A Survey: Protection Schemes in MANET from various attacks with Routing Protocols

[1]Niharika Sood , [2]Er.Rasbir Singh
1M.Tech, 2Assistant Professor
Department of Computer Engineering, RIMT university , MGG
Sood.niharika3@gmail.com
Rasbir.rai@gmail.com

Abstract—The increase in availability and popularity of mobile wireless devices has lead researchers to develop a wide variety of Mobile Ad-hoc Networking (MANET) protocols to exploit the unique communication opportunities presented by these devices. Devices are able to communicate directly using the wireless spectrum in a peer-to-peer fashion, and route messages through intermediate nodes, however the nature of wireless shared communication and mobile devices result in many routing and security challenges which must be addressed before deploying a MANET. In this paper we investigate the range of MANET routing protocols available and discuss the functionalities of several ranging from early protocols. In this paper we discuss various attacks such as 'Black hole attack', 'Gray hole attack' & various prevention schemes like OSPF, RIP, IGRP, EIGRP to protect it from the attack.

Keywords – Mobile Ad-hoc Networks, Characteristics, Routing protocols, Challenges, Security.

Introduction: Mobile ad hoc networks (MANETs) are freely self- organized networks without infrastructure support. In a mobile ad hoc network, nodes move readily. Because nodes in a MANET normally have low transmission ranges, some nodes cannot communicate directly with each other. Hence, routing paths in mobile ad hoc networks potentially contain multiple hops, and every node in mobile adhoc networks has the responsibility to act as a router. Mobile Ad-hoc networks are self- configured multihop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes [2]. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multihop forwarding. The node in the network not only acts as hosts but also as routers that route data to/from other nodes in network [1]. Some examples include interaction of students during lecture, sharing of files by business associates in an airport terminal. The group of mobile hosts may form their ad hoc network, if every mobile host is equipped with wireless local area network interface.

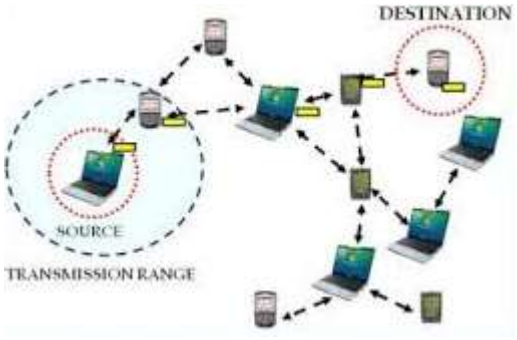

Fig 1: MANET Network

Applications of MANET: MANETs are useful in places where no communication infrastructure or the infrastructure is damaged. Typical applications are.

- Military or police exercises.
- Disaster relief operations.
- Mine cite operations.
- Urgent Business meeting

MANETs characteristics:

1) Distributed operation: There is no background network for the central control of the network operations; the control of the network is distributed among the nodes. The nodes involved in a MANET should cooperate with each other and communicate among themselves and each node acts as a relay as needed, to implement specific functions such as routing and security.

2) Multi hop routing: When a node tries to send information to other nodes which is out of its communication range, the packet should be forwarded via one or more intermediate nodes.

3) Autonomous terminal: In MANET, each mobile node is an independent node, which could function as both a host and a router.

4) Dynamic topology: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable time. The nodes in the MANET dynamically establish routing among themselves as they travel around, establishing their own network.

5) Light-weight terminals: In maximum cases, the nodes at MANET are mobile with less CPU

capability, low power storage and small memory size.

6) Shared Physical Medium: The wireless communication medium is accessible to any entity with the appropriate equipment and adequate resources. Accordingly, access to the channel cannot be restricted.

MANET Routing Protocol:

A Proactive Routing: Proactive protocols rely upon maintaining routing tables of known destinations, this reduces the amount of control traffic overhead that proactive routing generates because packets are forwarded immediately using known routes, however routing tables must be kept up-to-date; this uses memory and nodes periodically send update messages to neighbours, even when no traffic is present, wasting bandwidth [5]. Proactive routing is unsuitable for highly dynamic networks because routing tables must be updated with each topology change, this leads to increased control message overheads which can degrade network performance at high loads [6].

