A Review of Routing Protocols and Attacks in Mobile Ad-hoc Network

[1]S. Anusuya, [2]Dr. S.Meenakshi

[1]Research Scholar, Department of Computer Science, Gobi Arts & Science College, Tamilnadu, India.
[2]Associate Professor in Computer Science, Gobi Arts & Science College, Tamilnadu, India.

Abstract -

A Mobile Ad-hoc Network (MANET) is a group of wireless mobile devices or nodes that communicate with each other without any help of a pre-installed infrastructure and centralized access points. The mobility and the easy use of mobile devices have motivated researches, to develop MANET protocols to exploit a reliable communication facilities provided by these devices. There are number issues such as medium access control, routing, resource management, congestion control and power control which affects the reliability of secured communication in MANET. Routing is an important issue in MANET since the establishment of effective communication between nodes is a challenging task due to the dynamic network topology. Routing is the process of selecting paths in a network to transmit data packets from one node to another node in the network. Due to the lack of a predefined centralized administration for route discovery process which leaves MANET vulnerable to attacks, that results in degradation in the performance of the network. The development of an effective routing protocol to prevent against various attacks in MANET is important for secured transmission of data between mobile nodes. This research paper reviews various attacks posed on routing and existing routing protocols to provide secure transmission of data between nodes in mobile ad-hoc networks.

***Index Terms* - MANET, routing attacks, routing protocols, security.**

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without any predefined infrastructure or centralized administration [1]. MANETs are collections of self-organizing and self-configuring multichip wireless networks, where the structure of the network changes dynamically. MANETs offer several advantages over traditional networks including reduced infrastructure costs, ease of establishment and fault tolerance. MANET is completely different from other network since it provides various characteristics such as dynamic topology, node mobility and self-organizing capability. MANET is used in applications such as data network, device network, virtual classroom, disaster recovery, sensor networks, automated battlefields, emergency relief scenarios and other security sensitive computing environment. Due to the dynamic configuration, the field of MANET is rapidly growing and changing. The various issues that need to be faced by the designer of the MANETs are resource constraints, cooperation and secure communication between dynamic mobile nodes [2]. In order to carry out secure and effective communication within a MANET, an efficient routing protocol is required to discover routes between mobile nodes.

Routing is an important issue in MANET since efficient route establishment between pair of nodes is important for delivering messages in time. Routing is the process of forwarding packets from source to destination using most efficient route. All the Efficiency of the route is measured in various metric like number of hops, traffic and security [4]. The goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency.

The infrastructure less and the dynamic nature of MANET demands secured routing strategies for reliable communication between mobile nodes. Due to the lack of a predefined centralized administration for route discovery process which leaves MANETs vulnerable to attacks, that results in degradation in the performance of the network. Attacks disturb routing operations which create many problems such as denial of service, jamming the network. To preserve the security of MANETs from attacks, a routing protocol should satisfy certain sort of requirements to ensure proper functioning of the path from source to destination in presence of malicious nodes.

In MANET, routers are free to move randomly and organize themselves arbitrarily and the

ISSN: 2278 – 1323

information is exchanged and updated dynamically from time to time [7]. The lack of centralized management makes each wireless node in the MANET to perform routing to its neighbours in order to maintain the connectivity and the network stability. Thus specially configured routing protocols are required to ensure both connectivity and security to achieve the network stability for secured communication in a MANET.

Developing a routing protocol for MANET has been a challenging task due to the various characteristics of MANET such as: dynamic change in the network topology because of mobility of nodes, resource constraints, limited bandwidth and limited battery power [17]. Thus the main goal of routing protocol is to correctly establish a route between a pair of nodes to deliver a message in correct time with minimum overhead and maximum network throughput. In order to achieve this goal a number of routing protocols have been developed for secured routing in MANET.

This research paper reviews various attacks posed on routing and routing protocols to achieve a secure transmission of data between mobile nodes in MANETs. The structure of this paper is organized as follows. Section II describes the routing attacks in MANET. Section III presents the existing MANET routing protocols. Section IV concludes this research paper.

