RESEARCHERID
THOMSON REUTERS

ISSN: 2277-9655
[Kotak * *et al.*, 6(8): Augsut, 2017] Impact Factor: 4.116
IC™ Value: 3.00 CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

CRYPTOGRAPHIC APPROACH TO ELIMINATE BLACK HOLE ATTACK IN MANET

Dr V.C Kotak[*1] & Nivedeeta Banerjee[2]

[*1&2]Department of Information Technology, Shah and Anchor Kutchhi College of Engineering, India

DOI: 10.5281/zenodo.845302

ABSTRACT

In Manets, nodes usually cooperate and forward each other packets. But in hostile environment some nodes may intentionally misbehave or would not forward disrupting from communication. One of the attacks is black hole attack. The black hole attack intentionally drops the packet or jeopardize. Black hole node claims to have shortest path and participate in communication.

The proposed system uses AODV encryption and decryption to prevent black hole attack .it is simulated using NS 2.34.

KEYWORDS: RREQ,RREP,ADOV,Black hole attack, Caesar Cipherencryption, decryption.

I. INTRODUCTION

MANET are formed using dynamic topologies meaning that means any node can join or leave network. There is no centralized administrator hence any node can act as router or host, thoughany node can come and go, there isa fear of vulnerability. As router, the node finds an optimum path and manages delivery of packetsthrough a routing protocol mechanism [1].

In this paper, we have emphasizedonthe AD-HOC On Demand DistanceVector routing protocol as the routing protocol mechanism. This protocol is a reactive protocol, meaning routes are discovered when required. In AODV when a source node establishes a communication with the destination node it, broadcasts a RREQ(route request) message. When an intermediate node has a route towards the destination node, it sends a reply to the source node RREP(Route Reply).The AODV function with attributes is based on a destination sequence number and hop count, to evaluate the shortest path. This works smoothly when there are no occurrences of an attack. AODV is not designed with security mechanisms, so there are chances of it getting attacked. This may give rise to various attacks. One of the attacks is the black hole attack [2].

II. BLACKHOLE ATTACK IN MANETS.

In AODV, duringthe route discovery phase, when a node receives RREQ, it replies to the source node with RREP .The RREP containsthe sequence numbers andthe hop count , that determine the data packets that flow to the destination node and through these values it evaluates the shortest path from the source to the destination
When a malicious node enters into the network, it sends a forged route reply (RREP) that leads to packet drop [3]

The main motive of a black hole attack is to disrupt the routing services in the network by attracting traffic towards it and block data packets by dropping them.In fig1.Source node ‘S’ is initiated by route discovery phase by broadcasting RREQ packet.If any malicious node receives RREQ packets by just adding high sequence number as in fig2.Since AODV depends on sequence number to know the freshness of the route.The source gets duped by fake RREP packet [4].

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

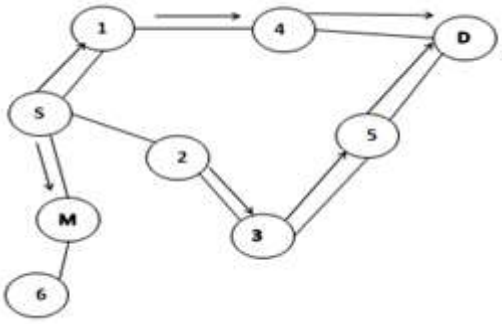

Fig1.Propagation of RREQ packet [4].

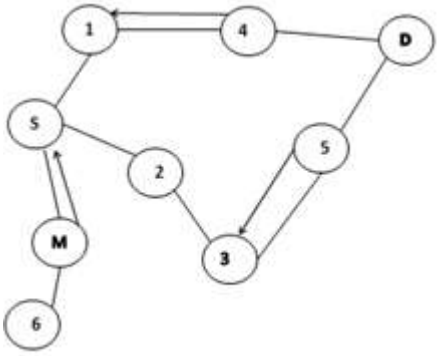

Fig 2.Propagation of RREP packet [4].

III. PROPOSED SYSTEM TO PREVENT BLACK HOLE ATTACK.

In this paper,we have proposed a mechanism by adding a function of encryption and decryption in AODV to prevent the Black Hole Attack. Forthe encryption and Decryption feature, we have implemented the Caesar cipher with a pre-shared key of 3. This cryptographic function takes an input as a string of plain text and shifts the ASCII value of each character in (text) three positions. The RREQ messages of the source node are encrypted before being forwarded to its neighbors. Nodes which know the pre-shared key can decrypt the RREQ correctly and generate RREP message and send it to the source node.

If any Black hole node enters the network, it cannot decrypt the RREQ.The proposed mechanism is implemented in NS2.34

IV. SIMULATION RESULTS

1. Simulation Parameters.

Table 1.Simulation Parameters.

Constraint	Value
Simulator	NS-2
Topology	1000M*800m

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Number of Mobile nodes	O7
Routing Protocol	AODV
MAC layer Protocol	IEEE 802.11
Mobility Model	Random waypoint
Simulation time	1000 sec
Placement of nodes	Random.

2. Simulation Results

Table 2 AODV. Under black hole attack.

Number of nodes	Packet size	Packet delay ratio	End to end delay	Throughput
7	100	1	0.129	254 kbps
7	1000	0.53	0.0097	79.90 kbps
8	10	1	0.05	18.52 kbps
8	100	0.664	0.01	82.248 kbps
8	1000	0.941	0.0099	81.86 kbps
9	1000	0.512	1.92	154.81 kbps

Table 3.Encryption and decryption on AODV.

Number of nodes	Packet size	Packet delay ratio	End to end delay	Throughput
6	100	0.05	1.360	22.63 kbps
6	1000	0.512	1.93	154.81 kbps
7	10	1	0	753.24 kbps
7	100	0.05	1.426	21.89 kbps
7	1000	0.384	2.36	96.23 kbps
8	100	0.05	1.419	21.94 kbps
8	1000	0.512	2.618	111.341 kbps

V. CONCLUSION.

The black hole attack is the main security threat that degrades the performance of the routing protocol in a Mobile Ad hoc network. To detect and prevent the black hole attack is one of the most important factors to ensure better quality of network performance. It has been found that as the malicious node tends to drop the packets, a packet delay is causedand throughput is minimized. The proposed System, using encryption, has helped to improve the security among the nodes.

In the future, the proposed scheme is enhanced by computing hash with a more innovative approach to find out the processing time the nodes take, to examine their performance further. If the processing time gets reduced, then the system can be further improved to minimize delay and to provide a system which will be of utmost importance for MANET.

A tool like NS2 is a discrete event simulator targeted at networking research. A Network simulator provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

VI. REFERENCES

[1] Zaid Ahmad, KamarularifinAbd. Jalil, Jamalul-lailAbManan"Black hole Effect Mitigation Method in AODV Routing Protocol" IEEE in 2011.
[2] NidhiChoudhary, Dr.LokeshTharani, "Preventing Black Hole Attack in AODV usingTimer-Based Detection Mechanism" SPACES 2015
[3] Ms.Nidhi Sharma,Mr. Alok Sharma"The Black hole node attack in MANET"in IEEE 2012.
[4] Rajesh Yermani, Anil KSarje "Secure AODV protocol to mitigate Black hole attack in Mobile Ad Hoc Networks" IEEE in 2012..

CITE AN ARTICLE

Kotak, V. C., & Banerjee, N. (2017). CRYPTOGRAPHIC APPROACH TO ELIMINATE BLACK HOLE ATTACK IN MANET. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, 6*(8), 344-347. Retrieved August 18, 2017.