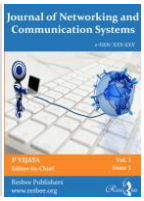
Resbee Publishers

Journal of Networking and Communication Systems

Received 18 April, Revised 27 June, Accepted 14 July



Hybrid PSGWO Algorithm for Trust-Based Secure Routing in MANET

Moresh Madhukar Mukhedkar
Dept. of Electronics Engineering
Ramrao Adik Institute of Technology,
Navi Mumbai, Maharashtra, India
moreshmadhukarmukhedkar@gmail.com

Uttam Kolekar
Dept. of Electronics Engineering
A. P. Shah Institute of Technology
Thane, Maharashtra, India

Abstract: In Mobile Ad Hoc Networks (MANETs), routing is considered an important issue because of the dynamic nature of the network. The interim communication associations are guaranteed because of the infrastructure-independent ability of MANET. However, with no appropriate centralized monitoring procedure that creates routing in MANETs regarding trust and security as a most important challenge. Hence, this works proposed the Advanced Encryption Standard-enabled Trust-based Secure Routing protocol on the basis of the proposed Particle Swarm-Grey Wolf Optimization Algorithm (AES-TPSGWO), that is trust and energy-aware routing protocol. The proposed Particle Swarm -Grey Wolf Optimization Algorithm is affianced in the best route chosen on the basis of the modeled objective model on the basis of the trust factors, new trust, direct as well as indirect trust, historical trust, with respect to the distance delay, and link lifespan. The Particle Swarm-Grey Wolf Optimization Algorithm is the incorporation of Particle Swarm and Grey Wolf Optimization technique which takes over the faster global convergence.

Keywords: Trust; Routing; Protocol; MANET; AES; Optimization

1. Introduction

Generally, to form a network, MANETs are considered as a group of mobile wireless nodes, which works collectively. These kinds of networks can exist without an associated infrastructure and they have the ability to work in an independent way. As the nodes are mobile, at any point of time, the connection breakage might take place, which depends on the spatial representation of the nodes. Two mobile nodes that are farther than the communication range have the ability to communicate with each other with the aid of other devices within their communication range. MANET presents communication abilities to regions, whereas insufficient or no set communication infrastructures subsist [9]. Moreover, MANET does not employ a lifeless network model. To present network connectivity it exploits multi-hop routing. In the routing protocols, network communication would be possible, which is exploited to find out the dynamic path in network communication. Additionally, the data are forwarded to the network. For a dynamic environment, the route continuation process is exploited to build the network. The network performance to the users is the decisive problem to sustain the Quality of service (QoS) [10].

MANETs are convenient networking pattern and it encompasses extensive applications in rapid consumption situations without need any prior arrangements similar to the circumstances of crisis, tactical operations, disaster relief. Additionally, the conception is helpful and suitable for the configuration of short-term multi-hop wireless connectivity allowing information sharing in commercial as well as technical meets and so on [11].

For pre-deployed communications, mobile devices reveal self organize proficiencies as well as form a network without the obligation. These networks are simple to organize, scalable as well as show enhanced suppleness [1]. Mobile ad hoc networks extravagance each obtainable node as a forwarding device, therefore, it expands the communication range. Through radio transmission, ad hoc networks encompass wireless facilitated connectivity of nodes and carry out multi-hop communication. Also, these networks can be fond of the fixed network to enhance the attainability. In the domain of Wireless Sensor Network (WSN), the applicability of these networks is additionally increasing, delay, intelligent transportation system, disruption-tolerant networks, and wireless mesh network [12]. Using the multi-hop idea of ad hoc, the drawback of the single-hop wireless connectivity is surmounting that needs every transitional node to do the routing function [13]. From the transmitter to the receiver node, the routing

of packets in deviating states and dynamic network topology because of the probable movements of the nodes is a confusing chore.

A MANET consists of a dynamic place of self-organizing mobile nodes otherwise devices without any fixed infrastructure directly communicates with each other. Hence, nodes in MANET carry out both routers the tasks as well as hosts in order to transmit packets toward their receivers on the basis of using a routing protocol. By MANET the routing protocols are used, which can be categorized on the basis of the topology such as reactive, proactive, as well as hybrid protocols [14].

Packets transmit by the sender node are communicated by a count of intermediary nodes previous to attaining the receiver node in a multi-hop case. In MANETs, because of the node mobility, recurrent path malfunctions and route discoveries happen. This may cause maximizes the end to end delay, minimizes the ratio of packet delivery as well as further prominently maximizes the overhead of the routing protocols. Hence, minimizing the routing overhead in route discovery in MANET is a necessary factor. In MANET, multipath Routing approaches are exploited to minimize the routing overhead. The multipath routing is the critical problem of routing, which will give load balancing, the augmented number of throughput, and the hard fault tolerance approaches in MANET [15]. It can be attained by minimizing network traffic. The removal of the bottleneck issue is considered as the main problem for reducing the congestion. The multipath routing algorithm is mostly exploited for enhancing the QoS in the network. The main intention of minimizing routing overload is to enhance the effectiveness of flourishing messages broadcasting. If the data packet is ineffective to distribute, it is the reason for the issue. By enhancing the flourishing rate of broadcasting, data packets are sent out to the last node from the start node. A number of techniques are unsuccessful to minimize the routing overload by itself [16].