II. ROUTING ATTACKS

Security is one of the challenging issues for secure transmission of the data in MANETs. A secure MANET environment should provide confidentially, integrity, authenticity, availability and non-repudiation. The vulnerabilities that make MANETs highly insecure are: dynamic nature of wireless communication, node security and tampering, limited power in nodes and absence of infrastructure.

Understanding the form of attacks is always the primary step towards the secured communication between mobile nodes. MANETs are unsecure from various attacks. The attacks in MANET are done in order to interrupt the communication or to steal the information. A number of attacks affect the safe exchange of information in MANETs, which can be categorized using different criteria. The various types of attacks Wormhole attack

that affect MANET communication and its security can be classified into two types: passive attacks and active attacks [3].

Passive attacks

In a passive attack an unauthorized node continuously monitors the network and attempt to learn the information from the network. The attacker analyzes network traffic and does not try to modify or change the data packets. A Passive attack does not disturb the operation of the routing protocol. In passive attacks, the attacker eavesdrop the traffic and extract the valuable information without damaging the network. Passive attacks are usually difficult to detect and it can be prevented using various encryption mechanisms. The various passive attacks posed on routing protocols are eavesdropping, traffic analysis, traffic monitoring and snooping.

Active attacks

Active attacks disturb the functionality of the network. Active attacks actively alter the data such as message modifications, message replays and message fabrications. In active attacks, the malicious nodes can disturb the correct functioning of a routing protocol such as modification of routing information, impersonating other nodes and false routing information between nodes. An active attack injects arbitrary packets and tries to disrupt the operation of the routing protocol. Active attacks are carried out at routing level either be external or internal. The goal of this attack is to attack all packets and disable the network. An active attack causes various problems in routing such as increase latency of particular packets, divert packets to affect link bandwidth and decrease overall network throughput [10].

Apart from the basic attacks prevailing in MANETs, there are a variety of other threats which are divided into two categories: threats to network mechanism and threats to security mechanism. Recently various network layer targeted attacks have been identified. As a consequence of attacking network layer routing protocols, adversaries can easily disturb and absorb network traffic, inject themselves into the selected data transmission path between the source and destination. The following are the various network layer attacks related with the routing protocols [5].

In wormhole attack, two malicious nodes make a tunnel between them and the tunneling is

ISSN: 2278 – 1323

called as wormhole. An attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The worm hole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location based wireless security system. The occurrence of wormhole attack causes packet drop, listening of confidential information between nodes, alteration of transferred data packets For example, most existing ad hoc network routing protocols, without some against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication [6].

Grey hole Attack

Grey hole attack is a kind of Denial of Service (DoS) attack in mobile ad hoc networks. It is specialized type of black hole attack which changes its states from honest to malicious and vice versa. Grey hole attack is an event that degrades the overall networks performance by intentional malicious activity. In grey hole attack the data packets are dropped selectively or in statistical manner. For instance they may drop packets from a particular node or in some other pattern. This type of attacks is more difficult to detect/prevent compared to black hole attack [16].

Sybil Attack

The sybil attack in computer security is an attack where in a reputation system is forging identities in peer –to-peer networks. In a sybil attack the attacker subverts the reputation system of a peer –to-peer network by creating a large number of pseudonymous identities, using them to gain a disproportionately large influence. A reputation system vulnerability to a sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trusted entity, and whether the reputation system threats all entities identically. Evidence shows large –scale Sybil attack can be carried out in a very cheap and efficient way in realistic systems [11].

Byzantine Attack

Byzantine attack means that attackers may modify the coded packets. In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behavior [10].

Routing Table Overflow

In this type of attack, an adversary node advertise routes to non –existent nodes, to the authorized nodes present in the network. The main objective of such an attack is to cause an overflow of the routing tables, which would in turn prevent the creation of entries corresponding to new routes to aututhorized nodes. Proactive routing protocols are more vulnerable to this attack compared to reactive routing protocols. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation [15].

