International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

A Trust Based Multipath Routing for Black Hole Attacks with Group Search Optimization Routing

G. Mahalakshmi, A.Suresh.

Abstract*: *The Mobile Ad hoc Network (MANET) is the collection of some mobile devices that communicate with one another without any help from a centralized administration. For this, the energy is an important issue that has to be addressed since the ad-hoc network nodes have a limited battery power. A secure routing in the MANETs is an area of research that is emerging. The designing of a security protocol which is trustworthy for the ad hoc routing is an extremely challenging task owing to all its unique traits. Due to its minimal configuration and its quick deployment, the MANETs are found to be well-suited for situations in the case of an emergency such as the natural disasters or the military applications. This way, a transfer of data among two nodes need some security. A MANET black-hole attack will occur owing to the malicious nodes attracting data packets by means of a false advertisement of a fresh route to its destination. For this work, the trust-based routing along with the packet forwarding probability. For this work, the Ad hoc On-Demand Multipath Distance Vector Routing (AOMDV) protocol is used and for finding the routing path a trust value will be piggybacked with a route request packet. There was yet another novel algorithm for optimization known as the Group Search Optimizer (GSO) algorithm that was proposed inspired by the behaviour of animals. This GSO-AOMDV was for the purpose of improving the performance of the network. The results of the experiment proved that this method proposed could achieve a better performance compared to the other methods.

Index Terms*: *Adhoc on-Demand Multipath Distance Vector Routing (AOMDV), Black Hole Attack, Group Search Optimization (GSO), Security, Trust and Mobile Ad hoc Network (MANET,.

I. INTRODUCTION

The Mobile Ad hoc Network (MANET) is that collection of terminals of digital data that was equipped with some wireless transceivers which communicate with each other without any infrastructure for fixed networking. This way the communication can be maintained by means of data packet transmission over a wireless channel that is common. In the absence of an infrastructure, like the base station array, the ad hoc networks have been made to be radically different from that of the other LANs. The ad-hoc network topology is dependent on the power of transmission during the time and location of mobile nodes that can keep changing. A major problem in an ad-hoc networking is its efficient data packet delivery to mobile nodes in which the topology has not been predetermined and the network has a certain centralized control. Thus, owing to the frequency in the change of topology, ad hoc networks are viewed to be a major challenge [1]. The major characteristics of the MANETs are as follows: The dynamic topologies: as the nodes are able to move freely and arbitrarily, the network topology can also randomly change in an unpredictable fashion. All links can either be unidirectional or even bi-directional. The bandwidth constrained variable capacity links: there are wireless links with lower capacity compared to their counterparts that are hardwired. Further, owing to multiple access available, conditions of interference, noise and fading, the wireless links will have a low throughput. The energy constrained operation: either some or all nodes found in a MANET are dependent on the batteries. For this scenario, there are some important criteria for system design in which the optimization can be for the conservation of energy. A limited physical security: the mobile networks will be prone to some physical threats to security compared to the fixed cable networks. There has been an increase in the chances of attacks of denial-of-service, spoofing, and eavesdropping [2]. The challenges faced by the MANETs: A limited bandwidth: on being compared to the wired networks, the wireless networks will continue having a lower capacity. The routing overhead: In the case of a wireless ad hoc network, there can be some unwanted routing overheads owing to random node movement generating stale routes within the routing table. The packet losses owing to errors of transmission: there is a higher packet loss found in the wireless ad hoc network owing to the hidden terminals. The limited capabilities of the mobile nodes: the limited capacity and the short battery life of the mobile nodes [3]. The ad hoc network routing protocols have been classified into two different approaches which are the proactive and the reactive routing protocols. In the former which is also called the table-driven approach, every node will maintain some routing information for every node within this network. all this information has been kept within the routing table that has been updated for each change in the topology of the network. As there is no process of route discovery needed, a proactive routing protocol will have rapid initiations. There is some periodic topology information exchange and in the case of the reactive routing protocol, every node will not need a maintenance of routing table.

Manuscript published on 30 September 2019.
***Correspondence Author(s)**
G. MAHALAKSHMI, Guest Lecturer, Computer Science, Muthurangam Govt. Arts College(Autonomous), Otteri, Vellore - 632 002, priyamahamga@gmail.com
Dr.A.SURESH , M.C.A., M.Phil., Ph.D., SET. PRINCIPAL, Computer Science, SIRI PSG College of Arts and Science for Women, Sankagiri.asuresh1975@yahoo.com

At the time a source node has some data to be sent, it will initiate the process of route discovery and will maintain the routes.

Thus, in spite of a delayed initiation of this session has been a result of route discovery and a reactive routing protocol can bring down the routing overhead and this was called an on-demand approach [4].

The multipath routing approaches have been introduced for finding multiple paths among the pairs of source destination. There are multiple routes found between the source-destination pair that provides various benefits like: a higher bandwidth utilization, a low end-to-end delay, a higher throughput, and a higher network life. This further applies the load balancing within the network, its congestion and its protection against all route failures. The mechanism of path discovery found in the multipath routings is very similar to the MANET and its single path routing. In most situations, this will choose all disjoint paths for carrying the traffic between the source and the destination forward. The multi-paths are of two different types: the link-disjoint and the node-disjoint. For a certain pair of source-destination(s-d), a set of the link-disjoint routes will contain paths that do not have a link which is in common compared to the constituent s-d path. Likewise, in an approach of a node-disjoint, there are paths without a common node and the MANET multipath protocols will compute many numbers of paths in a pair of source-destination. There is a new operation of route discovery that was initiated at the time all these paths had failed [5].

