Comparative Study Of Secure Routing Protocol For Manet: A Review

Snehal T. Kalokhe1, Sayali N.Mane2
1 Second Year PG student,DPCOE,Akurdi
2 Assistant Professor, DPCOE,Akurdi
Correspondence Author: Snehal T. Kalokhe

ABSTRACT:
MANET is self-structured wireless network (ad-hoc network) with fewer infrastructures connecting mobile devices wirelessly. The extensibility and portability of mobile ad-hoc network becoming more popular. Security in ad –hoc network has recently boosted to drive in the research community. Due to open nature of ad-hoc network, dynamic topology and lack of infrastructure security issue can be barrier to basic network operation. To address these security goals like Confidentiality, Integrity non-repudiation, privacy, etc. has to be maintaining in order to meet the reliable and secure ad-hoc network environment.

KEYWORDS: *MANET, Table Driven, AODV, DSR, OLSR, Black whole, Gray whole ,WRP*

Date of Submission: 04-07-2018 Date of acceptance: 19-07-2018

I. INTRODUCTION

There has been increasing growth in the use and development of wireless network. MANET is designed collection of wireless mobile nodes that are able to correspond with each other beyond the structured network infrastructure. MANET is also called as "Infrastructure less Networking". Since the mobile nodes in ad-hoc network dynamically build routing network among themselves to form their own network to communicate. Features of MANET make it useful and popular. Present Wireless research signify that the wireless MANET present a larger security problem. MANET communication is wireless communication and it can be insignificantly (block, defect) by any node in the range of transmitter. Resulting the network an open variety of attacks MANET s easily affected due to decentralized network, lack of well-defined boundary, unstable. Structure of nodes resulting less assurance in QoS .Attacks in MANET are classified as 1) Passive attacks 2) Active attacks Routing plays vital role in security of whole network .In this article we study the security mechanisms, comparing the routing techniques according to its result.

Routing Security for MANET:
Each device inside MANET is known as a node. It acts as both client and router. Communication in the MANET is accomplished by forwarding packets to destination node .Node in an ad-hoc network function as router. It derives and maintains the path /routes to other nodes in the network. Hence routing security is becoming necessary in present era. The constitutional goal of MANET routing protocol is to create a perfect and efficient route between the nodes within network. If routing become mismanage, the entire network can be enfeeble. Here we study the basic routing protocols for MANET Security attacks in network are Repudiation, Data corruption, Worm hole, Black hole, Message tampering attack, message dropping attack etc are available[6]

MANET routing protocol
Classification of routing protocols in MANET's can be done in various approaches, but most of these are done depending on routing strategy and network architectures. Routing protocol for MANET can be classified as Proactive and Reactive, determined on how they react when topology changes. Classification of MANET routing protocols are classified as follows

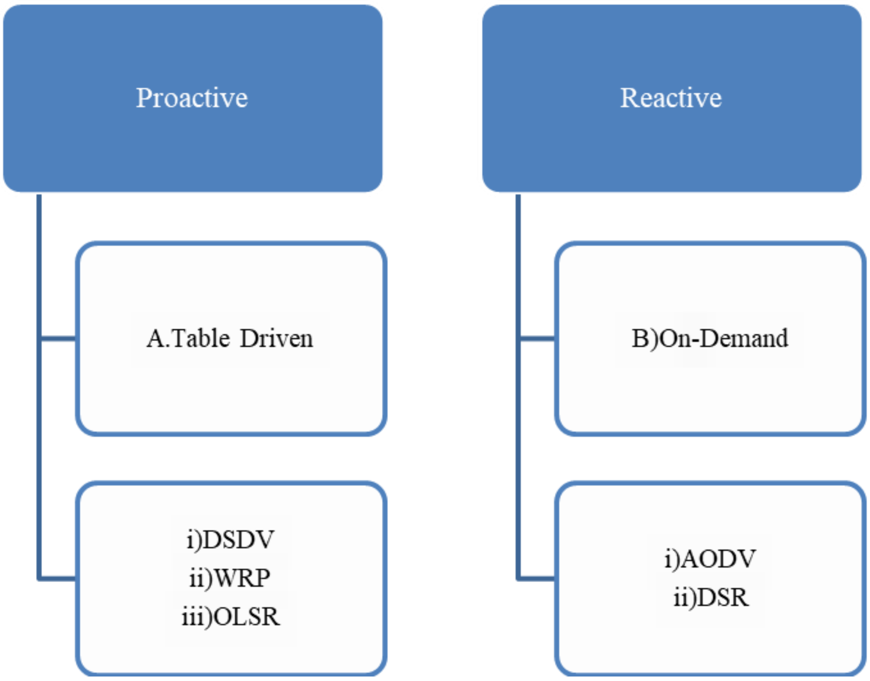

Fig1.Classification of MANET routing protocols

A) Table Driven-Table driven is proactive approach. This type of Protocol mange recent list of destination and their routes by repeatedly providing routing tables in present network. It avoids and tries to hold back data from being attacked by using some cryptographic techniques. Router discovery is unnecessary. Table driven protocol modify in the way they maintain and update routing tables, which directly affect the efficiency of each protocol. Bandwidth is occupied by unused path.