B. Reactive Routing: Reactive Protocols use a route discovery process to flood the network with route query requests when a packet needs to be routed using source routing or distance vector routing. Source routing uses data packet headers containing routing information meaning nodes don't need routing tables; however this has high network overhead. Distance vector routing uses next hop and destination addresses to route packets, this requires nodes to store active routes information until no longer required or an active route timeout occurs, this prevents stale routes [5]. Flooding is a reliable method of disseminating information over the network, however it uses bandwidth and creates network overhead, reactive routing broadcasts routing requests whenever a packet needs routing, this can cause delays in packet transmission as routes are calculated, but features very little control traffic overhead and has typically lower memory usage than proactive alternatives, this increases the scalability of the protocol [3].

C. Hybrid Routing: Hybrid protocols combine features from both reactive and proactive routing protocols, typically attempting to exploit the reduced control traffic overhead from proactive systems whilst reducing the route discovery delays of reactive systems by maintaining some form of routing table [5]. The two survey papers [3], [4] successfully collect information from a wide range of literature and provide detailed and extensive reference material for attempting to deploy a MANET, both papers reach the conclusion that no single MANET routing protocol is best for every situation meaning analysis of the network and environmental requirements is essential for selecting an effective protocol. Whilst these papers contain functionality details for many of the protocols available, performance information for the different protocols is very limited and no details of any testing methodologies is provided, because of this the validity of some claims made cannot be verified.

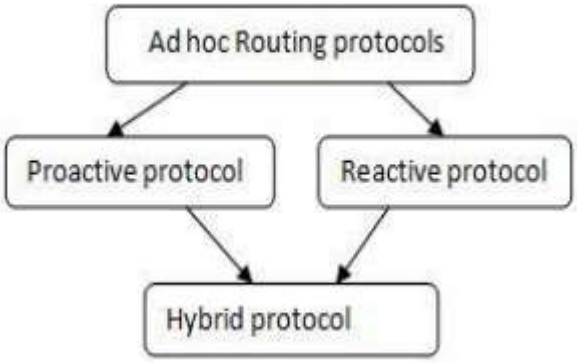

Fig 2: MANET Routing Protocol

MANET Attack:

1. Black Hole Attack: The black hole attack is a kind of denial of service attack. In this attack, the malicious node sends false route replies to the source node claiming to have the shortest path to the destination node. When the source node established the route through the malicious node, the malicious node then misuse or discards any or all of the network traffic being routed through it.

2**. Grey Hole attack**: It is a special type of black hole attack in which the attacking node first agrees to forward packets and then fails to do so. In this the selected packets are dropped. Gray Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface.

3. Wormhole attack: It is also known as tunnelling attack. In this an attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunnelled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

4. Eavesdropping Attacks: It is also known as disclosure attack. These are passive attacks by

external or internal nodes. The attacker gathers information e.g. Private key, public key or even passwords of the nodes and analyzes broadcast messages to reveal some useful information about the network.

5. Traffic Analysis: In this the network traffic and messages are examined to find out information. It can be performed on encrypted messages. In this the attackers use techniques such as traffic rate analysis, and time correlation monitoring etc.

Securing Routing Protocols in MANET:

1. Routing Information Protocol (RIP): RIP stands for Routing Information Protocol in which distance vector routing protocol is used for data/packet transmission. In Routing Information protocol (RIP), the maximum number of Hop is 15, because it prevents routing loops from source to destination. Mechanism like split horizon, route poisoning and hold down are used to prevent from incorrect or wrong routing information. [9]. Compared to other routing protocol, RIP (Routing Information Protocol) is poor and limit size i.e. small network. The main advantage of using RIP is it uses the UDP (User Datagram Protocol) and reserved port is 520 [13].

