# ANALYSIS OF STRUCTURAL & PLANNING DESIGN OF WIRELESS WORK SYSTEM & ROUTINE NETWORKS

**Vishal Khatri, Research Scholar,**
**Department of CSE, CMJ University.Shillong (Meghalaya)**

**Dr. P. K. Vashishtha, Supervisor ,**
**Dept. of Computer Science & Engineering ,CMJ University.Shillong (Meghalaya)**

***Abstract:*** Wireless work systems (WWS) comprise of work switches and work customers, where work switches have insignificant mobility and structure the foundation of WMNs. They give system access to both work and traditional customers. The integration of :WMNs with different systems, for example, the Internet, cell, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor systems, and so forth., can be practiced through the entryway and connecting capacities in the work switches. Work customers can be either stationary or portable, and can frame a customer work organize among themselves and with work switches. WMNs are foreseen to determine the impediments and to significantly improve the presentation of specially appointed systems, remote neighborhood (WLANs), remote individual advancement and moving various arrangements. WMNs will convey remote ser-indecencies for an enormous assortment of uses in close to home, nearby, grounds, and metropolitan regions. Regardless of ongoing advances in remote work organizing, many research difficulties stay in all convention layers. This paper introduces an itemized investigation on ongoing advances and open research issues in WMNs. Framework structures and uses of WMNs are depicted, trailed by examining the basic variables influencing convention plan. Hypothetical system limit and the cutting edge conventions for WMNs are investigated with a goal to call attention to various open research issues. At last, proving grounds, mechanical practice, and current standard exercises identified with WMNs are featured.

*IndexTerms*: Wireless work systems; Ad hoc systems; Wireless sensor systems; medium access control; Routing convention; Transport convention; Scalability; Security.

## I. *Introduction*

A wireless network is a computer network that uses wireless data connections between network nodes. Wireless networking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a

connection between various equipment locations.Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure. Examples of wireless networks include cell phone networks, wireless local area networks(WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks. Wireless telecommunications is the transfer of information between two or more points that are not physically connected. Distances can be short, such as a few meters for television remote control, or as far as thousands or even millions of kilometres for deep-space radio communications. It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of wireless technology include GPS units, Garage door openers or garage doors, wireless computer mice, keyboards and Headset (audio), headphones, radio receivers, satellite television, broadcast television and cordless telephones. A **mesh** refers to rich interconnection among devices or nodes. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. Mobility of nodes is less frequent. If nodes constantly or frequently move, the mesh spends more time updating routes than delivering data. In a wireless mesh network, topology tends to be more static, so that routes computation can converge and delivery of data to their destinations can occur. Hence, this is a low-mobility centralized form of wireless ad hoc network. Also, because it sometimes relies on static nodes to act as gateways, it is not a truly all-wireless ad hoc network Mesh clients are often laptops, cell phones, and other wireless devices. Mesh routers forward traffic to and from the gateways, which may, but need not, be connected to the Internet. The coverage area of all radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud depends on the radio nodes working together to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicated each other, directly or through one or more intermediate nodes. Wireless mesh networks can self form and self heal. Wireless mesh networks work with different wireless technologies including 802.11, 802.15, 802.16, cellular technologies and need not be restricted to any one technology or protocol. Remote work design is an initial move towards giving practical and low portability over a particular inclusion region. Remote work framework is, basically, a system of switches less the cabling between hubs. It is worked of companion radio gadgets that don't need to be cabled to a wired port like conventional WLAN passages (AP) do. Work framework conveys information over enormous separations by parting the separation into a progression of short jumps. Middle hubs support the

