Routing AODV Defending Black Hole Attack through NS3 in Manet

Anupam Mishra
M.Tech Scholar ECE
SHUATS

Rajeev Paulus, PhD
Assistant Professor ECE
SHUATS

Aditi Agrawal
Assistant Professor ECE
SHUATS

ABSTRACT
A mobile-ad hoc network system is a infrasturcture less system which comprises of various versatile hubs that progressively frame an impermanent system for the transmission of information from source to goal. They are made out of hubs that transfer on each other to oversee and for secure transmission of activity because of absence of unified organization. As MANETs turn out to be broadly utilized, the security issue has ended up being one of the essential worries for everybody of the circumstances. One of the outstanding assault is the Black Hole attack which is most basic in the on-request steering conventions, for example, AODV.

In this paper, the proposed arrangement is to adjust the AODV directing convention such that it can battle the agreeable Black Hole assault. The outcomes demonstrate a successful increment in throughput and PDR.

Keywords
MANET, AODV, Black Hole Attack, NS-3

1. INTRODUCTION
A mobile ad hoc network system (MANET), otherwise called remote specially appointed network or impromptu remote system, is a constantly self-designing, foundation less system of cell phones associated wirelessly.

Every gadget in a MANET is allowed to move autonomously toward any path, and will in this way change its connection to different gadgets often. Each must forward movement irrelevant to its own particular utilize, and accordingly be a switch. The basic test in building a MANET is setting up each device to diligently keep up the information required to really course movement. Such systems may work without anyone else's input or might be associated with the bigger Internet. They may contain one or various and assorted handsets between center points. This results in an especially intense, self-decision topology.

MANETs are a sort of wireless ad hoc network system (WANET) that more often than not has a routable systems administration condition over a Link Layer specially appointed system MANETs comprise of a distributed, self-framing, self-mending system. MANETs around 2000– 2015 commonly impart at radio frequencies (30 MHz – 5 GHz). The development of workstations and 802.11/Wi-Fi remote systems administration have made MANETs a well known research point since the mid-1990s. Numerous scholarly papers assess conventions and their capacities, accepting changing degrees of portability inside a limited space, for the most part with all hubs inside a couple of jumps of each other. Different protocols are then assessed in light of measures, for example, the packet drop rate, the overhead presented by the directing convention, end-to-end packetl delays, arrange throughput, ability to scale, etc

Flexible extraordinarily selected frameworks can be used as a piece of numerous applications, extending from sensors for condition, vehicular impromptu correspondences, street security, wellbeing, home, shared informing, debacle protect operations, air/arrive/naval force guard, weapons, robots, and so forth.

Accordingly, early work in MANET inquires about concentrated on giving steering administration least cost regarding transmission capacity and battery control. There are a wide assortment of assaults that objective the shortcoming of MANET. For instance, directing messages are a fundamental part of versatile organize correspondences, as every packet should be passed rapidly through middle hubs, which the packet must navigate from a source to the goal. Vindictive steering assaults can focus on the directing disclosure or support stage by not following the details of the specific protocols. There are also attack that objective some specific routing protocol, for example, DSDV, or AODV. More advanced and unpretentious specific attack have been recognized in late distributed papers, for example, the dark gap (or sinkhole), Byzantine, and wormhole assaults. As of now directing security is one of the most blazing exploration territories in MANET.

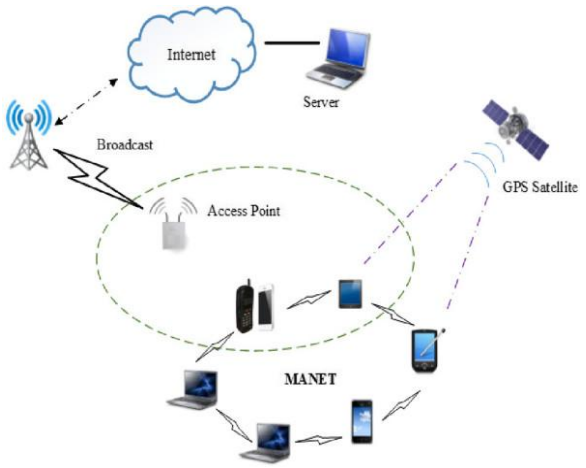

Figure 1: Block Diagram of MANET

2. ROUTING PROTOCOLS IN MANET
A specially appointed directing convention is a tradition, or standard, that controls how nodesdecide which approach to course packet between processing gadgets in a versatile impromptu system. In impromptu systems, hubs are not acquainted with the topology of their systems. Rather, they need to find it: normally, another hub declares its essence and tunes in for declarations communicate by its neighbors. Every hub finds out about others adjacent and how to contact them, and may report that it also can contact them.

