International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

ATTACKS AND ROUTING PROTOCOLS IN MANET: A REVIEW

Neha Sharma[1], Dr. Harpal Singh[2]

[1] Student , [2] Professor, CGC Landran

Abstract: *An analysis on mobile ad hoc network has been provided in this paper which is considered as a temporary network with the nodes moving freely from one position to other position without the need of an administrator. All the nodes communicate with each other through radio link and follow different topologies and protocols for transmitting the data packet within the network. Description of MANET with its characteristics has been provided along with its types. For finding the route within the network having no congestion, different types of routing protocols are defined. The routing protocols are basically divided into reactive, proactive and hybrid protocols. The examples for the same are also drawn following their comparison on the basis of characteristics and parameters. In MANET routing protocols, occurrence of different attacks exists that are considered as a problem while sending the information. In this review, attacks, namely, black hole attack, gray hole attack and DoS (Denial of Service) are mentioned with an appropriate example.*

Keywords: Mobile ad hoc network, Routing protocols, black hole attack, DoS attack, gray hole attack

1. Introduction

MANET is a network comprises of a large number of wireless nodes without any need of centralized administrator. The structure of MANET changes continuously as the nodes are free to move and make self organized network [1]. All the nodes utilize the same wireless channel. The node in the network usually acts like a router as well as a host and transfers the data from source to destination. The architecture of Ad hoc network is shown in figure 1. Nodes in MANET communicate at radio frequency ranges from 30 MHz to 5 GHz. Due to the increasing use of laptop and wireless networks, MANET has become a hot topic for research.

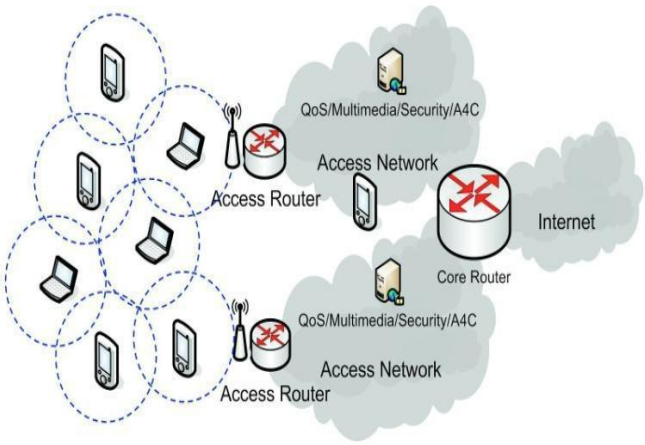

Fig.1Architecture of Ad-hoc network

Ad hoc network comprises of various devices such as Access point, router, nodes, and router. The handover of data from one to another node is purely different from handover on mobile networks, because in ad hoc network the control information needs to be minimized [2].

1.1 Types of MANET

MANET is mainly classified into three types including:

- InVANET- It is known as intelligent vehicular ad hoc networks and is used to detect vehicle accidents by using artificial intelligence.
- VANET- It is known as Vehicular ad hoc network and used for communicating with vehicles.
- IMANET- named as Internet based mobile ad hoc network used to communicate with fixed as well as mobile nodes

The main characteristic of the MANET is to retain bandwidth and battery power. The researcher's main aim is to design a network in which nodes consumes less power and used small bandwidth [3].

1.2 Routing protocols in MANET

Routing protocols are used in the network to set some rules that must be followed by every node in the network for the transmission of data packet. In MANET, numbers of routing protocols are used and the selection of accurate protocol is dependent upon the situation. There are three types of routing protocols as defined below:

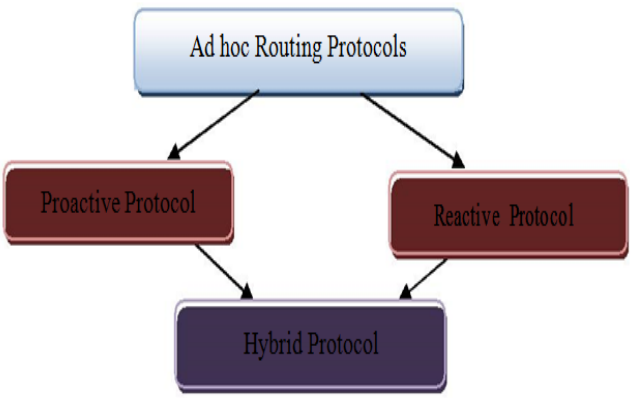

Fig.2 Classification of routing protocols

i. Proactive routing protocol

These protocols are also known as Table driven routing protocols because they maintain the routing information in the tabular form. All the nodes in the networks maintain the routing information for every single node. Routing information in the table is updated automatically as per the network topology. The proactive protocols are not used for the large network as it requires the routing information of each and every node in the network which requires more bandwidth. Examples of proactive routing protocol are DSDV, OLSR, and HSR [4].

a. DSDV (Destination sequenced distance vector routing)

DSDV is modified from the traditional RIP (Routing Information Protocol) for ad hoc networks routing. Every mobile node in the network keeps a routing table for all probable destinations in the network and the number of hops for every destination node. Every entry is taken with a sequence number and the number given by the destination node. The updates of routing table are periodically transferred throughout the network for maintaining the table consistency. A lot of route updates, network traffic may employ into packets, namely, "Full Dump" and "Incremental routing".

b. OLSR (Optimized Link State Routing)

It is a protocol drawn for MANET and VANET, that utilizes hello and TC (topology control) messages for discovering and later disseminating link state information for mobile ad-hoc network. The individual nodes utilize the topology information for computing the subsequent hop destinations for each node in the network by utilizing shortest hop forwarding paths.

c. HSR (Hierarchical state routing)

The main feature of HSR is logical partitioning of mobile nodes and multilevel clustering. The network is categorized in clusters and a cluster-head is considered as a cluster dependent algorithm. The cluster-heads later maintain it as clusters. The physical cluster nodes transfer the link information towards each other. The cluster head outline the cluster's information and transfers it to neighboring cluster-heads through gateway.

ii. Reactive routing protocol

These protocols are also known as on demand routing protocols. In this protocol, the routing table is not maintained for each and every node in the network. The route is maintained only for communicating or active nodes. Whenever a node wants to transmit data packet from one node to other node, its route is determined in route table using on demand approach and connection is established between them. The route is determined by passing route request packets in the whole network. AODV and DSR are the examples of reactive routing protocols [5].

a. AODV (Ad Hoc On-Demand Vector)

AODV maintains the request via route request plus route request Query. The varied types of control messages intended for route maintenance in AODV are: RREQ, RREP and RRER.

b. DSR (Dynamic Source Routing)

This protocol utilizes the source routing rather on depending on routing table at every subsequent device. It takes every address by means of source towards destination when route discovery takes place. For avoiding the long paths or huge addresses, DSR permits the packet to be passed via hop-by-hop.

iii. Hybrid routing protocol

It is a combination of both the above mentioned proactive and reactive routing protocols. Example of hybrid routing protocol are ZRP, AMDMM, and SALMA etc.

a. AMDMM (Audit Misbehavior Detection and Monitoring Method)

This protocol is used to provide a secure environment in MANET. The main work of this protocol is to detect a malicious node within the network and secondly, look after the nodes that are continuously dropping the data packets. It basically monitors each and every node and accordingly decides that which node is malicious so that the network performance can be increased. It mainly works in three phases, namely, reputation process, auditing process, and route discovery process.

b. ZRP (Zone Routing Protocol)

ZRP protocol is used to reduce the control overhead of proactive routing protocols and latency occur due to route. The secure communication can take place between the nodes that are close to each other. ZRP is used to provide a framework to other protocols.

c. SALMA (State Aware Link Maintenance Approach)

This protocol is a combination of both proactive and reactive routing protocol and it helps to decrease the load on the network. By using this protocol, the nodes are divided into three types (1) Aware and active nodes known as black node, (2) aware but not performing data transfer except data forwarding which are called gray nodes, and (3) white nodes which are idle and do not keep any routing information. Buffer is used to determine the type of node. This buffer stores a numerical value in order to identify the state and operation of the active node. The value of keep-

awake buffer was triggered by the counter known as keep awake counter. A white node is denoted by 0 (zero) and it is stored into the keep-awake buffer. A gray and black node is recognized by the odd or even numbers in the buffer. The comparison between these three routing protocols is provided below in table 1. The comparison has been drawn on the basis of number of characteristics, namely, Routing structure, routing overhead, scalability, mobility, routing information, bandwidth, power and storage.

