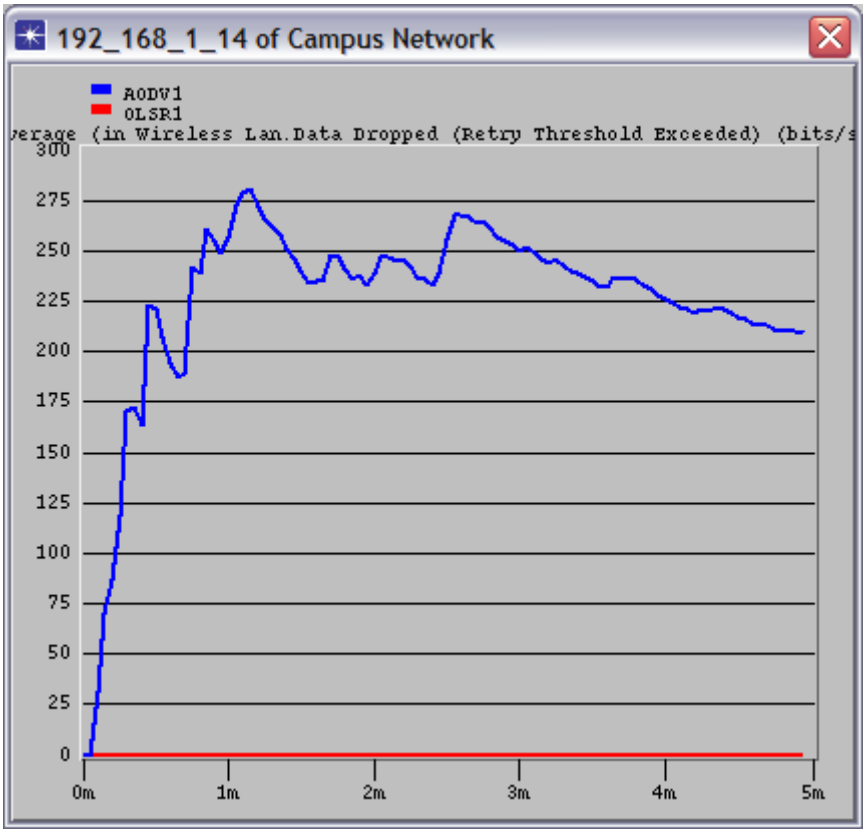

Figure 5.4.1 Data dropped due to Retry Threshold on node 192.168.1.14 only when using AODV

