ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Detection of Cosmic Dust Attack in MANET under AODV Routing Protocol

Shabnam Malik[1], *Jitendra Arora*[*2]

[#]*Department of CSE, Deen Bandhu Chotu Ram University*

Abstract: ***The cosmic dust attack problem is one of the security attacks that occur in mobile ad hoc networks (MANETs). We show two feasible solutions. The main is to find more than one route to the destination. The another is to exploit the packet sequence number included in any packet header. Computer simulation shows that in comparison to the original ad hoc on demand distance vector (AODV) routing scheme, the another solution can verify 75% to 98% of the route to the destination depending on the pause time at a minimum cost of the delay in the networks. The main objective of this paper is to examine cosmic dust attack in MANET and its solutions. To secure a mobile ad hoc network (MANET) in antagonistic environments, a particularly challenging programs can be combined into existing routing protocols for MANETs, such as ad hoc on demand distance vector routing (AODV) .The simulation results have demonstrated the important advantages of the proposed attack detection and routing algorithm over some known protocols.***

KeyTerms: AdHoc Networks, Security Issues, Cosmic Dust Attack, AODV

1. INTRODUCTION

Mobile Ad-Hoc Networks are independent and decentralized wireless systems. A Mobile Ad-hoc Network (MANET), as the name suggests, is a self-configuring network of wireless and hence mobile devices that comprises a network capable of vigorously changing topology. The network nodes in a MANET, not only act as the ordinary network nodes but also as the routers for other peer devices [1]. Nodes are the system or gadget i.e. mobile phone, laptop, personal digital assistance, and personal computer that are participating in the network and are mobile. The dynamic topology having less of a fixed infrastructure and the wireless nature make MANETs capable to the security attacks. Due to the unique features of MANET, developing an Intrusion Detection System (IDS) in this network is very challenging task. There is no centred gateway device to monitor the traffic within network. Since the medium is open for all nodes, both legitimate and malicious nodes can access it. Moreover, there is no clear separation between normal and unusual activities in a mobile environment. Since nodes can move randomly, false routing information can come from a compromised node or a legal node that has outdated information. Cosmic Dust or sequence number attack is one of the most common attacks made against the reactive routing protocol in MANETs. The Cosmic Dust attack involves malicious node(s) assemble the sequence number, hence pretending to have the shortest and freshest route to the destination. The aim of this paper is to investigate cosmic dust & detection methods within the scope of ad hoc on demand distance vector (AODV) routing protocol.

ISSN: 2321-9653

II.RELATED WORKS

The current secure routing protocols for MANETs can roughly be divided into two categories, i.e., 1) those adding security methods to the existing routing protocols and 2) those designed to expose and preserve specific attacks. In the this category, the main practice is to secure the popular on-demand routing protocols, such as ad hoc on-demand distance vector routing (A ODV), destination sequenced distance vector (DSDV), and dynamic source routing (DSR), by using a security association between the source and destination.

III.SECURITY ISSUES

Security in MANET is a major issue as to provide secure communication between the nodes in the infrastructure less Environment. As ad hoc network is self organizing, open node to node connections, active topology, and modified resources. A secure network is that which possess the
Following attribute:

1. Confidentiality- To keep the information secret from the unknown users. It is necessary to maintain the information safe and secure from the attacks.
2. Integrity of Message – To keep the accuracy and consistency of the data during its transit from node to node. So that the data is not limited by the unwanted access.
3. Availability of Nodes –As in MANET for communication the nodes are required to be available all the time so that the information can be relayed over such path.
4. Authorization –it specify the permissions of the entity to take part in the communication over network.

IV.Ad Hoc Routing Protocol and Cosmic Dust Attack

In Cosmic Dust attack, a malicious node uses its routing protocol to advertise itself for having the shortest path to the destination node it wants to anticipate. The malicious node advertises availability of fresh routes to the other nodes irrespective of checking its routing table. In this way attacker node shows the route availability as reply to the route request messages and thus capture the data packet and hold it. In protocol which is based on flooding, the ill-disposed node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is created, now it's up to the node whether to drop all the packets or forward it to the unknown address

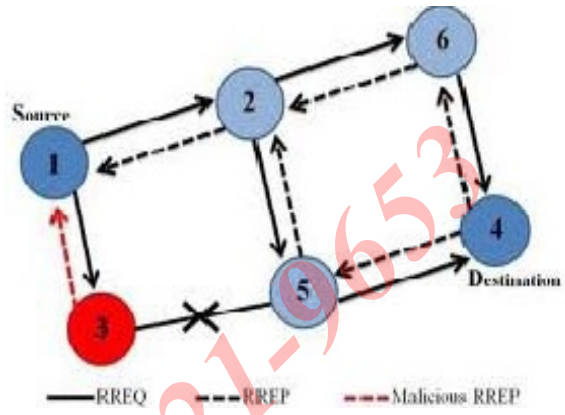


Figure 2: Cosmic Dust Attack

An ad-hoc routing protocol[8] is a practice, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. Being one of the variety of ad-hoc routing protocols, on-demand protocols such as AODV [4] (Ad-hoc on demand Distance Vector) and DSR (Dynamic Source Routing) creates routes between nodes only when they are need to route data packets. AODV is the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name shows AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network.

