International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 11 (2019) pp. 2704-2716

Power-Aware Secure Routing protocol in MANET based on Reputation Model and Optimization

Nukam Reddy Srinadh[1], Dr. B. Satyanarayana[2]

[1]*Research Scholar, Rayalaseema University, Kurnool. & Associate Professor, Dept of CSE, VEC, Kavali, A.P, India.*

[2] *Professor in Computer Science &Technology., Sri Krishnadevaraya University, Anantapur ,A.P , India.*

Abstract:

The Mobile Ad Hoc Network (MANET) is a self governed communication network connected by wireless links, where mobile nodes transfer data packets with each other using wireless links without depending on any other infrastructures or central control. Offering power aware secure routing protocol is a challenging task in this kind of network because of its changing topologies and fewer resources. This work introduces a power-aware secure routing protocol considering a reputation model. Here, Krill Herd based Grasshopper Optimization Algorithm (KH-GOA) along with the reputation model and power is developed for establishing a secure path from initial node to destination. The reputation model contains reputation parameters, which include node mobility, actual capability of the node, previous records, and reputation among the neighbours. The reputation factors are considered for each node along with proposed KH-GOA algorithm, which is the integration of Krill Herd (KH) and Grasshopper Optimization Algorithm (GOA), for establishing a secured path from the initiating node to destination. The proposed KH-GOA based routing protocol uses multi-objective functions, such as reputation, power, distance, and delay. The performance analysis for the proposed KH-GOA produces better power, throughput, delay, and detection rate with value 27.313W, 0.670, 0.114, and 0.734ms, respectively.

Keywords: MANET, Reputation model, Routing, Node mobility, Power, Krill Herd, GOA

1. INTRODUCTION

MANETS are self-governed wireless network, which is responsible for initiating communication and reside in self-directed mobile application framework, in which every mobile node can send information from one node to another node using equipped wireless interfaces without depending on other services [1]. The MANET is not depended on static infrastructures and administrator. The limited resources are acquired by the wireless sensor network, which involves computational memory, battery capabilities, bandwidth, and memory [2]. MANETs have several applications, such as communications set up in conferences, emergency search, rescue operations, virtual classrooms, exhibitions and meetings in battlefield, military communications, and data acquisition in hostile environments [8]. The purpose of routing protocol is to build a right and proficient path linking two nodes to transmit messages on time. The whole network is collapsed if routing is misdirected leading to loss of data. Therefore, routing security is responsible for addressing the security issues produced in the entire network [16] [6]. MANETs initiate a secure communication between the nodes, which are responsible for initial communication and to provide a challenging environment. The nodes participating in the communication tend to move towards the receiving range of signals that captures each data packet and produces arbitrary reactions. The performance of the routing protocol is degraded due to the routing attacks, which are supposed to obstruct the process of routing. The mobility of nodes is responsible for varying topologies of the network [8]. The failures in power cause more severity than the common network failures in MANET topologies [4]. In addition, the varying topologies produced by the mobility of the nodes influences the power consumed for transmitting data. Thus, routing schemes, which contain methodologies that can handle the challenges sustained by the node's mobility, varying topologies and power constraints, are required in MANETs. Moreover, the routing protocols must be effective in power consumption and Quality of Service (QoS) for guarantying the transmission of data through the wireless medium [11].

MANETs process two stages of attacks, in which the first stage of attack occurs in basic methods like routing whereas the second stage destroys the methods based on security adapted through network. The attacks are categorized in two categories that involve external attacks and internal attacks. The internal attacks is linked with nodes contained in the network to connect the interfaces linking them, whereas the external attacks avert the network from normal communication by providing extra network overhead [19]. The external attacks are classified into active attacks and passive attacks. The transmission of data from network is not altered in case of passive attacks, whereas the active attack behaves severely while preventing the flow of messages between the nodes [20] [9]. The routing algorithms are devised using the MANET features and thus, they integrate multiple factors, such as dynamic changing of network topology, power saving, overhead, and node's trust. The safety measure of multi-hop communication is based on reliability of node's participating in the route formation using trusted nodes. Thus, it is essential that the routing protocols would be familiar with the reliability of the participating nodes [1]. Although, the cryptography based algorithms

addressing security take more time, and thus, it becomes simple for the attackers to acquire the crucial information using powerful computers. Trust management is a solution that can effectively manage the packet security sent over the network. The trust value is assigned dynamically for each node and the key factor involved in the trust calculation is node's behaviour [4]. The security is enhanced under the infrastructure-less mode of communication by adapting trust management concepts in MANETs. The modelling of trust is useful to provide secure communication and optimizing power parameters in MANETs. The conventional security methods, such as cryptographic techniques, firewalls, and intrusion detection systems are less effective in providing security during MANET communication [5].

The classes that protect MANETs are hybrid, reactive, and proactive in nature based on routing. The protocol which is proactive are based on tables, which depict the routes to the required destination over the network. The major challenge relies on control overhead in preserving the routes, which may not be useful for reaching the destination. The routing protocols which are proactive include Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), and Optimized Link State Routing (OLSR). Reactive protocols process on-demand basis, where the routes are revealed on demand. The routing is essential in QoS support, whereas its performance is susceptible while changing network topologies. The node mobility is responsible for the changes caused by the mobile wireless networks [18]. The result of broadcast nature of wireless networks generates additional security disclosure [17]. Due to the insecure physical medium, there is a need of designing security-aware routing algorithms in MANETs. The security solutions in MANETs aim to offer services related to security that involves anonymity, authentication, availability, integrity, and confidentiality for mobile users. Different routing protocols are designed in the literature, which includes Link Stable Multicast Routing [13], Adhoc On-demand Distance Vector (AODV), Defence against Sybil attacks [9], and OLSR [12] [15].

This paper proposes an efficient routing scheme based on reputation factors and power for providing secured paths in MANET. The technique utilized for initiating secured routing is KH-GOA that combines KH in GOA and provides most favourable path considering the reputation factors. The parameter used in the technique contains power, distance, delay and reputation. Thus the above parameter is considered for evaluating the fitness function and is evaluated as a maximization function. Thus, the proposed scheme maximizes the network lifetime and performance. The steps considered for the proposed KH-GOA routing algorithm are given below: Discovering the possible number of disjoint paths, and then, finding the best path using the above parameters. Hence, the proposed KH-GOA technique offers the best possible route for transmitting data with suitable detection rate, delay, power, and throughput.

The major contributions of the secured routing protocol are as follows,

- To design a hybridization technique, named KH-GOA, by combining KH and GOA for initiating safe routing in MANET by adapting measures that include security and power.
- To discover a best route using k-disjoint paths and on the basis of the multi-objective model, i.e., power, delay, reputation, and distance to initiate a data transmission in such a way that the adapted route is protected and effectual.

The organization of the paper is described as mentioned below where Section 2 elaborates the existing techniques on the basis of routing that are utilized in the previous research that inspired for developing the proposed method. Section 3 explains the model of system and challenges faced by the existing techniques. Section 4 describes the proposed KH-GOA technique for secure routing and Section 5 provides the results with respect to the proposed techniques and Section 6 presents the conclusion.

