CROSS-LAYER IDS FOR GRAYHOLE ATTACK IN WIRELESS MESH NETWORK

Project Report submitted in partial fulfillment of the requirement for the degree of

Master of Technology

in

Computer Science & Engineering

under the Supervision of

Dr. HEMRAJ SAINI

By

PRABHAT RANJAN(142202)

Jaypee University of Information Technology

Waknaghat, Solan – 173234, Himachal Pradesh

Certificate

This is to certify that project report entitled **"Cross-layer Intrusion Detection System for Grayhole Attack in Wireless Mesh Networks"**, submitted by **PRABHAT RANJAN** in partial fulfillment for the award of degree of Master of Technology in Computer Science & Engineering to Jaypee University of Information Technology, Waknaghat, Solan has been made under my supervision.

This report has not been submitted partially or fully to any other University or Institute for the award of this or any other degree or diploma.

Supervisor's Name - Dr.Hemraj Saini

Date:

Signature

Acknowledgement

I would like to take this opportunity to acknowledge all those who helped me during this report work. I would like to thank my Supervisor (**Dr.Hemraj Saini**) for his valuable suggestions and guidance during the report work.

Name of the student- Prabhat Ranjan

Date:

Signature

Table of Content

List of Figures

List of Tables

List of Acronyms

Acronym	Description
WMN	Wireless Mesh Network
IDS	Intrusion Detection System
DSR	Dynamic Source Routing
MAC	Media Access
DoS	Denial of Service
RREQ	Route Request
RREP	Route Reply
NS	Network Simulator

Abstract

Wireless Mesh Networks (WMN) is one of the promising technology in providing wireless internet connectivity.It contains clients and routers,where mesh routers have minimal mobility and form the backbone of WMN.They give access to network for previous clients as well as mesh.Mesh clients can be either stationary or mobile and can form a client mesh network among themselves and with mesh routers. WMN's are anticipated to resolve the limitations and to significantly improve the performance of other networks. Since it allows faster, easy and cheaper network deployment they are becoming a popular choice. WMN applications are in broadband home networking, community etc. Security is the important aspect in WMN. Due to its open medium, dynamic topology and lack of physical security they are vulnerable to various kinds of attacks and intrusions at different layers. Security in WMN is still its infancy as very little attention has been devoted so far and so it has become vulnerable to various types of attacks. Various DoS attacks have been described.DoS attacks can compromise the availability of wireless mesh networks as it would hinder nodes from accessing or providing specific services. Gray hole is one kind of routing disturbing attacks and can bring great damage to the network.Intrusion is something which is unwanted work hindering the functions of wireless network.Wireless network is very much prey to many threats at OSI layers due to mainly cooperation among their noses Intrusion detection is a passive defense strategy to inform administrator about attacks on the network. Cross layer IDS, to accommodate the combined characterstics of link with routing information in wireless mesh networks to detect attacks on multiple layers.We choose DSR protocol to test the algorithm by ns-2 as simulation tool. Using cross layer mechanism on Dynamic Source Routing (DSR) protocol we can detect Gray hole attack in the network.

CHAPTER 1

INTRODUCTION

Wireless Mesh Networks are self dependent systems. WMNs are easy to setup,cost effective, offer network elasticity and auto recovereable.It consists of Mesh Routers (MR) and Mesh Clients. Mesh Routers can relay data on behalf of other nodes, thus increasing communication range and bandwidth. In WMNs, each node is connected to many other nodes. If any node drops out of the network, due to some hardware problem or any other reason, its neighbors easily find another route. The principle is data will hop from one node to other until it reaches the destination. The characteristics of WMNs like the open medium, dynamic topology and lack of physical security make them extremely risky to many types of threats. As WMNs provide supportfor heterogeneous networks, there is no complete secure protocol.Securing WMNs is the most challenging task. Many attacks are possible at different layers of the network.

WMNs are more vulnerable especially in routing layer followed by MAC layer and Physical layer. Routing layer attacks are mainly of two types: control plane attacks and data plane attacks.Control plane attacks affect the route discovery and maintenance phases of reactive, proactive and hybrid routing protocols.Data plane attacks affect the actual data packets by dropping or modifying. Gray hole attack is one of the routing layer attack.Once it is in active route it will start data plane attack by dropping packets.Data plane attacks also called Denial of Service(DoS) attacks.DoS attacks resultsin massive service disrupton.

Intrusion Detection Systems (IDS) [6] are widely used in networks as a second line of defense to secure against attacks.Intrusion detection can be defined as the process of monitoring events happening in the network and assessing them for the signs of violation of security policies. These are of two types: single layer IDS and cross layer IDS. Single layer IDS functions based on information from a single layer whereas in cross layer IDS,behavioral information from two or more layers is used for detection.

The analysis show that Cross layer IDS is more effective than Single layer IDS.We used multi-layered approach to detect malicious nodes on DSR protocol with parameters like Packet Drop Ratio (PDR),hop-count and other routing flags.

CHAPTER 2

LITERATURE SURVEY

2.1 Motivating Factors:

Cross-layer design[2] emphasizes on the network performance optimization by enabling different layers of the communication stack to part state data or to manage their activities in order to jointly optimize network performance. It is our perception and mindset that if a new proposal paradigm is proposed, we compare it with the existing one. Therefore ,the notion of the comparison of cross layer design with the traditional layered architecture so that people can be inspired towards the practice of the defilement of the layered design. For example let us consider the cross-layer proposal for sensor networks and ad hoc network. The distributed infrastructure-less nature of ad hoc and sensor networks offers new challenges and chances for network inventors, like the distribution of network management across resource-limited nodes. To meet the exceptional and special experiments of wireless ad hoc and wireless sensor networks and to utilize the limited node properties capably and dependably this idea of cross-layer design is used. Researchers have proposed some new tactics and designs that indirectly violate the strict layered design, cutting across traditional layer boundaries.

Motivating factors for cross layer design are as follows:

1. *Power*: As medium access and routing decisions have large impact on power consumption taking both their consideration can give more efficient power consumption and can lead to improvement in battery life.

2. *Mobility*: As routing protocols have to deal with the mobile terminals by regularly adapting routing state to changing user position. It poses a challenge to battery powered nodes. Mobility creates changes for the physical layer(like interference levels),the data link layer(for link schedules),the routing layer(for new adjacent nodes) and the transport layer(e.g. connection-time outs).Cross layer approach increases the node capability to manage mobile environment resources.

3. *Wireless link parameters*: Vulnerability of wireless links is more as compared to wired links to interference variations and channel errors. Wireless links are also security attacks vulnerable because of their easy access to wireless channel as they are open in nature. If at higher layer wireless link status information is given, the nodes at physical layer can accommodate in a better way.

4.*New communication modalaties*:To progress performance of the networks can abuse the broadcast nature of the channel.Like in order to evaluate and estimate the quality links of neighbours ,nodes can sneak on neighboring transmissions. The cooperation among different layers like data link,routing and physical layer can ensure the data arrival at all connections within time.

5. *Inherent Layer Dependencies*: there exists a number of layered protocol stacks which leads to motivation of cross layer designs. Both data link layer and physical layer are closely related.The data link layer deals with error control and flow control while the physical layer deals with the channel state.If at physical layer, the change in channel state is provided to data link layer then it can adapt error control mechanisms in a adaptive way to improve throughput.

6. *Resource Constrained Nodes*: The size of mobile nodes are decreasing in size which results in smaller use of batteries for these nodes. At several layers, cross layer design approach can expose power related variables, enabling node to make use of energy resources and increase battery life of node.

7. *Security*: As wireless channel is open and are easily are approachable by an attacker .Security is very important to secure communication. Security is a priority concern in wireless networks due to greater vulnerability and exposure to many types of attacks. Unreliable links in wireless, increasingly changed network topology and lack of centralized system to handle needs of security lead to insecure systems in wireless systems. IDS placed on points like network gateways and wireless access points lead to security in the network. Every layer is vulnerable to attacks by adversary nodes in case of network protocol stack. At different layers independent security solutions might lead to conflicting actions and results decrease in performance. Hence, network reliability and security has to be jointly addressed in all the protocol layers. Physical layer authentication for the intruder detection with the cross layer can improve wireless network security.

2.2 WMN

With the advancement in technologies of wireless networks improved services are taking place, Wireless Mesh Networks[5] in one of the emerging technology.It has clients and routers. In it each node not only receives packets but also sends packets in the forward direction by routing them.In WMN,nodes creates and preserve connectivity among themselves.This causes many benefits in WMN such as cheaper,easy maintenance,adaptive and dependable service.Daily use devices like laptops,phones etc. can be attaches with the routers.So,WMN can connect with users any time.It has wide applications in broadband home networking, community and neighborhood networks,enterprise networking, building automation etc.It is wooing from Internet service providers to carriers as it needs less investment.WMNs are scalable as nodes may be upgraded and downgraded according to the need.Seeing the benefits of it many companies have started installing it.

Network Architecture

WMN has two kinds of nodes as routers and clients.Mesh router contains additional functions as compared to its previous versions of having routing capability.Elasticity can be extended by joining numerous wireless interfaces.Present day routers have less power transmission as compared to their previous counterparts because of multihop characterstics.

Having so much variability,both of them are made on alike hardware platform.Embedded system routers are shown in figure which are used for general purpose.

In mesh,clients which has capability to work as a router also.They have a single interface.Platform for clients is naiver in comparison to routers.From laptop,pocket PC to RFID reader they can be any devices,as shown in Fig.1

Fig.1 . Examples of mesh routers based on different embedded systems: (a) PowerPC and (b) Advanced Risc Machines(ARM).

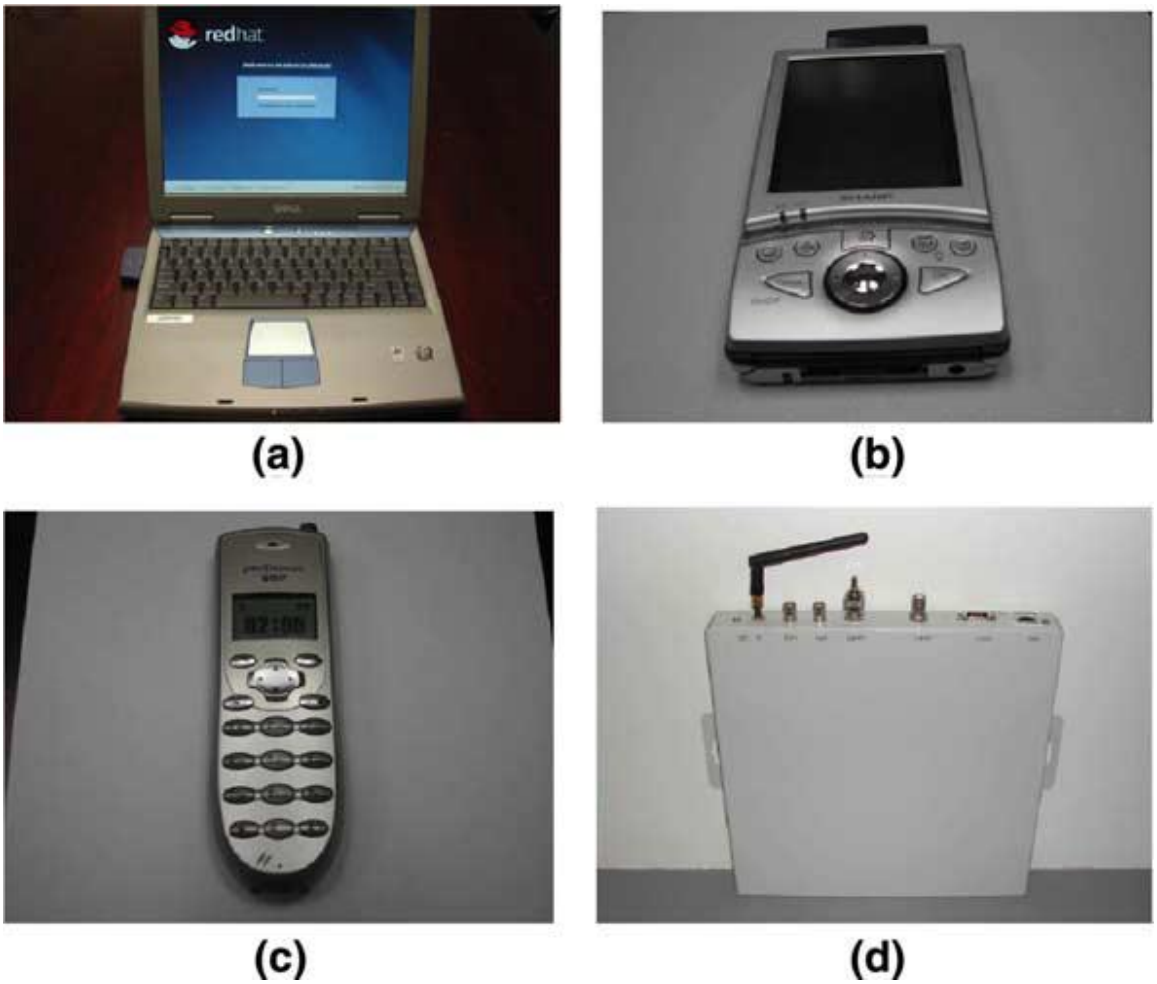


Fig.2 . Examples of mesh clients: (a) Laptop, (b) PDA, (c) Wi- Fi IP Phone and (d) Wi-Fi RFID Reader.

WMNs consist of three types of architectures according to their functions:

Infrastructure WMNs.WMN infrastructure can be developed using radio technology like IEEE 802.11.Routers along with gateways can connect to the internet.This method leads to meshing of infrastructure where there is combination of clients with present networks by gateways.Orthodox clients can be combined with routers to have interface each other.

Infrastructure/Backbone WMNs are used widely.Their applications are mostly used in community and neighbor networks.They are localized on terraces to help around streets.Interaction for backbone and user are the varieties of nodes used.Directional antennas can be used for long range directional antennas.

Client WMNs It provides peer to peer service.Clients does the actual routing along with configuration facilities and applications of end user.The architecture is shown in the figure. There is multi hopping among nodes to reach the destination.They are made by same type of radios shown in Fig.3

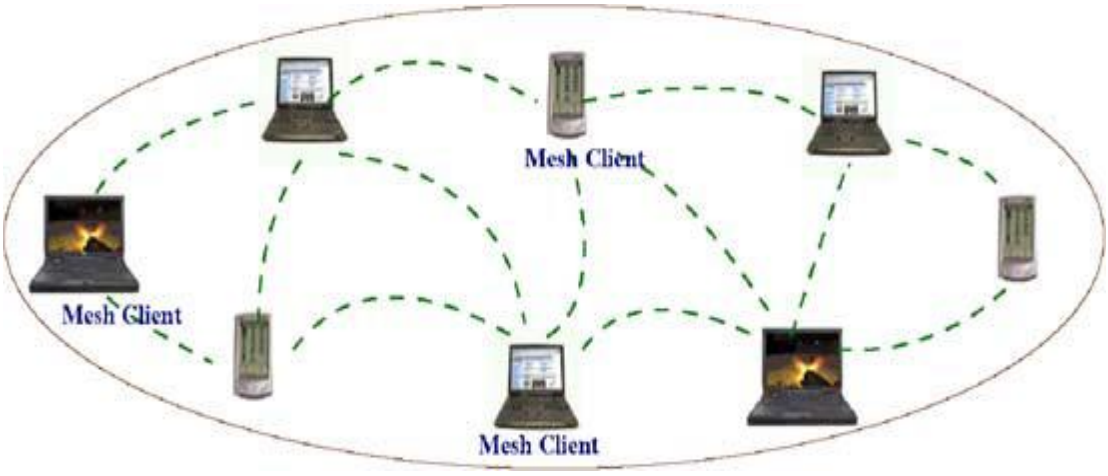


Fig.3 Client WMNs.

They have more functions like routing and self configuration.

Hybrid WMNs Infrastructure and clients are mixed in this type of architecture.Internet connectivity is given to the networks like cellular and sensor networks,the abilities like routing and networks can be improved. The hybrid architecture is shown in figure 4 below.