Black hole attack

Black hole Attack is one of the major attacks in MANETs mainly for proactive & reactive type of routing protocols Black hole attack is an active attack. Black hole attack can also be called as packet drop attack since it drops many packets. This attack stops the forwarding of data packets. If there is a malicious node, it keeps waiting for its neighbor node to initiate RREQ (Route Request) packet. As a node receives the RREQ packet, it will send a false RREP (Route Reply) packet instantly with a modified high sequence number. So that the source node will assume that there is a new route is available towards the destination. The source node ignores the RREP packet from the other nodes including the accurate nodes where it automatically denies the other nodes and it will start sending the packets towards the malicious nodes [5].

The occurrence of attacks results in degrations in the performance of the networks. The above attacks disturb routing operations which create many problems for secured transmission of data in MANET. To preserve the security of

ISSN: 2278 – 1323

MANET from the above attacks routing protocols are important to ensure proper functioning of the path from source to destination in the presence of malicious nodes. A number of secure routing protocols have been developed to prevent the attacks on the routing and those routing protocols are discussed in the next sections.

III. MANET ROUTING PROTOCOLS

Routing is the process of selecting paths in a network to transmit data packets from one node to another node in the network .Routing in MANETs is an important issue since collaboration between nodes is required to relay packets on behalf of one another. A number of routing protocols have been developed to perform routing in MANET. A routing protocol is a standard that controls flow of data packets in the network and also decide that which path should be followed by the packets to the reach the particular destination [1].

In order to preserve the security of MANETs from attacks, a routing protocol must fulfil certain requirements to ensure proper functioning of the path from source to destination in presence malicious nodes are i) authorized nodes should perform route computation ii) Minimal exposure of network topology iii) Detection of spoofed routing messages iv) Detection of fabricated routing messages v) Detection of altered routing messages vi) Avoiding formation of routing loops vii) Prevent redirection of routes from shortest paths. A number of secure routing protocols have been developed that conform to most of the above requirements.

A preliminary classification of the routing protocols can be done via the type of cast property such as Uncast, Broadcast, Multicast protocols. Uncast refers a communication to describe a piece of information to send from one point to another. There are only sender and receiver. All LANs support Uncast transfer mode and most applications that employ TCP transport protocol use Uncast messaging. Broadcast describes communication that is sent a piece of information from one point to all other points. There is one sender and multiple receivers. All LANs support broadcast transmission [7]. Multicast communicates a piece of information sent from one or more points to a set of other points. The senders and receivers are one or more.

MANET routing protocols can be categorized into three major groups such as: A) Proactive or Table driven, B) Reactive or On-demand and C) Hybrid based on the routing strategy [4]. This section describes the various routing protocols proposed under this classification as shown in Fig.3.1

