Indian Journal of Science and Technology, Vol 8(13), DOI: 10.17485/ijst/2015/v8i13/58200, July 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Detection of Black Hole Attack in Mobile Ad-hoc Networks using Ant Colony Optimization – simulation Analysis

C.V. Anchugam* and K. Thangadurai

P.G. and Research Department of Computer Science, Government Arts College (Autonomous), Karur - 639005, Tamil Nadu, India; anchugam.mca@gmail.com, ktramprasad04@yahoo.com

Abstract

Background: Security in Mobile Ad hoc Networks (MANETs) is an essential component for basic network function. Black hole attack may cause packet dropping, misrouting the information from source to destination. **Methods:** Biology-inspired techniques like as Ant Colony Optimization (ACO) is used to modify the Ad-hoc On Demand Distance Vector (AODV) routing protocol. The ant place of at each node calculates its pheromone value by using the forwarding ratio at node. This modified protocol is compared with existing protocol by using various parameters i.e. packet delivery ratio, end-to-end delay and throughput. **Results:** The results shows to increase in packet delivery ratio, throughput and decrease in end-to end delay show better performance of proposed work as compared existing.

Keywords: ACO, Black Hole Attack, Challenges, MANETs, Security

1. Introduction

In Mobile Ad-hoc Networks (MANETs), all nodes are mobile and can enter and leave the network at any time. They communicate with each other via wireless connections. All nodes are equal and there is neither centralized control nor fixed infrastructure to rely on. The mobile nodes can be enter and leave the network at any time[35]. The Mobile Ad hoc Network has many applications such as military, disaster relief applications, mini site operations where infrastructure are not available, unfeasible, or exclusive[32]. There are no designated routers: all nodes can serve as routers for each other and data packets are forwarded from node to node in a multi-hop fashion.

In ad hoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it: typically, a new node announces its presence and listens for announcements broadcast by its neighbors. Each node learns about others nearby and how to reach them and may announce that it too can reach them. After that each node forwards data to other nodes willingly. Each node communicates with other nodes within its transmission ranges[1,2]. There are two scenarios of ad hoc networking; they are very different from each other in many ways:

- The mobile devices need to work only in a safe and friendly environment where the networking conditions are predictable[3,4]. Thus no special security requirements are needed.
- The devices operate in an extremely hostile and demanding environment, in which the protection of the communication and availability and operation the network both very vulnerable without strong protection[4,5].

Reactive routing protocols can dramatically reduce routing overhead because they do not need to search for and maintain the routes on which there is no data traffic[6]. The main difficulties are high latency time in route finding and excessive flooding can lead to network clogging[10]. Single path routing is based on single route establishment between source and destination. In this

*Author for correspondence

routing, the packet is transmitted to the destination using a single route[7]. Multipath routing gives the choice to the source to choose the path between source and destination by taking advantage of the connectivity redundancy of the underlined network[8]. Routing tables can be statically assigned or dynamically built and updated. In static routing systems, the path to forward traffic between pairs of nodes is determined without regard to the current network state. Once defined the paths to be used for each source and destination pair, data are always forwarded along these paths. In dynamic (or adaptive) routing system, the routing tables are dynamically updated according to the current traffic events and topological modifications (e.g. Link/Node failures, Link/Node addition/removal).

Swarm Intelligence (SI) is the collective behavior of decentralized, self organized systems, natural or artificial. The expression was introduced by Gerardo Beni and Jing Wang in 1989, in the content of cellular robotic systems[9]. The inspiration often comes from nature especially biological systems. Principle of SI is a multi agent system that has self organized behavior that shows some intelligent behavior. Bonabeau[11] provide the following definition of swarm intelligence: "Swarm Intelligence (SI) is the properly of a system whereby the collective behavior of (unsophisticated) agent interacting locally with their environment cause coherent functional global patterns to emerge".

Nature's self-organizing systems, such as insect societies, termite hills, bee colonies, bird flocks and fish schools, provide precisely these features and hence have been a source of inspiration for the design of many routing algorithms for MANETs[12]. Out of all the techniques inspired by the behavior of social insects, Ant Colony Optimization (ACO) algorithms have evolved as a promising solution for efficient routing in MANETs. In recent years models of collective intelligence of ants have been transformed into useful optimization and control algorithms. For last many years, ant based algorithms have captivated the researchers for solving routing problem in MANETs. Many algorithms have been proposed by researchers in last few years and many more are in pipeline.

