BLACK HOLE DETECTION AND PREVENTION IN AODV PROTOCOL USING MODIFIED CUCKOO SEARCH ALGORITHM

Moolchand sharma[1], Shubbham Gupta[1], Suman Deswal[2]
[1]Maharaja Agrasen Institute of Technology, Delhi, India
[2]Deenbandhu Chhotu Ram University of Science and Technology, Murthal, Sonipat, Haryana, India

Email: moolchand@mait.ac.in, shubbham.gupta28@gmail.com, sumandeswal.cse@dcrustm.org

Abstract

Mobile ad hoc network (MANET) is a network without centralized administration for sending data through multi-hop mobile nodes. Routing is the biggest challenge that happens due to the absence of rigid infrastructure in a MANET. The efficiency of routing protocol depends on the accuracy with which it sends data from source to destination. Routing protocol has a crucial role because of rapidly varying topology. In this paper, we've aimed to increase the efficiency of routing protocols using cuckoo search optimization. The technique is to be tested on NS2 simulator. Quality of Service (QoS) parameters like Delay, Throughput, Packet loss, and Packet delivery ratio is used for evaluating the performance of routing protocol and its optimization in this paper. It is seen that as nodes increase the mentioned method shows better results of 95.45% Packet Delivery Ratio

Keywords: Black Hole, Mobile Ad-hoc Network, Bio-Inspired Algorithms, Cuckoo Search Optimization

1. Introduction

Mobile Ad-hoc network is a network in which the communication happens in a remote medium utilizing an access point. In Mobile Ad-Hoc Networks (MANETs), all communication among nodes happen via wireless connections without any centralized control or rigid framework and can join or exit the network anytime. The MANET is useful in different scenarios like disaster relief operations, military, remote scene operations where are unfeasible, exclusive, not available [1]. Nodes are not familiarized with the surrounding topology of network in ad-hoc networks. They have to find the topology. A fresh node declares its existence and then searches for neighbor's broadcast announcement. Each node discovers other nodes and find a way to reach them and tell others node a way to reach those nodes. Each node then transmits the data willingly to other nodes[2][3]. Each node has its transmission range and communicates with nodes within its range. Routing overhead are reduced dramatically in Reactive routing protocols(AODV) as routes are not searched and maintained regularly when data traffic is not present[4]. High packet delivery time in excessive flooding and route searching are main difficulties which can lead to network congestion. MANET is more prone to attacks because of its variable infrastructure. Therefore, the security of the routing protocol is of most significance. In this project, our main focus is to secure MANET from black hole attack. Analysis and mitigation of black hole attack in AODV protocol is the main aim of this project.

Swarm Intelligence is the mutual behavior of self-organized, decentralized organisms, artificial or natural. Incentive of SI often derives from the surrounding, particularly biological systems. Swarm intelligence is a multi-agent system that has self-organized behavior that demonstrates extraordinary

Received: 10 May 2019/Accepted 08 July 2019.

intelligent behavior. Two phenomena results in Global cooperation. First phenomena is that every species is pre-programmed genetically to execute a particular set of tasksin given same stimuli set. Second phenomena is performing these procedures implicitly to modify their environment, creating new stimulation for themselves and those which are around them. Many routing algorithms for MANETs are developed from taking inspiration from Nature's different self-arranging systems, like termite hills, insect societies, bird flocks, bee colonies, and fish schools[5]. Among various swarm intelligence algorithm, this research paper uses Cuckoo Search Algorithm with aim to analyze and mitigate black hole threat in AODV protocol. The performance of research work has been calculated by different parameters, like, throughput, delay, packet loss, and PDR (Packet delivery ratio).

The major focus of this project is as follows:

- A modified Cuckoo Search Algorithm is created for routing purpose in MANET
- The modified algorithm is simulated along with ADOV routing protocol in ns2
- The result will be compared on a number of nodes and various number of black holes

2. Literature Review

Most common attack in MANET is Black hole attack and many researchers have developed different methods and algorithms to detect black hole and prevent the network from black hole and safely transmit data across the network. In this section, different methods are reviewed.

Al-Shurman et al. introduced an easy approach in Adhoc On-demand distance vector (AODV) protocol to prevent the black hole attack [6]. In this method, more than one route to the destination is discovered and the sequence number included in each packet header is manipulated. Suspicious replies are quickly recognized by this arrangement. This method also uses bandwidth efficiently as sequence number itself is incorporated in each packet in the base protocol thus no overhead will be added. However, group attacks are may be hard to find using this approach.