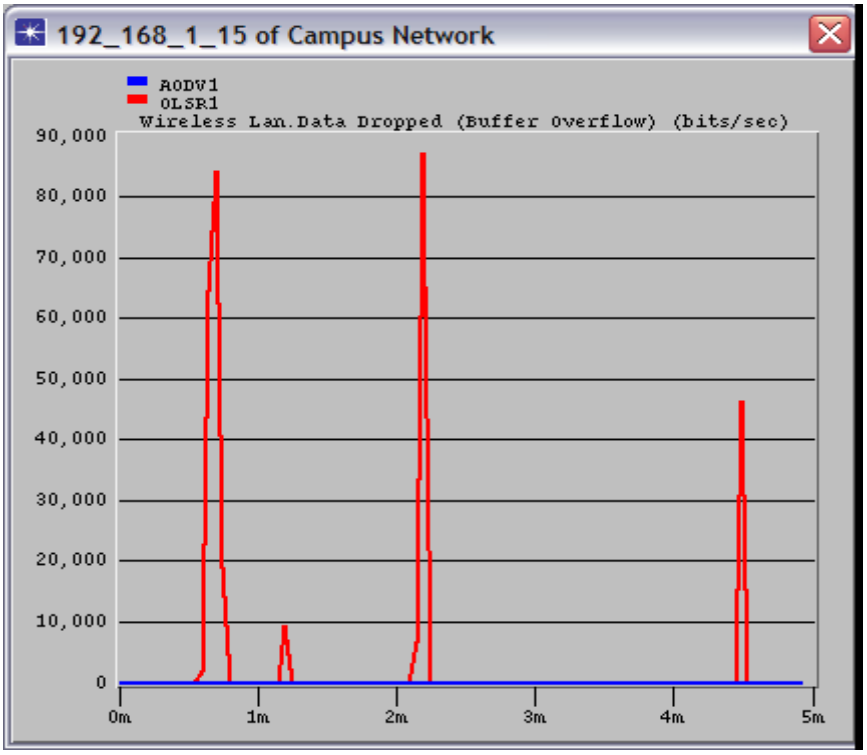

Figure 5.4.2 Data dropped with OLSR due to Buffer Overflow at node 192.168.1.15

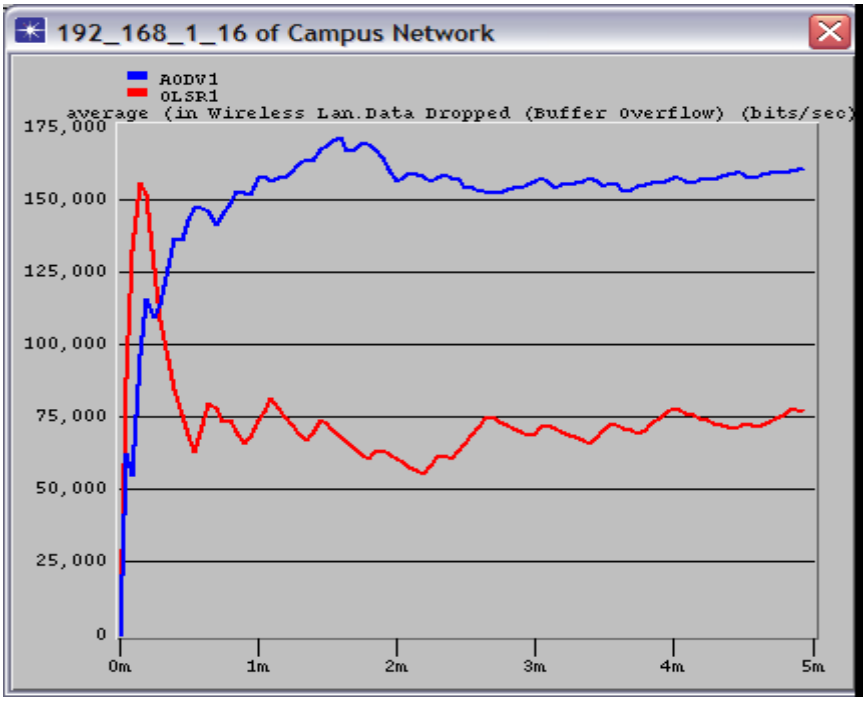

Figure 5.4.3: Node 192.168.1.16 has more data dropped due to Buffer Overflow when using AODV

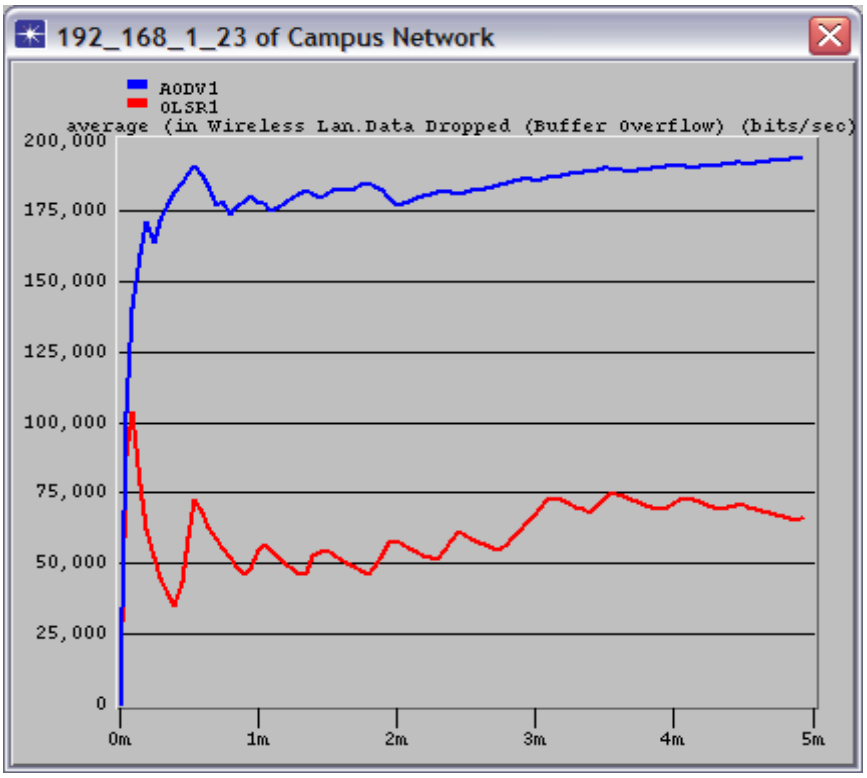

Figure 5.4.4: Node 192.168.1.23 has more data dropped due to Buffer Overflow when using AODV

