Simulation Analysis for improvement of network efficiency by preventing Black hole Attack using ACO

Navjot Kaur¹, Harleen Kaur²

¹Chandigarh engineering collage, Mohali, Punjab, India
Email id: Navjotkrjoti@gmail.com

ABSTRACT

In this paper, the research work deals with the black hole attack prevention and its effect on network performance and then optimization using ACO approach is done in which fitness function optimization takes place. The packets transmitted in this way are made to drop so as no unauthorized access is available to transmitted data. The whole simulation has been done in MATLAB environment to carry out the performance of the proposed work.

Keywords: Black Hole Attack, ACO, Security, MANET.

1. Introduction

Computer networks differ on the basis of physical media used to transmit their signals, the communication protocols used to organize network traffic, the size of the network, topology used in the network. Ad-hoc network is a new standard of wireless communication for mobile hosts. Basically it’s a network which is used in case of urgent situations. All the nodes act as router in this network [1].

The primary challenge in building a MANET is equipping each device to continuously maintain the information which is necessary to properly route the traffic. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes [2]. As MANETs are illustrated by limited bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes. The network is de-centralized and all the network activities like discover the topology and delivering messages must be execute by the nodes.

However, similar to other networks, MANET also vulnerable to many security attacks. MANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself [3]. In MANET, security is a challenging issue due to the vulnerabilities that are associated with it. When initiating a Route Discovery, the sending node saves a copy of the original packet in a local buffer called the Send Buffer. The proposed ACO uses the elitism technique to retain the best solution in each generation. Further, the rest of the chromosomes are replaced by using crossover and mutation operations [4].

2. DSDV Protocol

Destination sequenced distance vector routing (DSDV) is adjusted from the customary Routing Information Protocol (RIP) to ad hoc networks routing [5]. It includes another characteristic, sequencing number, to every route table passage of the routine RIP. Utilizing the recently included sequence number, the mobile hubs can recognize stale route data from the new and accordingly keep the arrangement of routing loops.

In DSDV, every mobile hub of adhoc network keeps up a routing table, which records every single accessible destination, the metric and next bounce to every destination and a sequence number produced by the destination hub. Utilizing such routing table put away as a part of every mobile hub, the packets are transmitted between the hubs of a specially adhoc network. Every hub of the adhoc system upgrades the routing table with ad intermittently or when huge new data is accessible to keep up the consistency of the routing table with the powerfully changing topology of the specially appointed system. Occasionally or quickly when system topology changes are recognized, every mobile hub promotes routing data utilizing television or multicasting a routing table update packet [6].

The update packet begins with a metric of one to direct joined hubs. This demonstrates that every accepting neighbor is one metric (jump) far from the
hub. It is unique in relation to that of the ordinary routing algorithms. Subsequent to accepting the redesign packet, the neighbors upgrade their routing table with augmenting the metric by one and retransmit the update table to the relating neighbors of each of them. The procedure will be rehashed until every one of the hubs in the adhoc network have gotten a duplicate of the update parcel with a comparing metric [7].

![Figure 1: Routing procedure in DSDV](image)

Here Node 4 transmits packet to next node

### 3. Ant Colony Optimization (Aco)

ACO algorithm is a new intelligent optimization algorithm implying the winged animal swarm practices, which was proposed by analyst Kennedy and Dr. Beernaert in 1995.

Assuming $X_i= (x_{i1}, x_{i2}...x_{iD})$ the position of $i$-th ANT COLONY in $D$-dimension, $V_i= (v_{i1}, v_{i2},...,v_{iD})$ is its velocity which represents its direction of searching [8]. In iteration process, each ANT COLONY keeps the best position $p$ best found by it, besides, it also knows the best positioning best searched by the group ANT COLONYs, and changes its velocity according two best positions. The standard formula of ACO is as follows:

$$v_{id}^{k+1} = w v_{id}^k + c_1 r_1 (p_{id}^k - x_{id}^k) + c_2 r_2 (p_{id}^k - x_{id}^k)$$  \hspace{1cm} (1)

$$x_{id}^{k+1} = x_{id}^k + v_{id}^{k+1}$$  \hspace{1cm} (2)

In which $i=1,2,...N,N$-the population of the group ANT COLONYs; $d=1,2,...D$; $k$-the maximum number of iteration; $r_1$-the random values between $[0,1]$, which are used to keep the diversity of the group ANT COLONYs; $c_1,c_2$; the learning coefficients, also are called acceleration coefficients; $v_{id}^k$-the number $d$ component of the position of ANT COLONY in $k$-the iterating; pad, the number $d$ component of the best position particles has ever found; pad, the number $d$ component of the best position the group ANT COLONYs have ever found [9].