sign, yet helpfully pass information from indicate A point B by settling on sending choices dependent on their insight into the system, for example perform directing by first inferring the topology of the system. Remote work systems is a generally "stable-topology" arrange with the exception of the periodic disappointment of hubs or expansion of new hubs. The way of traffic, being totaled from countless end clients, changes rarely. For all intents and purposes all the traffic in a foundation work system is either sent to or from a door, while in remote impromptu systems or customer work organizes the traffic streams between subjective sets of nodes.[2]On the off chance that pace of portability among hubs are high, i.e., interface breaks happen every now and again, remote work systems begin to separate and have low correspondence performance.This sort of framework can be decentralized (with no focal server) or halfway oversaw (with a focal server).[4] Both are moderately cheap, and can be truly dependable and strong, as every hub needs just transmit similar to the following hub. Hubs go about as switches to transmit information from close-by hubs to peers that are excessively far away to reach in a solitary bounce, bringing about a system that can traverse bigger separations. The topology of a work system must be generally steady, i.e., not all that much portability. On the off chance that one hub drops out of the system, because of equipment disappointment or some other reason, its neighbors can rapidly discover another course utilizing a directing convention.

**Functional areas of Wireless Work Systems**

Work systems may include either fixed or cell phones. The arrangements are as various as correspondence needs, for instance in troublesome conditions, for example, crisis circumstances, burrows, oil rigs, front line reconnaissance, rapid versatile video applications on board open vehicle, constant hustling vehicle telemetry, or self-sorting out Internet access for communities.[5] A significant conceivable application for remote work systems is VoIP. By utilizing a nature of administration conspires, the remote work may support steering nearby phone calls through the work. Most applications in remote work systems are like those in remote specially appointed systems.

Some present applications:

U.S. military powers are presently utilizing remote work systems administration to associate their PCs, basically ruggedized PCs, in field operations.[citation needed. Electric keen meters currently being conveyed on living arrangements, move their readings starting with one then onto the next and inevitably to the focal office for charging, without the requirement for human meter perusers

or the need to associate the meters with cables. PCs in the One Laptop for every Child program utilize remote work systems administration to empower understudies to trade records and jump on the Internet despite the fact that they need wired or PDA or other physical associations in their general vicinity. Google Home, Google Wi-Fi, and Google OnHub all help Wi-Fi work (i.e., Wi-Fi impromptu) networking.makers of Wi-Fi switches started offering network switches for home use in the mid-2010s.

The 66-satellite Iridium heavenly body works as a work organize, with remote connections between neighboring satellites. Calls between two satellite telephones are directed through the work, starting with one satellite then onto the next over the group of stars, without experiencing an earth station. This makes for a littler travel separation for the sign, diminishing dormancy, and furthermore takes into consideration the heavenly body to work with far less earth stations than would be required for 66 customary correspondences satellites.

Activity

The standard is like the manner in which bundles travel around the wired Internet—information bounces starting with one gadget then onto the next until it in the end arrives at its goal. Dynamic directing calculations executed in every gadget enable this to occur. To actualize such unique directing conventions, every gadget needs to convey steering data to different gadgets in the system. Every gadget at that point figures out how to manage the information it gets – either pass it on to the following gadget or keep it, contingent upon the convention. The steering calculation utilized should endeavor to consistently guarantee that the information takes the most fitting (quickest) course to its goal.

Multi-radio work

Multi-radio work alludes to having various radios working at various frequencies to interconnect hubs in a work. This implies there is an extraordinary recurrence utilized for every remote jump and consequently a devoted CSMA impact space. With progressively radio groups, correspondence throughput is probably going to increment because of increasingly accessible correspondence channels. This is like giving double or different radio ways to transmit and get information.Remote work systems (WMNs) are progressively self-organized and self-arranged, with the hubs in the system automatically building up a specially appointed system and keeping up the work availability. WMNs are involved two kinds of hubs: work switches and work customers. Other than the directing capacity for passage/connect works as in a regular remote switch, a work switch contains extra steering capacities to help work organizing. Through multi-