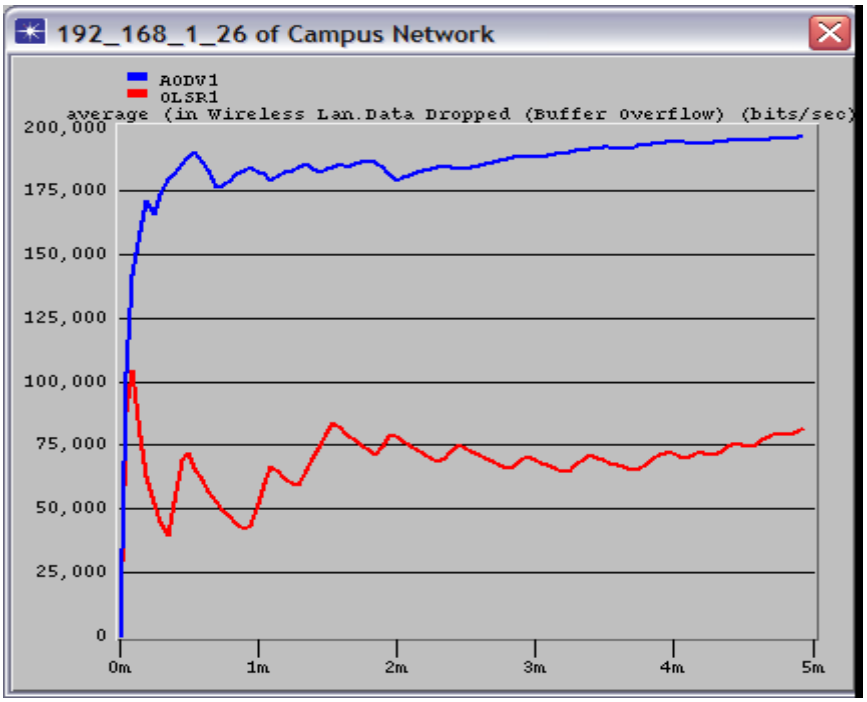

Figure 5.4.5 Node 192.168.1.23 has more data dropped due to Buffer Overflow when using AODV