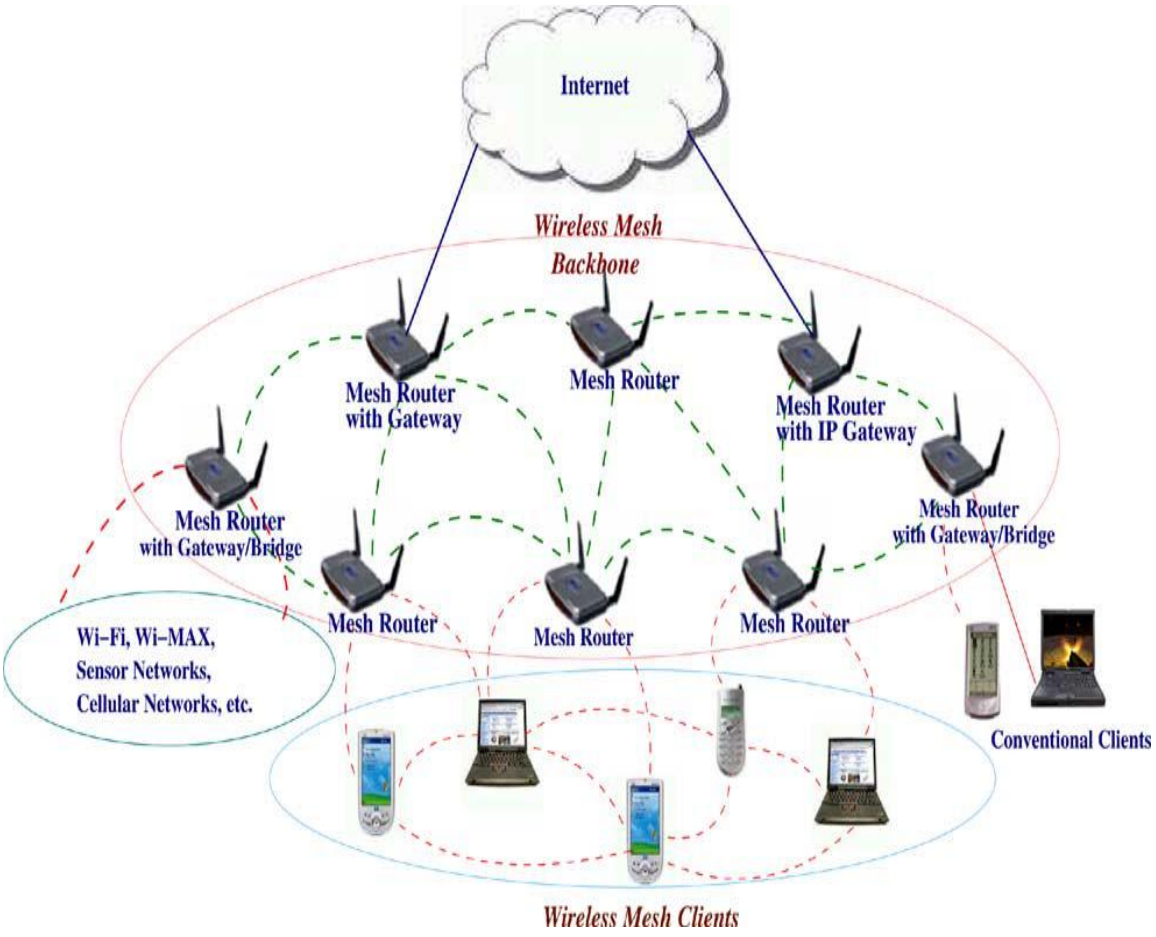


Fig.4. Hybrid WMNs.

Characteristics*:*

WMN properties are as below:

Multi-hop wireless network WMN needs to increase its area without changing any capacity of the channel.It also gives connectivity as non-line-of- sight without any links.The multi-hopping[8] in mesh is vital as throughput is reached not affecting node distances and frequency.

Self forming, self-healing and self organizing capability

It increases performances of the network because of its elastic architecture,easy installation and easy connectivity.These characterstics lead to less cost and high scalability of WMN.

Type of mesh nodes on mobility

Mesh clients are both stationary as well as mobile whereas mesh routers have less mobility.

Multiple types of network access

Both the backhaul and P2P(peer to peer) communication are sustained.With the WMN combination end user service can be given with the help of WMN.

Dependence of power-consumption constraints on the type of mesh nodes.

There is no restrictons on the power dissipation in routers.Whereas clients in mesh will be requiring capable protocols.e.g.mesh capable sensors.With power as the priority for sensor networks, so optimization of routing protocol is done.

Compatibility and interoperability with existing wireless networks. E.g. There must be suitability between the IEEE 802.11 and its standard for both previous Wi-Fi clients and mesh capability.These WMN's and Wireless networks should be in resonance with each other.

These properties lead to WMN as ad-hoc networks because of scarcity of wired set up by installing base stations.WMNs need extra skills like latest algorithms for the recognition.Due to its pros in WMN hybrid architecture is taken.

Wireless infrastructure/backbone. Routers are the strength of WMN.It gives wide coverage and association in the wireless domain.Due to the end users connectivity of ad hoc networks are less reliable.

Integration

With the same usability of radio technique of the routers WMN supports previous versions clients.Mesh routers contain the host routing function which does it.WMNs combines the networks like Wi-Fi,cellular,internet and sensors through gateways/bridge functions in the routers.By making use of wireless technology services in the inter networks can be used.The integration of networks and WMNs makes the backbone of internet,as location does not matter as compared to the capacity and topology of the network.

Dedicated routing and configuration. End user devices do routing and configuration functionalities in case of the ad hoc networks.Which leads to the low energy dissipation and more capabilities which in turns decreases the load on end users.The device value is decreased in WMN due to the end user limitations.

Multiple radios

Radios are contained in mesh routers which do routing and access functions.It differentiates two types of areas.Routing is done among routers ,network could be accessed on another radio.It leads to network ability increase.This leads to degradation in performance degradement in ad hoc networks where functions are at the same channel.

Mobility The topology of the network depend upon the users as routing is done using end user devices in the ad hoc network.It leads to further compications of the configurations of network.

Application scenarios:

Several uses of WMN illustrates its significance as compared to the other wireless networks like cellular networks ,WSN,ad hoc networks etc. Some of the applications are as below:

Broadband home networking.

It is done by IEEE 802.11 WLANs.One of the main difficulty is the access point location.Site survey of home is needed without which there are many dead zones in the coverage area. Site based survey and and many access points installation is costly because of wired architecture.Also,the node interaction must be checked by the hub.It is not a good solution for broadband networking.Mesh network for home networking is shown in Fig.5.Mesh router take the place of access points with connectivity done between them.

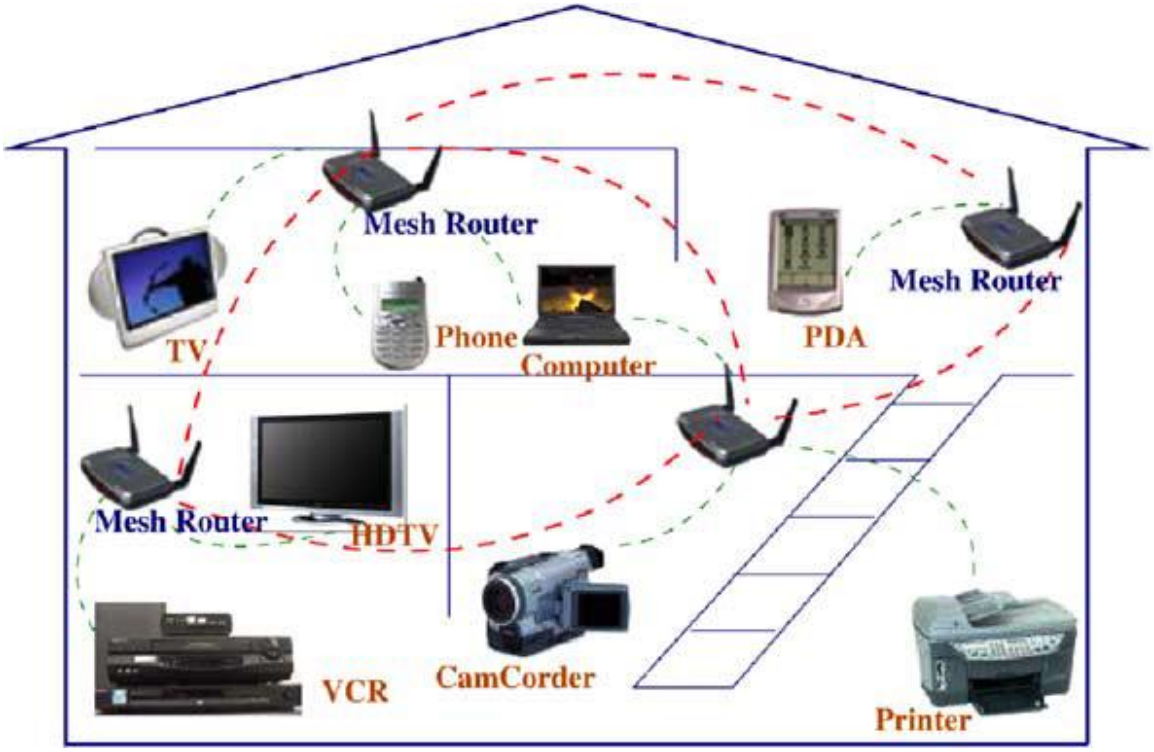


Fig.5. WMNs for broadband home networking.

Therefore,communication is more elastic and robust to errors. Dead zones can be removed by adding mesh routers, changing locations of routers, or themselves regulating power intensities of mesh routers. Home networking communication is done through hub everytime.Therefore,backhaul access can help in avoidance of network traffic.There is no limit

of power and mobility on wireless mesh routers.Therefore,ad hoc networks and wireless sensor networks are very difficult to achieve.Ad-hoc networking of multihop is not supported by Wi-Fi's.Broadband networks are well suited for WMN.WMNs fits in broadband home networking.

Community and neighborhood networking

The public architecture of network is based on the DSL linked internet and it has many limitations as below.

-Data going through internet is shared among the communities and the network,which in turn reduce the congestion.

-no service for the big range of wireless application.

– a costly need not to be given among network and wireless services need to be installed. Therefore,cost of the service may increase.

– Only one path is accessible for home through Internet or communicate with neighbors.

WMNs mitigate the above drawbacks via mesh connections which are flexible between homes, as shown in Fig.6. WMNs can also enable many uses like file access and storage which are distrbuted, and video streaming.

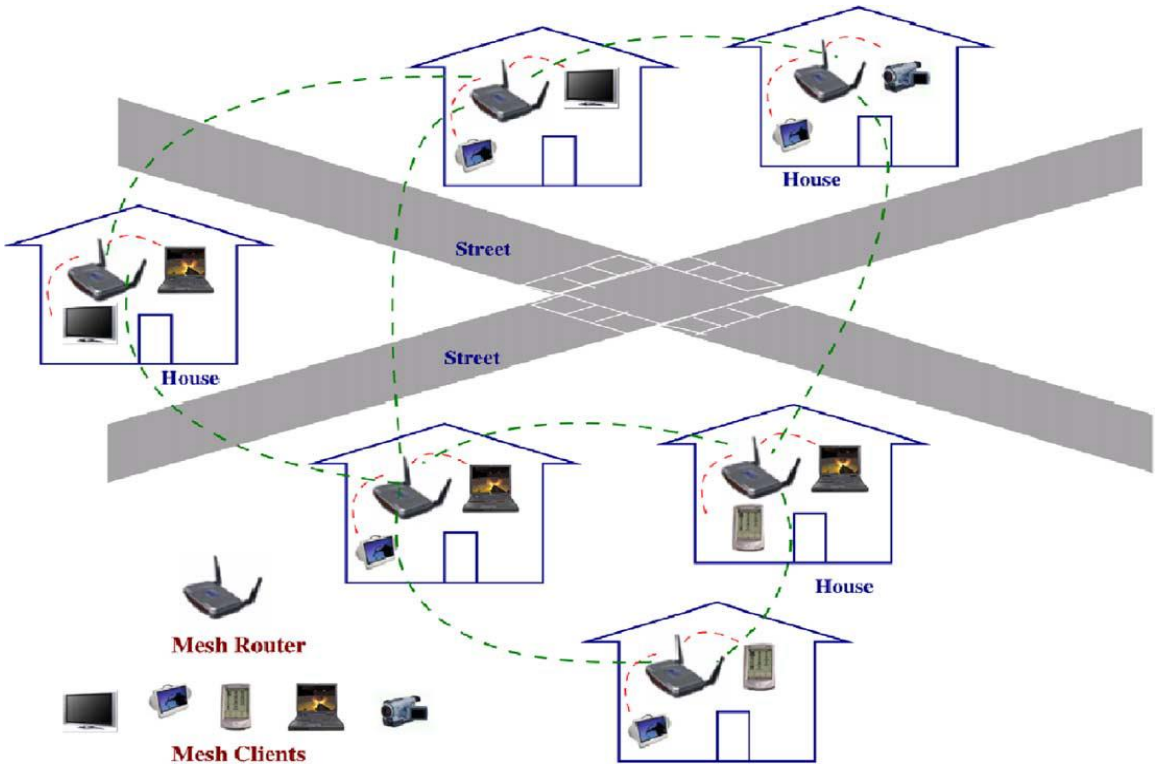


Fig.6 . WMNs for community networking.

Enterprise networking. It is tiny network lying in office or within the network for all offices in an entire building, or a large number of workplaces in multiple constructions. Presently, standard IEEE 802.11 wireless networks are widely used in many workplaces. Though, these wireless nets are still lonely landmasses. Connections among them have to be achieved via wired Ethernet networks, which is the main cause for the high cost of enterprise networks. In addition, adding more backhaul contact modems scale up volume, but does not improve robustness to link failures, network crowding and other difficulties of the network. If the access points are substituted by routers, as displayed in Fig. 8, Ethernet wires can be eradicated. Multiple backhaul access modems can be pooled by every nodes of network, and thus, increase the strength and consumption of the resource of enterprise systems. WMNs can develop simply as the size of network increases. WMNs networking are much more problematical than at home because more nodes and more difficult arrangements of the network are involved. The service model of enterprise networking can be applied to many other public and marketable facility interacting situations such as airports, hotels etc. an option to broadband networking, in developing areas. Wireless mesh MAN shields a huge area than community networks, as shown Fig. Thus, the requisite on the network dimensionability via wireless mesh MAN is much higher than that by other applications.

Metropolitan area networks. Have many benefits. The transmission rate in physical layer is much greater than that of any cellular links. Also,interaction among WMN is not based on a wired backbone. Compared to wired networks, e.g., optical or cable are cost-effective

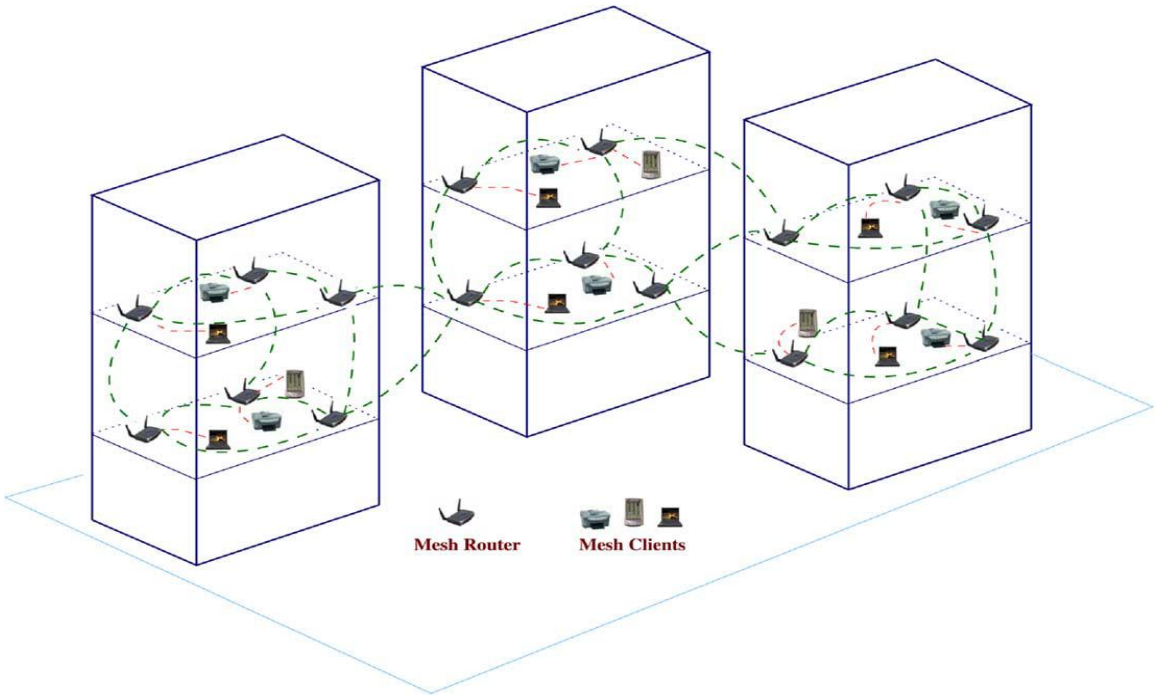


Fig.7. WMNs for enterprise networking.

alternative to broadband networking, especially in underdeveloped area. MAN shields a much larger area compared to home, enterprise, building, or community networks, as depicted in Fig. 7. Thus, the requisite on the linkage scalability by wireless mesh MAN is much higher than that by other applications.

