A Survey on Various Routing Protocols in Manet with Various Protection Schemes

[1]Suman Bala
M.Tech, Department of Electronic & Communication
Punjabi University, Patiala
sumanbala151191@gmail.com

[2]Er.Amandeep Singh Bhandari
Assistant Professor, Department of Electronic & Communication
Punjabi University, Patiala
singh.amandeep183@gmail.com

[3]Dr. Charanjit Singh
Asst. Professor, Department of Electronic & Communication
Punjabi University, Patiala
channisingh@yahoo.com

Abstract- A MANET is a dynamic collection of the wireless mobile devices that can communicate and move at the same time. The demand of MANET is increasing due to its application in the various fields such as the military and commercial operations, sensor networking, flood affected areas etc. This is so, as the MANET nodes can communicate through wireless links and transfer the data packets from one point to another. But, the main challenge in MANET is to design the robust security solution that may protect the MANET from various routing attacks. Without any centralized administration, these mobile nodes are placed at different ranges in a particular defined area. Flooding attack is kind of the security threat in which source node sends huge amount of data, Root Request (RREQ) and Sync packet to destination node, due to which the receiver shall not work properly as it would be engaged in receiving the excessive amount of data, RREQ and Sync packets from the attacker. To attain the optimal improved results, various routing protocols are implemented and used. In this paper we shall discuss various attacks such as Black Hole, Gray Hole attack & various prevention schemes like OSPF, RIP, IGRP, and EIGRP to protect it from the attack.

Index Terms: *MANET, Routing Protocol, Security,Attacks.*

*****

I. Introduction:

MANET is an infrastructure less network which is established automatically on demand. It is a set of wireless nodes that are configured automatically on the fly thus making it suitable candidate as it is useful in emergency situations, as shown in fig. 1 [1], [2]. In other words it is a multi-hop communication network organized temporarily with nodes that have receivers and transmitters [3]. The topology of network is dynamic which is created and modified on the fly [4]. MANET supports many routing protocols such as Dynamic MANET On-demand routing protocol (DYMO), Optimized Link State Routing protocol (OLSR), Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR) and Ad Hoc On-demand Vector Routing (AODV). Mobility is the fundamental difference between other networks and MANET [5]. Wireless Sensor Network (WSN) traffic also can be relayed over MANET. It does mean that WSN communications are possible between devices of MANET [6]. MANET supports TCP/IP protocol to integrate communication with wired networks as well [1]. Every node in MANET acts as a host in the network and also router which can cooperate in communication [7]. As MANET topology is dynamic in nature which makes the procedure of routing more difficult and vulnerable to Denial of Service (DoS) attacks such as flooding which results in network congestion [8]. MANETs are vulnerable to attacks such as location disclosure, black hole, replay, worm hole, blackmail, Denial of Service and routing table poisoning.

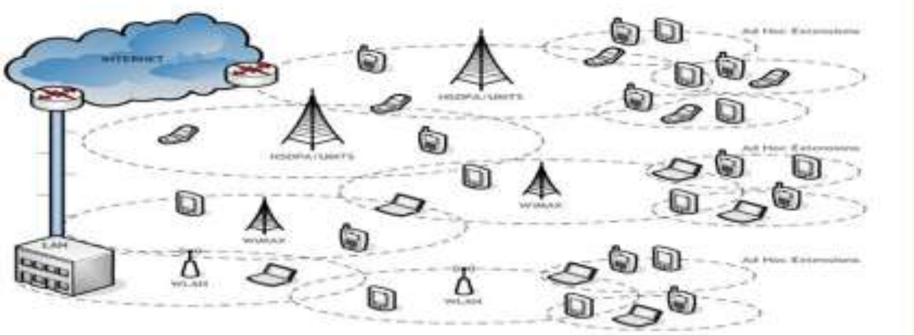

Fig 1: MANET Network

II. Routing Protocols:

There are three types of routing protocols:

[1] Reactive routing protocol.
[2] Proactive routing protocol.
[3] Hybrid routing protocol.

