International Journal of Advance Research in Science and Engineering
Volume No.07, Issue No.09, September 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

SECURE MANET ROUTING WITH BLACKHOLE AVOIDANCE

[1]Snehalkalokh, [2]Sayali Mane

[1]PG student , D. Y. Patil College of Engineering, Akurdi,Pune, India-411044

[2]Assistant Prof. E&TC, D. Y. Patil College of Engineering, Akurdi,Pune, India-411044

Abstract:.*MANET is self-designed wireless network (Ad-hoc network) with minimum infrastructure connecting mobile devices wirelessly. The wide popularity and portability of mobile ad-hoc network becoming more famous, to provide security to these networks, Security protocols have make progressto protect routing information and data. Network topology is expeditiously changes due to nodes mobility, Resource constraints Bandwidth limitations. In infrastructure less network node needs to cooperate to each other to provide necessary network functionality. AODV routing protocol is most preferably used in MANET. Due to open nature of ad hoc network lack of infrastructure security issue can be barrier to basicnetwork operation. If routing become mismanage, the entire network can be enfeeble. Hence routing security is becoming necessary in present era.*

Indexterms:*MANET,Security attacks, AODV, DES,Black- Hole Attack*

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.Recently wireless research signify that the wireless MANET present a larger security problem. As compared to other conventional network, MANET has somecharacteristic such as open medium dynamically changing network topology, self-considering ability distributed cooperation. There are some other characteristics of a MANET such as limited bandwidth and limited battery power. These characteristics makes MANET more vulnerable to several different attacks, for instant black hole attack, wormhole attack, link spoofing attack to name a few. One of the major attacks possible in MANET that can easily be implemented is black hole attack.

MANET communication is wireless communication and it can be insignificantly block by any node in the range of transmitter Network topology in present system is dynamic. Each node acts as both host and router 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. This paper proposes novel security framework for MANET routing with Ad-hoc on demand approach reactive protocol with DES security algorithm for secure transmission of data to reach destination and detecting black hole attack,

II. SECURITY ISSUES IN MANET

MANET is little secure as compare to wired network. Every node has self-considering ability. User mobility is high in it.Nodes connections are deviant and lack of security because of network topology is dynamic. Resulting MANET becomes less Secure.[1]

III.SECURITY ATTACKS IN MANET[7]

OSI Layers	Attacks
1.Physical Layer	Jamming. Tampering
2.Data link Layer	Collision, Traffic analysis
3.Transport Layer	Energy Drain attacks, session hijacking ,Inject false message

Table1. Type of security attacks on layers basis

IV. PROBLEM FORMULATION

1.Ad hoc-on Demand Distance Vector(AODV) :

AODV protocol constructs routes between nodes only if they are called by source node, hence known as on – demand. It does not introduce any traffic error for communication along links. The routes between the communications links are maintained as long as they required by the source.AODV promote routing table to store routing information.) Routing table for unicast routers ii) Routing table for multicast routers A route table stores destination address, next hop address destination sequence number, life-time. AODV eliminate "Counting to Infinity" error by introducing destination numbers. It makes AODV "loop free". AODV defines three basic message types namely Route Requests (RREQ), Route Reply(RREP) and Route Error(RERR).RREQ messages are used to establish route finding process. RREQ messages are used for confirmation of the routes. RERR are used to inform the network of link breakage in an active route.AODV has two stepsRoute discovery and Route maintenance. 2.Black-Hole Attack: The attacker send false routing information, conveying that it has a best route and attract other nodes to transfer data.Attacker node participates in route finding methods by sending RREP message. When source node starts transmission of data, the faulty node do not forward them to

destination and destroy them. It is more destructive than grey hole attack.In an ad-hoc network that uses the AODV protocol, a Black-Hole node captures the network traffic and drops all packets. To analyse the Black-Hole Attack we compute a malicious node that illustrate Black-Hole. If the sending node deliver UDP data packets the errors are not detected because the UDP data connections unable for waiting the ACK[1]

