

# Ant Based Black Hole Detection and Prevention in MANET

Mr. Salman Bhimla<sup>1</sup> Mr. Sunil Gupta<sup>2</sup>  
<sup>1,2</sup>North South University

*Abstract*--- Mobile ad hoc network (MANET) consists of a set of mobile hosts that carry out basic networking functions like routing, packet forwarding and service discovery without the help of an established infrastructure. The nodes of an ad hoc network rely on one another in forwarding a packet to its destination; due to the limited range of each mobile host's wireless transmissions. Security in MANET is an essential component for basic network functions like packet forwarding and routing: network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. In MANET, Black hole attacks may cause packet dropping, misrouting the information from source to destination. So the performance of the network is totally degraded. The biology-inspired techniques like as ant colony optimization (ACO) which have proven to be very adaptable in other problem domains have been applied to the MANET routing problem as it forms a good fit to the problem.

## I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator also the wireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure [1]. MANET is a self-configuring infrastructure less network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction and will therefore change its links to other devices frequently. Every must forward traffic unrelated to its own use and therefore be a router. Primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. These networks may operate by themselves or may be connected to the larger Internet. Mobile ad-hoc networks (MANETs) are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network.

## II. BLACK HOLE ATTACK IN MANET

Black hole problem in MANETS [2] is a serious security problem to be solved. In this, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. Whenever the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created in flooding based protocol. That malicious node then can choose whether to drop the packets to

perform a denial-of-service attack or to use its place on the route as the first step in a man-in-the-middle attack.

In this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. The attacker listens the requests for routes in a flooding based protocol. Although the attacker receives a request for a route to the destination node, that creates a reply consisting of an extremely short route. Although the malicious reply reaches the initiating node before the reply from the actual node, the fake route gets created. And once the malicious device has been able to insert itself between the communicating node, that are able to do anything with the packets passing between them. That can drop the packets between them to perform a denial-of-service attack or alternatively use its place on the route as the first step in a man-in-the-middle attack. E.g.: in Figure, source node S wants to send data packets to destination node D and initiates the route discovery process. Here we assume that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets and immediately sends the response to node S. Whenever, the response from the node 2 reaches first to node S then node S thinks that the route discovery is complete ignores all other reply messages and begins to send data packets to node 2. So as a result, all packets through the malicious node is consumed or lost.

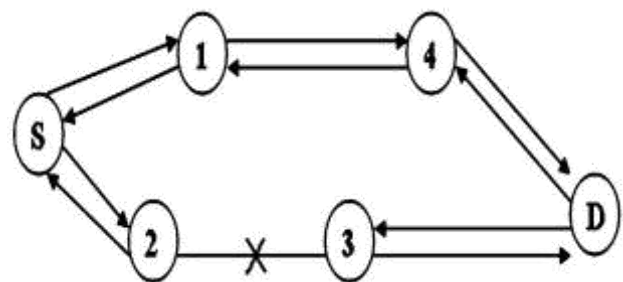


Fig. 1: Black hole attack [2]

## III. SOLUTION FOR BLACK HOLE ATTACK

The traditional routing protocols face many problems due to the dynamic behavior and resource constraints in MANETS. To overcome this limitation, an approach to achieve such feature is to use a biologically-inspired mechanism. The social organization of the ant is genetically evolved commitment of each individual to the survival of the colony. This is a key factor behind their success. Moreover, these insect societies exhibit the fascinating property that the activities of the individuals as well as of the society as a whole are not regulated by any explicit form of centralized control. Most successful and most popular research direction in ant algorithms is dedicated to their application to

combinatorial optimization problems and it goes under the name of Ant Colony Optimization meta heuristic (ACO). ACO finds its roots in the experimental observation of a specific foraging behavior of colonies of Argentine ants *Linepithemahumile* which under some appropriate conditions are able to select the shortest path among the few alternative paths connecting their nest to a food reservoir. When moving, the ants deposit a volatile chemical substance called pheromone and, according to some probabilistic rule preferentially move in the directions locally marked by higher pheromone intensity.