In an ad-hoc network that uses AODV[4][6] as a routing protocol, a mobile node that wishes to cconvey with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired target node. This process is called route detection. Every neighboring node that receives RREQ emit first saves the path the RREQ was transmitted along to its routing table. It afterwards checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQ message. The freshness of a route is showed by a target sequence number that is attached to it. If a node finds a fresh route, it unicast an RREP (Route Reply) message back along the saved path to the source node or it re-broadcasts the RREQ message otherwise. Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, which rivel can exploit to perform a cosmic dust attack on mobile ad-hoc networks. A untrustful node in the network receiving an RREQ message replies to source nodes by sending a fake RREP

message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising (by sending a fake RREP to confirm it has a path to a destination node) to source nodes that it will forward data, a malicious node starts to fall all the network traffic it receives from source nodes. This gradual dropping of packets by a malicious node is what we call a cosmic dust attack. The RREQ messages and RREP messages are shown in the figure2 and figure3.

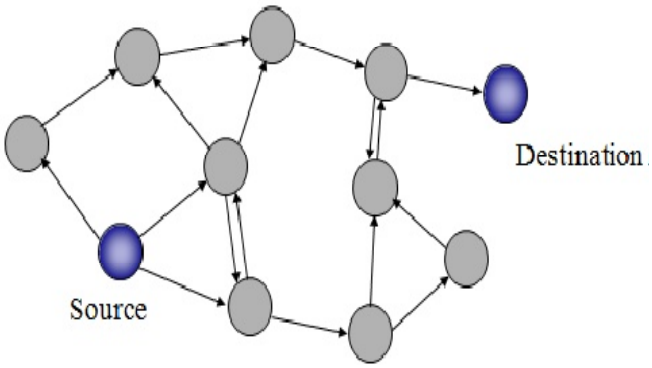


Fig 1:RREP messages

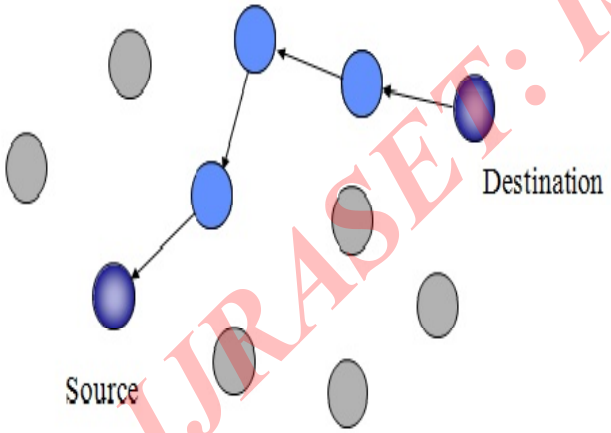


Fig 2: RREQ messages

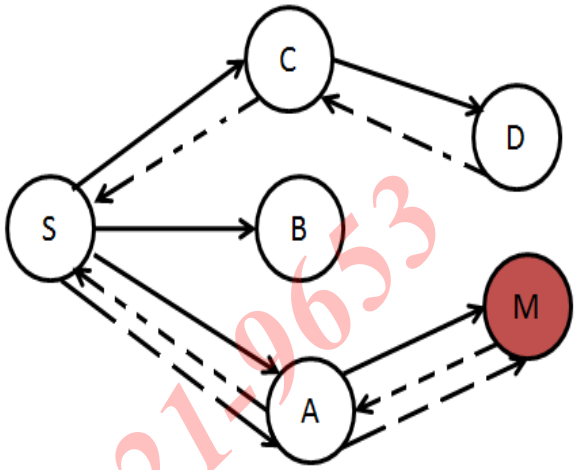


Fig 3: Black hole

V. PROPOSED SOLUTION AGAINST COSMIC DUST ATTACK

Detection of list of Malicious Nodes

The Communication in an Ad Hoc network is a multihop communication wherein a source node communicates with a distant node using intermediate nodes in order to save the power. Thus the major activity in an ad hoc network environment is to find a suitable route such that the delivery of the message is ensured beyond doubt. The route should be so chosen that all the nodes in the path are trustworthy, non malicious, unselfish and the hop count is minimum. The first receiver of the message to a distant node is some immediate neighbor of the source node. Therefore, it is necessary that every node in the ad hoc network must be aware of its immediate neighbor at every moment. To remain aware of about its neighbor nodes, a node in the network keeps on broadcasting hello requests on the periodic basis and keeps on receiving the