2. MOTIVATION

2.1 Literature Survey

In this section, the techniques used in the previous researches are analyzed for secured routing in MANET topology, which provides inspiration for executing the proposed secure routing scheme.

Md. Mahbubur Rahman and Md. Akhtaruzzaman [5] designed a technique on the basis of weighted metric by considering certain parameters, such as distance, speed between nodes, and remaining battery power to determine the routes in MANET. The method adopts a weighted combination of parameters, which include distance, battery power and velocity for choosing Most Forward within Radius (MFR) method. The method maximizes the performance and lifetime of the network, but loses the packet while transmitting data.

Menaka, R [23] proposed a model using fuzzy, trust and reputation parameters to enhance the performance of the network containing unreliable nodes. Thus, a protocol, named Dynamic Source Routing (DSR), is investigated to evaluate the performance under unreliable environment. The reputation system is responsible for taking input from past records of success transmissions, node capability computed as a value of trust and mobility of node. The reputation and trust parameters detect the secure route for transmitting data in the network.

S. Sharma [24] designed a technique, named reputation based secure routing protocol, for identifying the paths between sources and destinations by avoiding the malicious nodes. The method adapts a legitimacy value table and the reputation level table for maintaining the backbone network. The best path is discovered using the tables by ignoring the suspicious nodes.

ChrispenMafirabadza and PallaviKhatri [4] designed an Efficient Power Aware Ad-hoc on-Demand Distance Vector (EPAAODV) protocol, which is the modified version of AODV protocol. The method maximizes the network lifetime in the MANET. The analysis depends on energy consumption,

throughput, and Packet Delivery Ratio (PDR) is done to evaluate the performance of method.

S. Sathish *et al.* [7] designed Intelligent Beta Reputation and Dynamic Trust (IBRDT) model to provide security in wireless ad hoc networks. The model integrates beta reputation trust and dynamic trust to provide secure routing using wireless ad hoc networks. The packet is dropped due to link error and presence of malicious node, which could be identified by Secured AODV (SAODV). The protocol uses Pseudo-Random Function (PRF) for succeeding in storage scalability by fixing the client secret key using server's secret key.

K. Vanitha and A. M. J. Zubair Rahaman [10] developed a method, named Improved Failure aware Third-Party Auditor (IFTPA), using Homomorphism Linear Authenticator Mechanism (IFHM) and SAODV. The method has an ability to verify the suspicious data packet and permits the detection of malicious nodes.

Almazyad, A.S. [21] designed a reputation scheme and applied the scheme in different ways considering the throughput parameter in MANET. The simulation of the scheme is done based on four different scenarios, where the reputation of the node is evaluated for choosing the most effective route and to negotiate the effects of suspicious node performing grey-hole effects.

Mukherjee, S *et al.* [22] developed a trust-based routing protocol, named Enhanced Average Encounter Rate-AODV (EAER-AODV), which adapts the trust using the estimation of nodes. In EAER-AODV, estimation denotes the trust in between the nodes that is enhanced recurrently based on the specifications of the protocol. Trust based on the recommendationis utilized for exchanging the information related to trust from nodes. These protocols uses a node for selecting a routing path based on the values of trust using its neighbor nodes.

2.2Challenges

The challenges faced by the existing techniques to obtain a secure route among MANET nodes are listed as follows:

-There are different factors, like link load, node reliability and route hops, which are responsible for route efficiency, making the routing algorithm more challenging [1].

-The existing MANET routing protocols consider that each nodework in a compassionate manner, which results in susceptible behavior of MANETs against suspicious attacks, in which suspicious nodes are considered. The attackers consider data, bandwidth, battery power and routing protocols for initiating the attack [3] [1].

-The establishment of routes and data transmission is prone to various types of attacks while considering MANET setup, in which the misbehaving of nodes affects the overall path discovery process using impersonation or respond to information that governs to false route. Thus, the information transfers the whole control of network to the intruder [14].

-Various protocols are designed for MANETs, which are subjected to deal with several issues, such as more power consumption, large rates of errors and less bandwidth [5].

-In [23], a fuzzy-based model is developed that adapts a centeroid method in the defuzzification process, but it faced the difficulty while computing complex membership functions.

-The reputation-based secure routing protocol designed in [24] determines the optimal path with less overhead, but for improving the false positive and false negative rate, it requires secured algorithms.

3. MANET system model

The system model of MANET, represented in figure 1, elaborates the data transmission from source node to destination node by selecting a single path as the optimal path for routing the data. Here, the gateway is a communicating device responsible for providing an interface in between intermediate networks for improving connectivity and coverage. The mobile nodes access the internet connectivity for initiating the communication with wireless devices and to access the information. Assume a graph $S(X,Y)$ in a MANET, where $X=\{x_1,x_2,\ldots x_a,\ldots x_q\}$ represents a node set, where q represents the total nodes present in the network where $1\le a\le q$ and Y denotes a link set, where $y=\{y_1,y_2,\ldots,y_j\}$, which connects two nodes x_p and x_s where $1\le p\le s\le q$. The multi-objective functions considered for designing the MANET are reputation factor, power, distance, and delay. The links between the MANET nodes use the multi-objective functions for transmitting data between two nodes x_p and x_s. Assume A represents the source node, which sends information towards the destination, expressed as B.

While transmitting data from one node to another, distance is considered as an important paradigm, and the node mobility is used for determining the paths. The last parameters to be considered for the data transmission are reputation factor. The reputation factor is computed using the records of successful transmissions for computing the capabilities of nodes for evaluating the value of trust and the mobility of the nodes to yield secure transmission. Hence, reputation is important for MANET routing to provide secure transmission in the network. Thus, it is important to construct a model using distance, power, delay, and reputation factor for secured MANET routing. The reputation factor is responsible for choosing the optimal path by ignoring the suspicious nodes while discovering paths. Each node requires high power for transmitting data from one node to another node. Due to large transmission, the powerof nodes is drained out, which degrades the behavior of the node and finally, becomes a dead node. Hence, the node having high power is taken for initiating the routing of the data. Moreover, the power is considered as an important parameter for a secure transmission in MANET. The mobile nodes participating in

the communication require high power consumption [25] for transmission and reception of data packets from another node. The modes used for splitting the total power are as follows, Idle Mode, Transmission Mode, Overhearing Mode, and Reception Mode.

The total power is represented as,

$$J^a = H^T + H^R + H^I + H^O \quad (1)$$

where, H^T denotes transmission power, H^R denotes reception power, H^I denotes power consumed in idle mode, and H^O denotes power consumed in overhearing mode. The modes considered are briefly defined as follows,

3.1 Mode while transmitting data packets

In the transmission state, a node transmits data packets to another node in the network. Thus, a node needs more energy for transmitting a data packet, and this energy is calledtransmission energy of the nodes. The transmission energy is directly proportional to the data packet size, which means if the data packet size increases, the transmission energy is increased, and the transmission power is represented as,

$$H^T = \frac{W}{Q_y} \quad (2)$$

where, W represents the transmission energy, and Q_y expresses time used for transmitting the data packet.