Transportation systems. As an alternative of restraining IEEE 802.11 or 802.16 access to stations and stops, mesh networking evolution can spread access into trams, railways etc. Thus, convenient passenger information services, remote checking of in-vehicle interactions can be supported. To enable such mesh networking for a transportation arrangement, two main practices are required: the high-speed mobile backhaul from a vehicle (car, bus, or train) to the Internet and mobile mesh systems inside the automobile, as displayed in Fig.

Building automation. In a building, various circuits need to be measured and monitored. Currently this job is done via regular networks, as is very expensive due to the complexity in deployment and care of a wired system. Presently Wi-Fi based networks have been accepted to reduce the cost of such networks. However, this exertion has not realized suitable job yet, because installment of Wi-Fis for this use is still rather costly as of wiring of Ethernet. If building automation and regulator systems contact sockets are swapped by mesh routers, as

shown in Fig.8, the deployment cost will be considerably condensed. The installment method is also much naiver as of the connectivity among routers.

Health and medical systems. In a clinic diagnosis of data

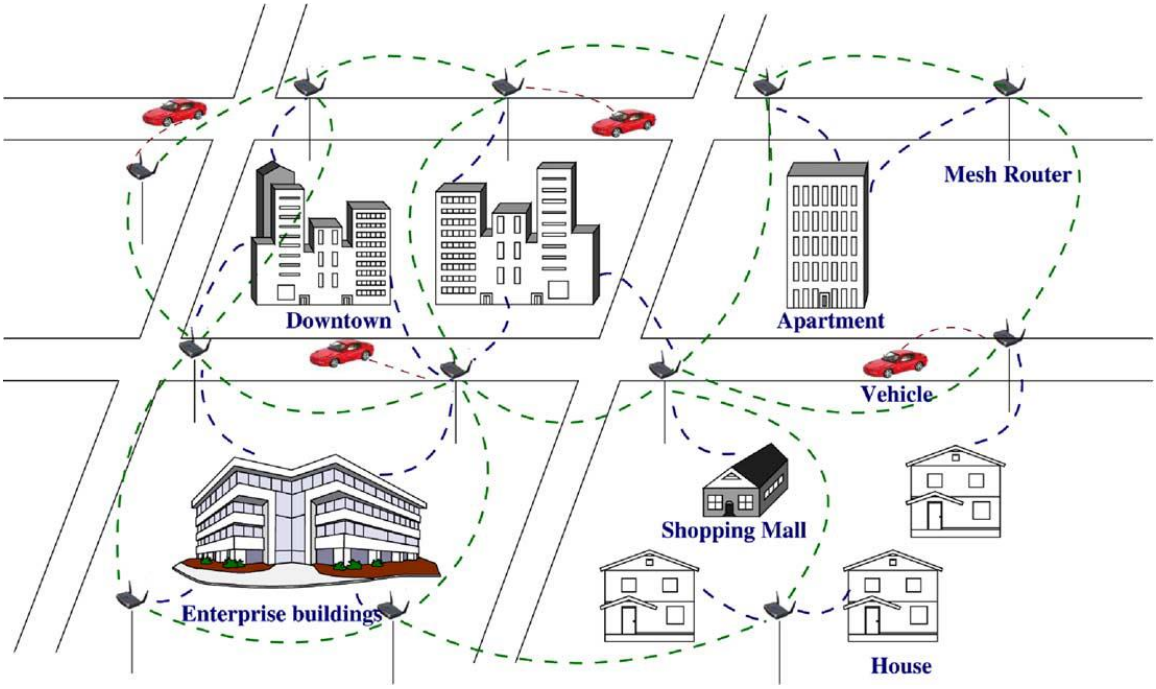


Fig.8. WMNs for metropolitan area networks.

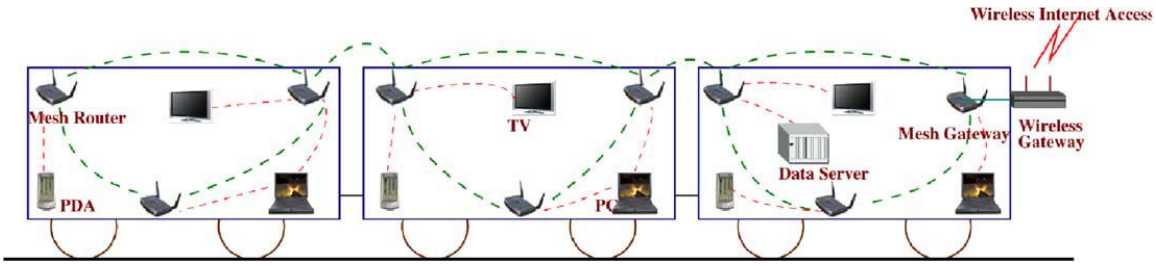


Fig.9. WMNs for transportation systems.

need to be managed and transferred from one point to another for several purposes. Data transmission is usually broadband, as of high quality images and many continuous monitoring information can easily produce a constant and huge quantity of information. Old wired networks can only offer restricted access of network to certain fixed medical appliances. Wi-Fi based systems must depend on on the presence of Ethernet connections, which may cause high system cost and ambiguity but without the skills to remove deficiencies. However, these issues do not exist in WMNs.

Security surveillance systems. Security is becoming a topic of high concern, security surveillance systems become a wide application. In order to deploy such structures at places as necessary, WMNs are a much more practicable answer than wired networks to connect all devices. Since still images and videos are the main traffic rolling in the system, this application demands much higher network capacity than other uses.

WMNs can also be applied to Spontaneous

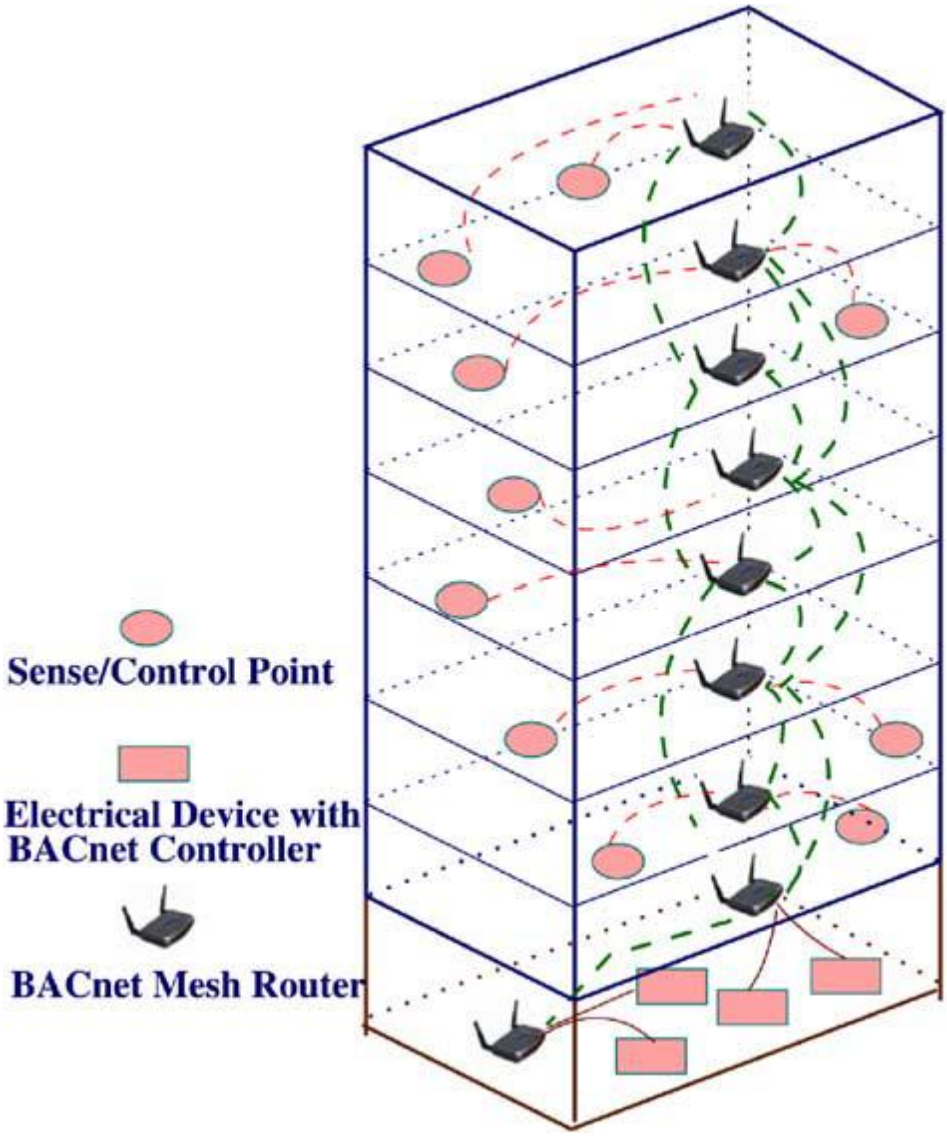


Fig. 10. WMNs for building automation.

Networking and P2P Communications. Like wireless system for an emergency response team and firefighters do not have sophistication of where the network should be installed. By simply placing wireless mesh routers in desired locations, a WMN can be rapidly proven. For a group of

people holding devices with wireless networking capability, e.g., computers, P2P communication anytime anywhere is a resourceful answer for data sharing. WMNs are able to see this mandate. These claims exemplify that WMNs are a superset of ad hoc networks, and thus can achieve all purposes delivered via ad hoc networking.

Serious issues inducing system performance

Before a network is designed, deployed, and operated, factors that seriously impact its act need to be measured. For WMNs, the critical factors are summarized as follows:

• *Radio methods* Compelled by the quick growth of semiconductor, RF technologies, and communication theory, wireless radios have experienced a major insurrection. Currently many approaches have been proposed to increase capacity and flexibility of wireless methods. Characteristic cases contain directional and smart antennas, MIMO systems,and multi-radio/multi-channel organizations .To this time, MIMO has become one of the important expertise for IEEE 802.11n, the high speed extension of Wi-Fi. Multi-radio chipsets and their expansion podiums are accessible on the marketplace.To further improve the performance of a wireless radio and control by upper layer procedures,new advanced radio technologies such as reconfigurable radios, frequency agile/cognitive radios, and even software radios have been secondhand in wireless communication.Although these radio technologies are starting in their beginning, they are predictable to be the future platform for wireless networks due to their capability of vigorously supervising the radios.These advanced wireless radio technologies all require a revolutionary design in upper layer protocols, mainly routing protocols. For example, when directional antennas are applied to IEEE 802.11 nets, a routing procedure desires to take into account the selection of directional antenna sectors. Directional aerials can decrease show nodes, but they also generate more hidden nodes. Thus, MACprotocols need to be re-designed to determine this matter. As for MIMO systems, new MAC protocols are also necessary. When software radios are considered, much more dominant MAC protocols, like programmable MAC, need to be developed. • Scalability. Multi-hop communication is public in WMNs. For many hop networking, it is well known that communication protocols suffer from scalability problems, i.e., when the magnitude of system rises, the system performance degrades significantly. Routing protocols may unable to discover a dependable routing path, transport protocols may loose connections, and MAC protocols may experience substantial througput fall. As a characteristic example, current IEEE 802.11 MAC protocol and its derivatives cannot achieve a practical

throughput as the number of hops upsurges to4 or higher (for 802.11b, the TCP throughput WMNs for building automation. The reason for low scalability is that the end-to-end reliability sharply descents as the size of the system increases. In WMNs, due to its ad hoc architecture, the centralized multiple access systems such as TDMA and CDMA are tough to implement due to their complexities and a general requirement on timing management for TDMA (and code management for CDMA). When a distributed multi-hop network is considered, accurate timing synchronization within the global system is hard to realize. Thus, distributed multiple access schemes such as CSMA/ CA are more promising. However, it has very low frequency spatial-reuse efficiency, which significantly restricts the size of CSMA/CA-based multi-hop networks. To improve the scalability of WMNs, designing a hybrid multiple contact order with CSMA/CA and TDMA or CDMA is an interesting and challenging research issue. • Mesh connectivity. Many advantages of WMNs originate from mesh connectivity which is a serious necessity on protocol plan, especially for MAC and routing protocols. Network self organization and topology control procedures are normally wanted. Topology-aware MAC and routing protocols can significantly improve the performance of WMNs.

• *Broadband and QoS*. Dissimilar from other ad hoc systems, most applications of WMNs are broadband services with various QoS necessities. Thus, in adding to point-to-point transmission delay and fairness, more performance metrics like as delay jitter, collective and per node output, and packet loss ratios, must be considered by communication protocols.

• *Adjustaibility and inter-operability*. It is a desired feature for WMNs to support network access for both orthodox and mesh clients. So, WMNs want to be backward compatible with conventional client nodes; otherwise, the incentive of installing WMNs will be ominously conceded. Integration of WMNs with other wireless networks requires some mesh routers to have the skill of interoperation between mixed wireless networks.

• *Security*. Without a convincing security solution,

WMNs will not be able to succeed due to lack of incentives by customers to subscribe to dependable services. Although several safety arrangements have been proposed for wireless LANs, they are still not ready for networks. For example, there is no central reliable authority to distribute a public key in a WMN due to the distributed system architecture. The existing security schemes proposed for ad hoc networks can be adopted for WMNs, but several matters exist:

– Utmost security way out for ad hoc systems are still not settled enough to be practically implemented.

– The network construction of WMNs is different from a orthodox ad hoc network, which causes differences in security mechanisms. As a significance, new security arrangements stretching from encryption algorithms to security key distribution, secure MAC and routing procedures,intrusion illuminating, and security monitoring need to be developed.

• *Ease of use*. Protocols must be designed to permit the system to be as self-directed as probable, in the sense of power management, selforganization, dynamic topology device, strong to short-term link disaster, and fast network subscription user-authentication procedure. In totaling, network managing tools must be established to efficiently maintain the operation, monitor the performance, and arrange the factors of WMNs. These tools together with the autonomous mechanisms in protocols will enable rapid deployment of WMNs.

Capacity of WMNs

The capability[1] of WMNs is hindered by many issues such as network architecture, network topology, traffic form, system node density, quantity of channels used for each node, transmission power level, and node mobility. A strong thought of the connection between network capacity and the above factors provides a guideline for procedure growth, architecture design, installment and task of the system.

Capacity analysis

In the last period, much study has been carried out to study the ability of ad hoc systems which can be adopted to examine the capacity of WMNs.

