Simulation Based Performance Comparison Of Various Routing Protocols In MANET Using Network Simulation Tool

Dr.K.Thangadurai, Asst. Professor,  
P.G. and Research Department of Computer Science,  
Government Arts College (Autonomous), Karur, India.  
Email:ktramprasad04@yahoo.com

C.V.Anchugam, Research Scholar,  
P.G. and Research Department of Computer Science,  
Government Arts College (Autonomous), Karur, India.  
Email: anchugam.mca@gmail.com

ABSTRACT
A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a network temporarily without any centralized administration of the mobile networks. Each node in MANET moves arbitrarily making the multi-hop network topology to change randomly at unpredictable times. Two nodes in such a network can communicate in a bidirectional manner if and only if the distance between them is at most the minimum of their transmission ranges. When a node wants to communicate with a node outside its transmission range, a multi-hop routing strategy is used which involves some intermediate nodes? Because of the movements of nodes, there is a constant possibility of topology change in MANET. There are several familiar routing protocols like DSDV, AODV, DSR, etc., Which have been proposed for providing communication among all the nodes in the network? This paper presents a performance comparison of proactive and reactive protocols AODV, DSDV and DSR based on metrics such as throughput, packet delivery ratio and average end-to-end delay by using the NS-2 simulator.

Key words: MANET, DSDV, DSR, AODV, throughput, packet delivery ratio and average end-to-end delay.

Date of Submission:23, January 2013  Date of Acceptance: 10, March 2013

1. INTRODUCTION
A network can be characterized as wired or wireless. Wireless can be distinguished from wired as no physical connectivity between nodes is needed. Routing is an activity or a function that connects a call from origin to destination in telecommunication networks and also plays an important role in architecture, design and operation of networks. Ever increasing days, Mobile ad hoc network is becoming the latest thrust era for researchers. MANET (Mobile Ad Hoc NETworks) is an independent system [1] and also collection of various cooperative mobile terminals. In present scenario, there are currently two variations of mobile wireless networks [2,3]. The first kind is known as the infrastructure networks or Base Stations. This network communicates with the nearest base station which lies within the range. Typical applications of this type of network include office Wireless Local Area Networks (WLANs) [4]. The second type of wireless network is called as infrastructure less mobile network, commonly known as an Ad hoc Network. Due to no stationary infrastructure, all nodes can move freely, topology may change rapidly and unpredictably over time, and nodes have to form their own mutual infrastructures. To find a path between two hosts using routing protocol is a very herculean task due to their highly dynamic topology, absence of centralized administration [1].

MANET is wide network so different node may communicate over the same limited bandwidth. So there may be the problem of congestion, so to cover such problem appropriate routing is required to be done. The routing protocol is structured for purposes such as fully distributed, adaptive frequent and stable topology, loop free and minimum number of collisions.

MANET routing protocols are traditionally divided into three categories which are Proactive Routing Protocols, Reactive Routing Protocols, Hybrid. The most popular routing protocols [5,6] in MANET are AODV (reactive) [7,8], DSR (reactive) [9], DSDV [10] (proactive) and GRP (hybrid) [10]. Reactive protocols find the routes when they are needed. Proactive protocols are table driven protocols and find routes before they need it. And finally hybrid routing protocols offer an efficient framework that can simultaneously draw on the strengths of proactive and reactive routing protocols.
We consider three parameters to evaluate the performance of these routing protocols: Throughput, Packet delivery ratio and Average end-to-end delay by using the NS-2 simulator. The rest of this paper is organized as follows. In section 2 we briefly describe the routing protocols that we evaluate. In Section 3 presents the Simulation environment used for evaluation of the said protocols. In Section 4 we present our simulation results. Finally, section 5 concludes the paper.

2. ROUTING PROTOCOLS IN MANETS

In this section, a brief overview of the routing operations performed by the familiar protocols AODV, DSDV and DSR are discussed.

2.1. Ad Hoc On-demand Distance Vector Routing (AODV) protocol:

The Ad Hoc On-demand Distance Vector Routing (AODV) protocol [11, 12] is a reactive unicast routing protocol that means to maintain the routing information about the active paths. Routing information is maintained in routing tables at nodes and every mobile node keeps a next-hop routing table, which contains the destinations to which it currently has a route. When the nodes need to send data to the destination, if the source node doesn’t have routing information in its table, route discovery process begins to find the routes from source to destination. In AODV, when a source node S wants to send packets to the destination node D but no route is available, it initiates a route discovery operation. In the route discovery operation, the source broadcasts route request (RREQ) packets. A RREQ includes addresses of the source node S and the destination node D, the broadcast ID, which is used as its identifier, the last seen sequence number (Seq. no) of the destination as well as the source node’s sequence number (Seq. no). Sequence numbers (Seq. no) are used for remove the duplicate route and provides loop-free, up-to-date routes. Discovery operation reduce the flooding overhead, a node discards RREQ. The main feature of AODV is quick response to link breakage in active route. AODV [13, 14] builds routes using a route request and route reply query cycle. For destination source nodes with no prior information it broadcasts a route request (RREQ) packet. Nodes receiving RREQ update their information and set-up backward pointers to the source node. When the source node receives the RREP it begins to forward data packets to the destination. Another important feature of AODV is the maintenance of timer based states in each node, regarding utilization of individual routing table entries. A routing table entry is expired if not used recently. The advantage of this protocol is low Connection setup delay and the disadvantage is more number of control overheads due to many route reply messages for single route request.

2.1.1. Critiques of AODV

AODV is an on demand approach but still use periodic broadcast of “hello!” message to track neighboring nodes. This propagation causes network overhead in AODV [15]. In AODV a route has to discover the actual data packet transmission. This initial search latency may degrade the performance of interactive applications [15]. The quality of path must be monitored by all intermediate nodes in an active session at the cost of additional latency and overhead penalty [15]. In AODV is not suitable for real life applications. AODV cannot utilize routes with asymmetric links between nodes and thus require symmetric links [15]. Nodes in AODV store only route that are needed. Nodes use the routing caches to reply to route queries. The result is “uncontrolled replies and repetitive updates in hosts”.

2.2. Destination-Sequenced Distance-Vector (DSDV) protocol:

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm that was used successfully in many dynamic packet switched networks [16]. The Bellman-Ford method provided a means of calculating the shortest paths from source to destination nodes, if the metrics (distance-vectors) to each link are known. It eliminates route looping, increases convergence speed, and reduces control message overhead.

DSDV maintains consistent network view via periodic routing updates. Routing information is stored inside routing tables maintained by each node. New route broadcasts contain the address of the destination, the number of hops to reach destination, the sequence number of the destination and a new sequence number unique to broadcast. In DSDV, each node is required to transmit a sequence number, which is periodically increased by two and transmitted along with any other routing update messages to all neighboring nodes. On reception of these update messages; the neighboring nodes use the following algorithm to decide whether to ignore the update or to make the necessary changes to its routing table:

Step 1: Receive the update message
Step 2: Update the routing table if any one of the following condition satisfies:
   i) Sn > Sp
   ii) Sn=Sp, Hop count is less
Otherwise, ignore the update message.

Here, Sn and Sp are the Sequence numbers of new message and existing message respectively. When a path becomes invalid, due to movement of nodes, the node that detected the broken link is required to inform the source, which simply erases the old path and searches for a new one for sending data. The advantages are latency for route discovery is low and loop-free path is guaranteed. The disadvantage is the huge volume of control messages.

2.2.1. Critiques of DSDV

DSDV requires nodes to periodically transmit routing table updates packets regardless of the network traffic [15]. When the number of nodes in the network grows the size of the routing tables and the bandwidth required to update them also grows [15]. This is considered as the main weakness of
Dynamic source routing protocol [17] is a reactive protocol. 2.3. Dynamic Source Routing (DSR) Threat for the entire network. It has a high degree of complexity especially during link failure [15]. Maximum settling time is difficult to determine in DSDV. DSDV does not support multi-path routing. Fluctuation is another problem of DSDV. In some simulation studies, DSDV is much more conservative in terms of routing overhead but because link breakages are not detected quickly more data packets are dropped. Specification of DSDV is silent over security issue [15]. DSDV assumes that all nodes are trustworthy and cooperative. Once the false sequence has been established the attacker will continuously send out new packets to update the value. Therefore more hosts will be cheated [15] as a single misbehaving node can pose a serious threat for the entire network.

2.3. Dynamic Source Routing (DSR)
Dynamic source routing protocol [17] is a reactive protocol. DSR requires no periodic updates of any kind at any level within the network. DSR uses source routing through which sender knows the complete hop-by-hop route to the destination. These routes are stored in a route cache. A data packet carries the source route in the packet header. There are two major phases in DSR such as: Route discovery and Route maintenance.

When a source node wants to send a packet, it first consults its route cache [18]. The source node initiates a route discovery process by broadcasting route request packets. Receiving a route request packet, a node checks its route cache. If the node doesn’t have routing information for the requested destination, it appends its own address to the route record field of the route request packet. Then, the request packet is forwarded to its neighbors.

If the route request packet reaches the destination or an intermediate node has routing information to the destination, a route reply packet is generated. When the route reply packet is generated by the destination, it comprises addresses of nodes that have been traversed by the route request packet. Otherwise, the route reply packet comprises the addresses of nodes the route request packet has traversed concatenated with the route in the intermediate node’s route cache.

Whenever the data link layer detects a link disconnection, a ROUTE_ERROR packet is sent backward to the source in order to maintain the route information. After receiving the ROUTE_ERROR packet, the source node initiates another route discovery operation. Additionally, all routes containing the broken link should be removed from the route caches of the immediate nodes when the ROUTE_ERROR packet is transmitted to the source. The advantage of this protocol is reduction of route discovery control overheads with the use of route cache and the disadvantage is the increasing size of packet header with route length due to source routing. 2.3.1. Critiques of DSR
DSR is not designed to track topology changes occurring at a high rate [15]. Two sources of bandwidth overhead in DSR are route discovery and route maintenance [15]. These occur when new routes need to be discovered or when the network topology changes. In DSR this overhead can be reduced by employing intelligent caching techniques in each node at the expense of memory and CPU resources. The remaining source of bandwidth overhead is the required source route header included in every packet. This overhead cannot be reduced by techniques outlined in the protocol specification [15].

DSR is based on source routing thus requires considerably greater routing information. In DSR a route has to discover prior to the actual data packet transmission. This initial search latency may degrade the performance of interactive applications [15]. Moreover, the quality of path is not known prior to call setup. It can be discovered only while setting up the path. This quality of path needs monitoring by all intermediate nodes during a session. It increases the cost of additional latency and overhead penalty [15].

Due to source routing DSR has major scalability problem. Nodes use routing caches to reply to route queries. This results in an “uncontrolled” replies and repetitive updates in hosts caches. In addition, early queries cannot stop the propagation of all query messages which are flooded all over the network. Therefore when the network becomes larger, the control packets and message packets also become larger. This could degrade the protocol performance after a certain amount of time.

A comparison of the characteristics of the three ad hoc routing protocols AODV, DSDV, DSR is given in following Table 1.

<table>
<thead>
<tr>
<th>Property</th>
<th>AODV</th>
<th>DSDV</th>
<th>DSR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loop free</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multicast Routes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Distributed</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Unidirectional Link support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Multicast</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Periodic Broadcast</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>QoS support</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Routes maintained in</td>
<td>Route Table</td>
<td>Route Table</td>
<td>Route Cache</td>
</tr>
<tr>
<td>Route Cache / Table Timer</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Reactive</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 1: Property Comparison of AODV, DSDV and DSR
3. SIMULATION ENVIRONMENT
The simulation study is to analyze the performance of AODV, DSDV and DSR routing protocols in Wireless MANET Networks environment. The simulations have been performed using Network Simulator 2 version 2.34, a software that provides scalable simulations of Wireless Networks and an open source software. In our simulation, we consider a network of 5 nodes (one source and one destination) that are placed randomly within a 500m X 500m area and operating over 280 seconds. Multiple runs with different node speed and number of nodes are conducted for each scenario and collected data is averaged over those runs. To evaluate the performance of routing protocols, both qualitative and quantitative metrics are needed. Most of the routing protocols ensure the qualitative metrics. Therefore, we use different quantitative metrics to compare the performance. They are

**Throughput**: Ratio of the packets delivered to the total number of packets sent.

**Packet Delivery Ratio**: Packet Delivery Ratio in this simulation is defined as the ratio between the number of packets sent by CBR sinks at destination and the number of packets received by CBR sources. It describes the percentage of packets, which reach the destination.

