7th National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(1st and 2nd March 2019)
International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

A Survey of Routing Protocols and Network Security In Manets

Bhavika Thakur[1], Akshata Raut[2]

[1]Department of Computer Engineering, VIVA Institute of Technology, Virar (East)
[2]Department of Computer Engineering, VIVA college of Diploma Engineering and Technology, Virar (West)

Abstract— *Mobile Ad-Hoc networks are the collection of wireless nodes which communicate with each other without the support of centralized infrastructure. MANET is a frame less network. Nodes of these networks perform tasks as a routers which determines and preserves the routes to other nodes in the network. In such networks, nodes are capable to move and coordinate with their neighbours. The network topology is speedily change due to nodes mobility, source constraint and bandwidth restriction of wireless medias. Routing is a crucial and foremost concern for operative and consistent communication between mobile nodes in a MANET. A number of protocols have been found for efficient routing. Security has become a primary concern in order to deliver secure communication among mobile nodes in hostile surroundings. This Paper provides a summary of routing protocols for MANET by giving their features, functionality, benefits and limitations and also describes the types of security attacks.*

Keywords— MANETs, Mobility, Network Security, Routing Protocols, Wireless

I. INTRODUCTION

A Mobile Ad-hoc Network is a group of wireless mobile nodes forming a temporary network devoid of any help of predefined configuration. The node in the network works as a router that route data to and from other nodes in the network. All devices in a MANET are free to move in any direction independently, and because of this its links to other devices changes frequently. Designing a routing for MANET has been a challenging job due to dynamic topology of the network and the reason for the same is high node mobility. The various protocols have been introduced for this task. The method of selecting routes in a network to transmit data packets from one node to another node in the network is Routing.

In a MANET, topology of the network is not static due to its dynamic nature. Because of it, we do not have a fixed path for communication in the network. MANET routing protocols can be classified into three groups based on the routing policy. These are: (1) Proactive or Table-driven routing protocols, (2) Reactive or On-demand routing protocols and (3) Hybrid routing protocols. In proactive routing protocols routes to a destination are determined when a node joins the network or changes its location and are kept by periodic route updates. In reactive routing protocols routes are exposed each time when needed. Hybrid routing protocols associates the features of proactive and reactive routing protocols. MANET is defined as a self-configurable and quickly deployable wireless network. Therefore, the routing protocol must check both connectivity and security to achieve the network stability. The widely used routing protocols perform their algorithms over MANET routing protocols inappropriately, assuming all the nodes are reliable. If the routing data has been invented and the direction of the route has been improved, then the attacker or intruder would perform different types of attacks such as Black Hole Attack (BHA) [1]. There are some tasks that make the design of Mobile Ad-hoc Network routing protocols a difficult task.

II. CLASSIFICATION OF ROUTING PROTOCOLS

2.1 Pro-active Routing Protocols

These protocols require each node to maintain one or more tables to store, update routing information throughout the network. These protocols try to maintain effective routes to all communication mobile nodes all the time. Periodic route updates are exchanged in order to synchronize the tables [2]. Table driven protocols maintain steady and up to date routing information about each node in the network.

- Some of the existing proactive/table driven routing protocols are:
- Destination Sequenced Distance Vector routing (DSDV)

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

- Wireless Routing Protocol (WRP)
- Cluster Gateway Switch Routing protocol (CGSR)
- Fisheye State Routing (FSR)
- The logical Hypercube-based Virtual Dynamic Backbone protocol (HVDB)

2.2.1 Destination Sequenced Distance Vector routing (DSDV)

DSDV (Perkins & Bhagwat, 1994) is a distance vector routing protocol that assurances 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. Each DSDV node keeps a routing table which stores; destinations, next hop addresses and number of hops as well as sequence numbers; routing table updates are sent frequently to a limited size of 1 packet holding only new information.

2.2.2 Wireless Routing Protocol (WRP)

WRP (Murthy & Garcia-Luna-Aceves, 1995) is a distance vector routing protocol that tries to reduce the possibility of producing temporary routing loops in mobile ad-hoc networks. It is a proactive, destination-based protocol. WRP belongs to the class of route-finding algorithms, is that they use information about distance and second-to-last hop (predecessor) along the path to each destination. In this protocol, each node maintains four different tables as in many other table-driven protocols.