The procedure of standard ACO is as following:

1) Initialize the original position and velocity of ant swarm.
2) calculate the fitness value of each ANT COLONY;
3) For each ANT COLONY, compare the fitness value with the fitness value of p best, if current value is better, then renew the position with current position, and update the fitness value simultaneously;
4) Determine the best ANT COLONY of group with the best fitness value, if the fitness value is better than the fitness value of g best, then update the g be stand its fitness value with the[8] position;
5) Check the finalizing criterion, if it has been satisfied, quit the iteration; otherwise, return to step 2.

### 3. BLACK HOLE ATTACK AGAINST MANET

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious 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 establish, now it’s up to the node whether to drop all the packets or forward it to the unknown address [10].

### 4. Proposed System

The whole implementation has been done using ACO in DSDV protocol.

1. Input No. of nodes by user
2. Input width
3. Input length
4. Step2 and 3 are called network deployment.
5. Evaluate X and Y axis location of the network.
6. Find source and destination.
7. Find coverage set of the network.
8. Plotting of source and destination.
9. Find routes to proceed.
10. Black hole nodes occur.
11. Detect black hole attack.
12. Evaluate parameters.
13. Degradation has been found = TRUE/NO
14. If no, then Stop.
15. If Yes, then
16. Call ACO in DSDV network.
17. Evaluate parameters.
18. Compare with and without optimization algorithm.

In proposed work firstly source and destination are found out. Then coverage set evaluation is being done. The node that receives the BACKWARD ANT packet first checks the value of sequence number in its routing table. The BACKWARD ANT packet is accepted if it has BACKWARDANT sequence number higher than the one in routing table. Our solution is by checking the performance of the network by using various parameters like Packet Loss, End Delay, Packet Delivery and Packet Overhead, if they are degraded it can be easily found out that packet dropping is done. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors. The ALARM packet has the black list node as a parameter so that, the neighboring nodes know that BACKWARD ANT packet from the node is to be discarded. Further, if any node receives the BACKWARD ANT packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. It simply ignores the node and does not receive reply from that node again. So, in this way, the malicious node is isolated from the network by the ALARM packet. ACO uses the following fitness function to optimize the network [11]:

\[ P_{FIT} = \text{Min} (\sqrt{A(x)^2 - B(x)^2}) \]

Where B is the energy at next node and A is the energy of first block.

The ACO optimizes the fitness function in following way:
1) calculate the fitness value of each ANT COLONY;
2) For each ANT COLONY, compare the fitness value with the fitness value of p best, if current value is better, then renew the position with current position, and update the fitness value simultaneously;
3) Determine the best ANT COLONY of group with the best fitness value, if the fitness value is better than the fitness value of g best, then update the g best and its fitness value with the position;
4) Check the finalizing criterion, if it has been satisfied, quit the iteration; otherwise, return to step 2.

In the end various parameters are evaluated like Packet Loss (The packet lost and received ratio is checked in the process of black hole detection and correction. This includes actual number of packet reaching the destination node), End Delay (Average End-to-End delay is the average time of the data packet to be successfully transmitted across a MANET from source to destination. It includes all possible delays such as buffering during the route discovery latency, queuing at the interface queue, retransmission delay at the MAC (Medium Access Control), the propagation and the transfer time), Packet Delivery (Total number of packets sent over given time) and Packet Overhead (Number of packets that get delayed due to slow routing or due to packet dropping in the network) when whole optimization has been done using ACO. To implement the results the whole simulation has been done in MATLAB 7.10 environment. From the results it has been concluded that the network performance and optimization using ACO approach which will help to increase the lifespan of the designed network. The packets transmitted this way are made to drop so as no unauthorized access is available to transmitted data [12].