The major intention of this work is to present the AES-TPGWO method for the optimal selection routing paths. The proposed AES-TPSGWO method is the hybridization of the Particle Swarm and Grey Wolf Optimization technique that plays a main role in choosing the best paths to improvement routing in MANET exploiting trust as the constraint. The main aspire model is used to select the optimal paths that are on the basis of historical trust, recent trust, indirect trust, delay, direct trust, distance, as well as link lifetime.

2. Literature Review

In 2019, Trilok Kumar Saini and Subhash C. Sharma [1], worked on routing, and methodical symbol of the suggestions, which was attractive. Here, a review of the extensive range of routing suggestions in the past 20 years for the ad hoc and mobile network was provided. Moreover, they had devised many types and categorization criteria untouched in many of the reviews. This review article presents an important general idea of the protocols, in addition arranges and classifies the routing protocols for logical design. In this review, protocol classification helps to methodically way in a huge set of protocols and places of interest the research developments in the domain.

In 2018, Dipika Sarkar et al [2], presented a novel method for routing selection integrating Ad-hoc On-Demand Distance Vector (AODV) protocol with Ant Colony Optimization (ACO) to enhance QoS in MANET. For data delivery, the optimum route was chosen by means of pheromone value of the path on the basis of the approach of the ant colony with AODV. Here, the pheromone value of a route was computed on the basis of the congestion, end to end reliability of the path, and a number of hops and remaining energy of the nodes beside the path. For transmission of the data packet the path that has uppermost pheromone value would be chosen.

In 2019, Subramanian Balaji et al [3] designed a cooperation algorithm and an infinitely-repeated game in order to discover malicious nodes and to improve energy-effectiveness. The main aim of an Infinitely-repeated game to guarantee the defector or malicious node in the network it possesses a long-run loss as well as a short-run gain. The major contribution of the proposed algorithm was to attack defense and detection, precision for avoiding the packet drops.

In 2019, M. Vigenesh and R. Santhosh [4] worked on merely discovering the energy or congestion parameter in the hops of routes that do not tend to competent performance in real-world circumstances. Therefore, an Efficient Stream Region Sink Position Analysis (ESRSPA) method in order to enhance the attack detection in MANETs was presented. Attack detection is the procedure of recognizing malicious nodes that were positioned in the system. The MANET encompasses many nodes that were free to move about in any direction. The mobile nodes carry out supportive routing and choose the head node for receiving updates, and this was called as base station location analysis. Under the stream location, the nodes arrive and transmit updates to the base station.

In 2019, Y. Harold Robinson et al [5], presented a reliable routing algorithm to attain the QoS in MANET. By exploiting the potency of the node's signal in the well-known nodes the bandwidth obligation was computed. The routing selection was on the basis of the less number of delays and sturdy stability.

To determine the route more competent than a conventional broadcasting method, rebroadcast was performed with the help of neighbor knowledge algorithms. Here, the NKR (Neighbor Knowledge-based Rebroadcast) method and LVC (Loose Virtual Clustering) method were exploited for routing overhead lessening in MANETs.

In 2018, Ruo Jun CAI et Al [6] presented an Evolutionary Self Self-Cooperative Trust (ESCT) method, which emulates human cognitive procedure and lies on trust-level information to put off several routing disruption attacks. In this system, mobile nodes will transmit trust information and investigate received trust information on the basis of their own cognitive decision. Ultimately, every node dynamically develops its cognition to rule out malicious entities. The major attractive aspect of ESCT was that they cannot concession the system even if the internal attackers be familiar with how the security method works. Here, the performance of the ESCT method in several routing disruption attack circumstances was evaluated.

In 2019, Aly M. El-Semary and Hossam Diab [7], presented a secure MANET routing protocol named BP- AODV to surmount the security breaches associated with the SAODV protocol beside with the new AODV protocol. Additionally, the BPAODV had the capability to secure over a cooperative black hole attack starts on the routing procedure and guards over the black hole attack, which may happen in the forwarding procedure. Moreover, the BP-AODV was presented by improving the functionality of the AODV protocol besides using the chaotic map features.

In 2018, Jingwen Bai et al [8] presented a new Constructive-Relay-based Cooperative Routing (CRCPR) protocol exploiting the topological information saved and sustained in a Relay Table and Cooperative Table. CRCPR improves flexibility to alleviate the mobility problem by self-managing to build sufficient relays for data forwarding. Moreover, presumptuous nodes were frequently battery operated; CRCPR presented a novel route selection method that considered energy harvesting, energy utilization, and probability link break, to decide a suitable route over the network.

3. Problem Definition

Let us assume a MANET with n nodes involved in sensing as well as gathering the information of the environment. Every n node has the communication and communication range among the sender and the receiver nodes that happen within this range via a set of nodes. Here, the nodes are considered as mobile, as well as they can alter their position within the communication environment, and therefore, the new location of the node happens within the communication environment. Hence, to set up a well-planned route for communication, trust and distance are used. The optimally selected paths are represented in eq. (1).

$$h = \{h_1, h_2, ..., h_j, ..., h_m\} \tag{1}$$

In eq. (1), i indicates the total number of the optimal paths selected. In the environment the mobility models [17] of the MANETs that explain the movement of the nodes, and it states the location, velocity, and acceleration of the nodes and updating their positions occasionally within the communication range. Conversely, trust is considered as one of the main elements which portray the MANETs security, as well as the node for the trust of the nodes [17], which explains the trust degree of the network.