Sharma et al suggest an approach to guard against the wormhole attack [7]. To detect a wormhole attack in any network, the author uses digital signatures in the proposed arrangement. When a node needs to transmit a packet, it starts RREQ along with a unique digital signature. Each node in the network verifies the received digital signature with the signature saved in the database and if it matches, node approves that the RREQ comes from a genuine source. The corrupt node either does not have a signature or has one copied from another node while replaying RREQand subsequently is recognized and isolated from further transmission.

Raj et al exhibited Detection, Prevention and Reactive AODV (DPRAODV) to anticipate the security risk of the black hole by informing different nodes in the network[8][9]. The recreation results show that our protocol avoids black hole attack but also in the presence of a black hole attack, our protocol improves the general performance of (typical) AODV. However, it still has an issue with delay performance.

Sen et al presented a defense mechanism for managing black hole attack[10]. In this research, the black hole attack has been depicted and routing security issues in MANETs are examined. A new security protocol has bee introduced that can differentiate between black holes and general nodes thus found a protected routing path from the source node to the destination node without interfering any black node.

Sharma Shivanioptimize the path selection procedure in the MANET so that packets can

Received: 10 May 2019/Accepted 08 July 2019.

be delivered successfully in the network [11]. The proposed scheme starts with the normal broadcasting of the Forward Ants by the source node. This will be the same as route finding the behavior of the facts as described in ACO. The second is the route reply phase. When the forward ants reach the destination node, the destination would generate backward ants straight away, which would trace back the path to the source node. However, in the proposed scheme, the attractiveness of the links defined by the firefly algorithm will be taken into account. When the backward ants would reach the source node, the source node would sort out the paths in the order of highest pheromone value and highest attractiveness. The first path in the sorted order will be considered for data transmission while the other can be stored in the cache memory for the use in case any failure occurs in the first path.

S.Gayathri et al proposed a method to prevent black hole attack using Ant Colony Based Optimization with Elliptic Curve Digital Signature Algorithm based Secure Routing called ACO-ECDSA [12]. It initially find a route using route selection as a NP complete optimization problem using ACO-based algorithm. Then an optimal route is established via an opportunistic method rather than the blind flooding based on both local and global pheromone (based on the Quality of Service of routing paths), using both forward and backward ants. After route selection process, source nodes through dynamic intersection selections initiate data packets transmission.

2.1. Ad hoc On-Demand Distance Vector (AODV) Routing Protocol

Many issues are present which influence the performance of network such as, unnecessary use of the battery in nodes, bandwidth overhead, entry of unnecessary redundant route, etc[13]. Ad hoc On-Demand Distance Vector (AODV) routing protocol is thus one of the better protocol as it solves these issues too much extent. AODV is a synergetic protocol enables nodes to disperse the information regarding other nodes to each other [14]. It fixes broken links faster, provides loop free and quick convergence in case of the progressive network topology [15][16]. When source node requires a route only then, AODV assembles a route, made out of two primary tasks, Route Discovery and Route Maintenance. A routing table is kept for finding routes in the middle of the nodes. Route discovery function initialized by source node helps to find a new route. Data packets are kept in buffers during route discovery and then transmitted when the path is found. Route maintenance procedure keeps a route active as long as it is required by the network [17]. RREQ route request packets are sent by the source node to form a route to the destination, each time it needs to send data to the destination[18][19]. When the destination receives an RREQ, it sends an RREP reply to the source via the shortest path, then data is transmitted through this path. In this way, the routing tables are progressive when required. In any case, it looks exceptionallystraightforward, yet this sort of protocol endures several vulnerabilities of attack.