2. Enhanced Interior Gateway Protocol (EIGRP): EIGRP stands for Enhanced Interior Gateway Protocol which allows router to share information to the neighbouring routers which are within the same area. Instead of sending the entire information to the neighbouring router, the information which is needed are shared which reduces the workload and amount of data needs to be transmitted. EIGRP (Enhanced Interior Gateway Protocol) designed by CISCO system which can be used only in CISCO routers, but in 2013 it became open source, so it can be used in other routers [8] – [10]. Neighbor table and Topology table are maintained by the EIGRP (Enhanced Interior Gateway Protocol) [13].

3 Open Shortest Path First (OSPF): OSPF stands for Open Shortest Path First which uses link-state routing algorithm. Using the link state information which is available in routers, it constructs the topology in which the topology determines the routing table for routing decisions [10]. It supports both variable-length subnet masking and classless inter-domain routing addressing models. Since it uses Dijkstra's algorithm, it computes the shortest path tree for each route. The main advantages of the OSPF (Open Shortest Path first) is that it handles the error detection by itself and it uses multicast addressing for routing in a broadcast domain [11].

4. Interior Gateway Routing Protocol (IGRP): IGRP stands for Interior Gateway Routing protocol which uses distance vector protocol (interior) to exchange data within a system [7]. It supports multiple metrics for each node which includes delay, load and bandwidth, in order to compare the 2 routes which are combined into single metrics. The port number for IGRP is 9 which are used for communication and by default every 90 seconds it updates the routing information [8].

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] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. A review of routing protocols for mobile ad hoc networks. Technical report, Telecommunication and Information Research Institute, University of Wollongong,Wollongong, NSW 2522.

[2] Xiaoyan Hong, Kaixin Xu, and Mario Gerla. Scalable routing protocols for mobile ad hoc networks. 2002.

[3] E. Alotaibi and 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.

[4] A. Boukerche et al., "Routing protocols in ad hoc networks: A survey," Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 55, no. 13. pp. 3032–3080, May 2011.

[5] H. Amri, M. Abolhasan, and T. Wysocki, "Scalability of MANET routing protocols for heterogeneous and homogenous networks," Computers and Electrical Engineering, vol. 36, no. 4, pp. 752–765, 2010.

[6] C. Liu andS.Chang,"The study of effectiveness for ad-hoc wireless network," in Proc. of ICIS 2009 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea, 24-26 Nov., 2009, pp. 412-417

[7] S. Barakovićand J. Baraković, "Comparative Performance Evaluation of Mobile Ad Hoc Routing Protocols,"Proceedings of the 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2010), Opatija, Croatia, May 2010.

[8] Nurul I. Sarkar & Wilford G. Lol "A Study of MANET Routing Protocols: Joint Node Density, Packet Length and Mobility" 978-1- 4244-7755-5/10/$26.00 ©2010 IEEE Page no. 515-520

[9] Vasudha Arora & C. Rama Krishna"Performance Evaluation of Routing Protocols for MANETs under Different Traffic Conditions" 2010 2nd International Conference on Computer Engineering and Technology [Volume 6] 978-1-4244-6349, 2010 IEEE

[10] Patel, B.; Srivastava, S.;, "Performance analysis of zone routing protocols in Mobile Ad Hoc Networks," Communications (NCC), 2010 National Conference on, vol.,pp.1-5, 29-31 Jan. 2010.

[11] J. Wang, F. Xu, F. Sun. "Benchmarkinng of Routing Protocols for Layered Satellite Networks". In Proceedings of Multiconference on Computational Engineering in Systems Applications, pp. 1087-1094, vol. 2, Oct 2006.

[12] Lachhman,S., Asad, Y., Malkani "Performance analysis of WLAN standards for video conferencing applications", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 6, December 2011

[13] Rajan, R., Shipra, S. "WLAN Performance Improvisation by Fine Tuning IEEE 802.11 Parameters", International Journal of Computer Applications, April 2012