**Minimum Delay**: Minimum Time taken for the packets to reach the next node.

**Maximum Delay**: Maximum Time taken for the packets to reach the next node.

**Average End-to-End Delay**: Time taken for the packets to reach the destination.

**Simulation Time**: The time for which simulations will be run i.e. time between the starting of simulation and when the simulation ends.

**Network size**: It determines the number of nodes and size of area that nodes are moving within. Network size basically determines the connectivity. Fewer nodes in the same area mean fewer neighbors to send request to, but also smaller probability of collision.

**Number of nodes**: This is constant during the simulation. We used 5 nodes for simulations.

### Table 2: Comparison Table of Throughput

<table>
<thead>
<tr>
<th>Pause Time (Sec)</th>
<th>DSDV</th>
<th>AODV</th>
<th>DSR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50N</td>
<td>75N</td>
<td>100N</td>
</tr>
<tr>
<td></td>
<td>50N</td>
<td>75N</td>
<td>100N</td>
</tr>
<tr>
<td>20</td>
<td>314333</td>
<td>304192</td>
<td>173867</td>
</tr>
<tr>
<td>40</td>
<td>326862</td>
<td>315232</td>
<td>903909</td>
</tr>
<tr>
<td>60</td>
<td>230399</td>
<td>207078</td>
<td>575215</td>
</tr>
<tr>
<td>80</td>
<td>290288</td>
<td>242423</td>
<td>127322</td>
</tr>
<tr>
<td>100</td>
<td>278990</td>
<td>260093</td>
<td>168829</td>
</tr>
</tbody>
</table>

4. PERFORMANCE RESULTS OF AODV, DSDV, DSR

4.1. Throughput:
It is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet. When comparing the routing throughput by each of the protocols, DSR has the highest throughput. It measures the effectiveness of a routing protocol. He throughput values of DSDV, AODV and DSR Protocols for 50, 75 and 100 Nodes at Pause time 20s, 40s, 60s, 80s and 100s are noted in Table-2 and they are plotted on the different scales to best show the effects of varying throughput of the above routing protocols (Fig. 2,3 & 4). Based on the simulation results, the throughput value of DSDV increases initially and reduces when the time increases. The throughput value of AODV slowly increases initially and maintains its value when the time increases. AODV performs well than DSDV since AODV is an on-demand protocol. The throughput value of DSR increases at lower pause time and grows as the time increases. Hence, DSR shows better performance with respect to throughput among these three protocols.
4.2. Packet Delivery Ratio:

Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. A high packet delivery ratio is desired in any network.

The ratio of the Originated applications’ data packets of each protocol which was able to deliver at varying time are shown in Fig. 5, 6 & 7 as per Table 3. As packet delivery ratio shows both the completeness and correctness of the routing protocol and also measure of efficiency the Table 3.

<table>
<thead>
<tr>
<th>Pause Time (Sec)</th>
<th>Protocol</th>
<th>DSDV</th>
<th>AODV</th>
<th>DSR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50N</td>
<td>75N</td>
<td>100N</td>
<td>50N</td>
</tr>
</tbody>
</table>

Table 3: Comparison Table of Packet Delivery Ratio
PDR value of AODV is higher than all other protocols. The PDR values of DSR and AODV are higher than that of DSDV. The PDR value of DSDV is worse in lower pause time and gradually grows in higher pause time. From the above study, in view of packet delivery ratio, reliability of AODV and DSR protocols is greater than DSDV protocol.

4.3. Average End-to-End delay:
The packet End-to-End delay is the average time that a packet takes to traverse the network. This is the time from the generation of the packet in the sender up to its reception at the destination’s application layer and it is measured in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges.

Various applications require different levels of packet delay. Delay sensitive applications such as voice require a low average delay in the network whereas other applications such as FTP may be tolerant to delays up to a certain level. MANETs are characterized by node mobility, packet retransmissions due to weak signal strengths between nodes, and connection tearing and making. These cause the delay in the network to increase. The End-to-End delay is therefore a measure of how well a routing protocol adapts to the various constraints in the network and represents the reliability of the routing protocol.

The Fig. 8, 9 & 10 depict the average End-to-End delay for the DSDV, AODV and DSR protocols for the number of nodes 50, 75 & 100 respectively as per Table 4. It is clear that DSDV

<table>
<thead>
<tr>
<th>Pause Time (Sec)</th>
<th>Protocol</th>
<th>DSDV</th>
<th>AODV</th>
<th>DSR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50N</td>
<td>75N</td>
<td>100N</td>
<td>50N</td>
</tr>
<tr>
<td>20</td>
<td>0.1209</td>
<td>0.12271</td>
<td>0.32939</td>
<td>0.16027</td>
</tr>
<tr>
<td>40</td>
<td>0.08996</td>
<td>0.11878</td>
<td>0.12486</td>
<td>0.17764</td>
</tr>
<tr>
<td>60</td>
<td>0.09036</td>
<td>0.11678</td>
<td>0.16708</td>
<td>0.19782</td>
</tr>
<tr>
<td>80</td>
<td>0.13211</td>
<td>0.14668</td>
<td>0.24473</td>
<td>0.20944</td>
</tr>
<tr>
<td>100</td>
<td>0.13813</td>
<td>0.15047</td>
<td>0.23451</td>
<td>0.21646</td>
</tr>
</tbody>
</table>

Table 4: Comparison Table of Average End To End Delay
5. CONCLUSION

In this paper, the performance of the three MANET Routing protocols such as DSDV, AODV and DSR was analyzed using NS-2 Simulator. We have done comprehensive simulation results of Average End-to-End delay, throughput, and packet delivery ratio over the routing protocols DSDV, DSR and AODV by varying network size, simulation time.

DSDV is a proactive routing protocol and suitable for limited number of nodes with low mobility due to the storage of routing information in the routing table at each node.

Comparing DSR with DSDV and AODV protocol, byte overhead in each packet will increase whenever network topology changes since DSR protocol uses source routing and route cache. Hence, DSR is preferable for moderate traffic with moderate mobility. As AODV routing protocol needs to find route by on demand, End-to-End delay will be higher than other protocols. DSDV produces low end-to-end delay compared to other protocols. When the network load is low, AODV performs better in case of packet delivery ratio but it performs badly in terms of average End-to-End delay and throughput.

DSR and AODV reached approx 100% packet delivery ratio when pause time equal to 200 while DSDV obtained only approx 94% packet delivery ratio. DSR and DSDV has low and stable routing overhead as comparison to AODV that varies a lot. Avg. End to End delay of DSDV is very high for pause time 0 but it starts decreasing as pause time increases.

DSR performs well as having low end to end delay. When we compare the three protocols in the analyzed scenario we found that overall performance of DSR is better than other two routing protocols.

6. ACKNOWLEDGEMENT

We would like to thank Guide in Government Arts College (Autonomous), Karur, Tamil Nadu, India and We would like to extend my sincere thanks to the Principal, HOD and faculty members of P.G and Research Department of Computer Science, Research Scholar, Government Arts College (Autonomous), Karur for their encouragement to publish this paper.

7. REFERENCES


Authors Biography

Dr.K.Thangadurai, is presently working as Assistant professor in research and PG Department of Computer science, Government Arts College (Autonomous), Karur. He has Fourteen years of rich teaching experience with Ten years of Research experience in the field of Computer Science. He has worked as the HoD of PG Department of Computer Science at Government Arts College (Autonomous), karur. He has published technical papers in many National and International Conferences and Journals. His areas of interest are Software Engineering, Network Security, Data Mining, etc.,

C.V.Anchugam is presently doing Ph.D in P.G. and Research Department of Computer Science, at Government Arts College (Autonomous), Karur, Tamilnadu, India. She has received her B.Sc(Computer Science) degree from Sri Saradha College of Arts and Science, Karur, Tamilnadu, India in 2002. She has received her MCA degree from M.Kumarasamy College of Engineering, Karur, Tamilnadu, India in 2005.She has published number of papers in esteemed national/international conferences and journals. Her interests are in Cryptography, Network security and Ad hoc networks.
Fuzzy Cost Based Multipath Routing Protocol for MANETs

Dr. K. Thangadurai, Asst. Professor,
P.G. and Research Department of
Computer Science,
Government Arts College (Autonomous),
Kuruk, India.
Email: ktramprasad04@yahoo.com

C. V. Anchugam, Research Scholar,
P.G. and Research Department of
Computer Science,
Government Arts College (Autonomous),
Kuruk, India.
Email: anchugam.mca@gmail.com

Abstract—Routing is a challenging issue in MANET due
to node mobility, unstable links and limited resources.
Swarm Intelligence (SI), as demonstrated by social
behavior of ant based on self organization, which allows
exploiting to coordinate population of artificial ants
the
collaborative to solve computational problems. However
already existing SI based routing protocols find a
optimal path by considering one or two route selection
metrics, such as time delay or node count. Conventional
routing algorithm found to be unsuitable for routing
multimedia traffic or real time applications which
requires optimization of several qualities of service
parameters. They are not considering correlations
among multiple route selection parameters. In the
proposal a approach called fuzzy ant colony based
routing protocol using fuzzy logic and SI of different
objectives while retaining the merits of swarm based
intelligence algorithm. Simulation results show that
great improvement for existing SI based routing
protocols for routing in MANET.

Keywords— MANET; SI; ACO; Fuzzy Logic

I. INTRODUCTION

In the past few years, researchers focus on
improving the performance of the different routing
protocols in MANETs. The Internet Engineering
Task Force (IETF) [1] to arrange number of peoples
to deal with major problems to the complexity of
designing routing protocols. These protocols are
classified into based on the time when routing
information is updated, the proactive routing
protocol, and reactive routing protocol. The
combination of both is called hybrid routing protocol
converged to most of the researchers [3]. The main
goal of all these protocols is to find reliable and
flexible path.

Swarm Intelligence (SI) means “The
emergent collective intelligence of groups of simple
agents” (Bonabeau et al., 1999). SI introduced by
G. Beni and U. Wang in 1989. It is a form collective
intelligence in swarms. The characteristics of SI are
flexibility, robustness and self organization [7]. The
principles of SI are self organization and Stigmergy
stimulation.

It is mostly based on amplification by
positive feedback, balancing by negative feedback,
amplification of random fluctuations, and multiple
interactions and behavioral responsible to the
environment state [8].

II. LITERATURE SURVEY

Ad Hoc network is a dynamically rearrange
wireless network with no fixed infrastructure. The
characteristics are dynamic topology, low channel
bandwidth, high node mobility and limited battery
power [4]. The protocol controls how nodes decide
which way to route packets between computing
devices in a MANET [5]. The proactive protocols
maintains new list of destination and their routes by
continually spread routing tables throughout the
network. An example is Destination Sequence
Distance Vector Routing (DSDV), Optimized Links
State Routing (OLSR) [9, 2]. The drawbacks of these
algorithms are maintaining group of data and slow
reaction on modifying and failures.

The reactive protocol used to find a route on
demand by flooding the network with RRP (Route
Request Packets). An example is Ad-hoc On Demand
Distance Vector Routing Protocol (AODV) and
Dynamic Source Routing (DSR) [10, 2]. The
drawbacks of these algorithms are high latency time
in route finding and reasonable flooding to the
network clogging. Hybrid is combination of both
proactive and reactive protocols. The protocols use
distance-vector for determine the best paths source to
destination and when there is any changes in the
topology of the network routing information can be
reported [6, 11]. An example is Zone Routing
Protocol (ZRP) and Sharp Hybrid Adaptive Routing
Protocol (SHARP). The drawbacks of these type of
algorithms are advantage is depends on other nodes
activated and reaction to traffic demand, it’s depends
on gradient of traffic volume.