- These four tables are:
- Distance table,
- Routing table,
- Link- cost table and
- Message Retransmission List (MRL) table.

2.2.3 Clusterhead Gateway Switch Routing protocol (CGSR)

CGSR (Chiang, Wu, Liu, & Gerla, 1997) is a cluster based tiered routing. A stable clustering algorithm Least Clusterhead Change (LCC) is used to partition the complete network into clusters and a Clusterhead is selected in each cluster. Data packets are transmitted through routes having a format of Clusterhead Gateway between any source and destination pairs. The main advantage of CGSR is that it can expressively decrease the routing table size comparing to DV protocols. Only one entry is mandatory for all nodes in the same cluster. Thus the broadcast packet size of the routing table is reduced.

2.2.4 Fisheye State Routing (FSR)

FSR (Pei, Gerla & Chen, 2000) is an improvement of GSR. GSR requires the entire topology table to be exchanged among neighbours. The Fisheye State Routing (FSR) is a proactive unicast routing protocol based on Link State routing algorithm with efficiently reduced overhead to maintain network topology data. 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.

2.2.5 The logical Hypercube-based Virtual Dynamic Backbone protocol (HVDB)

The logical Hypercube-based Virtual Dynamic Backbone (HVDB) is a proactive, QoS-aware and hybrid multicast routing protocol for large gauge MANETs. It contains proactive logical route maintenance, summary-based involvement update and logical location-based multicast routing. Due to the symmetry and regularity properties of hypercube, no leader is needed in a logical hypercube, and every node plays nearly the same part excluding for the slightly dissimilar roles of border cluster heads and inner cluster heads. Thus, no single node is overloaded than any other nodes, which is expected to occur in tree-based architectures.

2.2 Reactive routing protocols

Every node in this routing protocol maintains information of only active paths to the destination nodes. A route exploration is desired for every new destination therefore the communication overhead is reduced at the expense of delay to search the route.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

Quickly changing wireless network topology may pause active route and cause subsequent route search. Routes in reactive algorithms are established when they are required, in order to minimize the communication overhead.

Some of the existing proactive/table driven routing protocols are:

- Ad-hoc On-demand Distance Vector routing (AODV)
- Dynamic Source Routing (DSR)
- Light-weight Mobile Routing (LMR)
- Associativity Based Routing (ABR)
- The Enhanced On Demand Multicast Routing Protocol (EODMRP)

2.2.1 Ad-hoc On-demand Distance Vector routing (AODV)

The Ad-hoc On-demand Distance Vector (AODV) routing is an enhancement on DSDV as it usually reduces the number of required broadcasts by creating routes on a demand basis, as at variance to maintaining a complete list of routes as in the DSDV algorithm. AODV make the most of sequence numbers and routing beacons from DSDV but implements route discovery using on-demand route requests (RREQ). AODV is different to DSR as it is uses distance vector routing; this requires every single node in the route to preserve a provisional routing table for the duration of the communication. AODV has improved upon the DSR route request process using an escalating ring search mechanism based upon incrementing time-to-live (TTL) to prevent unwarranted RREQ flooding.

Nodes within an active route record the senders address, sequence numbers and source / destination IP address within their routing tables, this data is used by route reply (RREP) to create reverse paths. AODV deals with node mobility by means of sequence numbers to identify and discard outdated routes, this is combined with route error (RERR) messages which are sent when broken links are detected, RERR packets travel upstream to the source informing nodes to delete the broken links and trigger new route discovery if alternative routes are not available [6].

2.2.2 Dynamic Source Routing (DSR)

DSR permits nodes in the MANET to dynamically determine a source route through multiple network hops to any destination. In this protocol, the mobile nodes are essential to maintain route caches or the well-known routes. The route cache is updated when any new route is known for a particular entry in the route cache. Routing in DSR is completed using two levels- route discovery and route maintenance. When a source node desires to send a packet to a destination, it first accesses its route cache to determine whether it already be familiar with about any route to the destination or not. If an entry for the destination is already there, the source uses that to send the packet. If not, it initiates a route request broadcast. This request includes the destination address, source address, and a unique identification number. Each intermediary node checks whether it be acquainted with about the destination or not. If the intermediary node does not know about the destination, it again forwards the packet and ultimately this reaches the destination. A node processes the route request packet only if it has not previously processed the packet and its address is not present in the route record of the packet. A route reply is generated by the destination or by any of the intermediate nodes when it knows about how to reach the destination [3].