jump interchanges, a similar inclusion can be accomplished by a work switch with much lower transmission control. To further improve the adaptability of work organizing, a work switch is generally outfitted with various remote interfaces based on either the equivalent or distinctive remote access advancements. Regardless of every one of these distinctions, work and regular remote switches are normally assembled dependent on a comparative equipment stage. Work switches have insignificant versatility and structure the work spine for work customers. Along these lines, in spite of the fact that work customers can likewise fill in as a switch for work organizing, the equipment plat-structure and programming for them can be a lot more straightforward than those for work switches. For instance, correspondence conventions for work customers can be light-weight, portal or scaffold capacities don't exist in work customers, just a solitary remote interface is required in a work customer, etc. Notwithstanding cross section organizing among work switches and work customers, the passage/connect functionalities in work switches empower the coordination of WMNs with different systems. Customary hubs outfitted with remote system interface cards (NICs) can associate legitimately to WMNs through remote work switches. Clients without remote NICs can get to WMNs by associating with remote work switches through, for instance, Ethernet. Therefore, WMNs will significantly assist clients with being consistently on-line anyplace, whenever. Therefore, rather than being another sort of impromptu net-working, WMNs expand the abilities of specially appointed systems. This element carries numerous preferences to WMNs, for example, low straightforward cost, simple system support, heartiness, solid administration inclusion, and so forth. Thusly, notwithstanding being generally acknowledged in the customary application divisions of specially appointed net-works, WMNs are experiencing quick commercialization in numerous other application situations, for example, broadband home net-working, network organizing, building mechanization, rapid metropolitan territory systems, and endeavor organizing. Until now, a few organizations have officially understood the capability of this innovation and offer remote work arrangeing items. A couple test beds have been built up in university examine labs. Notwithstanding, for a WMN to be everything it tends to be, significant research endeavors are as yet required. For instance, the accessible MAC and steering conventions are not adaptable; throughput drops essentially as the quantity of hubs or bounces in WMNs increments. Hence, existing conventions should be upgraded or re-created for WMNs. Specialists have begun to return to the convention structure of existing remote systems, particularly of IEEE 802.11 systems, impromptu systems, and remote sensor systems, from the point of view of remote work organizing. Mechanical measures

gatherings, for example, IEEE 802.11, IEEE 802.15, and IEEE 802.16, are all effectively working on new determinations for WMNs.

In this article we present an overview of late advances in conventions and calculations for WMNs. Our point is to give a superior comprehension of research difficulties of this rising innovation. The remainder of this article is sorted out as pursues. The system models of WMNs are first displayed, with a goal to feature the qualities of WMNs and the basic components affecting convention plan. An investigation on late advances of WMNs is then completed, with an accentuation on open research issues. The article finishes up with conclusive comments.

System Architecture and

Basic Design Factors

System Architecture

The design of WMNs can be grouped into three kinds:

Framework/Backbone WMNs. In this engineering, work switches structure a foundation for customers, as appeared in Fig. 1, where dashed and strong lines show remote and wired connections, individually. The WMN foundation/spine can be fabricated utilizing different kinds of radio advancements, notwithstanding the for the most part utilized IEEE 802.11 advances. The work switches structure a work of self-designing, self-recuperating joins among themselves. With door usefulness, work switches can be associated with the Internet. This methodology, likewise alluded to as framework fitting, gives a spine to ordinary customers and empowers incorporation of WMNs with existing remote systems, through portal/connect functionalities in work switches. Traditional customers with an Ethernet interface can be associated with work switches through Ethernet joins. For conven-tional customers with indistinguishable radio advances from work switches, they can straightforwardly speak with work switches. In the event that diverse radio advancements are utilized, customers must communi-cate with their base stations that have Ethernet associations with work switches. Customer WMNs. Customer cross section gives shared net-works among customer gadgets. In this kind of design, customer hubs comprise the real system to perform steering and arrangement functionalities just as giving end-client applications to clients. Consequently, a work switch isn't required for these sorts of systems. In this way, a Client WMN is really equivalent to a regular impromptu system. Nonetheless, the prerequisites on end-client gadgets is expanded when contrasted with framework fitting, since in Client WMNs the end-clients must play out extra capacities, for example, steering and self-arrangement. Mixture

WMNs. This engineering is the blend of foundation and customer coinciding, as appeared in Fig. 2. Work customers can get to the system through work switches just as straightforwardly coinciding with other work customers. While the infra-structure gives availability to different systems, for example, the Internet, Wi-Fi, WiMAX, cell, and sensor arranges, the directing abilities of customers give improved network and inclusion inside WMNs.

