Protection Dealings for Black Hole Attack in Mobile Ad hock Network

Ankita Choorasiya
Assistant Professor
IET DAVV Indore

Subhash Waskle
IET DAVV Indore

Ravindra Verma
Assistant Professor
IET DAVV Indore

Abstract

The set of mobile nodes which are arranged randomly and with dynamism is called a Mobile Ad-hoc Network. These are positioned in a way that the connections between the nodes are proficient enough to alter constantly. The wireless ad-hoc network stays in the continuous state of threat as there are securities susceptibilities present in the network. Black-hole Attack is one of such threats. Here in this paper, the security of AODV is discussed in order to analyze and improve. The approach that is used to achieve this task is Algorithmic approach. In MANET, the AODV is considered as the most widely known protocols. The main objective that we are working so hard upon is ensuring the security against the Black hole attack. The resolution which is propounded is competent to detect and remove the nodes of Black hole in MANET in the very beginning. A simulation study will also be illustrated in this paper focusing on the consequences of Black hole attack upon performance of network.

Keywords: AODV, Mobile Ad-Hoc Network, MANET, Routing Protocol and Black Hole Attack.

I. INTRODUCTION

The self-supervised autonomous nodes makeup the wireless ad-hoc network devoid of any sort of infrastructure [1]. The topology of the ad-hoc networks is dynamic which allows its nodes to join easily or leave the network at anytime. There are many possible applications, particularly, in the areas of military and rescue, in order to connect the soldiers on the battlefield. This also helps in setting up the network in the places where the network is damaged due to any natural calamity like an earthquake. The ad-hoc networks are preferably set up in the places where there is no permanent infrastructure. The nodes have this unique ability to be in touch with other by providing the connectivity through packets which they forward over each other. The Destination-Sequenced Distance-Vector (DSDV), Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance Vector (AODV) are utilized by the nodes in support of the connectivity. The nodes also have a quality to act as router in order to communicate by forwarding the packets to the required node in a network. The wireless ad-hoc network stays in the continuous state of threat and due to the lack of infrastructure there are security susceptibilities present in the network. Black-hole Attack is one of the attacks [2][3]. The Black hole attack is defined as the attack which engulfs the data packets as whole, exactly like a hole which consumes almost everything. By this mode the packets are dropped in a network. By utilizing all the susceptibilities of the Route Discovery Packets, like, AODV the malicious nodes are dropped in the network traffic [4]. The intermediate nodes in AODV play a vital role in finding a new way towards the goal [5]. Malicious nodes never utilize these processes. Black hole attack can take place due to the misdemeanor of the malicious node and the wrecked node interface. At any given condition the nodes of the network continuously finds the goal, due to which the packets are lost and the battery is consumed.

II. ROUTING PROTOCOLS

Creating the Optimal Path is the main objective of the Routing Protocol [6] (minimum hops) among sources and the target along with the minimum bandwidth and minimum overhead consumption in order to deliver the packets on time. Over the huge range of the context of network a MANET protocol must function efficiently from tiny ad-hoc collection to the big multiple-hop networks.

The categorization of these routing protocols are shown in figure 1.