To conquer this limitation, an approach to
gain such feature is to use a biological inspired
mechanism is known as swarm intelligence. It means
solving problem that takes inspiration from the social
behavior of insects and some other animals. ACO is
the most popular swarm intelligence techniques,
because ants have inspired a number of methods and
techniques [12].
A. Ant colony optimization routing algorithm

Ant Colony Optimization meta-heuristic takes inspiration from various foraging behavior of different ants. The method is solving hard combinatorial optimization problems [13]. The meta-heuristic is a multi-agent framework. The main components are: a set of ant like agent, the use of memory and of stochastic decisions and strategies of collective and distributed. The ants are find shortest path between nest and food source using evaporate chemical is called phenomone. It is an indirect form of communication. An individual agent leave signals in the environment and other agents sense them to drive their own behavior. The strength of phenomone deposit directs the artificial ants toward the best paths and phenomone evaporation allows the system to forget old information and avoid quick convergence to suboptimal solutions. The probabilistic selection paths allow the artificial ants search for a large number of solutions [14, 15]. Ant agents can be divided into two sections: FANT (Forward ANT) and BANT (Backward ANT). Routing algorithms can be used to set multipath, complete which data packets can be forward probabilistic. This can be result for throughput optimization, automatic data load balancing and improve robustness to failures.

A combinatorial optimization problem can be represented as a tuple P=(S, F), where S is the solution space with s ∈ S a specific candidate solution and F : S → R, is a fitness function assigning positive values to candidates solution. The goal of the algorithm is find a solution s*, or set of solution S*, s* ∈ S* ⊆ S the increase the fitness function. Here, the s* is called optimal solution and S* is called the set of optimal solutions [16].

B. Fuzzy Logic System: Introduction

In 1965, fuzzy logic is introduced by Lotfi A. Zadeh, means a form of reasoning, derived from fuzzy set theory. The fuzzy logic variables have a truth value that ranges between 0 (False) and 1 (True) [17]. These truth values can be used to determine how the brakes should control. Linguistic variables are the input and output variables of the system that is decomposed into a set of linguistic terms. Example is if water filthness is a fuzzy variable, then linguistic variables such as clean, almost clean, dirty and normal.

C. Multiple Selection Parameters

In this section, recently multi-path protocols select number of redundant paths. The protocols are select one or two route parameters without considering the correlated parameters. The four routing parameters are: a) energy consumption rate, b) buffer occupancy rate, c) link stability between neighboring nodes, and d) the number of intermediate hops in the route. Mobile nodes have only limited battery capacity. The battery power consumption rate denoted by BPC, is evaluated by linear function as,

\[BPC = (Wr X Mr + Ws X Ms + Wr X Mo) / T\]

Where, Wr, Ws and Wo are the battery power consumed by the network interface, such as sends, receive, or overhears a packet; Mr, Ms, and Mo are the amount of three types of packets. T is a averaging the total amount of the power consumed. The maximum lifetime of a given path, Lp, is determined by

\[Lp = \min R_i\]

∀ni ∈ P

Where R, minimum value over the path, P is a available path. The energy consumption rate at a node R, is calculated in the following formula:

\[R_i = \frac{RBP}{BPC}\]

III. DESIGN OF FUZZY INFERENCE

Fuzzy inference is the process of formulating the mapping forms a given input to an output using fuzzy logic. Fuzzy logic has been applied in control system either to improve performance or to avoid difficult mathematical problems [19].

Fig. 1 shows the three major processes of fuzzy inference system. There are three major processes in the fuzzy logic system. They are fuzzification, Fuzzy inference and defuzzification [18]. The inputs into our FLS are: (i) the number of intermediate hops, (ii) band width (iii) delay.

A. Step 1: Fuzzification of Inputs and Outputs

The three input variables are to be fuzzified are the energy consumption rate (B), the packet buffer occupancy rate (Q), and the signal strength (SS). On the existing knowledge of MANET, the term "Low", "Medium", and "High" are used to describe the energy consumption rate. "Empty", "Medium", and "Full" to describe packet buffer occupancy rate. "Strong", "Medium", and "Weak" are terms for representing the signal strength. The fuzzy cost form lowest to highest are defined as LL (very low), LM, LH, ML, MM (Medium), MH, HL, and HH (Very high). We show these membership functions in fig. 2,3, 4, and 5. The linguistics values of inputs and we show these membership functions in fig. 2,3, 4, and 5. The linguistics values of inputs and outputs in the range 0 to 1.
Figure 1. Selection of multi objective optimal route

Figure 2. Fuzzy Member function for signal strength

Figure 3. Fuzzy Member function for battery capacity (energy consumption)

Figure 4. Fuzzy Member function for buffer occupancy

Figure 5. Fuzzy Member function for fuzzy cost

Network status at each node (signal strength, battery capacity, buffer occupancy)
B. Step 2: Inference Engine and Knowledge Base

Knowledge is a set of rules developed by expert system and also used them. We design knowledge base rules are connecting inputs and outputs. The constructions of the fuzzy rules use IF-THEN structure. The inputs are combined using the AND / OR operators. Example is, describes the input and output mapping.

If signal strength is weak and battery power is medium and buffer occupancy is empty then the fuzzy cost is medium.

Each input have three linguistics variables, the number of possibilities of fuzzy inference rules is 3 * 3 * 3 = 27. The table 1 shows the fuzzy rules for the signal weak strength in FLS.

<table>
<thead>
<tr>
<th>B</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMPTY</td>
<td>MH</td>
<td>MM</td>
<td>ML</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>HM</td>
<td>MH</td>
<td>MM</td>
</tr>
<tr>
<td>FULL</td>
<td>HH</td>
<td>HM</td>
<td>MH</td>
</tr>
</tbody>
</table>

C. Step 3: Defuzzification

Most useful of defuzzification technique is center of gravity of the solution of fuzzy sets. It refers the way of crisp value is extracted from a fuzzy set as representation value. There are many kinds of defuzzifiers, such as centroid, maximum, center of maxima, and height defuzzifiers. For a continuous aggregated fuzzy set, the centroid is given by,

\[
F_C = \frac{\sum \mu(x_i) x_i}{\sum \mu(x_i)}
\]

Where FC is the fuzzy cost, x_i is the element and \(\mu(x_i)\) is a membership function. This is extracted as the output of the applying fuzzy rules.

IV. OVERVIEW OF SIMULATION RESULTS

The objective of the fuzzy inference system is to reducing the overheads to decide that in which types network conditions the protocol performs poor, satisfactory or acceptable. Figure 1 show the basic inference system for applying Fuzzy Rules, it is help to implementing the model, figure 2 represents how the inputs metrics are strengthened by FIS to relate the effect on output metrics. With the help of
The proposed model using FIS and after tuning out the behavior, MANET environment will be able to improve the performance by using ACO with AODV, according to the model it is observed that which parameters are to be focused to increase the performance in terms of more packet delivery fraction with minimum routing load, and delay, the fuzzy rules are described in Fig. 6, after applying the rules of behavior of MANET for AODV is satisfactory, sample crisp output shown in Fig. 7.

V. CONCLUSION AND FUTURE WORK

In this paper we proposed a fuzzy logic based on the selection method. It is interrelation of different route selection parameters that affect the network performance is captured by fuzzy art technology. Research will be able to acquire advantages of the FIS that provides some way how to achieve the challenges for higher throughput at minimum cost and delay. By observing the model that fuzzy art colony based routing algorithm can be found that which input parameters influence output parameters. It is concluded by increasing the number of nodes or changing speed of movements. It will be reduce the performance of the routing protocols. By using the proposed modal, performance of routing protocol is increased then it is able to have low signal loss, and high energy consumption rate. In the future the next generation networks will have capabilities some features and allow such an intelligent agent based routing algorithm to update the routing tables independently, replaced by conventional routing algorithms.

ACKNOWLEDGMENT

We would like to thank the Principal, HOD and faculty members of P.G and Research Department of Computer Science and Research Scholars at Government Arts College (Autonomous), Karur for their courage and encouragement to publish this work.

REFERENCES

Detection Approach for Black Hole Attack on AODV in MANETs using Fuzzy Logic System

C.V.Anchugam,
Research scholar,
P.G. and Research Department of Computer Science,
Government Arts College (Autonomous),
Karur-639 005, Tamilnadu, India.
Email_id: anchugam.mca@gmail.com

Dr.K.Thangadurai,
Assistant Professor and Head,
P.G. and Research Department of Computer Science,
Government Arts College (Autonomous),
Karur-639 005, Tamilnadu, India.
Email_id: ktramprasad04@yahoo.com

Abstract— Mobile Ad-hoc Networks (MANETs) technology has gain popularity in recent years by researchers on account of its flexibility, low cost and ease of development. Hence ad hoc networks needs very specialized security methods. But there is no single approach fitting all the networks, as the nodes can be any devices. MANETs are much more vulnerable to attack than the wired network. The black hole attack is a type of denial-of-service attack which passed out disrupts the service of network layer. A Fuzzy Inference System (FIS) is implemented to be MATLAB 7.0 and the model is found to be satisfactory with the fuzzy input metrics and de-fuzzified output metrics. In this paper, we proposed to detect the attack by using detection system that uses FIS for routing protocol. FIS offers a natural way of representing and reasoning the problems with uncertainty and imprecision. We have analyzed and improved the performance of Ad-hoc On Demand Distance Vector in the parameters such as packet loss rate, data rate and energy.

Index Terms — AODV, Black hole attack, Detection, Fuzzy inference system, MANETs.

I. INTRODUCTION

An Independent Basic Service Set (IBBS) or Ad hoc Networks is no fixed infrastructure, there is no access point and it’s simply communicated directly with each other. Because of the mobility of nodes in ad hoc networks, they are commonly called as MANET. Mobile Ad hoc Networks (MANETs) [1] is a group of mobile nodes which are freely to move unsystematically. These nodes are communicated with each other without the help of an existing network infrastructure. Because the nodes are mobile, the network topology changes rapidly, capriciously over time and nodes have to form their own mutual infrastructure [2]. Ad hoc networks are more susceptible to security problem than the wired networks and there are several security issues [3] such as limited energy resource, no centralized control facility, antagonist inside the network and changing scale. Ad hoc networks are suitable for used in situation, where any wired and wireless infrastructure is inaccessible, overloaded, damaged or destroyed. MANETs have several potential applications, like tactical networks, sensor networks, education, entertainment, medical service, personal area network, especially in military and rescue operations such as connecting soldiers in the battlefield or creating a temporary network in place of one, which collapsed after a disaster like tsunami.

MANETs important task is a node to transfer data to another node, through searching and establishing a route from source to destination. Many researchers developing number of routing protocols have been used to execute this task. In this protocol, to find a path between two hosts using routing protocol is a very herculean task due to their highly dynamic topology, absence of centralized administration.

The security thread are extensively mentioned and investigated within the wired and wireless [4], the correspondingly unclear scenario has jointly happened in MANETs because of the inherent style defects [5]. There is a unit several security problems that are studied in recent years. For example, snooping attacks, wormhole attacks, black hole attack [6], routing table overflow and poisoning attacks, packet replication, Denial of Service attacks (DoS), Distributed Denial of Service attacks (DDoS) [7]. Especially, the misconduct routing [8] downside is one amongst the popularized security threats like black hole attacks. Some researchers propose their secure routing plan [9, 10] to resolve this issue; however the protection downside continues to be unable to stop fully.

In this paper, we have a tendency to concentrate on differing kinds of black hole attack in MANETs which may be divided in to single black hole attack and cooperative black hole attack. Furthermore many detection schemes are mentioned clearly and suggested appropriate scheme for detection malicious node. The analysis metrics of routing protocol embrace packet delivery magnitude relation, quality variation with total variety of errors, packet routing overhead, end-to-end delay by varied in node density [11].

II. BLACK HOLE ATTACK IN MANETS

Security is one amongst the foremost primary considerations in MANETs for the protection of communication and security of data. For network operation it's necessary to perform routing and packet forwarding. Hence numbers of security mechanisms has been created to counter live the malicious attacks. Mechanisms used for the protection of MANETs area unit referred to as preventive
and reactive mechanism. In preventive mechanism, authentications, access controls, and secret writing techniques are unit concerned. Whereas in Reactive mechanism, totally different schemes like intrusion detection systems (IDS) and cooperation mechanisms are unit used. Just in case of MANET’s intrusion is employed for detection of misuse. Black hole downside in MANETs [12] could be a serious security downside to be resolved.