3.2 Mode while receiving data packets

In the reception state, a packet is received from another node, and the received energy is known as reception energy. The power acquired after receiving packets is formulated as,

$$H^R = \frac{U}{Q_z} \quad (3)$$

where, U represents the reception energy, and Q_z expresses the time used for receiving the data packet.

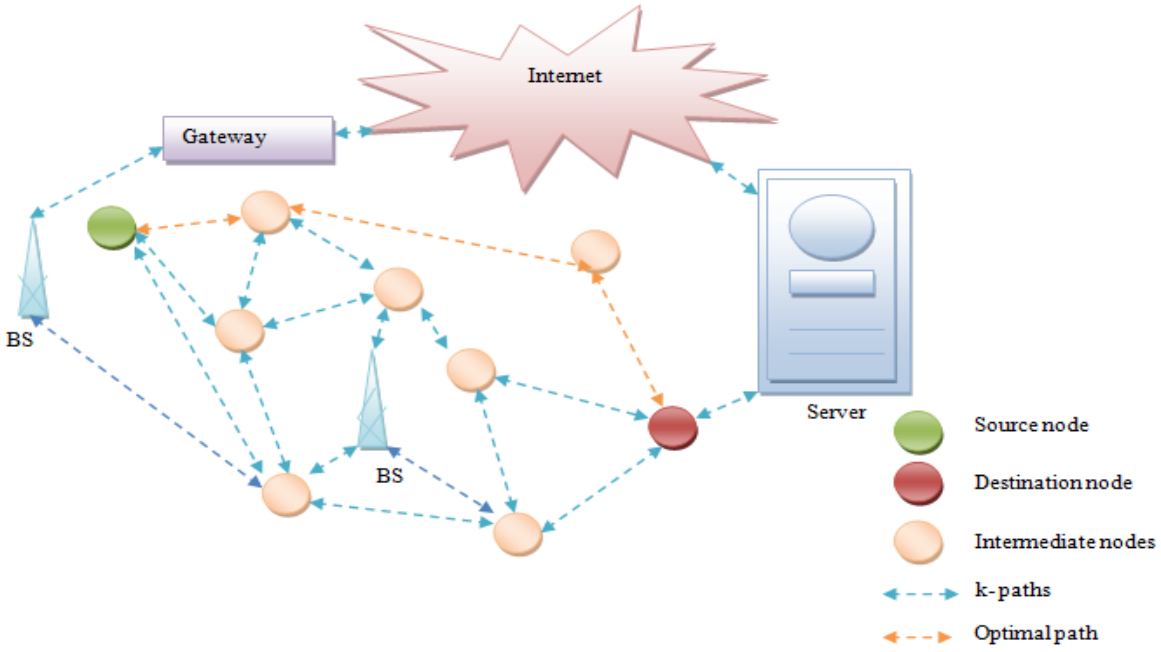


Figure 1. System model of MANET

3.3 Mode in Idle state

A node is in idle mode if it neither transmits the data packets nor receives any data packet. However, this node requires power for hearing the wireless medium for detecting a packet and after the detection of packet, the mode is switched into receiving mode from the idle mode. The idle mode consumes power, which is represented as,

$$H^I = H^R \quad (4)$$

where, H^I denotes the power consumed in idle mode.

3.4 Mode in Overhearing state

A node receives a data packet, which is not intended for it, and it requires energy while receiving in case of overhearing mode. Thus, the power consumption in overhearing mode is represented as,

$$H^O = H^R \quad (5)$$

where, H^O denotes the power consumed in overhearing mode.

4. Proposed KH-GOA for secure MANET routing

This section describes the scheme of initiating secure routing of data from initial node to the destination using the proposed KH-GOA algorithm, as illustrated in figure 2. It contains three steps, namely path discovery, application of optimization technique and discovering optimal paths for routing. In the first step, a possible number of paths to transmit the data from the source to destination are discovered and the optimal paths are selected using the proposed KH-GOA. Later, the data packets are sent from one node to another using the obtained optimal path. The routing of data packets is carried out optimally based on power, reputation factor, distance, and delay parameters, and thus, the proposed KH-GOA provides secure transmission. The proposed KH-GOA adapts node factor for calculating the fitness to evaluate the optimal path. The paths having maximum reputation factor, and reduced delay, minimum distance, and minimum power consumption, make the fitness maximum and thereby, form an optimal path for secured data transmission. The purpose of the proposed KH-GOA is to choose the optimal path from the detected paths using the above described parameters for secure data transmission. The next section elaborates the solution encoding, newly designed fitness function and the elaboration of the proposed KH-GOA.

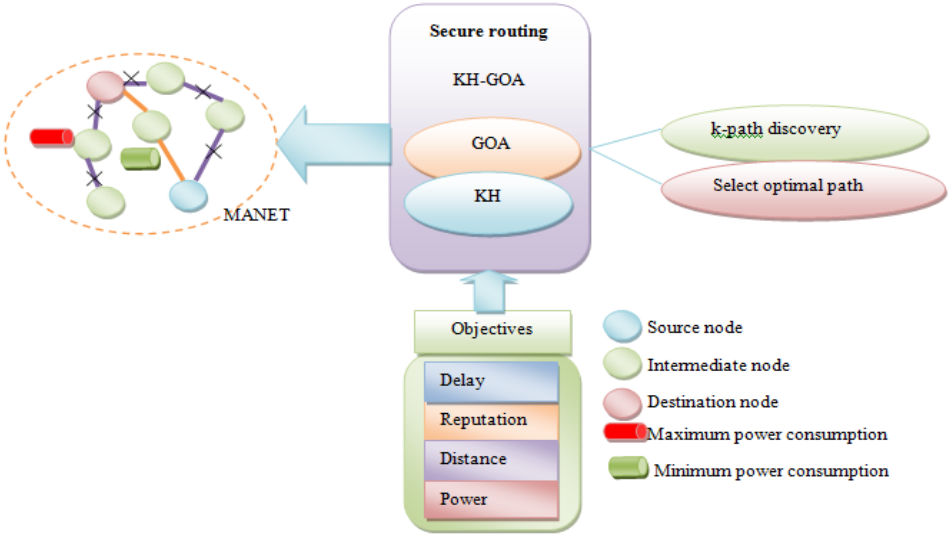


Figure 2 Schematic diagram of the proposed KH-GOA based secured routing

4.1 Solution representation

Solution representation is an important for determining an optimal solution in optimization problems from a set of solutions. Here, the solution encoding is to determine the optimal path for transmitting data. This encoding helps to selectthe optimal path and represents the path with its binary representation. Assume a WSN with k number of paths among which the proposed KH-GOA algorithm selects f optimal path, where $1 \le f \le k$ for transmitting the data from the one node to other node. The solution of KH-GOA represents k paths, from which f optimal path is selected based on the newly designed fitness function.