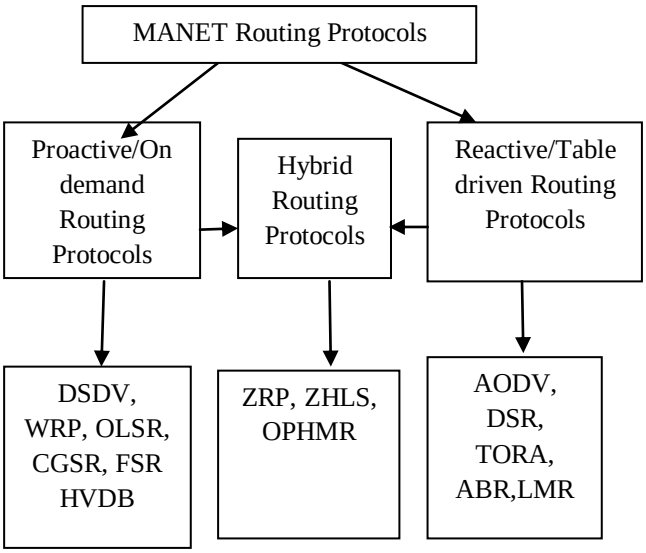

Fig.3.1 Classification of MANET Routing Protocols

A) Proactive or Table driven Routing protocols

In proactive routing protocol, routes to a destination are determined when a node joins the network or changes its location, and are maintained by periodic route updates. This protocol maintains routes between nodes in the network at all times, even when the routes are not currently being used. Updates to the individual links within the networks are propagated to all nodes or a relevant subset of nodes, in the network such that all nodes in the network eventually share a consistent view of the state of the network. Thus in proactive routing scheme every node continuously maintains complete routing information of the network. This information is stored in tables. Each node maintains a routing table which contains the list of destinations and routes.

The advantage of this protocol is that less latency involved when a node wishes to begin communicating with an arbitrary node that it has not yet been in communication with. Since these protocols rely upon maintaining routing tables of known destinations, however routing tables must be kept up-to-date; The disadvantage of this protocol is that the control message overhead of maintaining all routes within the network can

ISSN: 2278 – 1323

rapidly increase the capacity of the network. Thus this routing protocol is not suitable for highly dynamic networks because increased control message overheads can degrade network performance at high loads. Also this protocol wasting the bandwidth and memory since it periodically sends update messages to neighbours, even when no traffic is present**.** The various existing proactive routing protocols are the following:

- Destination Sequenced Distance Vector routing (DSDV)

Perkins and Bhagwat [20] have proposed a distance vector routing protocol that ensures a loop-free routing by tagging each route table entry with a sequence number and is based upon the Bellman-Ford algorithm to calculate the shortest number of hops to the destination. Byzantime attack and novel broken attack are occurred in this protocol. However DSDV prevents the black hole attack. Each DSDV node maintains a routing table which stores destinations, next hop addresses and number of hops as well as sequence numbers. Routing table updates are sent periodically as incremental dumps limited to a size of one packet containing only new information.

- Wireless Routing Protocol (WRP)

Murthy & Garcia-Luna-Aceves [18] have proposed a distance vector routing protocol that aims to reduce the possibility of forming temporary routing loops in mobile ad-hoc networks. This protocol is table-based that inherits the properties of Bellman-Ford algorithm similar to DSDV. The main goal of this approach is to maintain the routing information among all nodes in the network based on the shortest distance to every destination. WRP is a loop free routing protocol.

WRP belongs to the class of path-finding algorithm with an exception of avoiding the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbours. Each node in the network uses a set of four tables such as Distance table (DT), Routing table (RT), Link-cost table (LCT), Message retransmission list (MRL) table to maintain accurate information. Also the nodes send update messages to their neighbours in case of link failure between two nodes. In this protocol stealthier attack are occurred and black hole attack are prevented.

- Optimized Link State Routing (OLSR)

Clausen and Jacquet [8] have proposed a point-to-point proactive protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying. This protocol optimizes the pure link state routing based on two ways. One is by reducing the size of the control packets and the other is by reducing the number of links used for forwarding the link state packets. Link spoofing attack, Denial of Service (DoS) attack are occurred in this protocol. However OLSR prevents the wormhole attack, black hole attack. Here each node maintains the topology information about the network by periodically exchanging link-state messages among the other nodes. OLSR detects the changes in the neighborhood of node based on neighbor sensing. Each node determines an optimal route to every known destination using the shortest-path algorithm and stores this information in a routing table.

- Cluster Gateway Switch Routing protocol (CGSR)

Chiang et al., [9] have proposed a typical cluster based hierarchical routing. A stable clustering algorithm Least Cluster head Change (LCC) is used to partition the whole network into clusters and a Cluster head is elected in each cluster. A mobile node that belongs to two or more clusters is a gateway connecting the clusters. Data packets are routed through paths having a format of Cluster head Gateway between any source and destination pairs.