VI.METHODOLOGY AND SIMULATION

DES Security Algorithm: DES (Data Encryption Standard) algorithm purpose is to provide a standard method for protecting sensitive commercial and unclassified data. In this same key used for encryption and decryption process

Black holeDetection :A population of network nodes is generated and distributed randomly in the search space.After initialization, the fitness values of the population are evaluated and the best candidate in the population, which has the best fitness value, is selected to be the black hole and the rest form the normal nodes. The fitness is calculated by Rosenbrok fitness function ,

$$f\ (x, y) = (a - x^2) + b(y - x^2)\text{^}2$$

Where x and y are position of nodes and parameters values are taken constant as a=1 and b=100The black hole has the ability to absorb the data transmitted sent by surrounding nodes. After initializing the black hole and nodes, the black hole starts absorbing the nodes around it and all the nodes start moving towards the black hole. The absorption of nodes by the black hole is formulated as follows:

$$Xi(t + 1) = xi(t) + ran \times \left(XBH - Xi(t)\right)$$

$$i = 1,2,3,4 \dots \dots . . N$$

where xi(t) and xi(t + 1) are the locations of the ith node at iterations t and t + 1, respectively. xBH is the location of the black hole in the search space. rand is a random number in the interval [0,1]. N is the number of nodes (candidate solutions).While moving towards the black hole, a node may reach a location with lower cost than the black hole. In such a case, the black hole moves to the location of that node and vice versa. Then the BH algorithm will continue with the black hole in the new location and then nodes start moving towards this new location. In addition, there is the probability of crossing the event horizon during moving nodes towards the black hole. Every node (candidate solution) that crosses the event horizon of the black hole will be sucked by the black hole. Every time a candidate (node) dies – it is sucked (absorbed) in by the black hole – another candidate solution (node) is born and distributed randomly in the search space and starts a new search. This is done to keep the number of candidate solutions constant. The next iteration takes place after all the nodes have been moved.

The radius of the event horizon in the black hole algorithm is calculated using the following equation:

$$R = \frac{fBH}{\sum_{i=1}^{N} fi}$$

wherefBH is the fitness value of the black hole and fi is the fitness value of the ith node. N is the number of nodes (candidate solutions). When the distance between a candidate solution and the black hole (best candidate) is less than R, that candidate is collapsed and a new candidate is created and distributed randomly in the search space. The distance is calculated using Euclidean distance algorithms.

Algorithm

Initialize a population of nodes with random locations in the search space

Loop : For each node,

- evaluate the objective function
- Select the best node that has the best fitness value as the black hole
- Change the location of each node according to,If a node reaches a location with lower cost than the black hole, exchange their locations and If a node crosses the event horizon of the black hole, replace it with a new node in a random location in the search space
- If a termination criterion (a maximum number of iterations or a sufficiently good fitness) is met, exit the loop

End loop

While transmission if any node becomes blackhole then retransmission will occur as no of packets increases, more energy will be consumed by it and it will increases as packet increases.

Parameter	Specification
Simulation Software	MATLAB R2013
Number of Nodes	50,100,150,200 etc
Area of Simulation	1000 X 1000 m
Maximum Range	200 m
Mobility Model	Random Way Model
Traffic Model	Single CBR Flow per node
Speed	10 m/s

Initial Energy	0.01 to 0.1
ETx	5*10^-8
ERx	5*10^-8

In this paper, we have studied AODV routing protocol with shortest path estimate the effects of the Black-Hole attacks in the mobile Ad-hoc Networks To accomplish this we have simulated this using MATLAB.We have calculated node energy and energy dissipation. When Dmin is greater than range then

Energy dissipation=Ed=E0-(ETx+Emp*Dmin^2)

And when Dmin is less than range then

Energy dissipation=Ed=E0-(ETx+Emp*Dmin)

If the Dmin is greater than range then node requires more energy to transmit data because energy dissipation is directly proportional to distance and vice versa