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

Several problems on the network[13] such as bandwidth overhead, wastage of battery power of the nodes, entry of unnecessary redundant route etc. Due to these complexities, Ad hoc On Demand Distance Vector (AODV) routing protocol is number one. AODV is a collaborative protocol[14] and allow nodes to distribute the information they hold about other nodes. It provides loop free routes, repair broken links[15] and quick convergence in case of the dynamic network topology[16]. AODV builds routes only when desired by source node[17], composed of two main processes, Route Discovery and Route Maintenance.

The route in between the nodes is discovered by the entries in routing table[34]. A route is acquired by the initiation of a route discovery function by the source node. The data packets transmitted as a route finding is in process are buffered and are sent when the path is established. An established route is maintained as long as it is required during a route maintenance procedure[18]. Every time source node wants to send a data to the destination, it seeks to establish the path through numerous techniques by sending several route request packets. When destination sends a reply for route request to the source during shortest path, the source send data through this path. So, the routing tables are dynamically when needed. However it glances very simple, but this kind of protocol endures several vulnerabilities of assault.

Figure 1 shows the message exchanges of the AODV protocol. In general, the nodes participating in the communication can be classified as source node, neighbor node and destination node. Hello messages may be used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that its entire neighbor receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected.

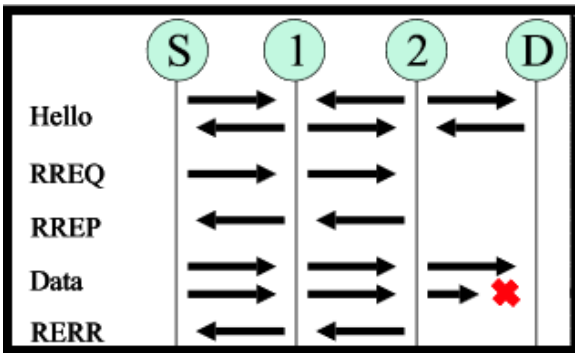

Figure 1. AODV Architecture

In AODV, there are three types of control messages: Route Request (RREQ), Route Reply (RREP), Route Error (RERR) messages. Figure 2, Figure 3 and Figure 4 are the packet format of RREQ, RREP and RERR respectively.

Route Request (RREQ) Message: When a source node want to send a data packets to destination it generate RREQ packet and flood it in the whole network route discovery.

Route Reply (RREP) Message: When the destination receives RREQ, it generates the RREP packet and unicast it to the source node.

Route Error (RERR) Message: When a link break is detected in any active route RERR message is generated.

Each node in the network can get to identify its neighboring node by using periodic HELLO message[19]. HELLO messages are used to inform the neighboring node that the link is still alive and never be forwarded[20].

Source IP Address
RREQ ID
Source Sequence Number
Destination IP Address
Destination Sequence Number
Originator IP Address
Originator Sequence Address
Hop Count

Figure 2. Route Request (RREQ).

Source IP Address
Destination IP Address
Destination Sequence Number
Originator IP Address
Hop Count
Life Time

Figure 3. Route Reply (RREP).

Source IP Address
Unreachable Destination IP Address
Unreachable Destination Sequence Number
Additional Unreachable Destination IP Address
Additional Unreachable Destination Sequence Number
Destination Count

Figure 4. Route Error (RERR).

Destination IP Address
Destination Sequence Number
Hop Count
Next Hop
First Hop
Valid Bit
Count

Figure 5. Fields of AODV Routing Table.

An important feature of AODV is the maintenance of timer based states in each node, regarding utilization of individual routing table entries. Route error propagation in AODV can be visualized conceptually as a tree whose root is the node at the point of failure and all sources using the failed link as the leaves[21].

3. Ant Colony Optimization (ACO)

Nature-inspired meta-heuristics algorithms are flattering popular and powerful in solving optimization problems. Ant Colony Optimization is one of the finest algorithms for path finding[23]. They develop their inspiration from the real world behavior of ants and the method they use for finding food. ACO is based on the indirect communication of a colony of simple agents, called artificial ants, when an ant moves along a path; it deposits a chemical called pheromone on it. As more and more ants move along the same path, the pheromone concentration of the path increases. The path with the maximum pheromone concentration is then chosen to be the optimal path.