Table.1 Comparison of routing protocols

Characteristics	Proactive	Reactive	Hybrid
Routing structure	Hierarchical and flat	Flat	Hierarchical
Route type	Table driven	On demand	Both table driven and on demand
Routing overhead	High	Low	Medium
Scalability	Low	Not used for large network	Used for large area
Routing information	Available always	Available when needed	Integration of both
Mobility	Updated periodically	Maintain route	Combined both
Storage	Require large space	Require low space	Require medium space
Bandwidth	Need large bandwidth	Need small bandwidth	Need medium bandwidth
Power	Require high power	Require less power	Require medium power

Below table 2 is showing the comparison of DSDV, AODV and ZRP routing protocols. The comparison has been drawn on the basis of parameters, namely, routing protocol type, route selection, routing structure. The advantages and disadvantages are also shown for AODV, DSDV and ZRP.

Table 2 Comparison of AODV, DSDV and ZRP routing protocol

Parameters/Advantages /Disadvantages	AODV	DSDV	ZRP
Routing protocol Type	Reactive	Proactive	Hybrid
Routing structure	On-demand	Table driven	Combination of both
Route selection	Short and updated path	Link state	Link reversal
Route maintenance	Route table	Route table	Link table
Advantages	1. Adaptive to high dynamic topology 2. Loop free 3. Large bandwidth due to less overheads	1. Loop free 2. Shortest route to all designations is selected.	1. Performed in properly configured area in which both reactive and routing protocols are performed.
Disadvantages	1. More delay 2. More time to make the routing table	1. High overhead 2. Multiple routing is not possible.	1. Route to sink node is suboptimal 2. Require more memory space

3. Attacks on MANET protocol

A number of attacks like black hole attack, wormhole attack, sink hole attack, and gray hole attack occurs in MANET routing protocol. The explanation for the same is defined below.

i. Black hole attack

Black hole attack is the serious problem for the MANET, in which a malicious node sends wrong routing information, defining that it suggests the shortest path to the sink node with the packets it wants to interrupt and then grip them without promoting to the destination. For example, in AODV, the malicious node can send fake route reply (RREP) packets. Due to which all the traffic is conveyed through the malicious node and thus, the malicious node can misuse or reject the traffic [6].

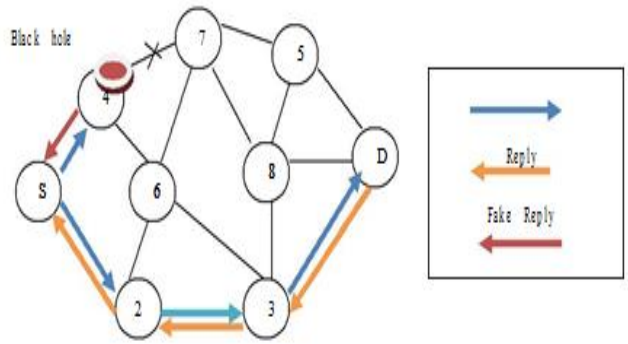

Fig.3 Black hole attack

As shown in the figure above, at node four in the network black hole attack occurs. Here, S is the source node and D is the destination node. When source node wants to transmit data packet, it will send the request which is indicated by blue arrow. When destination node receives the request then in response to this, request destination node send a reply message which is shown by yellow arrow. When the node with black hole attack receives the request message then it will also send a fake reply which is indicated by red arrow [7].

ii. Gray hole attack

A gray-hole attack is an expansion of black-hole attack which is used to fraud the source node and networking system by partial forwarding. The attackers behave as a true node and try to take part in the full transmission and reception of data packet process. When gray hole attack occurs in the network it will update the routing table falsely and tell the source node that gray hole malicious node is the shortest path to transmit the data. Thus, source node considers it as next hop node and transmits data to the malicious node. Malicious node catches all the incoming packets but drops on arbitrary basis. The detection and prevention of node become difficult as the drop of the packet may be due to overloading, congestion etc. [8].