4. Proposed MANET Routing Protocol

4.1 Trust-Based Secure Routing based on the Proposed AES

In this section, the developed AES-TPSGWO is considered as a protocol to set up the secure routing in MANET with the association of the trust factor, PSGWO method, and AES. In AES-TPSGWO, the processing steps comprise the finding of k-paths, optimally chosen of the paths, as well as communication. The encrypted data transmit the message via the Route Request (RREQ) and Route Reply (RREP) stages exploiting AES-128. The paths are recognized on the basis of the delay, trust factors, distance, and link lifetime, as well as the paths, are optimally chosen on the basis of the proposed optimization method, PSGWO. The chosen path is utilized for the data routing that is encrypted by exploiting AES-128 to assure security. The schematic illustration of the proposed routing protocol is exhibited in Fig 1.

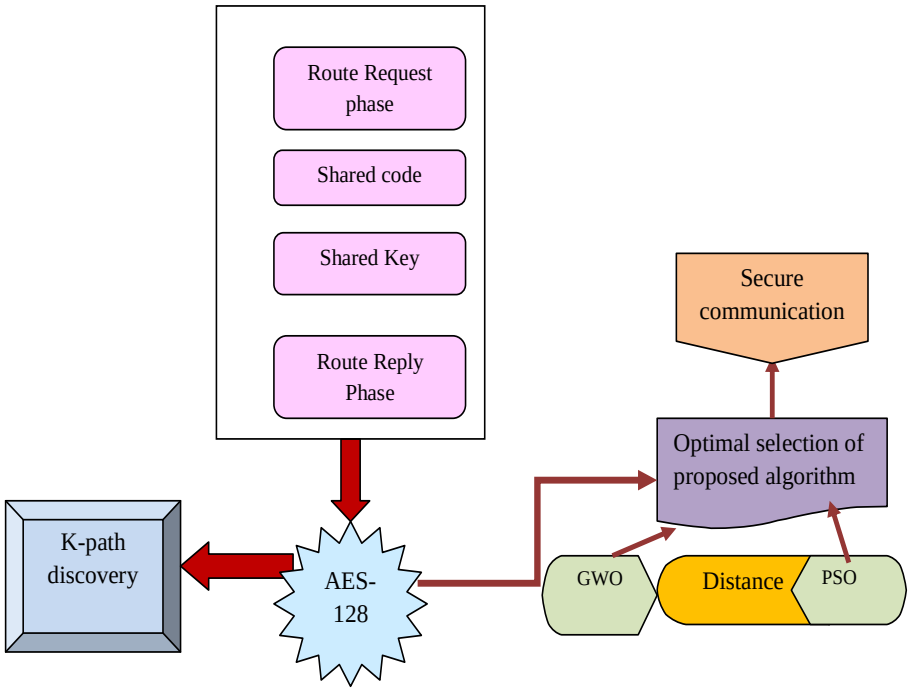


Fig. 1. *Block diagram of the proposed methodology*

4.2 AES-128 based on the Trust

In the proposed AES-TPSGWO, the routing path is recognized by exploiting the shared key and code on the basis of the AES-128. In the process of communication, security in MANET is important to evade the vulnerable attacks in the channels. For that, both the sender as well as receiver nodes are fundamental to share the key as well as code. Here, the two stages related to route finding are RREP as well as RREQ, correspondingly that captures in finding the routes. By the individual nodes the routing table is retained which comprises the source node ID's (I_r), a receiver node I_f, cost (S) and the information of the subsequent hop. The source node starts the communication and requests the neighboring nodes with an RREQ message, which comprises the shared code S_d, message flag, I_f, and Time To Live field (TTL). In the RREQ message scenario, the message flag is set to 'one' and with the aid of AES-128 the shared code is encrypted [18], and its key length is 128-bits. The importance of AES-128 is that it reduces the vulnerability and improves the data protection and therefore, the encrypted shared code $(AES(S_d))$ becomes the element of RREQ message.

On the basis of the trust and distance, the cost function is designed in that the trust must be high, and distance must be less when engaging in transmission. While receiving the request message, the node attains the shared code S_d and ends if it is the receiver node, as well as the transmission concludes with the receiver node or else, the data is forwarded via other nodes in the path.

Conversely, to estimate the node trust, the received shared code S_d^* is decrypted on the basis of the shared key and at last, it evaluated with the shared code of the sender S_d. In addition, in the received message I_f^* the destination ID is equivalent to the node ID I_f, as well as if the equivalent outcome is similar, the specific node is concluded as the receiver node, as well as the transmission will complete. Through the other nodes, the data packets are forwarded if it is true that the receiver node is not a specific node receiving the message, and concurrently, the data packets are obstructed while the TTL finishes.

