Journal of Engineering and Applied Sciences 14 (18): 6675-6684, 2019
ISSN: 1816-949X

SAMR: Discovery of Short Distance and Secured Routing in MANET

[1]Jayanthi Chandrashekar and [2]Arun Manoharan
[1]Department of Electronics and Communication Engineering, Vemana Institute of Technology, #1, Mahayogi Vemana Road Koramangala, 560034 Bangalore, Karnataka, India
[2]SENSE, VIT University, 632006 Vellore, Tamil Nadu, India, jayansri@yahoo.com

Abstract: Mobile Ad hoc Network (MANET) faces significant problem and challenges in multiple path routing over wireless communication compared to the wired network. Routing is one of the important protocol and acts as a major connection between the nodes for providing reliable and effective communication in MANET. It is hard to implement a secure routing protocol for various attacks due to its several potential MANET security threats and network environments. A bio-inspired routing protocol was used in this study by incorporating swam based approach for an identification of malicious attack. A multi-agent immune system is used by accompanying Intrusion Detection System (IDS) in order to reduce the false alarm rate successfully. Moreover, in this study, we find the shortest distance and provide security between the nodes source and destination using Ant Colony Optimization (ACO). As a result, the proposed SAMR (Secured Ant-Based MANET Routing) method is compared with some existing technique based on throughput, control packet overhead, end to end delay and packet delivery ratioto show better performance analysis, respectively.

Key words: AODV, mobile ad hoc network, throughput, ant colony optimization, SAMR, immune system

INTRODUCTION

MANET which is said to be a group of self-governing wireless nodes are not secured because it is dynamic in nature and high mobility. So, MANET act as an important communication during transmission of data. Comparing to the wired network, the wireless MANET is highly susceptible to security attacks, caused by its low bandwidth dynamic network topology, memory and battery limitations of mobile devices. There are three different types of the routing protocol. They are reactive, hybrid and proactive routing protocol. In MANET routing, attackers can engage continuously by sensing the network traffic intruding into the path from source to destination. Intrusion detection system, Yang *et al.* (2014) is an important tool to give an assurance for network security. There are two types of IDS such as misuse detection and anomaly detection. Misuse detection IDS is defined as patterns of weak spots or well-known attacks which use the type of system to match and to identify the known intrusions commonly. An anomaly detection IDS states that it is automatically detected by the system using this method such as machine learning, sequential analysis, statistical analysis and neural networks. Also, it is used to determine the unknown attacks but leads to false alarm rate because of its anomalies (Jain and Saxena, 2016). The performance of IDS can be increased by the use of an agent. Some of the advantages of agent-based IDS are as follows:

- Improvement is autonomous computing and adaptation capacity
- Consists of better maintainability
- Decrease in network flow
- Platform irrelevance

There is no need of requirement for fixed infrastructure excluding connections to the wired digital networks because wireless mobile devices gathered together to form a network known as Mobile Ad hoc Network (MANET). Individual nodes act as relay and host in routing capability which is a basic function for MANET. Here, the router that forwards the packets to the neighboring nodes is not in the transmission range of destination. An artificial immune system adopted in this study acts as a branch for the technique based on the principle of the invertebrate immune system. The problem of false alarm rate is reduced due to the combination of multi-agent based immune system and IDS, respectively. By adopting agent-based artificial systems to the

Corresponding Author: Jayanthi Chandrashekar, Department of Electronics and Communication Engineering, Vemana Institute of Technology, #1, Mahayogi Vemana Road Koramangala, 560034 Bangalore, Karnataka, India, jayansri@yahoo.com

dendritic cells, the human immune systems are initiated through lymphocyte cell management behaviors. Also, the corresponding signals are identified to check whether the antigens are malicious or not. The identification can only be achieved when an individual agent consists of goals and defined duties because a multi-agent system is capable of its collaboration and coordination. The existing agent-based mechanism influences low consumption of resources, adaptability, flexibility and robustness. However, using non-fuzzy and a non-sharing strategy, the detection accuracy may not be satisfied. Furthermore, a bio-inspired routing protocol was developed in this study by incorporating swarm based approach for malicious activity detection. The bio-immunity mechanism has brought an enormous reference for network security. For example, let us consider IDS based on artificial immunity which determines that an ant, bee or any other insects as far as an individual is concerned, the action is not inspected and hence, the intelligence is low. Rather, the colony technique has the ability to show very high swarm intelligence and solve any complicated problem. In this study, we consider an ant which quickly determines the shortest route approach to food source from a lot of possible routes. The ant possesses swarm intelligence due to some characteristics such as self-organization, stability and flexibility.

In recent techniques, Ant Colony Optimization (ACO) is gaining popularity as a new methodology for feature selection. ACO algorithm is the inspiration of social behavior in ant colonies. Though, they have no sights, ants have the capability to determine the shortest path between the nest and food source and by chemical materials known as a pheromone that has left when moving. ACO algorithm was originally applied to the traveling salesman problem and later it was successfully applied to other optimization problem such as quadratic assignment problems, routing in the telecommunication network, scheduling and graph coloring and so on (Aghdam and Kabiri, 2016).