**A. ANT IN NATURE**

The main source of inspiration behind ACO is a behaviour that is displayed by certain species of ants in nature during foraging. That has been observed that ants are able to find the shortest path between their nest and a food source. Only way that this difficult task can be realized is through the cooperation between the individuals in the colony (Caro & Dorigo, 1998) [3]. A key behind the colony level shortest path behaviour is the use of pheromone. It is a volatile chemical substance that is secreted by the ants in order to influence the behaviour other ants and of it. The pheromone is not only used by ants to find shortest paths but is in general is an important tool that is used by many different species of ants (Caro & Dorigo, 1998) [3]. The ants moving between their nest and a food source leave a trail of pheromone behind and they also preferably go in the direction of high intensities of pheromone. Ants moving between their nest and a food source leave a trail of pheromone behind and they also preferably go in the direction of high intensities of pheromone.

**B. ANT Based AODV(AAODV)**

AAODV is an ACO algorithm for distributed and traffic-adaptive multipath routing in wired best effort IP networks. The AAODV design is based on ACO’s general ideas as well as on the work of Schoonderwoerd et al. [4,5] that was a first application of algorithms inspired by the foraging behaviour of ant colonies to routing tasks (in telephone networks). AAODV behavior is based on the use of mobile agents.

Informally, the behavior of AAODV can be summarized as follows [6]:

- 1) From each network node *s* mobile agents are launched towards specific destination nodes *d* at regular intervals and concurrently with the data traffic. The agent generation processes happen concurrently and without any form of synchronization among the nodes.
- 2) Each forward ant is a random experiment aimed at collecting and gathering at the nodes non-local information about paths and traffic patterns. Forward ants simulate data packets moving hop-by-hop towards their destination. They make use of the same priority queues used by data packets.
- 3) Ants, once generated, are fully autonomous agents. They act concurrently, independently and asynchronously. These communicate in an indirect, stigmergic way through the information they locally read from and write to the nodes.
- 4) Specific task of each forward ant is to search for a

minimum delay path connecting its source and destination nodes.

- 5) The forward ant migrates from a node to an adjacent one towards its destination. At each intermediate node, a stochastic decision policy is applied to select the next node to move to. The parameters of the local policy are: (i) the local pheromone variables, (ii) the status of the local link queues (playing the role of heuristic variables), and (iii) the information carried into the ant memory (to avoid cycles). The decision is the results of some tradeoff among all these components.
- 6) When moving, the forward ant collects information about the traveling time and the node identifiers along the followed path.
- 7) They have returned to their source node, the agent is removed from the network.

**IV. RESULTS**

In the research the implementation is performed on the NS2 that is installed over fedora 17. The AWK scripts are used to evaluate various parameters. The AWK script use the TR file to get result. The parameter evaluated by running AWK scripts on the TR file generated by TCL file are shown in following tables.

Number of nodes	Generated Packet	Received Packet	PDF	E2EDelay(ms)	Delay Jitter	Normalized Routing Load
10	1246	1176	0.9438	34.725	41.41	0.998
20	1932	1904	0.9855	34.7228	64.70	0.955
30	5817	5777	0.9931	34.6093	134.70	0.992
40	2900	2876	0.9917	34.7239	33.20	0.833

Table1: Various Parameters on Different Number of Nodes in Existing System (AODV)

Number Of Nodes	Generated Packet	Received Packet	PDF	E2EDelay(ms)	Delay Jitter	Normalized Routing Load
10	2700	2660	0.9852	8.621	20.20	0.964
20	576	574	0.9965	10.3627	55.50	0.930
30	3054	3054	1.0	18.3308	101.94	0.979
40	678	676	0.9971	8.2495	28.12	0.478

Table2: Various Parameters on Different Number of Nodes in Proposed System (AAODV)

Figure 2 and Figure 3 shows the graph of number of packets generated and the number of packets Received in the existing system and in the proposed system. The graphs are

drawn for the various numbers of nodes.