In the same way, the reply is transmitted to the requesting node while receiving the request message. The reply message comprises of the subsequent fields, message flag of the reply which is flagged as one', in the occurrence of the nodal reply, and encrypted message of shared code, the ID of the node/intermediate node, and shared key, correspondingly. The source node decrypts the shared code and examines the shared code while receiving the reply. Conversely, the malicious or normal node is checked, and if the node is the normal node, in the routing table the ID is updated. The routing table comprising the sender and receiver nodes ID's, cost, as well as next-hop is updated at the conclusion of the individual iteration. Subsequent to the updating, the cost of the nodes chosen for k-path discovered is calculated. Hence, the proposed protocol, AES-TPSOGWO checks the shared code and nodes key at the instantaneous of each data transmission, and therefore, it shows the secure transmission.

a) Solution Encoding:

The solution is the indication of the optimal possible paths selected by exploiting the proposed DPSGWO method that is selected on the basis of the distance, trust, and delay. Consider the solution vector as, $SV = \{SV_1, SV_2, ..., SV_t\}$, whereas, t indicates the total paths chosen by exploiting the proposed optimization method. The solution is indicated as a binary value, and the optimal solution is selected on the basis of the maximal objective model.

b) Objective Model Formulation:

On the basis of the maximal objective model, the optimal paths are determined which is on the basis of the delay, trust, and distance as stated in eq. (1). It is to make sure that the optimal solution be consistent with the solution with minimum delay and distance, as well as maximum trust, with the only objective to provide the maximum trust for data transmission. Eq. (2) states the objective model.

$$F = \frac{1}{d}\sum_{s=1}^{d}\frac{1}{|d_s|}\sum_{a=1}^{|d_r|}N_a^s \tag{2}$$

In eq. (2), d indicates the discovery paths, d_s indicates to the s^{th} path in s discovered paths and N_a^s indicates for the a^{th} node in the s^{th} path which is calculated as eq. (3).

$$N_a^s = \frac{1}{2}\left[\eta_a^s + \left(1-\partial^s\right) + \left(1-\Delta^s\right)\right] \tag{3}$$

In eq. (3), η_a^s denotes the trust of the a^{th} node available in s^{th} path, ∂^s denotes the distance among the nodes in d_s and Δ^s denotes the delay in transmission of the packets among the nodes in the path d_s. The value of the trust deviates between 0 and 1 that must be high, where the delay and distance must be minimum deviating between 0 and 1, and thus, delay and distance are subtracted from unity. Eq. (4) is used to measure the distance.

$$\partial^s = \frac{\left\|\partial_a^s, \partial_{a+1}^s\right\|}{B} \tag{4}$$

In eq. (4), $\|.\|$ indicates the norm indicating the distance among a^{th} and $(a+1)^{th}$ node as well as B denotes the experimentation area. The trust factor [19] is calculated on the basis of the trust factors, like direct, recent, indirect, and historical trust, and it is calculated using eq. (5).

$$\eta_a^s = \omega_1 \times \eta^{direct} + \omega_2 \times \eta^{indirect} + \omega_3 \times \eta^{recent} + \omega_4 \times \eta^{hist} \tag{5}$$

In eq. (5), η^{direct}, η^{recent}, $\eta^{indirect}$ and η^{hist} indicates the direct, recent, indirect, as well as historical trust factors. As recent trust [19], the current behaviors of the node is inherited this represents the summation of the indirect and direct trust as stated in eq. (5).

$$\eta^{recent} = \kappa_1 \times \eta^{direct} + (1-\kappa_2)\eta^{indirect} \tag{6}$$

In eq. (6), κ_1 indicates the weight equivalent to the direct trust as well as it uses a higher weight while comparing with the weight κ_2 as the interaction among the nodes a and v that exhibits the node confidence a on the node v is higher. The direct trust [19] is on the basis of the experience of the node a regarding its target and it is stated in eq. (7).

$$\eta^{direct} = \frac{1}{n}\sum_{\substack{v=1 \\ a\in v}}^{n} sat_{av} \tag{7}$$

In eq. (7), n indicates the total neighboring nodes and sat_{av} indicates the fulfillment between the nodes a and v. The direct trust indicates the fulfillment among the nodes as well as the fulfillment is calculated as the ratio of the accomplished transactions to the total nodes, as stated in eq. (8).

$$sat_{av} = \frac{t_{av}}{N} \tag{8}$$

In eq. (8), t_{av} indicates the accomplished transactions among nodes a and v, and N indicates the total nodes. Indirect trust contemplates the occurrence of the neighbors additionally with the occurrence of the target node which is stated in eq. (9).

$$\eta^{indirect} = \frac{1}{Y * Z}\sum_{\substack{v=1 \\ a\in v}}^{Y}\sum_{\substack{u=1 \\ u\in v}}^{Z} sat_{vu} \tag{9}$$

In eq. (9), Y indicate the neighbors of a and Z indicates the neighbors of u. The historical trust [20] is on the basis of the behavioral patterns in the last, and it is stated in eq. (10).

$$\eta^{hist} = \frac{\delta \times \eta_{y-1}^{hist} + \eta^{recent}}{2} \tag{10}$$

In eq. (10), δ denotes the forgetting factor that deviates between 0 and 1.