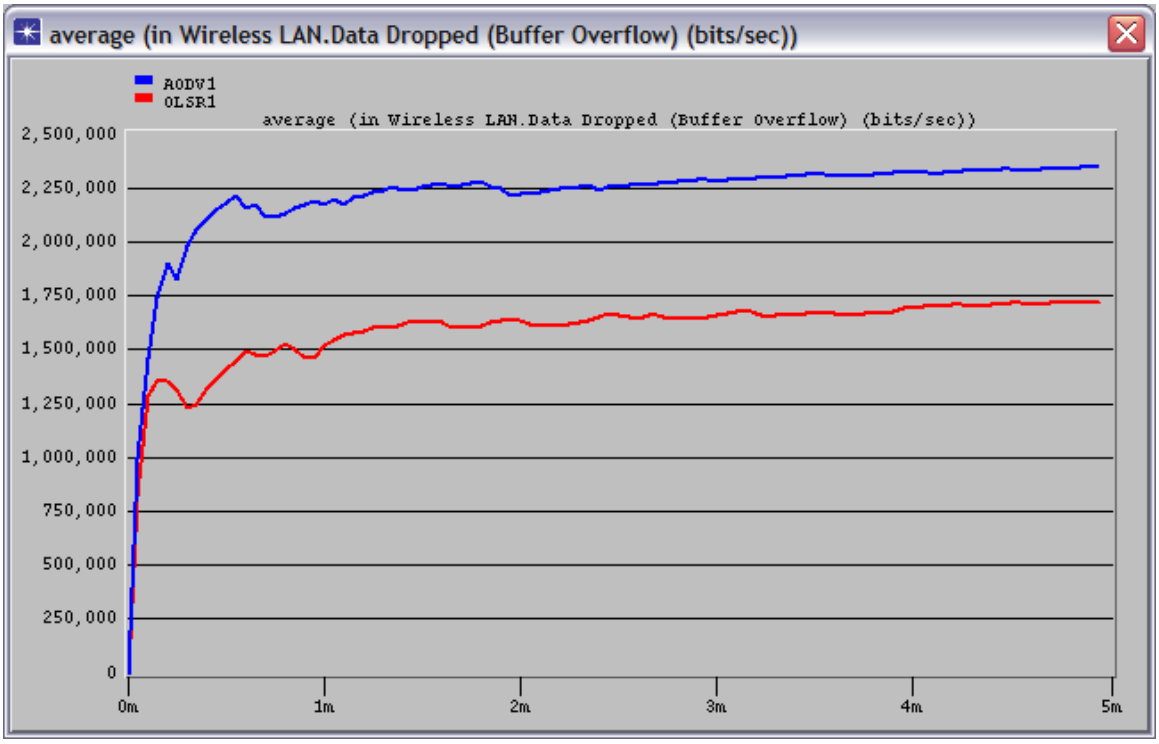

Figure 5.4.6 Overall average data dropped with AODV and OLSR

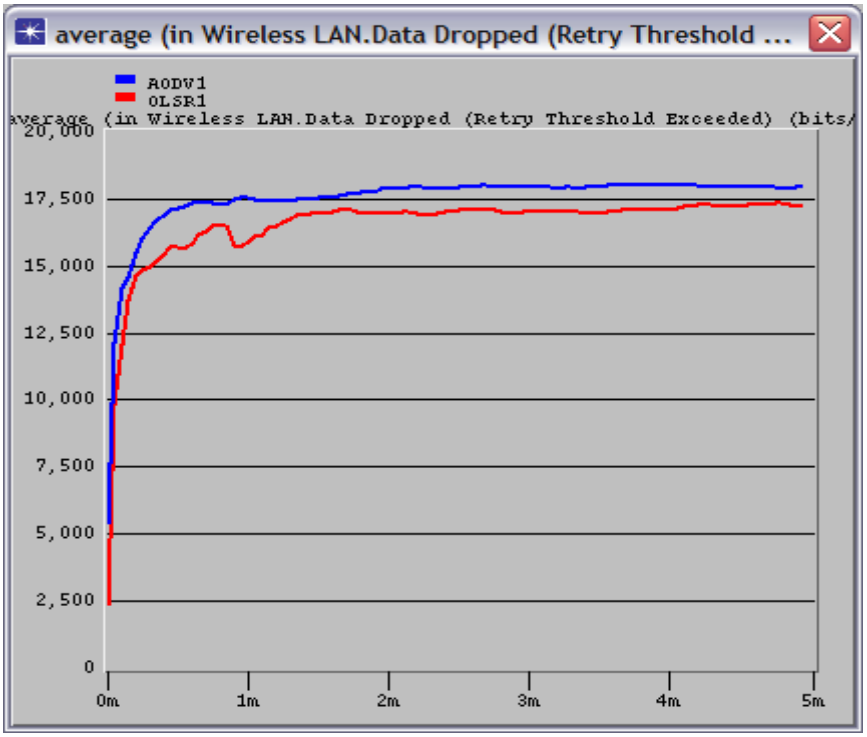

Figure 5.4.7 Overall average data dropped with AODV and OLSR is almost same.