The Ad-hoc On-Demand Distance Vector Routing (AODV) based protocol that was on the basis of a reactive routing discovery employs three types of messages: The Route request (RREQ), the Route Reply (RREP) and the Route Error (RERR). Additionally, there is a destination of sequence numbers that have been used for ensuring a loop-freedom and for the AODV, every source will find another newer route by a limited flooding of the RREQ along with a ring expansion and this can obtain a route to the destination using the RREP. An AOMDV protocol can expand the AODV to its protocol of multipath routing wherein the source node tends to keep various routes from different RREPs. A static selection of routes of that of the AOMDV may not be able to handle any dynamic network change like a severe congestion that was caused due to a biased traffic [6].

Security techniques of the MANET have not be different from that of the other networks. The primary aim of such techniques was providing security from different attacks and their abnormal behaviour to the information and the resources. An effective technique of security will have to guarantee the security requirements below [7].

- Availability: the system guarantees availability of services to the network.
- Authentication: the system also provides some access to the known or authenticated nodes alone and the malicious nodes will not enter a system.
- Confidentiality of data: the system further guarantees either a message or a data packet that may not be understood by the other nodes and the data is thus encrypted by using certain cryptographic techniques.
- The integrity of data: the integrity of data will be the message or the data packet sent from a sender to a server which is not misused, modified or distorted.
- Non-repudiation: either a sender or a client may not be able to refute or even deny the fact that a data packet or a message had not been sent by him. A digital signature is used to guarantee non-repudiation.

Being an important concept in the security of the network, the trust has been interpreted to be a set of the relations among the nodes or the entities that participate in the activities of the network. The trust relations will be based primarily on the earlier behaviour or the entities or the nodes. The trust concept is similar to the one as in the case of real-life. The very purpose development of a notion of trust inside an ad hoc network was to be able to provide a new heuristic for the purpose of security. Permitting either the faulty or the malicious nodes to get detected and further removed from the network having a minimal restriction is made. There are three different definitions of trust which are as below [8]:

- Trust denotes the subjective probability of a certain entity which expects another entity to perform a certain action upon which its welfare is dependent. The first one is called the trustor and the other the trustee.
- A direct trust indicates the belief of the entity and its trustworthiness in a certain interaction for a particular direct experience.
- A recommendation trust is the one where there is one entity that believes another entity in relation to their results of the evaluation.

For this work, the multipath routing along with the GSO algorithm for the MANET is used. The rest of the investigation has been organized thus: Section 2 will discuss the works that are related in the literature. Section 3 gives explanations of different methods that are used in this work. The experimental results are discussed in Section 4. The conclusion is made in Section 5.

II. RELATED WORK

Zhou et al., [9] have been improving the performance of the AOMDV protocol making use of the AOMDV that is based on the Node state (NS-AOMDV). In the NS-AOMDV, a node state for improving performance is introduced. In the process of route discovery, a routing update rule will calculate the weight of the node and will sort the path weight by means of a descending value. The NS-AOMDV makes use of the RREQ packet delay forwarding and the energy threshold for easing congestion of the network. This is for avoiding the low nodes for participating in the path of this establishment.

Amirtharaj et al., [10] had made an investigation of the problem of this cryptographic key authentication found in a MANET. Employing the digital trust theory, the work had proposed a scheme of authentication for the MANETs which includes a new hybrid trust model that is between the direct and the indirect approaches. Trust data is supplied to decentralized webs by the trust model.

Retrieval Number: K24830981119/19©BEIESP
DOI: 10.35940/ijitee.K2483.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The work further ran into certain simulations belonging to the scheme of authentication for the purpose of verifying the security and also for investigating its potential trust based threshold values.

Furthermore, the authors had also designed and implemented an iOS application called the proof-of-concept for implementing the scheme of authentication. There is some future work which includes many different implications of the aspect of mobility of the MANETs on the trust management like the maximum levels of its trust concentration.

Muhammad et al., [11] had proposed a new Subjective Logic (SL) model to handle the ignorance between the ad hoc network and the neighbour nodes. A Trust Model that is based on the SL has been applied to the multi-path routes found in a distributed environment for knowing if there is an uncertainty between all random entities. For this work, the SL is highlighted and evaluated in order to provide a selection operator as its SL extension. By means of employing the subjective opinion nodes, a trust evaluation can be made with regards to both first hand and second-hand information. The results will be simulated and then validated and once the results are calculated on the basis of the trust judging algorithm, a path with a higher value of the trust is chosen for purposes of communication.

Jain et al., [12] had presented a Trust based AODV (TAODV) protocol of routing that handled the effect of the Black Hole Attack. In an indoor environment, in case the node mobility and its behaviour were based on the Gauss Markov mobility with its exponential condition of traffic has been preferred for achieving the best Packet Delivery Ratio (PDR) and the throughput results.

Jhaveri and Patel [13] had addressed the issue using a trust-model that was integrated along with a pattern of attack and its technique of discovery. As an extension of the AODV routing protocol, a trust-based scheme was found which adopted a mechanism of pattern discovery for detection of suspicious activities which are from the malevolent nodes even before they begin dropping the data packets. The work further presented a new and detailed mode of operations for three adversary models that launch different misbehaviour or packet forwarding. The experimental results and their theoretical analysis had proved that the method of pattern discovery integrated with the trust-based model had provided the adversaries to follow patterns of attack and thus weaken their effects of damage compared to the solitary trust-based model.