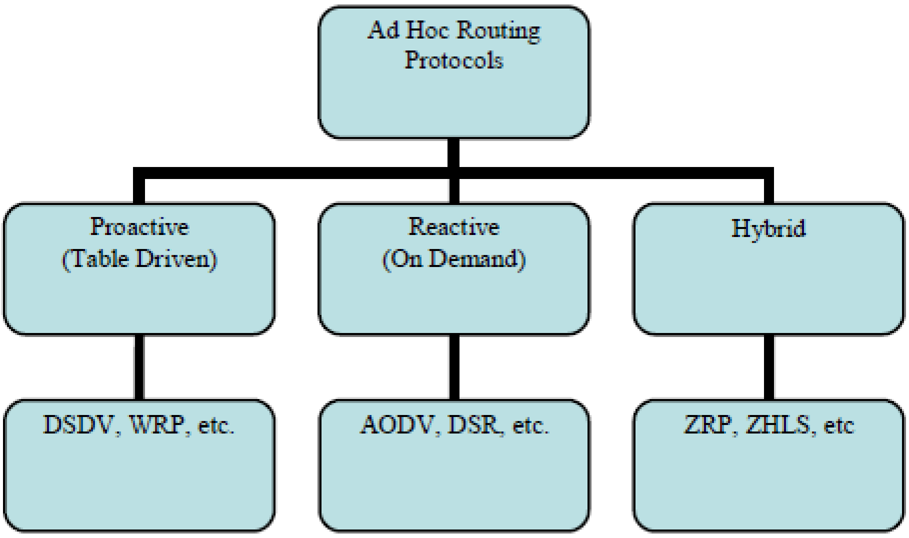

Fig 1: Hierarchy of Routing Protocols

This protocol is sub-divided into 3 types; 1). Hybrid Protocols, 2). Reactive Protocols and 3). Proactive Protocols. These are sub-divided on the basis of the topology of routing. Pro-active protocol is driven by the table, e.g. DSDV. Au contraire the Reactive Protocols never update the routing information periodically. It activates and spread when there is any need. E.g., DSR (Dynamic Source Routing) and AODV. The combination of reactive and proactive protocol is the Hybrid protocol. E.g. ZRP (Zone Routing Protocol), ZHLS etc.

III. BLACK HOLE PROBLEM IN AODV

Routing protocols are vulnerable to a diversity of attacks. One sort of Denial of Service (DoS) is the black hole attack. Here, a malign node exploits the route discovery packets by claiming itself to have a shortest path to the intercept packets. The attacker controls the route followed by the network traffic by modifying the routing protocols. RREQ packets are given away to the intermediate nodes by the source node in the route discovery process in order to look for a secure path to the destination. Since the malign nodes do not abide by the routing table, the respond the source node's message in no time. The source node thus regards the process to have completed and ignores RREP messages from other nodes while taking up the path directed by the malign nodes. In place of relaying the messages as per the protocol's requirement, the malign node drops the received messages.

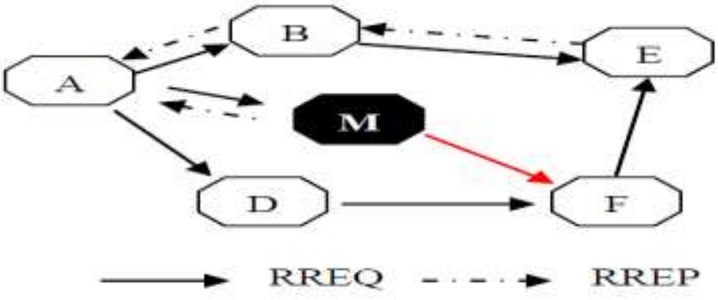

Fig 3: Black hole Attack in AODV

In the above figure 2, imagine a malicious node „M". When node „A" broadcasts a RREQ packet, nodes „B" „D" and „M" receive it. Node „M", being a malicious node, does not check up with its routing table for the requested route to node „E". Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node „A" receives the RREP from „M" ahead of the RREP from „B" and „D". Node „A" assumes that the route through „M" is the shortest route and sends any packet to the destination through it. When the node „A" sends data to „M", it absorbs all the data and thus behaves like a "Black hole".
For determining the security of routing protocols in AODV, a sequence number is used in the form of a message from the original node. The RREPs sequence number is determined by the destination node by comparing it to the current sequence number. Black hole attack catches all source packets and does not forward them to the destination and thus the packets get discarded midway.