The major advantage of CGSR is that it can greatly reduce the routing table size comparing to Distance Vector protocols. CGSR considers a clustered mobile wireless network instead of a flat network. For structuring the network into separate but interrelated groups, cluster heads are elected using a cluster head selection algorithm. By forming several clusters, this protocol achieves a distributed processing mechanism in the network. In this Protocol Eavesdropping, Spoofing attacks are occurred and Denial of Service Attack are prevented. However, one drawback of this protocol is that, frequent change or selection of cluster heads might be resource hungry and it might affect the routing performance. CGSR uses DSDV protocol

ISSN: 2278 – 1323

as the underlying routing scheme and, hence, it has the same overhead as DSDV.

- Fisheye State Routing (FSR)

Pei et al., [19] have proposed a proactive unicast routing protocol based on Link State routing algorithm with effectively reduced overhead to maintain network topology information. As indicated in its name, FSR utilizes a function similar to a fish eye. The eyes of fishes catch the pixels near the focal with high detail, and the detail decreases as the distance from the focal point increases. Similar to fish eyes, FSR maintains the accurate distance and path quality information about the immediate neighboring nodes, and progressively reduces detail as the distance increases. Link State routing algorithm is used for wired networks.

In Link State routing, link state updates are generated and flooded through the network whenever a node detects a topology change. In FSR, however, nodes exchange link state information only with the neighboring nodes to maintain up-to-date topology information. FSR is an improvement of GSR. In this protocol flooding attack are occurred. The large size of update messages in GSR wastes a considerable amount of network bandwidth. In FSR, each update message does not contain information about all nodes.

- Hypercube-based Virtual Dynamic Backbone protocol (HVDB)

Luo Junhai et al., [14] have proposed a proactive, Quality of Service-aware and hybrid multicast routing protocol for large scale MANETs. Transient Ischemic Attack (TIA) are occurred in this protocol. Due to the regularity and symmetry properties of hypercube, no leader is needed in a logical hypercube, and every node plays almost the same role except for the slightly different roles of border cluster heads and inner cluster heads. Thus, no single node is more loaded than any other nodes, and no problem of bottlenecks exists, which is likely to occur in tree-based architectures.

B) Reactive or On-demand Routing Protocols

In reactive routing protocols routes are discovered when needed and expire after a certain period of time. In this approach a route discovery process is invoked, when a node wishes to communicate with another node for which it has no route table entry. When a route is discovered, it is maintained only for as long as it is needed by a route maintenance process. Thus the reactive routing protocols are based on some sort of query-reply dialog. In this routing, the nodes do not need periodic transmission of topological information of the network. When there is a need for a route to a destination, route request messages are flooded periodically with new networks status information. Every node in this routing protocol maintains information of only active paths to the destination nodes.

The advantage of this protocol is that the nodes do not need periodic transmission of topological information of the network. When there is a need for a route to a destination, route request messages are flooded periodically with new networks status information. Every node in this routing protocol maintains information of only active paths to the destination nodes. Reactive protocols have the advantage of being more scalable than table-driven protocols. Thus this approach requires less control traffic to maintain routes that are not in use than in table-driven methods. The disadvantage of this protocol is that an additional latency is incurred in order to discover a route to a node for which there is no entry in the route table. The various existing proactive routing protocols be following

- Ad-hoc On-demand Distance Vector Routing (AODV)

Perkins and Royer [21] have proposed a widely accepted on-demand routing protocol which is a combination of both DSR and DSDV. This protocol follows the basic on-demand mechanism of route discovery and route maintenance from DSR and use hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. AODV uses destination sequence numbers to ensure loop freedom at all times and by avoiding the Bellman-Ford count-to infinity problem offers quick convergence when the ad hoc network topology changes. This protocol finds routes only when required and hence AODV is reactive in nature. In this protocol grey hole attack, sybil attack and wormhole attack are occurred. Flooding attack and black hole attacks are prevented.

- Dynamic Source Routing (DSR)

Johnson et al., [13] have proposed DSR is an on-demand protocol to restrict the bandwidth consumed by control packets in ad hoc wireless

ISSN: 2278 – 1323

networks by eliminating the periodic table update messages required in the proactive routing protocols. The two basic parts of DSR protocol are route discovery and route maintenance and its distinguishing feature is the use of source routing.