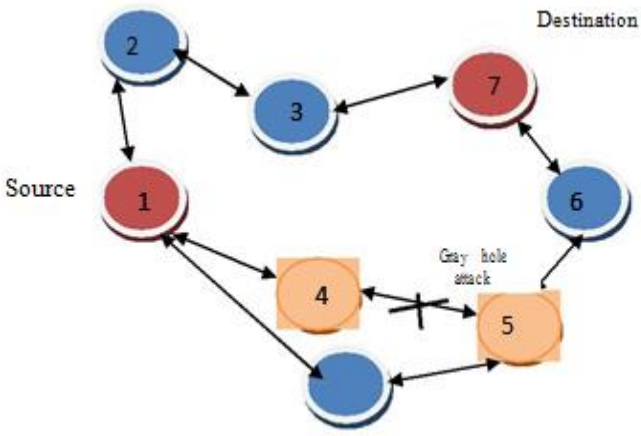

Fig.4 Gray hole attack

iii. DoS (Denial of Service) attack

In this type of attack, an attacker transmits a large number of packets to the server to slow down the speed of server. Thus, the resources are not available to the users and hence, the genuine user cannot access the facility. As shown in the figure below, PC 1 send request to all PC's named as 2, 3, 4, 5and 6. When these PC's gets the request than it is being forwarded to the server. It is concluded that server has a number of requests at the same time due to this process the user can not access the resources [9].

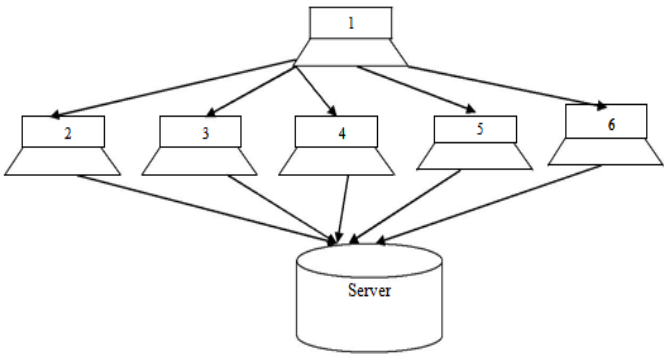

Fig.5 DOS Attack

4. Related work

Z. Li and Y. Wu [10, 2017] proposed a method that used Optimized link state routing (OLSR) protocol. The proposed scheme has been used for increasing the reliability of the node and the simulation results proved that the proposed method has greater accuracy along with fewer overheads. Y. H. Chen et al. [11, 2017] proposed a multicast routing protocol that has been used for reducing the total bandwidth consumption. Y. Fang, et al. [12, 2017] proposed a method that has been considered both buffer size and packet lifetime. The problem of end to end delay has been overcome by using a practical MANET.C. Wu et al. [13, 2017] presented an approach for MANET, where nodes are individual and strategic users. A single route has been used for securing the data, forwarding the packets. Chin et al. [14, 2002] implemented a network by using different protocols named as MAD-HOC, AODV and DSDV. All the simulations have been carried out in NS-2 simulator tool. A number of problems like packet loss, handling unreliable, and neighbor discovery and filtering sub layers have been resolved. S. Abbas et al. [15, 2013] proposed an approach to identified Sybil attackers. Authors had not used any extra hardware device such as directional antennae or a GPS system. Better accuracy has been obtained in the presence of Sybil attack. P. S. Hiremath et al [16, 2016] proposed asystem that has been used to detect and prevent the black hole attack. For detection and prevention, Fuzzy logic interface method has been used. AODV routing protocol has been used and the code has been run on NS- 2 simulator tool. K. A. A. Kumar [17, 2016] proposed an algorithm named as FPGA mused for

detection of black hole and warm hole attack in the system. When attack occurs in the network the packet traveling time has been changed.

5. Conclusion

In this paper, we have described MANET (Mobile ad hoc network). Firstly, the brief introduction along with the basic idea of MANET has been provided. Then, types of MANET along with routing protocols have been discussed and comparison among routing protocols have been provided. At last, different attack named as black hole attack, DOS attack and gray hole attack are described in detail. It is being concluded that mobile networking has become an important and essential technique that supports future computing methods.

