A Methodology for Secured Routing and Intrusion Detection in Wireless Mesh Networks

S. Aarthi,
Asst Professor, Dept of CSE, G.Pullareddy engg college(autonomous),Kurnool.
Email:aarthis1@gmail.com

M. Padma,
Asst Professor,
Dept of CSE, GPREC, Kurnool.
Email:padma.gprec@gmail.com

B. Kiranmayee,
Asst Professor, Dept of CSE, GPREC, Kurnool.
Email:kiranmayeereddy67@gmail.com

Abstract:-The basic aspect of evolution of wireless mesh networks is its characteristic of dynamically self organising, self configured nodes in the network that establish a mesh connectivity with lower mobility mesh routers, low power consumption of nodes that has put this technology into the emerging trends of the day to day networking applications. In general, throughput and security are two vast areas of research. Here we propose the methodology of handling both the security aspect and efficient routing. Initially the main aspect of an efficient communication is through exchange of information that shouldn't avail ease of access by unauthenticated parties, therefore security issues have to be concentrated. Here we discuss various aspects optimal path selection for efficient routing considering the relevant routing metrics that proportionately affects the throughput. Finally several intrusion detection mechanisms are followed and basic approaches of their prevention for the black hole and grey hole attacks. All these aspects can be visualised by the network simulator tools like ns2, ns3, nctuns etc.

Keywords: *WMN, routing metric, throughput, end-end delay, black hole, grey hole attack, intrusion detection, network simulators.*

*****

I. Introduction

Today, internet has become an indispensible part of our lives. It has become the most important aspect from banking transactions to online entertainments.The evolution of wireless mesh network started from emerging categories of several networks starting with the wireless networks like wlans, wmans, wi-fi, adhoc networks, MANETS .The concept of an adhoc network is the self organising of the nodes into a network when they come into a vicinity where exchange of data takes place for their interoperability. Later evolution of MANETS i.e the mobile adhoc networks provide the similar characteristics of an adhoc network with an enhanced feature of mobility of the nodes. Several drawbacks were identified and concentrated by various researchers like the continuous link breakages, route maintenance issues, power consumption of the nodes had adverse effects on the throughput and delay.

Focusing on the drawbacks of the mobile adhoc networks the evolution of wireless mesh networks has overcome the issues and became the most used technology for the day to day emerging applications. .A WMN is a dynamically self-organized and self- configured with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves .This feature brings in many advantages to WMNs such as low up-front costs, easy network maintenance, robustness, and reliable service coverage.

Wireless Mesh Networking has become an evolving technology for several day to day applications like broadband home networking, community and neighbourhood networks, enterprise networking, building automation, etc. It has great significance as a cash-strapped service for Internet service providers (ISPs), carriers, and others to bring in robust and reliable wireless broadband service which requires minimal up-front investments. The basic characteristic features of self-organization and self-configuration helps in deploying WMNs incrementally, one node at a time, as per the need. As the no of nodes increase, the reliability enhances, also the connectivity thereby all the subscribers will enjoy the service.

Deploying a WMN is not too difficult, since the required components are readily available in the form of various ad hoc routing protocols like MAC protocol, wired equivalent privacy (WEP) security, etc. These routing protocols cannot be directly applied to WMN's since they do not have enough scalability; e.g., throughput drops significantly as the number of nodes or hops increases. Several existing security schemes can be applied to WMNs but in certain issues they require more to be worked on the levels of protocols ranging from MAC to application layers.

II. ARCHITECHTURE

The WMN architecture comprises of mesh routers and mesh clients. Other than the routing capability for gateway/repeater functions as in a conventional wireless router, a wireless mesh router contains additional routing functions[1] to support mesh networking. Optionally, the medium access control protocol in a mesh router is enhanced with a better scalability in a multi hop mesh environment.

The architecture of WMNs can be classified into three main groups based on the functionality of the nodes.

• Infrastructure/Backbone WMNs: The architecture can be viewed in the fig 2.1 where the dashed and the solid lines represent the wireless and wired links, respectively. The wireless mesh router acts as a backbone router that helps connectivity across several clients also across the network nodes belonging to other networks still in the same radio frequencies, in addition to the heavily used IEEE 802.11 technology.