For a immobile multi-hop network, it has been shown that the finest transmission power level of a node is extended when the node consist of six adjacent nodes . With this value, an optimum tradeoff is achieved between the amount of hops from source to endpoint and the channel spatial-reuse efficiency. This result is useful for infrastructure WMNs with marginal movement. When the movement is a concern as in hybrid WMNs, no theoretical results are reported so far. Some investigational trainings have been achieved in , where the simulation results of a stationary network validate the theoretical results of.

Analytical lower and upper bounds of network capacity are given in. From the analytical results, it tails that the data capacity per node shrinks significantly when the node density increases. An

important implication is derived in as a guideline to improve the capacity of ad hoc networks: A node should only communicate with adjoining nodes. To appliancte this idea, two chief arrangements are suggested in:

• Throughput capacity can be increased by using relaying nodes.

• Nodes need to be congregated into groups.

Therefore, interactions of a node with a different node that is not adjacent must be shown through relaying nodes or clusters. However, these schemes have limitations. In the first arrangement, a very large amount of transmitting nodes are wanted in order to increase the throughput by a significant percentage. This will certainly upsurge the overall cost of a network. In the second scheme, clustering nodes in ad hoc systems or WMNs is not a favored method, because it is difficult to manage clusters in a distributed system. But, this inference has driven other research work such as ,where a hybrid network architecture is considered to recover the size of ad hoc systems. In the hybrid architecture, nodes only communicate with nearby nodes. If they want to connect with nodes with many hops away, base stations or access points are used to relay packets via wired systems.The hybrid construction can advance capacity of ad hoc networks, however, it may still not be favored by many claims because wired networks among base stations do not exist in many ad hoc networks.The implication given in can also be reflected in . The scheme proposed in increases the network capacity of ad hoc networks by using the node movement. When a node wants to send packets to other node, it will not direct until the destination node is near to the source node. So, through the node mobility, a node only interconnects with its adjacent nodes. This arrangement has a restriction: The broadcast delay may become large and the requisite buffer for a node may be endless. The analytical approach in has significantly driven the progress in capacity research of ad hoc systems. But, it contains limits. The networking protocols have not been fully captured by the examination. Like, power control devices, commonly used to advance the network capacity, is not considered in the examination. As another sample, the features of ad hoc routing procedures have not been totally taken in the inspection. In any routing procedure, the route for packages does not essential trail the path along the straight-line section between the source and destination as given in the study, because the routing protocol determines a path agreeing to certain parameters like as the number of hop counts, link quality, etc.

As a result, the applicability of the hypothetical results on real-world network designs still leftovers vague. A near equal between the theoretical results in and IEEE 802.11 based ad hoc networks is reported in. Though, this learning trust on the statement that the traffic design in a large ad hoc system tends to be local and thus, nodes usually communicate with nearby

This assumption is invalid in a network except it is purposely designed so. Most of the existing analytical approaches are based on asymptotic study. The upper or lower bulk limits derived from these approaches do not reveal the strict size of an ad hoc system with a given number of nodes, in particular when the number is small. Recently, an analytical approach is proposed in to study the exact capacity of WMNs. The analysis is simplified by taking benefit of the low mobility feature of WMNs. However, the analytical model in contains three assumptions that are not necessarily valid.

• The traffic in all nodes is sent to a single gateway which is not the case in WMNs.

• Each node accepts an equal part of the bandwidth to attain justice. However, this supposition is invalid if the system nodes have dissimilar spaces between them.

• The unidirectional traffic case is mentioned to be easily extendable to the bidirectional transportation case. However, the system capacity becomes totally diverse if bidirectional traffic is considered.

• The network construction measured is actually unmoving an ad hoc network. Furthermore, only a specific MAC protocol very like to CSMA/ CA with RTS/CTS is considered. However, CSMA/CA is not the only MAC solution for mesh networks. For example, the IEEE 802.11e or a TDMA MAC can attain higher throughput than CSMA/CA, because of the existence of contention free periods (CFP).

Open research issues

Several study matters still occur in the capacity analysis of WMNs for several reasons:

1. The theoretical results on the size of each ad hoc systems or WMNs are still based on some simplified assumptions, as explained before. The origin of fresh consequences by seeing serious issues such as transmission power levels, traffic patterns, optimal routing path, etc., is still a puzzling investigation issue.

2. Despite much research progress has been made in network size examination of ad hoc systems, WMNs have not been fully explored due to the differences between WMNs and ad hoc systems. The investigation consequences about system capacity and optimum node density of ad

hoc networks may not directly be applicable to WMNs. For example, in, the network architecture in the analysis does not match that of WMNs, because both stationary and mobile ad hoc nodes exist in WMNs.

3. Important techniques of increasing capacity of WMNs have not been measured in the logical prototypes for ad hoc networks. For example, multi-channels per radio or multi-radios per node will be functional in WMNs. Then, a serious query that arises is: what is the optimum number of channels or radios for each network node. Although the analytical model in allows multi-channels in a node, it does not contain a scheme to find the optimum number of channels. When other advanced techniques such as directional antennas, multi-input multi-output (MIMO) systems, are considered, new analytical models are required.

Physical layer

This type of practice spread reckless as circuit design for wireless communications evolve. Present wireless radios are able to upkeep multiple transmission rates by a combination of different modulation and coding amounts. Through these modes, adaptive error resilience can be delivered through link adaptation. It should be noted that below a frequency selective fading atmosphere, a connection adaptation algorithm cannot take signal-to-noise ratio or carrier-to-interference ratio as a solitary input from the physical layer, because SNR or CIR alone does not sufficiently define the passage feature.

In order to increase the capacity of wireless networks, various high-speed physical methods have been created. For instance, orthogonal frequency multiple access (OFDM) has significantly increased the speed. A much advanced broadcast rate can be achieved through ultra-wide band (UWB) techniques. Yet, UWB is solitary valid to short-distance presentations such as wireless personal area networks (WPANs). If a broadcast as high as that of UWB is desired in a wider area network such as WLANs or WMANs, new physical layer techniques are needed.Issues in the physical layer are twofold. First, it is necessary to further improve the transmission rate and the show of physical layer methods. Recent wideband broadcast arrangements other than OFDM or UWB are needed in demand to attain difficult transmission rate in a wide network area. Multiple-antenna systems have been researched for long time. Yet, their difficulty and charge are still too great to be widely accepted for WMNs. An example of low-cost directional antenna implementation is reported in. Frequency agile techniques are still in the early phase. Many challenging matters need to be determined afore they can be recognized for commercial use

MAC layer

The protocols of MAC have the following variations as compared to classical counterparts for wireless networks:

• MAC for WMNs is apprehensive with atleast one hop interaction. Classical MAC protocols are limited to one-hop communication whereas the routing procedure takes precaution of multihop communication. This assumption makes protocol design easier, since MAC and routing are apparent to each other. Though, this method does not work well in WMNs, because data transmission and response at a node is not only impacted by nodes within one hop but within two or more hops away. The hidden node concern in a multi-hop wireless LAN is such an instance.

• MAC is distributed and cooperative and works for multipoint-to-multipoint interaction. In WMNs, no centralized supervisor is vacant. The MAC function is accomplished in a distributed way, i.e., the MAC procedure need to guarantee all nodes to collaborate in broadcast. In addition, any network node with mesh networking capability is able to connect all its adjacent mesh nodes. Therefore, multipoint-to-multipoint communications can be established between these nodes.

• Network self-organization is desired for the MAC. MAC protocol should have the knowledge about network structure which can help better cooperation between neighboring nodes and nodes in multi-hop distances. This can considerably progress the MAC act in a multi-hop environment. In some circumstances, network self-organization based on power control can optimize network topology, minimize the interference between neighboring nodes, and thus, improve the network capacity.

• Mobility affects the MAC performance. Mobility dynamically changes network configuration, and thus, may considerably influence the performance of the MAC protocol. In order to be adaptive to mobility or even to use the motion, the network nodes need to interchange network topology information.

Network layer

WMNs will be closely combined with the Internet, and IP has been accepted as a network layer protocol for many wireless systems comprising WMNs. However, routing protocols for WMNs are different from those in wired networks and cellular networks.

Based on the performance of the existing routing protocols for ad hoc systems and the precise necessities of WMNs, we believe that an optimal routing protocol for WMNs must capture the resulting structures:

• *Performance parameters.* Many current routing protocols use minimum hop-count as a performance parameter to choose the route. This has been verified not to be valid in many situations. Suppose a link on the minimum hop count track amid two nodes has bad value. If the minimum hop count is used as the performance metric, then the throughput between these two nodes will be very low. To solve this problem, throughput parameters related to link quality are needed. If congestion occurs, then the minimum-hop count will not be an accurate performance metric either. Usually Round trip time (RTT) is used as an additional performance metric. The bottom-line is that a routing path must be selected by considering multiple performance metrics.

• *Fault tolerance with link failures*. One of the objectives to deploy WMNs is to ensure robustness in link failures. If a link breaks, the routing protocol should be able to quickly select another path to avoid service disruption.

• *Load balancing*. One of the objectives of WMNs is to share the network resources among many users. When a part of a WMN experiences congestion, new traffic flows should not be routed through that part. Performance metrics such as RTT help to attain load balancing, but are not continually operative, because RTT may be impacted by link quality.

• *Scalability*. Installing up a routing path in a very bulky network may take a long time, and the end-to-end delay can become big. Also, even when the path is recognized, the node states on the path may change. Thus, the scalability of a routing protocol is critical in WMNs.

• *Adaptive Support of Both Mesh Routers and Clients*. Considering the minimal mobility. Built on the show of the current routing procedures for ad hoc networks and the specific necessities of WMNs, there is an optimal routing protocol for WMNs must capture the following types:

• *Throughput metrics*. Many current routing rules use minimum hop-count as a performance metric to select the routing path. This has been established be in valid in many situations. Suppose a link on the minimum hopcount track amid two nodes has bad value. If the minimum hop count is used as the performance metric, then the throughput amid these two knots will be very little. To resolve this difficulty, performance parameters linked to link quality are wanted. If overcrowding happens, then the minimum-hop count will not be an precise presentation paramter either. Usually Round trip time is used as an extra presentation metric. The main point is that a routing track must be selected by considering multiple performance parameters.

• *Error tolerance with link disasters.* One of the purposes to deploy WMNs is to safeguard robustness in link letdowns. If a link disrupts, the routing procedure must be able to quickly select another track to dodge service disturbance.

• *Load balancing*. One of the aims of WMNs is to part the network resources amid several consumers. When a part of a WMN involves overcrowding, new traffic flows must not be routed through that part. Performance parameters like RTT help to realize load balancing, but are not always effective, because RTT may be impacted by link excellence.

• *Scalability*. Setting up a routing track in a very large wireless network may take a long time, and the node-to-node postponement can become big. Also, even when the path is established, the node states on the path may alterate. Thus, the scalability of a routing procedure is serious in WMNs.

In hierarchical routing, a certain self-organization scheme is employed to collection network nodes into groups. Each band has one or more cluster heads. Nodes in a cluster can be one or more hops far from the cluster head. As connectivity between clusters are needed, some nodes can communicate with at least a cluster and task as a gateway. Routing within a cluster and routing between

clusters may use different mechanisms. For example, within-cluster routing can be a proactive protocol, while intra-cluster routing can be on request. When the node thickness is great, hierarchical routing protocols tend to achieve much better performance because of less overhead, smaller average routing path, and quicker set-up procedure of routing path. However, the complexity of preserving the hierarchy may negotiatiate the throughput of the routing protocol. In WMNs, hierarchical routing actually may face the execution trouble, because a node designated as a cluster head may not necessarily have higher processing ability and medium capacity than the other nodes. Until being intentionally designed so, the cluster head may become a bottleneck.

Hierarchical routing delivers a promising method for scalability. However, whether or not these hierarchical arrangements can really resolve the scalability problem still rests a question.

Scalability is the most critical question in WMNs. Hierarchical routing protocols can only incompletely solve this problem due to their complexity and difficulty of controlling. Terrestrial routing relies on the being of GPS or similar positioning technologies, which increases cost and complexity of WMNs. Furthermore, the review of endpoint position produces additional traffic

load. Thus, new scalable routing procedures need to be established. Current presentation metrics incorporated into routing protocols need to be expanded.

Furthermore, how to mix multiple presentation metrics into a routing protocol so that the optimal overall performance is achieved is a challenging issue.

Routing for multicast requests is another vital research topic. Many applications of WMNs need multicasting ability. For example, in a public or a city-wide system, video distribution is a common application.

Cross-layer design amid routing and MAC protocols is another fascinating research topic. Previously, routing protocol research was concentrated on layer-3 functionality only. Though, it has been shown that the performance of a routing protocol may not be acceptable in this case. Adopting multiple show metrics from layer-2 into routing protocols is an example. Though, communication between MAC and routing is so close that merely exchanging parameters between protocol layers is not satisfactory. Amalgamation many functions of MAC and routing is a promising approach. When multi-radio or multi-channel nodes are measured, fresh routing protocols are needed for two reasons. First, the routing protocol not only wants to choose a path in-between dissimilar nodes, it also needs to select the most appropriate channel or radio on the track. Second, cross-layer scheme becomes a necessity because change of a routing path involves the passage or radio swapping in a mesh node. Deprived of considering cross-layer design, the switching process may be too slow to lower the presentation of WMNs. The current routing protocols treat all network nodes in the same way. However, such answers may not be well-organized for WMNs, because the mesh routers in WMNs backbone and mesh clients have significant changes in power restraint and mobility. More well-organized routing protocols that take into account these differences are desired for WMNs.

Transport layer

To date, a large number of reliable transport protocols have been proposed for ad hoc networks. They can be categorized into two sorts: TCP variants and completely new transport protocols. TCP variants protocols that are an improved form of the traditional TCP for wired systems.The performance of classical TCPs degrades significantly in ad hoc networks.and the corresponding solutions. One of the well-known reasons for TCP performance degradation is that the traditional TCPs do not distinguish congestion and non-congestion harms. As a result, when non-congestion losses occur, the network output rapidly descents. Furthermore, once wireless channels are back

to the normal operation, the classical TCP cannot be recovered quickly. The protocol in enhances TCP through a feedback mechanism to differentiate between damages produced by overcrowding or wireless channels. This notion can be adopted to WMNs. However, how to design a loss differentiation method and consequently adapt the TCP for WMNs consequently is subject to future study. Link failure also degrades the TCP performance. Link disaster may occur often in mobile ad hoc networks since all nodes are mobile. As far as WMNs are concerned, link failure is not as serious as in mobile ad hoc networks, because the WMN infrastructure avoids the subject of single-point-of-loss. Yet, due to wireless channels and mobility in mesh clients, link failure may still occur. To improve TCP throughput, overcrowding losses and link failure also need to be differentiated. Schemes alike to open link disaster notice (ELFN) arrangement can perform such differentiations. TCP is critically dependent on ACK, so its throughput can be strictly obstructed by network asymmetry which is defined as the situation where the forward way of a system is meaningfully diverse from the reverse direction in terms of bandwidth, loss rate, and latency.In order to lessen the influence of system asymmetry on TCP performance, cross-layer optimization is a challenging but effective solution, meanwhile all difficulties of TCP throughput degradation are actually related to protocols in the lower layers. For example, it is the routing procedure that regulates the path for both TCP data and ACK packets. To avoid asymmetry between data and ACK packets, it is wanted for a routing procedure to select an optimal path for both data and ACK packets but without increasing overhead. As it is also know that the link layer performance directly impacts packet loss ratio and network asymmetry. For real-time delivery, no existing solution from ad hoc networks can be adopted and custom-made for the usage of Network. Thus, brand-new RCPs need to be developed considering the features of WMNs. In addition, new loss distinction arrangements must be industrialized to work together with RCPs. Since WMNs will be integrated with various wireless networks and the Internet, an actives rate regulator protocols are also needed for WMNs.