The attributes of WMNs are laid out beneath, where the half and half engineering is considered for WMNs, since it com-prises every one of the upsides of WMNs:

- WMNs bolster specially appointed systems administration, and have the capacity of self-framing, self-recuperating, and self-association.
- WMNs are multi-bounce remote systems, however with a remote foundation/spine given by work switches.
- Mesh switches have insignificant portability and perform devoted steering and design, which fundamentally diminishes the heap of work customers and opposite end hubs.
- Mobility of end hubs is bolstered effectively through the wire-less foundation.
- Mesh switches coordinate heterogeneous systems, including both wired and remote. Consequently, various kinds of system access exist in WMNs.
- Power-utilization limitations are distinctive for work switches and work customers.
- WMNs are not remain solitary and should be good and interoperable with different remote systems.

Subsequently, WMNs expand the capacities of specially appointed net-works rather than basically being another kind of impromptu system. These extra capacities require new calculations and structure standards for the acknowledgment of WMNs.

**Basic Design Factors**

The basic components affecting the exhibition of WMNs are abridged as pursues.

Radio Techniques.

Numerous methodologies have been proposed to expand limit and adaptability of remote frameworks as of late. Common models incorporate directional and shrewd reception apparatuses, various information different yield (MIMO) frameworks, and multi-radio/multi-channel frameworks.

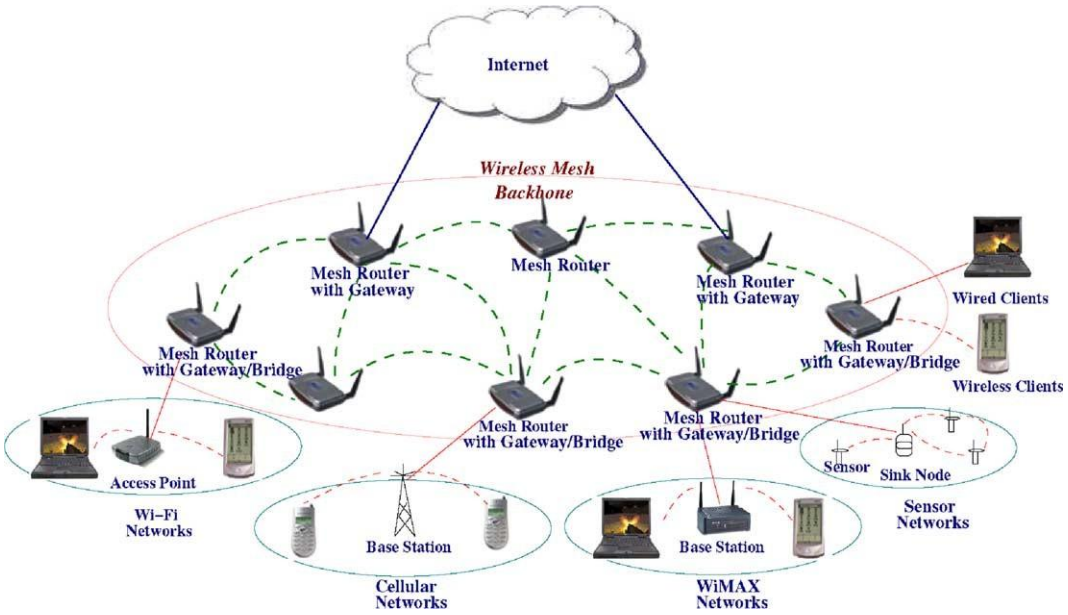
To further improve the presentation of a remote radio and control by higher layer conventions, further developed radio innovations, for example, reconfigurable radios, recurrence deft/subjective radios, and even programming radios, have been utilized for remote correspondence. In spite of the fact that these radio tech-nologies are still in their early stages, they are relied upon to be the future stage for remote systems because of their dynamic control capacity. These propelled remote radio advances all require a progressive plan in higher-layer conventions, particularly MAC and steering conventions.

Adaptability.

