A SURVEY OF VARIOUS ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS (MANET)

Vidya Shree.P [1],
M.Phil Research Scholar,
Department of Computer Application, PSGR Krishnammal College for Women,
Coimbatore-641004.
E-mail Id:[1] vidhya_sree1@yahoo.co.in.

Sophia Reena.G. [2]
Lecturer & HoD,
Department of Computer Application,PSGR Krishnammal College for Women,
Coimbatore-641004.
E-mail Id:[2] sophiareena@psgrkc.com.

ABSTRACT

Mobile ad hoc networks is a collection of mobile nodes that dynamically change the topology of MANETs ,that allows nodes to join and leave the network at any point of time. In MANET mobile nodes are communicate each other without any infrastructure. MANET is widely used in many applications such as military purpose, disaster area, and personal area network as so on. The generic characteristic of MANET has more vulnerable to security attacks due to highly dynamic environment. Recently many routing protocols have been proposed for MANET. This research paper presents a overview of the protocols characteristics, functionality, benefits and limitations also brief on the possible attacks in Mobile Ad-Hoc networks. The main motive is to make observation about the performance of Mobile ad hoc routing protocols.

Index Terms- MANET, MANET Routing Protocols, AODV.

INTRODUCTION

Wireless mobile Ad hoc network mobile nodes communicate each other without without any infrastructure. MANET is a self-configuring network which is organized several movable user equipment. In recent years MANET [2] has a great impact on wireless networks, there are no basic network work devices, such as routers or access points to transfer data among nodes. Instead each node act as a router to establish a route and transfer data by means of multiple hops. Mobile Adhoc networks [2] are more vulnerable to security problem than the wired networks and several security issues In MANET each and every node communicate with neighbors, all the nodes works as a router and maintaining a routing tables, node cooperation essential in the Mobile Ad hoc networks. There are no of process is involved in route a packet from source to destination through the intermediate node, To accomplish this task in MANET no of different routers helps to carry out this. Further more MANET routing protocols broadly classified into there categorized such as proactive routing protocols, reactive routing protocols and hybrid routing protocols. There are many security issues, which has been encounter in recent years. Table 1 depicts the types of attacks in MANET.

The rest of the paper is organized as follows, Sec. 2 configured An overview of Routing protocols in MANET, SEC. 3 expands of proactive (table driven Routing) Protocol and Sec. 4 expands of Reactive (on demand) Routing Protocols, Sec. 5 briefs of Hybrid (both Proactive and Reactive) Routing Protocols. Sec. 6 explains of Conclusions and Future Work.

Attacks in MANET	**Classification of attacks**	**Description of attacks**
Passive Attack	**1.1 Snooping**	Snooping is Unauthorized access to another person's data. Its similar to eaves dropping but is not necessarily gaining access of data. Eg: Monitoring the activities of some one through snooping software.

Active Attacks	**2.1 Network Layer Attack**	
	2.1.1Wormhole Attack	Two malicious attacker encapsulate the packet and falsified the route length between two networks through wired or wireless
	2.1.2 Black hole Attack	An attacker uses the routing protocol to inform itself as having the shortest path to the node.
	2.1.3 Byzantine Attack	A compromised intermediate node or set of compromised intermediate node s organize and carries out attacks such as creating rooting loops and dropping packets on non optimal paths.
	2.1.4 Information Disclosure	Network communication confidentiality is more important such as network topology, geographic location or optimal routes to authorized nodes. A attackers compromised node hijack the related information of network topology.
	2.1.5Resource Consumption Attack	The attacker tries to consume resources of nodes such as battery power, bandwidth and computational power.
	2.1.6 **Routing Attacks**	
	2.1.6.1 Routing Tables Overflow	A malicious node that prevent the creation of new node entries by routing table overflow updating.
	2.1.6.2 Routing Table Poisoning	A compromised node may change the routing table and forward modified route packet to other node and congestion of network. Create a traffic .
	2.1.6.3 Packet Replication	Attacker replicate the old packet for creating additional battery power and causes confusion in the routing process.
	2.1.6.4 Route Cache Poisoning	Similar to route poisoning. In this case in AODV protocol nodes maintain a route cache, it may affect.
	2.1.6.5 Rushing Attack	Source node imagine that a intermediate malicious node translate the duplicate packet over network it seems to discard the legitimate route request packet.
	2.2 Transport Layer Attacks	
	2.2.1 Session Hijacking	Gives an opportunity to malicious node work as legitimates systems and accessing the target machine, make that larges system un avail for some times in the network.
	2.3 Application Layer Attacks	
	2.3.1 Repudiation	A malicious node involved in all communication or part of the communication eg: attacker may hijack business application in specific of credit card access.
	2.4 Multi-layer Attacks	
	2..4.1 Denial of Service	Attacker involved denying the access of legitimate users. Restrict the user to access centralized resources .Eg; jamming signals, disturb rooting protocols