Literature review: The techniques that were used for providing better security in MANET are illustrated in this study. MANET has a self-establishing property and hence, providing runtime security is a difficult task.

Kaur and Rao (2017) proposed a key management mechanism which provided the security in MANET. This scheme aimed at overcoming the eavesdropping attack. The encryption key distribution among the authorized user was a difficult task it's because of the dynamic nature. A new session key was regenerated every time the nodes disconnects and gets connected again. This key management approach achieved minimum congestion and it reduced the key distribution time. This security system removed the malicious node. Key is generated and every time a new node was added. The drawback of this approach was its centralized approach.

Shakshuki *et al.* (2013) developed an intrusion detection method for protecting the MANET from packet dropping attack. This Enhanced Adaptive Acknowledgement (EAACK) prevented the third party attack like forged acknowledgement attack. The scheme implemented the digital signature which ensured that the acknowledgement packet was authentic. It used a Misbehavior Report Authentication (MRA) which ensured that the missing packets reached the destination through some other route. The cryptographic technique that used a Digital Signature Algorithm (DSA) which resulted with minimum network overhead than Rivest Shamir Adleman (RSA) algorithm because the key size was smaller for DSA than RSA. The EAACK outperformed AACK in terms of limited transmission power, false misbehavior statement and receiver overhead. The drawback of this system was it generated additional routing overhead.

Chang *et al.* (2015) suggested a defending mechanism in MANET with Cooperative Bait Detection (CBD) scheme. This scheme was developed to prevent the malicious nodes from launching blackhole or grayhole attacks. The routing algorithm that was used was Dynamic Source Routing (DSR). It included both reactive and proactive defense architectures. It implemented a reverse tracing technique to identify the malicious nodes. The Cooperative Bait Detection Scheme (CBDS) reduced the routing overhead and same time provided a better packet delivery ratio as well as the Best Effort Fault-Tolerant Routing (BEFTR), compared to DSR. The CBDS system required more amount of time to detect the track the malicious node.

Chatterjee and Das (2015) proposed an enhanced DSR algorithm for MANET. The Ant Colony Optimization (ACO) technique was developed in such a way that it satisfied the quality of service requirements. It achieved the low end to end delay, energy consumption and routing head as well as the high data packet delivery ratio. The routes were founded using the route request control packets that were broadcasted. These packets were known as request ant packets. The security issue was not considered in this ACO technique.

Rafsanjani and Fatemidokht (2015) proposed a secure network for MANET. This network was developed based on the fuzzy network. The ad hoc network faces challenges like the mobility of the node, no infrastructure, very limited security for the nodes physically to overcome this a routing protocol was designed. The bio-inspired

routing algorithm was used to avoid the vulnerabilities in the MANET. This security framework used the fuzzy technique and the digital signature scheme and the BeeAdHoc protocol which collected the data about the status of the network and the quality of the traversed path was evaluated. The digital signatures protected the information from the forager. The selfish nodes in the network were not found through swarm intelligence methods.

Ghasemnezhad and Ghaffari (2018) proposed a dependable and routing protocol for real-time applications based on fuzzy logic for MANET. It was developed to overcome the issues like hopping in the network. Using the fuzzy logic it found the stable route which had the minimum hops and the shortest path. This Fuzzy Logic Reliable Routing Protocol (FRRP) optimized the system and improved the efficiency. This technique outperformed the Ad hoc On Demand Distance Vector (AODV) by reduction of an end to end delay rate an improvement over packet delivery and throughput. The security issues were not taken into consideration in this system.

Singh *et al*. (2014) proposed a MANET with an Ant Algorithm (ANTALG) to keep track of the changing topology. This ant logarithm based on Ant Colony Optimization (ACO) established a better routing mechanism for efficient communication. This ANTALG chose a source and a destination nodes randomly swapped agents among them. It kept a track of trip time of nodes and with it, the pheromone table and the data structure were constructed. The ANTALG algorithm transmitted the Transport Control Protocol (TCP) through a better window size. It reduced the packet drop and an end to end delay compared to that of the AODV and ADSR. This increased the network overhead due to the control vpackets that were transmitted in order to keep the network stable.

Abuhmida *et al*. (2015) proposed an ANTMANET protocol which identified the shortest path based on the ACO. The overhead in the network due to control packets transmission was rectified using the ANTMANET. This network minimized the search area by using the location information and this eventually decreased the network overhead. The protocol that was used here was the bio-inspired protocol, this outperformed the methods like AODV and the LANMAR in terms of network overhead and the delay. It did not consider the packet delivery ratio and the pause time.

Zhang *et al*. (2018) proposed an automatic optimization for routing through smart perception. This method adopted the Bio-inspired Hybrid Trusted Routing Protocol (B-iHTTP) based on the trust evaluation. The perceptive ants were obtained using the cross-layer perception with ACO. This divided the network into multiple zones each zone consisted of a routing table which was maintained by the perspective ants. The perceptive ants were used to sense the concerned parameters. The B-iHTRP used the Physarums Autonomic Optimization (PAO) to automatically optimize the routes at the time of multi-zone communication session. This was only designed in order to find the nearest path and security issues were not taken into account.