4.2 Fitness function

The solution encoding procedure is followed by the computation of fitness function to find the optimal path. Here, the optimal path is selected by adapting the node factors, such as distance, power, delay and reputation. The fitness computed for the proposed KH-GOA must be greater. Thus, the fitness computed for the proposed KH-GOA is given by,

$$Fitness = \sum_{i=1}^{|q|} L_i \quad ...(6)$$

where, i denotes the total intermediary nodes in the selected route, q denotes total nodes, and L_i denotes the node factor.

The node factor is responsible for obtaining a secured path for transmitting data from the one node to the other node. The factors responsible for checking the node stability during path discovery is evaluated using node factors, which involve reputation factor, power, distance, and delay.

The node factor is given by,

$$L_i = \frac{1}{4} \times \left[Z^a + [1 - H^a] + [1 - C^a] + [1 - G^a] \right] \quad ... (7)$$

where, Z^a denotes the reputation factor of the a^{th} node, H^a represents the power consumed by the a^{th} node, C^a expresses the distance between the a^{th} node and previous node, and G^a represents the delay of a^{th} node.

4.2.1 Reputation factor

Reputation factor [23] is defined as a factor, which is employed for selecting the optimal path by ignoring the suspicious nodes, while initiating the path discovery process. The reputation table is maintained for collecting the reputation values to separate the suspicious nodes and thereby, makes a path from one node to other node. The reputation system is responsible for node selection to transmit data packets from the one node to the other node. The reputation value is computed using node's capability, previous records, mobility, and reputation among the neighbours. Thus, a secured transmission is performed using the maximum reputation values.

$$Z_a^w = \frac{1}{4}\left[O_a^w + [1 - Q_a^w] + E_a^w + F_a^w\right] \quad ...(8)$$

where, w denotes the current time, O_a^w denotes the previous records that is history for the a^{th} node at a time w, Q_a^w denotes the mobility for the a^{th} node at a time w, E_a^w denotes the actual capability for the a^{th} node at a time w, and F_a^w denotes the reputation among the neighbors for the a^{th} node at a time w.

a) **Previous records**

The reputation system is responsible for taking input from previous records of successful transmissions.

$$O_a^w = [Z_a^{w-1} + \frac{1}{2} \times Z_a^{w-2}] \times \frac{1}{2} \quad (9)$$

where, Z_a^{w-1} represents the reputation value at the time $w-1$, and Z_a^{w-2} indicates the reputation value at the time $w-2$.

b) Node capability

The node's capability is the ratio of total bytes sent and the total capacity.

$$E_{a_{\max}}^w = \left[\frac{U_s}{V}\right] \quad (10)$$

where, U_s represents the number of bytes sent, and V expresses the total capacity.

c) Node mobility

The next parameter is node mobility [23], in which certain nodes move in the predefined path, and some node moves randomly. The mobility of the nodes in the MANET is discovered individually according to their own responsibilities and is considered as arbitrary. The node selection process is affected while the movement of the nodes is fast, whereas it is improved if the movement of the nodes is slow as it becomes simple for managing the neighborhood nodes. The mobility values can attain high, medium, and low values while the moving of the node is steady, and fast respectively. The mobility of the nodes is calculated based on the location of the nodes as,

$$Q_a^w = \frac{Dist(I_a^{w-1}, I_a^w)}{\alpha} \quad (11)$$

where, $Dist(I_a^{w-1}, I_a^w)$ indicates the distance between the location of a^{th} node at time $w-1$ and location of a^{th} node at time w, and α represents the normalization factor.

d) Reputation neighborhood

The total number of neighbors present close to a node is known as reputation neighbourhood. It is computed as a relation between neighborhood characteristics and reputation.

$$F_a^w = \frac{1}{|L|}\sum_{j=1}^{|L|} L_{j,a} \quad (12)$$

where, $|L|$ represents the number of neighbors, and j indicates neighboring node.

4.2.2 Power

The minimum power consumed by the node is responsible for transmitting data packets and is calculated for each node as given in equation (1).

4.2.3 Distance

The difference between the distance of a^{th} node and $(a-1)^{th}$ node is divided by the normalization factor for computing the distance and is represented as,

$$C^a = \frac{Dist(a, a-1)}{\alpha} \quad (13)$$

where, α represents the normalization factor.

4.2.4 Delay

The delay is computed based on the total nodes and is high for the increasing total nodes. Hence, the parameter delay must be less while selecting the optimal path for transmitting data. The delay is given by the ratio of the total nodes in a route to the total number of nodes.

$$G^a = \frac{o}{q} \quad (14)$$

where, o indicates the total nodes in the corresponding path, q represents the total nodes.

4.3 Proposed KH-GOA

KH-GOA is proposed by combining Krill Herd (KH) algorithm [26] and Grasshopper Optimization Algorithm (GOA) [27] for selecting the optimal path to send the data

from the one node to the another node. KH algorithm is inspired from krill herding motions used for solving the complex optimization problems. It simulates the krill behavior carefully and utilizes the real world empirical studies for obtaining the coefficients using the fine-tuning process. It is considered as an effective algorithm as compared to other nature-inspired algorithms due to the fine-tuning of the time parameter. The initial testing of KH algorithms represents that it is encouraging for future application in optimizing the tasks. Meanwhile, GOA contains changing comfort zone coefficient for balancing exploitation and exploration, which assist GOA not to be fascinated in local optima and discovers an accurate in a global medium. GOA has the potential to solve real problems in unknown search spaces. Hence, the integration of KH algorithm and GOA is made for finding the routing paths effectively from the source to the destination and to improve the performance of the optimization problem. The update rule of KH algorithm is induced in GOA to provide an optimum solution with the security using a multi-objective function. The proposed reputation model contains certain reputation parameters, which include node mobility, actual capability of the node, previous records, and reputation among the neighbors. The steps involved in KH-GOA algorithm are elaborated in the given steps,

I. Initialization

Initially, the set of the solution, algorithmic parameters and criterion for the termination are defined. The algorithm starts with the initialization phase, where the solution size S having l solutions, is initiated at random. Each solution in S is represented as,

$$S = \{S_1, S_2, \ldots, S_m, \cdots S_l\} \quad . \quad \text{.. (15)}$$

where, l represents total population size where, $1 \le m \le l$.

II. Evaluation of fitness

The next step is the computation of fitness function for searching the best solution. The node factors, such as power, reputation factor, distance and delay, are considered for evaluating the fitness function. Here, the fitness function is computed for an individual solution using equation (6) to get the best solution. The best solution is found at the last iteration as every solution seeks to obtain the optimal position**.**

III. Update Positions and evaluation

Consider l number of solutions is obtained with $k_{\max}$ iterations, where worst solution and best solution are generated. The updated solution considers only the parameter, which has the tendency to move to the best solution and discards the solution that is close to the worst solution.

According to KH algorithm, the position vector of krill in interval k and Δk is formulated as follows,

$$S_m(k + \Delta k) = S_m(k) + \Delta k \frac{dS_m}{dk} \quad (16)$$

where, $S_m(k)$ represents the m^{th} solution during k^{th} interval. The parameter Δk should be set carefully considering the optimization problem because this parameter works as a scale factor for the speed factor.