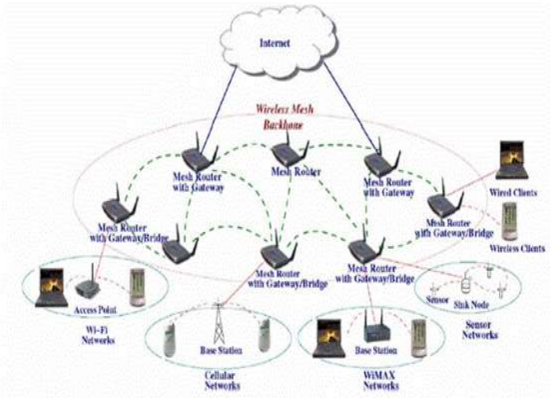

Fig 2.1 Infrastructure/Backbone based network

The mesh routers form a mesh of self-configuring, self healing links among themselves. With gateway functionality [1], the mesh routers can be connected to the internet.

• *Client WMNs*: Client meshing provides peer-to-peer networks among client devices. This type of network reflects that the client nodes themselves form a network there by the mesh router need not act as a backbone and is not required in this type of network. The basic architecture is shown below.

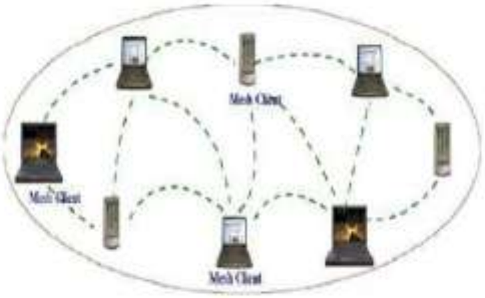

Fig 2.2 Client based network

• Hybrid WMNs: This architecture is the combination of infrastructure and client meshing as shown in Figure 2.3. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, Wi-MAX, cellular, and sensor networks, the routing capabilities of clients provide improved connectivity and coverage inside the WMN.

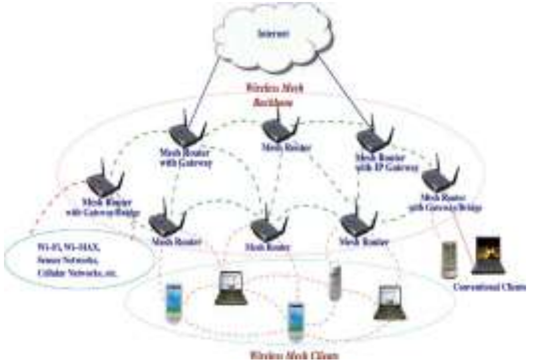
Internet
Wireless Mesh Backbone
Mesh Router with Gateway
Mesh Router
Mesh Router with IP Gateway
Mesh Router with Gateway/Bridge
Mesh Router with Gateway/Bridge
Mesh Router
Mesh Router
Mesh Router
Wi-Fi, Wi-MAX, Sensor Networks, Cellular Networks, etc.
Conventional Clients
Wireless Mesh Clients

Fig 2.3: Hybrid networks

III. Characteristics of WMNs:

The characteristics of WMNs can be listed as follows:

- ***Multi-hop wireless network****:* The basic objective of WMNs is to increase the coverage area without sacrificing the channel capacity. Another objective is to provide non-line-of-sight (NLOS) connectivity among the users. These objectives can be met following the multihopping concept of mess networks that enhances the throughput with low channel interferences with short links between nodes and channel reusage.
- ***Support for ad hoc networking, and capability of self-configuring, self-healing, and self-organization.*** WMNs enhance network performance, because of flexible network architecture, easy deployment and configuration, fault tolerance, and mesh connectivity, i.e., multipoint-to-multipoint communications.
- ***Mobility dependence:*** Mesh routers usually have minimal mobility, while mesh clients can be stationary or mobile nodes.
- ***Multiple types of network access***. In WMNs, both backhaul access to the Internet and peer-to-peer (P2P) communications are supported.
- ***Dependence of power-consumption***: Mesh routers do not have much pressure for power consumption rather the clients have to be concentrated due to their greater mobility. Thus protocols designed for mesh routers need to undergo various changes to get applied to the clients.