4.3 Proposed AES-TPSGWO Protocol for Secure Communication

By exploiting the proposed AES-TDCO method the routing starts and it depends on the chosen of the optimal routes and the data communication happening via the source and destination. When the source node attempts to exchange information with the receiver node through the intermediary nodes, the sender-receiver pair shares the key as well as code among each other that are unrevealed to the intermediary nodes. Initially, by exploiting the standard AES-128, the data packets are encrypted with the shared key and code, when on the receiver side, the encrypted keys and code are decrypted. Hence, the aforesaid case indicates the security guarantees in the MANET routing so that the sender and the receiver nodes be aware of the abnormal as well as normal nodes that are saved in the routing table at the termination of routing. The k-paths produced are selected optimally exploiting the optimization method which is on the basis of the trust-based objective model. Fig. 2 demonstrates data transmission insecure manner by exploiting the proposed routing protocol in MANET.

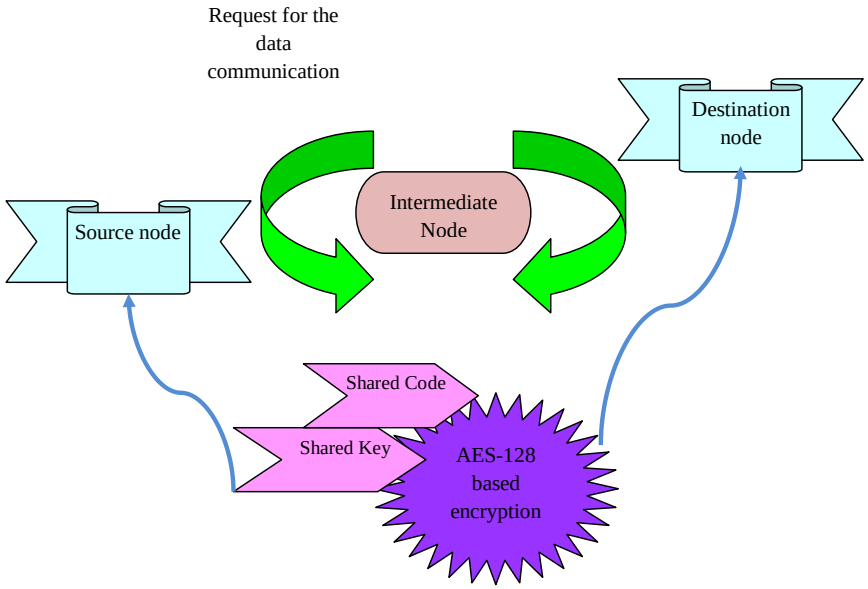


Fig. 2. *Diagrammatic representation of secure data communication*

5. Proposed Methodology

In this paper, the hybridization method is presented which uses the GWO and PSO meta-heuristic algorithms. Generally, PSO is a renowned and extensively exploited algorithm [20]. A hybrid algorithm has been proposed exploiting these two methods, which produce flourishing outcomes. In the following sections, the proposed algorithm has been described clearly.

5.1 Conventional PSO Algorithm

The conventional PSO is a population-based meta-heuristic optimization approach [21], which is enthused by the social behavior of fish schooling or bird flocking while searching for food. In the PSO algorithm at first, the initial population is produced arbitrarily in the search domain. The optimal position of every particle, as well as the location information of the optimal particle in the swarm, is continuously kept in memory. In the swarm, all particles update their locations by exploiting the eq. (11) and (12) in each iteration.

$$y_{n+1}^{j} = \bar{y}_{n}^{j} + \bar{u}_{n+1}^{j} \tag{11}$$

$$\bar{u}_{n+1}^{j} = \omega \bar{u}_{n}^{j} + c_1 a_1 \left(\bar{s}_{n}^{j} - \bar{y}_{n}^{j}\right) + c_2 a_2 \left(\bar{s}_{n}^{h} - \bar{y}_{n}^{j}\right) \tag{12}$$

In eq. (11) and (12), j indicates the particle in the swarm. n indicates the iteration step performed, as well as a_1 and a_2 values indicate arbitrary numbers in the range (0, 1), and ω represents the parameter of the inertia weight. c_1 and c_2 indicates the optimization coefficients parameters, $\bar{u}$

indicates the velocity vector, y indicates the location vector and $\bar{s}^{j}$ indicates the optimal location information that i^{th} particle has attained, at last, $\bar{s}^{h}$ indicates the optimal location information present in the swarm.

In the conventional PSO approach, the novel position, as well as the velocity of a particle, is not established with a minimum prospect; as a substitute, it is replaced by a random location within the search space. The main aspire of this operation is to run off from the local minimums. The search carries on till the best effect is attained or an utmost predefined number of iterations is accomplished.