The above equation is rearranged and is represented as,

$$S_m(k) = S_m(k + \Delta k) - \Delta k \frac{dS_m}{dk} \quad (17)$$

According to GOA, the current position, target position, and grasshopper position is used for defining the next position. The first component of the equation deals with the location of the current grasshopper with respect to other grasshoppers. The status of grasshoppers is used to describe the position of the search agents around the target. The update equation of grasshopper to solve the optimization problem is given by,

$$S_m^r(k + \Delta k) = g\left(\sum_{\substack{n=1 \\ n \ne m}}^{l} g \frac{M_r - N_r}{2} t(|S_n^r - S_m^r|) \frac{S_n - S_m}{h_{mn}} \right) + \hat{P}_r^* \quad (18)$$

where, r represents the dimension, g represents the decreasing coefficient, l denotes the total number of grasshoppers in dimension r, n, m denote the position of grasshoppers in dimension r, M_r and N_r represent the upper bound and the lower bound in r^{th} dimension, t represents the strength of social forces, $h_{m,n}$ represents the distance between two grasshoppers in dimension r, P_r^* represents the best solution obtained so far.

Assume $l = 1$,

$$S_m^r(k + \Delta k) = g^2 \frac{M_r - N_r}{2} t(|S_1^r - S_m^r|) \frac{S_1(k) - S_m(k)}{h_{m1}} + \hat{P}_r^* \quad (19)$$

Substituting equation (17) in (19),

$$S_m^r(k + \Delta k) = g^2 \frac{M_r - N_r}{2} t(|S_1^r(k) - S_m^r(k)|) * \frac{S_1(k) - S_m(k + \Delta k) + \Delta k \frac{dS_m}{dk}}{h_{m1}} + \hat{P}_r^* \quad (20)$$

After rearranging, the equation obtained is represented as follows,

$$S_m^r(k+\Delta k)+g^2\frac{M_r-N_r}{2}t(|S_1^r(k)-S_m^r(k)|)\frac{S_m(k+\Delta k)}{h_{m1}}=$$
$$g^2\frac{M_r-N_r}{2h_{m1}}g(|S_1^r(k)-S_m^r(k)|)[S_1(k)+\Delta k\frac{dS_m}{dk}]+\hat{P}_r^* \quad (21)$$

$$S_m^r(k+\Delta k)\left[1+g^2\frac{M_r-N_r}{2}t(|S_1^r(k)-S_m^r(k)|)\right]=$$
$$g^2\frac{M_r-N_r}{2h_{m1}}g(|S_1^r(k)-S_m^r(k)|)[S_1(k)+\Delta k\frac{dS_m}{dk}]+\hat{P}_r^* \quad (22)$$

The final expression for proposed KH-GOA for determining the optimal path is given by,

$$S_m^r(k+\Delta k)=\frac{2h_{m1}}{2h_{m1}+g^2M_r-N_rt(|S_1^r(k)-S_m^r(k)|)}*$$
$$\left\{g^2\frac{M_r-N_r}{2h_{m1}}t(|S_1^r(k)-S_m^r(k)|)[S_1(k)+\Delta k\frac{dS_m}{dk}]+\hat{P}_r^*\right\} \quad (23)$$

IV. Replace with the best solution

After evaluating the update position, the fitness of each solution is calculated and the solution yielding maximum fitness is replaced to form the best solution.

V. Termination

The process is continued till the optimal solution is detected, and the algorithm is stopped after reaching the maximum iteration $k_{\max}$ or in the case when no fittest solution is obtained.

The pseudo code of the proposed KH-GOA algorithm for secure routing is given below in Table 1.

Table 1. Pseudo code of KH-GOA algorithm

	KH-GOA Algorithm
1	**Input:** Population S
2	**Output:** Optimal Solution P_r^*
3	Begin
4	Initialize the population
5	Update M_r, N_r, g, t and h
6	while $(k < \mathrm{k}_{\max})$
7	for each solution in the population
8	Calculate the fitness using equation (6)
9	Update the position using equation (23)
10	Generate new set of solutions
11	Compute the fitness for the new solutions
12	Choose the solution having maximum fitness as P_r^*
13	$k = k+1$
14	end while
15	Return P_r^*
16	Terminate

5. RESULTS AND DISCUSSION

This section demonstrates the results of the proposed KH-GOA based secure routing protocol with respect to the existing methods.

5.1 Experimental Setup

The proposed KH-GOA is executed in a system with Windows 10 OS, 2 GB RAM, and Intel CPU 2.16 GHz processor. The experimentation of KH-GOA is carried out in NS2 simulator using different metrics, such as delay, detection rate, power, and throughput.

5.2 Performance Evaluation

In this section, the parameters, which are used for computing the performance of the algorithms used for secured routing. The measures used for evaluating the performance are throughput, PDR, and energy.

Power: The data transmitted in MANET from the nodes uses considerable power. The power consumed in the proposed routing protocol is measured using equation (1).

Throughput: The behaviour of the methods can be evaluated using throughput values, which provide the total data a packet received at a time and in this manner, it acknowledges the packet delivery.

$$Throughput = q/k$$

where, q is the total number of nodes received per simulation time k .

Detection rate: The detection rate is defined as the ratio of the number of malicious node that is detected correctly to the number of nodes available in the MANET.

Delay: The delay is computed as the time taken by application request or information to give a response.