In black hole attack, a malicious node uses its routing protocol so as to advertise itself for having the shortest path to the destination node or to the packet it desires to intercept. This hostile node advertises its availability of contemporary routes regardless of checking its routing table. During this means offender node can continually have the supply in replying to the route request and so intercept the information packet and retain it [13]. In protocol supported flooding, the malicious node reply are going to be received by the requesting node before the reception of reply from actual node; thence a malicious and cast route is formed. Once this route is established, currently it’s up to the node whether or not to drop all the packets or forward it to the unknown address [14].

The method how malicious node fits in the data routes varies. Fig. 1 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 “4” is a malicious node then it will claim that it has active route to the specified destination as soon as it receives Route Request (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 seeding data packets to node “4”. In this way all the data packet will be lost consumed or lost.

A. Black Hole Attack Caused By RREQ

An assaulter will send pretend RREQ messages to create Black hole attack [2]. In RREQ Black hole attack, the assaulter pretends to air a RREQ message with a non-existent node address. Different nodes can update their route to travel by the non-existent node to the destination node. As a result, the conventional route is going to be counteracted.

The assaulter will generate Black hole attack by faked RREQ message as follows:
1. Set the sort field to RREQ (1).
2. Set the conceiver informatics address to the originating node’s informatics address.
3. Set the destination informatics address to the destination node’s informatics address.
4. Set the supply informatics address (in the informatics header) to a non-existent informatics address (Black hole).
5. Increase the supply sequence range by a minimum of one, or decrease the hop count to one.

The assaulter forms a Black hole attack between the supply node and therefore the destination node by faked RREQ message because it is shown in Fig. 2.

Figure 2: Black hole node is formed by faked RREQ

B. Black Hole Attack Caused By Route Reply (RREP)

The assaulter could generate a RREP message to create part as follows:
1. Set the sort field to RREP (2).
2. Set the hop count field to 1.
3. Set the conceiver informatics address because the originating node of the route and therefore the destination informatics address because the destination node of the route.
4. Increase the destination sequence range by a minimum of one.
5. Set the supply informatics address (in the informatics header) to a non-existent informatics address (Black hole).

The assaulter unicasts the faked RREP message to the originating node. Once originating node receives the faked RREP message, it'll update its route to destination node through the non-existent node. Then RREP Black hole is made because it is shown in Fig. 3.

Figure 3: Black hole node is formed by faked RREP

III. FUZZY LOGIC SYSTEM: INTRODUCTION

Contrary to the conventional hard computing techniques, the prime inherent advantage associated with the soft computing techniques is the non requirement of a mathematical model and hence are becoming increasingly
popular of a system identification methodology. Three powerful soft computing techniques which are very popular are the Neural Network, fuzzy Logic and the Genetic Algorithm. The pivotal contribution of fuzzy logic is a methodology for computing with words which can deal with imprecision and granularity.

Fuzzy logic (FL) was initiated in 1965 [15], by Lotfi A. Zadeh, professor for computer science at the University of California Berkeley. Unlike, crisp logic based on binary sets which are essentially a two-valued logic, “fuzzy logic” is a form of multi-valued logic and is based on fuzzy set theory. To deal with fluid or approximate reasoning, fuzzy logic variables can take a truth value that ranges in degree between 0 and 1. Fuzzy logic is a super set of conventional logic that has been extended to handle the concept of partial truth: the truth values between completely true and completely false.

A. Design Of Fuzzy Inference System

The fuzzy inference system (FIS) is based on the concepts of fuzzy set theory, fuzzy if – then rules and fuzzy reasoning. The framing of the fuzzy if – then rules forms the key component in FIS. FIS is a very popular technique and has been widely applied in different field like data classification, automatic control, expert system, decision making, robotics, time series analysis, pattern classification, system identification, etc.

The inference system is known by copious different names, such as fuzzy-rule-based system, fuzzy expert system [16], fuzzy model [17], fuzzy associative memory [18], fuzzy logic controller [19] and simply fuzzy system.

The basic structure of a fuzzy inference system consists of three principal components viz a rule base comprising of the selected fuzzy rules, a database defining the membership functions of the fuzzy rules, and a reasoning mechanism which performs a fuzzy reasoning inference with respect to the rules so as to derive a reasonable output.

FIS is shown in fig. 4, does the mapping from crisp inputs into crisp outputs. The crisp inputs may be measurement or observation data, which is the case of the large majority of practical applications. These inputs are fuzzified (mapped to fuzzy sets), which can be viewed as the activation of relevant rules for a given situation. Once the output fuzzy set is computed through the process of inference, a defuzzification is performed, since in practical applications crisp outputs are generally required. The rules are linguistic if – then statements sentences and constitute a key aspect in the performance of a fuzzy inference system.

IV. EXISTING SYSTEM

Fuzzy logic may be a mathematical tool for addressing uncertainty and impreciseness in human reasoning regarding universe information [20]. It is often wont to infer the degree of malicious behavior of a node, or to calculate the trust level between the nodes. Examples of these approaches square measure [21], [22]. In [21], a distributed strategy supported symbolic logic is employed to live the degree to that symptom of attack square measure gift at every node (by using symptom-attack relationship).

However, this method consumes lots of power that affects the network life. In [22], each node works in promiscuous mode to gather info for the fuzzy system. The fuzzy system exploits this info to assign a fidelity level to every node. If a node’s fidelity level is a smaller amount than a selected threshold, it’s marked as a malicious node. However, this method consumes additional power from the nodes.

The proposed system is predicated upon fuzzy logic [24] [27]. Fuzzy logic may be a style of multi valued logic derived from fuzzy pure mathematics to upset reasoning that's approximate instead of precise. In
distinction with “crisp logic”, wherever binary sets have binary logic. Fuzzy logic variables could have a truth worth that ranges between 0 and 1 and isn’t unnatural to the reality values of classic propositional logic.

The fuzzy model [25] is integrated with Ad-hoc On Demand Distance Vector (AODV) [23] [26] routing protocol as shown in figure one. It consists of following four parts specifically Fuzzy Parameter Extraction, Fuzzy Computation, Fuzzy Verification Module and Alarm Packet Generation Module. Throughout fuzzy parameter extraction, the system extracts the parameters needed for analysis from network traffic. These parameters are passed to fuzzy computation module, which applies numerous fuzzy rules and membership functions to calculate fidelity level of the node. This fidelity level is compared with threshold value in fuzzy verification module to visualize the behavior of node and if, fidelity level is a smaller amount than intensity, Associate in Nursing alarm packet with the information processing address of detected malicious node is broadcasted within the network.

Deng et al. [29], author proposed solution for individual black holes. However they don’t contemplate the cooperative black hole attacks. According to their solution, information concerning subsequent hop to the destination ought to be enclosed within the RREP packet once any intermediate node replies for RREQ. Then the supply node sends a further request (FREQ) to subsequent hop of replies node and asks concerning the replied node and route to the destination. By mistreatment this technique we will establish trustiness of the replied node given that subsequent hop is trusted. However, this answer cannot stop cooperative region attacks on MANETs. For instance, if subsequent hop additionally cooperates with the replied node, the replies for the FREQ are merely “yes” for each query. Then the supply can trust on next hop and send information through the replied node that could be a region node.

LathaTamilselvan, Dr. V. Sankaranarayananet [28], author planned associate approach to combat the part attack. In MANETs, the absence of a set infrastructure, therefore nodes got to collaborate so as to supply the mandatory network practicality. One in all the principal routing protocols employed in impromptu network is impromptu on demand distance vector protocol. The safety of the AODV protocol is compromised by a specific style of attack referred to as part attack. During this attack a malicious node advertise itself as having the shortest path to the node whose packets it desires to intercept. To scale back the likelihood it’s planned to attend and check the replies from all the neighboring nodes to search out a secure route. Their approach to combat the part attack is to create use of a fidelity table whereby each taking part node are going to be appointed a fidelity level that acts as a live of responsibility of that node. Just in case the amount of any node drops to zero, it’s thought of to be a malicious node, termed as a part and is eliminated. The share of packets received through our system is best than that in AODV in presence of cooperative part attack. The answer is simulated victimization the worldwide sensing element machine and is found to realize the desired security with stripped-down delay and overhead.

V. PROPOSED WORK

Black hole attack is dangerous active attacks in mobile ad hoc networks. This type of attack is performed by a single node, called as single black hole attack or combination of nodes, called collaborative black hole attack. This attacker node is also called selfish node, stingy node [30].

Detection algorithm of malicious node:
1. On receiving the route request (RREQ) it first makes an entry in its routing table for the node that forwarded the RREQ.
2. If it is the destination node or if it has a fresh enough route to the destination node, it replies to the RREQ with a route reply (RREP).
3. If it is neither the destination nor does it have a fresh enough routes to the destination, then it forwards the RREQ to its neighbors.
4. On receiving an RREP, it again makes a note of the node that sent the RREQ in its routing table and then forwards the RREP in the reverse direction.
5. On receiving a request to enter into the indiscriminate mode, it starts listening in the network for all the packets destined to that particular IP address and monitors its neighbors, for the movement of the data packet.
6. After data transmission, identified and analysis the parameters, such as packet loss rate, data rate and energy.
7. At that time source node entered into fuzzy system and start analyzing the parameter.
8. If it is the data packet loss and data rate parameter is low then to set priority is also low. In case, it find out the neighboring node energy is low then the node is called malicious node.
9. To finds out that the priority is high then to continue data transmission.
10. Otherwise, collecting low priority nodes details and maintaining black list table for black hole node. Broadcast the malicious node IP address in the network. So that the node they can’t participate in the route discovery again.

We suggest an elucidation that’s an improvement of the basic AODV routing protocol, which will be able to evade black holes. To shrink the possibility it is suggested to wait and check the replies from all the neighboring nodes to locate a safe route. According to this suggested resolution the requesting node without sending the data packets to the reply node at once, it has to wait till other replies with next hop details from the other neighboring nodes. After receiving all replies and to start transmit a data for source to destination through neighboring node with safe route. The following flowchart fig. 5 shows detection of malicious node in the network.
VI. IMPLEMENTATION OF FUZZY INFERENCE SYSTEM

The proposed system is based upon fuzzy logic. The fuzzy mode integrated with ad-hoc demand distance vector routing protocol as shown in fig. 6. It consists of following components i.e.,

A. Fuzzy parameter extraction
B. Fuzzy Computation
C. Fuzzy Verification
D. Attack Node Identification

A. Fuzzy Parameter Extraction

The input of the fuzzy system in node “s” is extracted by listening to the traffic received and generated by its immediate neighbors and create a fuzzy parameter list in new neighbor table for its every neighbor. Each node in the network works in the promiscuous mode and listens to the routing and network traffic of their neighbors and collects the information for fuzzy system.

We have a tendency to planned associate formula that relies on higher than factors. During this formula first off we have a tendency to outline the network with N range of nodes and we set supply node to S and destination node D and at that time we let current node is as supply node. We have a tendency to repeat the steps till current node isn’t capable destination node. During this currently we discover the list of neighboring nodes of current node. We have a tendency to determine the parameter S of every neighbor node i.e., packet loss, data rate. During this planned formula we have a tendency to use the idea of priority, solely high priority nodes participate in communication.

The following fig. 7.a, b and c shows a fuzzy membership function for packet loss rate, data rate and energy and figure 8 shows a fuzzy membership function for priority level.

![Figure 5: Flowchart for detection of malicious node in the network](image)

![Figure 6: Proposed System](image)

![Figure 7.a: Fuzzy membership function- Packet Loss Rate](image)

![Figure 7.b: Fuzzy membership function- Data Rate](image)

![Figure 7.c: Fuzzy membership function-Energy](image)
B. Fuzzy Computation

The fuzzy rules have IF-THEN structure. The inputs are combined using the AND operator. The proposed system receives packet loss rate, data rate and energy as input from routing and has one output, priority level. The following is an example of rules which describes the input and output mapping.

