Review of Exposure of Black Hole Attack AODV based Routing Protocol in Mobile Ad Hoc Network

Amreen Sharif
M.Tech Scholar, (D.C.), Department of Electronics & Communication Engineering
Truba Institute of Engineering & Information Technology, Bhopal

Neelesh Gupta
Professor in Electronics & Communication Engineering
Truba Institute of Engineering & Information Technology, Bhopal

ABSTRACT

Black hole attack is a category of denial of service attack in mobile ad hoc network (MANET) which broadcast itself as having the freshest or optimal route to deliver the packet from source to destination and all these kinds of attack happens due to the dynamic behavior of the wireless network. It is self configuring and infrastructure less network and uses different routing protocols to deliver the packet from one to another end such as AODV, DSR, DSDV and ZRP etc. In this paper, literature study of detection techniques of black hole attack in AODV based routing protocol is explaining also discusses some counter measures for the analysis of black hole attack in mobile ad hoc network.

Keywords

AODV; Black hole attack; DSDV; DSR; Routing Protocol

1. INTRODUCTION

The use of wireless network is growing very rapidly in the field of communication technology. The network uses wired or wireless technology for the communication, but due to the static topology of network the use of such kind of network transmission has diminished and in place of that wireless communication for mobile node is uses enormously. The mobile ad hoc network [1] is collection of nodes and in this each node behaves as router or host which has the ability to route the path for packet transmission. The architecture of the mobile ad hoc network is shown in fig. 1. Such network uses dynamic topology to form the network and due to its dynamic behavior the network get affected from severe kind of threats or attack which may influence the network due to this the performance and effective use of the resources degraded. The mobile ad hoc network utilize the routing protocols to transmit the packet from source to destination or one end to another end but for efficient delivery of the packet it uses routing protocols which are classified into different categories [2]: Reactive routing, Proactive routing and Hybrid routing protocol. In proactive routing, every node periodically broadcast the routing information to its neighbor such as DSDV while in reactive routing; the routing starts only when node wants to transmit the packet such as AODV and DSR. The hybrid routing protocol if designed by using the best features of both the protocol such as ZRP. But the security issues are the challenging task of such type of network which gets affected from numerous kind of attack. In wireless network the attacks are classified in two namely; active attack and passive attack. The well known example of active attack replay, masquerade and denial of services (black hole attack) and passive attack examples are release of message content and traffic analysis. In this paper, we are mainly focuses on kind of denial of service attack known as black hole attack in AODV routing protocol. This attack publicizes itself that; it has the novel or shortest route to the destination and after receiving the packets it drops or discards the entire packet which goes from its route. For the exposure of such serious threats various researchers has been worked in this area but all the approaches has some merits and demerits, still not any such techniques has implemented which efficiently or completely abolish such threats. In this paper, study of literature of different techniques to thwart the black hole is discussing and explains about the some metrics to measure the performance of the system.

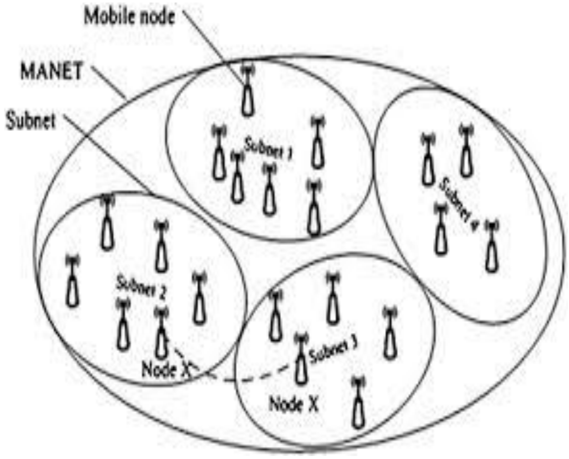

Fig. 1: Architecture of the mobile ad hoc network (MANET)

The organization of the remaining section of the paper is done in this manner: The section II deals with the literature of the previous work done. Next section deals with the Routing protocols. Section IV describes the black hole attack in AODV and counter measures and last section gives overall conclusion of this paper to prevent the network from malicious node and its future enhancement.