IV. PROPOSED SOLUTION

An additional route is propounded to the intermediate node to verify the existence of the destination node via the RREQ message. When the next hop responds to the source node's message, the reply packets provide check results for the same. A route is set up to the target and it starts to give away data packets if the verification is complete. The reply packets are discarded in cases where there is no route between the next hop and the destination. Simultaneously, for the isolation of the malign node, an alarm message is given away. The black hole problem is thus prevented and the network is secured from any malign behavior. Even so, we have put forth a hack taking into account that the black hole nodes do not always work in groups but sometimes independently. Yet, this solution can not be employed for multiple black hole nodes. For countering group attacks by multiple black hole nodes, we have brought a slight modification in the AODV protocol and made use of the DRI table along with the cached and current routing tables. The black hole has two salient features. The first being, the Ad-hoc routing protocol is exploited by the node and the second being the consumption of intercepted packets by the node.

4.1. Algorithmic approach to avoid black hole attack in MANETs

In the propounded solution, only the source node is being modified with no alteration in the intermediate node and destination node. We have included two crucial components to the methodology, namely the Data Routing Information table and cross checking.

```
Steps:
1: RREQ broadcast by source node
2: RREP received by source node
3: Routing data packets from SN if the RREP is reliable
4: Otherwise

Proceed further and identify the reliability of the IN node to next hop node
Receive further request, next Hop node of current next hop node, and Data Routing Information entry for next hope nodes next hop. Document a data routing information entry for current intermediate node.
5: if (next hop node is a reliable node)

Check intermediate node for black hole using DRI entry
If (intermediate node is not a black hole)
Route data packets (source route)
Otherwise

Insecure route
Intermediate node is a black hole
All the nodes along the reverse path from
IN to the node that generated
RREP are black holes (i.e. a malicious node)


Otherwise
Current intermediate node = next hop node

6: Repeat step 4 & 5 until intermediate node does not become reliable
```

Fig 4: Proposed Algorithm to prevent Black hole Attack

4.2. Working Principle

Identification of black holes is a collective solution which comprises of two bits of extra information from nodes that respond to RREQ messages from source nodes. There is an additional Data Routing Information (DRI) table maintained by each node.

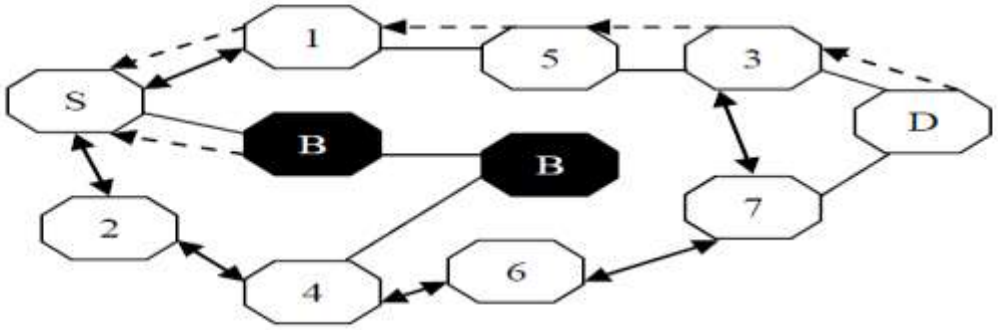

Fig 5: Solution to avoid multiple Black hole attack

In the DRI table, 1 stands for „true‟ and 0 for „false‟. The first bit "From" stands for information on routing data packet from the node (in the Node field) while the second bit "Through" stands for information on routing data packet through the node (in the Node field). In reference to the example of Figure 3, a sample of the database maintained by node 4 is shown in Table 1. The entry 1 0 for node 3 implies that node 4 has routed data packets from 3, but has not routed any data packets through 3 (before node 3 moved away from 4). The entry 1 1 for node 6 implies that, node 4 has successfully routed data packets from and through node 6. The entry 0 0 for node B2 implies that, node 4 has NOT routed any data packets from or through B2