hello replies as well. Using these hello request and replies a node in the ad hoc network constructs and maintains a table of its neighbors known as neighbor table. Since the nodes in the ad hoc networks are mobile the neighbor table keeps on changing with time. There is no destination address in this packet as hello request is a diffused mechanism. Hello reply is multiple unicast mechanism wherein a node responds to the node from whom it has received a hello request.

Fig 4. Proposed Algorithm to find out the list of neighbors to maintain neighbor table.

Algorithm 4.1

Notations:

ST: Slot Time, S: Source Node, NL (Node_id): Neighbor List of Node_id node

Neighbor List (Node_id)

```
1  Begin
2  For (Node_id)
3  {
4  For (every ST)
5     {
6            broadcast hello_pkt;
7           receive hello_reply_pkt;
8            put node address in NL (Node_id) ;
9     }
10}
11 End
```

Explanation of Algorithm 4.1/ Fig 4.1 (Neighbor list(Node_id)):

1) This algorithm takes Node_id as argument.
2) First of all node with this Node_id will broadcast the hello packet.
3) After broadcast it will wait for hello reply for a particular slot time.
4) RREP packets received within this slot time are processed.
5) Node_id of sender of RREP packet is stored in Neighbor list (NL).

4.2 Finding the probable list of Malicious Nodes

In normal AODV, Route Discovery process is initiated by broadcasting a Route Request (RREQ) packet to its neighbors. Each neighboring knob either responds the RREQ by sending a Route Reply (RREP) back to the source node or rebroadcasts the RREQ to its own neighbors after increasing the hop count field. The node that receives the RREP packet first checks the value of sequence number in its routing table. The RREP packet is received if it has RREP_seq_no higher than the one in routing table. Our solution does an addition check to find whether the RREP_seq_no is higher than the threshold value. The threshold value is actively update as in every time interval.

Calculation of Threshold Value

- The threshold value is dynamically renewed using the data collected in the time interval.
- The time interval to update the threshold value is as soon as a node receives a RREP packet Rule used to calculate Threshold value.

Rule used to calculate Threshold value

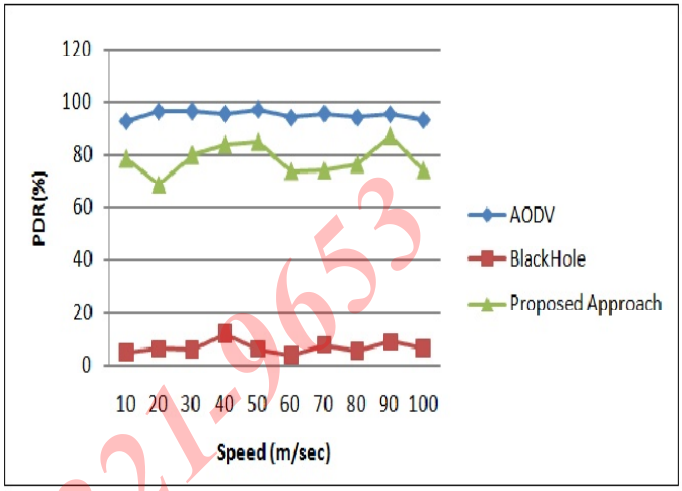
After comparison, if the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be untrusty and this node will be added to the black list. Black list is the list of distrustful nodes which may act as cosmic dust in network.

VI. METHODOLOGY FOR EVALUATION

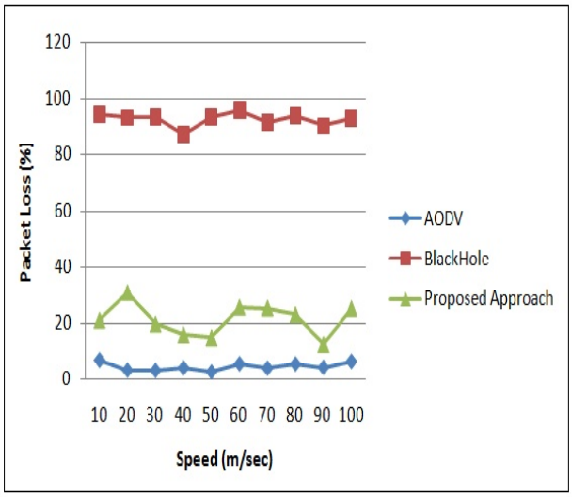
1. Packet delivery ratio (PDR):
   The percentage of data packets delivered to destination with respect to the number of packets sent. This metric indicates the reliability of data packet delivery.