Elmazi *et al*. (2015) proposed a node security in clustering MANET and a comparative study was made between the fuzzy-based systems. Due to the mobility of nodes in the network, the bandwidth was limited also there exists a dynamic change in network topology. This clustered MANET resulted with better stability and scalability in the network. Different clustering schemes were implemented in this network namely energy efficient clustering, weighted and mobility based clustering and connectivity based clustering. When the comparison was made between the two fuzzy systems like F2SMC1 and F2SMC2, the latter was more secure and reliable, yet, it was complex. Though it was centralized in a failure of the centralized node the whole network gets affected.

Khinchi and Bhushan (2016) proposed a routing model to improvise the quality of service in the MANET. This Secure Synchronous Routing (SSR) Model used the synchronous decision-making scheme which was used to synchronize the nodes for better communication. This achieved time synchronization integrity, maximum throughput, reliability and the data loss was reduced. It reduced the failure and the communication was on time. This network was not eligible for long networks.

Manickavelu and Vaidyanathan (2014) proposed an algorithm for MANET for recovering the route. This technique implemented the Particle Swarm Optimization (PSO) lifetime prediction algorithm to recover the route. This PSO in MANET predicted the lifetime of the link and there is an availability of node in bandwidth. The status of the node is decided using the fuzzy rules with the predicted and fuzzified parameters. The information exchange was made among the nodes. The node status was evaluated before every data transmission. The weak node was identified and the routes were diverted towards the strong node. This reduced the data loss and the communication overhead. The optimization of the path was considered but this PSO system did not consider the malicious attacks.

Wei *et al*. (2014) proposed an enhanced security for MANET using a trust management. The trust management consisted of two types they were direct observation and indirect observation trust. The direct observation was the Bayesian information and the indirect

observation was the second-hand information which was obtained from the neighbor nodes. The Dempster Shafer Theory (DST) was used to derive the trust value. This theory was a type of uncertain reasoning. The combination of the two models obtained more accurate trust values. The packet delivery ratio and the performance were increased. The messages overhead were increased.

Dhananjayan and Subbiah (2016) proposed a trust to provide awareness over ad hoc routing protocol in MANET. The trust level was improved between the nodes source and destination by an introduction of trust for awareness in MANET. The traditional AODV routing protocol was modified with the constraints of mobility based malicious behavior prediction, energy and trust rate. Then, the trust rate was determined to avoid the malicious report generation through the packet sequence ID that matched from a lot of the neighboring nodes. The comparative analysis between the existing method and proposed T2AR like FBR, RBT, DICOTIDS, TRUNCMAN and GR showed the effectiveness of introduced scheme in the secure MANET environment design regarding the packet delivery ratio, false positives, throughput and average end to end delay. Hence, from the comparative analysis, the proposed approach proved that it achieved a high-performance metrics than the existing methods.

Patel and Sharma (2013) proposed a detection mechanism for malicious attacks. Due to the dynamic characteristics of MANET topology the network was susceptible to the Denial of Service attack (DOS). The most susceptible attack in MANET was a black and grayhole attack. Automatic security mechanism was focused on the use of SVM (Support Vector Machine) to defense against the malicious attack. A new algorithm was introduced to detect the attacks in ad hoc networks based on SVM behavioral routing protocols. The QoS of a link was evaluated by the performance metrics such as PMISR, PDER and PMOR. These metrics were also used to predict the attacks in MANET.

He *et al.* (2013) proposed an efficient and secured password authenticate group key exchange protocol for MANET. Based on the dynamic scenario, group session key was generated where the key generation overhead acted as an independent of the size of the whole group. Consequently, the security weakness had been removed here which appeared on the modified NEKED protocol at the time of forgery attacks over the system. The performance analysis and security was compared with the related schemes and proved that it is applicable for real-world applications in enhancing the security of wireless communication.

Persis and Robert (2015) presented an ant based multi-objective routing optimization in MANET. The successive route maintenance and discovery was performed by routing algorithm. The multi-objective vector was considered and enabled the routing algorithm for the combination of better routes than the AODV protocol. The comprehensive performance of other meta-heuristic application can still be analyzed and explored for the implementation of the multi-objective optimization model.

Abdelshafy and King (2015) proposed a dynamic source under routing attacks and studied the DSR protocol performance and delay of the flow state in the presence of a selfish, flooding, grayhole and blackhole attacks. DSR was known to be a renowned reactive routing protocol in MANET which does not maintain the routing messages securely. Since, the aforementioned attacks consist of severe attacks on a static network than the high mobility network, it can be concluded that the flow-state DSR contains better performance than the original DSR, respectively. Rather, blackhole attacks contain dramatic impact over PDR of the original DSR in a static network.

Dorri *et al.* (2018) proposed the detection and elimination of black holes in MANET. The novel approach utilized additional black hole check and data control packet for detecting and eliminating the malicious node. The simulation results showed that DEBH decreased the packet overhead and delay as well as increase the network throughput in comparison with other approaches. Further, DEBH has the ability to detect every active malicious node that generated fault routing information. In case of a single blackhole, delay and packet overhead caused by this approach were greater than the other approach.