Mukherjee et al., [14] had proposed a routing protocol that was trust-based called the Enhanced Average Encounter Rate-AODV (EAER-AODV) which had employed a trust model based on the opinion of the nodes. In the case of an EAER-AODV, the opinion indicates the trust among the nodes that are frequently updated in accordance with the specification of the protocol. The trust based on a recommendation was used for exchanging the information of trust made among the nodes. For this protocol, the node will choose a routing path in accordance with the trust values of the neighbouring nodes. there was some extensive analysis of simulation made to prove that the EAER-AODV was able to avoid effectively all malicious nodes and the nodes with a frequent mobility for choosing routes. It has been shown that the EAER-AODV may be duly compared to the currently existing methods that prove its efficacy. An Optimized Link State Routing (OLSR) protocol suffered from various security threats that were difficult to resist through mechanisms of security. Tan et al., [15] further proposed a new mechanism of routing based on trust for alleviating such issues. For this mechanism, a model of trust reasoning which was based on the Fuzzy Petri Net (FPNT) had been presented for the evaluation of the trust values of these mobile nodes. additionally, for avoiding the malicious or the compromised nodes, there was an algorithm that was trust-based proposed to choose a path having a maximum value of path trust among all the possible paths. After this, an extension of the OLSR was made using the trust model and the routing algorithm known as the FPNT-OLSR. The results of a simulation proved that the FPNT-OLSR was quite effective in their establishment of secure routes.

Banerjee et al., [16] had further presented another new on-demand power-balanced algorithm for the mobile and the multi-hop ad-hoc networks. This protocol has been based on a swarm intelligence technique primarily on the metaheuristics based on the ant colony. All these approaches attempt at mapping the capability of the swarms to find solutions to both engineering and mathematical problems. This method is adaptive, scalable and also efficient. The results of simulation prove that this method proposed was quite different from that of the currently existing protocols.

Robinson and Rajaram [17] had proposed another Energy-aware multipath routing scheme that was based on the Particle Swarm Optimization (EMPSO) using a Continuous-Time Recurrent Neural Network (CTRNN) that solved the problems of optimization. The CTRNN further identifies an optimal path that is loop-free in order to solve the MANETs and their link disjoint paths. In the CTRNN, a Particle Swarm Optimization (PSO) based method is mainly used to train a Recurrent Neural Network (RNN). This scheme proposed made use of measures of reliability like optimal traffic ratio, energy factor, and cost of transmission. For this scheme, all optimal loop-free paths were found by employing the PSO to look out for better quality nodes in the phase of route discovery.

A routing in the case of multicasting will involve the maintenance of routes and the finding of newer locations which is Non-Deterministic Polynomial (NP)-complete owing to the network's dynamic nature. Rajan and Shanthi [18] had proposed another genetic-based optimization for an algorithm of multicast routing. This algorithm also made use of the best features belonging to a Genetic Algorithm (GA) and the PSO for improving such solutions. The simulations had been conducted using different numbers of mobile nodes and their results had been compared with the Multicast AODV (MAODV) protocol, the GA-based solutions and the PSO-based solutions. This optimization further improves the PDR, the end-to-end delay and the jitter with a faster convergence.

III. METHODOLOGY

A detection of the black hole attack with the AOMDV protocol, the trust model and the GSO algorithm methods have been discussed in this section.

A. Black Hole Attack

The Black hole attack is an attack of a special type which occurs normally in the reactive protocols. The black-hole node has been a malicious node attracting packets by claiming it has a short and fresh route for reaching a destination after which it drops the packets. All Black hole nodes perform different actions that are harmful within the network which is [19]:

- It behaves like a source node by means of falsifying an RREQ packet.
- It also behaves like a destination node by falsifying an RREP packet.
- It decreases the hop count numbers while forwarding an RREQ packet.

Here for this approach, in case the ratio of the packets received to the packets sent have been lower than the threshold and this way the destination node begins the process of detection. The primary difference between the packets received by the node and the actual number of packets are forwarded by a significant node. In this case, the node will be the malicious node which is isolated from its network.

The process of route discovery in the AODV is quite vulnerable to a black hole attack and this mechanism will be of an intermediate node that can respond to an RREQ message with a route that is fresh enough and is devised for reducing the delay in routing. For this attack, at the time the malicious nodes listen to RREQ that are in a network, it will respond having the shortest and also the freshest route to its destination node. The malicious nodes will direct the network traffic and will drop the packets transitory [20].

B. Adhoc on-Demand Multipath Distance Vector Routing (AOMDV)

An AODV protocol will begin with a process of route discovery using a Route REQuest (RREQ) for the entire network. As soon as a non-duplicate RREQ has been received, all intermediate nodes will record the earlier hop and will check for a valid and also a fresh route entry. The route will send a Route REPly (RREP) with another unique sequence number. While updating its route information, it will propagate a route reply and will get some additional RREPs in case the RREP which will have a sequence number for a larger destination or even a shorter route that is found. For the purpose of eliminating the frequent failures of the link and the route breaks found in ad hoc networks that are highly dynamic, the AOMDV has now developed from the unipath on-demand routing protocol, the AODV [21].

An AOMDV has multiple paths involving two stages as below:

- The route update rule establishes and maintains loop-free paths for nodes.
- A new distributed protocol to find the link-disjoint paths.