Application layer

Applications define the need to install WMNs. Thus, it is always a key step to find out what current applications can be sustained by WMNs and what new applications need to be developed.Various Internet uses offer vital timely material to public, make life more convenient, and increase work efficiency and output. Like, email, search engine like Google, on-line actions like eBay, on-line purchase, chatting, video streaming, etc. For this type of applications,

backhaul access to the Internet is not necessary. Users of these applications connect within WMNs. A customer may need to store high-volume data in disks owned by other users, download archives from other customers disks centered on peer-to peer networking , and query/retrieve information located in distributed database servers.Again, this type of applications does not need backhaul access to the Internet. For example, when a cellular phone talks to a Wi-Fi phone through WMNs, no Internet is needed. Similarly, a user on a Wi-Fi network might presume to observe the position in many sensors in a wireless sensor network. All these applications must be sustained by new software in the application layer of the end-users.To study application protocols for dispersed data distribution in WMNs. Like, for wired networks, application protocols are available for end-to-end data distribution, on-line gaming, etc. Though, WMNs have much different characteristics than wired networks.WMNs still short of effective security clarifications because their security is easier to be compromised due to : vulnerability of passages and nodes in the collective wireless passage, absence of infrastructure, and dynamic change of network topology. The attacks may advertise routing updates in and for DSR and AODV, respectively. Another type of attacks is packet forwarding, i.e., the aggressor may not modify routing tables, but the packets on the routing path may be lead to a different destination that is not constant with the routing procedure. Moreover, the attacker may sneak into the network, and impersonate an authentic node and does not trail the essential terms of a routing protocol.

2.3 Cross Layered Approach

Cross layer [3] as the name suggests means the exploitation of multiple layers to get information and then to optimize that information to get improvement in the performance.The most commonly used OSI model which consist of many layers as below:

1. *Physical layer*- used for bits transmission.
2. *Data link layer*-used for frames transmission.
3. *Network layer*-used to route packets to node.
4. *Transport layer*-used to transmit packets to applications.
5. *Session layer*-used to manage connections.
6. *Presentation layer*-used to encode/decode messages for security.
7. *Application layer*-used to provide services to application program.

Each layer makes uses the services given by the layers below it,as shown in Fig.11

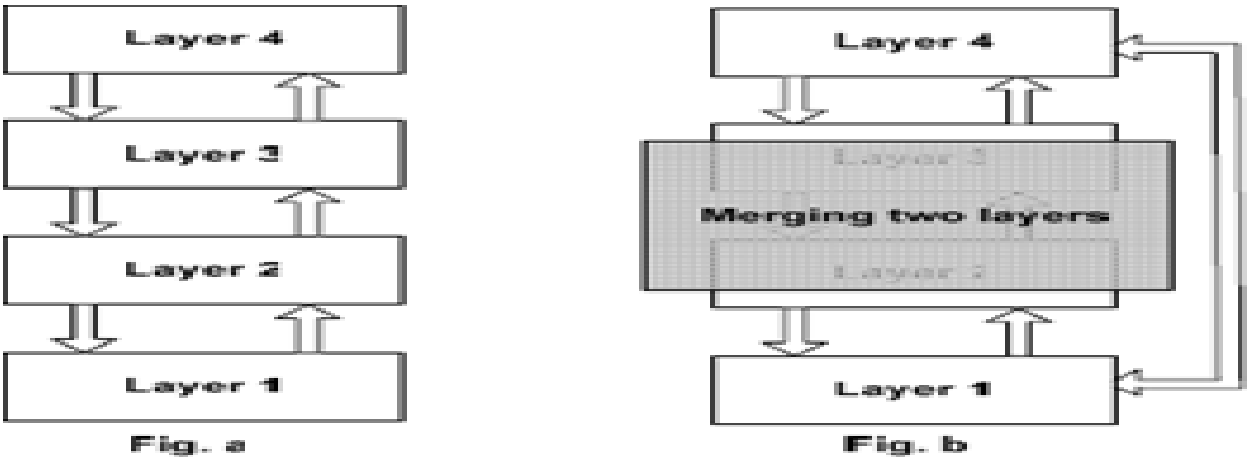


Fig.11. Example showing interfaces (Fig.a) and its violations (Fig.b)[3]

Open System Interconnection, an ISO normal for worldwide communications that defines a networking outline for executing in seven layer protocols. ISO shorts for International Organization for Standardization. Started in 1946, ISO is an international association composed of national standards bodies from over 75 countries. For example, ANSI is a member of ISO. ISO has defined a number of important computer criteria; the most important of them is perhaps OSI a uniform design for scheming networks.Layers are discussed one by one.

The physical layer is troubled with diffusing raw bits over a interaction passage. The design issues have to do with making sure that when one end transfers a 1 bit, the other end as a 1 bit, not as a 0 bit accepts it. Typical questions here are how several volts must be used to signify a 1 and how many for a 0, how many microseconds a bit lasts, whether transmission may continue concurrently in both ways, how the initial connection is established and how it is torn down when both sides are over, and how many pins the system connector has and what each pin is used for. The design issues here deal mostly with mechanical, electrical, and practical boundaries, and the physical transmission medium, which lies below the physical layer.

Then we have data link layer.The main task of the data link layer is to take a raw transmission capability and alter it into a line that seems free of transmission errors in the network layer. It accomplishes this chore by having the source breakdown the input data up into data frames (typically a few hundred bytes), transmit the frames in order, and process the greeting frames sent back by the receiver. Since the physical layer merely takes and transfers a torrent of bits without any favor to meaning of structure, it is up to the data link layer to make and know frame

borders. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. If there is possiblity that these bit designs might occur in the data, special care must be taken to avoid misunderstanding. The data link layer must offer error control between adjacent nodes.A noise burst on the line can destroy a frame totally. In this situation, the data link layer software on the source machine must resend the frame. However, multiple broadcasts of the identical frame present the possibility of duplicate frames. A duplicate frame could be sent, like, if the acknowledgment frame from the receiver back to the sender was destroyed. It is up to this layer to solve the difficulties caused by injured and replica frames. The data link layer may offer several different service programs to the routing layer, each of a dissimilar quality and with a different price.

Next,we have network layer.This layer provides switching and routing technologies, creating logical paths, known as simulated paths for transferring data from node. Routing and forwarding are functions of this layer, as well as addressing, interconnection error handling, overcrowding control and packet sequencing.The network layer is concerned with controlling the process of the subnet. The main plan issue is shaping how packets are routed from source to destination. Routes could be created on static tables that are "wired into" the network and rarely changed. They could also be determined at the beginning of each discussion, for example a terminal time. Finally, they could be highly dynamic, being determined a new for each package, to imitate the current system load.If too many packets are present in the subnet at the same time, they will get in individually other's way, creating bottlenecks. The control of such congestion also belongs to the network layer.Subsequently the workers of the subnet may well imagine remuneration for their efforts, there is often some accounting purpose built into the routing layer. At the very least, the software must count how many packets or characters or each client directs bits, to harvest billing data. When a packet crosses a national border, with different rates on each side, the accounting can become complex.When a packet has to travel from one network to another to get to its endpoint, many difficulties can ascend. The addressing used by the second network may be different from the first one. The additional one may not receive the packet at all because it is too large. The protocols may differ, and so on. It is up to the routing layer to overwhelm all these difficulties to allow heterogeneous networks to be interconnected. In transmission networks, the networking problem is modest, so the network layer is often thin or even nonexistent.

Then we have transport layer. This layer provides transparent transfer of data between end systems, or hosts, and is responsible for point to point error retrieval and flow control. It ensures complete data transfer.

The basic function of the transport layer is to receive data after the session layer, split it up into smaller units if need be, pass these to the network layer, and safeguard that the bits all arrive correctly at the other end. Furthermore, all this must be done efficiently, and in a way that separates the session layer from the unavoidable changes in the hardware technology.

Under normal conditions, the transport layer makes a separate network assembly for each transport connection required by the session layer. If the transport connection needs a high output, however, the transport layer might create multiple network networks, separating the data among the system connections to improve throughput. On the other hand, if creating or sustaining a network joining is expensive, the transport layer might multiplex several transport connections onto the same network connection to reduce the cost. In all cases, the transport layer is required to make the multiplexing transparent to the session layer.

The transport layer also regulates which service to deliver to the session layer, and ultimately, the users of the system. The most general type of transport connection is an error-free point-to-point channel that delivers messages in the order . Though, other likely kinds of transport, service and transport isolated messages with no assurance about the order of transfer, and distribution of messages to multiple destinations. The type of service is determined when the connection is established.

Then is session layer. This layer establishes, manages and terminates associates between applications. The session layer makes, coordinates, and terminates conversations, exchanges, and interchanges amid the applications at each end. It deals with session and connection coordination.

The session layer lets users on dissimilar technologies to establish sessions between them. A session allows ordinary data transport, as ensures the transport layer, but it also offers some enhanced services beneficial in some applications. A session might be used to permit a user to log into a remote time-sharing system or to transfer a file between two machines.

One of the services of the session layer is to accomplish dialogue control. Sessions can allow traffic to go in both directions at the same time, or in only one way at a time. If circulation can only go one way at a time, the session layer can help keep track of whose turn it is.

Next is presentation layer. This layer provides independence from differences in data representation .The presentation layer works to transmute data into the system that the application layer can accept. This layer formats and encrypts data to be sent crossways a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

The presentation layer accomplishes many purposes that are demanded sufficiently often to warrant finding a general solution for them, rather than allowing each user crack the difficulties. In particular, unlike all the lower layers, which are just interested in moving bits dependably from one end to other,the presentation layer is concerned with the syntax and semantics of the information transferred.

A typical example of a performance facility is encoding data in a standard, agreed upon way. Maximum user programs do not altercate random binary bit strings. They exchange things such as people's names, dates, amounts of money, and invoices. These matters are characterized as character strings, integers, floating point numbers, and data structures collected of numerous simpler items.

Diverse computers have dissimilar codes for representing character strings, integers and consequently. In order to make it likely for computers with different depiction to communicate, the data structures to be swapped can be explained in an abstract way, along with a standard encoding to be used "on the wire". The presentation layer grips the work of handling these intangible data structures and converting from the representation used inside the computer to the network standard representation.

Finally, we have application layer. This layer supports application and end-user processes. Communication partners are recognized, eminence of service is known, user authentication and privacy are considered, and any constraints on data syntax are recognized. All of this layer is application-specific. This layer provides application services for file transfers, e-mail and other system software facilities. Telnet and FTP are applications that exist entirely in the application level. Tiered application designs are part of this layer. The application layer contains a variety of protocols that are commonly needed.

Many cross layer designs have been given.Different proposals are there.Different cross layer proposals are there based on the violations of architecture they defy .The architecture is inspired form the five layers of model. Thus, it is assumed that the reference architecture has the

application layer, the transport layer, the network layer, the link layer which comprises the data-link control (DLC) and medium access control (MAC) sub- layers, and the physical layer—with all the layers performing their generally understood functionalities.

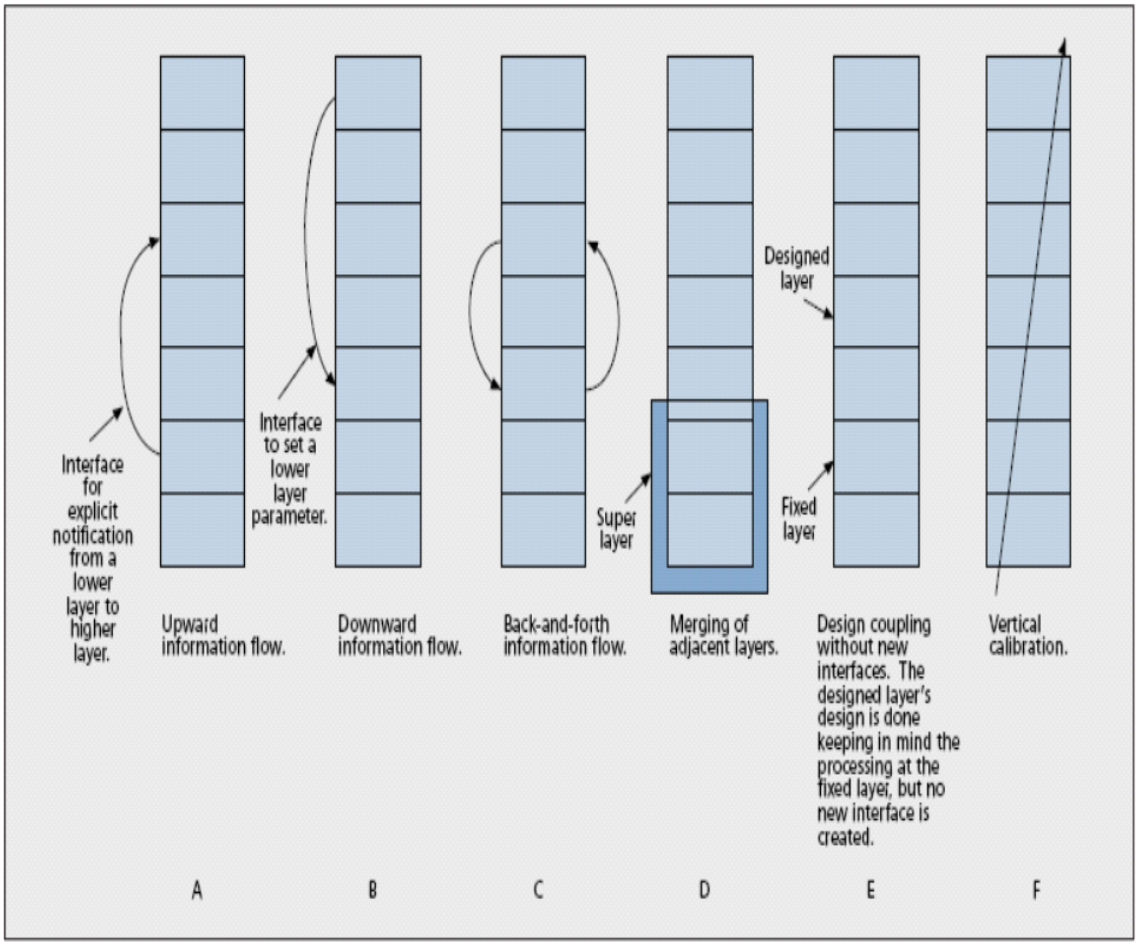


Figure 12: The different kinds of CLD proposals.

Interface is needed among the layers for cross layer design.They are classified regarding the data flow direction.

i) Upwards: From lower layer(s) to a higher-layer.

ii) Downwards: From higher layer(s) to a lower-layer.

iii) Back and forth: Iterative flow between the higher and lower layer.

The further sub-categories are discussed are as below:

i) *Upward information flow:* In this there is information flow from the bottom layer to upper layer as shown in Fig12.A.The upward flow of information can be named as the self adaptation

loops at a layer.This self adaptation loop contains constraints that can be seen at the layer itself. Self-adaptation loop means an adaptive higher layer protocol that respond to events that,within the constraints of layering, are directly observable at the layer itself. Hence, self-adaptation loops do not require new interfaces to be created from the lower layer(s) to the higher layer and cannot be classified as Cross Layer Designs.Data rate increses on successive delivery of packets and is decreased on the failure of packet.

ii) *Download information flow:*

Some CLD proposals rely on setting parameters on the lower layer of the stack at execution time having a communication from upper layer, as illustrated in Fig.12 (B). As an example, the applications can notify the link layer regarding the delay, and the link layer could use packets of data with sensitive information priority wise.

iii) *Back and forth information flows:*

Two layers, performing unlike jobs, can cooperate with each other at execution-time. Often, this manifests in an iterative circle among the two layers, with data 6flowing between them, as highlighted in Fig12.(C) and Fig12 (D).This is the idea in NDMA proposal. Basically, upon detecting a collision, the base station first estimates the number of users that have collided, and then ask the required number of users. Thereupon, signal processing lets the base station differentiate the colliding users with signals.Basically, power control determines the effective topology of the network by determining which nodes can communicate with one another in a single hop. If the transmitted power is too large, then many nodes may be connected by a single hop, but the interference also would be large. On the other hand, keeping the power too small can make the network fragmented or create too many hops and hence added MAC contention. Protocols causing from having the combinned difficulty of power and arranging often result in an iterative solution: Trying to keep the power level at an optimal level by responding to the changes results in normal throughputAn algorithm is selected for the transmission and then a power control algorithm determines if the transmissions of all the chosen users can simultaneously go on. If no, the scheduling algorithm is repeated. This iteration between scheduling and power control is repeated till a valid transmission schedule has been found.