5.2 Conventional GWO Algorithm

The conventional GWO method and enthused by the leadership hierarchy of grey wolves [23]. There are 4 kinds of grey wolves are α, β, δ and ω wolves in the leadership hierarchy. In the conventional GWO method, α wolves indicate the solution with the optimal outcome. β and δ wolves indicate the second and third optimal solutions in the population and the ω wolves indicate the optimal solution candidates. The conventional GWO method supposes that hunting is done by α, β, and δ wolves when ω wolves go after these wolves. Grey wolves' hunting comprises the subsequent three important elements such as (a) chasing, tracking, and similar to the prey, (b) encircling, pursuing, and harassing the prey until it stops moving, and (c) Attacking the prey. Eq. (13) and (14) states the mathematically model of the encircling the prey.

$$E = \left| N \times Y_p(t) - Y(t) \right| \tag{13}$$

$$Y(t+1) = Y_p(t) - M \times E \tag{14}$$

In eq. (13) and (14), t indicates the number of immediate iterations, Y_p indicates the location of the prey, Y indicates the position of grey wolves and M, N indicates the coefficients of the vector. M and N coefficients are computed using eq. (15) and (16).

$$M = 2 \times (2 \times a_1 - 1) \tag{15}$$

$$N = 2 \times a_2 \tag{16}$$

In the above equation, the count m is linearly minimized from two to zero, as the count of iterations minimizes. a_1 and a_2 indicate uniformly chosen random numbers among [0, 1].

Grey wolves are lead by α wolves to notice the position of the prey. Occasionally β and δ wolves aid α wolf. The GWO method supposes that the optimal solution is the α wolf, as well as the second optimal with the third solution, are β and δ wolves, correspondingly. Consequently, the other wolves in the population move based on the location of these three wolves and it is stated in the below equations.

$$E_\alpha = \left| N_1 \times Y_\alpha - Y(t) \right| \tag{17}$$

$$E_\beta = \left| N_1 \times Y_\beta - Y(t) \right| \tag{18}$$

$$E_\delta = \left| N_1 \times Y_\delta - Y(t) \right| \tag{19}$$

In each iteration, the values Y_α, Y_β and Y_δ indicates the optimal three wolves, correspondingly.

$$Y_1 = \left| Y_\alpha - m_1 E_\alpha \right| \tag{20}$$

$$Y_2 = \left| Y_\beta - m_2 E_\beta \right| \tag{21}$$

$$Y_3 = \left| Y_\delta - m_3 E_\delta \right| \tag{22}$$

$$Y_p(t+1) = \frac{Y_1 + Y_2 + Y_3}{2} \tag{23}$$

Here, the new location of the prey is stated as $Y_p(t+1)$ the mean of the locations of three optimal wolves in the population.

By attacking the prey Grey wolves terminate the hunting. For attacking, they have to gather together sufficient to the prey. While eq. (15) is investigated, M uses values that deviate from $[-2m, 2m]$ when m takes minimizing values from two to zero. While $|M|$ value is higher than or equivalent to one, traditional hunts are discarded to discover enhanced solutions. Let us assume that the prey gathers together adequate for values lesser than one, grey wolves are forced to assault the prey. This algorithm stops the wolves' attainment wedged on the local minimum. While the GWO method attains the desired number of iterations, the search is finished.

5.3 Hybrid PSGWO Algorithm

The proposed PSO–GWO method (PSGWO) is introduced without altering the common operation of the GWO and PSO methods. In almost all real-world issues, the PSO method can attain flourishing outcomes. Nevertheless, a solution is required to minimize the prospect of the PSO method to catch into a local minimum. In the proposed algorithm, the GWO method is used to hold up the PSO method to minimize the opportunity of falling into a local minimum. The PSO method directs some particles to random locations with minimum prospect to evade local minimums. These directions might encompass a few risks reason to move away from the global minimum. The exploration capability of the GWO method is exploited to stop these risks by directing some particles to locations which are partly enhanced by the GWO method in place of directing them to random locations. Fig. 3 shows the flowchart of the proposed hybrid PSGWO algorithm.