A protocol of AOMDV will find the node-disjoint or the link-disjoint routes. The link failure can occur owing to node mobility, traffic congestion, packet collision, and node failure. To find the routes of node-disjoint, every node will be obtained using an RREQ, that arrives from another neighbour as the nodes may not be able to broadcast any duplicate RREQs. Two different RREQs will arrive at the intermediate node. For the purpose of getting many link-disjoint routes, the destination will send the RREP for duplicating the RREQs irrespective of the first hop. To ensure the link-disjointness, a destination will reply to the RREQs using unique neighbours. They follow reverse paths that are the node-disjoint and so the link-disjoint after its first hop. Every RREP intersects the intermediate node and takes a new reverse path to its source for ensuring its link-disjointness.

The primary idea behind a multipath routing was to look for multiple routes. There may be plenty of reasons for this and this can bring down an end-to-end delay even before the like used disappears. The advantages of the AOMDV protocol [22]: it can establish a route on demand. It creates nodes that are loop-free. It maintains a level of connectivity. It is fast and is also efficient in recovering from failures. The primary disadvantage of using this was that it has overheads at the time of route discovery owing to an increase in the flooding as it had a routing protocol where the destination replied to multiple RREQs having results in overhead packets which were longer which was in response to a single packet of RREQ resulting in a heavy overhead control.

C. Trust Model

In the MANET, a trust may be defined to be a level of its belief in accordance with the node behavior (or the entities/agents). A probability value of the trust that varies between 0 to1, wherein the 0 represents DISTRUST and 1 TRUST. The primary goal of this trust model was the provision of a combined solution that prevents malicious activities and some uniform utilization of resources by means of load balancing of packets that were forwarded. The model represents the manner in which trust can be calculated for the routing path by means of employing a trust value of the individual nodes. This trust model had created a new relationship between the metrics of trust and their network statistics. The primary contribution was the provision of uniform energy consumption solutions for increasing the lifetime of the network [23]. A trust model primarily consists of two different phases which are: the formation of trust and the usage of trust for the routing decisions. In the former phase, every node will collect network statistics such as packets that are forwarded, the packets that are dropped and the packets that were delayed. This is used only when the routing path consists of the node to be an intermediate one. As soon as the route from its source to the destination has been requested, intermediate nodes will be calculated from their respective trust values using equation (1):

$$T = \sum_{i=0}^{n} a_i p_i \qquad (1)$$

In which the n denotes the parameters, the a_i denotes a weighting factor of the i-th parameter and the p_i denotes a trust value of the i-th parameter.

The parameters are then analyzed such as the data packets that are dropped and forwarded and the remaining energy. All of these parameters will be useful for the prevention of malicious activities and are also used for the determination of their resource utilization, link reliability, congestion, and health. The legitimate nodes then perform flooding, requests for route initiation and also initiate route errors. So the trust model further includes the weightage of every parameter by means of considering the parameter and its effect on the network performance. A malicious node will perform the flooding and will also initiate the requests. This keeps the legitimate nodes more than that of the malicious nodes.

A direct trust representation and its computation

From the node N_J to N_i a direct trust has been represented as TR_D^{ij} and direct trust is as per (2) [24]:

$$TR_D^{ij} = \frac{t_m + a/2}{t + a} \; t_m, t \geq 0, \; a > 0 \tag{2}$$

Where there is not earlier interaction between that of mode N_J and N_i. the t denotes time transactions, t_m denotes a time success and the a denotes a positive real number. a will be inversely proportional to the model's evidence.

The recommendation of the representation and calculation of the trust value.

This is denoted as the t is denoted as TR_r^j and is calculated as per (3):

$$TR_r^j = \frac{\sum_{i=1}^{t} TR_D^{hi}.TR_D^{ij}}{\sum_{i=1}^{t} TR_D^{hi}} \; where \; TR_D^{hi} > H, \; i \neq j \tag{3}$$

TR_D^{hi} denotes the aggregation weight (a direct trust value for node N_i, which is computed using packets), TR_D^{ij} denotes the recommendation information of direct trust and the n denotes the current packets and their nodes.

The representation of total trust and its computation

This has been represented as $\Gamma(N_i, N_j)$ and is computed as per (4):

$$\Gamma(N_i, N_j) = \alpha TR_D^{ij} + \beta TR_r^i \tag{4}$$

Wherein the $\alpha, \beta \geq 0$ and the $\alpha + \beta = 1$. TR_D^{ij} denote the direct trust existing between the nodes N_i and N_j, α denote the impact weight belonging to the direct trust and the β denotes the impact weight for the recommendation trust.

D. Proposed Group Search Optimization (GSO) Algorithm

The GSO is a protocol for the population-based optimization and this uses the model known as the Producer-Scrounger (PS) along with the method of animal scanning. The PS as the optimal search design has its inspiration from the behavior of animal searching and theories of group living. There are two different methods of foraging, the producing (looking for food) and the scrounging (combining all resources that are discovered by the others) which are adopted by a protocol. The GSA further uses the method of ranger foraging. The GSO protocol's population is called the group and the individuals its members [25].