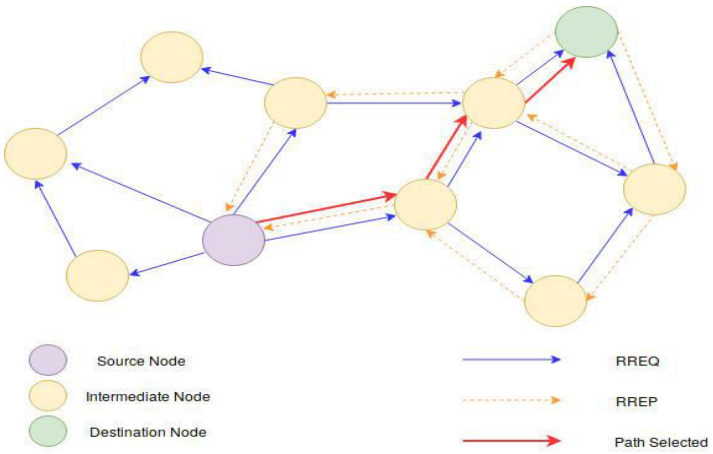


Fig 1. AODV Protocol

2.2. Cuckoo Search Algorithm

Received: 10 May 2019/Accepted 08 July 2019.

Cuckoo search algorithm is developed as a metaheuristic approach with an inspiration of bird cuckoo. This bird never makes its nest and usually lays the eggs in other bird‟s nest. Few host birds may engage straight with the intruding cuckoo[20][21]. If the host bird finds the eggs, which are, not even their egg than it throws the eggs from the nest or relieve its nest or make a new nest. In the nest, every egg shows a solution and cuckoo egg depicts a novel and better solution. The solution being obtained is a novel solution based on an existing solution with some amendments in the characteristics. Cuckoo search is utilized for solving the scheduling issues and for solving the design optimization issues in structural engineering. Cuckoo search admires the breeding behavior and may be developed for different optimization problems as mentioned below [22]:

i. Every cuckoo lays a single egg at one time and deposits it to an arbitrarily selected nest.

ii. The better nests having high egg quality would take to the subsequent generation.

Iii. There are a fixed number of accessible host nest and if a host bird finds the cuckoo egg having a probability of page[0,1] then the bird may throw or abandon them and generate a novel nest.

2.3. Black Hole

Due to the lack of fixed infrastructure, MANET is more prone to attacks. MANET security attacks are labeled as CONTROL and DATA attacks[23][24]. DATA traffic attacks deal with altering of data or losing it. These attacks can either in drop data or alter the sequence in which data is sent resulting in corrupt data. Some attacks are node specific i.e. it drops selected packets which are for specific victim nodes while some attacks drop every one of them affecting the whole network. CONTROL traffic attacks mainly hijack the routing tables or bypass valid routes thus disrupting the network. Some attacks include eavesdropping on the network while some include exchanging the original data corrupt data. Black Hole attack is a most basic DATA traffic attack which occurs in MANET, As the name suggests, a malicious node acts like a black hole and drops all data packets passing through it as like a black hole in the universe which consumes all matter and energy passing through it. If the attacking nodes act as the middle node between two components of a network, then it will make these two components as two separate networks.

A Black Hole Attack is executed by a combination of nodes or a single node known as selfish nodes. It attacks during the route discovery phase of the routing protocol. As soon as the attacking node receives RREQ packet, it will claim that it has the fastest route to the destination and send a response to source node before any node.[25] As AODV treats RREP replies having greater sequence number fresher, attacking node sends RREP having the highest sequence number. This will stop the route discovery phase and source will start sending data to the attacking node resulting in loss of data. As a result source node and destination node becomes inefficient to communicate, compromising the whole network eventually[26].

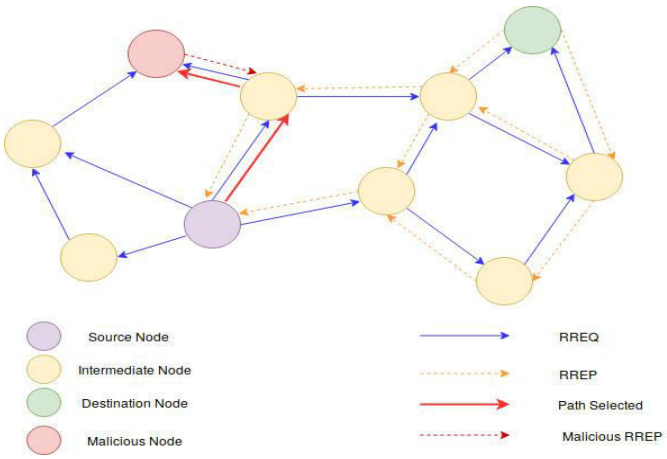


Fig 2. Black Hole Implementation

Received: 10 May 2019/Accepted 08 July 2019.