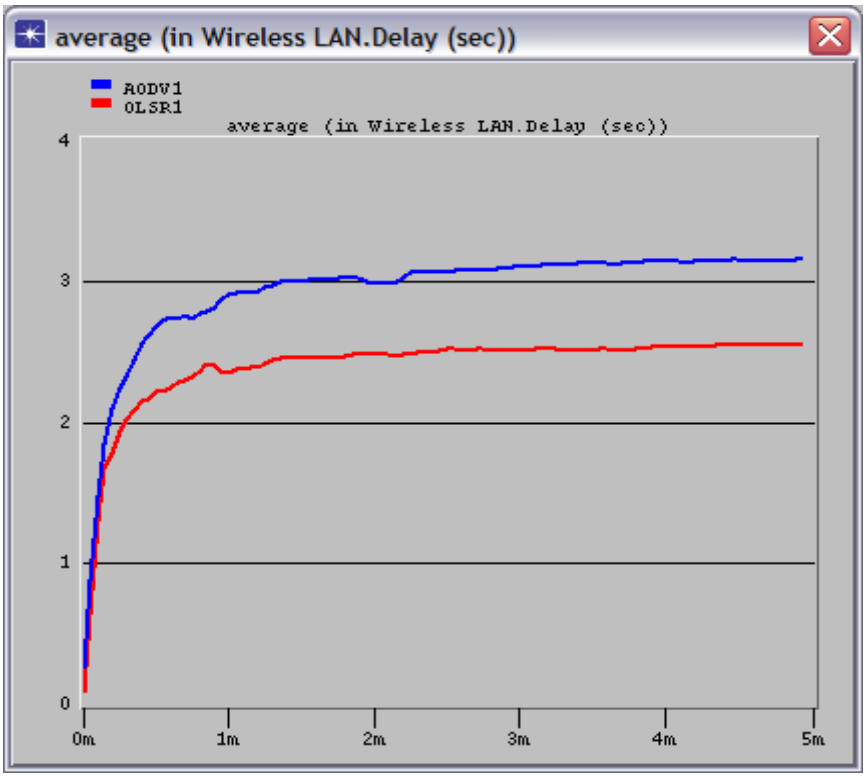

Figure 5.4.8 Overall network delay comparison between AODV and OLSR

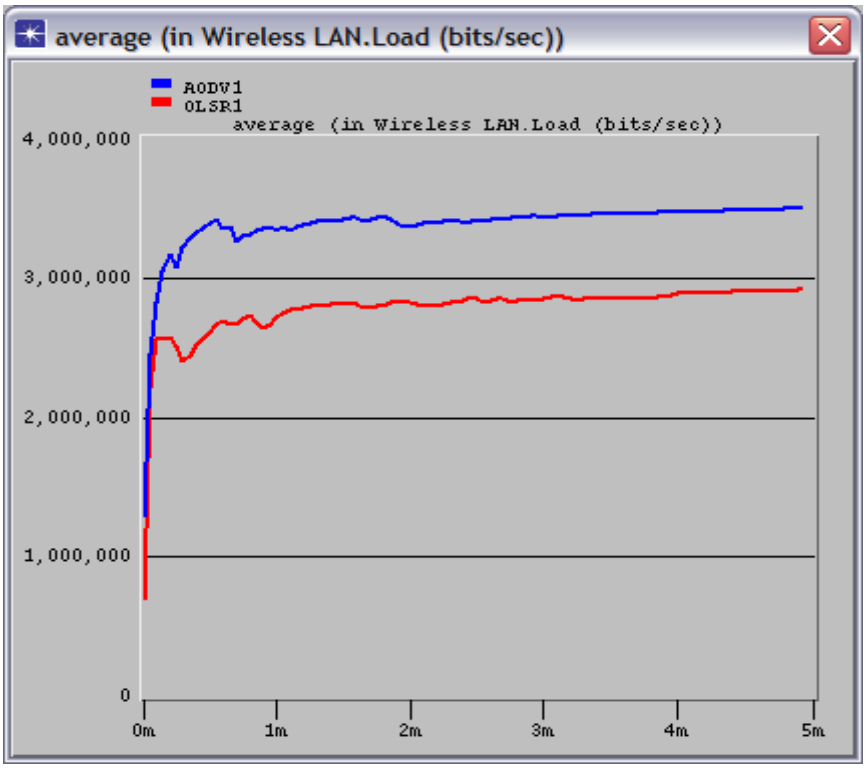

Figure 5.4.9 Average network load

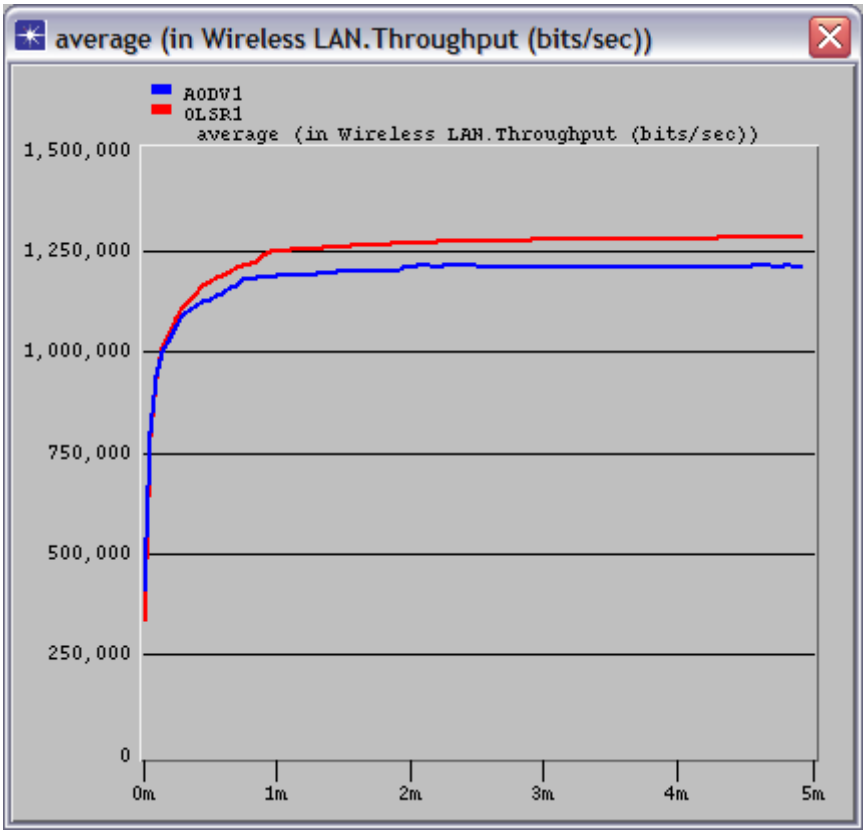

Figure 5.4.10 Average throughput of network

Node	Wireless Lan Data Dropped (Buffer Overflow) (bits/sec)	Wireless Lan Data Dropped (Retry Threshold Exceeded) (bits/sec)	Wireless Lan Data Traffic Rcvd (bits/sec)	Wireless Lan Data Traffic Sent (bits/sec)	Wireless Lan Delay (sec)	Wireless Lan Load (bits/sec)	Wireless Lan Throughput (bits/sec)
192_168_1_1	117,194.05	23.20	2,932,231.09	454,625.73	1.8898	222,623.25	15,166.93
192_168_1_11	10,264.77	11.60	3,416,216.35	161,718.27	2.2916	47,396.80	62,103.47
192_168_1_15	3,192.29	3.87	3,453,486.67	112,707.89	2.5113	28,650.80	34,865.07
192_168_1_16	76,572.45	2,041.60	2,661,532.48	167,953.23	1.6484	98,060.96	5,574.88
192_168_1_19	127,569.63	351.87	3,177,961.79	317,418.99	1.9419	188,739.39	13,973.49
192_168_1_2	114,063.97	88.93	3,318,447.12	394,922.27	1.8701	197,899.01	13,433.68
192_168_1_20	116,592.83	19.33	3,232,490.64	443,364.67	2.3410	219,344.43	36,698.99
192_168_1_22	110,239.84	162.40	2,987,363.44	375,917.67	1.8669	189,705.33	15,356.24
192_168_1_23	66,534.85	8,251.47	1,867,128.61	231,660.27	1.3586	80,966.75	4,641.81
192_168_1_24	117,151.15	266.80	3,319,036.13	339,012.75	1.7964	183,134.59	15,339.31
192_168_1_26	81,775.01	4,960.93	2,089,208.27	176,243.36	1.2452	96,354.93	5,684.05
192_168_1_28	109,185.63	34.80	3,048,669.97	452,009.31	1.9692	214,029.09	25,079.15
192_168_1_5	118,973.79	367.33	2,802,329.20	333,379.60	1.7978	187,132.43	21,935.39
192_168_1_6	100,847.49	58.00	3,373,277.20	399,537.68	1.8285	185,872.85	14,873.33
192_168_1_7	122,492.53	119.87	2,729,175.49	372,710.88	1.7514	198,283.41	16,057.04
192_168_1_8	106,207.89	30.93	3,200,375.60	441,353.97	2.0640	208,224.96	24,419.36
GATEWAY	0.00	0.00	3,501,858.48	5,423.04	2.7081	1,148.16	913,436.93