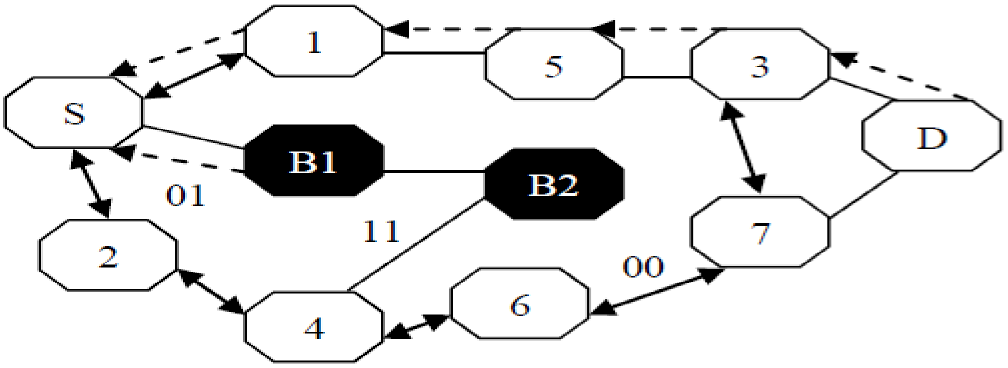

Fig 6: Solution to identify multiple Black hole nodes

We define the following convention for protocol representation in fig 5 & 6.

RREQ/RREP one way propagation Two way propagation Route indicator Cross Checking:
For data packet transfer, we have made use of the reliable nodes. Figure 6 explains the layout algorithm for the methodology we have propounded and also the modified AODV protocol. For discovery of a secure route to the target, an RREQ message is broadcast by the source node in the protocol. The DRI entry and NHN needs to be provided by the intermediate node. Thereafter, the source node evaluates the DRI table for the reliability of the intermediate node. The IN is regarded as reliable only if there is a history of data routing through it by the SN. In any case otherwise, an FRq message is forwarded by the SN to investigate the identity of IN through NHN. If:

- There has been any data routing between IN and NHN
- The current NHN's next destination hop
- Whether the current NHN has routed data through its own next hop

In response to this, the NHN sends an FRp message that comprises of:

- IN DRI entry
- Current NHN's next hop node
- DRI entry for next hop of current NHN

The reliability of the NHN depends on whether there has been any history of data routing between NHN and the source node. IN is regarded as a black hole if the first and second bit from the IN DRI entry is 0 and 1 respectively. If not, the source node updates its IN DRI entry with code 01 and starts to route data with IN. In case it is a black hole, SN traces and ignores all the nodes that come in reverse path from IN and gives away a list of cooperative black holes.

V. SIMULATION ENVIRONMENT

We have implemented Black hole attack in an ns-2 [13] simulator. For our simulations, we use CBR (Constant Bit Rate) application, TPC/IP (full duplex communication), IEEE 802.11b MAC and physical channel based on statistical propagation model. The simulated network consists of 30 randomly allocated wireless nodes in a 500 by 500 square meter flat space. The node transmission range is 250-meter power range. Random waypoint model is used for scenarios with node mobility. The selected pause time is 30s seconds. A traffic generator was developed to simulate constant bit rate (CBR) sources. The size of data payload is 512 bytes. In our scenario we take 30 nodes in which nodes 1-22 and 25-30 are simple nodes, and node 23 and 24 are malicious node or Black hole node. The simulation is done using ns-2, to analyze the performance of the network by varying the nodes mobility [14] [15]. The metrics used to evaluate the performance are given below.
a) Packet Delivery Ratio: The ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.
b) Throughput: Throughput is the average rate of successful message delivery over a communication channel.
c) Node Mobility: Node mobility indicates the mobility speed of nodes.

5.1. Result & Discussion

The fig.7 shows the effect to the packet delivery ratio (PDR) measured for the AODV protocol when the node mobility is increased. The result shows both the cases, with the black hole attack and without the black hole attack. It is measured that the packet delivery ratio dramatically decreases when there is a malicious node in the network. For example, the packet delivery ratio is 100% when there is no effect of Black hole attack and when the node is moving at the speed 10 m/s. but due to effect of the Black hole attack the packet delivery ratio decreases to 82 %, because some of the packets are dropped by the black hole node.