- ***Compatibility and interoperability with existing wireless networks**:* WMNs built based on IEEE 802.11 technologies must be compatible with various IEEE 802.11 standards in the sense of supporting both mesh capable and conventional Wi-Fi clients. Such WMNs also need to be inter-operable with other wireless networks such as WiMAX, Zig-Bee, and cellular networks.
- ***Wireless infrastructure/backbone**:* WMNs consist of a wireless backbone with mesh routers. The wireless backbone provides large coverage, connectivity, and robustness in the wireless domain.
- ***Integration***: WMNs support conventional clients that use the same radio technologies as a mesh router. This is accomplished through a host-routing function available in mesh routers.
- ***Dedicated routing and configuration***. In ad hoc networks, end-user devices also perform routing and configuration functionalities for all other nodes. However, WMNs contain mesh

routers for these functionalities. Hence, the load on end-user devices is significantly decreased, which provides lower energy consumption and high-end application capabilities that also decreases the device cost.

• ***Multiple radios***. This tells us regarding the radio frequencies of communication. When two different networks are within same frequency range they get connected easily else they need to connect through the corresponding access points i.e. through Ethernet.

• ***Mobility*** The client nodes accomplish mobility factor which affects the routing tables, links hence they must be handled using appropriate route maintenance.

IV. Application scenarios

The emerging trend of the WMNs shows its advantage over several day to day applications in the promising market. These applications cannot be supported directly by other wireless networks such as cellular networks, ad hoc networks, wireless sensor networks, standard IEEE 802.11, etc. The following are the list of several applications[1]

1. ***Broadband home networking:*** In general the broad band home networking is found by application of WLANs but in a home we can identify various dead zones, which is a great analysis. To overcome this issue no of access points need to be placed which is cost effective. In such scenario WMNs setup is a best choice.

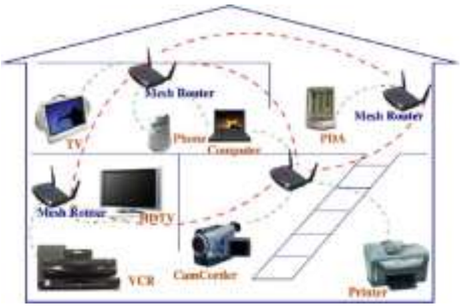

Fig 4.1 Broadband home network

2. ***Community and neighbourhood networking:*** This type of network enhances connectivity via dsl link connected to the service modem which has several drawbacks.

- ➢ For any information to be shared across connectivity to internet is required.
- ➢ There exist several dead zones that need to be identified in order to overcome.
- ➢ Large bandwidth is available which not used cannot be re use thereby degrading resource utilization which makes the service cost high for the users.

WMNs mitigate the above disadvantages through flexible mesh connectivity between homes. WMNs can also enable many applications such as distributed file storage, distributed file access, and video streaming.

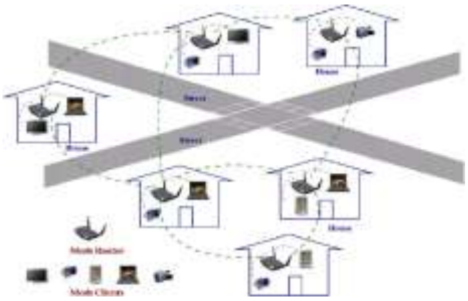

Fig 4.2 Community network

3. *Enterprise networking:* Enterprise here may represent an office or area. A single connection is available to the access point through which all information has to be transformed by backhaul access. Availability of large bandwidth, unused leads to low resource utilization. Instead if the access points are replaced by mesh routers, Ethernet wires can be avoided, multiple backhaul modems can be shared enhancing the resource utilization. The service model of enterprise networking can be applied to many other public and commercial service networking scenarios such as airports, hotels, shopping malls, convention centres, sports centres, etc.