2. LITERATURE REVIEW

Currently there is a lot of work has been done to thwart the black hole attack and enhances the security of mobile ad hoc network which also improves the overall performance of the communication system.

In [3] the author proposed a mechanism to detect the multiple black holes by modifying AODV protocol. In this method they used the fake RREQ message to attract the malicious node to respond the fake RREP message. In our scenario, there is more than one malicious node who will reply the fake RREQ packet. In this mechanism, before discovering the actual route for data transmission in AODV, a fake RREQ packet is broadcasted which includes the target or destination address which does not exist in reality. The multiple black hole nodes will immediately respond to the fake RREQ packet as they do not care about whether the fake target addressed node exists or not in the network. Basically, this mechanism enhances the security of AODV protocol with low routing overhead than other methods in MANET and also provide high packet delivery ratio. In [4] author proposed the method for detecting the single black hole node in MANET. In this method, the intermediate nodes send RREP message along with the next hop information. After getting this information, the source node sends further request to next hop node to verify that it has the route to the intermediate node or not. If the route exists, the intermediate node is trusted and source node will send data packets via that trusted node. If not, the reply message from intermediate node will be discarded and alarm message is broadcasted and isolate the detected node from network. By using this method, the routing overhead and end to end delay will be increased. If the black hole nodes work as a group in an attempt to drop packets, then this method is not efficient. In [5] they addresses the predicament of packet forwarding misbehavior and proposed a method to distinguish and confiscate the black and gray hole attacks. Their method is proficient in finding chain of cooperating malicious nodes which drop a momentous fraction of packets. In [6] proposed an adequate solution by checking RREP messages from intermediate nodes for possible intrusion activities. This technique is successful based on the assumption of cooperation between nodes. If a mobile node discovers a possible attack by an intruder, the discovering node notifies all other nodes the presence of an attack by broadcasting an ALARM message. This process takes a considerable amount of time to notify all nodes for a large network in addition to the network overhead that can be caused by ALARM broadcast. Produce a token, which is attached to the data packets to recognize the authenticity of the routing packets and to prefer correct route for data packets. TRP provides noteworthy reduction in energy consumption and routing packet delay by using hash algorithm. In [7] proposed an efficient solution for the detection of the Black hole nodes in the Mobile Ad hoc networks based on the AODV routing protocol. In this algorithm, known as Modified AODV mechanism a Watchdog mechanism is used. In this mechanism each and every node maintains two extra tables. First one is called the pending packet table and another one is called the node rating table. Pending Packet Table contains Packet ID, Next Hop, Expiry Time and Packet Destination while the Node Rating Table contains Node Address, Packet drops, Packet forwards and Misbehave. For the communication each and every node listens to those packets that are within the communication range of that particular node a threshold value is used for the detection of whether a node is malicious or not and also a node can repair all the nodes locally which contain the malicious node. In [8] provided an proficient techniques for the exposure of black hole and gray hole attack in mobile ad hoc networks based on the AODV routing protocol. In this technique malicious nodes are listed locally by each and every node when the nodes act as a source node. The protocol uses the concept of Core Maintenance of the Allocation Table. In the Allocation table when a new node joins the network, broadcast message for the request to get the IP address as it want to be a part of that network. The nodes, also called as the backbone nodes which receive this message chose a free IP address randomly and unicast this IP address to the requesting node. When the requesting node get this allotted IP address sends back an acknowledgement to the Black hole node. Thus the allocation is only done through the Backbone node and it has the overall control the malicious node can be easily detected. In [9] they anticipated a distributed and cooperative method to embark upon the black hole problem. The method is distributed so that it can vigorous with the ad hoc nature of network, and nodes in the protocol work cooperatively together so that they can investigate, distinguish, and eradicate possible multiple black hole nodes in a additional consistent fashion. The simulation results demonstrate that our method accomplishes a high black hole detection rate and high-quality packet delivery ratio, whereas the overhead is comparatively lower as the network traffic increases. In [10] they focused on analyzing and strengthening the security of routing protocol Ad-hoc On Demand Distance Vector (AODV) for MANET. The Proposed Method PL2 has the modification done in AODV protocol for ensuring the security against the Black hole attack using NS2 Simulation. PL2 method is PreLude, PostLude method. The proposed solution is an augmentation of the original AODV routing protocol to uncover a secure routes and thwart Black hole attack on MANET. The Major perception is based on time and neighborhood parameters. This method first check for malicious activity exists, and then starts detect and remove the Black hole nodes. Route discovery is same as original AODV, but when sending data packets, prelude and postlude messages are added. Simulation results show that the proposed method has good performance against Black hole attack and not much overhead. This solution holds good for gray hole attack also.