The GSO algorithm population is known as the group and every individual as its member. Within an n-dimensional space of search, its i_{th} member at its k_{th} searching bout (the iteration), will have a current position $X_i^k \in R^n$, a new head angle $\varphi_i^k = \left(\varphi_{i_1}^k, ..., \varphi_{i_{(n-1)}}^k\right) \in R^{n-1}$ and also a head direction $D_i^k\left(\varphi_i^k\right) = \left(d_{i_1}^k, ..., d_{i_n}^k\right) \in R^n$ that may be computed from the φ_i^k through a Polar to a Cartesian co-ordinates based transformation as per equation (5):

$$d_{i_1}^k = \prod_{q=1}^{n-1} \cos\left(\varphi_{i_q}^k\right)$$

$$d_{i_j}^k = \sin\left(\varphi_{i_{(j-1)}}^k\right) \cdot \prod_{q=j}^{n-1} \cos\left(\varphi_{i_q}^k\right) \quad (j = 2, ..., n-1)$$

$$d_{i_n}^k = \sin\left(\varphi_{i_{(n-1)}}^k\right) \cdot \tag{5}$$

For instance, within a 3-D search space, where the *k*th searching bout, an *i*th member and its head angle will be $\varphi_i^k = (\pi/3, \pi/4)$, by using this will obtain the unit vector of the direction of search $D_i^k = \left(1/2, \sqrt{6}/4, \sqrt{2}/2\right)$.

For the GSO, there is a group with three types of members. They are the producers, the scroungers, and the dispersed members. To aid computation, the PS model is simplified by making an assumption that there can be only one single producer and the rest of the members will be either the scroungers or the dispersed members. A simple policy of joining assuming that the scroungers join a resource which is identified by a producer has been used. For the problems of optimization, an optimum that is unknown is considered to be the open patches that are distributed randomly within the search space. The members of the group will look out for these patches in the search space. There is also an assumption that the producer and also the scrounger is not any different in their phenotypic traits. So, they may also be able to switch roles. For every iteration, the most promising area is identified and the best fitness value is determined to choose the producer. An important component for the orientation of search is scanning and this has a set of mechanisms that move the sensory receptors as well. Scanning is duly accomplished by means of physical contact or also by auditory, chemical or visual mechanisms. For a GSO vision, the scanning mechanism is used by several species of animals and is employed by producers. For performing the visual searches, animals encode a larger field with the retinas and variable spatial resolution using eye movements of a high speed for directing the regions of its highest resolution towards its target location.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

For the GSO, in its kth iteration, a producer X_p will behave as below [26].

1) The producer scans at a zero degree and will laterally scan by means of sampling three points in the field of scanning: one point at the zero degrees as in (6):

$$X_z = X_p^k + r_1 l_{\max} D_p^k \left(\varphi^k\right) \quad (6)$$

The one point found in the right-hand side hypercube is as per (7):

$$X_r = X_p^k + r_1 l_{\max} D_p^k \left(\varphi^k + r_2 \theta_{\max} / 2\right) \quad (7)$$

The one point found in the left-hand side hypercube will be as in (8):

$$X_l = X_p^k + r_1 l_{\max} D_p^k \left(\varphi^k - r_2 \theta_{\max} / 2\right) \quad (8)$$

Wherein the $r_1 \in R^1$ denotes a random number normally distributed with a mean 0 and a standard deviation which is 1 and $r_2 \in R^{n-1}$ which is a random sequence distributed uniformly within the range (0, 1).

2) A producer finds the best point having the best resource (the fitness value). In case the best point has a resource that is better than that of its current position, then it tends to fly to this particular point. Else it stays in the current position and will turn its head into an angle generated randomly as per (9):

$$\varphi^{k+1} = \varphi^k + r_2 \alpha_{\max} \quad (9)$$

Wherein $\alpha_{\max}$ denotes the angle of maximum turning.

3) In case the producer is not able to find an area that is better after a certain a iteration, it heads back to a zero degree as per (10):

$$\varphi^{k+a} = \varphi^k \quad (10)$$

Wherein the a ∈ R^1 denotes a constant.

At the time of a searching bout [27], there are members of the group that are chosen as the scroungers. These scroungers keep looking out for some opportunities for joining the resources that are found by producers. For their seminal work on a PS model, an observation was made by Barnard and Sibly with basic strategies in the house sparrows (Passer domesticus). 1) the area copying: denoting moving across for searching the immediate area surrounding the producer; 2) Following: this denotes following any other animal without exhibiting a search behavior; 3) Snatching: taking a direct resource from a producer. For the GSO algorithm, there is only area copying and this is very common as a scrounging behavior in the sparrows and for the kth iteration, the behavior of area copying of that of the ith scrounger will be a random walk to the producer as per (11):

$$X_i^{k+1} = X_i^k + r_3 \circ \left(X_p^k - X_i^k\right) \quad (11)$$

Wherein the $r_3 \in R^n$ denotes a uniform sequence that is within the range (0, 1). The operator "∘" denotes a product of Hadamard or Schur that computes the product of both vectors. At the time of scrounging, its ith scrounger will look out for other opportunities for it to join. This behavior was modelled by converting the ith scrounger and its head to an angle generated randomly by using (9).