Note that in a more extensive sense, specially appointed convention can likewise be utilized truly, to mean an ad libbed and regularly unrehearsed convention set up for a particular reason

Table.1. Types of Routing Protocols in MANET

ROUTING PROTOCOLS		
PROACTIVE	**REACTIVE**	**HYBRID**
DSDV	AODV	ZRP
OLSR	LMR	BGP
CGSR	TORA	EIGRP
WRP	DSR	
TBRF	LQSR	
QDRP		

3. AODV (AD-HOC ON-DEMAND DISTANCE VECTOR)

Ad-hoc On-request Distance Vector (AODV) steering convention is a responsive directing convention in which the system is set up just when the source hub wants to transmit information packets to the goal. The principle recognizing highlight of AODV is the utilization of succession numbers for each course section. It communicates the RREQ, i.e., Route Request packet to its neighboring hubs to discover a course to the goal hub. The source augments its grouping number each time it creates a demand packet and it has the current succession number of the goal which the source knows about. The RREQ packet is sent to alternate hubs until a RREP, i.e., Route Reply packet, originates from the goal or a middle hub which has a new course to the goal. In the wake of getting the RREP, the source advances the information packets to goal by means of the middle of the road hub.

The figure shows the route discovery process from source to destination in AODV:

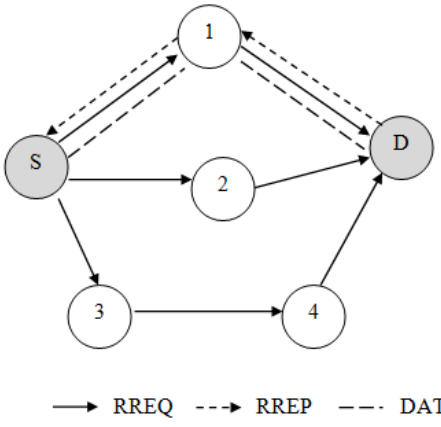

Fig 2: Topology graph of the network

4. BLACK HOLE ATTACK (PACKET DROP ATTACK)

In PC organizing, a packet drop attack or blackhole attack is a sign of disapproval of benefit attack in which a switch that should hand-off packet rather disposes of them. This as a rule occurs from a change getting the opportunity to be bargained from various diverse causes. One reason specified in inquire about is through a dissent of benefit attack on the switch utilizing a known DDoS tool. Because packet are routinely dropped from a lossy framework, the packet drop attack is hard to recognize and neutralize.

The packet drop attack can be as often as possible conveyed to attack remote specially appointed systems. Since remote systems have a vastly different engineering than that of a common place wired system, a host can communicate that it has the most limited way towards a goal. By doing this, all activity will be coordinated to the host that has been traded off, and the host can drop packets at will. Also finished a versatile specially appointed system, has are particularly helpless against synergistic attack where different hosts will move toward becoming bargained and fake alternate has on the network. Figure 3 below shows a black hole node 'X' which gives a false RREP to the source of having a fresh route to the destination. The source, then, routes all the data packtes towards the black hole node and this node absorbs all the data. Thus, the data packets are dropped and never reach the destination.

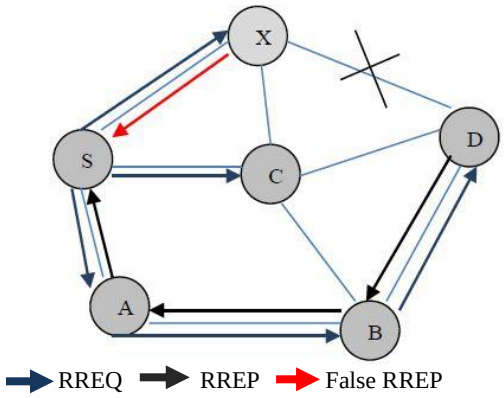

Fig.3. Black Hole Attack

5. SIMULATION MODEL (NS-3)

The NS-3 (Network Simulator Version 3) is a protest arranged, discrete occasion driven system test system created at UC Berkeley written in C++ and OTcl and is available as open source. It is widely used for simulating wired and wireless networks. It follows the layered approach and has protocols for governing the networks. The simulation is done using NS-3 to analyse the performance of wireless ad hoc network with and without the black hole attack. At the physical and data link layer IEEE 802.11 is used. The channel is wireless channel with Two Ray Ground Propagation model. The protocol used at the network layer is AODV. The AODV protocol can model the behaviour of nodes as normal nodes or black hole. The traffic pattern was generated using CBR as the data source and UDP protocol is used for transporting the data and the packet size is of 512 bytes. The simulations are done for various situations by fluctuating the quantity of nodes, mobility of the nodes, position of the black hole node, the number of flows and the number of black hole nodes.