In DSR, every node maintains a cache to store recently discovered paths. When a node wants to send a packet, it first checks the cache whether there is an entry for that. If yes, then it uses that path to transmit the packet. Also it attaches its source address on the packet. Grey hole attack and worm hole attack are occurred in this protocol. However DSR prevents the black hole attack and grey hole attack.

If there is no entry in the cache or the entry is expired, the sender broad casts a route request packet to all its neighbours asking for a path to the destination. Until the route is discovered, the sender host waits. When the route request packet arrives to any other nodes, they check whether they know the destination asked. If nodes have route information, they send back a route reply packet to the destination otherwise they broadcast the same route request packet.

- Temporally Ordered Routing Algorithm (TORA)

Vincent Park [25] have proposed a highly adaptive loop free distributed routing algorithm based on the concept of link reversal. It is designed to minimize reaction to topological changes. A key design concept in TORA is that it decouples the generation of potentially far reaching control message from the rate of topological changes. Messaging is typically localized to a very small set of nodes need the changes without having to result to a dynamic hierarchical routing solution with added complexity. TORA protocol occurred attacks such as internal and external attacks. Route optimality is considered of secondary importance and longer routes are often used if discovery of newer routes could be avoided.

- Associativity Based Routing (ABR)

Sunil Taneja and Ashwani Kush [23] have proposed a new type of routing metric and degree of association stability for MANET. In this routing protocol, a route is selected based on the degree of association stability of mobile nodes. Each node periodically generates beacon to announce its existence. Upon receiving the beacon message, a neighbor node updates its own associativity table. ABR Protocol Occurred attacks such as black hole and sybil attack. For each beacon received, the associativity tick of the receiving node with the beaconing node is increased. A high value of associativity tick for any particular beaconing node means that the node is relatively static. Associativity tick is reset when any neighboring node moves out of the neighborhood of any other node.

- Light-weight Mobile Routing (LMR)

Muralishankar et al., [17] have proposed the concept of link reversal a reactive algorithm algorithm i.e. routes are established to the destination only when necessary. LMR addresses the issue of partitioned network by providing a link erasure mechanism. The LMR protocol can be divided into three separate phases. First the required routes must be built. That is called a construction phase. As changes happen in the topology, some routes must be re established (maintenance phase). Finally the routes are not needed anymore and the route destruction phase begins. Fabrication attack are occurred in this protocol. However it is assumed that the topology of ad hoc networks change quite frequently, which causes the invalid routes to be removed, separate destruction is not really needed. The maintenance phase takes care of the deletion of invalid routes. Thus, the two important phases of the LMR protocol are the construction and the maintenance phases.

C) Hybrid Routing Protocols

Hybrid routing protocols combined the features of both proactive and reactive routing protocols. This protocol attempts to exploit the reduced control traffic overhead from proactive systems and also reducing the route discovery delays of reactive systems by maintaining certain form of routing table. Zone Routing Protocol (ZRP) is an example of hybrid routing which employs a combination of proactive and reactive methods. This protocol maintains groups of nodes in which routing between members within a zone is via proactive methods, and routing between different groups of nodes is via reactive methods.

- Zone Routing Protocol (ZRP)

ISSN: 2278 – 1323

Haas and Pearlman [12] have proposed a hybrid routing protocol for mobile ad hoc networks which localizes the nodes into sub-networks or zones. It incorporates the merits of on-demand and proactive routing protocols and the network is divided into routing zones according to distances between mobile nodes. Within each zone, proactive routing is adapted to speed up communication among neighbours and the inter-zone communication uses on-demand routing to reduce unnecessary communication. ZRP protocol occurred attacks such as stealthier attack, jellyfish recorder attack and rushing attack .Prevented attacks are black hole attack and wormhole attack.