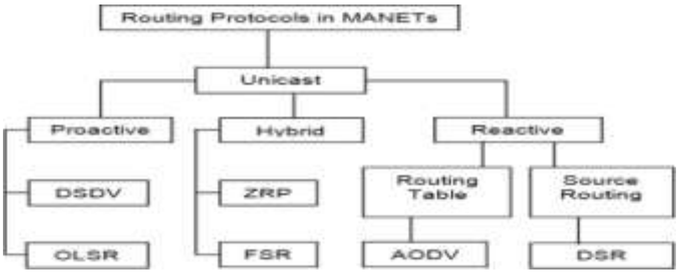

Fig 2: Hierarchy of MANET Routing Protocols

Reactive RoutingProtocols: Reactive protocols tend to decrease the control traffic messages overhead at the cost of increased latency in discover a new routes. Source initiated route discovery in reactive routing protocols and less delay. In reactive protocols there is no need of distribution of information [5]. It consumes bandwidth when data transfers from source to destination. Reactive Protocols are AODV (Ad-hoc On Demand Distance Vector), DSR (Distance Vector Routing) and ABR (Associativity Based Routing). MANET is also called Mesh network. It is highly adaptable and rapidly deployable network. MANET has a dynamic topology [11] [12] [13].

Proactive Routing Protocols:In proactive routing protocols, such as the Optimized Link State Routing (OLSR) protocol [10], nodes obtainroutes by periodic exchange of topology information. A malicious node can launch routing attacks to disrupt routing operations or denial-of-service (DoS) attacks [14] to deny services to legitimate nodes.

Hybrid Routing Protocols: Combination of both reactive and proactive routing protocols. It was proposed to reduce the control overhead of proactive routing protocols and also decrease the latency caused by route discovery in reactive routing protocols. Hybrid routing protocols are ZRP (Zone routing protocol) and TORA (Temporarily Ordered Routing algorithm) [12] [13] [15].

	Protocol Property	**Proactive**	**Reactive**	**Hybrid**
S.No.	**Protocol Name**	**OLSR**	**AODV**	**ZRP**
1	Complexity	Medium	Average	Average
2	Route	Dynamic	Dynamic	Dynamic
3	Memory Size	High	Low	Medium
4	Bandwidth	Minimum	Maximum	Medium
5	Topology Size	Small Network	Large	Both
6	Convergence Time	Slow	Mostly Fast	Average
7	Mission Failure	Low	Low	Very Low

Table 1: Comparison of Routing Protocols

MANETs Routing Attacks:MANET is a collection of mobile nodes, sometimesnodes in MANET can be bad or malicious and thesebad nodes cannot forward the packets due to their aimof conserving network resources such as band width,battery etc. by the denial of service.There are mainly two types of attacks in MANET. Active and Passive [9].

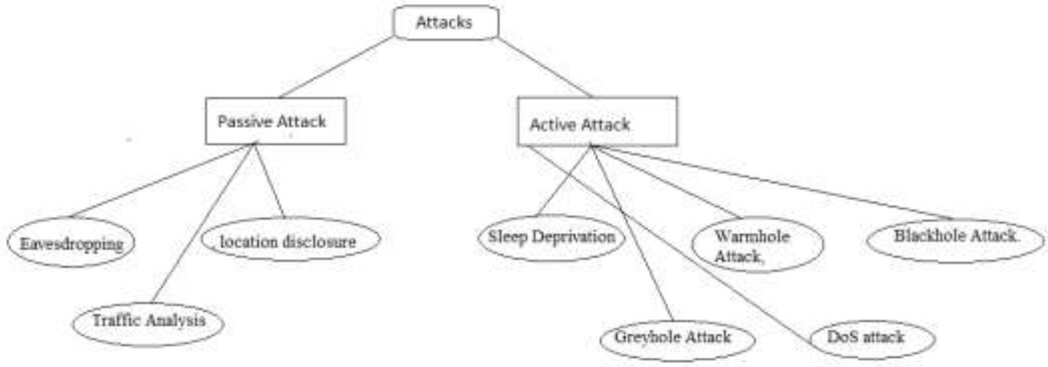

Fig 3:Attacks in MANET

1. Flooding Attack:

The aim of the flooding attack [11] is to exhaust the network resources such as bandwidth and to consume a node'sresources, such as battery power and computational or to disrupt the routing operation to cause severe degradation in network performance. Flood attacks occur when a network or service becomes so weighed down with packetsinitiating incomplete connection requests that it can no longer process genuine connection requests.