2. Packet Loss:
This metric informs us about the amount of control packets fails to reach its destination in a timely manner. Performance comparison is made on the basis of above two metrics between existing AODV and proposed AODV.

1. Packet Delivery Ratio (PDR): PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. In the Fig. it is cleared that PDR of AODV is heavily affected by the malicious nodes where as the PDR of Proposed AODV is immune to it.



2. Packet Loss
This graph shown in Fig. shows the packet loss for the each UDP connection in the simulation. We use total 9 UDP connections in the simulation. The graph concludes that there is very less packet lost percentile in the proposed AODV as compared to the AODV. Fig. Showing Packet Loss



VII.CONCLUSIONS

Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted separate techniques to propose different types of prevention mechanisms for cosmic dust problem. In this paper, we first summary the pros and cons with popular routing protocol in wireless mobile ad hoc networks.

MANET has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment.

In our thesis we have analyzed the behavior and challenges of security threats in mobile ad hoc networks with solution finding technique. In this paper, we have studied the routing security issues of MANETs, described the cosmic dust attack that can be mounted against a MANET, and proposed a worlable solution for it on the top of AODV protocol to avoid the cosmic dust attack, and also prevented the network form further malicious behavior. Proposed mechanism can be used to find the secured routes and prevent the cosmic dust nodes in the MANET by identifying the node with their sequence number; check is made for whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP or not? Our solution presents good performance in terms of packet ratio and minimum packet end-to-end delay and throughput. As future work, research work intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet over it, memory usage, mobility, extending number of malicious node, increasing number of nodes and scope of the cosmic dust nodes and also focusing on resolving the problem of multiple attacks against AODV.

VIII. FUTURE SCOPE

The proposed algorithm is efficient in discovery of Cosmic Dust nodes and its removal from network but improvement can be done in mainly two directions as follows:

- End-to-End Delay: Due to the processing involved in our proposed algorithm, end to end delay got increased. Further improvement can be done to decrease the end to end delay along with the successful removal of Cosmic Dust nodes.

ACKNOWLEDGEMENT

Assistant Prof. Jitendra Arora is the assistant professor in Department of Computer Science and Engineering at Royal Institutes of Technology and Management, Chidana, Haryana. I am especially grateful for his guidance and contributions by generously giving his time and carefully reviewing this manuscript.

REFERENCES:

[1] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation based incentive scheme for ad-hoc networks," *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, vol. 2, pp. 825–830, 21-25 March 2004.

[2] Y. F. Alem & Z. H. X. "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection" by from Tainjin 300222, China 2010, IEEE

[3] "An Adaptive Approach to Detecting Black Hole Attacks in Ad Hoc Network" 2010 24th IEEE International Conference.

[4] Dow CR, Lin PJ, Chen SC, Lin JH, Hwang SF (2005) A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-hoc Networks. Paper presented at the IEEE 19th International Conference on Advanced Information Networking and Applications, Tamkang University, Taiwan, 28-30 March 2005

[5]. Zhou L, Chao H-C (2011) Multimedia Traffic Security Architecture for the Internet of Things. IEEE Network 25(3):29–34. Doi: 10.1109/MNET.2011.5772059

[6]. Yang H, Lou H, Ye F, Lu S, Zhang L (2004) Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications 11(1):38–47. Doi: 10.1109/MWC.2004.1269716

[7] Su M-Y (2011) Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. IEEE Computer Communications.99

[8] Mohammad Al-Shurman and Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" Publisher ACM press, pp 96-97, April 2004

[9] Tamilselvan, L. Sankaranarayanan , V. "Prevention of Black hole Attack in MANET", Journal of Networks, Vol.3, No.5, May2008.
[10] Desire Weerasinghe and Huirong Fu, Member of IEEE, Preventing Cooperative Black Hole Attacks in Mobile Adhoc Networks: Simulation implementation And Evaluation, IJSEA, Vol2, No.3, July 2008.
[11]Jong-Pyng Li," Priority Based Real-Time Communication for Large Scale Wormhole Networks", 0-8186-5602-6/*9*04 1994 IEEE

[12]Junfeng Wu," Label-Based DV-Hop Localization Against Wormhole Attacks in Wireless Sensor Networks", 2010 Fifth IEEE International Conference on Networking, Architecture, and Storage 978-0-7695-4134-1/10© 2010 IEEE

[13]L. Lazos," Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", IEEE Communications Society / WCNC 2005 0-7803-8966-2/05 © 2005 IEEE