References

[1] C. T. Calafate, M. P. Malumbres, J. Oliver, J. C. Cano and P. Manzoni, "QoS Support in MANETs: a Modular Architecture Based on the IEEE 802.11e Technology," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, no. 5, pp. 678-692, May 2009.

[2] C. I. Katsigiannis, D. A. Kateros, E. A. Koutsoloukas, N. D. Tselikas and I. S Venieris, "Architecture for reliable service discovery and delivery in manets based on power management employing slp extensions," in IEEE Wireless Communications, vol. 13, no. 5, pp. 90-95, October 2006.

[3] H. Shen and L. Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," in IEEE Transactions on Mobile Computing, vol. 12, no. 6, pp. 1079-1093, June 2013.

[4] H. Xu, X. Wu, H. R. Sadjadpour and J. J. Garcia-Luna-Aceves, "A unified analysis of routing protocols in MANETs," in IEEE Transactions on Communications, vol. 58, no. 3, pp. 911-922, March 2010.

[5] K. Viswanath, K. Obraczka and G. Tsudik"Correction to "Exploring Mesh and Tree-Based Multicast Routing Protocols for MANETs"," in IEEE Transactions on Mobile Computing, vol. 6, no. 2, pp. 237-237, Feb. 2007.

[6] Sun, Bo, Yong Guan, Jian Chen, and Udo W. Pooch. "Detecting black-hole attack in mobile ad hoc networks," pp. 490-495, 2003.

[7] Tseng, Fan-Hsun, Li-Der Chou, and Han- Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," Human-centric Computing and Information Sciences, vol.1, pp. 4-10, 2011.

[8] J. Sen, M. G. Chandra, S. G. Harihara, H Reddy and P. Balamuralidhar, "A mechanism for detection of gray hole attack in mobile Ad Hoc networks," 2007 6th International Conference on Information, Communications & Signal Processing, Singapore, 2007, pp. 1-5.

[9] Nadeem, Adnan, and Michael Howarth, "Adaptive intrusion detection & prevention of denial of service attacks in MANET's Proceedings of the2009 international conference on wireless communication and mobile computing. Connecting the world wirelessly. ACM, 2009.

[10] Z. Li and Y. Wu, "Smooth Mobility and Link Reliability-Based Optimized Link State Routing Scheme for MANETs," in IEEE Communications Letters, vol. 21, no. 7, pp. 1529-1532, July 2017.

[11] Y. H. Chen, E. H. K. Wu and G. H. Chen, "Bandwidth-Satisfied Multicast by Multiple Trees and Network Coding in Lossy MANETs," in IEEE Systems Journal, vol. 11, no. 2, pp. 1116-1127, June 2017.

[12] Y. Fang, Y. Zhou, X. Jiang and Y. Zhang, "Practical Performance of MANETs Under Limited Buffer and Packet Lifetime," in IEEE Systems Journal, vol. 11, no. 2, pp. 995-1005, June 2017

[13] C. Wu, M. Gerla and M. van der Schaar, "Social Norm Incentives for Network Coding in Manets," in IEEE/ACM Transactions on Networking, vol. 25, no. 3,pp. 1761-1774, June 2017.

[14] Chin, K. W., Judge, J., Williams, A., & Kermode, R., " Implementation experience with MANET routing protocols," ACM SIGCOMM Computer Communication Review, vol.32, pp.49-59, 2002.

[15] S. Abbas, M. Merabti, D. Llewellyn-Jones and K. Kifayat, "Lightweight Sybil Attack Detection in MANETs," in IEEE Systems Journal, vol. 7, no. 2, pp. 236-248, June 2013.

[16] P. S. Hiremath, Anuradha T and P. Pattan"Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs," 2016 International Conference on Information Science (ICIS), Kochi, 2016, pp. 245-251

[17] K. A. A. Kumar, "Worm hole-black hole attack detection and avoidance in Manet with random PTT using FPGA," 2016 International Conference on Communication Systems and Networks (ComNet), Thiruvananthapuram, 2016, pp. 93-98.