2. Black Hole Attack:

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one.For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

3. Worm Hole Attack:

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point [2]. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole .In DSR (Dynamic Source Routing protocol), AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used to pass on information is usually not part of the actual network. Wormholes are dangerous because they can do damage without even knowing the network

4. Jellyfish attack:

In this type of attack firstly the attacker node tries to get access to the network. If the attacker node gets access network then it starts introducing the unwanted delays in the network i.e. as soon as the packet is received by the attacker node it will forward the packets after some delay as a result of which high end-to-end delay is generated by the intruder and it will affect the performance.

5. Gray-hole attack:

A gray-hole attack is extension of black-hole attack used to bluff the source and monitoring system by partial forwarding. Here, attackers uses selective data packet dropping method to behave as genuine node and try to participate into full communication. Gray-hole malicious node participate into route discovery process and update the source route cache/ routing table as shortest path. Afterwards, source always consider malicious node as next hop node and forward packet to same. Malicious node captures all the incoming packets but drop on random basis. The complete phenomena create toughness against detection and prevention mechanism because nodes can drop packets partially not only due to its malicious naturebut also due to overload, congestion or selfish nature.

Layer	Attack	Mode of Attack
Physical	Eaves dropping	By receiver tuning to proper frequency
Data Link	Traffic Analysis	Topology Information
Network	Black Hole Attack	Fake Optimum Route message
	Gray Hole Attack	Slow down the speed of the data
Transport	Session Hijacking	Spoofs victim node IP address
Application	Malicious Code attack	Viruses worms

Table 2: Comparison of MANET Attack

III. Security Protocols:

1.Open Shortest Path First: OSPF [16] [17] [18] is a routing protocol which was defined as version 2 in RFC 2328. It is used to allow the routers to dynamically learn routes from other routes and advertise them. Advertisements containing routes are referred to as link state advertisements that keeps the track of all the various links between itself and a networkto which it is trying to send data; summarizes the route information ,reduces the number advertised routes and reduces the network load. It also uses a designated router to reduce the quantity and frequency of link state advertisements. It has a router, processor, memory more than other routing protocols that selects the best routes of finding the lowest cost paths to a destination.OSPF is routing protocol for IP. It uses a Link State Routing (LSR) algorithm and falls into group of the Interior Gateway Protocols (IGPs), operating within single Autonomous System (AS). The state of the interface or link is used to decide the path on which the information is routed; multiple links with same state is possible. Demand to a destination can be routed on multiple paths.

2. Routing Information Protocol: The Routing Information Protocol (RIP) [16][19][21][22] is a distance-vector protocol that uses hop count as its metric. The Routing Information Protocol (RIP) provides the standard IGP protocol for local area networks, and provides great network stability, guaranteeing that if one network connection goes down the network can quickly adapt to send packets through another connection. It is widely used for routing traffic in the global Internet and is an interior gateway protocol (IGP), which means that it performs routing within a single autonomous system. RIP itself evolved as an Internet routing protocol, and other protocol suites use modified versions of RIP. IP RIP is formally defined in two documents: Request For Comments (RFC) 1058 and 1723. RFC 1058 (1988) describes the first implementation of RIP, while RFC 1723 (1994) updates RFC 1058. RFC 1058 enables RIP messages to carry more information and security features.