5.3 Comparative methods

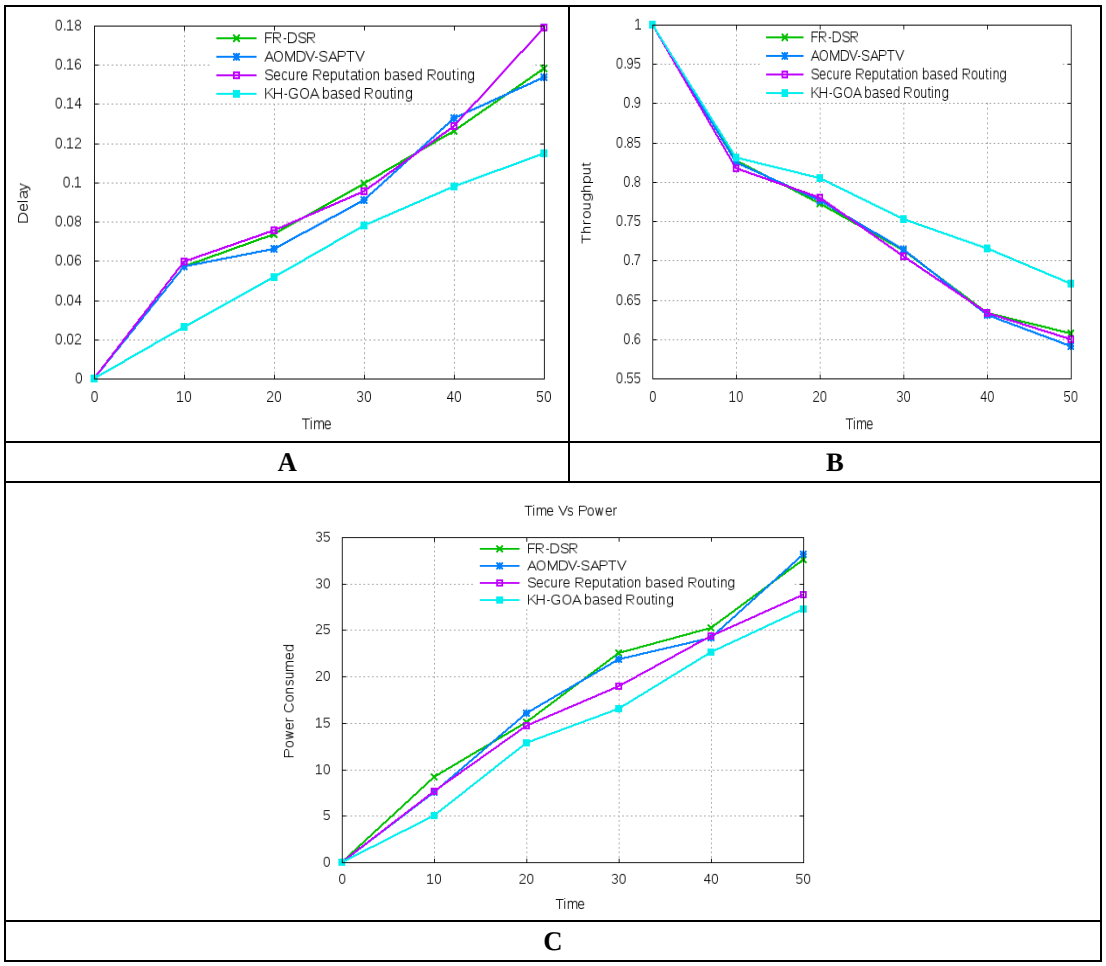
The performance of the proposed KH-GOA based routing protocol is estimated by comparing the proposed KH-GOA with the existing methods. Here, three existing methodologies, such as Fuzzy Reputation dynamic source routing (FR-DSR) [23], Ad hoc On-demand Multi-path Distance Vector protocol-Secure Adjacent Position Trust Verification (AOMDV-SAPTV) [6], and Secure reputation based routing [24], are taken for comparison.

5.4.1 Comparative Analysis

The comparative analysis of KH-GOA based routing protocol is carried out with respect to the existing approaches based on power, throughput, delay and detection rate, considering two attacks: Black hole attack, Flooding attack and without attack.

The analysis based on delay, throughput, and power consumed in case of without attack scenario is depicted in figure 3. The performance of the AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA with varying time is evaluated in terms of delay and the result is illustrated in Figure 3a. The time is varied from 0s to 50s for computing the delay values. At time 10s, the delay measured by AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA is 0.0570ms, 0.0598ms, 0.0572ms and 0.0263ms, respectively. Similarly, at 50s, AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA measure delay values as 0.153ms, 0.178ms, 0.157ms, and 0.114ms, respectively. Hence, the time taken to get response is faster in case of the proposed technique. Figure 3b shows the analysis based on detection rate using AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA for varying time ranging from 0s to 50s. The throughput for AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA at time 40s are 0.630, 0.633, 0.632, and 0.715. When the time is 30s, the corresponding rate of detection for AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA is 0.714, 0.704, 0.712, and 0.753. From the graph, it is seen that the throughput gradually increases in the proposed KH-GOA. Thus, it can be concluded that the proposed technique detects the malicious nodes more precisely than the existing methods. The power consumed by AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA is depicted in figure 3c. The power measured by AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA at 20s is16.017W, 14.722W, 15.084W, and in the proposed technique, the power consumed is 12.861W respectively. Considering the above data, it can be ruled out that the existing techniques consumed more power. The proposed technique outperforms the existing techniques and proves that it can successfully deploy the services with respect to existing techniques. The analysis based on delay, detection rate, throughput, and power considering flooding attack scenario is depicted in figure 5. The delay for the existing methods and the proposed KH-GOA are compared and is depicted in figure 5a. When the time is 30s, the corresponding delay values measured by AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA are 0.112ms, 0.103ms, 0.113ms, and 0.098 ms. The proposed technique shows least delay amongst other methods. Figure 5b shows the analysis based on detection rate with the comparative methods, AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA with the time varying from 0 to 50s.

A. Analysis considering without attack scenario



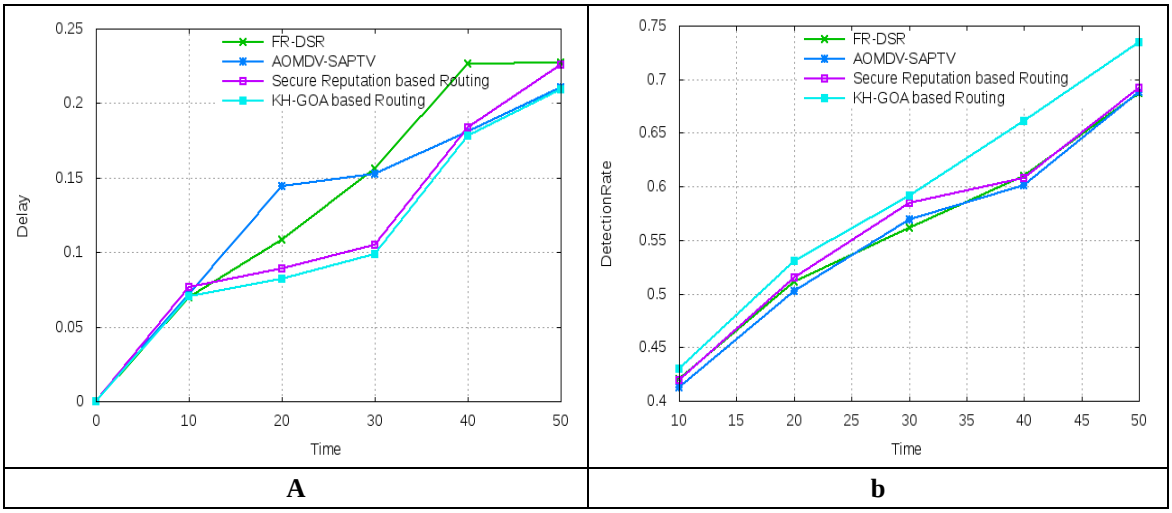
A **B**

C

Figure 3. Analysis based on without attack scenario using a) Delay b) Throughput c) Power

When the time is 50s, the corresponding values of detection rate measured using AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA are 0.689, 0.713, 0.690, and 0.721.