- Zone-based Hierarchical Link State (ZHLS)

Murthy & Garcia-Luna-Aceves [18] have proposed the mobile nodes are assumed to know their physical locations with assistance from a locating system like GPS. The network is divided into non-overlapping zones based on geographical information. In ZHLS protocol, the network is divided into non overlapping zones as in cellular networks. Black hole attack are occurred in this protocol. Each node knows the node connectivity within its own zone and the zone connectivity information of the entire network. The link state routing is performed by employing two levels: node level and global zone level.

- Optimized Polymorphic Hybrid Multicast Routing Protocol (OPHMR)

Luo Junhai et al., [14] have proposed a proactive, polymorphic energy efficient and hybrid multicast routing protocol. It attempts to benefit from the high efficiency of proactive behavior and the limited network traffic overhead of the reactive behavior, while being power, mobility, and vicinity-density aware. Denial of Service (Dos) attack are occurred in this protocol. The protocol is based on the principle of adaptability and multi-behavioral modes of operations. It is able to change behavior in different situations in order to improve certain metrics like maximizing battery life, reducing communication delays, improving deliverability. OPHMR defines four different behavioral modes of operation, two power level thresholds, one mobility level threshold and one vicinity density thresholds. Under the four different modes, the lifetime of its corresponding entry is also different. Power threshold determines the node's behavior in order to extend its battery life. Speed threshold is required to maintain better connectivity and awareness of the topology changes. Density threshold is considered when the mobility speed is high.

IV. CONCLUSION

Due to the dynamic configuration, the field of MANET is rapidly growing and changing. In order to carry out secure and effective communication within a MANET, an efficient routing protocol is required to discover routes between dynamic mobile nodes. In order to carry out the effective communication within a MANET, an efficient Routing protocols is required to prevent the packet loss and long delay between dynamic nodes. This research paper has given a review of various Routing algorithms in MANETs. The various routing protocols reviewed in this paper defend against routing at a certain level with limitations. Hence, further research is needed to develop effective routing algorithm to detect and control routing in MANETs for secured data transmission between mobile nodes.

ACKNOWLEDGMENT

I am grateful to Dr. S.Meenakshi, Assistant professor, Department of Computer Science, Gobi Arts & Science College, Tamilnadu, India.

REFERENCES

[1] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi, "A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)", *International Journal of Information and Education Technology,* Vol. 3, No. 1, February 2013.

[2] E. Alotaibi, B. Mukherjee, "A survey on routing algorithms for wireless Ad-Hoc and mesh networks", Computer Networks: The *International Journal of Computer and Telecommunications Networking*, Vol. 56, No. 2, pp. 940–965, October 2011.

[3] Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", *IEEE 15th International Conference on Computer Modeling and Simulation,* Vol.2,No.1,pp.930-945(UKSim), 2013.

[4] K. Anuj Gupta, Harsh Sadawarti, Anil K. Verma, "Review of Various Routing Protocols for MANETs" *International Journal of Information and Electronics Engineering,* Vol. 1, No. 3, November 2011.

[5] V. Athira Panicker, G. Jisha , "Network Layer Attacks and Protection in MANET A Survey", *International Journal of*

ISSN: 2278 – 1323

Computer Science and Information Technologies, Vol. 5, No. 3, pp. 3437-3443, 2014.

[6] Bounpadith, Kannhavong "A Survey of Routing Attacks in Mobile Ad hoc Networks" *IEEE/WCM (Wireless Contact Mointor)* transaction, ISSN : 1536-1284, Vol. 14, No. 5, October 2010.

[7] Charu Wahi, Sanjay Kumar Sonbhadra "Mobile Ad-Hoc Network Routing Protocols: A Comparative Study", *International Journal of Ad hoc, Sensor &Ubiquitious Computing (IJASUC)* Vol.3 No.2,April 2012.

[8] T.Clausen and P.Jacquet, "Optimized Link State Routing Protocol" *International Engineering Task Force (IETF)* October1996.

[9] C-C Chiang, H-K Wu, W .Liu, M .Gerla "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel". Proceedings of *IEEE SICON*, pp.197–211, 1997.