In a GSO search process, in case a scrounger finds a location which is better compared to the current producer its next bout of search will be to be a producer and all other members that include the producer perform strategies of scrounging. This mechanism of switching will help the group escape from the local minima in the earlier bouts of search. The remaining members are dispersed from all of their present positions. The group members have various searching abilities and the less efficient foragers other than those that are dominant are dispersed. There are several forms of dispersions ranging from the simple insects to the human beings. The animals that are dispersed can adopt a behavior of ranging and this is the initial phase of the search that has no cues resulting in a particular resource. In the case of a GSO algorithm, in case the ith group member gets dispersed it performs a ranging. This will call and disperse the member rangers. These ranging animals will perform strategies of search that include the random walks along with systematic strategies of a search for locating the resources in an efficient manner. The random walks that are considered to be as effective as the methods of search for the resources distributed randomly were employed by rangers. For the k-th iteration, a random head angle φ_i in (9); and a random distance as in (12).

$$l_i = a \cdot r_1 l_{\max} \quad (12)$$

Then it is moved to its new point as in (13):

$$X_i^{k+1} = X_i^k + l_i D_i^k \left(\varphi^{k+1}\right) \quad (13)$$

For maximizing the chances of finding the resources, the animals make use of various strategies for restricting their search to a patch that is profitable. An important strategy was to turn it back into a patch at the time an edge has been detected. The strategy was employed by the GSO for handling the bounded search space: this is when the member is found outside the space and then turns back within the search space setting variables violating bounds to the earlier values. This proposed algorithm has been based on the protocol of AOMDV with a group search to be its PS mode. The nodes in this network were asynchronously and periodically sent out as group members to the destination nodes. All group members will be the small control packets that have the primary task of finding the destination and then gather information regarding this. The message packets of the RREQ are called the PS model in relation to a standard algorithm of the GSO that is used. The choice of the path of transmission will dynamically go through some regular updating of the model of PS which has a path of transmission expecting to improve the performance of routing [28].

IV. RESULTS AND DISCUSSION

In this section, the AOMDV-5% and 10% malicious and GSO-AOMDV-5% and 10% malicious methods are used. The PDR, average end to end delay, average number of hops to destination and percentage of malicious node detected as shown in Tables 1 to 4 and Fig 1 to 4.

Table 1 Packet Delivery Ratio for GSO-AOMDV-5% Malicious

Node Pause time (s)	AOMDV-5% Malicious	AOMDV -10% Malicious	GSO-AOMDV-5% Malicious	GSO-AOMDV-10% Malicious
10	0.6272	0.6111	0.7615	0.757
30	0.681	0.673	0.8663	0.8156
50	0.7079	0.6876	0.8932	0.8698
70	0.7242	0.7003	0.9024	0.8712
90	0.7865	0.7386	0.9189	0.8425

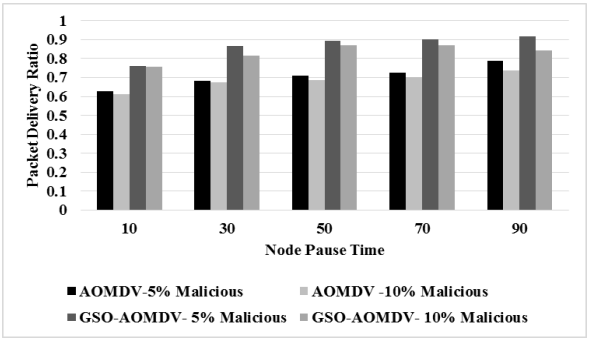

Fig 1 Packet Delivery Ratio for GSO-AOMDV-5% Malicious

From the Fig 1, it can be observed that the GSO-AOMDV-5% malicious has higher PDR by 19.34%, 21.91% & 0.59% for 10 node pause time, by 23.95%, 25.11% & 6.02% for 30 node pause time, by 23.14%, 26.01% & 2.65% for 50 node pause time, by 21.91%, 25.21% & 3.51% for 70 node pause time and by 15.52%, 21.75% & 8.67% for 90 node pause time when compared with AOMDV-5% malicious, AOMDV-10% malicious and GSO-AOMDV-10% malicious.

Table 1 Average End to End Delay for GSO-AOMDV-5% Malicious

Node Pause time (s)	AOMDV-5% Malicious	AOMDV -10% Malicious	GSO-AOMDV-5% Malicious	GSO-AOMDV-10% Malicious
10	0.0186	0.0121	0.0079	0.0135
30	0.0057	0.002	0.0013	0.0044
50	0.004	0.0019	0.0013	0.0029
70	0.0019	0.0017	0.0011	0.0013
90	0.0015	0.0014	0.0009	0.0011

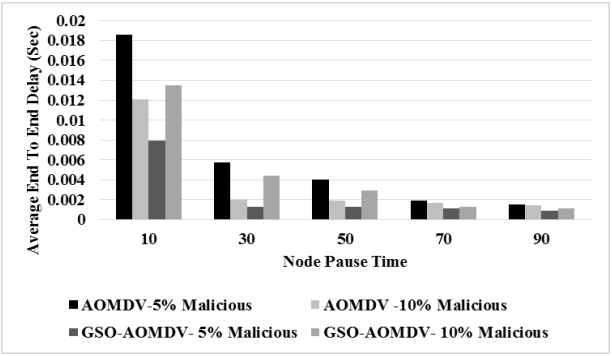

Fig 2 Average End to End Delay for GSO-AOMDV-5% Malicious

From the Fig 2, it can be observed that the GSO-AOMDV-5% malicious has lower average end to end delay by 80.75%, 42% & 52.33% for 10 node pause time, by 125.71%, 42.42% & 108.77% for 30 node pause time, by 101.88%, 37.5% & 76.19% for 50 node pause time, by 53.33%, 42.85% & 16.66% for 70 node pause time and by 50%, 43.47% & 20% for 90 node pause time when compared with AOMDV-5% malicious, AOMDV-10% malicious and GSO-AOMDV-10% malicious.