Adaptability is a basic prerequisite of WMNs. Without help of this component, the system execution debases fundamentally as the system size increments. For instance, steering conventions will most likely be unable to locate a dependable directing way, transport conventions may free associations, and MAC conventions may encounter huge throughput decrease. To guarantee the adaptability in WMNs, all conventions from the MAC layer to the application layer should be scal-capable.

Work Connectivity. Numerous favorable circumstances of WMNs start from work network. To guarantee solid work availability, arrange self-association and topology control calculations are required. Topology-mindful MAC and steering conventions can sig-nificantl y improve the exhibition of WMNs.

Broadband and QoS. Not quite the same as traditional impromptu net-works, most uses of WMNs are broadband administrations with heterogeneous QoS necessities



## LITERATURE SURVEY

Ajesha Patel and AnuragJain(2015) defined a study of various Black Hole Attack techniques and IDS in MANET.Mobile Ad Hoc Network (MANET) is said to be as a group of wireless mobile nodes vigorously forming a impermanent network that does not use any accessible heterogeneous network infrastructure. In this period of wireless devices, Mobile Ad-hoc Network (MANET) has become an inseparable element for communication for mobile device. Consequently, significance in research of Mobile Ad-hoc Network has been growing since last few years

PrachiGoyal and ChitvanGupta(2016) find an approach for Security Measures of Black Hole Attack in MANET. Mobile Ad Hoc Network (MANET) is a major next generation wireless technology which is mostly used in future. MANET is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predefine organization of available links. In a MANET mobile node will be increases and moveable, so that attacker will be attack by a malicious node which brings great challenges to the security of Mobile Ad Hoc network. The Black hole attack is one of such security issue in MANET.

JunhaiLuo, Mingyu Fan, and DanxiaYe(2008) presented Black Hole Attack Prevention Based on Authentication Mechanism. The black hole attack is one of the security attacks that occur in Mobile Ad-hoc Networks (MANETs). In the attack, a malicious node exploits the routing protocol to advertise itself as having the shortest path to the node whose data packets it wants to intercept. In this paper, the black hole problem is addressed.

Nigahat and Dr. Dinesh Kumar(2017) has defined a work on robust security solution.Security is a major concern for protected communication between mobile nodes in a hostile environment. In hostile environments adversaries can bunch active and passive attacks against intercept able routing in embed in routing message and data packets. In this paper, we focus on Black Hole attack in Mobile ad hoc networks. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers.

T.Manikandan, S.Shitharth, C.Senthilkumar, C.Sebastinalbina, N.Kamaraj(2014) “Removal of Selective Black Hole Attack in MANET by AODV Protocol”**.**MobileAdHoc networks are self-configuring and self-organizing multi-hop wireless networks. A mobile Adhoc Network (MANET) is a collection of autonomous mobile users communicating over bandwidth

constrained wireless links. Due to the mobile nodes, the topology of the network keeps changing unpredictably and rapidly over time. A selective black hole attack on MANET refers to an attack by a malicious node, which forcibly acquires the route from source to a destination by the falsification of sequence number and hop count of the routing message.

Kavi Joshi, Er. ManojKumar(2016) find three way techniques for Preventing Black Hole Attack in MANET Using AODV Protocol. Mobile Ad-hoc Networks (MANET) are acquiring popularity today, as it offers wireless connectivity to the user irrespective of their geographical position. An Ad-hoc network does not have a centralized infrastructure. It is a wireless network where nodes communicate with each other through multiple hops. If nodes in the ad-hoc network changes there position dynamically, it is called Mobile ad-hoc network (MANET).

EiEiKhin andThandarPhy(2014) has explores the impact of blackhole attack on aodv routing protocol. A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes that dynamically self-organize to form an arbitrary and temporary network. The mobile nodes can communicate with each other without any fixed infrastructure. MANET can be set up quickly to facilitate communication in a hostile environment such as battlefield or emergency situation. The various severe security threats are increasing on the MANET. One of these security threats is black hole attack which drops all received data packets intended for forwarding. In this paper, we are simulating and analyzing the impact of black hole attack on Ad Hoc On-Demand Distance Vector (AODV) protocol.