MATERIALS AND METHODS

In this study, a bio-inspired routing protocol was developed by the incorporation of swam based approach for malicious activity detection like packet dropping attack, misrouting, energy drain attack and so on.

Also, a problem of false rate was mitigated by the utilization of multi-agent based immune system with an intrusion detection system. Multi-agent is a software component build up with chip consisting of network applications and functions. The responsibility of multi-agent is to check the availability of attacks in the node. The multi-agent system visits each and every node to check whether the node receives the packet or not based on the routing algorithm. In case, the destination has not received the packets sent by the source, then multi-agent assumes that attack has been taking place.

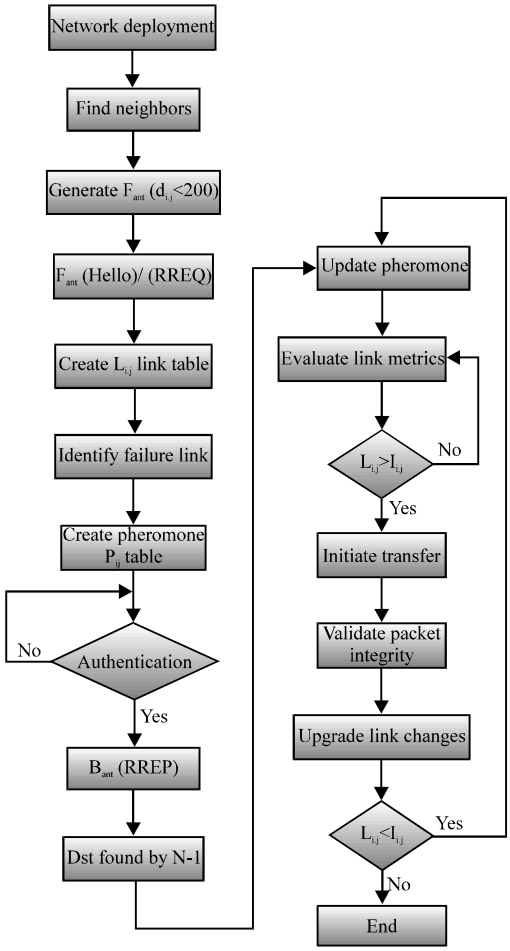

Fig. 1: Proposed flow diagram

Then, it identifies the location of an attack and removed by the use of multipath base station, respectively. The overall flow diagram of the proposed method is shown in Fig. 1. The flow help us to determine the best alternative path for transmitting the data packets in a limited time period, availability of bandwidth and route distance, respectively.

Neighbor discovery: A node is set initially where ACO works in the principle of reactive technique on-demand way for MANET. ACO is used to reduce the overhead for routing. A neighbor node is determined by choosing the source node S. The node list is created to the source node (S) in terms of the neighbor discovery process and the neighbor node is determined. Here, the Hello message is not used to find its neighbor node. When a packet arrives a node, then, it checks the availability of routing information for a destination in its routing table.

Route discovery: There are two types of ant agents. They are the Forward ant (F_{ant}) and Backward ant (B_{ant}). First F_{ant} is generated after the determination of neighbor node. While generating, the distance between the nodes i and j should be <200. Where the F_{ant} is responsible for the establishment of pheromone path to the source node. The sender broadcast F_{ant} in the route discovery phase which consists of source address, request hop count, destination address and bandwidth. The F_{ant} sends the Hello message through RREQ. Hello message is used to inform the neighboring node that the line is still alive and need not be forwarded. The overall steps for route discovery are as follows.

Algorithm 1; Ant colony routing algorithm:

Step 1: Let us assume that the source node S contains data packets to be transmitted to the destination D with the necessities of QoS such as energy efficient, fault tolerant, less delay, transmission rate and high bandwidth. A node lists that contains the ant visitation in a step by step manner is known as visited node list. This list forms the multipath routing table Rt between the source and destination node

Step 2: Source node S is initially chosen. Also, initialize the visited node list to the source node (S) in terms of a neighbor discovery process

Step 3: Initiate F_{ant} (Forward ant-Route Request) to destination D over all its neighbors that are at 1-hop distance from S. The F_{ant} consist of the destination address, bandwidth, address and required hop count

Step 4: All 1-hop node distance are calculated after the pheromone evaporation. Each node 'i' preserves a table named "PhTab" which consist of pheromones identifying the measure of pheromone that areavailable on every link (V_i, V_j). This quantity is then adjusted to Constant C:

$$Ph(i,j) = \frac{\left[\tau_{i,j}\right]^{\alpha}.\left[\eta_{i,j}\right]^{\beta}}{\sum_{k\in M}\left[\tau_{i,j}\right]^{\alpha}.\left[\eta_{i,j}\right]^{\beta}}$$

$\tau_{i,j}$ = The measure of pheromone on the link
$\eta_{k,j}$ = The link visibility
α and β = The two parameters that demonstrates the relative significance of the pheromone and visibility in the process of QoS route discovery
M = Set of all probable neighbor nodes v_k, not yet visited by the ant