2.2.3 Light-weight Mobile Routing (LMR)

The LMR protocol is based on the concept of link reversal algorithm. LMR addresses the issue of partitioned network by providing a link deletion mechanism. LMR requires two passes to re-establish and converge to an alternate route, if one exists. LMR can erase invalid routes and detect partition in a single pass. The benefit of this protocol is that routes will be found rather quickly and broken links will have only local affect. It has good performance if the network connectivity, i.e., in the case of dense network.

2.2.4 Associativity Based Routing (ABR)

ABR protocol defines a new type of routing metric, degree of association stability for mobile ad hoc networks. In this routing protocol, a route is selected based on the degree of association stability of mobile nodes.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

2.2.5 The Enhanced On Demand Multicast Routing Protocol (EODMRP)

The Enhanced On Demand Multicast Routing Protocol (EODMRP) is an enhancement of ODMRP, which is a reactive mesh-based multicast routing protocol. It is an enhanced version of ODMRP with adaptive refresh. Adaptation is driven by receivers' reports. The second enhancement is the "unified" local recovery and receiver joining scheme. The major advantage is reduced overhead, which translates into a better delivery rate at high loads, yet keeping the same packet delivery ratio as the original ODMRP [4].

2.3 Hybrid routing protocols

Hybrid routing protocols are a new generation of protocols, where both proactive and reactive in nature. These protocols are designed to increase scalability by allowing nodes with close proximity to work together to form some sort of a backbone to reduce the route discovery overheads.

- Some of the existing hybrid routing protocols are:
- Temporally Ordered Routing Algorithm (TORA)
- Zone Routing Protocol (ZRP)
- Zone-based Hierarchical Link State (ZHLS)
- Sharp Hybrid Adaptive Routing Protocol (SHARP)
- Optimized Polymorphic Hybrid Multicast Routing Protocol (OPHMR)

2.3.1 Temporally Ordered Routing Algorithm (TORA)

Temporally Ordered Routing Algorithm (TORA) is a reactive routing algorithm based on the thought of link reversal. TORA expands the partial link reversal method by distinguishing partitions and preventing non-productive link reversals. It can be used for vastly dynamic mobile ad hoc networks.

2.3.2 Zone Routing Protocol (ZRP)

ZRP (Haas, 1997; Haas & Pearlman, 1998) it is a hybrid routing protocol which gives the advantages of both proactive and reactive methods. It takes benefit of proactive protocol to find node's local region as well as reactive protocol for routing between these neighborhoods.

In a Mobile Ad-hoc Network, it can be presumed that most of the communication takes place between adjacent nodes. The ZRP splits the entire network into overlapping zones of flexible size. Each node may belong to multiple overlapping zones. The zone size is defined by a radius which is evaluated in number of hops.

2.3.3 Zone-based Hierarchical Link State (ZHLS)

The Zone-based Hierarchical Link State routing (ZHLS) is a hybrid routing protocol. In ZHLS, mobile nodes are presumed to recognize their physical locations with support of locating system like GPS. In ZHLS protocol, the network is distributed into non- overlapping zones as in cellular networks. Each node identifies the node connectivity inside its own zone and the zone connectivity data of the entire network. The link state routing is done by commissioning two levels: node level and global zone level. ZHLS does not consume any cluster head in the network like other hierarchical routing protocols.

2.3.4 Sharp Hybrid Adaptive Routing Protocol (SHARP)

SHARP explains reactive and proactive routing by energetically changing the volume of routing data shared proactively. This protocol defines the proactive zones nearby nodes. The number of nodes in a precise proactive zone is determined by the node-specific zone loop. All nodes inside the zone loop of a node become the member of that proactive zone for that node. If for a given destination a node is not present within a precise proactive zone, reactive routing mechanism is used to produce the route to that node.

2.3.5 The Optimized Polymorphic Hybrid Multicast Routing Protocol (OPHMR)

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

The Optimized Polymorphic Hybrid Multicast Routing protocol (OPHMR) is 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. The protocol is based on the principle of flexibility and multi-behavioral ways of operations.