A combinatorial optimization problem can be represented as a tuple P = (S, F), where S is the solution space with $s \in S$ a specific candidate solution and $F: S \rightarrow R_+$ is a fitness function assigning positive values to candidate's solution. The goal of the algorithm is find a solution s*, or set of solution S*, $s^* \in S^* \subseteq S$ the increase the fitness function. Here, the s* is called optimal solution and S* is called the set of optimal solutions[22].

ACO features a multi-agent organization, stigmergic communication among the agents, distributed operations, and use of stochastic decision policy to construct solutions, stigmergic learning of the parameters of the decision policy. The ACO algorithm is basically interplay of three procedures: 1. AntBasedSolution Construction, 2. Pheromone Updation and 3. Daemon Actions, as represented by algorithm as shown in Figure 6. The schedule

Algorithm 1: ACO Metaheuristic

1. Input: An instance I of a combinatorial problem p
2. Initialize Pheromone values(Γ)
3. WHILE termination condition not met do
   Schedule Activities
   $S_{iter} \leftarrow \varphi$
   for j = 1, ……n_a do
   S ← AntBasedSolution Construction (Γ)
   S ← LocalSearch (S)
   $S_{iter} = S_{iter} \cup \{S\}$
   end for
   Pheromone Updation (Γ)
   DaemonActions ( ) {optional}
   END Schedule Activities
   END WHILE
4. Output: Best solution found

Figure 6. Ant Colony Optimization Algorithm.

activities construct does not specify how these three activities are scheduled and synchronized. The designer is therefore free to specify the way these three procedures should interact.

The *AntBasedSolution Construction ( )* procedure performs probability of choosing the next sub solution of *i*, which is defined as follows:

$$P_{ij}^{k} = \begin{cases} \dfrac{\left[\Gamma_{ij}\right]^{\alpha}\left[\eta_{ij}\right]^{\beta}}{\sum_{j \in N_i^k}\left[\Gamma_{ij}\right]^{\alpha}\left[\eta_{ij}\right]^{\beta}} & if\ \ j \in N_i^k \\ P_{ij}^{k} = 0, & otherwise \end{cases}$$

Where N_i^k, is the set of feasible sub-solution that can be next sub-solution of *i;* Γ_{ij} the pheromone value between the sub-solution of *i* and *j*; and η_{ij} the quality of the sub-solution *j* that will affect each ant's determination to move to *j* when at *i*. The parameter α and β are used to adjust the weight of exploration and exploitation.

The *Pheromone Updation ( )* procedure is employed in updating the pheromone value Γ_{ij} on each edge, which is defined as follows:

$$\Gamma_{ij} = (1-\rho)\Gamma_{ij} + \rho \sum_{k=1}^{m} \Delta\Gamma_{ij}^{k}; \qquad \Delta\Gamma_{ij}^{k} = {}^{1}\!/_{L^k}\ \rho \in (0,1)$$

Where m denotes the number of ants, L^k the quality of solution created by ant k, ρ denotes the evaporation rate of pheromone value on the pheromone table. The *LocalSearch ( )* procedure is improving the quality of the solution of ACO.

3.1 Simple Ant Colony Optimization Metaheuristic Algorithm

Let us consider $G = (V,E)$ be a connected graph with $n = |V|$ nodes. The ant system can be used to find the shortest path between a source node v_s to destination node v_d on the graph G. The path length is given by the number of nodes on the link. Each edge $e(i,j) \in E$ of the graph connecting the nodes v_i and v_j has a variable $\varphi_{i,j}$ (artificial pheromone), which modified by an ants when they visit the node. The pheromone concentration $\varphi_{i,j}$ is an indication of the usage of this edge. An ant located in node v_i uses pheromone $\varphi_{i,j}$ of node $v_j \in N_i$ to compute probability of node v_j as next hop. N_i is the set of one-step neighbors of node v_i.

$$P_{i,j} = \begin{cases} \dfrac{\phi_{i,j}}{\sum_{j \in N_i}\phi_{i,j}} & if\ \ j \in N_i \\ 0 & if\ \ j \notin N_i \end{cases}$$