Table 1 : Average summary of node statistics with OLSR routing protocol

Node	Wireless Lan Data Dropped (Buffer Overflow) (bits/sec)	Wireless Lan Data Dropped (Retry Threshold Exceeded) (bits/sec)	Wireless Lan Data Traffic Rcvd (bits/sec)	Wireless Lan Data Traffic Sent (bits/sec)	Wireless Lan Delay (sec)	Wireless Lan Load (bits/sec)	Wireless Lan Throughput (bits/sec)
192_168_1_1	120,507.55	72.13	2,893,607.09	463,100.53	2.5236	227,203.01	5,237.12
192_168_1_11	0.00	1.28	3,469,062.43	17,367.07	3.4270	1,871.39	5,278.75
192_168_1_14	0.00	208.64	1,974,753.09	20,749.76	3.5085	1,017.49	3,149.65
192_168_1_15	0.00	0.00	3,471,536.21	17,965.68	3.5213	2,068.11	5,523.55
192_168_1_16	160,937.84	2,526.37	2,604,185.89	146,963.20	2.2708	175,758.00	4,390.40
192_168_1_18	156,081.79	328.64	3,003,891.97	332,218.80	3.0831	217,903.01	4,989.87
192_168_1_19	150,340.29	309.31	3,132,004.45	338,064.88	2.9154	213,441.73	5,254.77
192_168_1_2	143,345.79	143.07	3,277,889.79	403,334.96	3.0032	227,016.03	5,718.83
192_168_1_20	117,092.19	46.40	3,166,886.19	469,678.48	3.1952	225,259.44	5,899.31
192_168_1_22	139,766.35	83.76	2,905,658.13	412,518.83	3.0076	225,313.95	5,293.01
192_168_1_23	193,973.57	8,430.08	1,893,297.68	247,622.59	1.9071	209,471.60	3,122.56
192_168_1_24	161,333.95	324.35	3,290,383.52	328,485.57	2.9061	221,899.33	5,541.55
192_168_1_26	196,455.73	4,838.37	2,070,154.24	181,771.01	1.6600	211,197.55	3,781.97
192_168_1_28	115,135.84	15.47	2,991,997.63	482,817.79	2.5291	226,623.76	5,621.33
192_168_1_5	145,659.07	208.77	2,746,052.16	371,351.60	2.4026	220,686.40	4,895.25
192_168_1_6	140,650.11	97.95	3,340,402.29	406,708.75	2.9019	224,412.93	6,086.19
192_168_1_7	144,386.91	122.43	2,661,655.81	375,196.19	2.8664	219,241.60	5,545.28
192_168_1_8	117,298.96	28.35	3,122,068.03	480,135.45	3.0140	228,211.92	5,699.63
GATEWAY	0.00	2.56	3,456,113.41	14,878.40	3.2273	1,422.08	1,111,926.00

Table 2 : Average summary of node statistics with AODV routing protocol

5.5 Conclusion

Simulation results show both AODV and OLSR protocols are generating overhead traffic to exchange routing information. Data drop due to threshold retry and buffer over flow is high and observed in many nodes. When compared among AODV and OLSR, later has better performance than former. Even with that performance as intended for WMNs to be used at backbone is not very suitable. We observe through obtained results some nodes are not participating at all or throughput of router nodes is very low. These under utilized nodes can participate more actively and further traffic can be routed through those nodes in order to distribute traffic load. AODV and OLSR does not take into account physical layer link information (as investigated in cross layer routing). This information can be helpful to enhance performance of network and distribute traffic load.

Special requirement and topology of WMN requires a new protocol to be developed for WMN which considers link quality, load balancing, scalability, adaptive support for mesh routers and clients, various performance metrics, use of multi-radio/multi-channels and cross layer approach.

6 Conclusions and Future Work

WMN is the next generation promise to provide cost effective and efficient solution for network service providers. The perceived ability of WMNs to reconfigure in case of failure is fast. Also most of the bandwidth resources in conventional networks are under utilized and wasted. WMNs are supposed to distribute network load and guarantee real-time and non-real time connectivity.