3. Proposed Methodology

In this research paper, Cuckoo Search Optimization is embedded into AODV protocol for better routing discovery. The proposed method is simulated in NS2 and results are calculated for a various number of nodes.

For the experiment minor modifications are made to basic cuckoo search for embedding purposes and for better working. As NS2 is compiled in C, cuckoo search is written in C and it is embedded in route discovery part. In general AODV, nodes with a higher sequence number and less hop count are selected. Using cuckoo search, these nodes are selected after multiple iterations ensuring the path efficiency. If efficiency is reduced new path is found in the next iteration. During black hole attack, when packets do not receive by destination cuckoo search drops the current path and finds a new path and mark the malicious nodes and restrict them from selecting them further in route discovery.
The algorithm used in the experiment is shown below:

Cuckoo search Algorithm

```
Begin
Objective function Gi
Produce initial population for n number of host nest equal to nodes
While (m<Max Generation) or (halt criteria)
        Obtain a cuckoo arbitrarily
        Execute its fitness Gi
        Decide a nest between n arbitrarily
                If (Gi<Gj)
                Change j with novel solution
                End if
A fraction of inferior nest is discarded and novel ones are developed
Keep the better solutions
Rank the solution and evaluate the solution and existing best
End while
        Post process results
End begin
```

For the project purpose, the basic flowchart which will be followed is presented below

Received: 10 May 2019/Accepted 08 July 2019.