Step 5: Then, the pheromone evaporation of all the 2-hop distance nodes are calculated

Step 6: The probability of every path from source S calculates the path preference using pheromone evaporation. A node j from the adjacent nodes (i.e., from j, k, ..., n) in which i is chosen as MPR node, so that, it envelopes all the 2-hop distance nodes. Hence, the probability of path preference is improved when compared to other

Step 7: F_{ant} is converted to B_{ant} when it reaches the destination. Then, it is forwarded to an original source. The B_{ant} will take the same path of the F_{ant} but in reverse direction

Step 8: The path which has the probability of higher path preference will be deliberated as the best path and hence, the transmission ofdata takes place along the path

AntNet 2.0 method, Baran and Sosa (2001) is used in this study for updating the routing tables. When the B_{ant}

arrives a neighboring node then the traffic local model will be updated by B_{ant} and the probabilities of the neighbor node will be associated with the destination in the routing table. The corresponding updates will be performed for each and every node between source and destination in the sub paths, followed by F_{ant} after visiting its neighboring node. If sub path trip time is good, then, it can be updated in the routing table and related statistics. Suppose, the trip time is bad then it cannot be used anywhere. This because it will not provide a true idea about the requirement of time to arrive the sub path nodes. Hence, the traffic local model and routing table are updated for generic destination, respectively.

Link measurement: After the initialization of F_{ant}, the pheromone evaporation of 1-hop distance nodes must be calculated. Each node "i" preserves a pheromone table denoted as "PhTab" which specifies the quantity of availability of pheromone in an individual link (V_i, V_j). Then, this measure can be initialized to Constant C. The pheromone between the two nodes are calculated based on the formula presented in algorithm step 4. Based on this formula, the pheromone evaporation of every 2-hop distance nodes are also calculated. The probability of path preference is calculated for each path to transmit the packet with the shortest distance without any congestion or traffic. The path is calculated from source node by using pheromone evaporation for every node. Suppose, the estimated value of the path seems to be better than the path needed, then, a gained path can be accepted and stored in a memory. Once, the F_{ant} reaches its destination, it is converted to B_{ant} and hence, F_{ant} towards the original source. Thus, B_{ant} considers the path similar to that of the F_{ant} in opposite direction. Finally, the path which consists of high probability is considered such that data transmission will be started from the best path.

Node verification: The source consisting of n number of nodes contains some secret key sharing between source and destination. The source node consist of n number of nodes with some key generation and share those nodes with the destination as a secret key. When the destination receives the node and again resends it, the source checks whether the transmitted node matches the received node for security purpose. In case, any one of the node does not matches the corresponding key, then, it is assumed that the node is not secured and hence, there exists an attack over the node. This secret key sharing and reconstruction is provided by the Shamir's algorithm (Harn and Lin, 2010).

Algorithm 2; Secret key sharing:

Step 1: Source S first selects a polynomial f(x) of degree (t-1) randomly. Where, f(x) is given by:

$$f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1}$$

where, the secret key $s = a_0 = f(0)$ and all coefficients $a_0, a_1, \ldots, a_{t-1}$ are in a finite field $IF_p = GF(p)$ with p elements

Step 2: S computes all shares $s_i = f(i) \pmod p$ for $i = 1, \ldots, n$

Step 3: S produce an outputs in the form of list as n shares $(s_1, s_2, \ldots, s_n)$ and distributes each share s_i to corresponding shareholder P_i Privately

Algorithm 3; Secret reformation:

Any t shares $(s_{i1}, \ldots, s_{it})$ can be considered as an input, that can be able to reform the secret s as:

$$s = f(0) = \sum_{i \in A} s_i \beta_i = \sum_{i \in A} S_i \left(\prod_{j \in A - [i]} \frac{x_j}{x_j - x_i} \right) \pmod p$$

where, $A = \{i_1, \ldots, i_t\} \subseteq \{1, 2, \ldots, n\}$, β_i for $i \in A$ are lagrange coefficients

When a group key generation request have been received from users, then, it is the responsibility of the source to select the group key and access every shared secret key among the group members. Then the source node must distribute the group key to each and every participants of the group in a safe manner. Moreover, the transmission between the source and group members lies over the broadcast channel.

Link failure: In an initial stage, either the failed unicast transmission of control or data packets detects the link failures or it is detected by using the Hello messages. Thus, the failed unicast transmission detection is straightforward. The success or failure of an unicast transmission information is shared by the mechanism of MAC layer protocol.

The link failures are detected by using the hello message in the proposed system. For t_{hello} seconds fixed interval of time, the messages are sent out asynchronously by every nodes of the network. A new node n_j sends the Hello message to a node n_i. When a node n_i obtains Hello message from a new node n_j, it assumes that n_j is the neighbor node and establishes into a new entry known as $L_{i,j}$ for n_j in the neighboring table. P^i_{ij} entry is created in its pheromone table to indicate that there exists only one-hop route from n_i-n_j. Once an entry is created, n_i expected to receive the message from n_j for every t_{hello} seconds, respectively. Suppose n_j have not sent a message to n_i for a certain number of second intervals, say for 2 intervals, then, automatically n_i assumes that there is a disappearance of wireless communication to n_j.