3. ROUTING PROTOCOL IN MANET

The mobile ad hoc network uses different routing protocols to transmit the packet from source to destination. The routing protocol is classified into three categories: proactive routing protocol, reactive routing protocol and hybrid routing protocol. The classification of routing protocol is illustrated in fig. 2 and description of these protocols is specified below.

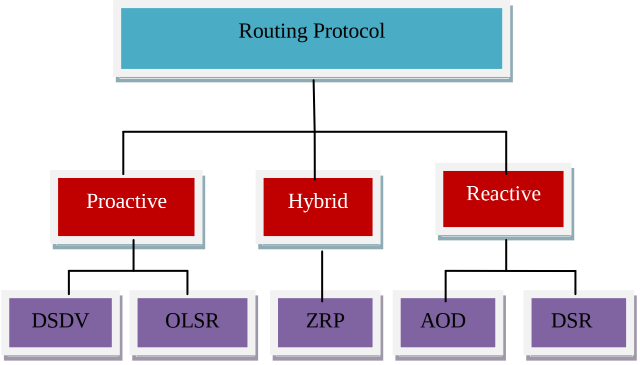

Fig.2: Classification Routing Protocol

3.1 Proactive or table driven routing protocol

This protocol is also called table-driven routing protocol. In such kind of protocol, nodes from time to time broadcast their routing information to the neighbors. Every node needs to sustain their routing table which not simply records the neighboring nodes and reachable nodes but also the number of hops. In other words, each of the nodes has to assess their neighborhoods as long as the network topology has distorted. Consequently, the shortcoming is that the overhead rises as the network size increases, a noteworthy communication overhead within a larger network topology. Nevertheless, the benefit is that network status can be instantaneously reflected if the malevolent attacker joins. Example of this protocol is DSDV (Destination sequence distance vector) and OLSR (Optimized link state routing) [11, 12].

3.2 Reactive or On demand Routing Protocol

Every node in this routing protocol maintains information of only active paths to the destination nodes. A route search is needed for every new destination therefore the communication overhead is reduced at the expense of delay to search the route. Rapidly changing wireless network topology may break active route and cause subsequent route search [13]. The example of reactive routing is AODV, DSR and TORA etc.

3.3 Hybrid Routing Protocol

This routing protocol is formed by using the essential features of both the reactive and proactive routing protocols. The well known example of this routing protocol is ZRP (Zone routing protocol) [13].