B. Analysis considering Black hole attack scenario



A **b**

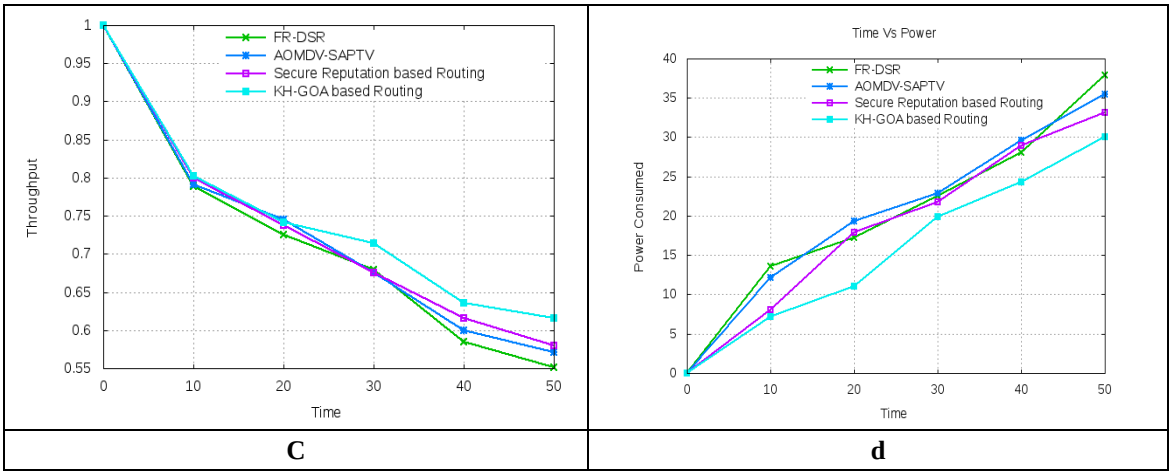


Figure 4. Analysis based on Black hole attack scenario using a) Delay b) Detection rate c) Throughput c) Power

C. Analysis considering Flooding attack scenario

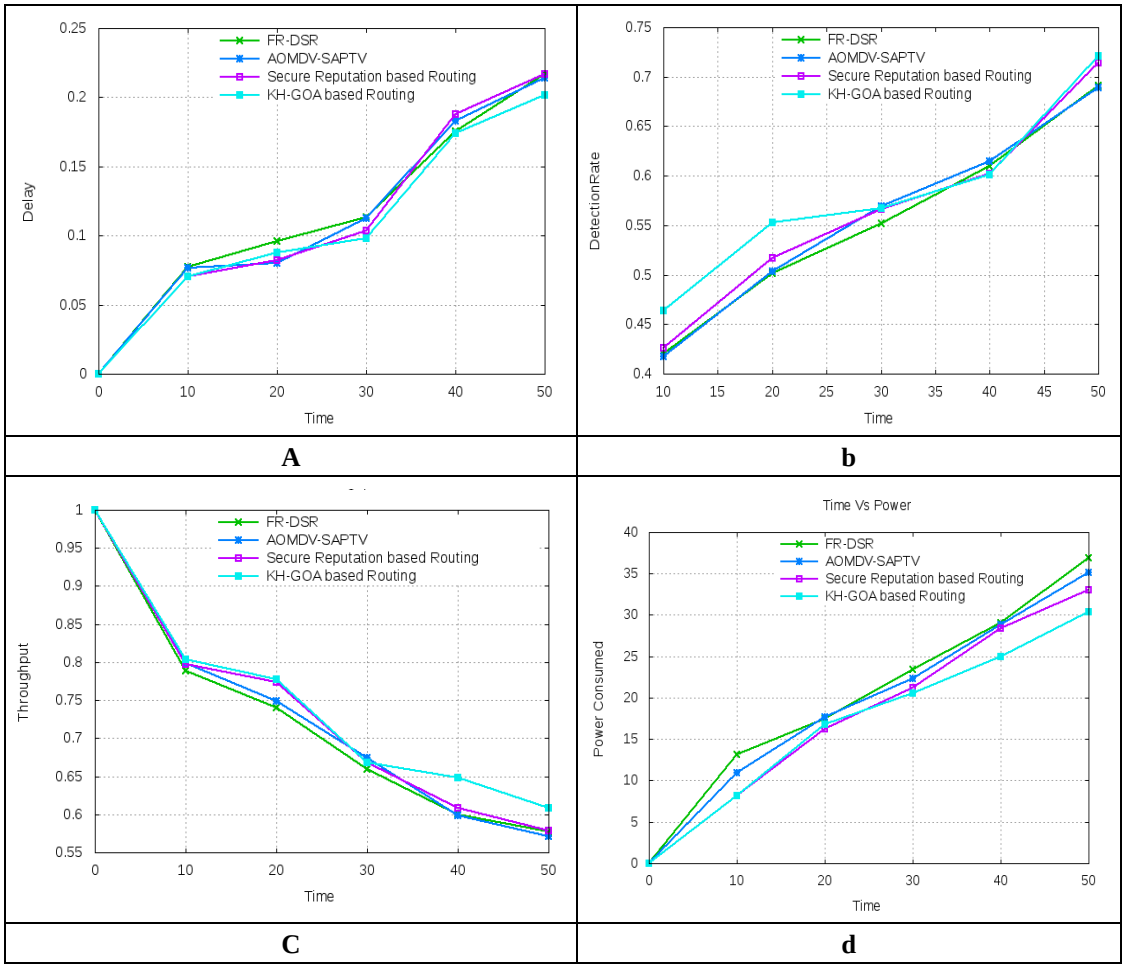


Figure 5. Analysis based on without attack scenario using a)Delay b) Detection rate c) Throughput c) Power

The throughput values measured by AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA with varying time is analysed and depicted in figure 5c. The throughput values of AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA when the time is 50s are 0.571, 0.578, 0.577, and 0.607. The analysis based on power consumption for varying time measured by the methods is depicted in figure 5d. When the time is 50s, the corresponding values of power measured by AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA are 35.082W, 33.058W, 36.0897W, and 30.354W, respectively.

5.5 Comparative Discussion

Table 1 presents the discussion of the comparative analysis to prove the superiority of the proposed method. In the case of the detection rate, AOMDV-SAPTV, Secure reputation based routing, FR-DSR, and proposed KH-GOA attain 0.689, 0.713, 0.690, and 0.734 at 50s respectively. Hence, the ability to detect the malicious nodes is higher in the proposed method. Similarly, the delay, and the throughput for the proposed technique is 0.114ms, and 0.670. Moreover, the power is lesser for the proposed method with value 27.313W. From the comparative analysis, it is seen that the proposed method has the maximum performance with detection rate, delay, throughput, and power of 0.734, 0.114ms, 0.670 and 27.313W, respectively. Thus, it is clearly proved that the proposed method is superior to the existing methods in terms of delay, detection rate, throughput, and power.

Table 1. Comparative Discussion

Techniques	Detection Rate	Delay	Throughput	Power
AOMDV-SAPTV	0.689	0.153	0.590	33.143
Secure reputation based routing	0.713	0.178	0.599	28.792
FR-DSR	0.690	0.157	0.606	32.590
KH-GOA	**0.734**	**0.114**	**0.670**	**27.313**

6. CONCLUSION

In this paper, the technique, named KH-GOA, is proposed for initiating secure routing in MANET. The hybridization of KH and GOA is adapted to select the best path to reach the destination. The algorithm evaluates the best path using certain parameters, which are power, distance, delay, and reputation factor. After evaluating the security parameters, the nodes yielding minimum power, minimum delay, minimum distance, and maximum reputation factor are used for selecting the optimal path. Reputation is the security parameter adapted in KH-GOA that offers security using the reputation factors while transmitting data packets from one node to another node. The reputation factors, such as node mobility, previous records, actual capability and reputation neighbourhood are considered to attain a secured path for routing data packets. The execution of the proposed KH-GOA is in NS2 simulator. The performance of the proposed KH-GOA is evaluated using power, throughput, delay and detection rate with values 27.313W, 0.670, 0.114, and 0.734ms and is compared with existing techniques, such as AOMDV-SAPTV, Secure reputation based routing, and FR-DSR .