The pheromone informations are carried in the diffusion process, also, the link failures are detected by

using either Hello or RREQ messages. n_i is capable of detecting the link with the neighbor n_j either it is lost or present in a table. If n_i finds that the link to the neighbor n_j is lost then it removes the node from the neighbor table. After removing the lost table, a pheromone table P_i is updated by building a link failure notification message. Consequently, the pheromone table will be scanned to control the destinations d which consist of non-zero regular pheromone value τ^d_{ij} viz. for destination n_d, neighbor n_j is used as the next hop from n_i. Hence, for each destination, n_i sets τ^d_{ij} to 0 correspondingly. Moreover, it checks whether the lost pheromone τ^d_{ij} is one of the best or simply regular pheromone value that is available for n_d. If this is the case, it adds an address of the destination n_d to the link failure notification message along with a new best regular pheromone for available d. In case τ^d_{ij} is the only non-zero regular pheromone entry for n_d, then, it will be indicated in the link failure notification message, respectively.

Secure authentication: A secure authentication is provided over routing between source and destination based on Ant Colony Optimization (ACO) method. The population is initialized by calculating the distance from the node source to destination, respectively. The pseudo code for secure ACO Model is given below:

Algorithm 4; Pseudo code for secure ACO Model:

Input: Feature matrix
Output: Fitness value
Step 1: Initialize population

$$p = \sqrt{(x(i)-x(j))^2+(y(i)-y(j))^2}//$$

where, x and y-input features of node
Step 2: Initialize path, R = Random value for size of each matrix
Step 3: Initialize velocity (Validate the intermediate nodes)
For i = 1
V (i) = V+P (R (i), R(j))
End loop
For k = 1 to number of neighbors
ω, 0(k+1) = max (ω)-(max (ω))-min (ω).max (R)
V(k+1) = 0 (k)^{v}v (k)+P^{b*} (pb (k)-x(k))+P^{b*} random* (Gb (k)-x (k));
//Where, pb-previous best; Gb- Global Best; k-size of feature vector; b-number of updation
Pd = trial intensity (k)* Pb (path (k))
Step 4: Check chosen link have max then estimated
Step 5: Update P Best and G Best
Step 6: Fitness value updating

The pseudo code was generated for secure ACO model. Based on this model it is being analyzed that feature matrix is given as an input and fitness value as output. Then the distance is calculated for two input nodes and initialize path as random value for the size of an each matrix. The intermediate nodes are validated through the calculation of the velocity of nodes. The PB and GB are said to be a previous best and global best, through which the best path is identified. If one node is said to be a global best node, it is compared to the next nearest node. While comparing, the second node is known to be superior to that particular node is called global best. By the way, the best path is identified between the nodes. During this process, there may be some occurrence of jitter. Hence, jitter value is reduced by using the proposed methodology. Symbol representation of the proposed SAMR method is shown in Table 1.

Table 1: Symbols in SAMR

Symbols	Representation
x, y	Input features of node
V	Velocity
K	Size of feature vector
ω	Jitter
R	Random value
Pb	Previous best
Gb	Global best
B	Number of updates
i, j	Neighbor nodes

RESULTS AND DISCUSSION

This study shows the performance analysis of SAMR compared with the existing techniques such as AODV, BeeAdHoc and FBeeAdHoc protocol Rafsanjani and Fatemidokht (2015). The metrics considered in SAMR for performance comparison are overhead in control byte, packet delivery ratio, throughput and an E-E delay.

PDR: PDR (Packet Delivery Ratio) is defined as the proportion of the quantity of packets that are being obtained by the destination to packets started from the source. PDR can be formulated as follows:

$$PDR = \frac{\text{No. of packets received by the destination}}{\text{No. of packets originated from the source}} \times 100 \quad (1)$$

The performance comparison of PDR is shown in Fig. 2. The graph shows the comparison between SAMR and existing techniques of the routing protocol.

Figure 2, it has been analyzed that the SAMR method provides an enhanced performance compared to the existing methods of Free ad hoc, AODV, Bee ad hoc routing protocol. If the value of packet delivery ratio is greater, then, it provides better performance over the routing protocol. Where the SAMR consist an average packet delivery ratio of 85.74. Whereas, the existing protocol consists of 84.59, 85.158 and 71.55. Hence, based on these values it is clearly known that SAMR contains a greater value when compared to the other.