Ad Hoc on Demand Distance Vector (AODV) Routing Protocol

AODV is an ad-hoc on demand distance vector routing protocol that establishes route to the destination when it is desired by the source node. It maintains this route as and when needed by the source node. It recommended speedy adaptation to dynamic link circumstances, low processing, memory overhead, low network utilization, and decides on unicast routes to destinations surrounded by the ad hoc network [14]. One of the distinguishing features of AODV protocol is its use of destination sequence number associated with every route. Destination sequence number is fashioned by the destination to comprise route information about it send to the requesting node. In order to communicate among the mobile nodes, [14] the route requests (RREQs), route reply (RREPs), and route errors (RERRs) are the types of message defined by AODV. When a source node wants to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination is available or not. Fresh enough route means a valid route entry whose sequence number is greater than it in the RREQ. Larger the sequence number, fresher is the route. If a fresh enough route is available, it uses the same. Otherwise the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbors. This RREQ message will further be forwarded by the intermediate nodes to their neighbors having a fresh route to the destination. The RREQ message will eventually reach the destination node, which will react with a route reply message (RREP). The RREP is sent as a unicast to the source node along the reverse route established during the RREQ broadcast. Similarly, the RREP message allows intermediate nodes to learn a forward route to the destination node. Therefore, at the end of the route discovery process, packets can be transported from a source node to a destination node and its reverse. A route error message (RERR) allows nodes to notify errors due to link breakage, such as when a previous neighbor moves to a new position and is no longer reachable. Each mobile node would periodically send Hello messages (HELLO), thus, each node knows which nodes are its neighboring nodes. AODV as a reactive routing protocol does not give nodes a complete view of network topology. That is, each node only knows its neighbors, and for the non - neighbors, it only knows the next hop to reach them and the distance in hops. However, the security of AODV is compromised by the Black Hole nodes, as it accepts the received RREP having fresher route. The standard AODV routing protocol cannot fight the threat of Black Hole attacks, because during the phase of route discovery, malicious nodes may counterfeit a sequence number and hop count in the routing message; thereby, acquiring the route [15], eavesdropping and dropping all the data packets as they pass or forward some selective packets to the destination.

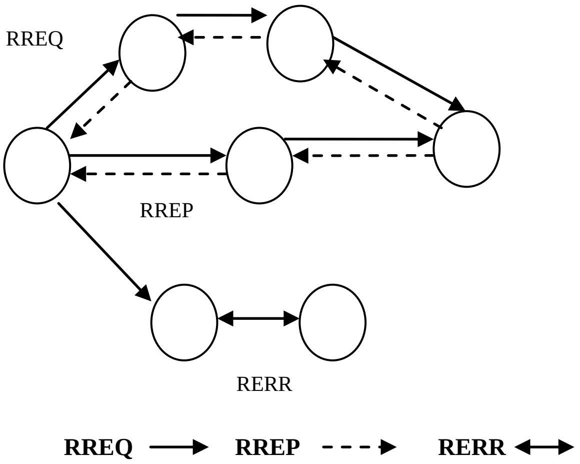

Fig. 3 AODV routing protocol in MANET

4. PROBLEM STATEMENT

BLACK HOLE ATTACK IN AODV & COUNTER MEASURES

A Black hole attack is one of the active DoS attacks possible in MANETs. In this attack, a malicious node sends a false RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbor to the actual destination node. When a source node broadcasts the RREQ message for any destination, the black hole node immediately responds with an RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source assumes that the destination is behind the black hole and discards the other RREP packets coming from other nodes. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other [16]. As shown in Fig. 4, we assume that Node B is the malicious node. When Node S broadcasts the RREQ message for Node D, Node B immediately responds to Node S with an RREP message that includes the highest sequence number of Node D, as if it is coming from Node D. Node S assumes that Node D is behind Node B with 1 hop and discards the newly received RREP packet come from Node 2. Afterwards Node S starts to send out its data packet to the node B trusting that these packets will reach Node D but Node B will drop all data packets. In a Black Hole Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets.

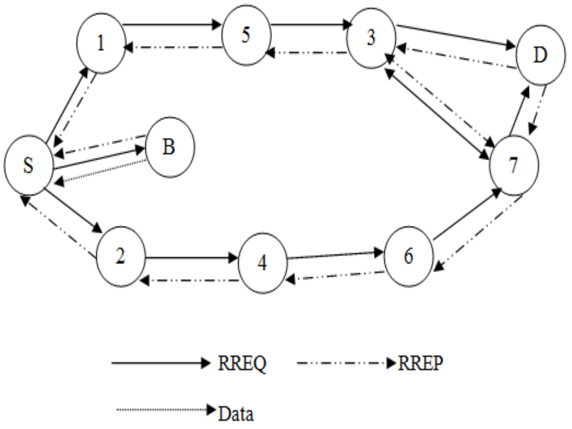

Fig. 4 Blackhole attack in AODV

Cooperative Black-hole Attack

It is a type of attack in which black hole nodes act in a group together. For example when multiple black hole nodes are acting in coordination with each other, the first black hole node refers to the one of its teammate in the next hop .This type of attack harms the system very much and affect the throughput of the system [19].