	2.3.2 Impersonation	A malicious node controls the network management system of the network and change the configuration as a user who has privileges.

2) ROUTING PROTOCOLS

Routing is a function [5] contains much activity to connect source to destination, It plays a important roles in architecture, design and operation of networks. Hence carry out this task routing protocols are essential. Routing protocols classification have seen in introduction part, further more look of the specific protocols in MANET. The studies of Routing Protocols are more important in the area of research to detect the vulnerabilities of Mobile Ad hoc Networks in recent years.

3) TABLE DRIVEN ROUTING PROTOCOLS

These protocols are the conventional routing schemes and similar to as wired networks. Each node has maintaining one or more route tables with the information of the next hops/subnet. Periodically table has been updated for new entry of network node. It is not suitable for large topology network. Main draw back of this routing causes more overhead consumption of more

Bandwidth. Table driven protocols differ from their changes in topology spreads through all nodes in the networks .We describe some of the following proactive routing protocols in MANET.

3.1) Destination-sequenced distance vector (DSDV)

C E Perkins & T J Warson [10] have discussed DSDV algorithms is a modification of DBF (distributed Bellman-Ford), It provides a loop free routers and establish a single path to a destination. The path has been selected using distance vector shortest path routing algorithm. There are two types of updated packets are used to reduce the overhead of the transmission network such “full dump” and “incremental” packets. Full dump carries the all information of packets incase of incremental packets carries only the information changed since the last full dump. DSDV overheads grows according to $O(N^2)$. Therefore the protocol is not more efficient for large network. Distance- Vector algorithms, every node i maintains for each destination x, a set of distances $\{d_{ij}^{x}\}$, the choose of next hop in this manner leads to shortest path. In DSDV Routing table must be changed in periodically due to the updates of node routing loops occur in the network, to eliminate routing loops each node is trigged with a sequence number. e sequence number of the nodes must be in even number.

3.2) OLSR (Optimized Link State Routing Protocols.

P. Jacquet described, Due to the nature of Pro-active the routes information’s available when heeded available. To reduce the sizes of control packets, MRP (Multi point relay selectors)used to declares only a subset of links with its neighbors who are its MPR. Benefit of the MRP is large subset of nodes are communicating with each other, its leads to offer services to large and dense networks. OLSR performs the hop-by-hop routing. MRP minimize the flooding of broadcast retransmission in the same region, Periodically HELLO messages has been forwarded to each node, which consisting information about its neighbors and their link status. Each node constructs its MPR Selector table with the nodes who have selected it as multipoint relay. The link state as MPR implies that link with neighbor node is bi-directional and that node is also selected as multipoint relay by this local node.

Link state routing protocols specially designed for ad-hoc networks. To reduces the control flooding by declaring the links of neighbors within its MRPs instead of all links. Important uses of OLSR for 4G global ubiquitous networks by embedding mobile IP management with IP agent into the OLSR MPR-flooding [12]. Several extensions of OLSR are available that correspond to different network scenario such as faster change topology and security. Compare with DSDV Protocol control overhead is higher than link state. Qos routing mechanism is better than the reactive routing protocols. In [13] for security purpose in OLSR, digital signature added into the transmission of OLSR. Energy consumption high for CPU utilization, hence efficient only in high topology than small network topology. Control Packets can be reused in order to support certificate authority (CA) without introducing additional overhead.

3.3) TBRPF (Toplology Dissemination Based on Reverse-Path Forwarding.