III. SECURITY CHALLENGES IN MANET

Security is a very challenging problem for designing a well-organized and secure routing protocol for MANETs. The infrastructure less and the dynamic nature of MANET demands new set of networking policies to be executed in order to provide effective and secure end-to-end communication. Due to the absence of a predefined centralized management for route discovery process which leaving MANETs susceptible to attacks, that results in degradation in the performance of the network. Security attacks interrupt routing processes which create many problems like Denial of Service, Jamming the network or other types of serious attacks in the network.

IV. TYPES OF SECURITY ATTACKS

Security is one of the highly challenging issues for Mobile Ad-hoc Networks. Understanding possible form of attacks is always the primary step towards the development of good security solutions for routing algorithms as well as secure communication. Security of communication in MANET is significant for secure data transmission in MANET. Lack of any central administration mechanism and shared wireless mode makes MANET more susceptible to digital attacks than wired networks.

There are various types of attacks that affect MANET communication and its security. These attacks can be classified into two types:

- Passive attacks
- Active attacks

4.1 Passive attacks

In Passive attacks, attacker don't harm any data in the network instead of it he analyze network traffic like identify communicating nodes, monitor data which is exchanged between them and steal valuable information. A passive attack attempts to learn or make use of information from the network. In passive attacks, attackers don't interrupt the procedure of routing protocol, but only attempt to notice valuable information by snooping to the routing traffic. The attacker only observed the transmission and does not try to alter the data packets. Recognition of these attacks is tough since the operation of network itself does not get affected. Passive attacks are performed the eavesdropping, traffic analysis and monitoring operations.

Some passive attacks are:

- Traffic analysis
- Eavesdropping
- Traffic monitoring
- Release of message contents
- Snooping

4.2 Active attacks

In active attacks, attacker dynamically modify the data such as message alterations, message replays and message fabrications. It disrupts normal functionality of the network. Active attacks consist in perturbing the algorithm process to obtain an abnormal behavior and/or an erroneous computation result that can be exploited to recover entirely or partially the secrets [5].

Some active attacks are:

- Network Jamming
- Denial of service

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

- Impersonating
- Modification
- Message reply
- Spoofing
- Masquerade

V. CONCLUSION

A Mobile Ad-hoc Network (MANET) contains self-configuring, self-organizing and self-operating nodes, each of them communicates with other nodes directly, without any help of centralized management or fixed infrastructure, within transmission range of nodes.

Due to the quickly installation behavior, dynamic configuration, various advantages and different application areas, the field of MANETs is rapidly growing and changing. Although there are still many challenges and issues that need to be faced by the Mobile Ad-hoc Network. In order to secure and effective communication within a MANET, an effective routing protocol is required to determine routes between mobile nodes. The common objective of routing protocol is to provide better efficient energy conscious and secure routing schemes to MANET. We have focused on the several routing protocols that can be well-suited for certain conditions. Therefore, more study is required to combine and integrate some of the protocols presented in this paper to keep MANETs effective for a longer period. Developing efficient and secure routing protocols for MANET appears to be a promising direction of future research works.

REFERENCES

[1] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan, "A Local Intrusion Detection Routing Security over MANET Network", IEEE International Conference on Electrical Engineering and Informatics (ICEEI), 2011.

[2] P. Shrivastava, S. Kumar and M. Shrivastava, "Study of Mobile Ad hoc Networks", International Journal of Computer Applications, Vol. 86, No 3, January 2014.

[3] Shiv Prakash, Rajeev Kumar, Brijesh Nayak and Manindar Kumar Yadav, "A Survey on Reactive Protocols for Mobile Ad Hoc Networks (MANET)", Proceedings of the 5th National Conference; Computing For Nation Development, March 2011.

[4] 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.

[5] Frederic Amiel, et al., "Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel Analysis", Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), September 2007

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

[7] Shesh Kumar Sharma, Ramendra Kumar, Anshul Gangwar, Kamljeet Pakhre, "Routing Protocols and Security Issues in MANET: A Survey", International Journal of Emerging Technology and Advanced Engineering, Vol. 4, No. 4, April 2014.

[8] Amara korba Abdelaziz, Mehdi Nafaa and Ghanemi Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks", IEEE 15th International Conference on Computer Modelling and Simulation (UKSim), 2013.