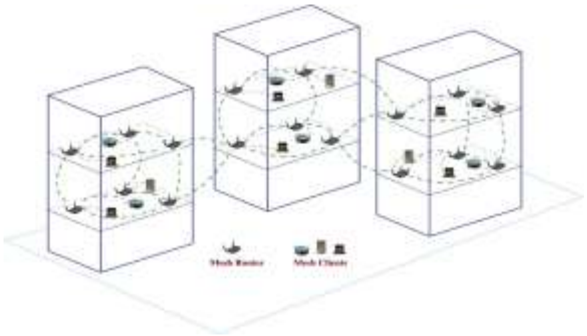

Fig 4.3 Enterprise network

4. ***Metropolitan area networks:*** Usage of WMNs in MANs reflects several advantages. The physical layer transmission of a node in WMNs is greater than any other cellular networks and moreover communication between the nodes doesn't rely upon the backbone. Fig 4.4 Compared to wired networks, e.g., cable or optical networks, wireless mesh MAN is an economic alternative to broadband networking, especially in underdeveloped regions. Wireless mesh MAN covers a potentially much larger area than home, enterprise, building, or community networks. Thus, the requirement on the network scalability by wireless mesh MAN is much higher than that by other applications.

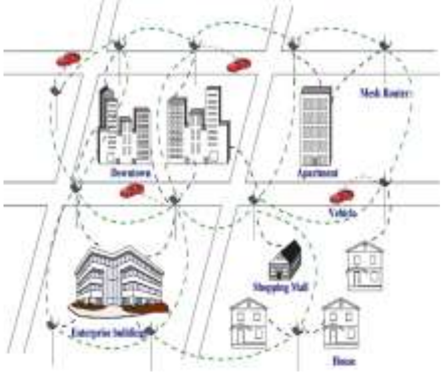

Fig 4.4 Metropolitan area network

5. *Transportation systems:* Instead of limiting the technology IEEE 802.11 or 802.16 just to access stations and stops it can be extended evn into moving vehicles like cars, buses, ferries and trains.Using this applications like passenger information services, remote monitoring of in-vehicle security video and driver communications can be supported. To support this WMN for a transportation system, two key techniques are needed: the high-speed mobile backhaul from a vehicle (car, bus, or train) to the Internet and mobile mesh networks within the vehicle. The architecture is shown in Fig 4.5.

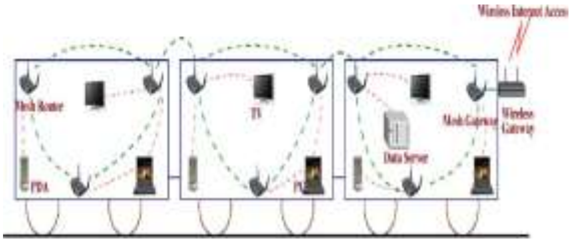

Fig 4.5 Transportation systems

6. ***Building automation*** In a building, various electrical devices like power, light, elevator, air conditioner, etc., need to be controlled and monitored. In general it is done using wired networks which is very expensive later replaced using wi-fi which also was found unsatisfactory. If access points in BAC are replaced by mesh routers, as shown in fig 4.6, the deployment cost gets significantly reduced. The deployment process is also much simpler due to the mesh connectivity among wireless routers.

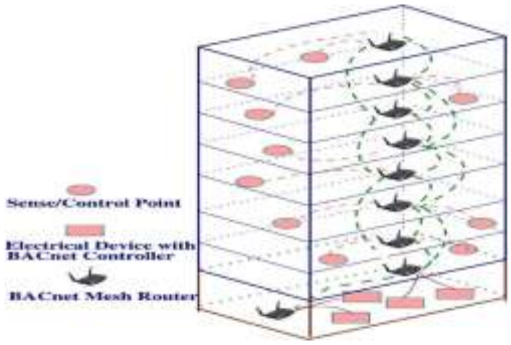

Fig 4.6 Building automation

7. ***Health and medical systems:*** In a hospital or medical center, monitoring and diagnosis data need to be processed and transmitted from one room to another for various purposes. In such areas WMNs can be used.
8. ***Security surveillance systems:*** As security is turning out to be a very high concern, security surveillance systems become a necessity for enterprise buildings, shopping malls, grocery stores, etc.

V. ROUTING SCENARIOS

The main motto of any network is sharing of the information across; technically we name this process of data transfer starting from the source to the intended location (destination) as ROUTING. To attain efficient data transfer with no ease of access by unauthorised users, security is essential. For the efficient or optimal path selection, corresponding routing metrics or measures are to be followed .