REFERENCES

[1] Zhang, M., Yang, M., Wu, Q., Zheng, R. and Zhu, J., “Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs,” Future Generation Computer Systems, 2017.

[2] Sathiamoorthy, J. and Ramakrishnan, B., “Design of a proficient hybrid protocol for efficient route discovery and secure data transmission in CEAACK MANETs,” Journal of Information Security and Applications, vol. 36, pp.43-58, 2017.

[3] Ahmed, M.N., Abdullah, A.H., Chizari, H. and Kaiwartya, O., “F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs,” Journal of King Saud University-Computer and Information Sciences, vol. 29, no. 3, pp.269-280, 2017.

[4] ChrispenMafirabadza and PallaviKhatri, "Efficient Power Aware AODV Routing Protocol for MANET," Wireless Personal Communications, vol. 97, no. 4, pp. 5707-5717, 2017.

[5] Md. MahbuburRahman and Md. Akhtaruzzaman, "An Efficient Position based Power Aware Routing Algorithm in Mobile Ad-hoc Networks," International Journal of Computer Network and Information Security, vol. 7, pp. 43-49, 2016.

[6] Borkar, G.M. and Mahajan, A.R., “A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks,” Wireless Networks, vol. 23, no.8, pp.2455-2472, 2017.

[7] Sathish, S., Ayyasamy, A. and Archana, M., "An Intelligent Beta Reputation and Dynamic Trust Model for Secure Communication in Wireless Networks," In Industry Interactive Innovations in Science, Engineering and Technology, Springer, vol.11, pp. 395-402, July 2018.

[8] Navin Mani Upadhyay, KumariSoni, and Arvind Kumar, "Power Aware Routing in Mobile Ad Hoc Networks by using Power Aware Matrices," International Journal of Computer Applications, vol. 166, no. 11, pp. 24-29, 2017.

[9] Kumari, S.V. and Paramasivan, B., “Defense against Sybil attacks and authentication for anonymous location-based routing in MANET,” Wireless Networks, vol. 23, no. 3, pp.715-726, 2017.

[10] Vanitha, K. and Rahaman, A.Z., "Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol," Cluster

Computing, pp.1-9, March 2018.

[11] Jabbar, W.A., Ismail, M. and Nordin, R., "Energy and mobility conscious multipath routing scheme for route stability and load balancing in MANETs," Simulation Modelling Practice and Theory, vol. 77, pp.245-271, 2017.

[12] Z. Li and Y. Wu, "Smooth Mobility and Link Reliability-Based Optimized Link State Routing Scheme for MANETs," in IEEE Communications Letters, vol. 21, no. 7, pp. 1529-1532, July 2017.

[13] Singal, G., Laxmi, V., Gaur, M.S., Todi, S., Rao, V., Tripathi, M. and Kushwaha, R., "Multi-constraints Link Stable Multicast Routing Protocol in MANETs," Ad Hoc Networks, vol. 63, pp. 115-128, 2017.

[14] S. Surendran and S. Prakash, "An ACO look-ahead approach to QOS enabled fault- tolerant routing in MANETs," in China Communications, vol. 12, no. 8, pp. 93-110, August 2015.

[15] Tan, S., Li, X. and Dong, Q., "Trust based routing mechanism for securing OSLR-based MANET," Ad Hoc Networks, vol. 30, pp.84-98, 2015.

[16] Hongmei Deng, Wei Li and D. P. Agrawal, "Routing security in wireless ad hoc networks," in IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct 2002.

[17] E. Ayday and F. Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks," in IEEE Transactions on Mobile Computing, vol. 11, no. 9, pp. 1514-1531, Sept. 2012.

[18] Palanisamy, V., &Annadurai, P. "Impact of rushing attack on multicast in mobile ad hoc network," International Journal of Computer Science and Information Security, vol. 4, no. (1&2), 2009.

[19] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J. and Qiu, D., "Security of the internet of things: Perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp.2481-2501, 2014.

[20] D. He, C. Chen, S. Chan, J. Bu and A. V. Vasilakos, "ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks," in IEEE Transactions on Information Technology in Biomedicine, vol. 16, no. 4, pp. 623-632, July 2012.

[21] Almazyad, A.S.,"Reputation-based mechanisms to avoid misbehaving nodes in ad hoc and wireless sensor networks," Neural Computing and Applications, vol.29, no.9, pp.597-607, May 2018.

[22] Mukherjee, S., Chattopadhyay, M., Chattopadhyay, S. and Kar, P., "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, May 2018.

[23] Menaka, R., V. Ranganathan, and B. Sowmya, "Improving Performance Through Reputation Based Routing Protocol for Manet," Wireless Personal Communications, Vol. 94, No. 4, pp. 2275–2290, 2017.

[24] S. Sharma, "A secure reputation based architecture for MANET routing," in proceedings of 4th International Conference on Electronics and Communication Systems (ICECS), Coimbatore, pp. 106-110, 2017.

[25] Tantubay, N., Gautam, D.R. and Dhariwal, M.K., "A review of power conservation in wireless mobile adhoc network (MANET)," International Journal of Computer Science Issues, vol.8, no.4, pp.378, 2011.

[26] Gandomi, A.H. and Alavi, A.H., "Krill herd: a new bio-inspired optimization algorithm," Communications in Nonlinear Science and Numerical Simulation, vol.17, no.12, pp.4831-4845, 2012.

[27] Saremi, S., Mirjalili, S. and Lewis, A., "Grasshopper optimisation algorithm: theory and application," Advances in Engineering Software, vol.105, pp.30-47, 2017.

AUTHORS:

Mr.Nukam Reddy Srinadh received his B.Sc Degree in Mathematics, Physics and Chemistry from Sri Venkateswara University,Tirupti, A.P , India in 1997, Master of Computer Applications from Sri Venkateswara University in 2000,Mater Of Technology From AAIDU in 2006. Now He is pursuing Ph.D. from Rayalaseema University,Kurnool ,AndhraPradesh,India. His research areas Include Computer Networks/Secure Routing in MANET.

Prof. B. Sathyanarayana received his B.Sc Degree in Mathematics, Economics and Statistics from Madras University, India in 1985, Master of Computer Applications from Madurai Kamaraj University in 1988. He did his Ph.D in Computer Networks from Sri Krishnadevaraya University, Anantapur, A.P. India. He has 24 years of teaching experience. His Current Research Interest includes Computer Networks, Network Security and Intrusion Detection. He has published 30 research papers in National and International journals.