6. SIMULATION RESULT

The simulation is done using NS3, i.e., Network Simulator version 3. NS3 is an occasion driven reproduction device that is used to study the dynamic idea of communication systems.

The parameters used in the simulation are shown below:

Table.1. Simulation Parameters

Parameters	Values
Network size	700 m * 700 m
Number of Nodes	10-70
Max. speed/mobility	15.0 m/sec
Pause Time	3.0 s
Traffic Model	CBR
Routing Protocol	AODV
Simulation Time	100

6.1 Packet Delivery Ratio

It can be defined as the ratio of total number of data packets delivered to the destination to the total number of data packets generated by the source. It is figured as –

$$P = \frac{number\ of\ packets\ sent}{number\ of\ packets\ received} \times 100$$

A decrease in PDR is seen at the same time that is a black hole attack on AODV. In the outcomes, we can see which is a successful increment in the PDR of modified AODV.

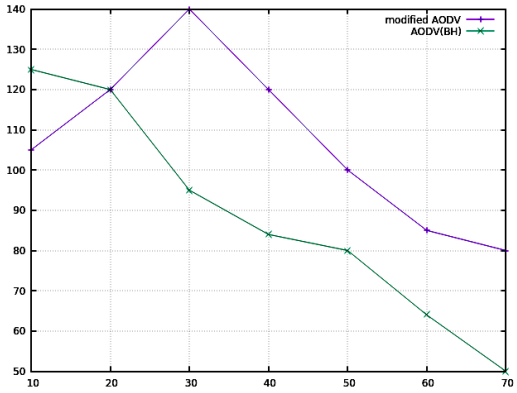

Fig.3. Packet Delivery Ratio vs No. of nodes

6.2 Average Throughput

It is the average rate of successful message delivery over a communication channel. It is measured in data packets per second.

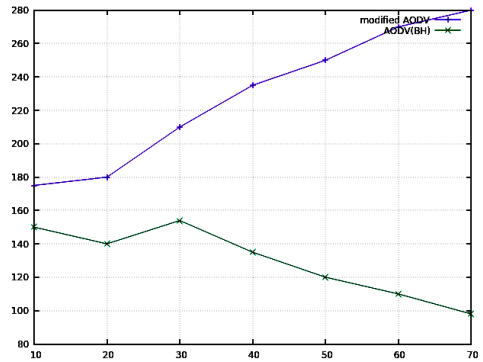

Fig 4: Average Throughput Vs No. of Nodes

Fig.4. shows that the throughtput is decreases due to black hole attack but without black hole it is increases in modified routing AODV.

6.3 Average End-to-End delay

It is the average delay between the sending of packets by the source and its receipt by the receiver.

Fig..4. shows that the Average End to End Delay with black hole attack is much higher than without black hole attack in AODV routing protocol.

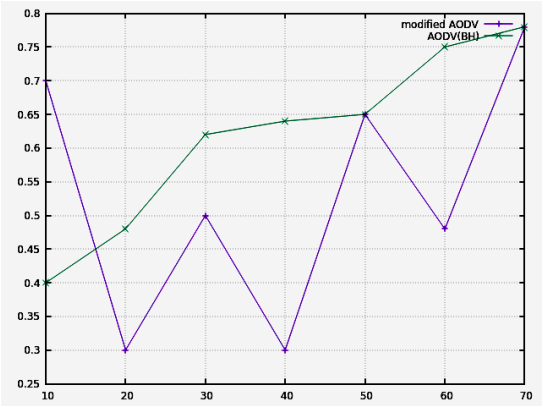

Fig 5: Average End to End Delay vs Number of Nodes

6.4 Packet Drop Ratio

It is the ratio of the data lost at destination to those generated by the CBR sources. The packets are dropped when the node is not able to find the valid route to the node specified as an intermediate node in the route to reach the destination node.