Routing in WMNS[2] is a research area. Many routing objectives are same as the conventional networks with several additional objectives as follows:

1. Node mobility
2. Wireless propagation.
3. Lack of centralized control
4. Minimum hop count (shortest path first)

Besides these objectives several other factors need to be concentrated.

Generally in order to select the best path from the available we need to have certain measure. This task can be done considering both the network and system measures. These are done by the routing algorithm. The main objectives of a routing algorithm are:

- Minimise delay
- Maximize probability of data delivery
- Maximize path throughput
- Maximize network throughput
- Minimise energy consumption
- Equally distribute the traffic load
  Also the link and path metrics need to be calculate this can be done using certain mathematical function on the available values.

Besides gathering several factors to compute the metric it considers the

- Locally available information of the nodes
- Passive monitoring
- Active probing
- Piggyback probing

There are several types of routing metrics available for the wireless mesh networks [2] they can be broadly categorised under four groups namely:

1. Topology based metrics
2. Signal strength based
3. Active probing based
4. Energy based

The **topology based metric** is popular due to its simplicity. It takes into account no of hops, connectivity information etc. This has several drawbacks since it doesn't consider any additional active or passive requirements. EX: Hop count

The **signal strength based** as such concentrates on the strength of the signal although its data transfer and follows attenuation where ever required.

The **active probing based metric**: With respect to the data loss incurred in signal based due to network links active probing based has evolved in. In this we use the probe packets which need to be similar to that of data packets to easily get connected across but shouldn't be prioritized or treated preferentially in the network. On the other hand, if the probing packets are interlaced with the regular traffic (so-called intrusive or in-band measurement), the probes themselves impudence the amount of traffic. These approaches have proved fine as they would analyse from direct measurements rather than inferring it from indirect measurements, and do not rely on analytical assumption. The basic start arouse with **Expected transmission count (ETX)** metric; then a whole family of metrics has emerged out which attempts optimizing routing performance under various assumptions for the link rates and the channel usage in the network.

5.2.1 ***Expected Transmission Count:*** ETX is the first routing metric introduces w.r.t. active probe based metric specifically designed for MANETs. The consideration of minimal hop count may not be proved to be the optimal solution all the times hence, De Couto proposed a metric which concentrates on the bi-directional loss ratios**[4].** ETX, as the name itself suggests it expects the no of transmissions (including retransmissions) during transmission of a packet over a link. Minimizing them optimizes throughput, minimizes the total energy consumed, the resulting interference in the network assuming constant power intervals.

$$ETX = \frac{1}{d_f.d_r}$$

$\boldsymbol{d_f}$ the expected forward delivery ratio and $\boldsymbol{d_r}$the reverse delivery ratio.

The main advantages of the ETX metric are it is independent from link load since it doesn't route through congested links there by its immune to self interference. The essential disadvantage of the ETX metric is the overhead injected in the network in the form of probe packets.

Several other routing metrics can be applied to a mesh environment. For all these the ETX metric acts like a base idea.

5.2.2 ***Expected Transmission Time (ETT) and Weighted Cumulative Expected Transmission Time (WCETT):*** Draves observed that ETX does not perform optimally under certain circumstances. For example, ETX generally prefers heavily congested links to unloaded links; in certain cases the link-layer loss rate of congested links is smaller compared to unloaded links. This was the motivation for proposing expected transmission time (ETT) **[9]** metric considering throughput into its calculation. If S is the size of the probing packet and B the measured capacity of a link, then the link ETT is defined as follows:

$$ETT = ETX * \frac{S}{B}$$

In general we assume the 802.11a/b/g to provide services for non overlapping channels, extending the existing ETT metric for multiple channels lead to cumulative ETT (WCETT). Let k be the total number of channels of a network; the sum of transmission times over all hops on channel j is defined as:

$$X_{j=} \sum_{i \text{ uses channel } j} ETT_i$$

$$1 \leq j \leq k$$

The total path throughput in general is dominated by the bottleneck channel, which has the largest Xj, thus considering use of weighted average between the maximum value and the sum of all ETTs results in the following formula for WCETT:

$$WCETT = (1-\beta) \sum_{i=1}^{n} ETT_i + \beta \max_{i \leq j \leq k} X_j$$

with 0 ≤β ≤ 1 being a tuneable parameter.

The main disadvantage of the WCETT **[9]** metric is that it is not immediately clear if there is an algorithm that can compute the path with the lowest weight in polynomial or less time.