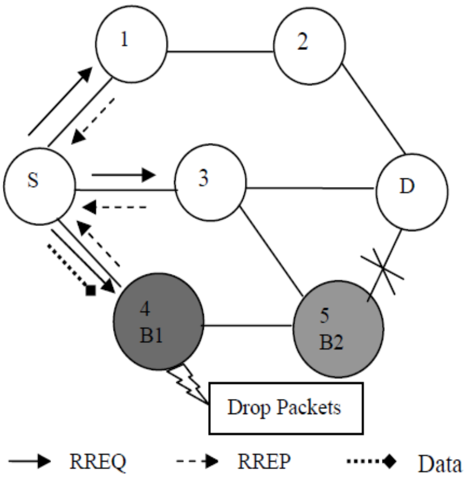

Fig. 5 Process of Cooperative black hole attack in AODV

Performance Parameter

For evaluating the performance of the communication system different parameter is used such as throughput, PDR, end to end delay and average jitter etc. The description of this parameter is depicted below [17]:

A. Throughput

It is defined as the total number of packets delivered over the total simulation time. It is symbolized in packets per second or bits per second.

$$Throughput\ (bps) = \frac{No.of\ deliverd\ packets * Packet\ Size * 8}{Simulation\ Time}$$

B. Packet Delivery Ratio

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by source.

$$PDR = \frac{Number\ of\ packet\ received}{No\ of\ packets\ sent}$$

C. End-to-End Delay

The average time acquired by the packets to pass through the network is called end-to-end delay.

$$E-2-E\ delay[packet\_\ id] = received\ time[packet\_id] - sent\ time[packet\_id]$$

$$Average\ Delay = \sum_{i=1}^{n} d_i/n$$

Where, d_i= average end to end delay of node of i_{th} application and n=number of application.

D. Average Jitter

The average Jitter is the undesired variation from true periodicity of an unspecified periodic signal in electronics and telecommunications, frequently in relation to a reference clock source.

E. Normalized Routing Load NRL

It is the amount of routing packets transmitted per data packet transported at the pursuit. Each hop-wise transmission of a routing packet is counted as one transmission [18].

$$NRL = \frac{Number\ of\ routing\ packet\ sent}{Number\ of\ routing\ packet\ received}$$

5. PROPOSED METHOD

Wireless ad-hoc network has dynamic topology and self-configuring network, due to these characteristic it is more vulnerable to security attacks and black-hole attack is in one of them. Hence, in the proposed method, a technique is being developed which will help to increase the battery lifetime and proper use of resources. This proposed method will detect and prevent the network from this attack, improve the performance of packet delivery ratio and throughput of the network and will also minimize the network overhead by increasing the resource utilization which helps in networking.

Expected Outcome

Multiple scenarios will be monitored under AODV protocol, in a network in order to measure the parameters such as throughput, PDR, average jitter, End-End Delay and NRL. As the AODV protocol is modified using the proposed technique, we will get the optimum solution.

6. CONCLUSION

Wireless network uses dynamic topology to form the network and due to their this behavior a number of attack make harms to the network and black hole attack is one of them which broadcast the fake route to transmit the data. To guard the network from such kind of denial of service various techniques has been proposed. In this paper literature study of the proposed methodology is summarized but some methods are efficient to diminish the overhead but it consumes more network bandwidth and less utilizes the network resources. We also mention some counter measures to analyze the performance of the network. In future work, need to design methodology which greatly reduces the network traffic and routing overhead and also improves packet delivery ratio.

7. REFERENCES

[1] Raut Deepali, Hande Kapil, "Detection and Prevention of Gray Hole and Black Hole Attack in MANET", IJCA 2014.