In this project we surveyed architecture of WMNs and its types. Current direction to develop new protocols and its metrics and how they can impact routing protocol performance was surveyed in next section where two selected research papers were discussed.

The new IEEE 802.16 (Wi-Max) standard is rapidly getting popularity and being deployed. Many telecom companies are producing IEEE 802.16 compliant solutions and deploying market. This is a high speed wireless point to point and point to multi point with LOS and NLOS solution. WiMax is the closest solution at the time to deploy WMN but still a lot of research is required to use WiMax for WMN. The reason behind is special requirement of routing protocols, consideration of link quality. These issues were touched briefly during research paper discussion and overview of IEEE 802.16 was discussed later.

At the end OPNET simulation tool was used to demonstrate performance of two MANET protocols AODV and OLSR to evaluate their suitability for WMNs. Comparison was made and controlled simulation results show due to MAC layer back off, and routing decision to select path was independent of link quality and other performance metrics resulting both OLSR and AODV perform poorly for WMNs. Although OLSR perform slightly better than AODV and number of over utilized and under utilized nodes is less in OLSR (Table 1 and Table 2).

Researchers are working towards development of better routing protocol and already proposed many protocol metrics which can enhance performance of WMNs. Also cross layer approach, multi-radio and multi-channel solutions are getting a lot of attention.

References:

[01] Ian F. Akyildiz, Xudong Wang, “A Survey on Wireless Mesh Networks”, IEEE Radio Communications, September 2005.

[02] Acharya, A., Misra, A., Bansal, S, Design and analysis of a cooperative medium access scheme for wireless mesh networks , BROADNETS 04, 2004, pp.621-631

[03] Jangeun Jun, Sichitiu, M.L., The nominal capacity of wireless mesh networks , Wireless Communications, IEEE, Volume 10, Issue 5, Oct 2003, pp.8-14

[04] Iannone, L., Khalili, R., Salamatian, K., Fdida, S., Cross-layer routing in wireless mesh networks , Wireless Communication Systems, 2004. 1st International Symposium, Sept. 2004, pp.319-323

[05] Ray-Guang Cheng, Cun-Yi Wang, and Li Hung Liao, Ripple: A Distributed Medium Access Protocol for Multi-hop Wireless Mesh Networks, Vehicular Technology Conference, 2006. VTC 2006-Spring. IEEE 63rd

[06] P. Gupta and P.R. Kumar, “The capacity of wireless networks,” IEEE Transactions on Information Theory, Mar. 2000.

[07] R. Khalili and K. Salamatian, “On the distribution of errors in convolutional codes,” Proceeding of IST’03, Aug. 2003.

[08] J. Jangeun and M. L. Sichitiu, "The nomial capacity of wireless mesh networks," IEEE Wireless Communications, pp. 8-14, Oct.2003.

[09] S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks?" IEEE Communications Magazine, P130-137, June 2001.

[10] A. Acharya and A. Misra, "High-performance architecture for IP-based multihop 802.11 networks," IEEE Wireless Communications, pp.22-28, Oct. 2003

[11] D. Raguin, M. Kubisch, H. Karl, and A. Woltz, "Queue-driven cut-through medium access in wireless ad hoc networks," Proc. ofIEEE WCNC, pp.1909-1914, 2004.

[12] J. Li, C. Blake, D. S. De Couto, H. I. Lee, and R. Morris, "Capacity of ad hoc wireless networks," Proc. ofACMMobiCom, pp. 61-69, July 200 1.

[13] V. Lo, D. Zhou, Y. Liu, C. GauthierDickey, and J. Li, “Scalable supernode selection in peer-to-peer overlay networks,” in Proc. IEEE International Workshop on Hot Topics in Peer-to-Peer Systems (HOT-P2P) 2005, pp. 18-27.

[14] J. Li, C. Blake, D. S. De Couto, H. I. Lee, and R. Morris, “Capacity of ad hoc wireless networks,” in Proc. ACM MobiCom, pp. 61-69, July2001.

[15] P.Jacquet, P. Muhlethaler, T.Clausen, A.Lauiti, A. Qayyum, L. Viennot, “Hipercom Project, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France” 2001 IEEE

[16] IEEE 802.16a-2003, "IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems - Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz", Apr. 1, 2003.

[17] Carl Eklund, Roger B. Marks, Kenneth L. Stanwood and Stanley Wang, "IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access", IEEE Communications Magazine, vol. 40, Issue: 6, June 2002, pp. 98 – 107.

[18] Intel Technical Journa, “ IEEE 802.16 Medium Access Control and Service Provisioning”, Volume 08, Issue 03 Published, August 20, 2004.

[19] Alan Barry, Georoge Healy, Cian Daly, Joseph Johnson and Ronan J. Skehill, “ Overview of Wi-Max IEEE 802.16”

[20] http://www.itr-rescue.org/bin/pubdocs/mtg-weekly/ , Karim M. El Defrawy, “WiMax for Broadband Wireless Access”.