RajibDas(2012) has defined a work on Security Measures for Black Hole Attack in MANET: An Approach. A Mobile Ad-Hoc Network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on continual basis.

NakkaNandini, ReenaAggarwal(2015) has provided the Prevention of black hole attack by different methods in MANET.An ad-hoc network is a temporary infrastructure less network which is a collection of mobile nodes in the dynamically form. This network is always independent and a isolated network. Due to the limitation power and mobility there is less sufficiency among them. In these wireless networks, the main things like confidentiality, availability authentication, anonymity, integrity to all the users of mobile communication.

Jaspal Kumar, M. KulkarniDayaGupta(2013) “Effect of Black Hole Attack on MANET Routing Protocols”. Due to the massive existing vulnerabilities in mobile ad-hoc networks, they

may be insecure against attacks by the malicious nodes. In this paper we have analyzed the effects of Black hole attack on mobile ad hoc routing protocols. Mainly two protocols AODV and Improved AODV have been considered. Simulation has been performed on the basis of performance parameters and effect has been analyzed after adding Black-hole nodes in the network.

Arshdeepkaurand Mandeepkaur (2015) has proposed a ssurvey on black hole attack on manet.The black hole attack is single of the well known safety intimidation in wireless mobile ad hoc networks. The intruder operates the get-out to carry out their spiteful behaviors since the route finding development is compulsory and foreseeable.

MANET is a wireless network formed by collection of mobile nodes without the preset infrastructure. When network topology changes nodes in range is still connected. The major shortcoming is their limited bandwidth, memory, processing capabilities and open medium and so these are more prone to malicious attacks [8]. Manet is flexible and maintains the connectivity between devices when a node moves from one location to another. Another property is neighbor and route discovery so that the data can be routed from source node to neighboring node till it reaches to the destination.

It has a wide usage. That's why there are several open issues about it, such as security threats, finite bandwidth, malicious broadcasting messages, reliable data delivery, dynamic path establishment and limited hardware. The security threats have been discussed and investigated in the wired and wireless network [4].

Routing protocol is principally a standard that decide the behavior of the node in the context to route the data packet from one node to another. Routing protocol can be classified as link state protocol and distance vector protocol. Link state protocol build the topology of the entire network for calculating routes and then calculate the best path. These protocols consume more power and memory resources. DLSR and OLSR are examples of such protocols. While in distance vector protocol router keeps information of their neighbors only and calculates the cost based on it. AODV is the example of this type of protocol.

Based on another classification routing protocols are of three types: Proactive, Reactive and Hybrid. In Proactive routing protocol each node maintains routing table periodically and therefore also known as table driven protocol. OLSR is one of the example of it. In Reactive routing protocol route is only determined when it is required and therefore it is also known as On

Demand routing protocol. AODV and DSR are the example of it. Hybrid routing protocol as the name suggests is a combination of Proactive and Reactive routing. Initially proactive routing is used to gather the unfamiliar routing information and then the reactive routing is used to maintain the information when network topology changes. Zone Routing Protocol (ZSR) is one of the hybrid protocols.

In rest of the paper, Section 2 is introduces the classification and definition of attacks. Section 3 briefly discussed about the literature review on detection and prevention of security attacks. Finally section 4 concludes the paper.

Attacks in MANET can be classified as Active and Passive attacks. An **Active attack** is one in which an attacker which is an authorized node destroy or alter the data that is being exchanged in the network. While a **Passive attack** attacker node which is an unauthorized node get the data without disrupting or damaging the network operation. Another classification can be External and Internal attacks. In **External attack,** the attacker node is one which does not belong to the network while in **Internal Attacks** the attacker node belongs to the network. Internal attacks are more severe than external attacks since attacker knows all secret information and have privileged access rights. Many security issues such as snooping attacks, wormhole attacks, black hole attacks [8], routing table overflow, poisoning attacks, packet replication and denial of services attack (DoS) have been studied in recent years.

Attacks can be classified on layered basis. Each layer undergoes different kind of attacks. Table 1 shows different kinds of attack.