- If packet loss rate is LOW and data rate is LOW and energy is LOW, then priority is LOW
- If packet loss rate is MEDIUM and data rate is MEDIUM and energy is MEDIUM, then priority is MEDIUM
- If packet loss rate is HIGH and data rate is HIGH, energy is HIGH, then priority is HIGH

The priority lies between 0 and 10. The minimum value for priority can occur as a result of more malicious behavior than rightful behavior of a neighboring node. Hence, a priority level of 0 represents complete malicious behavior and 10 represents rightful behavior of a particular node.

C. Fuzzy Verification

In the verification section, the energy of any node is low then set the priority of node is low and nodes don’t participate in communication. We have a tendency to increase the priority of node that they participate in communication. We have a tendency to area unit providing the condition information Transmitted from the node is larger than threshold and Rate of node is additionally greater than threshold then increase the amount of priority. Table 1.a, b shows some of the fuzzy rule base in the fuzzy controller and trust value of fuzzy level.

<table>
<thead>
<tr>
<th>Fuzzy logic system rules</th>
<th>Input</th>
<th>Output-Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Loss Rate</td>
<td>Data Rate</td>
<td>Energy</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fuzzy Discrimination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuzzy level</td>
</tr>
<tr>
<td>Very high</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Very low</td>
</tr>
</tbody>
</table>

Table 1.a: Fuzzy rule – FLS rule

Fuzzy trust is represented by the trust level that ranges over the set of values from very untrustworthy to very trustworthy levels. It enables to specify a range for a given trust level instead of giving it a particular discrete value. Trust levels ranging from very untrustworthy, untrustworthy, medium trustworthy, trustworthy, very trustworthy, unknown based on fuzzy logic.

D. Attack Node Identification

On this basis of information passed by fuzzy verification section, if the priority level and energy level is very low than this model generates an alert message with IP address of the node that is declared as black hole node. It refers to the way of crisp input value is extracted from a fuzzy set as a representation value using centroid of area strategy defuzzifier. For continuous aggregated fuzzy set, the centroid is given by [31] equation (1),

\[ F_C = \frac{\sum x \mu(x)}{\sum \mu(x)} \]

With the help of proposed model using FIS and after tuning out the behavior, MANET environment will be able to improve the performance by using ant colony with AODV, according to the model it is observed that which parameters are to be focused to increase the performance in terms of more data rate with minimum packet loss rate and energy, after applying the rules of behavior of MANET’s for AODV is satisfactory, sample crisp output shown in Figure 10.
The objective of the fuzzy system is to identifying the malicious node to decide that in which type of network conditions the protocol performs low, medium and high. With the help of proposed system using fuzzy system, according to the system it is observed that which parameters are to be focused to increase the performance. As the analysis result shows that the proposed system is performing better than existing routing algorithm in case of packet delivery ratio, through put, end-to-end delay so we can say that fuzzy logic does solves the problem of malicious node in the network and hence increases the overall performance of the network.

The proposed system can be enhanced in future by other researchers in the following ways:

1. We have worked only with Black Hole attack; the work can be enhanced by implementing some other attack such as worm hole, flooding attacks, Denial of Service etc.

ACKNOWLEDGMENT

We would like to thanks to the Principal, faculty members of P.G and Research Department of Computer Science and Research Scholars Government Arts College (Autonomous), Karur for their encouragement to publish this work.

REFERENCES


[24]. Fuzzy Logic with Engineering Applications by TIMOTHY J. ROSS McGRAW Hill, Inc.


[31]. C.V. Anchugam, Dr.K.Thangadurai, “Fuzzy Cost Based Multipath Routing Protocol for MANETS”, presented at the International Conference on IEEE World Congress on Computing and Communication Technologies (WCCCT’14), St. Joseph College, Trichy, on 27.02.14 to 1.03.14, pp. 286-290, DOI: 10.1109 / WCCCT.2014.11.

Authors Profile

Dr.K.Thangadurai, is presently working as Assistant Professor and Head in P.G. and Research Department of Computer Science, Government Arts College (Autonomous), Karur, Tamilnadu, India.

He has fifteen years of rich teaching experience with Ten years of Research experience in the field of Computer Science. He has worked as the Head of P.G. Department of Computer Science at Government Arts College (Autonomous), Krishnagiri. He has published technical papers in many National and International Conferences and Journals. His areas of interest are Software Engineering, Network Security, Data Mining, etc.,

C.V. Anchugam is presently doing Ph.D in P.G. and Research Department of Computer Science, at Government Arts College (Autonomous), Karur, Tamilnadu, India. She has received her B.Sc (Computer Science) degree from Sri Saradha College of Arts and Science, Karur, Tamilnadu, India in 2002.

She has received her Master of Computer Application (M.C.A) degree from M.Kumarasamy College of Engineering, Karur, Tamilnadu, India in 2005.She has published number of papers in esteemed National and International conferences and journals. Her interests are in Cryptography, Network security and Ad hoc networks.
A Fuzzy based detection technique of Malicious Node in Mobile Ad-hoc Networks

C.V.Anchugam,
Ph.D Research Scholar,
P.G and Research Department of Computer Science,
Government Arts College (Autonomous),
Karur-639 005, Tamilnadu, India.
anchugam.mca@gmail.com

Dr.K.Thangadurai,
Assistant Professor and Head,
P.G and Research Department of Computer Science,
Government Arts College (Autonomous),
Karur-639 005, Tamilnadu, India.
krtramprasad04@yahoo.com

Abstract – A Mobile Ad-hoc Network (MANET) could be a self-configuring network of mobile routers connected by wireless links. As the traffic increases over the network such type of network suffers from the problems like congestion and packet loss. A network can be affected from some malicious node over the network. As a result some loss of information occurs over the communication. The packet loss is acceptable up to some threshold value but as there is more packet loss we need some solution for this. In our technique, every node in the mobile ad-hoc network sends the route request and waits for the acknowledgment. The requesting nodes analyze the behavior of unknown node using fuzzy technique and on basis of result the node take this node in the route of the packet. Subsequently, node state information can be utilized by the routing protocol to bypass those malicious nodes. The proposed system will identify the attack over the node as well as provide the solution to reduce the data loss over the network.

Index Terms – MANET, Black hole attack, Cooperative black hole attack, Fuzzy logic system, Routing protocol

I. INTRODUCTION

Ad-hoc networks type form impulsively while not a necessity of an infrastructure or centralized controller. This kind of peer-to-peer system infers that every node, or user, within the network will act as a knowledge end or intermediate repeater. Thus, all users work beside to improve the consistency of network communications. These styles of networks also are popularly better-known to as “mesh networks” as a result of the topology of network communications resembles a mesh.

The redundant communication methods provided by spontaneous mesh networks drastically improve fault tolerance for the network. In addition, the power for information packets to "hop" from one user to a different effectively extends the network coverage space and provides an answer to overcome non-Line Of Sight (LOS) problems.

Mobile applications gift further challenges for mesh networks as changes to the network topology are swift and widespread. Such eventualities need the utilization of Mobile Ad hoc Networking (MANET) technology to confirm communication routes are updated quickly and accurately. MANETs are self-forming, self-maintained, and self-healing, giving extreme network flexibility. Whereas MANETs is utterly self-contained, they’ll even be tied to an IP-based world or native network (e.g. net or non-public networks). These are observed as Hybrid MANETs.

A Mobile Ad-hoc Network (MANET) [1, 2] could be a self-configuring network of mobile routers (and associated hosts) connected by wireless links - the union of that type a random topology. The routers are unengaged to move at random and organize themselves at random; therefore, the network's wireless topology might amendment apace and erratically. Such a network might operate in an exceedingly standalone fashion, or is also connected to the larger network. Exposed configuration and fast deployment create spontaneous networks suitable for emergency things like natural or human induced disasters, military conflicts, emergency medical things etc.

II. BLACK HOLE ATTACK IN MANETs

Security in MANETs can be often usually classified into route security and information security. In information security, information is protected against any form of unauthorized speech act, disruption and destruction. In route security, routing (packet forwarding) is protected against any form of deception. Solving all vulnerabilities associated with each route and information securities notice each information integrity and confidentiality. Typical attacks that may be simply performed against MANETs include: region, Denial of Service (DoS), Impersonation, Disclosure, Spoofing, and Sleep deprivation attacks [17], [19], [20], and [21].
A single part attack is definitely happened within the mobile ad hoc networks [5]. It's a nature of denial of service attack where a malicious node offers false data of getting shortest route to the destination so as to induce all the information packets and drop it [7]. In black hole attack, [12], [13] a malicious node (or stingy node [8]) takes advantage of route discovery procedure of routing protocol, to point out itself as having the shortest path to the destination node or to the node whose packet it desires to intercept. This hostile node advertises its convenience of recent routes regardless of checking its routing table. During this manner assaulter node can perpetually have the supply in replying to the route request and so intercept the information packet and retain it [11]. Therefore, all traffics are routed through the assaulter, and thus, the assaulter will misuse or discard the traffic [10].

There are unit varied mechanisms are projected for finding single part attack in recent years. However, several detection schemes are unit unsuccessful in discussing the cooperative part issues. Some malicious nodes collaborate along so as to beguile the conventional into their unreal routing data, moreover, hide from the present detection theme. As a result, many cooperative detection schemes area unit projected preventing the collaborative black hole attacks [6]. The part attack has two properties. First property is, the node exploits the painter protocol, like AODV (Ad hoc On-demand Distance Vector) to advertise itself as having a legitimate path to a destination node, even if the path is invalid, with the intention of intercepting packets. Second property is, the assaulter consumes the intercepted packets while not forwarding to the other node [9]. Some major destruction generated by part is listed below:
1. It will increase network overhead; thanks to unwanted transmission.
2. It decreases the network’s time period by boosting energy consumption unnecessarily.
3. It destroys the network by dropping the crucial knowledge packets over the present communication.

A. Single Black Hole Attack

In single part attack solely single node behaves as malicious node inside a network. It’s conjointly called part attack with single malicious node. An example is shown as Figure 1, node 1 stands for the source node and node 4 represents the destination node. Node 3 may be a misconduct node who replies the RREQ packet sent from source node, and makes a false response that it’s the fastest route to the destination node. Thus node 1 mistakenly judges the route discovery method with completion, and starts to send knowledge packets to node 3. As what mentioned above, a malicious node in all probability drops or consumes the packets. This suspicious node is thought to be a black hole node in MANETs. As a result, node 3 is ready to misroute the packets simply, and also the network operation is suffered from this downside. The foremost important influence is that the PDR diminished severely.

B. Collaborative Black Hole Attack

In collaborative black hole attack multiple nodes within a network behave as malicious node within a network. It is also known as black hole attack with multiple malicious nodes. Here node 1 is the source node and 6 is the destination node. Nodes are 2, 3, 4, 5 and 7 acts as the intermediate nodes. Nodes are 3 and 5 acts as the cooperative Black holes. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole node 3 reaches the source node, well ahead of the other RREPs, as it can be seen from the figure 2.
receipt of data packets, node 3 simply drops them, instead of forwarding to the destination or node 3 forwards all the data to node 5. Node 5 simply drops it instead of forwarding to the destination. Thus the data packets get lost and hence never reach the intended destination.

C. Defense against Black Hole Attack

There are three defense levels to counter act associate degree attack, namely, preventive, incentive and detective-corrective [11]. The preventive level forbids the malicious nodes from taking part in packet forwarding. The inducement level seeks to stimulate the cooperation among the router nodes via associate degree economic model. The detective-corrective level aims to reveal the identity of the malicious node and to exclude it from the network.

III. ROUTING IN MANETS WITH AND WITHOUT MALICIOUS NODE

Normally [16], routing in MANETs is done ad hoc on demand distance vector routing protocol. In case of table driven process, each and every node in MANETs maintains some up-to-date information about the network. Every node has the information about latest network topology, any changes happened to the network is generally propagated to the network; accordingly node updates their routing table. But this kind of protocol creates several problems to the network in terms of bandwidth overhead, wastage of battery power of the nodes, entry of unnecessary redundant route etc., due to these difficulties, Ad hoc On Demand Distance Vector (AODV) routing protocol is preferred. In this protocol, routing tables are dynamically created when needed. So, whenever source node wants to send data to destination, it tries to establish the path through several ways by sending some RREQ packets. When destination sends a RREP packet to source through shortest path, the source sends data through this path. Though it looks very simple, but this kind of protocol suffers from several vulnerabilities of attack. If the path cannot be established then REER messages is generated. AODV protocol is very much acquainted with dynamic network condition, low processing and memory overhead, less bandwidth wastage with small control messages.