5.2.3 ***EEC based routing metric:*** The expected effective capacity selects the optimal path taking into account the interference ratio **[9]** (both inter and intra flow) , dynamic traffic over the links aiming at maximum throughput and minimal delay.

5.2.4 ***SINR***: This is called the signal to noise plus the interference ratio metric. The main aim of it is to calculate the interference that indirectly affects the throughput considering various categories on interference like the self, co-channel, adjacent channel. Here an assumption of partially overlapped channels (POC) **[3]** or orthogonal channels are assumed to lessen the self interference ratio. Once the channel assignment is done based on all these assumptions then routing is performed to select the optimal path.

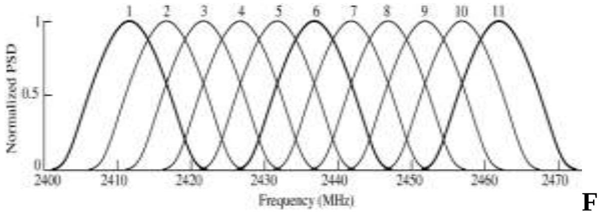

FIG:

5.2.4 Overlapping channels

The system model representation is visualized in the following fig:

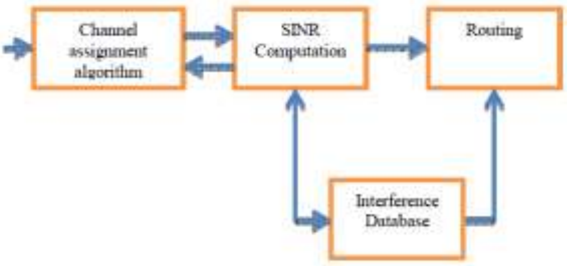

FIG : System model

*5.2.4.1.**Methodology of simulation using NS2:***

NS2 based simulation is used to simulate the Interference Aware Edge Coloring problem. The NS2 version NS2.33 and, the patch for multi-channel multi-radio is included. Diverse types of topologies like square, random were used in the simulation, and the comparison of the orthogonal channel inputs with POC inputs were observed. The area dimension for our simulation is within 1000m × 1000m flat grid topology. The physical distance between two nodes is 200m in square topology; the transmission range is 250m for all the nodes and the interference range is 550m. But, the random topology distance between two nodes can differ randomly. Each node is equipped with multiple radios and data transmission rate is 11Mbps. The thermal noise power is set to -90 dB; The Beta threshold is set to -16dB and the packet size is set to 1000bytes. Free space path loss model is used to predict signal strength. At -10 dB, network performance is optimal. The simulation was performed in 300s and the traffic types used in our simulation are Ftp and Cbr.

In the channel assignment algorithm network throughput and aggregate network capacity are calculated. Network throughput for a no of radio frequencies is calculated and an observation states that in interference aware edge colouring considering 11 channels has generated better throughput considering the spatial complexity. Hence from this observation we infer that throughput enhances with the no of channels and more radio frequencies. The dramatic increase in network capacity after 5 channels clearly states that POC increases overall network performance in wireless mesh networks.

For **simulation of SINR:** we assume a grid of 5*5 considering nearly 20 nodes, using the aodv protocol initially broadcast a RREQ, based upon the RREP analyse the optimal path for traversal. In case of any link breakages or node failures a RERR(Route Error) is generated at the point of breakage and traverses reverse to the source thus enhancing Route maintenance phase.

5.2.5MIL: Several routing metrics like ETX, ETT, WCETT, SINR and many more discuss the interference issue independently as interflow and intra flow. Here MIL talks about uniform description of both the interference and load **[7]** accordingly with the goal of attaining the minimum end-end delay.

Illustration of isotonicity: Assuming for any path a, its metric is defined by a metric function W(a) and the concatenation of two paths a and b is denoted by a + b, the metric function.