Table 2 Average Number of Hops to Destination for GSO-AOMDV-5% Malicious

Node Pause time (s)	AOMDV-5% Malicious	AOMDV -10% Malicious	GSO-AOMDV-5% Malicious	GSO-AOMDV-10% Malicious
10	7.8	7.4	5.5	6
30	7.1	7	5.4	5.4
50	6.4	6.6	4.6	5
70	5.6	5.9	4.9	4.9
90	3.8	4.3	3.5	3.1

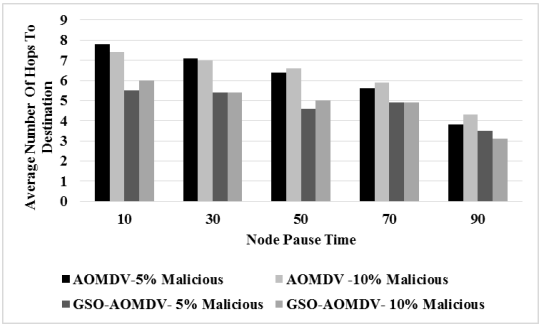

Fig 3 Average Number of Hops to Destination for GSO-AOMDV-5% Malicious

From the Fig 3, it can be observed that the GSO-AOMDV-5% malicious has lower average number of hops to destination by 34.58%, 29.45% & 8.69% for 10 node pause time, by 27.2%, 25.8% & same value for 30 node pause time, by 32.72%, 35.71% & 8.33% for 50 node pause time,by 13.33%, 18.51% & same value for 70 node pause time and by 8.21%, 20.51% & 12.12% for 90 node pause time when compared with AOMDV-5% malicious, AOMDV-10% malicious and GSO-AOMDV-10% malicious.

Table 3 Percentage of Malicious Node Detected for GSO

	Trust-5%	Trust-10%
Percentage	86	89

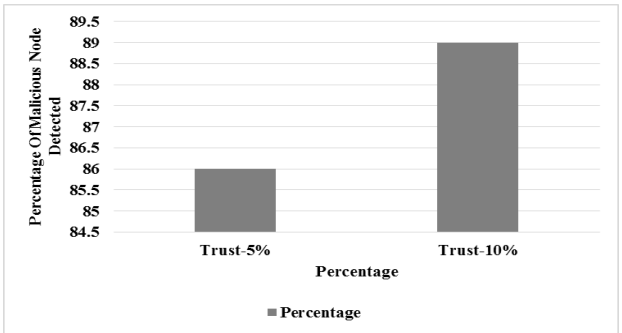

Fig 4 Percentage of Malicious Node Detected for GSO

From the Fig 4, it can be observed that the trust-10% of malicious nodes has higher percentage of malicious nodes detected by 3.42% compared for trust-5% of malicious nodes.

Retrieval Number: K24830981119/19©BEIESP
DOI: 10.35940/ijitee.K2483.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

V. CONCLUSION

Security has been an active topic of research and here the proposed AOMDV based trust model with the GSO algorithm will improve the performance of the security. This protocol is an extension of the AODV protocol that computes many loop-free and the paths of link disjoint. The trust measures its direct trust and for every node, the trust value is incremented on the successful packet forwarding. The primary aim of this was to optimize the consumption of energy for increasing the lifetime of this network and also for decreasing the nodes, their malicious activities and their effect. A GSO algorithm has been based on the model of PS assuming that members of the group will search for the finding (the producer) or for the joining (the scrounger) opportunities. On the basis of this framework, the animal search behaviour has been employed in a metaphorical manner to design a strategy of optimum search to solve problems of continuous optimization. The results have shown that a GSO-AOMDV-5% malicious has a higher PDR by about 19.34%, 21.91% and 0.59% for the 10 node pause time, by about 23.95%, 25.11% and 6.02% for the 30 node pause time, by about 23.14%, 26.01% and 2.65% for the 50 node pause time, by about 21.91%, 25.21% and 3.51% for the 70 node pause time and finally about 15.52%, 21.75% and 8.67% for the 90 node pause time on being compared to the AOMDV-5% malicious, the AOMDV-10% malicious and the GSO-AOMDV-10% malicious.