3. Interior Gateway Routing Protocol:The Interior Gateway Routing Protocol (IGRP)[16-19] [20-21] is a routing protocol to provide routing within an autonomous system (AS). Distance-vector routing protocols calls for each router to send all or a portion of its routing table in a routingupdate message at regular intervals to each of its neighboring routers. As routing information proliferates through the network, routers can calculate distances to all nodes within the internetwork. IGRP adheres to the following Distance-Vector characteristics: sends out periodic routing updates (every 90 seconds); sends out the full routing table every periodic update; uses a form of distance as its metric; uses the Bellman-Ford Distance Vector algorithm to determine the best “path” to a particular destination; supports only IP routing; utilizes IP protocol 9. Routes have an administrative distance of 100, by default, supporting a maximum of 100 hops. This value can be adjusted to a maximum of 255 hops. IGRP manages a routing table with the most optimal path to respective nodes and to the networks within the parent network. Since, it's a Distance Vector Protocol, IRGP uses several parameters to calculate the metric for the best path to a specific destination. These parameters include delay, bandwidth, reliability, load and Maximum Transmission Unit (MTU).

4. Enhanced Interior Routing Protocol: Enhanced Interior Gateway Routing Protocol (EIGRP) or Enhanced IGRP [16-21] is a Cisco proprietary routing protocol utilizing the Diffusing Update Algorithm (DUAL). EIGRP is a hybrid protocol as it incorporates features of a Distance Vector Routing Protocol and features of a Link State Routing Protocol. Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of IGRP. It used in TCP/IP and OSI internets. It is regarded as an interior gateway protocol (IGP) but has also been used extensively as an exterior gateway protocol for inter-domain routing. Key capabilities that distinguish Enhanced IGRP (EIGRP) from other routing protocols include fast convergence, support for variablelength subnet mask, support for partial updates, and support for multiple network layer protocols. A router running EIGRP stores all its neighbors' routing tables so that it can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbors to discover an alternate route. These queries propagate until an alternate route is found.

IV. Conclusion:

The future of ad- hoc networks is really appealing, giving the vision of ―anytime, anywhere‖ and cheap communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. In this paper we discuss different type of attack present in the MANET as well as the functioning of various security protocols are also define. With the help of that security protocols we find a better solution of these kinds of various attacks. In further work, these security protocols are implemented in MANET to reduce the effect of the attacks.

References:

[1] Pratap K. Meher and P. J. KulkarniAnalysis and Comparison of Performance of TCP-Vegas in MANET. IEEE, 2011, pp.67-70.

[2] Dinesh Singh, Ashish K. Maurya, Anil K. Sarje. Comparative Performance Analysis of LANMAR, LAR1, DYMO and ZRP Routing Protocols in MANET using Random Waypoint Mobility Model. IEEE. 2011. pp62-66.

[3] Xia Wen-jie, Yan Han and Liu Feng-yu. The analysis of M/M/1 queue model with N policy for damaged nodes in MANET. IEEE. 2011. pp289-294.

[4] Sudharson Kumar and Parthipan.V. SOPE: Self-Organized Protocol for Evaluating Trust in MANET using Eigen Trust Algorithm.IEEE. 2011. pp155-159.

[5] FahimMaan, NaumanMazhar. MANET Routing Protocols vs Mobility Models: A Performance Evaluation. IEEE. 2011, pp179-184.

[6] Giuseppe Cardone, Antonio Corradi, Luca Foschini. Reliable Communication for Mobile MANET-WSN Scenarios. IEEE. 2011, pp1085-1091.

[7] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen. CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture. IEEE. 2011, pp1-5.

[8] AlokparaBandyopadhyay, SatyanarayanaVuppala and PrasenjitChoudhury., Simulation Analysis of Flooding Attack in MANET using NS-3. IEEE. 2011, pp1-5.

[9] Adnan Nadeem member IEEE and Michael P.Howarth, "A Survey of MANET Intrusion

[10] Detection & Prevention Approaches forNetwork Layer Attacks",Communication surveyTutorials, IEEE Volume: 15, Issue: 4, 2013.

[11] Behrouz A Forouzan, Data Communications and Networking‖, Special Indian Forth Edition, 2006

[12] Morigere Subramanya Bhat, Shwetha .D, Manjunath .D and DevarajuJ.T,"Scenario Based Study of on demand Reactive Routing Protocol for IEEE-802.11 and 802.15.4 Standards", ISSN: 2249-57 Vol 1(2), Oct-Nov 2011, pp.128-135

[13] Naveen Bilandi and Harsh K Verma, "Comparative Analysis of Reactive, Proactive and Hybrid Routing Protocols in MANET", International Journal of Electronics and Computer Science Engineering 1660 ISSN- 2277-1956.