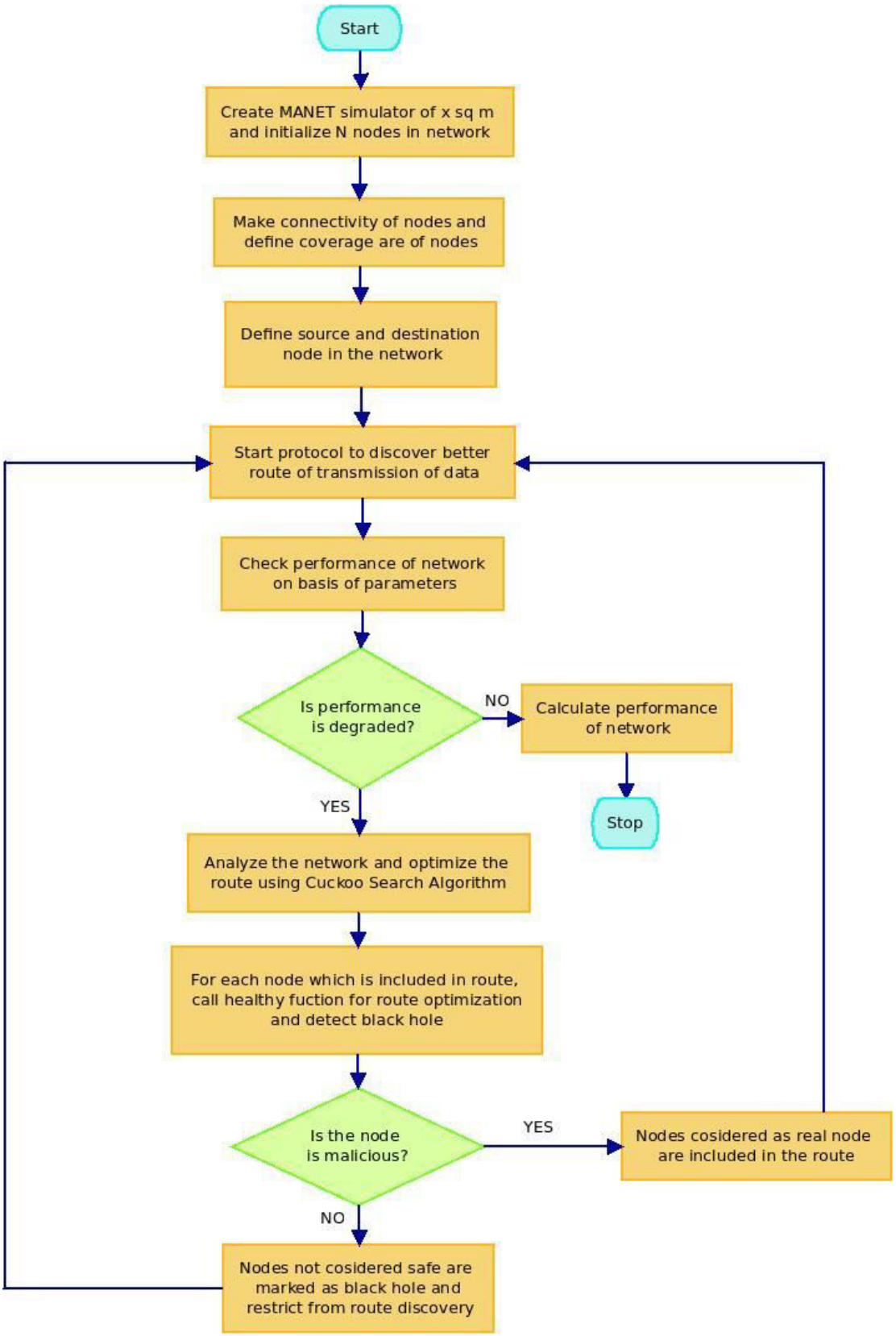


Fig 3. Flowchart

Received: 10 May 2019/Accepted 08 July 2019.

4. Implementation and Results

In this section, implementation of the proposed algorithm is done. The algorithm has been run multiple times with different numbers of nodes. The experiment has been executed multiple times to get better results.

4.1. Input Parameters

For efficient results number of nodes are varied sequentially from 20 nodes to 50 nodes. In each case number of black holes is also increased to maintain the node to blackhole ratio. To maintain a similar environment,a fixed amount of packets are sent over each case ie 490 packets and each simulation is run for a fixed 40 second period. Nodes are all placed in the XY plane.

Nodes	Blackholes
20	2
25	2
30	3
35	3
40	4
45	4
50	5

Table 1: Nodes and Blackhole

4.3. Calculating Paramenters

These QoS parameters are used to calculate performance of network:

- **Packet delivery ratio**: A ratio of data packets recieved by final node to those sent by source is known as Packet delivery ratio. In Mathematical terms, it can be written as:

$$PDR = P1 \div P2$$

Where, P2 is the total amount of packets sent by the every source and P1 is the total amount of packets received by the every destination.

- **End to End Delay**:Additional time required by packet to reach destination from source across a network is known as One-way delay (OWD) or End-to-end delay. It is the most used parameter to monitor IP network. It is different from round-trip time (RTT) as in OWD only one direction from source to destination is calculated.

- **Throughput**: Throughput is the rate with wich packets are succesfully transmitted over the network. It is usually represented as an average and calculated in data packets per second or in bits per second (bps). It is considered as a necessary indicator of the quality and performance of a network. Large amount of failed packets delivery will lead to lower throughput and reduced performance. Network throughput is affected by many factors. These involve features like physical hardware's processing power. Throughput can be affected by network congestion and packet loss

- **Packet Loss**: Packet loss is the count of number of packets which lost track of path and fails to reach their destination. Errors in data transmission, like network congestion, or across wireless networks is the main reason behind packet loss. In our project, main reson behind packet loss

Received: 10 May 2019/Accepted 08 July 2019.

is the existence ofblack holes in the network. Packet loss is calculated to show how much black hole will affect the network performance.

Packet loss is calculated addtionally because Packet Delivery ratio may not show us the proper amount of packet loss as it shows the ratio of total packets to lost packets

4.3. Results

The experiment has been performed in 7 different cases having different amount of nodes. The performance of each case is measured in respect of Throughput, End to End delay, Packet loss, and Packet delivery ratio.

In following figure Throughput of the network is shown. It can be seen throughput of the experiment is near the case where blackhole exists in simple AODV before the 35 nodes. After 35 nodes throughput of the experiment becomes almost equal to the case without any black hole in AODV.

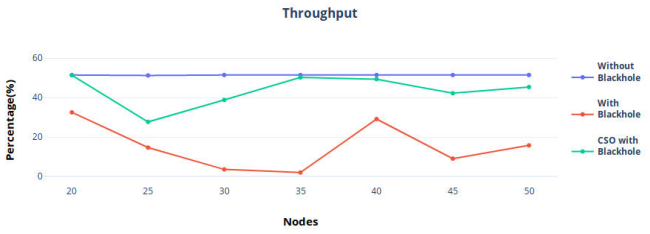
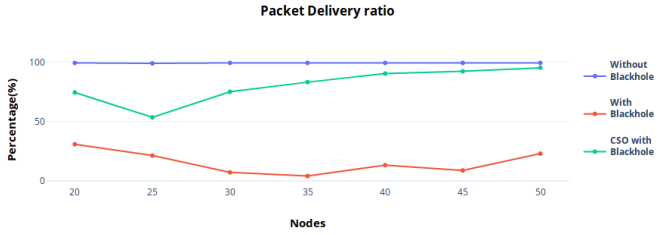


Fig 4. Throughput

In the following figures, Packet Delivery Ration and Packet loss is shown. The experiment has lost many packets when the number of nodes is less. But when the number of nodes increased, the packet loss is decreased eventually hence packet delivery ratio increased. It can be presumed that with more number of nodes packet delivery ratio will be equal to that of simple AODV without blackhole.