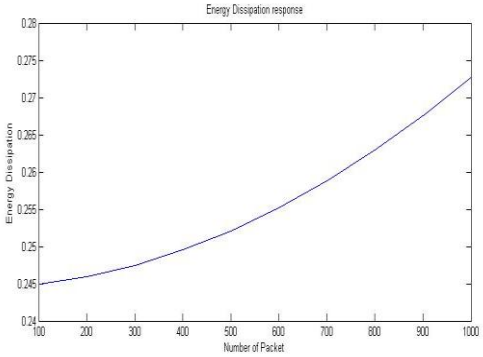

Fig.1 Energy Dissipation

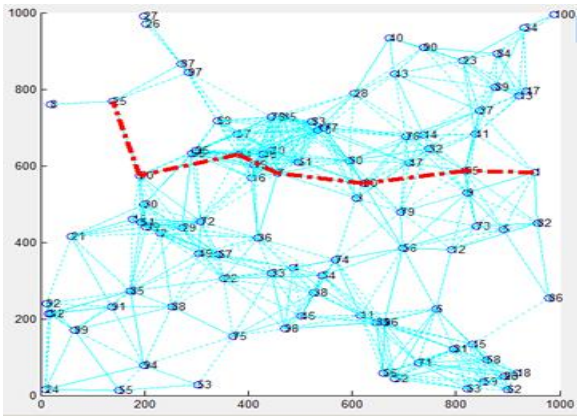

Fig2.Shortest Path finding

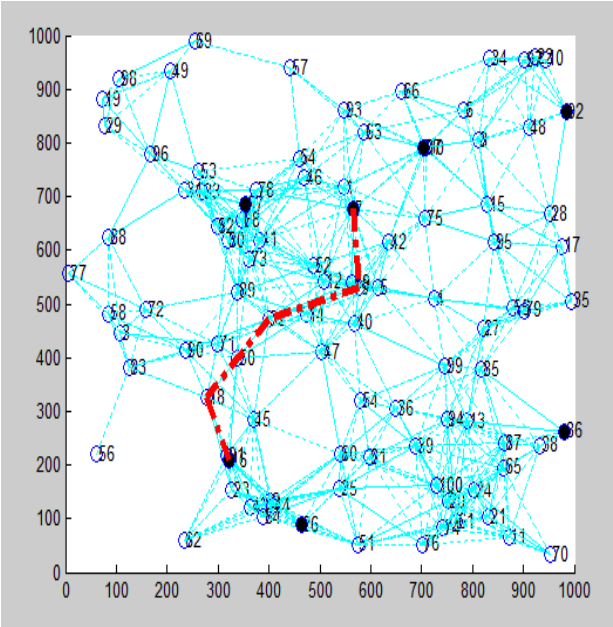

Fig 3.Black hole detection

VII. CONCLISION

This article covers MANET security issues and security attack.We implemented an AODV protocol findingshortest path for data routing from source node to destination node maintaining the secure transmission using DES security algorithm in MANET networkand Black hole avoidance.

REFRENCES

[1] HichamAMRAOUI1 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 SanthoshBaboo, "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

[7] sandeep Kumar, Monika Goyal, Deepak Goyal, RameshC. Poonia,"Routing Protocols and Security Issues in MANET"©2017 IEEE

[8] ToshaNaik,FenilKhatiwala,AchyutSakadasariya,"Search for Secure Data Transmission in MANET : A Review",2017 IEEE

[9] Sanjeet1, Asst Prof. Sonia Rani2 "Detection And Elimination Of Black-Hole Attack In Manet" International Journal For Technological Research In Engineering Volume 2, Issue 12, August-2015 ISSN (Online): 2347 – 4718. www.ijtre.com Copyright 2015

[10] Annu, MsDeepikaRana,"A Novel Technique of Finding the malcious node/black hole for WSN through vartingenergybased phenomenon ,International Journal For Technological Research In Engineering Volume 4, Issue 8, April-2017

[11] S. Kurosawa, H. Nakayama, and N. Kato, "DetectingBlack-Holeattackon AODV based mobile ad-hoc networks by dynamic learning method, "International Journal of Network Security, pp. 338–346, 2007.