[10] Gangandeep, Aashima, Pawankumar, "Analysis of Different Security Attacks In MANETs on Protocol Stack A-Review", *International Journal of Engineering and Advanced Technology*, ISSN: 2249 – 8958, Vol. 1, No.5, June 2012.

[11] M. Girish Chandra ,S.G.Harish Reddy,Jaydip Sen "A Mechanism for Detection of Gray hole attack in Manets"Proceeding of the 6th *International Conference on Information, Communication and Signal Processing(ICICS 07)* Singapore December 2010.

[12] J.Haas and Marc R.Pearlman, "Zone Routing Protocol (ZRP) in Adhoc Networks" *International Engineering Task Force (IETF),* pp 470-485, January 1998.

[13] D. B. Johnson, DA.Maltz and J.Broch "Dynamic Source Routing Protocol (DSR)", *ACM Digital Library*, pp 210-215, October 1996.

[14] Luo Junhai, Ye Danxia, Xue Liu and Fan Mingyu, "A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks", *IEEE* Communications Surveys & Tutorials, Vol. 11, No. 1, 2009.

[15] H. Li, Z. Chen, X. Qin, C. Li, H. Tan, "Secure Routing in Wired Networks and Wireless Ad Hoc Networks," Technical Report, Department of Computer Science, University of Kentucky, April 2002.

[16] H. Maulikdavda, R. Sheikh "A Review Paper on the Study of Attacks in MANET with its Detection & Mitigation Schemes ", *International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS)* Vol. 2, No.4, April 2014.

[17] V. G. Muralishankar and Dr. E. George Dharma Prakash Raj, "Routing Protocols for MANET: A Literature Survey", *International Journal of Computer Science and Mobile Applications*, Vol. 2, No.3, March 2014.

[18] Murthy & Garcia-Luna-Aceves, "An Efficient Routing Protocol for wireless Networks", *Springer*, vol. 1,No.2. pp.183-197,1996.

[19] G.Pei, M.Gerla & Tsu-Wei Chen, "Fisheye State Routing (FSR)" *IEEE Transaction* Vol.1 No.4, pp420-430 , October 2000.

[20] C.E.Perkins and P.Bhagwat, "Highly dynamic destination sequenced Distance Vector routing (DSDV) for mobile computers, *ACM SIGCOMM (Special Interest Group in Computer Communication)* pp.234-244,October 1994.

[21] C. E. Perkins and E. M.Royer "Ad-hoc On-demand Distance Vector Routing (AODV)" *International Engineering Task Force (IETF)* pp. 220-245,October 1999.

[22] Robinpreet Kaur & Mritunjay Kumar Rai, A Novel Review on Routing Protocols in MANETs, *Undergraduate Academic Research Journal (UARJ),* ISSN : 2278 – 1129, Vol.1, No.1, 2012.

[23] Sunil Taneja and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks", *International Journal of Innovation, Management and Technology,* Vol. 1, No. 3, August 2010.

[24] Xiaoyan Hong, Kaixin Xu and Mario Gerla, "Scalable Routing Protocols for Mobile Ad Hoc Networks", *IEEE Network*, Vol. 16, No. 4, 2002.

[25] Vincent Park, "Temporally Ordered Routing Algorithm (TORA)" International Engineering Task Force (IETF), pp. 450-465, January 1997.

Author's Profile

S.ANUSUYA is a M.Phil research scholar in Computer Science Department, Gobi Arts & Science College, Gobi. She received M.Sc (CS) from PSG College of Arts and Science in the year 2014. Her area of interest is Advanced Networks.

Dr. S.MEENAKSHI received M.C.A degree from University of Madras in 1990, M.Phil in 2001and Ph.D in Computer Science from Bharathiar University in 2014. She is presently working as an Associate Professor in Computer Science, Gobi Arts & Science College since 1990. Her area of interest includes Object Oriented Programming Systems, Advanced Database Systems and Data Mining.

ISSN: 2278 – 1323

ISSN: 2278 – 1323