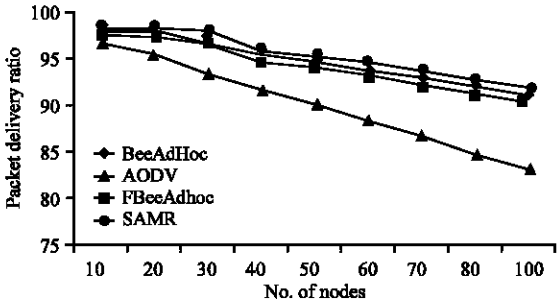

Fig. 2: Packet delivery ratio

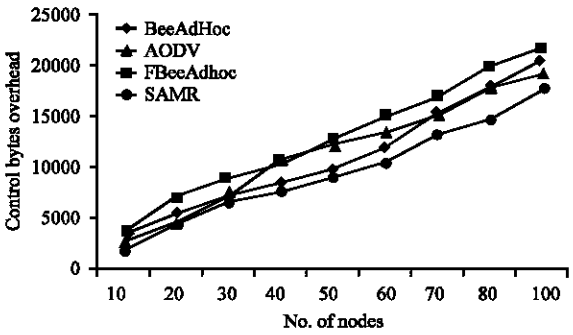

Fig. 3: Control packet overhead

Overhead in control bytes: The amount of control bytes sent by every nodes in the network. The time taken for the transmission of data in routing protocol from source to destination by means of traffic is reduced. Figure 3 shows the performance comparison of SAMR and existing routing protocol of control byte overhead.

Figure 3, it is analyzed that SAMR consist of lower bytes than the existing system. The average value of SAMR is 8615.9. The average values of existing methods are 9942.7, 11641.2 and 10240.3. Thus, from these values, it is shown that the SAMR consist of less value than Bee ad hoc, FBee ad hoc and AODV, correspondingly.

E-E delay: Once a data packet is generated, it is delivered to the destination in time interval based on the application node. The comparison of an E-E delay with existing techniques is presented in Fig. 4. An E-E delay should consist of less value, so that, the transmission of data packets consist of less delay. An E-E delay is defined as the ratio of an average difference between arrival and transmitted time to the number of paths. It can be formulated as:

$$\text{E-E delay} = \frac{\sum(\text{Arrive time-Sent time})}{\sum \text{Number of paths}} \quad (2)$$

From the above graph, it is determined that the average rate of an E-E delay for SAMR is 59.85 and the

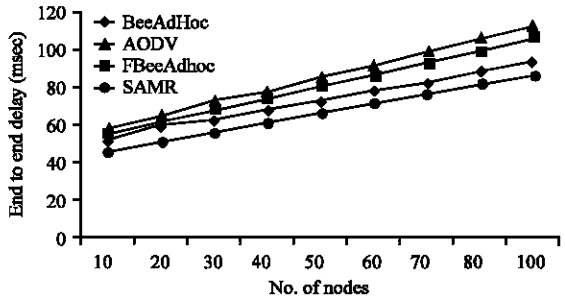

Fig. 4: End to end delay (msec)

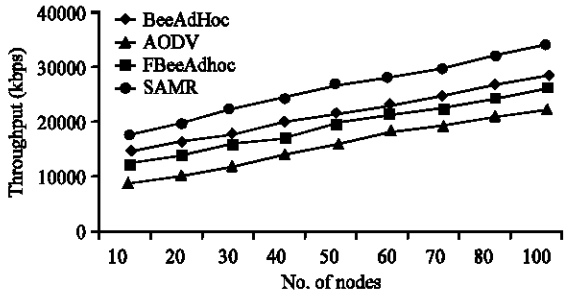

Fig. 5: Throughput (kbps)

existing routing protocol consists of 66.15, 72.45 and 76.95, correspondingly. Hence, from above values, it is seen that the average end delay of SAMR consists of less value when compared to FBeeAdHoc, AODV and BeeAdHoc network.

Throughput: The net amount of data packets provided to destination nodes for the period of simulation is separated by the time taken for simulation. In other words, throughput is also defined as the number of packets received successfully in a given time. It is represented in bits per second. The throughput comparison between SAMR and existing techniques is shown in Fig. 5. Throughput is given by:

$$\text{Throughput} = \frac{\text{Number of delivered packet} * \text{size of the packet}}{\text{Total duration for simulation}} \quad (3)$$

If throughput is greater on a network, then, it provides better performance over the routing protocol. Based on this formula the average throughput value of SAMR is 23481.6 kbps while BeeAd-Hoc, AODV, FBeeAdHoc network consist of 19291.7, 14307.1 and 17368.6. Hence, from these results it is being analyzed that SAMR consist of higher value and provides a superior performance in the network.

CONCLUSION

The bio-inspired routing protocol is inspired in this study by including swarm based approach for malicious attack. The malicious activity detection are misrouting, energy drain and packet dropping attack. The false alarm rate is reduced by the utilization of multi-agent based immune system upon intrusion detection system. The critical wireless networks are protected by applying some security techniques to the bio-inspired agents. Meanwhile, ant colony optimization method is adopted to determine the shortest path distance and security analysis among the source and destination. The simulation results of SAMR is compared with BeeAd-hoc network, AODV and FBeeAdHoc, respectively. The results are simulated based on metrics such as throughput, an E-E delay, control packet overhead and PDR. Hence, from the simulation results, it is proved that SAMR consists of better performance, high PDR and less delay. Further, the interoperable agent based artificial immune system is designed to protect mobile ad hoc network from attacks. The malicious attack can be detected and energy efficiency must be improved in future analysis to provide security over the path between the nodes.