The transition probabilities $P_{i,j}$ of a node v_i fulfill the constraint

$$\sum_{j \in N_i} P_{i,j} = 1, \quad i \in [1,N]$$

During the route finding process, ants deposit pheromone on the edges. In the simple ant colony optimization meta-heuristics algorithm, the ants deposit a constant amount $\Delta\varphi$ of pheromone. An ant changes the amount of pheromone of the edge $e(v_i, v_j)$ when moving from node v_i to node v_j as follows:

$$\varphi_{i,j} = \varphi_{i,j} + \Delta\varphi$$

Like real pheromone the artificial pheromone concentration decreases with time to inhibit a fast convergence of pheromone on the edges. In the simple ant colony optimization meta-heuristics, this happen exponentially:

$$\phi_{i,j} = (1-q) \cdot \phi_{i,j}, \quad q \in (0,1)$$

3.2 Ant Colony Based Routing Algorithm (ARA)

Ant Colony Based Routing Algorithm (ARA) works on the principle of reactive technique in an on demand way for MANETs. The main goal of ARA is to reduce the

overhead for routing. It is highly adaptive, efficient and scalable. It does not use any HELLO message to explicitly find its neighbors. When a packet arrives at a node, the node checks it to see if routing information is available for destination in its routing table. Route discovery and route maintenance are the phases of ARA. The sender broadcasts a forward ant in the route discovery phase and the ant is relayed by each intermediate node until it reaches the destination.

Ant agents can be divided into two sections: Forward ANT (FANT) and Backward ANT (BANT). It is used to create a new routing path. FANT agent is responsible for establishing the pheromone path to the source node and BANT agent is responsible for establishing the pheromone path to the destination node. During the journey of FANT from source to destination, when the FANT is received at the intermediate nodes for the very first time, the recipient node getting a FANT for the very first time builds a record of three parameters i.e., destination address, next hop, pheromone value in its routing table.

At this time, when the FANT reaches at the destination node, it is processed in a special manner. The destination node extracts the information from the FANT and then destroys the FANT. After that a BANT is created at the destination node and sent towards the source node on the reverse path that was followed b the FANT. In this manner, the route is established between source and destination and data packets can be sent.

As shown in Figure 7. The source node creates a forward ant (FANT) and sends the forward ant intended to route discovery to its neighbor nodes. Using probabilistic decision it decides the next hop node and forward the forward ant through all the next hop nodes until it reaches the destination.

As shown in Figure 8. The destination node creates a backward ant (BANT) and sends the backward ant in the same route traces made by the forward ant through the intermediate nodes until it reaches the source node.

ARA fulfills the requirements of distributed operation, loop-freeness, on demand operation and sleep period operation. (i.e., nodes are able to sleep when their amount of pheromone reaches a threshold). The expected overhead of ARA is very small, because there is no routing table information between two nodes. Unlike other routing algorithm, the forward and backward ants do not transmit much routing information. Only a unique sequence number is transmitted in the routing packets. Most route maintenance is performed through data packets, thus they do not have to transmit additional routing information.

4. Problem Description (Black Hole Attack Against AODV)

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. Attack can occur when the malicious node present in the network is intended to attack directly the data traffic and intentionally drops, delay or alter the data traffic passing through it[24]. Black Hole Attack is very dangerous active attacks on the MANETs. It is formed during the week routing infrastructure, when a malicious node joins the network this problem arises. In detection system for ad hoc networks are extremely difficult due to lack of central controller, bandwidth limitations, and dynamic topology in mobile ad hoc networks[33].

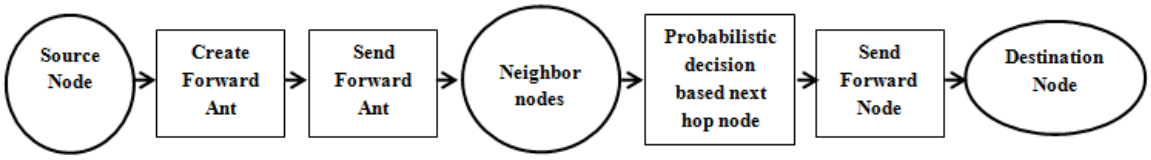

Figure 7. Transmission of FANT in ARA.