[21] OPNET 11.5 documentation distributed with software.

[22] Richard Draves, Jitendra Padhye, Brian Zill, "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks", International Conference on Mobile Computing and Networking, Proceedings of the 10th annual international conference on Mobile computing and networking, SESSION: Algorithms for multihop networks, ACM Press, September 2004, pp. 114-128,

Appendix A

Project: WMN	Report: User Selected
Scenario: AODV1	**Title: Top Objects for Wireless Lan**

Wireless Lan Data Dropped (Buffer Overflow) (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
192_168_1_26	196,455.73	293,613.33
192_168_1_23	193,973.57	222,882.67
192_168_1_24	161,333.95	380,848.00
192_168_1_16	160,937.84	286,629.33
192_168_1_18	156,081.79	279,485.33

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Data Dropped (Retry Threshold Exceeded) (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
192_168_1_23	8,430.08	10,863.25
192_168_1_26	4,838.37	6,439.76
192_168_1_16	2,526.37	3,820.76
192_168_1_18	328.64	926.00
192_168_1_24	324.35	1,265.71

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Data Traffic Rcvd (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
192_168_1_15	3,471,536.21	3,576,618.67
192_168_1_11	3,469,062.43	3,574,600.00
GATEWAY	3,456,113.41	3,566,130.67
192_168_1_6	3,340,402.29	3,514,986.67
192_168_1_24	3,290,383.52	3,441,418.67

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Data Traffic Sent (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
192_168_1_28	482,817.79	603,762.67
192_168_1_8	480,135.45	590,826.67
192_168_1_20	469,678.48	594,048.00
192_168_1_1	463,100.53	583,509.33
192_168_1_22	412,518.83	523,074.67

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Delay (sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
192_168_1_15	3.5213	11.937
192_168_1_14	3.5085	12.240
192_168_1_11	3.4270	11.223
GATEWAY	3.2273	3.526
192_168_1_20	3.1952	10.256

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Load (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
192_168_1_8	228,211.92	373,138.67
192_168_1_1	227,203.01	377,954.67
192_168_1_2	227,016.03	359,834.67
192_168_1_28	226,623.76	342,285.33
192_168_1_22	225,313.95	397,237.33

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Throughput (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
GATEWAY	1,111,926.00	1,170,090.67
192_168_1_6	6,086.19	30,026.67
192_168_1_20	5,899.31	27,274.67
192_168_1_2	5,718.83	29,834.67
192_168_1_8	5,699.63	27,520.00

All objects listed in this table are located in the "Campus Network" network.

Project: WMN Report: User Selected

Scenario: OLSR1 **Title: Top Objects for Wireless Lan**

Wireless Lan Data Dropped (Buffer Overflow) (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
192_168_1_19	127,569.63	296,869.33
192_168_1_7	122,492.53	326,074.67
192_168_1_5	118,973.79	650,058.67
192_168_1_1	117,194.05	365,274.67
192_168_1_24	117,151.15	347,824.00

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Data Dropped (Retry Threshold Exceeded) (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
192_168_1_23	8,251.47	12,547.30
192_168_1_26	4,960.93	7,366.83
192_168_1_16	2,041.60	3,953.18

192_168_1_5	367.33	1,344.43
192_168_1_19	351.87	1,915.47

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Data Traffic Rcvd (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
GATEWAY	3,501,858.48	3,747,096.75
192_168_1_15	3,453,486.67	3,700,400.00
192_168_1_11	3,416,216.35	3,845,342.78
192_168_1_6	3,373,277.20	3,813,246.18
192_168_1_24	3,319,036.13	3,590,899.38

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Data Traffic Sent (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
192_168_1_1	454,625.73	620,357.33
192_168_1_28	452,009.31	637,034.67
192_168_1_20	443,364.67	591,820.85
192_168_1_8	441,353.97	611,800.00
192_168_1_6	399,537.68	571,562.67

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Delay (sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
GATEWAY	2.7081	3.468

192_168_1_15	2.5113	8.556
192_168_1_20	2.3410	9.387
192_168_1_11	2.2916	10.874
192_168_1_8	2.0640	10.500

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Load (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
192_168_1_1	222,623.25	466,437.33
192_168_1_20	219,344.43	424,821.33
192_168_1_28	214,029.09	545,250.67
192_168_1_8	208,224.96	489,981.33
192_168_1_7	198,283.41	414,989.33

All objects listed in this table are located in the "Campus Network" network.

Wireless Lan Throughput (bits/sec)

Statistic sampling period is 3 seconds.

Sort By Node	Sorted By Average	Sort By Peak
GATEWAY	913,436.93	1,177,362.67
192_168_1_11	62,103.47	499,186.67
192_168_1_20	36,698.99	368,981.33
192_168_1_15	34,865.07	217,333.33
192_168_1_28	25,079.15	317,976.00

All objects listed in this table are located in the "Campus Network" network.