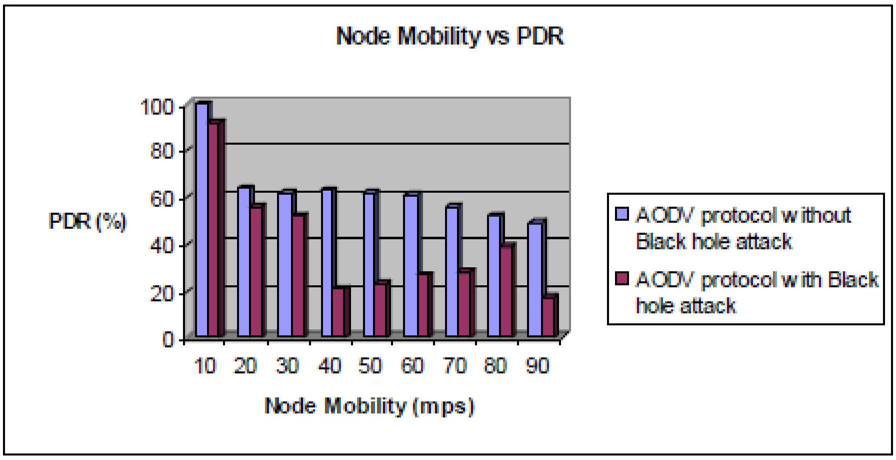

Fig 7: Impact of Black hole attack on PDR

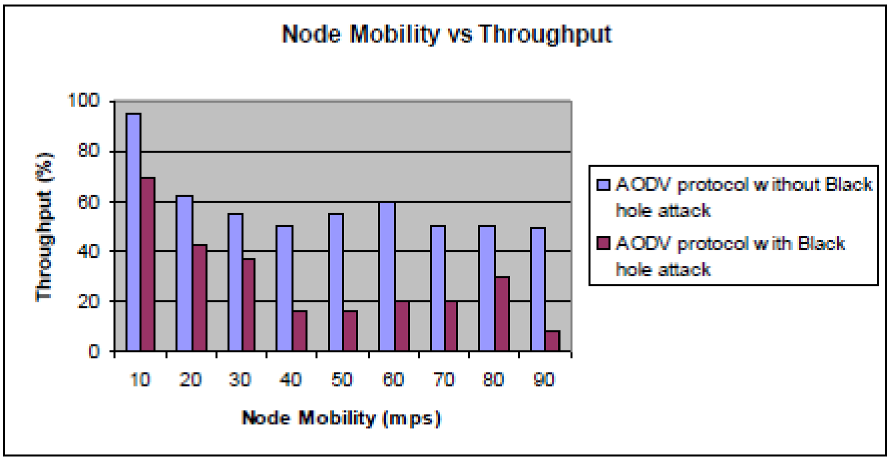

Fig 8: Impact of Black hole attack on Network Throughput

It is observed from the fig.8 that, the impact of the Black hole attack to the Networks throughput. The throughput of the network also decreases due to black hole effect as compared to without the effect of black hole attack. We vary the speed of the node and take the result to the different node speed.

VI. CONCLUSION AND FUTURE WORK

In this paper we have gone through the routing security issues of MANETs, described the black hole attack that can be mounted against a MANET and proposed a feasible solution for it in the AODV protocol. The proposed solution can be applied to a) Identify single and multiple black hole nodes cooperating with each other in a MANET; and b) Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation. Also we showed that the effect of packet delivery ratio and Throughput has been detected with respect to the variable node mobility. There is reduction in Packet Delivery Ratio and Throughput. In Black hole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and nodes as shown in the result of the simulation. The detection of Black holes in ad hoc networks is still considered to be a challenging task.