W (·) is isotonic if W(a) ≤ W (b) implies both W (a + c) ≤ W (b + c) and W(c ′+ a) ≤ W(c ′+ b), for all a, b, c, c ′ is shown in the following Fig :

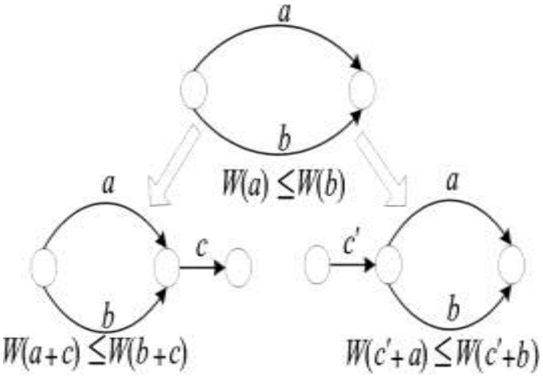

FIG: Isotonicity

MIL metric definition: Neigh boring links belonging to two different flows on a same channel cannot be active simultaneously and tis issue is called inter flow. The success or fail of a transmission is affected by the physical signal strength, therefore the equivalent bandwidth of link i under logical inter-flow interference and physical interference **[7]** can be calculated as follows:

$$B_{\text{Inter},i} = (1 - \text{CBT}_i) \times B_{\text{bas}} \times \text{IR}_i$$

Where B $_{\text{bas}}$ is the nominal link data rate and CBT $_i$ is the channel busy time, which denotes the utilization of channel used by link i. CBT $_i$ can be obtained from Equation:

$$\text{CBT}_i = \frac{\text{TotalTime} - \text{IdleTime}}{\text{TotalTime}}$$

Here Total Time refers the entire time duration where the channel is monitored and Idle Time refers to the time where no traffic occurred over the channel. Observation of CBT clearly describes the utilization value of a channel which is done through passive overhearing to avoid overhead onto the networks. CBT can measure logical interference more accurately than other measures.IR $_i$ is interference ratio, which is given in Equation:

$$\text{IR}_i = \frac{\text{SINR}_i}{\text{SNR}_i}$$

where SINR $_i$ is the signal-to-interference-plus-noise ratio and SNR $_i$ is the signal-to-noise ratio.

MIL routing metric for path p can be defined as

$$\text{MIL}(p) = \sum_{k \in p} \overline{L_k} \times \frac{S}{B_k}$$

where S is the packet size and $\overline{L_k}$ is the average load of link k. Route oscillation can be caused due to the dynamic load handoff whre the routing decisions oscillate. Say link k uses current sample load value L $_{k\text{ - cur}}$ and previous value L $_{k\text{ - pre}}$ to obtain average load $\overline{L_k}$ through exponential weighted moving average scheme

$$\overline{L_k} = (1 - \theta) \times L_{k-\text{cur}} + \theta \times L_{k-\text{pre}}$$

Where θ is the moving exponent.

Among the several available routing metrics the selection of a corresponding routing metric can be done based on the performance visualizations of the graphs produced over the network simulators like Ns2, NCTUNS etc.

SECURITY: Security is another major issue that requires attention during the period of data transfer. The attacks can be broadly classified as external and internal attacks **[3].** The malicious nodes are added in the path from the source to the destination. Once the malicious During a wormhole attack (shown in the fig below), two or more malicious nodes collude together by establishing a tunnel using an efficient communication medium (i.e., wired connection or high-speed wireless connection etc.).

A *black hole* attack (or *sinkhole* attack) is another attack that leads to denial of service in WMNs. It also exploits the route discovery mechanism of on-demand routing protocols. In a black hole attack **[8],** the malicious node always replies positively to a RREQ, although it may not have a valid route to the destination. Because the malicious node does not check its routing entries, it will always be the first to reply to the RREQ message. Therefore, almost all the traffic within the neighbourhood of the malicious node will be directed towards the malicious node, which may drop all the packets, causing a denial of service. The below fig. shows the effect of a black hole attack in the neighbourhood of the malicious node where the traffic is directed towards the malicious node. A more complex form of the attack is the cooperative black hole attack where multiple nodes collude together, resulting in complete disruption of routing and packet forwarding functionality of the network. Ramaswamy et al. have proposed a scheme for prevention of cooperative black hole attack in which multiple black hole nodes cooperate to launch a packet dropping attack in a wireless ad hoc network.