IV. LITERATURE SURVEY

Fuzzy logic may be a mathematical tool for addressing uncertainty and imprecision in human reasoning regarding universe information [23]. It is often wont to infer the degree of malicious behavior of a node, or to calculate the trust level between the nodes. Examples of these approaches square measure [24], [25]. In [24], a distributed strategy supported symbolic logic is employed to live the degree to that symptom of attack square measure gift at every node (by using symptom-attack relationship). However, this method consumes lots of power that affects the network life. In [25], each node works in promiscuous mode to gather info for the fuzzy system. The fuzzy system exploits this info to assign a fidelity level to every node. If a node's fidelity level is a smaller amount than a selected threshold, it's marked as a malicious node. However, this method consumes additional power from the nodes.

The proposed system is predicated upon fuzzy logic [27] [30]. Fuzzy logic may be a style of multi valued logic derived from fuzzy pure mathematics to upset reasoning that's approximate instead of precise. In distinction with “crisp logic”, wherever binary sets have binary logic, fuzzy logic variables could have a truth worth that ranges between 0 and 1 and isn't unnatural to the reality values of classic propositional logic.

The fuzzy model [28] is integrated with AODV [26] [29] routing protocol as shown in figure one. It consists of following four parts specifically Fuzzy Parameter Extraction, Fuzzy Computation, Fuzzy Verification Module and Alarm Packet Generation Module. Throughout fuzzy parameter extraction, the system extracts the parameters needed for analysis from network traffic. These parameters are passed to fuzzy computation module, which applies numerous fuzzy rules and membership functions to calculate fidelity level of the node. This fidelity level is compared with threshold value in fuzzy verification module to visualize the behavior of node and if, fidelity level is a smaller amount than intensity, Associate in Nursing alarm packet with the information processing address of detected malicious node is broadcasted within the network.

Deng et al. [32], author proposed solution for individual black holes. However they don't contemplate the cooperative black hole attacks. According to their solution, information concerning subsequent hop to the destination ought to be enclosed within the RREP packet once any intermediate node replies for RREQ. Then the supply node sends a further request (FREQ) to subsequent hop of replies node and asks concerning the replied node and route to the destination. By mistreatment this technique we will establish trustiness of the replied node given that subsequent hop is trusted. However, this answer cannot stop cooperative region attacks on MANETs. For instance, if subsequent hop additionally cooperates with the replied node, the replies for the FREQ are merely “yes” for each query. Then the supply can trust on next hop and
send information through the replied node that could be a region node.

LathaTamilselvan, Dr. V. Sankaranarayanan et. al [31], author planned associate approach to combat the part attack. In MANET, the absence of a set infrastructure, therefore nodes got to collaborate so as to supply the mandatory network practicality. One in all the principal routing protocols employed in impromptu network is impromptu on demand distance vector protocol. The safety of the AODV protocol is compromised by a specific style of attack referred to as part attack. During this attack a malicious node advertise itself as having the shortest path to the node whose packets it desires to intercept. To scale back the likelihood it’s planned to attend and check the replies from all the neighboring nodes to search out a secure route. Their approach to combat the part attack is to create use of a fidelity table whereby each taking part node are going to be appointed a fidelity level that acts as a live of responsibility of that node. Just in case the amount of any node drops to zero, it’s thought of to be a malicious node, termed as a part and is eliminated. The share of packets received through our system is best than that in AODV in presence of cooperative part attack. The answer is simulated victimization the worldwide sensing element machine and is found to realize the desired security with stripped-down delay and overhead.

V. FUZZY LOGIC SYSTEM

Fuzzy inference is the process of formulating the mapping forms a given input to an output using fuzzy logic. Fuzzy logic has been applied in control system either to improve performance or to avoid difficult mathematical problems [3]. Fuzzy logic [21] starts with and builds on a collection of user-supplied human language rules. The fuzzy systems convert these rules to their mathematical equivalents. This simplifies the task of the system designer and therefore the computer, and ends up in way more correct representations of the approach systems behave within the real world.

Additional advantages of fuzzy logic embody its simplicity and its flexibility. Fuzzy logic will handle issues with general and incomplete information, and it will model nonlinear functions of whimsical quality. Fuzzy logic models, referred to as fuzzy logical thinking systems, consists of variety of conditional “if – then” rules. For the designer who understands the system, these rules area unit straightforward to write down, and as several rules as necessary may be provided to explain the system adequately.

In fuzzy logic, in contrast to customary conditional logic, the reality of any statement could be a matter of degree. We tend to area unit accustomed to logical thinking rules of the shape p → q (p implies q). Fuzzy logical thinking systems admit membership functions to elucidate to the pc the way to calculate the proper price between 0 and 1. The degree to that any fuzzy statement is true is denoted by a price between 0 and 1.

VI. PROPOSED WORK

Mobile ad hoc network is one in every of commonest unexpected network with lot of issues associated with congestion and routing. We have a tendency to area unit providing one in every of the solutions to secure the transmission over the network. Security aspects play a very important role in most of the appliance situations given the vulnerabilities inherent in unexpected networking from the actual fact that radio communication takes place to routing, man-in-the-middle and elaborate information injection attacks [16]. Security has become a primary concern so as to supply protected communication between mobile nodes in an exceedingly hostile setting. The planned system is near to style associate intrusion detection system to detect the region attack on painter. This detection system relies on symbolic logic. We have a tendency to propose a detection system during which improvement is by creating use of two factors i.e., Packet Loss Rate, Data Rate. We will use each factors victimization symbolic logic that is downside determination system.

Fuzzy logic provides a straightforward thanks to reach a precise conclusion based mostly upon obscure, ambiguous, shouting or missing information. We have a tendency to planned associate formula that relies on higher than factors. During this formula first off we have a tendency to outline the network with N range of nodes and we set supply node to S and destination node D and at that time we let current node is as supply node. We have a tendency to repeat the steps till current node isn’t capable destination node. During this currently we discover the list of neighboring nodes of current node. We have a tendency to determine the parameter S of every neighbor node i.e., packet loss, data rate. During this planned formula we have a tendency to use the idea of priority, solely high priority nodes participate in communication.

For priority we have a tendency to outline the three steps at sender aspect. Table 1 shows some of the fuzzy rule base in the fuzzy controller.

Step 1: Packet loss is low and data rate is high then priority is high
Step 2: Packet loss is medium and data rate is high then priority is medium.
Step 3: Packet loss is low and data rate is low then priority is low.
<table>
<thead>
<tr>
<th>Packet Loss Rate</th>
<th>Data Rate</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

Table 1: Fuzzy rule

We set priority at receiver aspect additionally once the energy of any node is low then set the priority of node is low and node don’t participate in communication. We have a tendency to increase the priority of node that they participate in communication. We have a tendency to area unit providing the condition information transmitted from the node is larger than threshold and Rate of node is additionally greater than threshold then increase the amount of priority. The following algorithm to detect black hole attack using fuzzy logic:

1. Establish a network with N number of nodes.
2. Specify the properties of network.
3. Define the Source Node (SN) and the Destination Node (DN) over the network.
4. Route discovery process:
   - Source node broadcast the RREQ message to neighboring nodes and hop count is initialized.
5. Collecting replies:
   - Identify the list of Neighboring Nodes to called CN. Collecting the neighboring nodes information stored in routing table. NEN (1), NEN (2)… NEN (M)
   - Neighboring nodes receive the request then it will check whether the node is destination or not.
     - If yes then
       - The node is set to DN
     - else
       - it’s forwarded to all the neighbors.
6. Analysis parameter:
   - Identifying the analysis parameters for each neighbor node called Packet Loss Rate (PLR), Data Rate (DR).
     - [Sender that is Source node enter into fuzzy logic]
   - Fuzzified there rules under the fuzzification process
7. Identify malicious node:
   - Check packet loss rate and data rate value.
   - Packet loss is low and data rate is high then priority is high
   - Packet loss is medium and data rate is high then priority is medium.
   - Packet loss is low and data rate is low then priority is low.
   - The priority is high then now that neighbor node is malicious node.
8. Priority check:
   - Find the list of high priority received from the Neighbor node list called P(1), P(2)…P(K) [Find receiver level using fuzzy logic]
   - The energy level is also low then that node is a malicious node.
   - Otherwise, continue to transmit a data.
   - Find the node with maximum priority called node is P.
9. Broadcast the malicious node address in the network.
10. Collect malicious node information and stored into table called Malicious Node Table (MNT).
11. Route maintenance: Once route message have established route path between source to destinations and data packets are send along the same path. Source node always maintain routing table and MNT table.

The following figure 3 shows the flow of detect black hole attack in the network,

Figure 3: Flow of detect black hole attack using fuzzy logic

With the help of proposed model using FIS and after tuning out the behavior, MANET environment will be able to improve the performance by using AODV, according to the model it is observed that which parameters are to be focused to increase the performance in terms of more data rate with minimum packet loss rate and energy, after applying the rules of behavior of MANETs for...
AODV is satisfactory, sample crisp output shown in Figure 4.

Figure 4: Sample crisp output of inference system

VII. CONCLUSION

In this paper we've got given fuzzy based mostly trust worth routing algorithmic program to single black-hole and cooperative black-hole attack that are measure caused by malicious nodes. The purposed algorithmic program can give the answer of packet loss and rate against the part attack in network. The purposed work can foremost notice the black hole attack exploitation the fuzzy logic. The fuzzy logic is enforced on packet loss and rate at time of node communication. Currently rather than transferring information on this node, it'll be passing on from the encompassing nodes; it'll solely handle the transmission that's directed to it solely.

As the analysis result shows that the proposed system is performing better than existing routing algorithm in case of packet deliver ratio, through put, end-to-end delay so we can say that fuzzy logic does solves the problem of malicious node in the network and hence increases the overall performance of the network. In this paper, performed the work only with Black Hole attack; the future work can be enhanced by implementing some other attack such as worm hole, flooding attacks, Denial of Service etc.

ACKNOWLEDGMENT

We would like to thanks to the Principal, faculty members of P.G and Research Department of Computer Science and Research Scholars Government Arts College (Autonomous), Karur for their encouragement to publish this work.

REFERENCES

27. Fuzzy Logic with Engineering Applications by TIMOTHY J.ROSSMCRAW Hill, Inc.
Detection of Black Hole Attack in Mobile Ad-hoc Networks using Ant Colony Optimization – simulation Analysis

C.V. Anchugam* and K. Thangadurai
PG. 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 Ant Colony Optimization (ACO) is used to modify the Ad-hoc On Demand Distance Vector (AODV) routing protocol. The ants 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 time15. The Mobile Ad hoc Network has many applications such as military, disaster relief applications, mini site operations where infrastructure are not available, unfeasible, or exclusive15. 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 ranges12. 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 predictable14. 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 protection45.

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. The main difficulties are high latency time in route finding and excessive flooding can lead to network clogging10. 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 context 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 property 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\(^{14}\). 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.
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 wants to send a data packet to the destination, it generates the RREQ packet and floods it in the whole network route discovery.

Route Reply (RREP) Message: When the destination receives RREQ, it generates the RREP packet and unicasts 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 messages. HELLO messages are used to inform the neighboring node that the link is still alive and never to be forwarded.

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Request ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Destination IP Address</td>
<td></td>
</tr>
<tr>
<td>Destination Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Originator IP Address</td>
<td></td>
</tr>
<tr>
<td>Originator Sequence Address</td>
<td></td>
</tr>
<tr>
<td>Hop Count</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 2.** Route Request (RREQ).

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Destination IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Originator IP Address</td>
<td></td>
</tr>
<tr>
<td>Hop Count</td>
<td>Life Time</td>
</tr>
</tbody>
</table>

**Figure 3.** Route Reply (RREP).

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Unreachable Destination IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unreachable Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Additional Unreachable Destination IP Address</td>
<td></td>
</tr>
<tr>
<td>Additional Unreachable Destination Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Destination Count</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4.** Route Error (RERR).

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.

### 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. 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 \( F: S \to R \) 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.