i) DSDV (Destination Sequenced Distance Vector)-Routing information available immediately from routing table. It uses more bandwidth to send message. It is not scalable. It requires regular update of routing table.

ii) WRP (Wireless Routing Protocol): In WRP each node has to maintain four tables. These are Distance table, Routing table, Link cost table, and MRL table .It avoids the count-to-infinity problem. Four tables requires large amount of memory.

iii) OLSR (Optimized Link State Routing) - OlSR protocol execute hop by hop routing.it adopt the presently used information for routing packet to destination. It is necessary to maintain routing table for all possible routes. OLSR requires more processing power than other protocols. It accessible to variety of attacks like flooding attack, link withholding attack, replay attack, DOS attack called node isolation attack [5].

B) On demand-It is reactive approach. It firstly detects the threats and then reacts suitably. It searches a route on the basis of on demand by flooding the network with route request packets

i) AODV (Ad hoc-on Demand Distance Vector)-A source initiate a route discovery process by flooding route request (RREQ) packet in network. A route reply (RREP) is sent back to the source node using reversal link by destination node [2]. The main drawback of this protocol is High Latency time in route finding and Excessive flooding can lead network to be obstruct.

A black whole problem is eliminated with secured AODV protocol by disabling the ability of intermediate node to reply. Hence all reply messages sent out by only destination node. But these derived two disadvantages. First routing delay is increased second malicious node can take actions such as create reply of message instead of destination node

ii) DSR (Dynamic Source Routing)-In DSR source node initiate route discovery. All routes which contain breakage hop have to be removed from the route packet. Source node floods Route Request (RREQ) in the network and uses broadcast method to send Packet header size increase with increase in route path length due to inefficiency of source node. Reactive nature of this protocol exterminates the need of periodically flood the network with table updates in Table Driven type. Gray whole attack has high effect on DSR protocol, based on the number of attacks; the packet delivery ratio is high or low. If the number them increase packet delivery ratio will decrease, because gray whole is present

II. CONCLUSION

This article covers some important accepted routing protocol, security issues and security attacks. Every protocol has some advantages and disadvantages. We study both proactive and reactive routing protocol.

Different types of routing protocol techniques are compared with its advantages and drawbacks. An individual protocol is enable ton fulfill all network performance parameters. Hence according to requirements of network, routing protocol is selected

REFERENCES

[1]. Hicham AMRAOUI1 Ahmed HABBANI1, Abdelmajid HAJAMI, Essaid Bilal, “Security & Cooperation Mechanisms Over Mobile Ad hoc Networks: A Survey and Challenges” 3rd International Conference on Electrical and Information Technologies ICEIT’2017

[2]. Hongmei Deng, Wei Li,and Dharma P.Agrawal, University of Cincinnati, “Routing Security in Wireless Ad Hoc Networks”, IEEE Communications Magazine , October 2002

[3]. Mr. L Raja ,Capt. Dr. S Santhosh Baboo, “Comparative study of reactive routing protocol (AODV, DSR, ABR and TORA) in MANET” International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 3 March 2013

[4]. Mohammad S. Obaidat, Isaac Woungang, Sanjay Kumar Dhurandher, Vincent Koo, “Preventing Packet Dropping and Message Tampering Attacks on AODV-based Mobile Ad Hoc Networks” 2012 IEEE

[5]. K.URMILAVIDHYA, M MOHANA PRIYA,A “Novel Technique For Defending Routing Attacks in OLSR MANET”2010 IEEE International Conference

[6]. Mohammad S. Obaidat, Isaac Woungang, Sanjay Kumar Dhurandher, Vincent Koo, “Preventing Packet Dropping and Message Tampering Attacks on AODV-based Mobile Ad Hoc Networks” 2012 IEEE

Snehal T. Kalokhe"Comparative Study Of Secure Routing Protocol For Manet: A Review, International Journal of Computational Engineering Research (IJCER), vol. 8, no. 7, 2018, pp. 01-03.