We simulated the Black Hole Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Black Hole Attack may be determined.

References

[1] S. Ci et al., “Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks,” IEEE Trans. Vehic. Tech., vol. 55, no. 4, July 2006, pp. 1302–10.

[2] M. G. Zapata and N. Asokan, “Securing Ad-Hoc Routing Protocols,” Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[3] B. Wu et al., “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,” Wireless/Mobile Network Security, Springer, vol. 17, 2006.

[4] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On demand Distance Vector (AODV) Routing,” IETF RFC 3561, July 2003.

[5] IETF MANET Working Group AODV Draft, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-08.txt, Dec 2002.

[6] Elizabeth M. Royer et. al. “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, IEEE Personal Communication, April 1999.

[7] Dokurer, S.; Erten Y.M., Acar. C.E., SoutheastCon Journal, “Performance analysis of ad-hoc networks under black hole attacks”. Proceedings IEEE Volume, Issue, 22-25 March 2007 Page(s):148 – 153.

[8] A. Shevtekar, K. Anantharam, and N. Ansari, “Low Rate TCP Denial-of-Service Attack Detection at Edge Routers,” IEEE Commun. Lett., vol. 9, no. 4, Apr. 2005, pp. 363–65.

[9] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, “Black hole Attack in Mobile Ad Hoc Networks” Proceedings of the 42nd annual Southeast regional conference ACM-SE 42, APRIL 2004, pp. 96-97.

[10] Y-C Hu and A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing,” IEEE Sec. and Privacy, May–June 2004.

[11] K. Sanzgiri et al., “A Secure Routing Protocol for Ad Hoc Networks,” Proc. 2002 IEEE Int’l. Conf. Network Protocols, Nov. 2002.

[12] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard. **“**Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”. Department of Computer Science, IACC 258 North Dakota State Universities, Fargo, ND 58105.

[13] Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edu/nsnam/ns.

[14] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. “Detecting Blackhole Attack on AODV based Mobile Ad-hoc networks by Dynamic Learning Method”. International Journal of Network Security, Vol.5, No.3, PP.338– 346, Nov. 2007.

[15] P. Michiardi, R. Molva. "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks". European Wireless Conference, 2002.

[16] Mukesh Muwel ,Prakash Mishra ,Makrand Samvatsar, Roopesh Sharma , Upendra Singh , “Efficient ECGDH Algorithm Through Protected Multicast Routing Protocol In Manets” , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-7.

[17] Lokesh Baghel ,Prakash Mishra ,Makrand Samvatsar , Upendra Singh,“ Detection Of Black Hole Attack In Mobile Ad Hoc Network Using Adaptive Approach ”, Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-5.

[18] Amar Singh Chouhan ,Vikrant Sharma ,Upendra Singh, “A Modified AODV Protocol To Detect And Prevent The Wormhole Using Hybrid Technique ”, Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-5.

[18] Roshani Verma ,Roopesh Sharma ,Upendra Singh, “New Approach Through Detection And Prevention Of Wormhole Attack In MANET”, Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.

[20] Vibhavarsha Prakaulya ,Neelu Pareek ,Upendra Singh, "Network Performance In IEEE 802.11 And IEEE 802.11p Cluster Based On VANET" , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.

[21] Vidya Kumari Saurabh ,Roopesh Sharma ,Ravikant Itare , Upendra Singh , "Cluster-Based Technique For Detection And Prevention Of Black-Hole Attack In Manets" , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.

[22] Ravi Parihar ,Ashish Jain ,Upendra Singh , "Support Vector Machine Through Detecting Packet Dropping Misbehaving Nodes In MANET" , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-6.

[23] Divyanshu Wagh ,Neelu Pareek ,Upendra Singh, "Elimination Of Internal Attacks For PUMA In MANET" , Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of IEEE , 20-22 April 2017 ,pp.1-5.