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(τ)
3. WHILE termination condition not met do
   Schedule Activities
   \[ S_{bac} = \emptyset \]
   for \( j = 1, \ldots, n_a \) do
   \[ S = \text{AntBasedSolution \ Construction (I)} \]
   \[ S = \text{LocalSearch (S)} \]
   \[ S_{bac} = S_{bac} \cup \{S\} \]
end for
   Pheromone Updation (I)
   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:

\[
P^{k}_{ij} = \begin{cases}
\left[ \Gamma_{ij} \right]^a \left[ \eta_{ij} \right]^b & \text{if } j \in N_{i}^k ; \; P^{k}_{ij} = 0, \text{ otherwise}
\end{cases}
\]

Where \( N_{i}^k \) is the set of feasible sub-solution that can be next sub-solution of \( i \); \( \Gamma_{ij} \) the pheromone value between the sub-solution of \( i \) and \( j \); and \( \eta_{ij} \) the quality of the sub-solution \( j \) that will affect each ant’s determination to move to \( j \) when at \( i \). The parameter \( a \) and \( b \) are used to adjust the weight of exploration and exploitation.

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

\[
\Gamma_{ij} = (1 - \rho)\Gamma_{ij} + \rho \sum_{k=1}^{m} \Delta \Gamma_{ij}^k ; \; \Delta \Gamma_{ij}^k = \frac{1}{L^k} \rho \in (0,1)
\]

Where \( m \) denotes the number of ants, \( L^k \) the quality of solution created by ant \( k \), \( \rho \) 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 \( \varphi_{ij} \) (artificial pheromone), which modified by an ants when they visit the node. The pheromone concentration \( \varphi_{ij} \) is an indication of the usage of this edge. An ant located in node \( v_i \) uses pheromone \( \varphi_{ij} \) 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 \( v_i \).

\[
P_{i,j} = \begin{cases}
\frac{\varphi_{ij}}{\sum_{j \in N_{i}} \varphi_{ij}} & \text{if } j \in N_{i} \\
0 & \text{if } j \notin N_{i}
\end{cases}
\]

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

\[
\sum_{j \in N_{i}} P_{i,j} = 1, \; i \in [1,N]
\]

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:

\[
\varphi_{i,j} = (1 - q) \cdot \varphi_{i,j}, \; q \in (0,1)
\]

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 by 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. 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.
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. 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.

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. 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 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. 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. 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. 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. 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 discoverers 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 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.
8. For each FANT (currently in node i)
   - 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.
   - 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 $T$, 

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

Where, $N_i^r$ = average receiving node for the $i^{th}$ application, $N_i^s$ = 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.

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

Where, $N_i^s$, $N_i^r$ 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.

$$E-2-E \text{ delay} \ [\text{packet}_i] = \text{received time} \ [\text{packet}_i] - \text{sent time} \ [\text{packet}_i]$$

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.

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

Where, $N_i^s$, $N_i^r$ 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).
for the \textit{i}th application, and \textit{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

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.


A Nature Inspired Ant Colony Based Routing Protocol for MANETs

Dr. K. Thangadurai\(^1\) and C.V. Anchugam\(^2\)

\(^1\)Asst. Professor, P.G. and Research Department of Computer Science, Government Arts College (Autonomous), Karur, India.
\(^2\)Research Scholar, P.G. and Research Department of Computer Science, Government Arts College (Autonomous), Karur, India.
E-mail: \(^1\)ktramprasad04@yahoo.com, \(^2\)anchugam.mca@gmail.com

Abstract

A mobile ad hoc network (MANETs) is a collection of mobile user nodes which communicate over wireless medium. These kinds of networks are very flexible, because they do not have any central administration. Therefore, mobile ad hoc networks are suitable for temporary communication links. Many researchers interest in MANETs and particularly the design of routing protocols has gained a lot of consequence. However continuously changing network topology, limited bandwidth and energy issues formulate the challenges of MANETs. Recently researchers formed new class of routing algorithms based on swarm intelligent has been developed. These algorithms are inspired from nature self organizing systems such as ant colonies. Ant colony optimization identifies appropriate paths with the feedback of previously travelled packets and maintains routing table accordingly. The biological characteristics are self organization, robustness, adaption, self healing and local decision making. In this paper, we provides a comprehensive overview of the ant inspired routing algorithms for mobile ad hoc networks with its comparison and also bring out the character wise cost comparison table.

Index Terms: MANET, Routing Algorithm, Swarm Intelligence, Ant Colony Optimization.

1. Introduction To MANET

Mobile Ad hoc NETwork is a collection of mobile nodes that dynamically form a temporary network and are capable of communicating with each other without the use of a network infrastructure or any centralized administration. They are useful in many situations where it is not possible for information to be conveyed because of the limited cooperation and disaster relief missions, etc. Each node must act as a router, since routes are mostly multi-hop, due to the limited propagation range [1]. Due to the continuous movement of the nodes, the backbone of the network is continuously reconstructed.

Routing is a crucial service that specifies what node to take next at each decision node to reach the destination node. Due to the time varying nature of the topology of the networks, traditional routing algorithms that are used to fixed networks, cannot be directly applied to ad hoc networks. The main problem of the ad hoc network is mobility of the nodes resulting in fast variations of their availability and another problem is the power and battery lifetime of each device in the network [2]. There are many applications for MANET, for example, in a military battlefield, commercial sector, search and rescue or geographical area and local level, there is no base station for communication.

2. Overview Of Ant Colony Optimization (ACO)

Ant colony optimization was proposed by Dorigo and colleagues, as a method for solving hard Combinatorial Optimization Problems (COPs) [11]. In, COPs such as routing, it can be solved using Ant Colony Optimization in computer networks. One of the most powerful Swarm Intelligence (SI) [7, 8] techniques is Ant Colony Optimization [9], was first used in traditional networks. ARA was the first algorithm used in Mobile Ad-hoc Networks (MANETs).

The social behavior of ants is based on self-organization, which allows the highly coordinated behavior of real ants to be exploited to coordinate population of artificial ants that collaborate to solve computational problems [4]. In, ACO have been inspiration by the foraging behavior of ants [1]. When ants foraging for food, they wandering around the nests and upon finding food return to their nests and simultaneously deposit pheromone trails along the paths. Many ants may travel through different routes to the same food. They are two ways information transfer between ants: a direct communication (which include food exchange, visual and chemical contacts) and an indirect communication (which is called Stigmergy).

It can be derived as "Stimulation of work by the performance they have successes" [10]. It is an indirect form of communication. An individual agent leave signals in the environment and other agents sense them to drive their own behavior. The strength of the pheromone deposit directs the artificial ants toward the best paths and pheromone evaporation allows the system to forget old information and avoid quick convergence to suboptimal solutions. The probabilistic selection of paths allows the artificial ants to search for a large number of solutions. ACO has been applied successfully to discrete optimization problems such as the traveling salesman problem and routing [4, 5].

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 \(F: S \rightarrow \mathbb{R}\) is a fitness function assigning positive values to candidates solution. The goal of
the algorithm is find a solution \( s^* \), or set of solution \( S^* \), \( s^* \in S \) the increase the fitness function. Here, the \( s^* \) is called optimal solution and \( S^* \) is called the set of optimal solutions [3,11].

Each ant located at a city \( i \) hopes to a city \( j \) selected among the cities that have not yet been visited according to the probability:

\[
P_k(i,j) = \frac{\tau^\alpha \cdot d^\beta}{\sum_{r,s} \tau_{rs}^\alpha \cdot d_{rs}^\beta}
\]

Where,

- \( P_k(i,j) \) is the probability that ant \( k \) in city \( i \) will go to city \( j \).
- \( j \in J_k \) is the set of cities that have not yet been visited by ant \( k \) in city \( i \).
- \( \alpha \) is the relative importance of the pheromone trail.
- \( \beta \) is the relative importance of the distance between cities.

Therefore we choose probability of city is a function of how to close a city and how much pheromone is already exist on the trail. Each city has been visited exactly once by the ant, pheromone evaporation the edges to be calculated. The calculation formula is:

\[
\tau(i,j) = p \cdot \tau(i,j) + \sum_{k=1}^{\infty} \Delta \tau_k(i,j)
\]

\[
\Delta \tau_k = \begin{cases} 
1 & (i,j) \in \text{tour} \\
0 & \text{otherwise}
\end{cases}
\]

where,

- \( p \cdot \tau(i,j) \) multiplies the pheromone concentration on the edge between city \( i \) and city \( j \) \( p(\text{RHO}) \), which is called the "evaporation constant". This value between 0 and 1. The pheromone evaporates more rapidly for lower values.
- \( \sum_{k=1}^{\infty} \Delta \tau_k(i,j) \) is the amount of pheromone an ant \( k \) deposits on an edge, as defined by \( L_k \) which is length of the travelling is created by this ant.

2. 2 Ants as Agents

The biological insects like ants in the ant colony form a collective behavior. Their collective behavior is studied and applied to solve the complex problems. Ants live in colony and they possess the following characteristics [19] which are described below,

1) Scalability: The ants can change their group size by local and distributed agent interactions. This is an important characteristic by which the group is scaled to the desired level.
2) Fault tolerance: Each ant follows simple rule. They do not rely on a centralized control mechanism, graceful, scalable degradation.
3) Adaptation: Ants always search for new path by roaming around their nest. Once they find the food their nest members follow the shortest path. While nest members follow shortest path, some of the members of the colony always search for other shortest path. To accomplish this they change, die or reproduce for the colony
4) Speed: In order to make other ants to know the food source, they move faster to their nest. Other ants find more pheromone on the path and follow the path to the food source. Thus changes are propagated very fast to communicate to other nest mates in order to follow the food source.
5) Modularity: Ants follow simple rule of following the path which has higher deposit of pheromone concentration. They do not interact directly and act independently to accomplish the task.
6) Autonomy: No centralized control. No need to supervisor. They work for the colony and always strive to search food source around their colony.
7) Parallelism: Ants work independently and the task of searching food source is carried out by each ant in
parallelism. It is parallelism due to which they change their path, if a new food source is found near their colony. These characteristics of biological insects such as ants resemble the characteristics of MANETs.

C. Solving network routing using ACO:
Network routing is a big problem because network characteristics such as traffic load and network topology may vary randomly. The routing nature is matched by the multi agent nature of ACO algorithms [13]. The network can be represented by construction graph where the vertices correspond to set of routers and the links correspond to the connectivity among routers in that network. Now route finding problem is finding a set of minimum cost path between nodes present in the graph representation which can be done easily by the ant algorithms.

D. The properties of ant colony algorithm which is suitable for routing are [13]:
1) **Dynamic Topology**: this property is responsible for the bad performance of several routing algorithms in mobile multi-hop ad hoc network. The ant colony optimization meta-heuristic is based on agent systems and works with individual ants. This allows a high adaption to the current topology of the network.

2) **Link Quality**: It is possible to integrate to the connection/ link quality to the computation of the pheromone concentration, especially into the evaporation process. This will improve the decision process with respect to the link quality. It is here important to notice, that the approach has to be modified so that nodes can also manipulate the pheromone concentration independent of the ants, i.e., data packets, for this a node has to monitor the link quality.

3) **Support for multi-path**: Each node has a routing table with entries for all its neighbors, which also contains pheromone concentration. The decision rule, to select the next node, is based on the pheromone concentration on the current node, which is provided for each possible link. Thus, the approach supports multipath routing.

E. Exploration and Exploitation:
The success of any stochastic (random) search method heavily depends on striking an optimal balance between exploration and exploitation. These two issues are conflicting but very crucial for all the meta-heuristic algorithms. Exploitation is to effectively use the good solutions found in the past search whereas exploration is expanding the search to the unexplored areas of the search space for promising solutions. The intensification of the pheromone trail by the artificial ants exploits the good solution found in the past. However, excessive reinforcement may lead to premature convergence. To maintain the diversity in the search space the following methods are suggested:

(a) Control the exponent of the pheromone trail.
(b) Introduction additional randomization in the ants’ decision process.