Merging of adjacent layers

Two or more adjacent layers can be designed together such that the service provided by the fresh ―superlayer is the combination of the services provided by the constituent layers. While

possibly increasing the design complexity substantially, the super-layer can be communicated with the remaining of the stack by means of the lines that already exist in the real architecture.

Design coupling without new interfaces

Another category of CLD involves coupling between two or more layers at design time without making any extra borders for data sharing at execution-time. This is illustrated in Fig.(E). Considers the design of MAC layer for the uplink of a wireless LAN when the PHY layer is capable of providing multi-packet reception capability. Usually, the motivation for conditioning the design of a layer on another layer is a change in technology at one layer, which needs to be perfected by equivalent alterations to the other layer(s).

Vertical calibration across layers

The final category of CLD proposals, as the name suggests, refers to adjusting parameters that span across the layers, as illustrated in Fig. Fig12(F). The performance seen at the level of the application is a function of the parameters at all the layers under it. So,it is possible that a joint tuning can help to achieve better performance than what individual settings of parameters—as would happen had the protocols been designed independentl .Parameters within the layers of vertical calibiration at design time with the improvement of many parameters. It can also be done on demand at execution-time, which emulates a flexible protocol stack that reacts to the disparities in the network, traffic and overall system situations. Static vertical calibration does not generate major concern for operations since the restrictions can be adapted once at the time of designing and gone undamaged thereafter. Vertical calibration which is dynamic, on the other hand, needs devices to recover and bring up to date the parameter values being optimized from the different layers.

Due to the random nature of the wireless channel, layered approach to communication systems design is not optimal for wireless communications. Through utilizing cross-layer design, researchers are creating ‖smarter‖ communication methods, which make automated compromises among application requirements in order to meet specific optimization goals. They abuse these compromises to make improved and more well-organized use of the wireless channel. Cross-layer design emphasizes on the network throughput optimization by allowing dissimilar layers of the communication stack to share state information or to synchronize their activities in order to collectively enhance network throughput.

2.4 Attacks

Due to multihop routing of wireless mesh networking,it is vulnerable to various kinds of attacks such as Denial of Service attacks[2].DoS are common attacks in wireless systems.It is a serious factor to guard against DoS attacks in security systems.Traditional DoS attacks were involved around a particular host. However in wireless mesh networks,limited bandwidth,mobility,routing functionalities etc. associated with each node lead to many options for denial of service attack.An aggressor can generate crowding in system by generating excess amount of traffic itself.DoS attacks can cause severe downgrade of the performance of the network in terms of throughput and latency.

TABLE 1 THREATS IN WIRELESS MESH NETWORKS

Layer	**Threats**
Physical Layer	Jamming,scrambling
MAC Layer	Unfairness,Selfish MAC ,flooding
Routing Layer	Blackhole,Wormhole,Greyhole,Jellyfish,Rushing,Byzantine,Sybil,Flooding

In general ,these attacks[2] fall into two categories:passive attacks and active attacks.A passive attack is when a malicious node listens to or eavesdrop in a traffic network[6].It requires no security breach .All other attacks are active attacks except for eavesdropping of messages.

A.Physical layer:

Physical layer can generate denial of service threat by using radio jamming device or by source of strong noise to block the physical locations and can work out the service availability. For jamming attack in WMN, the attacker could generate the threat from wherever. Due to the vast coverage area and dense deployment of wireless mesh routers in WMN, it is more susceptible denial of service attacks at the physical layer.

Different types of jamming attacks [5] are:

1) Trivial Attack: Transmission of noise is regular.

2) Periodic Attack: Transmission of noise is periodically as short signal. These conductions can be arranged often enough to disrupt all other communications, for example, with a time a smaller amount than the AIFS. It is also called scrambling.

3) Reactive Jamming Attack: In which an attacker gives a indication whenever it discovers that extra node has started a broadcast, causing a collision during the second portion of the message.

B.MAC Layer

MAC layer includes the ability to discover ,join and leave the network,and coordinate the access to radio medium.DoS attacks are below:

1.*MAC Misbehaviour*: DoS attack can be implemented by corrupting frames.

2.*Selfish attack*: The selfish node decreases the resource of wireless channel which could have been used by legitimate nodes affecting network performance and service.There are two types of selfish nodes in WMN,selfish client node and selfish router node.Selfish client nodes to achieve increased throughput access WMN with selfish strategy,reduces consumption of power and QoS improvement.Selfish router uses selfish strategy top result in network congestion or even DoS.WMN is more vulnerable to selfish client node attack due to characteristics of multihop and public access.The router node attacks will have impact on the entire network performance.

C.Routing Layer

1. *Blackhole attack*: in this,vulnerable node transmits itself as most optimal node for the forwarding of data.This malicious node then denies service by dropping packets.

2.*Greyhole attack*:This attack varies a little from Blackhole attack.In comparison to Blackhole attack malicious node drops just selective packets.

3.*Womhole attack*:In it,an attacker gets packet at an end in the system,'tunnels' them to another end of the system to create a shortcut(wormhole).The malicious node maliciously drops packets to deny services in WMN.

4.*Jellyfish attack*:To deny the services packets are dropped in a malicious way and it is done by complying protocols.

5.*Byzantine attack*:The adversary has a full control of an authenticated device and to disrupt system it does arbitrary behavior.

6.*Sybil attack*:A malicious node behaves itself as a large number of nodes by fabricating itself in multiple identities.

7.*Flooding attack*:The attacker transmits a flood of packets to the target to congest the network and to decrease its performance.

2.5 INTRUSION DETECTION SYSTEM FOR WMN

An intrusion can be any of the unwanted activity in the form of active or passive attacks,which attacker uses to create unwanted situation and bad results for user's confidentiality, integrity of network or availability of network resources[7].Intrusion is simply an action that compromises data integrity, confidentiality of user, integrity of network or network resources availability.And a system that is used to detect such malicious actions of network or node, is called Intrusion Detection System or Intrusion Detection System.By realizing the Intrusion Detection System, wireless networks security can be increased to certain limit.The framework for cross layer in Intrusion Detection System consist of modules which collect information from different layers via interfaces of these layers.The data collected is then analysed in an analysis module where detection and classification of the information in terms of threats is done.On the basis of cross layer information if that attack is found in database than an alarm is being generated otherwise its information is stored in the database for the future use.

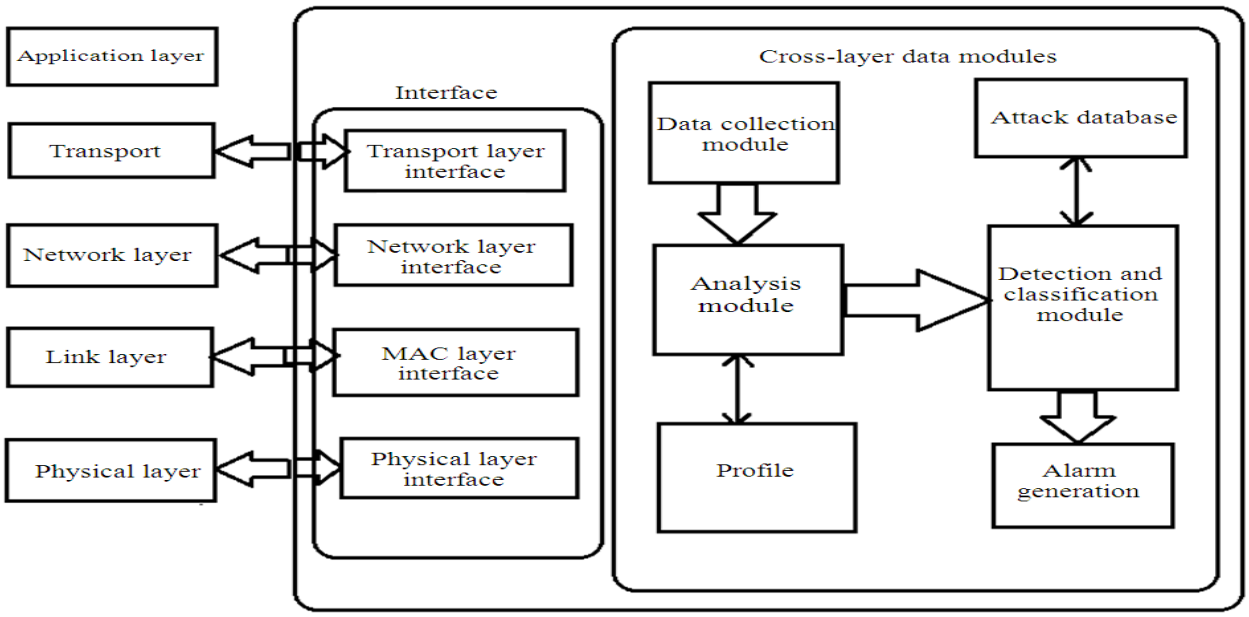


Fig13. Framework for cross-layer IDS

Two types of IDS exist.Pattern based IDS identifies all the unknown attacks,while anomaly based intrusion mechanism have intelligence to identify and respond to new intrusions which are not known.IDS are further classified into Stand-alone IDS,Distributive and Cooperative IDS and Hierarchical IDS.

Stand-alone IDS operates independently on each node to monitor the internal events that are recorded in system logs.In Distributive and Cooperative IDS,each node participate in detection and response of intrusion.And in hierarchical IDS,child nodes are monitored by cluster-heads

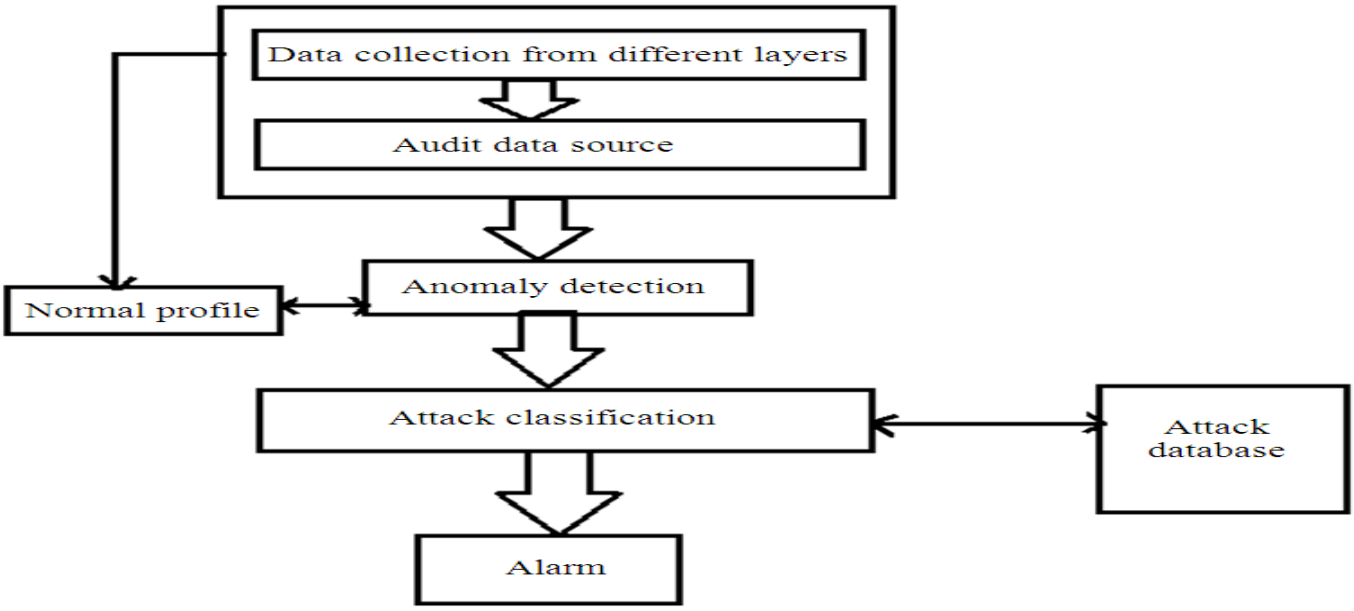


Fig14. Algorithm for IDS

and responds on intrusion detection.Previously, single layer intrusion detection systems were used which took information from single layer but with the coming of cross layer intrusion detection systems information from different layers are used for the optimization, and if the attack is found alarm is being generated. In cross-layer design,it uses behavioural information from many layers for the detection.It makes uses of parameters like packet drop ratio,delay,hop count etc. from many layers instead of single layer parameters as an optimized method in detection.

CHAPTER 3

3.1 PROBLEM DESCRIPTION

In WMN's,nodes are moveable and topology of the network changes dynamically which brings challenges to security.As a result attackers can take advantages of routing protocols and can carry out various Denial of Service (DoS) attacks like Black hole attacks ,Gray hole attacks etc. which can bring damage to the network 's topology. Present problem is the detection of Gray hole attack in WMN.

Grayhole Attack

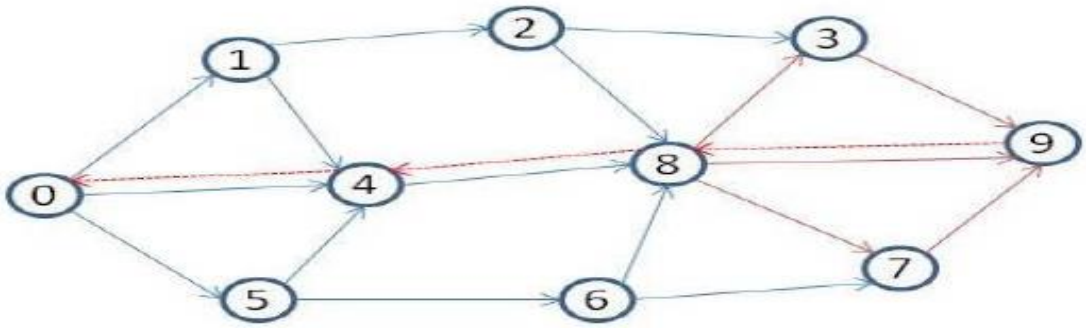


Fig 15 Node Network

On demand routing protocols like DSR[4] shown in Fig15 are more vulnerable to this type of attack in WMN.It is a reactive routing protocol as it discovers a path to endpoint only when it is required.It is a source routing as source is responsible for giving whole information of the path.

DSR consist of two phases:

1.Route Discovery 2.Route Maintenance

In Route Discovery phase,source node broadcasts Route Request (RREQ) message to the network to find path.Each node retransmits the RREQ packet and forwards to other nodes in Time-to-Live (TTL)time.Each RREQ carries a sequence number generated by source node and

the traversed path.The intermediate nodes contain cache that contains information in data packet extracted from source route.Destination on receiving RREQ packet, sends Route Reply (RREP) message back to the source listing the route taken by RREQ packet.Route with lowest latency is selected by the source node.In the route maintenance phase,if link gets broken,a RERR message is sent to the source node,which in turn starts new route discovery process. In above fig.4 Source node 0 broadcasts Route Request (RREQ)message in the network[3]. On reaching destination 9,destination sends Route Reply(RREP) message to the source ,on the path of RREQ message If the path is 0-4-8-9 AND node 8 is Gray hole.On receiving packets, it will discard some of them and will not send Route Error(RERR)message to the source node. Gray hole discards more than 60% of packets received where as Black hole discards 100%.