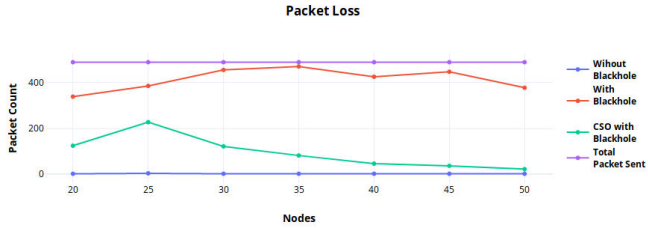


Fig 5. a) Packet Delivery Ratio b)Packet Loss

In the following figure, the end to end delay ratio is shown. It has shown mixed results as it on multiple factors. Initially, the delay is similar but as the number of nodes increased the end to end delay is been seen in the experiment and simple AODV as the new paths may include a number of nodes in the path which will result in a delay.

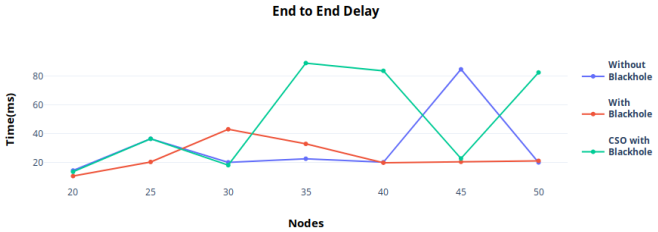


Fig 6. End to End Delay

5. Conclusion and Future Scope

This research has proposed an improvement in AODV routing protocol by embedding cuckoo search optimization into it. The improved algorithm has worked well against the black hole attack. We have compared the effects of black hole attack in respect of End to End Delay, Throughput, Packet delivery ratio, and Packet Loss in MANET and observed that improved algorithm has given better results in all ways. Proposed algorithm is implemented efficiently for the network and able to detect attack and prevent it. Along with detection it also improved the performance of the network effectively. It has been seen that the improvement has shown significant results as the number of nodes increased. Packet Delivery Ratio increased as number of nodes

Received: 10 May 2019/Accepted 08 July 2019.

are increased and it reaches 95.45% when 50 nodes are present in the network. The research also suggests that if the number of nodes will increase the improved routing protocol will work as efficiently as simple AODV protocol will work without blackhole.

In future, this protocol along with some modification may be used to secure AODV protocol against more security threats like white hole attack, jellyfish attacks and more.