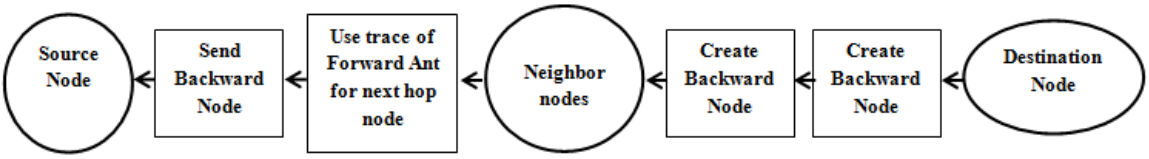

Figure 8. Transmission of BANT in ARA.

A Black Hole Attack is performed by a single node or combination of nodes, also called selfish node. The method how malicious node fits in the data routes varies. Figure 9 shows how black hole problem arises, here node "S" wants to send data packets to node "D" and initiate the route discovery process. So if node "3" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "S" before any other node. In this way node "S" will think that this is the active route and thus active route discovery is complete. Node "S" will ignore all other replies and will start sending data packets to node "3". In this way all the data packet will be lost consumed or lost.

As a corollary, the source and the destination nodes became inefficient to communicate with each other. While AODV treats RREP messages having higher sequence number to be fresher, the malicious node all the time send the RREP having higher sequence number[25]. So RREP message, once received by source node is treated anew, too. The outcome is that there is a high probability of a malicious node effort to organize the black hole attack in AODV. Black hole attack problem in MANETs could be very serious security problem to be resolved[31].

5. Existing System

In this section, we review different methods for the detection of black hole attack in AODV based mobile ad hoc networks.

Cauvery N.K. et al.[26] proposed an efficient algorithm that uses swarm intelligence to produce all feasible paths between a source and a destination node in a MANETs. In this algorithm, routing of data packets are made only passing through the finest path created by route discovery

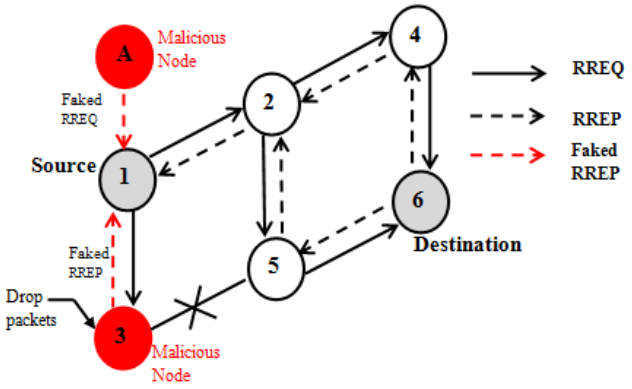

Figure 9. Black hole attack problem.

phase of the Ant colony based Routing Algorithm (ARA). Route maintenance is periodically done to maintain the finest path using data packets. Due to the dynamic topology of ad hoc networks, existing routes may fail or new paths may be created. Therefore, route refreshing is done periodically, when topology is changing.

Raj et al.[27] discusses a protocol viz. DPRAODV (Detection, Prevention and Reactive AODV) to counter the black hole attack. It checks whether the RREP_Seq_no is higher than the threshold value. The threshold value is dynamically updated in every time interval. If RREP_Seq_no is higher than threshold value, the node is malicious node and added to black listed nodes. Finally, send an ALARM message to neighbor nodes about black listed nodes. Thus the neighbor nodes know that malicious node and if any message come from malicious node automatically discarded the message. In the simulation results, the packet delivery ratio improved by up to 85% than normal AODV.

Sowmya et al.[28] proposed some changes in ant colony optimization. In this algorithm provided a finest path efficiently since it is fully distributed and so, there is no single point of failure, moreover it is very easy to perform the operations on all the nodes. Detect and prevent black hole attack used threshold value and it is added with the ACO algorithm. It is based on asynchronous and independent interaction of agents. Separate these malicious nodes from the data forwarding time with help of the alarm message to all its neighboring nodes.

Sarita Choudhary et al.[29] provides an efficient approach for the detection of blackhole and Gray hole attack in Mobile Ad hoc Networks based on the AODV routing protocol. In this approach 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.

M. Umaparvathi et al.[30] proposed algorithm is called as TTSAODV protocol to identify single and collaborative

black hole attack in mobile ad hoc networks. This protocol proves the trueness of the RREP message through the verification messages sent by neighboring nodes. The basic assumption in this solution is that there is a strong symmetric key distribution system in the MANET. Thus, every pair of nodes in the network has unique common secret key. In the proposed protocol, two levels of security are provided. One level is during the route discovery process and the next is during the data transfer. Even if the detection of Black hole attack fails at the route discovers process, in the next level, it will be identified. So, the proposed protocol has high degree of attack detection and prevention.