4.1 Flowchart

Similar to other networks, MANET also vulnerable to many security attacks. MANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself known as black hole attack.
Below flowchart shows the network model for prevention of black hole attack.

**Figure 2**: Proposed Work Flowchart

### 4.2 Pseudo Code

- node_count=input
- net_length=input
- net_width=input
- calculate the xloc y loc and time_stamp of each nodes
- measure of x location distance
- measure of y location distance
- clear coverage_set
- check that whether destination is available or not
- Source Will Directly Send Data To Destination.

- selecting any node from the coverage set of the current node
- current_node=selected_node;
- route(route_length)=current_node;
- route_length=route_length+1;
- destination_path=destination_path+1;
- Black hole nodes detected
- Packet Loss
- End Delay
- Packet Delivery
- Packet Overhead
- Call Ant Colony Optimization
• best value so far
• initial position
• evaluating position & optimal solution
• fitness evaluation
• if new position is better
  Comparison graph with and without optimization

5. Implementation And Results

The whole implementation has been done in MATLAB 7.10. Below graphs shows th performance of various parameters using ACO or without ACO usage.

Figure 3: Data Transmission

Above figure shows the transmission of data from source to destination. The above DSDV network has been plotted with 1000 * 1000 length and width space. Here blue color is denoted for number of participant nodes in the network. Green color is denoted for path from source to destination and red color is denoted for black hole node where packet dropping is done.

5.1 Packet delivery ratio

The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

Figure 4: Packet delivery in DSDV using ACO or without ACO

Packet delivery ratio is the number of packets sent/number of packets given, over the network in given time. Above figure shows the packet delivery ratio value after compensation through ACO algorithm or without ACO in DSDV. It has been seen that value of packet delivery ratio is being enhanced in the figure using proposed algorithm.

5.2 Packet Loss

It is the total number of packets lost during transmission of data from source to destination.

Figure 5: Packet loss comparison in DSDV using ACO or without ACO

Above figure shows that the variation in mobility nodes gives zigzag packet loss in proposed and DSDV protocol whereas the incremental variation in nodes shows an increase in packet loss in both DSDV-ACO and DSDV protocols. This figure shows the losses of the packet from end to end transceiver. These are done with the help of five distinct malicious nodes. This figure shows that if only one
malicious node then there is less packet drop compared with the nodes.

5.3 End To End Delay

End to End Delay is the summation of Transmitting Delay (at MAC layer), Propagation Delay and queuing Time of a packet.

Figure 6: End delay in DSDV using ACO or without ACO

The End to End Delay is a significant parameter for evaluating a protocol which must be low for good performance. Proposed algorithm shows less end delay. This increase in delay is due to the additional nodes through which then passes to the destination node. However increase in the numbers of nodes also increases the difference of delay. From above graph it has been shown that end delay in proposed algorithm is less in comparison to absence of ACO protocol in DSDV.

6. Conclusion And Future Work

This work has designed a novel method to detect black hole attack: ACO, which isolates that malicious node from the DSDV network. We have implemented the proposed method on every node of the DSDV network. The method stores the target sequence number in the routing table. Firstly it finds the source and destination node. Then it finds out the routing of packets are in order and if performance is maintained or not. Now if performance is degraded then packet evaluation takes place. After that ACO is called using fitness function that optimizes the dropping of packet. Our solution makes the participating nodes realize that, one of their neighbors is malicious; the node thereafter is not allowed to participate in packet forwarding operation.

In the end various parameters are evaluated like Packet Loss, End Delay, Packet Delivery and Packet Overhead. To implement the results the whole simulation has been done in MATLAB 7.10 environment.

The future work will be based on the realization of the Sybil attack and black hole attack comparative study and can optimize the network with other algorithms like particle swarm optimization, bacterial foraging optimization.

References


9. Yuteng Guo, Beizeng Wang, Xingxing Zhao, Xiaobiao Xie, Lidalin and Qinda Zhou, “Feature Selection based on Rough Set and modified