**Table 1. Types of attacks on layers**

| **Layers** | **Attacks** |
|---|---|
| Physical layer | Jamming, Interception, eavesdropping |
| Data link layer | Traffic Analysis, monitoring |
| Network layer | Wormhole, black hole, Gray hole, message tempering, flooding, Resource consumption, location disclosure attack |
| Transport layer | Session Hijacking, SYN flooding |
| Multiple layer | Denial of services(DoS), Man in the middle attack |

A**attacks in Adhoc Networks:**

In this kind of attack, a malicious node participate in route discovery mechanism by sending RREP message that includes the highest sequence number and this message is perceived as if it coming from the destination or from a node which has a fresh enough route to the destination[6]. The source then starts to send out its data packets to the black hole trusting that this packet will reach the destination. As soon as the data transmission starts, malicious nodes drop the packets that are needed to be forwarded to the destination. Black hole is more destructive as compared to gray hole attack.

In this attack, a malicious node does not participate in route discovery mechanism that is initiated by other nodes and is therefore not a part of active route. Such nodes would increase the route discovery failure and harm the overall network performance [5]. Another intention of such attacker is to conserve their energy by interpreting the message intended for them only and otherwise they do not cooperate with other nodes, which ultimately degrade the performance of network.

**Message Tempering**

In this kind of attack an intermediate node behaving as malicious node delete or add some bytes in the data packet received by him to forward to the destination. This change in data may cause abnormalities or destruction in network.

**Worm hole attack** is the attack a malicious node receives packet at one location in the network and tunnels them to another location in the network, where these packets are resent into the network [2]. Due to broadcast nature of radio channel the attacker may create a wormhole for those packets also that does not belong to him.

**Conclusions**

The world is changing the way it is operation currently and routine networks are playing an important role in it. It is a framework that makes an engineer's life easy while working on large sets of data. WWS has been very effective solution for companies dealing with the data in petabytes. It has solved many problems in industry related to huge data management and distributed system. As it is open source, so it is adopted by companies widely. The capacity of self organization in WMN.reduces the complexity of networks and maintenance. The capacity of self organization also provides user to access internet anywhere anytime.are based on direct and indirect or recommendation values from nodes of the networks and this trust information is incorporated with traditional security methods such as certificate and key

management. These kinds of systems are quite useful to improve numerous effects in the network such as routing efficiency, scalability, trust, reduce the search traffic, and reduce the processing overhead and memory. Simulation experiment executed using Network Simulator 2 (NS2) and under various network conditions show that localization trust technique results are superior as compared to AODV, TSQRS, ETRS-PD. QoS trust parameters security and quality of service routing in terms of overhead, packet delivery ratio and energy consumption.

**References**

[1] Hizbullahkhattak, Nizamuddin, FahadKhursid, "Preventing Black and Gray hole attack in AODV using optimal path and routing hash"

[2] G. Indiriani, Dr. K. Selvakumar, "Intrusion detection and defense mechanism for packet replication attack over MANET using Swarm Intelligence," pattern recognition, informatics and mobile engineering.

[3] SapnaGambhir and Saurabh Sharma, "PPN: Prime Product Number Based Malicious node Detection scheme for MANETs" International advance computing conference (IACC).

[4] Pramod Kumar Singh, Govind Sharma, "An Efficient prevention of black hole problem in AODV Routing protocol", 11th international conference on trust, security and privacy in computing and communication.

[5] Mohammed SaeedAlkatheiri, Jianwei Liu, Abdul Rashid Sangi, "AODV routing protocol under several routing attacks in MANETs" 2011 IEEE.

[6] RoopalLakhwani, Vikram Jain, "Detection and Prevention of black hole attack in Mobile ad hoc network" International Journal of Computer Application.

[7] Umang S, Reddy BVR, Hoda MN, "Enhanced intrusion Detection System for malicious node detection in ad hoc routing protocol using minimal energy consumption" IET Communication.

[8] Rutvij H. Jhaveri, " MR-AODV: A solution to mitigate black hole and gray hole attacks in AODV based MANETs" Third International Conference on Advanced Computing and communication technologies.

[9] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences 2011.