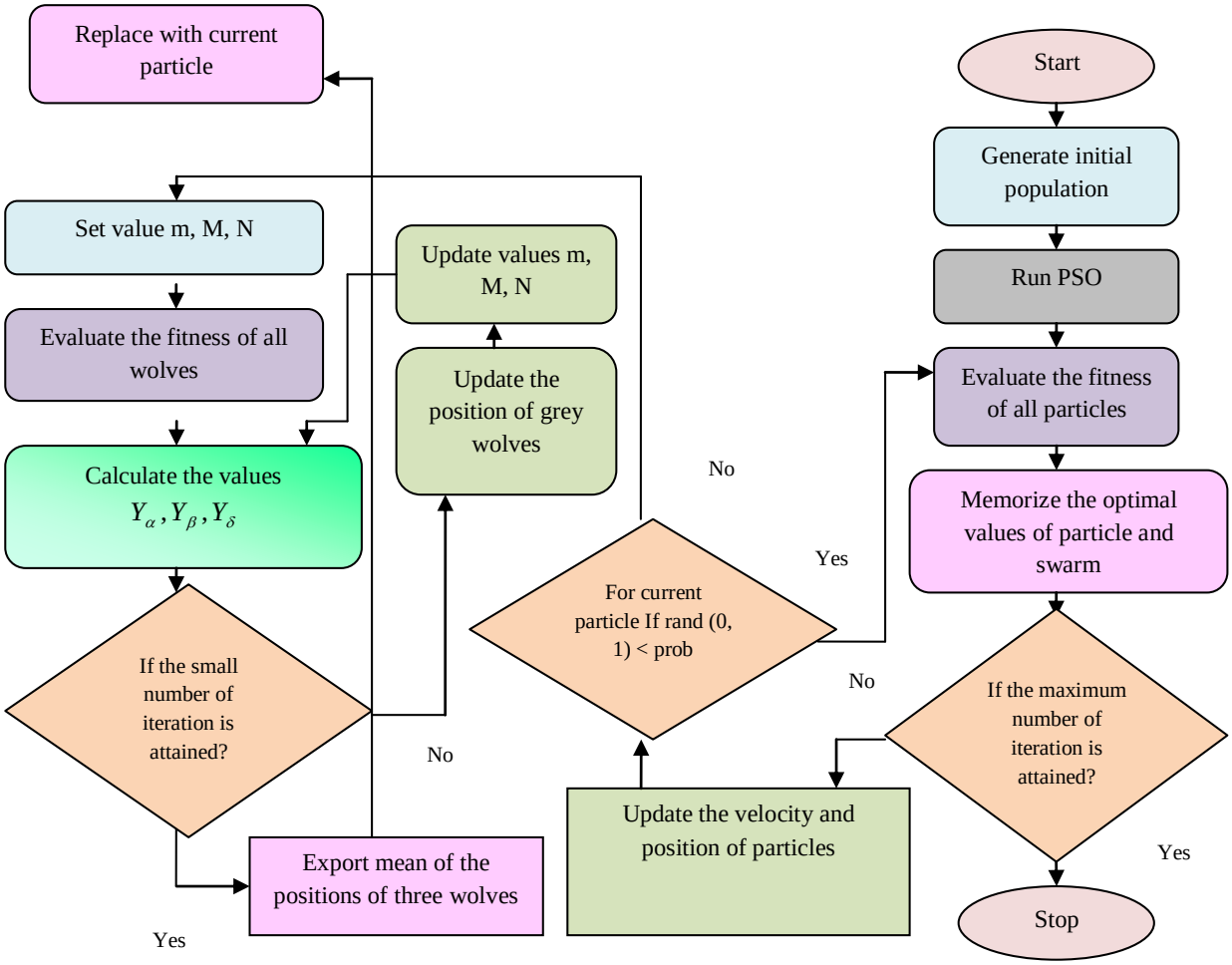


Fig. 3. *Flowchart of the proposed Hybrid PSGWO algorithm*

6. Result and Discussions

6.1 Experimental Set up

In this section, the efficiency of the proposed AES-TPSGWO protocol in the MANET routing with the main intention of rendering security for the communication purpose. The performance analysis of the proposed algorithm and the efficiency was demonstrated by means of the comparative analysis.

The algorithm exploited for the evaluation analysis comprises such as Trust-Based Security-Optimized Link State Routing protocol (TBS-OLSR), Advanced Encryption Standard based Dolphin Glowworm Optimization (AES-DGO), that is the optimization method with AES for secure routing without the inclusion of the trust factor; and Encrypted Trust-based Dolphin Glowworm Optimization (E-TDGO) is the optimization method with the inclusion of the trust factor for secure routing. The experimentation parameters of the proposed algorithm are shown in Table 1.

Table 1. *Experimentation Parameters*

Parameters	Values
Simulation Area	100mx100m
Mobility speed	30 ms
Number of sources	75 (nodes 1-75)
Number of nodes	50, 75
Channel type	Wireless channel
Number of sinks	1
Mobility model	Random waypoint model
Simulation time	50 rounds
Node placement	Random
Antenna type	Omni-directional
Size of packet	16 bytes
Radio model	Two-way ground

6.2 Performance Analysis

Fig 4 and 5 demonstrate the evaluation on the basis of the performance measures in the existence of the attacks. Fig 4 demonstrates the performance analysis of the proposed and conventional methods with the attendance of the black hole attack. Here, the detection rate of the proposed method is 11% better than the TBS-OLSR algorithm, 13% better than the AES-DGO, and 17% better than the E-TDGO algorithm. Moreover, the proposed technique attained the average throughput, packet drop, delay, and detection rate correspondingly. Fig 5 exhibits the evaluation analysis in the attendance of a Sybil attack. In Fig 5, the detection rate of the proposed method is 22% better than the TBS-OLSR algorithm, 23% better than the AES-DGO, and 26% better than the E-TDGO algorithm. The proposed algorithm attained the average throughput, delay, detection rate as well as packet drop, correspondingly. It is confirmed from Fig 4 and 5 that the proposed algorithm obtains an enhanced performance with superior throughput, less packet drop, less delay, and high detection rate.

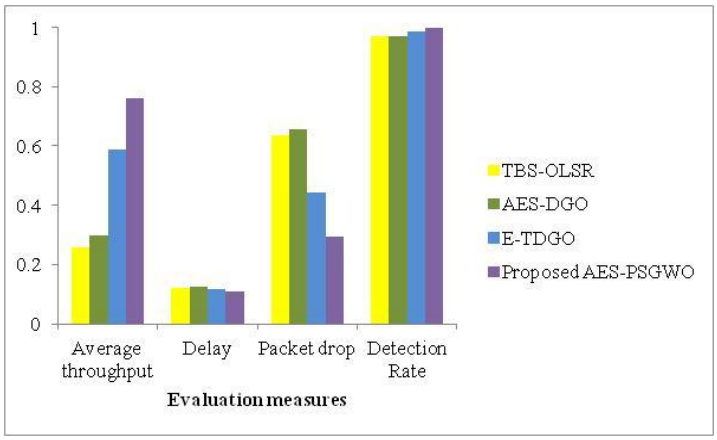


Fig. 4. *Performance analysis of network with black hole attack based on 75 nodes*