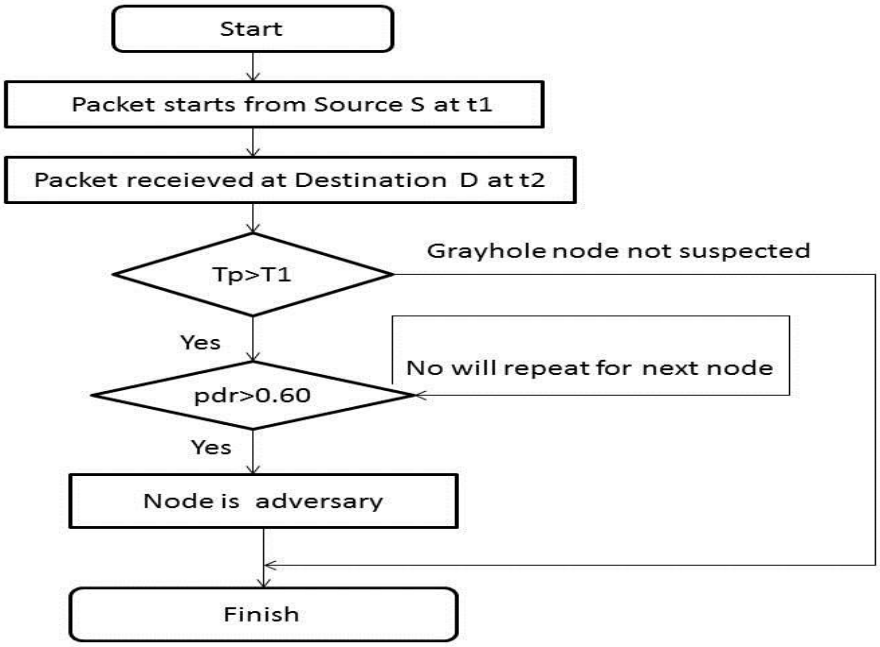
Grayhole attack will bring damage to the network.We found some of the detection systems on WMN. Sun et al [13] gave an approach for attack detection. They used a neighbourhood technique to perceive the attacker and used a recovery of route protocol to make a improved path to the real destination. They gave a neighbouring node set which is within the range of node. Two kinds of control packets are sent to distribute set of neighbors among the various nodes.One drawback of this scheme is that public key infrastructure is needed, unless it will be prone to attack. P.Yi et al. [3] made a scheme on path, in which a node does not lookout every node in the network but watches the neighbouring hop in the current path. Gao et al. [11], for detecting adversary nodes used a signature algorithm to trace the packets [12,17] dropped by those nodes. The advantages of this algorithm are reliability, wide application, good security and the overhead of bandwidth is low. Shila et al. [14] came up with the defending grayhole attack in WMN consists of two phases. i) Counter threshold based which uses the threshold to detect threats. ii) another is query based uses feedback from the neighboring nodes to detect the location of the attacker. Ping Y YI et al. [15,16] came up with a detection approach on distributed intrusion. PingYI [9] made a scheme based on path,in which a node is not watching every node in the neighbor but observing next hop of the current path using a threshold value.It overhears the action of next hop.This protects the resources of the perceiving node by not sending extra control packets. In MAC layer, a report on collision rate is made to develop dynamic detecting threshold. The experimental research shows that cross layer based detection methods are better and active than single layer techniques.Some of the approaches for detection are in the table .

TABLE 2 VARIOUS DETECTION METHODS

S.No	Detecting Method	
1	Neighborhood-based method[13]	Every node watches its neighbors to detect any malicious node.
2	Path based scheme[3]	Node watches the next hop in the present path and compares with the Threshold value
3	Signature based algo[11]	In it ,source route nodes are checked and then malicious nodes are located.
4	Distributed intrusion[15]	Cluster techniques are used where a node monitors the cluster for a time period.

3.2 METHODOLOGY

As on demand routing protocols like DSR are vulnerable to various kinds of attacks like Grayhole attack.So,the detection of these attacks is done with the help of cross-layered mechanisms taking parameters from mac layer as well as routing layer and is optimized than its previous counterparts utilizing single layer. Comparison between theoretical time and the practical time is done to suspect the possible grayhole attack in the route and if found then condition for grayhole is checked for each node in that route.



Flow chart

3.3 PROPOSED SOLUTION

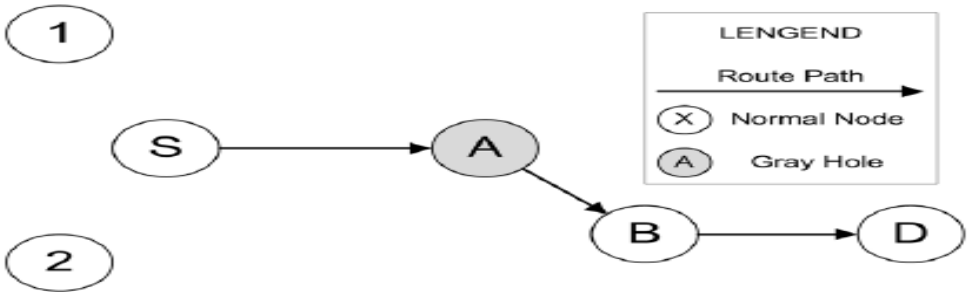


Fig.16. Grayhole node in the network

Cross layer detection mechanism

Proposed mechanism for the detection of Grayhole attack in WMNs[3] as below for Figure 16.Proposed solution is a cross-layer design because it uses behavioural information from two layers for the detection.It makes uses of parameters like packet drop ratio from MAC layer,delay

and hop count from routing layer.Packet drop ratio is the ratio of number of packets dropped to number of packets sent.

TABLE 3 PARAMETERS USED IN ALGORITHM

Tp	Time taken to deliver a packet from source to destination(Practical)
Tt	Time taken to travel a packet from source to destination(Theoretical)
Hc	No. of hops in route
D	Delay at each node to transmit the request
Pdr	Packet drop ratio
Pt	Periodic time interval

Algorithm:

1. Find the time (t1) at which packet starts from source node S.
2. The node S starts the process and sends packet to intermediate nodes through DSR protocol route until reaches it reaches destination node D.
3. Find time (t2) at which node D receives packet.
4. Calculate Tp using eq. Tp=T2-T1.
5. Get no. of hops in route Hc.
6. Calculate time Tt using:Tt=Hc*d.
7. If Tp > Tt then
8. Alert ”Grayhole attack is suspected in given route ”
9. For each node in the route do
10. If pdr > 0.60
11. Alert ”The node is adversary”
12. End if
13. End for
14. If no node is detected then
15. goto Step 9 and repeat for every pt.
16. End if
17. Down the current path and take another path
18. Else

19. Alert “Grayhole attack is not suspected in the given route”

20. End if

In our solution, we calculate theoretical time required for a packet to travel from source to destination. We also calculate practical time required for packet to travel from source to destination. Then we compare these two values. If practical time is greater than theoretical time, it will alert the grayhole attack is suspected. Whenever the grayhole attack is suspected, for each node in the route, check for packet drop ratio of it.If the packet drop ratio of a node is greater than 0.60(magnitude of the probability of packets dropped to become a Grayhole) then the node is an adversary node. In case, current route is suspected as Grayhole attacker but no such attack is identified in this path. However, this process will repeat for every periodic interval pt to identify the adversary nodes in the suspected path.

3.4 IMPLEMENTATION AND EXPERIMENT

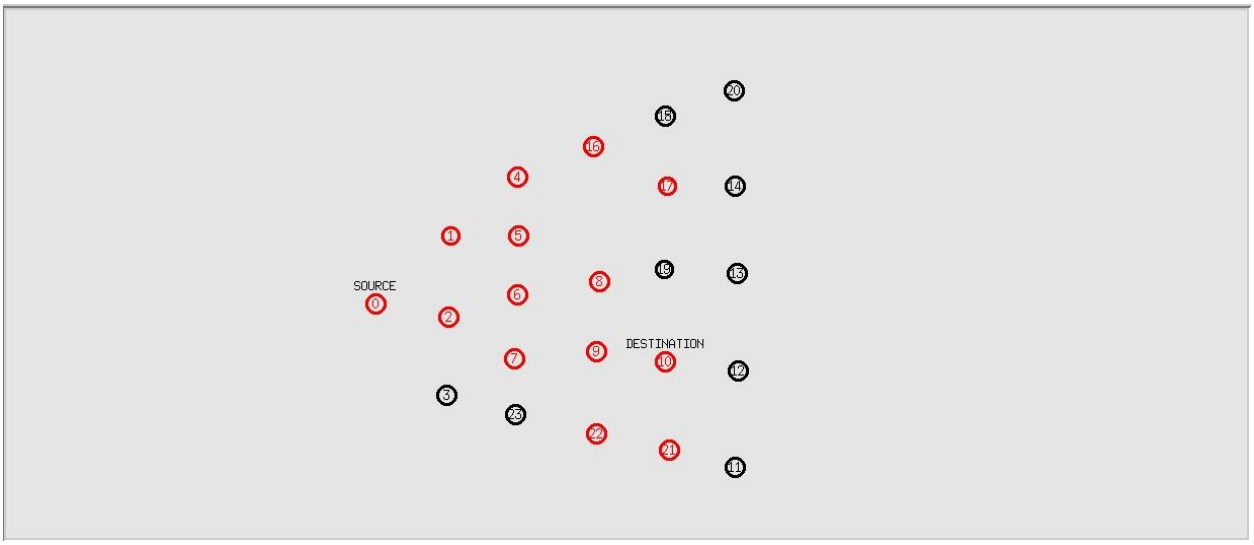


Fig17. Nodes at the starting stage

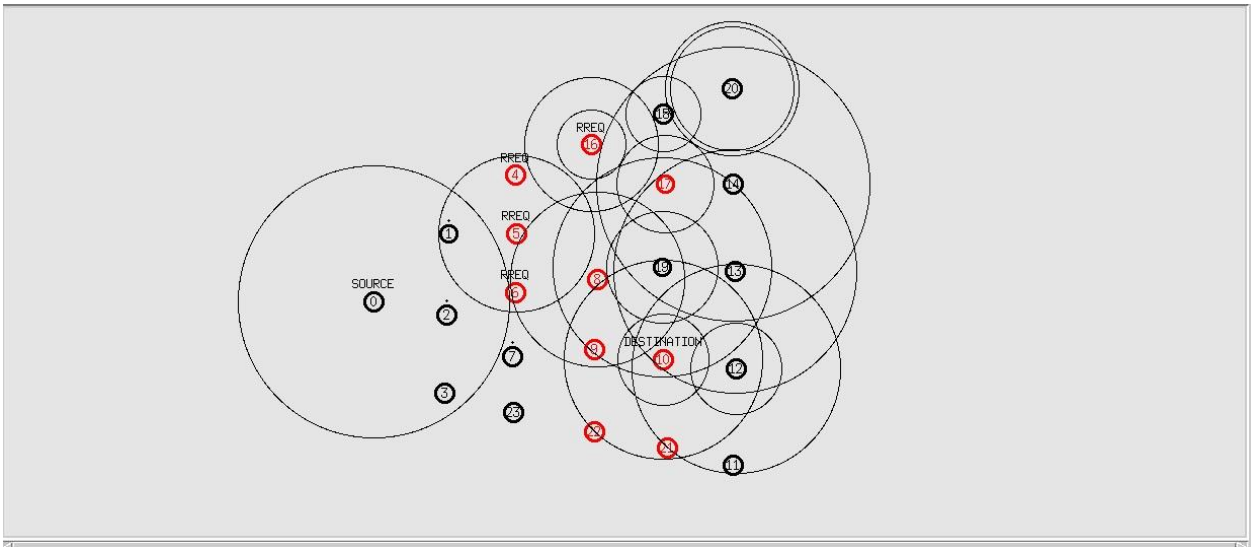


Fig18. Packet being transferred from Source to Destination using RREQ in DSR protocol

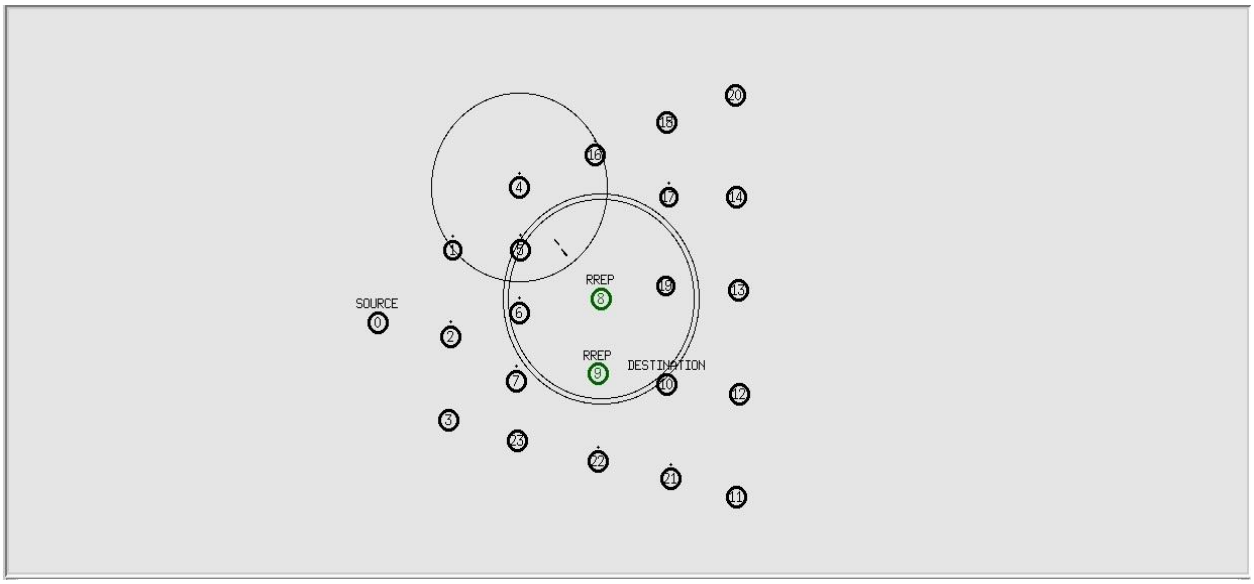


Fig19. Packet being replied using RREP from the destination to source in DSR protocol