R. Ogier [14] have discussed TBRPF is a link state routing protocol designed for MANET. Each node transmits the information of source tree to find out the shortest path. In order to reduce the overhead of the node each node transmits the “partial” information stored into topology table, using a modification of Dijkstras algorithm. DBRF uses a combination of periodic and differential updates to keep neighbors informed of the reported part of its source tree. HELLO message which reports only “changes” in the status of neighbors. It is containing two modules that neighbor discovery module and routing module. Compare to other link state protocols HELLO messages is too small TBRPF Protocol.

3.3.4) Wireless routing protocol (WRP)

Wireless routing protocols (WRP) [15, 16] is a path-finding algorithm with the exception of avoiding the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information

reported by all its neighbors. WRP is a loop free routing protocol. Each node maintains 4 tables: distance table, routing table, link cost table & message retransmission list table. Link changes are propagated using update messages sent between neighboring nodes. Hello messages are periodically exchanged between neighbors. This protocol avoids count-to infinity problem by forcing each node to check predecessor information.

4)4) ON DEMAND-DRIVEN REACTIVE PROTOCOLS

On demand protocols create routes only when desired by source nodes. When a node requires a route to destination, it initiates route discovery process within the network. This process is completed once a route is found or all possible route permutations are examined. Once a route is discovered and established, it is maintained by route maintenance procedure until either destination becomes inaccessible along every path from source or route is no longer desired.

4.4.1) Ad hoc on demand distance vector (AODV)

Ad hoc On-demand Distance Vector Routing (AODV) [7] is an improvement of the DSDV algorithm. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes. In AODV, when a source node S wants to send a data packet to a destination node D and does not have a route to D, it initiates route discovery by broadcasting a route request (RREQ) to its neighbors. The immediate neighbors who receive this RREQ rebroadcast the same RREQ to their neighbors. This process is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path where the RREQ arrived. The destination node will ignore the same RREQ that arrives later. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node.

4.2) Dynamic Source Routing (DSR)

The key feature of DSR is the use of source routing, which means the sender knows the complete hop-by-hop route to the destination. The node maintains route caches containing the source routes that it is aware of. Each node updates entries in the route cache as and when it learns about new routes. The data packets carry the source route in the packet headers. The delay and throughput penalties of DSR are mainly attributed to aggressive use of caching and lack of any mechanism to detect expired stale routes or to determine the freshness of routes when multiple choices are available. Aggressive caching, however, helps DSR at low loads and also keeps its routing load down. Several additional optimizations have been proposed and evaluated to be very effective [8]. These improvements includes

- Salvaging: An intermediate node can replace a failed route in the data packet with route information in its own cache.
- Gratuitous route repair: Source node notifies the neighbors the error found in its packet, in order to clean up similar error in the caches of its neighbors.
- Promiscuous listening: A node can update its own source routes in cache by overhearing a packet not addressed to it. The node also checks if the packet could be routed via it to gain a shorter path.

HYBRID ROUTING PROTOCOLS

The Ad Hoc network can use the hybrid routing protocols that have the advantage of both proactive and reactive routing protocols to balance the delay and control overhead (in terms of control packages). The difficulty of all hybrid routing protocols is how to organize the network according to network parameters. The common disadvantage of hybrid routing protocols is that the nodes that have high level topological information maintains more routing information, which leads to more memory and power consumption.

5.1) Zone Routing Protocol (ZRP)

The Zone Routing Protocol (ZRP) [9] localizes the nodes into sub-networks (zones). Within each zone, proactive routing is adapted to speed up communication among neighbors. The inter-zone communication uses on-demand routing to reduce unnecessary communication. An improved mathematic model of topology management to organize the network as a forest, in which each tree is a zone, is introduced in [17]. This algorithm guarantees overlap-free zones. Furthermore, the concept introduced in this algorithm also works with QoS control because the topology model is also an approach to estimate the link quality. An important issue of zone routing is to determine the size of the zone. An enhanced zone routing protocol, Independent Zone Routing (IZR),

Which allows adaptive and distributed reconfiguration of the optimized size of zone, is introduced in [18]. Furthermore, the adaptive nature of the IZR enhances the scalability of the ad hoc network.