References

1. Gomathi K, Parvathavarthini B. An enhanced distributed weighted clustering routing protocol for key management. Indian Journal of Science and Technology. Feb 2015; 8(4):342–8.
2. Raju B, Gulfishan A. Different approaches on cooperation in wireless ad hoc networks. International Journal of Computer Applications. 2011 Aug; 28(3):36–41.
3. Martin H, Deniele P. Routing in ad hoc networks: A case for long Hops. IEEE Communications Magazine; 2005. p. 93–101.
4. Vera K. Security in ad hoc networks. Seminar on Network Security; 2000. p. 1–16.
5. Abdel-Monien AM, Hedar A. An Ant Colony Optimization algorithm for the Mobile Ad hoc network Routing problem based on AODV protocol. 10th International Conference on Intelligent Systems Design and Application; 2010. p. 1332– 7.
6. *Al-Shurman, Mohammad, Seong-Moo YooandSeungjin Park, "Black hole attack in mobile ad hoc networks," Proceedings of the 42nd annual Southeast regional conference. ACM, 2004*
7. *Pallavi Sharma and Aditya Trivedi, "An Approach to Defend against Wormhole Attack in Ad Hoc Network Using Digital Signature," IEEE 3rd International Conference on Communication Software and Networks (ICCSN), Pp.307-311, 2011.*
8. *Raj, N.Payal and Prashant B. Swadas, "Dpraodv: A dynamic learning system against blackhole attack in aodv based manet," arXiv preprint arXiv:0909.2371, 2009.*
9. *C.V. Anchugam and K. Thangadurai, "Detection of Black Hole Attack in Mobile Ad-hoc Networks using Ant Colony Optimization simulation Analysis", Indian Journal of Science and Technology, Vol 8(13), DOI: 10.17485/ijst/2015/v8i13/58200, July 2015*
10. *Sen, Jaydip, SripadKoilakondaandArijitUkil, "A mechanism for detection of cooperative black hole attack in mobile ad-hoc networks," IEEE. Second International Conference on Intelligent Systems, Modelling, and Simulation (ISMS),2011.*
11. *Sharma Shivani, " Bio-Inspired Technique to Improve the Performance of VANETS", International Journal of Advanced Research, Ideas and Innovations in Technology.*
12. *S.Gayathri, S.Nithya, G.Shanthini, R.Janani, R.Ramachandiran, M. Shanmugam ,T. Kalaipriyan, RS. Raghav, G. Siva Nageswara Rao, " ACO- ECDSA BASED SECURE ROUTING IN VANET: A BIO-INSPIRED APPROACH", International Journal of Pure and Applied Mathematics Volume 119 No. 14 2018, 395-406*
13. *Thangadurai K, Anchugam CV. Simulation based performance comparison of various Routing Protocols in MANET using Network*

Received: 10 May 2019/Accepted 08 July 2019.

Simulation Tool. International Journal of Advanced Networking Applications. 2013 Apr; 4(5):1744–51.

14. *Devid C, Alessandro G. Securing AODV: The A-SAODV Secure Routing Prototype. IEEE Communication Magazine. 2008. p. 120–5.*
15. *Chanchal A. Black hole attack in AODV Routing Protocol: A review. International Journal of Advance Research in Computer Science and Software Engineering. 2013 Apr; 3(4):820–3.*
16. *Anuj KG, Harsh S, Anil KV. Performance Analysis of AODV, DSR and TORA routing protocols. IACSIT International Journal of Engineering and Technology. 2010 Apr; 2(2):226–31.*
17. *Govind S, Manish GA. Black hole detection in MANET using AODV routing protocol. International Journal of Soft Computing and Engineering. 2012 Jan; 1(6):297–303.*
18. *Anuj KG, Harsh S, Anil KV. Performance Analysis of AODV, DSR and TORA routing protocols. IACSIT International Journal of Engineering and Technology. 2010 Apr; 2(2):226–31.*
19. *Sun B, Guan Y, Chen J, Pooch UW. Detecting Black hole Attack in Mobile ad hoc Networks. 5th European Personal Mobile Communications Conference; 2003 Apr; Glasgow, United Kingdom.*
20. *N. Schweitzer, A. Stulman, A. Shabtai and R. D. Margalit, "Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes," in IEEE Transactions on Mobile Computing, vol. 15, no. 1, pp. 163-172, Jan. 1 2016.*
21. *J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao and C. F. Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," in IEEE Systems Journal, vol. 9, no. 1, pp. 65-75, March 2015.*
22. *J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao and C. F. Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," in IEEE Systems Journal, vol. 9, no. 1, pp. 65-75, March 2015.*
23. *Bhattacharyya, Aniruddha, Arnab Banerjee, Dipayan Bose, HimadriNathSaha and Debika Bhattacharyya. "Different types of attacks in Mobile ADHOC Network." CoRR abs/1111.4090 (2011): n. Pag.*
24. *L. Tamilselvan and V. Sankaranarayanan, "Prevention of Blackhole Attack in MANET," The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), Sydney, NSW, 2007, pp. 21-21.*
25. *Satoshi K, Hidehisa N Nei K, Abbas J, Yoshiaki N. Detecting black hole attack on AODV based Mobile ad hoc networks by Dynamic Learning Method. International Journal of Network Security. 2007; 5(3):338–46.*
26. *Thangadurai K, Anchugam V. Fuzzy cost based multipath Routing protocol in MANETs. IEEE World Congress on Computing and Communication Technologies; 2014. p. 286–90. DOI: 10.1109/WCCCT.2014.11.*

Received: 10 May 2019/Accepted 08 July 2019.