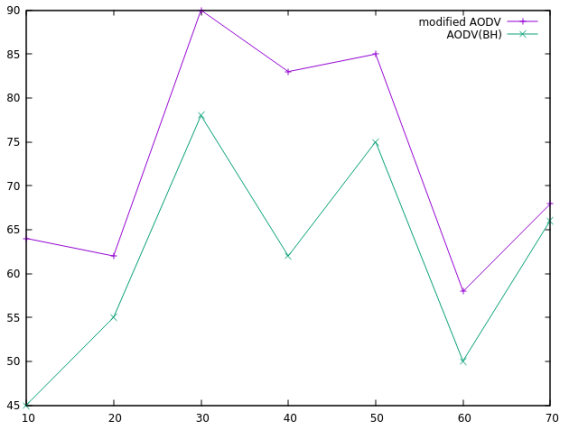

Fig 6: Packet Drop Ratio vs No. of Nodes

7. CONCLUSION AND FUTURE WORK

Mobile ad hoc network systems have picked up consideration because of its self-setup and self-sufficient abilities. Because of different troubles in planning of secure routing protocol, MANET has dependably been an essential concern. In this paper, our principle concern is of Black Hole Attack which is a dynamic dissent of administration attack in AODV routing which takes every one of the information packets from the source and retains them. The proposed arrangement which can be mounted against black hole attack in MANET. The proposed technique can be utilized to distinguish black hole nodes in the system and finding secured courses for transmission of information According to this work, we observe that how the AODV routing protocol works and the effect of black hole attack on AODV routing protocol and how to modified the AODV routing protocol.

According to performance analysis of MANETS routing protocol AODV with respect to different performance metrics like Packet Delivery Ratio (PDR), Packet Drop Ratio (PDRR), Throughput (Th), and End-To-End delay both with and without Black Hole attack in the network

As future work, we try to develop simulations to decrease the Packet Drop Ratio over the network.

8. REFERENCES

[1] F.H. Tseng, Li-Der Chou, H.C. Chou, Human-centric Computing and Information Sciences 2011, "A survey of Black Hole Attacks in wireless mobile ad-hoc networks".

[2] Gagandeep, Aashima, Pawan Kumar, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review".

[3] Teerawat Issariyakul, Ekram Hossain, Introduction_to_network_Simulator_NS2.

[4] L. Tamilselvan, V. Sankaranarayanan: "Prevention of Black Hole Attack in MANET", the 2nd international conference on wireless, Broadband and Ultra Wideband Communications (January 2007).

[5] M. AI-Shurrnan et al: "Black Hole Attack in Mobile Ad Hoc Network", ACMSE' 04, (April 2004).

[6] M. Medadian, K. Fardad, European Journal of Scientific Research, Vol. 69 No. 1 (2012), "Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol".

[7] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) "Improving AODV Protocol Against Blackhole Attacks", Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010.

[8] M. Umaparvathi, D.K. Varughese, European Journal of Scientific Research, Vol. 72 No. 3 (2012),"Two Tier Secure AODV against Black Hole Attack in MANETs".

[9] Pooja Jaiswal, Rakesh Kumar, International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501Vol.2, No5, October 2012, "Prevention of Black Hole Attack in MANET".

[10] S. A. Razak, S. M. Furnell, P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols",2004.

[11] Sun B, Guan Y, Chen J, Pooch UW (2003) "Detecting Black-hole Attack in Mobile Ad Hoc Networks", Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, U.K., 22-25 April 2003.

[12] Sweta Jain, Jyoti Singhai, Meenu Chawla, International journal of Ad hoc, Sensor & Ubiquitous Computing Vol. 2, No. 3, 2011, "A Review Paper on Cooperative Blackhole and Grayhole Attacks in MANETs".

[13] S.K. Chamoli, S. Kumar, D.S. Rana, International Journal of Computer Technology & Applications, Vol. 3 (4), 2012, "Performance of AODV against Black Hole Attacks in MANETs".

[14] S. Kurosawa, H. Nakayama, and N. Kato, "Detecting black hole attack on AODV based mobile ad-hoc networks by dynamic learning method, "*International Journal of Network Security"*, pp. 338–346, 2007.

[15] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA.

[16] Ujjwal Agarwal, K.P Yadav, Upendra Tiwari, International Journal of Research in Science and Technology, 2012, vol. no. 1, issue no. IV, Jan-Mar, "Security Threats in Mobile Ad hoc Networks".

[17] Yih-Chun, Adrian Perrig, David B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad Hoc Networks",sparrow.ece.cmu.edu/~adrian/projects/securerouting/ariadne.pdf, 2002

[18] E. Çayırcı, C.Rong, "Security in Wireless Ad Hoc and Sensor Networks," vol. I. New York, Wiley, pp. 10, 2009.

[19] 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.

[20] Zaid Ahmad, Jamalul-lali Ad Manan, Kamarularifin Abd Jalil,"Performance Evaluation on Modified AODV Protocols", IEEE Asia-Pacific Conference on Appiled Electromagnetics, Dec. 11-13, 2012.