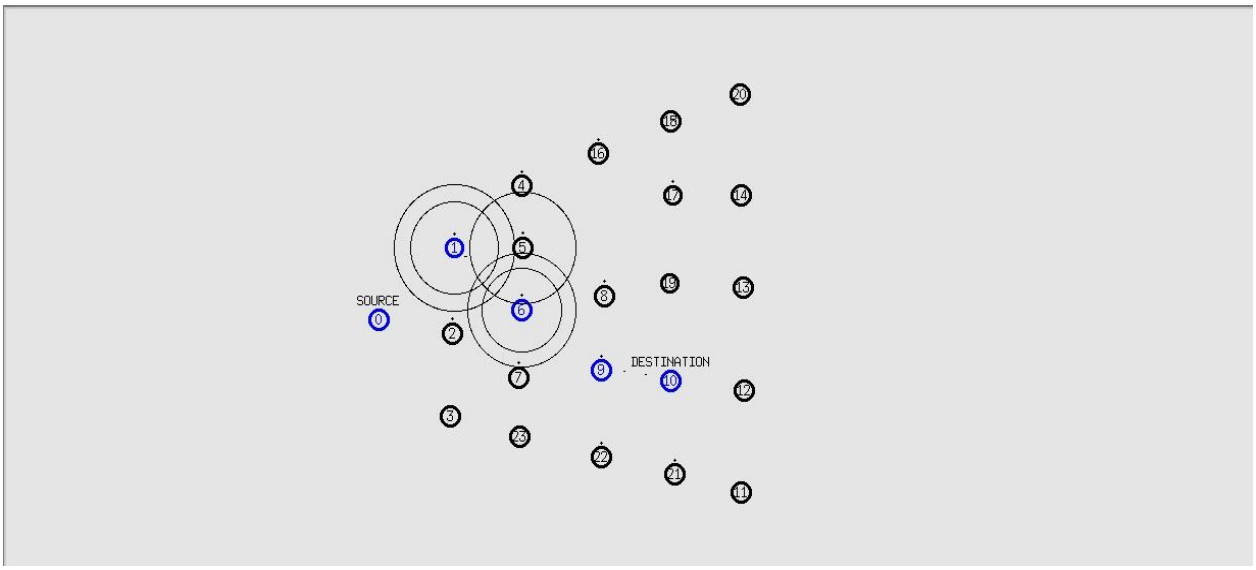


Fig20. Packet being sent from source 0 to destination 10 using DSR protocol

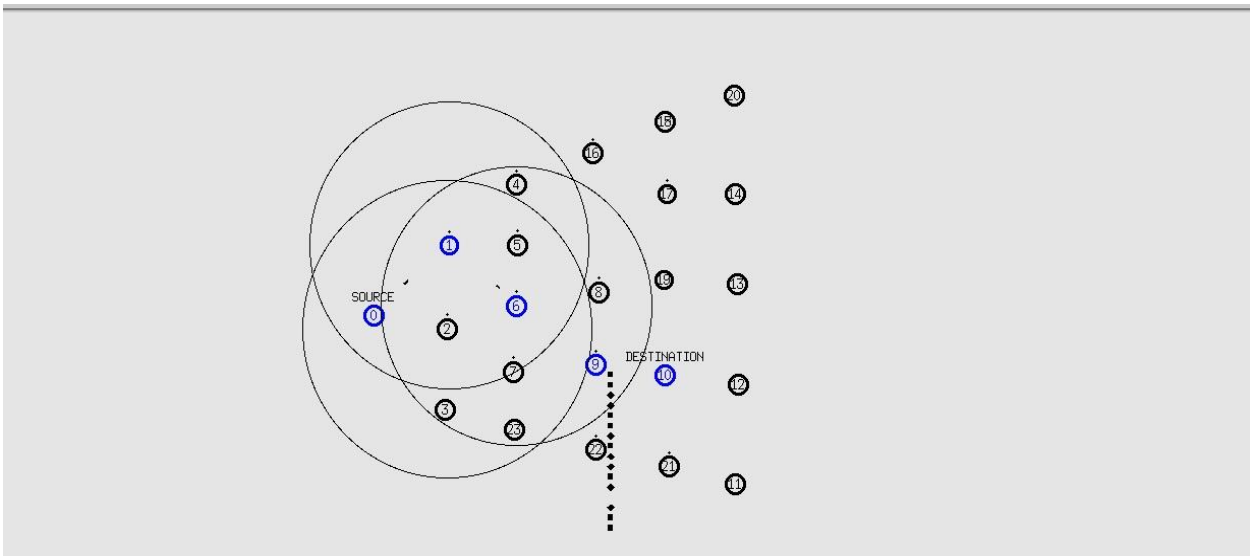


Fig21. Packets being selectively dropped at node 9

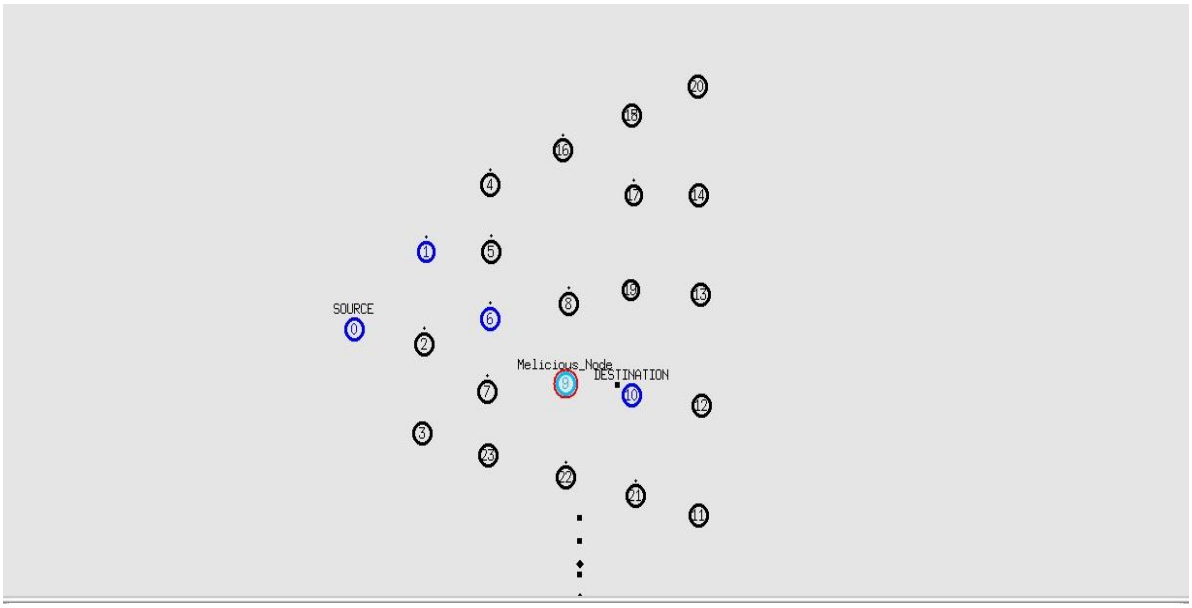


Fig22. Packet being sent with detection of node 9 as Grayhole

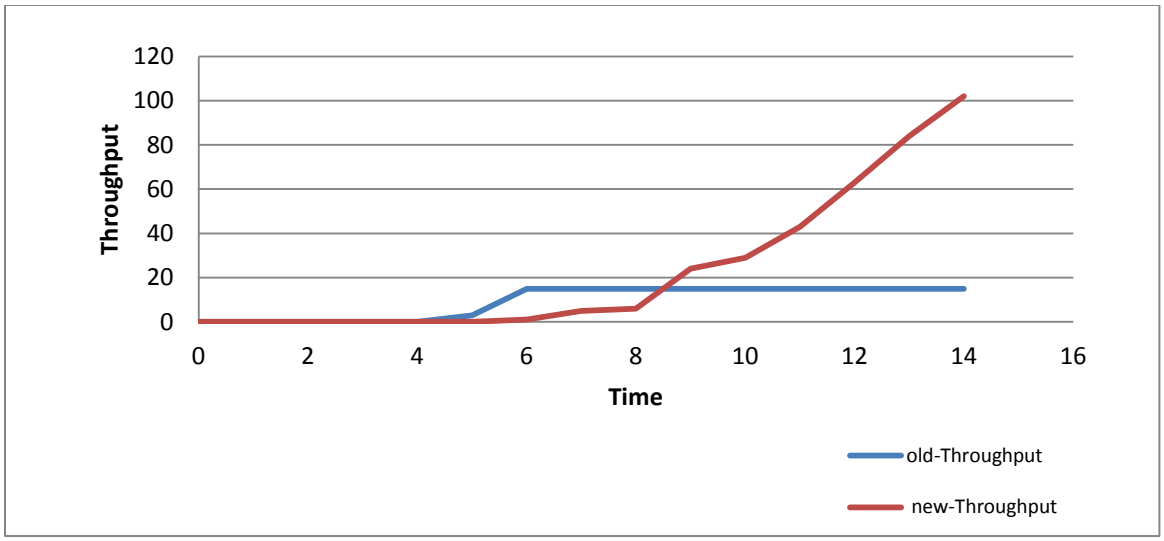


Fig23. Throughput vs Time

Throughput in this is defined as bits transmitted in per unit of time. Comparison of the scenarios using single layer and cross-layer.The figure 23 is plotted with throughput along X axis and the time taken along Y axis. The figure shows that with the increase in time throughput increases more in case of cross layers as compared to single layer.

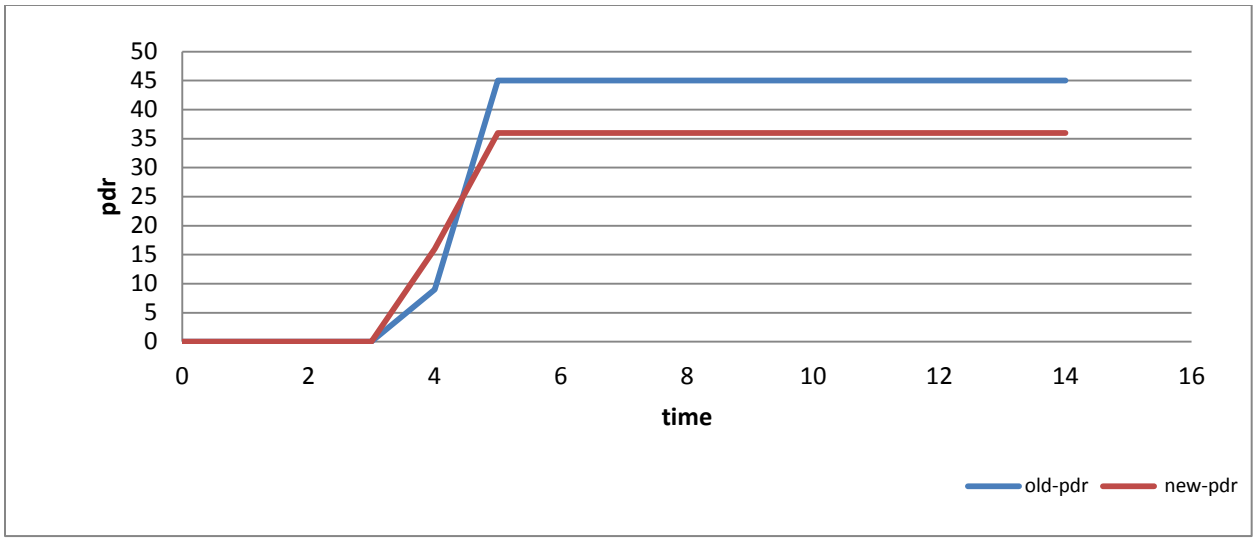


Fig24. Packet drop ratio vs Time

Similarly, figure 24 shows the packets dropped along Y axis and the time taken along X axis. The figure shows that the packet drop ratio increases along with the increase in time, packets dropped increases slowly in case of cross layers as compared to single layer where packets dropped are high with constant value.

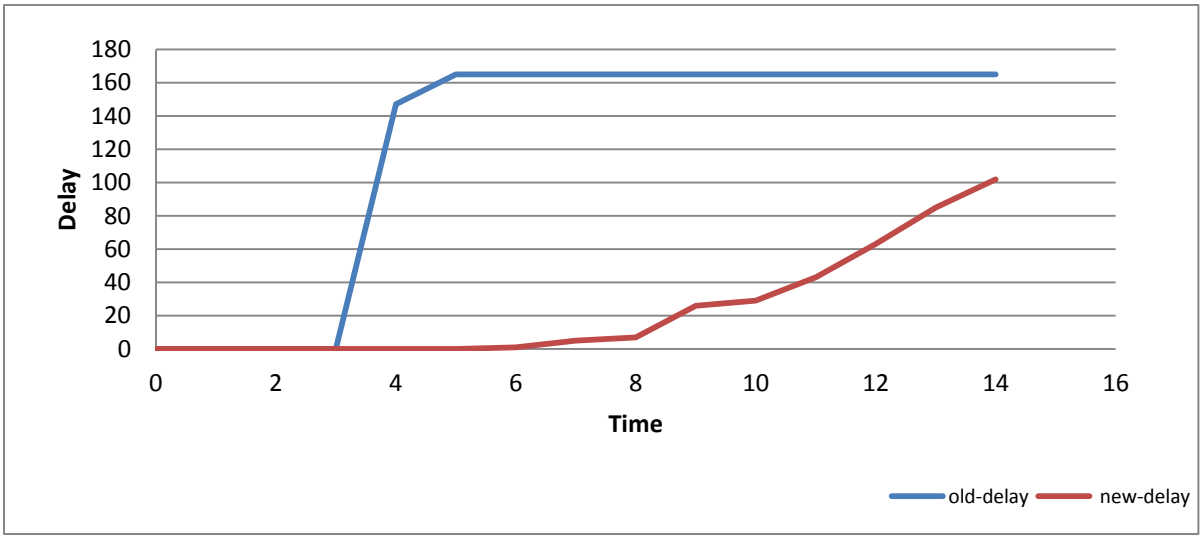


Fig25. Delay vs time

As delay is defined as the time taken by a bit to travel across a network from one node to another. Figure 25 is plotted with delay along Y axis and the time taken along X axis. The figure shows that with the increase in time,delay is more for single layer as compared to cross layer in the network.

CHAPTER 4

CONCLUSION

Cross layer taking parameters from both the MAC layer and the Routing layer. The solution is simulated using Network Simulator 2. The results shows there is an increase in throughput and the improvement in packet drop ratio. With the use of cross layer designs, researchers are implementing smart communication systems by stressing on the optimization of network performance with the help of different layers. At various layers information is being shared and actions are coordinated to jointly optimize the performance of the network.

FUTURE WORK

The future work will be on increasing throughput by improving detection rate.With the advancement of technology the need for security is rising.By making use of parameters of the more layers, cross layer intrusion detection mechanism can be improved.

5. References

Journal:

1. F.S.Al-Anzi and S.Khan,"Wireless Mesh Network Cross-layer Intrusion Detection",in Journal of Computer Science 2014,pp.2366-2368.
2. M.D.Nikose,"A review of Cross layer design",IJETET 2013, Vol.2,No.1,page-8.
3. P. YI, T.ZHU, N.LIU , Y. WU,"Cross-Layer detection for Blackhole Attack in Wireless Network", Jianhua LI Journal of Computational Information System 2012,Vol.8,No.10,pp.4103-4104.
4. M.Verma,N. C. Barwar,"A Comparative Analysis of DSR and AODV Protocols under Blackhole and Grayhole attacks in MANET" ,in International Journal of Computer Science and IT 2014, Vol.5,No.6,pp.7228-7230

Conference:

5. I.F.Akyildz,X. Wang,W.Wang ,"Wireless mesh networks:a survey" ,ELSEVIER 2005,pp. 444-448.
6. S.Seth, A. Gankotiya,"Denial of Service attacks and Detection Methods in Wireless Mesh Networks ", IEEE 2010,pp.238-239.
7. X.Wang, J. S. Wong, F. Stanley and S.Basu,"Cross-layer Based Anomaly Detection in Wireless Mesh Networks" , in Ninth Annual International Symposium on Applications and the Internet, IEEE 2009,pp.10-11 .
8. K. G.Reddy, P. S. Thilagam,B.N. Rao,"Cross-Layer IDS for Rushing Attack in Wireless Mesh Networks",ACM 2012,pp.396-398.
9. I. Askoxylakis, B. Bencsath, L.Buttyan, L. Dora, V.Siris and A.Traganitis Cross-layer security and resilience in wireless mesh networks, ,2013,pp. 3-6.
10. S.Khan, K.K.Loo and Z.U.Din ,"Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh",published in International Arab Journal of IT,Vol.7,No.4,2010,pp-436-437.
11. G.Xiaopeng, C.Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad Hoc Networks"in , IFIP International Conference on Network and Parallel Computing Workshops, 2007,pp.5-9.
12. D. Boneh, C. Gentry, B. Lynn, H. Shacham," Aggregate and Verably Encrypted Signatures from Bilinear Maps", Advances in Cryptology-EUROCRYPT'03: LNCS 2656. Berlin: Springer Veralg,2003,pp.2-4.

13. B. Sun, Y.Guan,J.Chen, Pooch U. W.,” Detecting Black-hole Attack in Mobile Ad Hoc Networks”,in Fifth European Personal Mobile Communications Conference, 2003,pp.6-9.
14. Shila, D. M., Anjali, T., “Defending selective forwarding attacks in WMNs”, IEEE International Conference on Electro/Information Technology,2008,pp.96-101.
15. P.Yi, X.Jiang, Y. Wu,” Distributed Intrusion Detection for mobile ad hoc networks”,Journal of Systems Engineering and Electronics, Vol. 19, issue 4,2008,pp.11-15.
16. P.Yi, Y. Wu, N.Liu, Z. Wang, “Intrusion Detection for Wireless Mesh Networks using Finite State Machine”,in China Communications 2010,pp.7-9.
17. S.Ravichandran, “Secured identity based approach with privacy preservation for wireless mesh networks”,in International Journal of Communication and Networking System.,Vol. 1, issue 2, 2012,pp.9-10.
18. S.Navitha,T.Velmurugan, “A survey on the Simulation Models and Results of Routing Protocols in Mobile Ad-hoc Networks”,in International Journal of Communication and Networking System ,Vol. 4, issue 2, 2015,pp.10-13.
19. S.Murugan,M.Sundara Rajan,”Role of Anomaly IDS in Network,International Journal of Communication and Networking System”, Vol. 2, issue 2, 2013,pp.12-14.

6. List of publications

Prabhat Ranjan, Hemraj Saini, "Cross-Layer IDS for Grayhole Attack in Wireless Mesh Networks," International Journal of Engineering and Technology ***[SCOPUS INDEXED]***. *(ACCCEPTED)*