More than resolutions for black hole attack discussed above involve supplementary overhead on either/both intermediate and destination nodes in anyway. Because the mobile nodes in ad hoc networks suffer from limited battery life, processing power and storage, it is necessary to devise a protocol with the intention of to reducing the overhead on neighboring and destination nodes. In addition, the process of selecting secure root, should involve minimum possible augment in end-to-end delay.

6. Proposed System

In this previous section, existing algorithm detect the black hole attack. ARA and AODV are evaluated by so many authors and identified ARA is always better than AODV. In this section, we have proposed AODV is modified to detect and prevent black hole attack by using ant colony algorithm such as ARA. Pheromone updates play a significant role in the performance of the ant algorithm. In ARA algorithm, initial pheromone value is calculated by number nodes during the route discovery process. The working principles of the algorithm are given below:

1. Establish a network with N number of nodes.
2. Specify the properties of network.
3. Define the source and the destination node over the network.
4. Place the ant at each node in the network.
5. Define the m malicious nodes over the network.
6. Route discovery process: Source node broadcast the RREQ message to neighboring nodes using FANT forward technique and hop count is initialized. It is an agent to establish pheromone value to the source node.
7. Collecting replies:
   - Collecting the neighboring nodes information stored in routing table.
   - Neighboring nodes receive the request then it will check whether the node is destination or not.

   If yes then
   FANT is sent to only that neighbor
   else
   it's forwarded to all the neighbors.
   A node is receiving a FANT for the first time, will create a record in its routing table and fields such as destination address, next hop and pheromone value.
8. For each FANT (currently in node i)
   Do
   - Choose the neighbor node, probability value will be high that route/neighbor needs to be considered.
   - Add that node pheromone value to neighboring pheromone table with the node, pheromone value between these nodes until the ant has reached the destination.

   End
9. The full process is mention above to get repeated until the Forward Ant (FANT) reaches the destination node.
10. When FANT destroy, it is reaches to the destination and create Backward Ant (BANT) send to along the path to the source node. It is an agent that establishes the pheromone value to the destination.
11. Route maintenance: Once FANT and BANT have established route path between source to destinations and data packets are send along the same path. The pheromone track value is strengthened means path is shortest path between these two nodes.

7. Assumptions

The complete methodology is based upon the following assumption to evaluate the network performance with and without the effect of malicious node at distributed levels.

- Malicious node does not acknowledge with data packet in the network.
- Black hole node will receive the packet but instead of forwarding the packet it will drop all the received to lower the packet delivery ratio and network efficiency.

8. Implementation and Results

The proposed methodology is compared with the existing algorithm of safe route method based upon the ant colony based routing algorithm on the basis of throughput, packet delivery ratio, end-to-end delay and so on. The performance and results of the routing algorithm as below:

8.1 Throughput

The throughput is the number of bytes transmitted or received per second. The throughput is denoted by T,
Throughput = received node/simulation time

$$T = \frac{\sum_{i=1}^{n} N_i^r}{\sum_{i=1}^{n} N_i^s} \times 100\%$$

Where, N^r= average receiving node for the i^{th} application, N^s = average sending node for the i^{th} application, and n = number of applications. In Figure 10 shows that the proposed algorithm improved good throughput compared to AODV with black hole attack.

8.2 Packet Delivery Ratio

It can be measured as the ratio of the received packets by the destination nodes to the packets sent by the source node.

PDR = (number of received packets / number of sent packets) * 100

$$T = \frac{\sum_{i=1}^{n} (N_i^s - N_i^r)}{\sum_{i=1}^{n} N_i^s} \times 100\%$$

Where, N^s, N^r node sent by the sender and the number of application data node received by the receiver, respectively for the i^{th} application, and n is the number of applications. In Figure 11 shows that packet delivery ratio of the proposed algorithm is more than AODV routing algorithm with black hole attacks. Black hole stimulate packet dropping, the original AODV decreases packet delivery ratio with increase in number of nodes.

8.3 End-to-End Delay

It represents the time required to move the packet from the source node to the destination node.