3. Ant Based Algorithms
3.1 Ant Based Control Algorithm
Ant Based Control algorithm is a one of the swarm intelligence techniques [16, 17]. It was designed for load balancing and applied for a wired circuit switched network such as telephone networking. It is used for call controlling. The basic concept is mobile routing agents, because exploring the network and updating routing tables according to the current network state [21]. When this algorithm adaptive and exhibits robustness under various network condition is using many simple agents, called ants. An ant, modify the routing policy at every routing node by depositing a pheromone trail on routing table entries. The ants’ goal is to develop routing table, and performance is measured by the rate of accepting incoming calls.

Ant based control algorithm, used only one class of ants, called as FANTs. The class is initiated at regular time interval from every source node to a randomly chosen destination, when immediately update the routing tables for their source node. The meaning is that the pheromone to pointing to the previous node in the travelling time. The important thing is backward path is influenced.

3.2 Ant Routing Algorithm:
The principal of the ant colony optimization is that Meta heuristic is taken food from various places using searching behavior of real ants. Ant agents can be divided into two sections: FANT (Forward ANT) and BANT (Backward ANT).

It is used to creating new routes. The first one is called route discovery, which is used to discover routes from the source to destination node. The FANT is a small packet with a unique sequence number. Depending on the sequence number and the source address of the FANT, the duplicate packets can be distinguished by the nodes. The second one is called establishment. The ants follow the same path established by the FANTs in order to establish the final route from source to destination. In route maintenance phase, the routes need to be monitored and strengthen during the communication. Once the forward ant and backward ant have been established the pheromone tracks for the source and destination nodes, subsequent data packets are used to maintain the path [10].

How these agents are passing routing information to each other are as follows:
- Each network nodes start FANT to all destinations at regular time intervals.
- Ants find a path source to destination randomly based on current routing tables.
- The FANT to create a stack, pushing in trip times for every node as that node has reached.
- When destination is reached, the BANT inherit the stack.
- The BANT pop the stack entries and follows the path in reverse.
- The routing tables of each visited node are updated based on trip times.

1) Properties of ARA
The following requirements [15] are to fulfill the routing algorithm for mobile ad-hoc network. They are:
a) **Distributed Operation:** Each node have own a set of pheromone counter \(O_{ij}\) in its routing table for a link between node vi and vj. Each node controls the counter independently, when ants visit the node on route searches.

b) **Loop-Free:** The nodes register the unique sequence number of route finding packets, FANT and BANT. The loops will not be generated.

c) **Demand-based operation:** Routes are established by manipulating the pheromone counter \(O_{ij}\) in the nodes. While the amount of pheromone counter visits to zero, ants do not visit this node.

d) **Sleep period operation:** Nodes are able to sleep when their amount of pheromone reaches a threshold. Others node will not consider this node.

e) **Locality:** The routing table and the stochastic information block of node are local and they are transmitted to any other node.

f) **Multi path:** Each node maintains several paths to the destination. Each route depends on the environment.

g) **Sleep mode:** In this mode a node is snoops, only packets which are destined to it are processed, thus saving power.

Let us consider \(G = (V,E)\) be a connected graph with \(n = |V|\) nodes. The amount of pheromone that is \(O_{ij}\) is clue of the frequent usage of the link \(ij\). An ant positioned at node \(Vi\) make use of pheromone value \(O_{ij}\) of node \(Vj\) and \(Ni\) to calculate the probability of node \(Vj\) as next hop. \(Ni\) is the set of one-step neighbors of node \(Vi\).

\[
P_{ij} = \begin{cases} \frac{T(ij)}{\sum_{k \in Ni} T(ik)} & \text{if } j \in N_i \\ 0 & \text{if } j \notin N_i \end{cases}
\]

The transition probabilities \(p(i,j)\) of a node \(vi\) satisfies the constraint:

\[
\sum_{j \in N_i} p(i,j) = 1 , \ i \in [1,N]
\]

### 3.3 AntNet Algorithm

In AntNet algorithm design is based on the Ant colony optimization framework. An ant to exploits the mechanism for shortest path behavior, which is define a Nature-inspired Meta heuristic for combinatorial optimization. Some features are a multi agent organization, stigmergic communication among the agents, distributed operations, use of decision policy to develop solutions, stigmergic learning of the parameters of the decision policy, and so on. These features are applied with success to various combinatorial problems. In 1997, the first work on ACO algorithm for routing in packet-switched networks. AntNet, some interesting properties are to work fully distributed way, traffic changes and highly adaptive network, is lightweight mobile agents, provide multipath routing, and take care of data load spreading. In great majority of AntNet has outperformed all its competitors, and showing adaptively and robustness.

### 3.4 AntHocNet Algorithm

AntHocNet [Caro, Ducatelle and Gambardella] algorithm is a multipath routing algorithm for Mobile Ad hoc networks [21] inspired by ACO that combines both reactive and proactive components means it is hybrid in nature. It has forward ants and backward ants for both proactive and reactive components. There are four types of ants in this algorithm, such as forward reactive ants, forward proactive ants, backward reactive ants, and backward proactive ants. This algorithm searches for new path between source and destination. This is done in Reactive Route setup phase, where reactive forward ants are sending by the source node to find multiple paths towards the destination. Backward ants are used to setup the route. While the data session is open, paths are monitored, maintained and improved proactively using different agents, called as proactive forward ants [23].

To accumulate routing information, this algorithm used two complementary processes. First, the repetitive end-to-end delay using ant agents. Second, pheromone diffusion means that information bootstrapping process. An algorithm combines both processes that can obtain an information gathering process. A main big disadvantage is the number of routing messages sent from source to the destination through needs to be the network for establishing routes [12, 22].

### 3.5 PERA:

PERA is a Probabilistic Emergent routing algorithm for ad hoc networks based on the Swarm Intelligence paradigm described in [24,25] and [26]. In this approach, to use a flooding approach to carried out the process of route discovery and maintain different paths between source to destination. The algorithm used three kinds of agents or ants such as regular forward ants, uniform forward ants and backward ants. Regular and uniform forward ants are agents that are routing packets now broadcast rather than unicasts. These agents are explore and strengthens the path of the routers in which the data’s are transmitted. They create and adjust a probability distribution at each node for its neighbor’s nodes. The ants or agent packets are relatively small size and data packet transfer to destination by taking the neighbor as a next node.

Backward ants are to make use of information about collected by forward ants through the network. To adjust the routing table entries related to the existing network status. Assume that this algorithm is bidirectional links in the network.

### 4. Simulation Parameters

We defined the performance parameters which can be evaluated for the comparison of the ant based algorithms. Consider the following two types of traffic can be taken:

1. **Session oriented:** All packets have same destination for a given session.
2. **Session less:** Destination of each packet selected from uniform distribution.

The following parameters are

a) **Average Through put:** Through put is a measure of how much traffic is successfully received at the intended destination in a unit interval of time. A routing protocol should try to maximize this value.

b) **Packet Delay:** A good algorithm should be able to deliver packets with minimum delay.

c) **Session Delay:** Time is an important parameter to
complete a session. An application layer at the destination node only gets the packets after all the packets are received in the correct order. Packet delay factors out this waiting time and hence favors multi-path algorithms which deliver packets in an out-of-order manner but with smaller delays.

d) *Session Completed:* The percentage of sessions which are completed without any support from transport layer protocols. For example if only one packet in a session is dropped due to congestion or TTL expiration, we report the session as an incomplete one. This parameter reports the way packets were deleted due to congestion.

e) *Packet Delivery Ratio:* This measure tells us how many data packets are successfully delivered at their destinations. Under saturated loads a 1% improvement in packet delivery ratio at times means about few 100,000 more data packets delivered at their destination.

f) *Packet Drop Ratio:* The percentage of data packets that are dropped because their time to live timer value expired or the queue buffers were full.

g) *Packet Loop Ratio:* The percentage of data packets that followed a cyclic path. A cyclic path is an error in an algorithm and should be reported.

h) *Routing Overhead:* The ratio of the bandwidth occupied by the routing / control packets and the total available bandwidth in the network. This parameter shows the control overhead of the routing algorithm.

i) *Suboptimal Overhead:* The difference between the bandwidth consumed when transmitting data packets from source to destination and the bandwidth that would have been consumed should the data packets have followed the shortest hop count path.

5. **Comparison Of Different Ant Based Routing Algorithms**

Table 1 below gives the comparison between different ants based routing algorithms based on some resources used by them.

6. **Conclusion**

In this paper, an assortment of ant based routing algorithm are analyzed and compared in requisites of protocol attributes, performance metrics and network parameters. Many researchers have fascinated in Ants-Based routing algorithm because they are more robust, consistent, and scalable than other predictable routing algorithms. The foraging actions of the ant colonies has been comprehensively investigated for more than 50 years and has explored the extraordinary track systems achieved through dynamic, decentralized communication. This cooperative astuteness has been shown to be one of the best examples of self organization. Hence these analyses will helpful researchers to choose right routing protocol for their work according to network scenarios. Among wired networks AntNet is best for maintain the established paths as compared to ABC routing. The reason is ABC algorithm used greedy method. AntNet always choose best paths based on the probability. For wireless network, AntHocNet is more efficient to exploring new paths based on probability compared to other algorithm. The fact is very costly and requires more resources for implementing an algorithm. PERA is better for less cost and efficient in maintain and established new paths. ARA is similar to PERA, but in ARA both forward and backward ants update pheromone value.

7. **Future Work**

In this paper, we have presented an optimization on routing algorithm in terms of the network layer based on ant colony optimization. In our discussion by using ant colony optimization, we have been able to support multiple routes MANET. In most of the routing protocols they provided a single route to the destination. In our study it is able to establish multiple routes from source to destination. So we may find a PERA and ARA algorithm is better than the other ant algorithm. It may encourage future work to do solve link failure. Using this algorithm, through put, end-to-end delay parameters can be improved. Probably overhead parameters will also improve as control packets used in this case are only forward and backward ants. Extend to design more robust and secured ant routing protocol and we plan to simulate the same using NS2 simulator so that accurate outcome can be found.

8. **Acknowledgement**

We would like to thanks to the Principal, HOD and faculty members of P.G and Research Department of Computer Science and Research Scholars Government Arts College (Autonomous), Karur for their encouragement to publish this work.
### Table 1: Comparison between different Ants based Algorithm

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>ABC routing</th>
<th>ANNET</th>
<th>ARA</th>
<th>PERA</th>
<th>ANTHOCNET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Types of Ants</td>
<td>FANT</td>
<td>FANT, BANT</td>
<td>FANT, BANT</td>
<td>FANT, BANT</td>
<td>Reactive FANT and BANT, Proactive FANT and BANT</td>
</tr>
<tr>
<td>Ant Structure</td>
<td>Source IP address, Destination IP address, Age of Ant</td>
<td>Source IP address, Destination IP address, Sequence number, field identify as FANT or BANT, memory</td>
<td>Source IP address, Destination IP address, Sequence number, Hop count</td>
<td>Source IP address, Destination IP address, Stack, Hop Count, Sequence number</td>
<td>Source IP address, Destination IP address, Next Hop IP address, Stack, Hop Count, Sequence number</td>
</tr>
<tr>
<td>Routing Table Structure</td>
<td>Destination address, Next Hop, Pheromone value</td>
<td>Destination address, Each neighbor, Pheromone value</td>
<td>Destination address, Next Hop, Pheromone value</td>
<td>Destination address, Next Hop, Probability</td>
<td>Goodness of next hop, Destination address, Next Hop</td>
</tr>
<tr>
<td>Traffic Statistic Structure [ Mean variance, Best value of travel time ]</td>
<td>Not used</td>
<td>Used</td>
<td>Not used</td>
<td>Used</td>
<td>Used</td>
</tr>
<tr>
<td>Amount of control overhead used</td>
<td>Less than others</td>
<td>More than ABC but less than others</td>
<td>More than PERA but less than others</td>
<td>Least</td>
<td>Less than HOPNET but more than others</td>
</tr>
<tr>
<td>Nature of algorithm</td>
<td>Proactive</td>
<td>Proactive</td>
<td>Reactive</td>
<td>Proactive</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Path type</td>
<td>Single</td>
<td>Single</td>
<td>Multipath</td>
<td>Single</td>
<td>Single</td>
</tr>
</tbody>
</table>

*FANT: Forward Ant, BANT: Backward Ant

---

### References