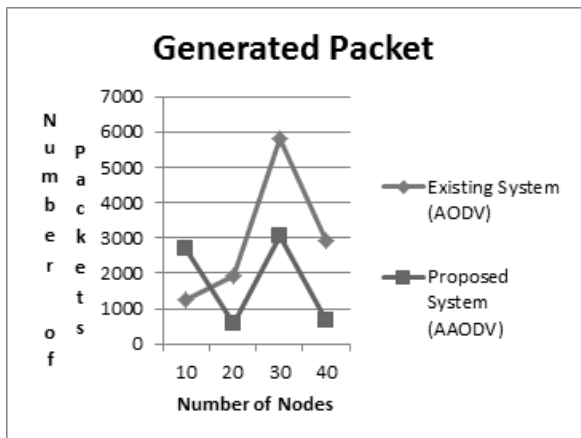


Fig. 2: Generated packet VS Number of Nodes

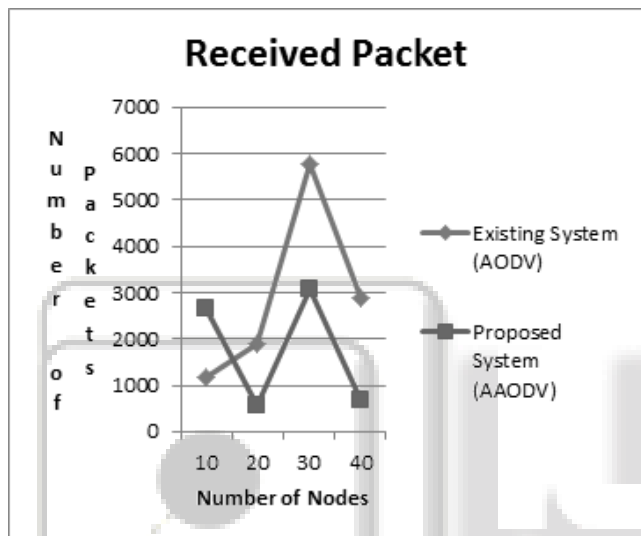


Fig. 3: Received packet VS Number of Nodes

Packet Delivery Ratio (PDR): The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

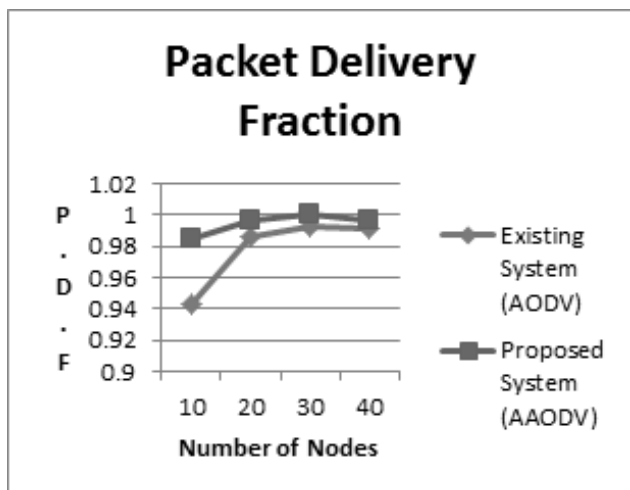


Fig. 4: Packet delivery Fraction VS Number of Nodes

$\sum$  Number of packet receive /  $\sum$  Number of packet send  
 End-to-end Delay: The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully

delivered to destinations that counted.

$$\frac{\sum (\text{arrive time} - \text{send time})}{\sum \text{Number of connections}}$$

The figure 4 and Figure 5 shows the packet delivery fraction and the end 2 end delay of the existing and the proposed system. The PDF and E2E delay is evaluated for the various numbers of nodes. The graph shows that the PDF increases while the E2E Delay decreases in the proposed system (AAODV).

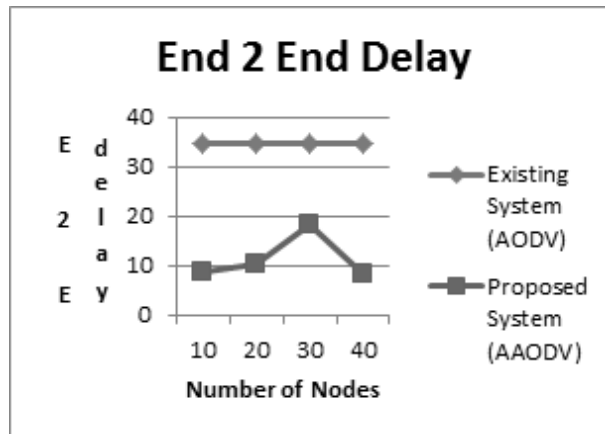


Fig. 5: END to END Delay VS Number of Nodes

The Figure 6 and Figure 7 show the Delay Jitter and the Normalized Routing Load of the existing and the proposed system. The delay jitter and normalized routing load is evaluated for the various numbers of nodes. The graph shows that the delay jitter and normalized routing load decreases in the proposed system (AAODV).