[2] Tseng Fan-Hsun, Chou Li-Der and Chao Han-Chieh, “A survey of black hole attacks in wireless mobile ad hoc networks”, Human-centric Computing and Information Sciences 2011, 1:4 a Springer open access journal.

[3] Kalia Nishu, Munjal Kundan, “Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.

[4] Deng Hongmei, Li Wei, and Agarwal Dharma P., “Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.

[5] Banerjee Sukla, “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks”, Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[6] N. Raj Payal and Swadas Prashant B., “DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET”, International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[7] Bhosle Amol A., Thosar Tushar P. and Mehatre Snehal, “Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET”, International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012 DOI: 10.5121/ijcsea.2012.2105 45.

[8] Choudhary Sarita, Sachdeva Kriti, “Discovering a Secure Path in MANET by Avoiding Black Holes”, International Journal of Recent Technology and Engineering (IJRTE) SSN: 2277-3878, Volume-1, Issue-3, August 2012.

[9] Yu Chang Wu, Wu Tung-Kuang, Cheng Rei Heng, and Chang Shun Chao, “A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks”, PAKDD 2007 Workshops, LNAI 4819, pp. 538–549. © Springer-Verlag Berlin Heidelberg 2007.

[10] S Vasanthavalli., Gowd R. Bhargava Rama, Thenappan S. “Peruse Of Black Hole Attack and Prevention Using AODV on MANET”, International Journal of Innovative Research in Science, Engineering and Technology”, Vol. 3, Issue 5, May 2014, ISSN: 2319-8753.

[11] CE Perkins, P Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”, Paper presented at the ACM SIGCOMM’94 Conference, London, United Kingdom, August 31 - September 2,1994

[12] P Jacquet, P Muhlethaler, T Clausen, A Laouiti, A Qayyum, L Viennot, “Optimized Link State Routing Protocol for Ad Hoc Networks” Paper presented at the IEEE International Multi Topic Conference, Lahore, Pakistan, 28-30 December 2001.

[13] Mario Joa-Ng, “A Peer-to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks”, IEEE Journal on selected areas in communications, Vol. 17, No. 8, Aug-1999.

[14] Funde Nitesh A., Pardhi P. R., “Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013, ISSN (Print) : 2319-5940

[15] Dokurer,Seimih “Simulation of Black hole Attack in wireless ad-hoc Networks” Master’s Thesis Atihm University, September 2006.

[16] Vipan Chand Sharma, Atul Gupta and Vivek Dimri, “Detection of Black Hole Attack in MANET under AODV Routing Protocol”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013 ISSN: 2277 128X.

[17] Kaur Ramanpreet, Kaur Anantdeep, “BLACKHOLE DETECTION IN MANETS USING ARTIFICIAL NEURAL NETWORKS”, International Journal For Technological Research In Engineering Volume 1, Issue 9, May-2014 ISSN (Online): 2347 – 4718.

[18] “Performance Evaluation of AODV routing Protocol under Black Hole attack with varying Black hole nodes”, 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[19] Tamilselvan Latha, “Prevention of Co-operative Black Hole Attack in MANET”, JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008.

8. APPENDIX

Table 1: Comparison of different detection mechanism

Author/Researchers	Publishing year	Types of black hole attack	Drawbacks
Kalia Nishu et al.	2013	Multiple	Packet delivery ratio is less
Deng Hongmei et al.	2002	Single	Overhead and end to end delay increased
Banerjee Sukla et al.	2008	Multiple	Packet drop increased
N. Raj Payal et al.	2009	Single	Less effective to reduce the end-2-end delay and overhead
Bhosle Amol A. et al.	2012	Multiple	Routing overhead increased
Choudhary Sarita et al.	2012	Single	Throughput decreased
Yu Chang Wu et al.	2007	Multiple	Less efficient to reduce the overhead
S Vasanthavalli et l.	2014	Single	Less efficient to reduce the overhead due to increase of network traffic