E-2-E delay [packet_ id] = received time [packet_ id]– sent time [packet_ id]

The average end-to-end delay can be calculated by summing the times taken by all received packets divided by its total numbers.

$$D = \frac{\sum_{i=1}^{n} d_i}{n}$$

Where, d_i = average end to end delay of node of i^{th} application and n = number of application. In Figure 12 shows that the proposed algorithm provided minimum end-to-end delay compared with original AODV with black hole attack.

8.4 Dropped Packets

It represents the number of packets that sent by the source node and fail to reach to the destination node.
Dropped packets = sent packets– received packets.

$$T = \sum_{i=1}^{n} (N_i^s - N_i^r) - \sum_{i=1}^{n} N_i^s$$

Where, N^s , N^r node sent by the sender and the number of application data node received by the receiver, respectively

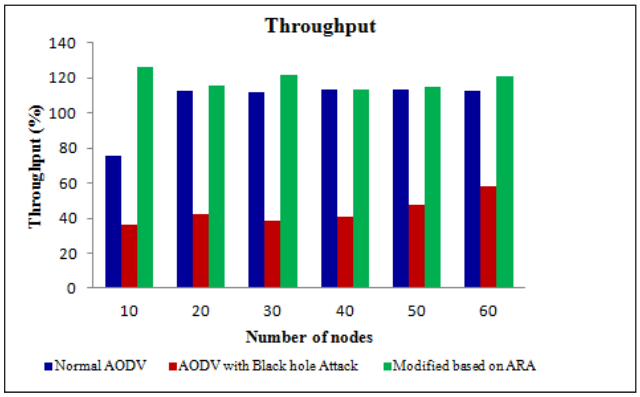

Figure 10. Throughput.

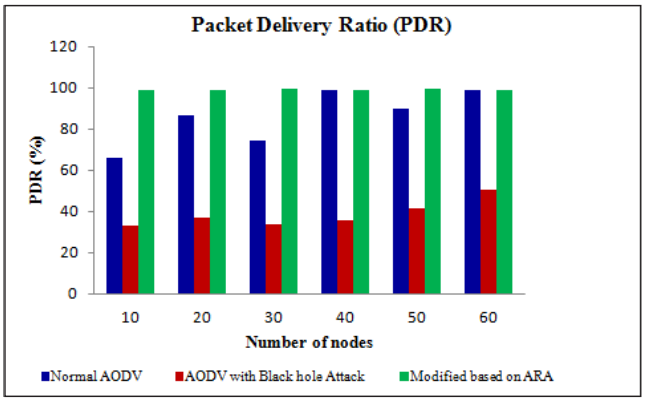

Figure 11. Packet Delivery Ratio (PDR).

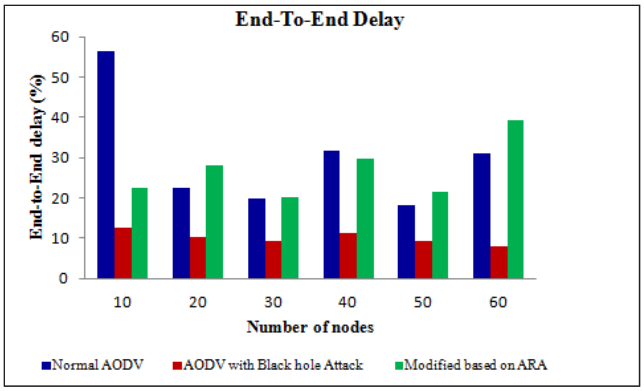

Figure 12. End-To-End Delay.

for the i^{th} application, and n is the number of applications. In this proposed system, get better performance to deliver the data packets. It easy to analysis packet dropped rate in the routing process.

9. Conclusion and Future Work

In this section, the paper summarized for study about Mobile Ad Hoc Networks; we initiate that most repeated attack is a black hole in MANETs. To discover a resolution for that various algorithms are available. But to decide security and performance issues some improvements on the routing technique is implemented. We are analyzed the effects of black hole attack in the light of network load, throughput and end-to-end delay in MANETs and simulating the black hole attack using reactive routing protocols (e.g. AODV). Compared and observed that AODV without attack gives better result in all situations. After observing the results it is found that under attack case system has more packet drop ratio it is always greater to threshold. Design and implement a security algorithm for detection of black hole attack based on Ad hoc On-Demand Distance Vector routing protocol and Ant Colony Algorithm.