REFERENCES

Abdelshafy, M.A. and P.J. King, 2015. Dynamic source routing under attacks. Proceedings of the 7th International Workshop on Reliable Networks Design and Modeling (RNDM), October 5-7, 2015, IEEE, Munich, Germany, ISBN:978-1-4673-8050-8, pp: 174-180.

Abuhmida, M., K. Radhakrishnan and I. Wells, 2015. Evaluating the performance of ANTMANET protocol for MANET. Proceedings of the 2015 International Conference on Internet Technologies and Applications (ITA), September 8-11, 2015, IEEE, Wrexham, UK., ISBN:978-1-4799-8036-9, pp: 109-114.

Aghdam, M.H. and P. Kabiri, 2016. Feature selection for intrusion detection system using ant colony optimization. Intl. J. Network Secur., 18: 420-432.

Baran, B. and R. Sosa, 2001. AntNet routing algorithm for data networks based on mobile agents. Inteligencia artificial. Rev. Iberoam. Inteligencia Artif., 5: 1-10.

Chang, J.M., P.C. Tsou, I. Woungang, H.C. Chao and C.F. Lai, 2015. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE Syst. J., 9: 65-75.

Chatterjee, S. and S. Das, 2015. Ant colony optimization based enhanced dynamic source routing algorithm for mobile ad-hoc network. Inf. Sci., 295: 67-90.

Dhananjayan, G. and J. Subbiah, 2016. T2AR: Trust-aware ad-hoc routing protocol for MANET. Springer Plus, 5: 1-16.

Dorri, A., S. Vaseghi and O. Gharib, 2018. DEBH: Detecting and eliminating black holes in mobile ad hoc network. Wirel. Networks, 24: 2943-2955.

Elmazi, D., E. Kulla, T. Oda, E. Spaho and S. Sakamoto *et al*., 2015. A comparison study of two fuzzy-based systems for selection of actor node in wireless sensor actor networks. J. Ambient Intell. Hum. Comput., 6: 635-645.

Ghasemnezhad, S. and A. Ghaffari, 2018. Fuzzy logic based reliable and real-time routing protocol for mobile ad hoc networks. Wirel. Pers. Commun., 98: 593-611.

Harn, L. and C. Lin, 2010. Authenticated group key transfer protocol based on secret sharing. IEEE Trans. Comput., 59: 842-846.

He, D., C. Chen, M. Ma, S. Chan and J. Bu, 2013. A secure and efficient password-authenticated group key exchange protocol for mobile ad hoc networks. Intl. J. Commun. Syst., 26: 495-504.

Jain, C. and A.K. Saxena, 2016. General study of mobile agent based Intrusion Detection System (IDS). J. Comput. Commun., 4: 93-98.

Kaur, I. and A.L.N. Rao, 2017. A framework to improve the network security with less mobility in MANET. Intl. J. Comput. Appl., 167: 21-24.

Khinchi, M.K. and B. Bhushan, 2016. Improving qos in manet by secure synchronous routing model. Intl. J. Res. Comput. Appl. Rob., 4: 7-14.

Manickavelu, D. and R.U. Vaidyanathan, 2014. Particle Swarm Optimization (PSO)-based node and link lifetime prediction algorithm for route recovery in MANET. EURASIP. J. Wirel. Commun. Networking, 2014: 107-117.

Patel, M. and S. Sharma, 2013. Detection of malicious attack in MANET a behavioral approach. Proceedings of the IEEE 3rd International Advance Computing Conference, February 22-23, 2013, IEEE, Ghaziabad, India, ISBN: 978-1-4673-4527-9, pp: 388-393.

Persis, D.J. and T.P. Robert, 2015. Ant based multi-objective routing optimization in mobile ad-hoc network. Indian J. Sci. Technol., 8: 875-888.

Rafsanjani, M.K. and H. Fatemidokht, 2015. FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs. AEU. Intl. J. Electron. Commun., 69: 1613-1621.

Shakshuki, E.M., N. Kang and T.R. Sheltami, 2013. EAACK-A secure intrusion-detection system for MANETs. IEEE Trans. Ind. Electron., 60: 1089-1098.

Singh, G. N. Kumar and A.K. Verma, 2014. ANTALG: An Innovative ACO based Routing Algorithm for MANETs. J. Network Comput. Appl., 45: 151-167.

Wei, Z., H. Tang, F.R. Yu, M. Wang and P. Mason, 2014. Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. Veh. Technol. IEEE. Trans., 63: 4647-4658.

Yang, F., V. Gondi, J.O. Hallstrom, K.C. Wang and G. Eidson, 2014. OpenFlow-based load balancing for wireless mesh infrastructure. Proceedings of the 2014 IEEE 11th International Conference on Consumer Communications and Networking (CCNC), January 10-13, 2014, IEEE, Las Vegas, Nevada, USA., pp: 444-449.

Zhang, M., M. Yang, Q. Wu, R. Zheng and J. Zhu, 2018. Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs. Future Gener. Comput. Syst., 81: 505-513.