[14] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala,"DoS Attacks in Mobile Ad-hoc Networks: A Survey", Second International Conference on Advanced Computing & Communication Technologies, 2012.

[15] SinemColeri, Ergen, ZigBee IEEE 802.15.4‖. LAN-MAN Standards Committeeof the IEEE Computer

Society, Wireless LAN medium access control (MAC) and physical layer(PHY) specification, IEEE, New York, NY, USA, IEEE Std802.11-1997 edition,1997 .Wireless Communication, Sept 10, 2004 pp. 35 – 54, ISBN 9781420045474.

[16] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks” ,Tseng et al. Humancentric Computing and Information Sciences 2011, a Springer open journal.

[17] Wu, Bing, “Simulation Based Performance Analyses on RIP, EIGRP and OSPF Using OPNET"

[18] Vishal sharma, Rajneesh Narula and Sameer khullar “Performance Analysis of IEEE 802.3 using IGRP and EIGRP Routing Protocols” International Journal of Computer Applications (0975 – 8887) Volume 44– No13, April 2012

[19] Ittiphon krinpayorm and Suwat Pattaramalai,"Link Recovery Comparison Between OSPF & EIGRP ", International Conference on Information and Computer Networks (ICICN 2012) IPCSIT vol. 27 (2012).

[20] Mr. R. M. Pethe, Miss S. R .Burnase technical era language of the networking - EIGRP International Journal of Engineering Science and Technology (IJEST) NCICT Special Issue Feb 2011

[21] Mehboob Nazim Shehzad, Najam-Ul-Sahar, "Simulation of OSPF Routing Protocol Using OPNET Module"(A Routing Protocol Based on the Link-State Algorithm)

[22] Bernard Fortz,Jennifer Rexford and Mikkel Thorup., Traffic Engineering With Traditional IP Routing Protocols." IEEE Communications Magazine. October 2002, pp. 118-124.

[23] Ahmad Karim, Minhaj Ahmad Khan "Behaviour of Routing Protocols for Medium to Large Scale Networks", Australian Journal of Basic and Applied Sciences, 5(6):, 2011,pp1605-1613.

[24] Amandeep Singh, Amandeep Singh Bhandari, “To evaluate and improve TDMA based MAC protocol for clock synchronization in WBAN”, International Journal in Applied Studies and Production Management, IJASPM, Volume2, Issue 3, 15 May 2016- 15 August 2016, pp. 32-41.

[25] Arjun Kumar, Amandeep Singh Bhandari, “Symbol Detection in MIMO Systems Using PSOGSA Optimization Algorithm”, International Journal of Research, IJR, e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015, pp. 801-808.

[26] Amandeep Singh Bhandari, Charanjit Singh, “Performance Analysis of Cyclostationary Spectrum Sensing Over Different Fading Channels”, International Journal of Computer Applications (0975 – 8887) Volume 129 – No.1, November2015, pp. 27-31.

[27] Sehleen Kaur, Amandeep Singh Bhandari, “Frequency estimation of ECG signals using FIR filter”, International Journal of Research, IJR, e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015, pp. 786-793.

[28] Khera, Ishan, and Ajay Kakkar. "Comparative study of scheduling algorithms for real time environment." International journal of computer applications 44, no. 2 (2012): 5-8.

[29] Kakkar, Ajay, M. L. Singh, and P. K. Bansal. "Dynamic Path Management Scheme for Multinode Network", International Journal of Communication Engineering Applications-IJCEA, Vol 02, Issue 03; July 2011, pp: 117-122.

[30] Sharma, Amandeep, Ajay Kakkar, and Sandeep Sachdeva. "Optimized WDM network with consideration of lesser blocking probability & shortest path selection." In Signal Processing, Computing and Control (ISPCC), 2012 IEEE International Conference on, pp. 1-6. IEEE, 2012.