5.2) Location Aided Routing (LAR)

LAR [19]is another kind of hybrid routing protocol. LAR is a scalable routing protocol that uses landmarks, location and distance of the nodes to reduce the periodical update costs. LAR is suitable for networks with large number of nodes, which need to establish a hierarchy. This protocol is more complex than zone routing protocols due to the fact that the maintenance of hierarchical network is more difficult when determining the level of the nodes in the hierarchy.

6) CONCLUSIONS

The recent research efforts have made big progress on ad hoc network routing, both in theory and in practical implementation. It is still difficult to determine which of them has overall better performance in MANET. From the study of the performance evaluation of routing protocols in MANET, we know the results are highly disturbed by the network model and network parameters. In future we make simulation model to meet out the security issues effectively in MANET.

REFERNCES:

[1] Hao Yang, Haiyun Luo; Fan Ye ; Songwn Lu; Lixia Zhang;"Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE , vol.11, no,1,pp. 38-47, Feb 2004.

[2] Sheikh. R. Singh Chande. M.Kumar Mishra. D;, " security issues in MANET, A review" Wireless And Optical Communications Networks(WOCN), 2010 Seventh International Conference On, vol., no., pp, 1-4, 6-8 Sept, 2010.

[3] Nishu Garg, RP Mahapatra, "MANET Security Issues" LICSNS International Journal of Computer Science and Network Security, Volume 9, No. 8, 2009.

[4] Hoang Lan Nguyen Uyen Trang Nguyen "A study of different types of attacks on multicast in mobile ad hoc networks". Ad Hoc Networks, Volume 6, Issues 1, Page 32-46, January 2008.

[5] Krishna Gorantala "Routing Protocols in Mobile Ad hoc Networks" Master Thesis in Computing Science, Umea University, June 15, 2006.

[6] Bing Win, Jianmin Chen, jie WU, Mihaela Cardei"A survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" Wireless/Mobile Network Security,@2006 Springer.

[7] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing," in Internet Engineering Task Force (IETF) draft, July 2003.

[8] N. Moghim, F. Hendessi, and N. Movehhedinia, "An improvement on ad-hoc wireless network routing based on aodv," in the 8th International Conference on Communication Systems ICCS, vol. 2. IEEE, 2002, pp. 1068–1070.

[9] Z. J. Haas and M. R. Pearlman, "Zrp: a hybrid framework for routing in ad hoc networks," pp. 221–253, 2001.

[10] C.E. Perkins, T.J. Watson, Highly dynamic destination sequenced distance vector routing (DSDV) for mobile computers, in: ACM SIGCOMM_94 Conference on Communications, Architectures, London, UK, 1994.

[11] P.Jacquet, P.Miihlethaler, "Optimized Link State Routing Protocol for Ad Hoc Networks", Hipercom Project, BP[105, 78153 Chesnay Cedex, France.

[12] M. Benzaid, P. Minet, K. A. Agha, C. Adjih, and G. Allard, "Integration of mobile-ip and olsr for a universal mobility," in Wireless Networks,vol. 10, 2004, pp. 377–388.

[13] zhijiang Chang, Georgi Gaydadjiev, "Routing Protocols for Mobile Ad-hoc Networks: Current Development and Evaluation", Mekelweg 4, 2628 CD Delft, The Netherlands.

[14] R. Ogier, F. Templin, and M. Lewis, "Topology dissemination basedon reverse-path forwarding (tbrpf)," in Internet Engineering Task Force (IETF) draft, February 2004.

[15] C.K.Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall, Publications, 2002. Driven Routing for Ad Hoc Wireless Networks'," in Proceeding of IEEE ICC, June 2000.

[16] Jyoti Raju and J.J. Garcia-Luna-Aceves, " A comparison of On-Demand and Table

[17] N. Nikaein and C. Bonnet, "TopologyManagement for improving routing and networkPerformances in mobile ad hoc networks" inMobile Networks and Applications vol. 9, 2004.

[18] p. Samar, M. R Peariman, and Z.J Haas,Independent zone routing an adaptive hybridRouting framework " in IEEE ACM TransactionsOn Networking (TON), vol. 12,2004, pp. 595–608

[19] Y. B. Ko and N. H. Vaidya, "Locationaided routing (lar) in mobile ad hoc networks,"Wirel. Netw., vol. 6, no. 4, pp. 307–321, 2000.