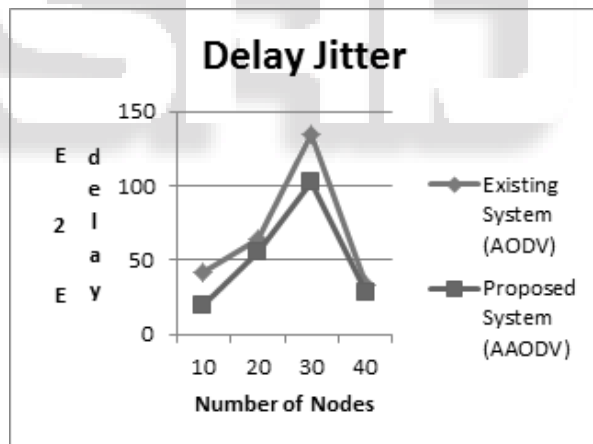


Fig. 6: Delay Jitter VS Number of Nodes

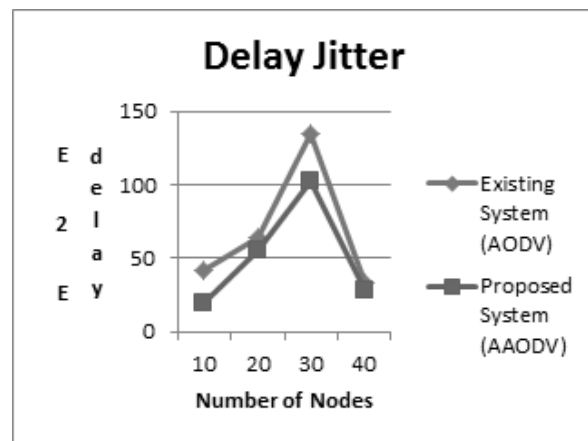


Fig. 7: Normalized Routing Load VS Number of Nodes

## V. CONCLUSION

Multi hop Mobile Ad hoc Network (MANET) is an infrastructure less in which mobile nodes communicate directly and cooperatively with each other. Biggest challenge in MANETs is to find a path between communicating nodes. MANET environment and the nature of the mobile nodes create further complications which results in the need to develop special routing algorithms to meet these challenges. In the ant societies activities of the individuals are not regulated by any explicit form of centralized control but are the result of self-organizing dynamics driven by local interactions and communications among a number of relatively simple individuals. That unique characteristic has made ant societies an attractive and inspiring model for building new algorithms and new multi-agent systems. Our results shows that ACO based protocols perform better than conventional protocols in terms of end-to-end delay and packet delivery ratio. Our research findings may be useful for researchers who wish to modify the existing ACO based protocols.

## REFERENCES

- [1] Saleh Ali K. Al-Omari, Putra Sumari, "An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications", *Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks (J GRAPH-HOC)* Vol.2, No.1, March 2010
- [2] Mohammad Al-Shurman et. al, "Black Hole Attack in Mobile Ad Hoc Networks", *ACMSE'04*, April 2-3, 2004, Huntsville, AL, USA. Copyright 2004 ACM 1-58113-870-9/04/04...\$5.00.
- [3] Caro, G.D. & Dorigo, M. (1998). Mobile agents for adaptive routing. *Thirty-First Hawaii Intl. Conf. Syst. Sci.*, pp. 74-83.
- [4] R. Schoonderwoerd, O. Holland, J. Bruten, and L. Rothkrantz. "Ant-based load balancing in telecommunications networks". *Adaptive Behavior*, 5(2):169–207, 1996.
- [5] R. Schoonderwoerd, O. Holland, and J. Bruten. "Ant-like agents for load balancing in telecommunications networks". In *Proceedings of the First International Conference on Autonomous Agents*, pages 209—216. ACM Press, 1997.
- [6] Arif, Mohammad, and Tara Rani. "ACO based routing for MANETs." *arXiv preprint arXiv:1205.1604* (2012).