REFERENCES

1. Oli, P., & Gupta, V. K. (2014). Simulation and Comparision of AODV and AOMDV Routing Protocols in MANET. International Journal of Engineering Research & Technology (IJERT), ISSN, 2278-0181.
2. Dahiya, P., Madan, G., & Gupta, R. (2014). Performance evaluation of AODV and AOMDV on the basis of throughput. International Journal of Computer Science and Mobile Computing, 3(9).
3. Raza, N., Aftab, M. U., Akbar, M. Q., Ashraf, O., & Irfan, M. (2016). Mobile ad-hoc networks applications and its challenges. Communications and Network, 8, 131-136.
4. Shin, D., Lee, J., & Kim, J. (2009). A2OMDV: An adaptive ad hoc on-demand multipath distance vector routing protocol using dynamic route switching. Journal of Engineering Science and Technology, 4(2), 171-183.
5. Manohari, P. K., & Ray, N. K. (2015, October). EAOMDV: An energy efficient multipath routing protocol for MANET. In Power, Communication and Information Technology Conference (PCITC), 2015 IEEE (pp. 710-715). IEEE.
6. Balakrishna, R., Rao, U. R., & Geethanjali, N. (2010). Performance issues on AODV and AOMDV for MANETS. International Journal of Computer Science and Information Technologies, 1(2), 38-43.
7. Verma, J., Shukla, P. K., & Pandey, R. (2016). Survey of various Trust based QoS aware Routing Protocol in MANET. traffic, 137(3).
8. Babu, B. S., & Venkataram, P. (2011). A trust model for routing in MANETs: A cognitive agents based approach. In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
9. Zhou, J., Xu, H., Qin, Z., Peng, Y., & Lei, C. (2013). Ad hoc on-demand multipath distance vector routing protocol based on node state. Communications and Network, 5(03), 408.
10. Amirtharaj, I., Bonilla, E., & Newton, P. (2017). Design and Implementation of a Direct/Indirect Hybrid Trust Model for Secure Authentication in a Mobile Ad Hoc Network.
11. Muhammad, S., Wang, L., & Yamin, B. (2017, October). Trust Model Based Uncertainty Analysis Between Multi-path Routes in MANET Using Subjective Logic. In China Conference on Wireless Sensor Networks (pp. 319-332). Springer, Singapore.
12. Jain, A., Prajapati, U., & Chouhan, P. (2016, March). Trust based mechanism with AODV protocol for prevention of black-hole attack in MANET scenario. In Colossal Data Analysis and Networking (CDAN), Symposium on (pp. 1-4). IEEE.
13. Jhaveri, R. H., & Patel, N. M. (2017). Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. International Journal of Communication Systems, 30(7), e3148.
14. Mukherjee, S., Chattopadhyay, M., Chattopadhyay, S., & Kar, P. (2018). EAER-AODV: Enhanced Trust Model Based on Average Encounter Rate for Secure Routing in MANET. In Advanced Computing and Systems for Security (pp. 135-151). Springer, Singapore.
15. Tan, S., Li, X., & Dong, Q. (2015). Trust based routing mechanism for securing OSLR-based MANET. Ad Hoc Networks, 30, 84-98.
16. Banerjee, S., Majumdar, A., Saha, H. N., & Dey, R. (2015, October). Modified Ant Colony Optimization (ACO) based routing protocol for MANET. In Computing and Communication (IEMCON), 2015 International Conference and Workshop on (pp. 1-7). IEEE.
17. Robinson, Y. H., & Rajaram, M. (2015). Energy-aware multipath routing scheme based on particle swarm optimization in mobile ad hoc networks. The Scientific World Journal, 2015.
18. Rajan, C., & Shanthi, N. (2015). Genetic based optimization for multicast routing algorithm for MANET. Sadhana, 40(8), 2341-2352.
19. Rashmi, A. S. (2014). Detection and prevention of black-hole attack in MANETS. International Journal of Computer Science Trends and Technology (IJCST)-Volume, 2, 204-209.
20. Raja, L., & Baboo, S. S. (2014). An overview of MANET: Applications, attacks and challenges. International Journal of Computer Science and Mobile Computing, 3, 408-417.
21. Brindha, G. S., & Rajeswari, M. (2014). AOMDV-multipath routing protocol in mobile networks to enhance network security. Int. J. Sci. Res, 3(12), 62-66.
22. Aggarwal, I., & Garg, E. P. (2013). AOMDV Protocols in MANETS: A Review. International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016), 32.
23. Patel, V. H., Zaveri, M. A., & Rath, H. K. (2015). Trust based routing in mobile ad-hoc networks. Lecture Notes on Software Engineering, 3(4), 318.
24. Dalal, R., Khari, M., & Singh, Y. (2012). Different ways to achieve Trust in MANET. International Journal on AdHoc Networking Systems (IJANS), 2(2), 53-64.
25. Shen, H., Zhu, Y., Niu, B., & Wu, Q. H. (2009). An improved group search optimizer for mechanical design optimization problems. Progress in Natural Science, 19(1), 91-97.
26. He, S., Wu, Q. H., & Saunders, J. R. (2009). Group search optimizer: an optimization algorithm inspired by animal searching behavior. IEEE transactions on evolutionary computation, 13(5), 973-990.
27. He, S., Wu, Q. H., & Saunders, J. R. (2006, July). A novel group search optimizer inspired by animal behavioural ecology. In Evolutionary Computation, 2006. CEC 2006. IEEE Congress on (pp. 1272-1278). IEEE.
28. Kanani, C., & Sinhal, A. (2013). Ant Colony Optimization based modified AOMDV for multipath routing in MANET. International Journal of Computer Applications, 82(10)

AUTHORS PROFILE

Chandrakala H L. Received B.E in CSE from Malnad College of Engineering ,Hassan, M.TECH IN CSE from VTU study center ,BMS College Of Engineering ,Bangalore. PhD in CSE from from VTU-RRC. He is now working as Associate professor of HKBK College of Engineering, Bangalore. His Academic experience is 23 years. He published his research work in 2 journals and attended Seminars and workshops.

Dr. Loganathan R. Received B.E in CSE from Bharathiar University, Coimbatore, M.TECH IN CSE CSE] from Visvesvaraya Technological University, Karnataka. PhD in CSE from from Sathyabama University, Chennai. He is now working as Professor and HOD/CSE of HKBK College of Engineering, Bangalore. His Academic experience is 20 years. He published his research work in several journals and conferences.

Retrieval Number: K24830981119/19©BEIESP
DOI: 10.35940/ijitee.K2483.0981119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)