Implementation of proposed method is quite efficient for network and able to detect attack. In addition, the performance of the network is improved effectively. The summary of performance is packet delivery ratio, end-to-end delay and throughput can be improved. The proposed protocol can able to improve two main problems such as security and performance, into one place, but this concept is able to detect only one attack and effective for black hole. In future a framework for security is required, where more than one attack are handled.

10. References

1. Gary B. Wireless ad hoc networks: Basic concepts. High Frequency Electronics. 2007; 6(3):44–6.
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. Haiyunluo Z, Jiejun K, Songwu L, Lixia Z. Self securing ad hoc wireless networks. 17th IEEE Symposium on Computers and Communications; 2002. p. 1–17.
6. Singla V, Kakkar P. Traffic pattern based performance comparison of reactive and proactive protocols of mobile ad hoc networks. Journal of Computer Application. 2010; 5(10):16–20.
7. Abolhasan M, Wysocki T, Dutkiewicz E. A review of routing protocols for Mobile Ad hoc Network. Journal of Ad hoc Networks. 2004; 2(1):1–22.
8. Di Caro GA. Two Ant Colony Algorithms for best-effort routing in datagram networks. 10th International Conference on Parallel Distribution Computer System; 1998. p. 28–31.
9. Beni G, Wang J. Swarm intelligence in cellular robotic systems. Proceedings of NATO Advanced Workshop on Robots and Biological Systems; 1989 Jun 26-30; Tuscanty, Italy.
10. Available from: http://en.wikipedia.org/wiki/List_of-ad_hoc_routing_protocols
11. Available from: http://en.wikipedia.org/wiki/swarm_intelligence
12. 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.
13. Thangadurai K, Anchugam CV. Simulation based performance comparison of various Routing Protocols in MANET using Network 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. 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.
18. 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.
19. Nisarg G, Rahila P. Performance evaluation of AODV protocol in MANET using NS2 simulator. 2nd National Conference on Information and Communication Technology (NCICT); 2011.
20. Hilmani Y, Rakesh K. A review of black hole attack in MANET. International Journal of Engineering Research and Applications. 2010 Jun; 2(3):1126–31.
21. Shweta M, Jitendra P. Performance comparison of IACO, AODV Networking Routing Protocols. International Journal of Smart Sensors and Ad Hoc Networks. 2011; 1(1):33–7.
22. 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.
23. Anchugam CV, Thangadurai K. A nature inspired ant colony based routing protocol for MANETs. Journal of Computer Science and Application. 2014; 6(1):123–30.
24. Pearlman MR, Haas Z. Determining the optimal configuration for the zone routing protocol. IEEE Journal on Selected Areas in Communications. 1999 Aug; 17(8):1395–414.
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. Cauvery NK, Viswanatha KV. Enhanced ant colony based algorithm for routing in mobile ad hoc network. World Academy of Science, Engineering and Technology. 2008; 2(10):26–31.
27. Raj PN, Swadas PB. DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET. International Journal of Computer Science Issues. 2009; 2:54–9.
28. Sowmya KS, Rakesh T, Hudedagaddi DP. Detection and prevention of blackhole attack in MANET using ACO. International Journal of Computer Science and Network Security. 2012 May; 12(5):21–4.
29. Sarita C, Kriti S. Discovering a secure path in MANET by avoiding black holes. International Journal of Recent Technology and Engineering. 2012 Aug; 1(3):88–93.
30. Umaparvathi M, Varughese DK. Two tier secure AODV against black hole attack in MANETs. European Journal of Scientific Research. 2012; 72(3):369–82.
31. Anchugam CV, Thangadurai K. Detection approach for black hole attack on AODV in MANETs using Fuzzy Logic System. International Journal of Advanced Information Science and Technology. 2015 Jan; 33(33):33–40.
32. Amir KA, Sahoo G. Behavior based high performance protocol for MANET. Indian Journal of Science and Technology. 2013 Oct; 6(10):5342–50.
33. Reza A, Marjan KR, Ehsan K. Black hole attack detection by invalid IP address in Mobile ad hoc Networks. Indian Journal of Science and Technology. 2014 Apr; 7(4):401–8.
34. Haripriya Y, Pavani KVB, Lavanya S, Visuwanatham VM. A framework for detecting malicious nodes in mobile ad-hoc network. Indian Journal of Science and Technology. 2015 Jan; 8(S2):151–5.
35. 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.