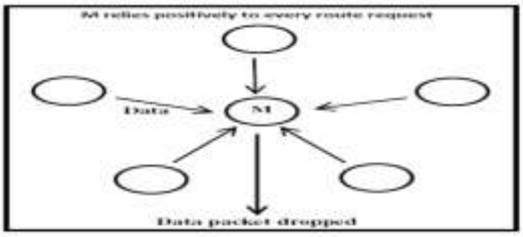

FIG Black hole Attack

A gray hole attack is a variant of the black hole attack. In a black hole attack, the malicious node drops all the traffic that it is supposed to forward. This may lead to possible detection of the malicious node. In a gray hole attack **[8],** the adversary avoids the detection by dropping the packets selectively. A gray hole does not lead to complete denial of service, but it may go undetected for a longer duration of time. This is because the malicious packet dropping may be considered congestion in the network, which also leads to selective packet loss.

To overcome the adverse effects of this attacks the avoidance is followed to overcome great loss. Also several security based routing protocols **[6]** are applied like security based AODV (SAODV), Secured routing protocol (SRP), Secured link state routing protocol (SLSP) are followed.

VI. Conclusion

This paper discusses the evolution of WMNs, motivation, concentrating on balancing of end to end delay and security which are the two major issues using the working environment of NCTUNS with the application of AODV protocol choosing an appropriate active probe based routing metric. An additional characteristic of security can be added through secured routing protocols.

VII. Future Enhancements

The same analysis can be applied on a different simulator upon usage of other routing metrics like topology base, mobility based or energy aware. Also the protocol application may differ like DSR, DSDV etc. A new routing metric can be proposed considering the drawbacks in environments of the existing ones by assumption values in simulation. Also here we have proposed a methodology of representation considering assumption orthogonal channels due to low levels of inter flow and intra flow interferences. The same can be enhanced to the partially overlapped channels (POC) **[2]** which is a complex issue.

REFERENCES

[1] Wireless mesh networks: a survey Ian F. Akyildiz a, Xudong Wang b,*, Weilin Wang b Available online 1January 2005 Computer Networks 47 (2005) 445–487

[2] An Efficient Interference Aware Partially Overlapping Channel Assignment and Routing in Wireless Mesh Networks International Journal of Communication Networks and Information Security (IJCNIS) Vol. 6, No. 1, April 2014 Sarasvathi V1, N.Ch.S.N.Iyengar2 and Snehanshu Saha3

[3] Security Issues in Wireless Mesh Networks Muhammad Shoaib Siddiqui, Choong Seon Hong 2007 International Conference on Multimedia and Ubiquitous Engineering(MUE'07) 0-7695-2777-9/07 $20.00 © 2007

[4] An Efficient Traffic-Load and Link-Interference Aware Routing Metric for Multi Radio Multi Channel Wireless Mesh Networks Based on Link's Effective Capacity Estimation Maheen Islam1, M. Lutfar Rahman2 & Mamun-Or-Rashid3 Computer and Information Science; Vol. 7, No. 4; 2014 ISSN 1913-8989 E-ISSN 1913-8997 Published by Canadian Center of Science and Education

[5] Routing Protocols and Metrics used on Wireless Mesh Networks Edmundo Chissungo, Hanh Le, Edwin Blake Computer Science Department, University of Cape Town, Cape Town.

[6] An Efficient Interference Aware Partially Overlapping Channel Assignment and Routing in Wireless Mesh Networks by Sarasvathi V1, N.Ch.S.N.Iyengar2 and Snehanshu Saha3 International Journal of communication Networks and Information Security (IJCNIS) Vol. 6, No. 1, April 2014

[7] Uniform description of interference and load based routing metric for wireless mesh networks Jihong Wang , Wenxiao Shi , Yinlong Xu and Feng Jin. EURASIP Journal on Wireless Communications and Networking © Wang et al.; licensee Springer. 2014

[8] Security and Privacy Issues in Wireless Mesh Networks: A survey by JaydipSen http://arxiv.org/ftp/arxiv/papers/1302/1302.0939.pdf.

[9] ANALYSIS OF ROUTING PROTOCOLS IN WIRELESS MESH NETWORK IJCSIT, Vol. 1, Issue 3 (June 2014) e-ISSN: 1694-2329 1Sarina Garg, 2Dr. Dinesh Arora 1,2Gurukul Vidyapeeth Institute of Engg. & Technology, Banur, Punjab, India