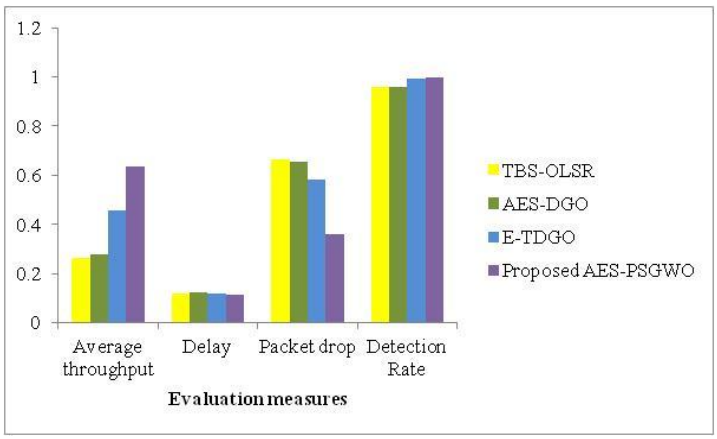


Fig. 5. *Performance analysis of network with Sybil attack based on 75 nodes*

7. Conclusion

In the MANETs, the trust and security-aware routing protocol on the basis of the optimization were utilized for routing for that at first the communication among the sender and receiver nodes was used the shared code as well as key by exploiting the AES. The routing protocol AES-TPSGWO connects in communication on the basis of the objective model that was on the basis of the delay, trust, as well as distance. Basically, the PSGWO was the combination of PSO and GWO algorithm to restrain enhanced global convergence and local convergence avoidance scheme. The experimentation was progressed exploiting 75 nodes on the basis of the performance measures as well as it was shown that the proposed routing protocol obtained the minimal delay, maximum throughput, and minimum packet drop, and detection rate.

References

[1] Trilok Kumar Saini, Subhash C. Sharma,"Prominent unicast routing protocols for Mobile Ad hoc Networks: Criterion, classification, and key attributes", Ad Hoc Networks, Volume 89, 1 June 2019, Pages 58-77.

[2] Dipika Sarkar, Swagata Choudhury, Abhishek Majumder,"Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network", Journal of King Saud University - Computer and Information Sciences, In press, corrected proof, Available online 28 August 2018.

[3] Subramanian Balaji, Eanoch Golden Julie, Yesudhas Harold Robinson, Raghvendra Kumar, Le Hoang Son,"Design of a security-aware routing scheme in Mobile Ad-hoc Network using repeated game model", Computer Standards & Interfaces, Volume 66, October 2019.

[4] M. Vigenesh, R. Santhosh,"An efficient stream region sink position analysis model for routing attack detection in mobile ad hoc networks",Computers & Electrical Engineering, Volume 74, March 2019, Pages 273-280.

[5] Y. Harold Robinson, R. Santhana Krishnan, E. Golden Julie, Raghvendra Kumar, Pham Huy Thong,"Neighbor Knowledge-based Rebroadcast algorithm for minimizing the routing overhead in Mobile Ad-hoc Networks", Ad Hoc Networks, Volume 93, October 2019.

[6] R. J. Cai, X. J. Li and P. H. J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," IEEE Transactions on Mobile Computing, vol. 18, no. 1, pp. 42-55, 1 Jan. 2019.

[7] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," IEEE Access, vol. 7, pp. 95197-95211, 2019.

[8] J. Bai, Y. Sun, C. Phillips and Y. Cao, "Toward Constructive Relay-Based Cooperative Routing in MANETs,"IEEE Systems Journal, vol. 12, no. 2, pp. 1743-1754, June 2018.

[9] Kannhavong B , Nakayama H , Nemoto Y , Kato N , Jamalipour A . A survey of routing attacks in mobile ad hoc networks. IEEE Wirel Commun 2007;14(5):85–91 .

[10] Khabbazian M , Mercier H , Bhargava VK . Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks. IEEE Trans Wirel Commun 2009;8(2):736–45 .

[11] Lavanya G , Kumar C , Rex Macedo Arokiaraj A . Secured backup routing protocol for ad hoc networks. In: Signal acquisition and processing, 2010. ICSAP'10. International conference on. IEEE; 2010. p. 45–50 .

[12] Le A , Markopoulou A . On detecting pollution attacks in inter-session network coding. In: 2012 Proceedings IEEE INFOCOM. IEEE; 2012. p. 343–51 .

[13] Mishra S , Satpathy SM , Mishra A . Energy efficiency in ad hoc networks. Int J Ad hoc Sen Ubiquit Comput 2011;2(1):139–45 .

[14] Nait-Abdesselam F , Bensaou B , Taleb T . Detecting and avoiding wormhole attacks in wireless ad hoc networks. IEEE Commun Mag 2008;46(4):127–33 .

[15] Nayak K , Gupta N . Energy efficient consumption based performance of AODV, DSR and ZRP routing protocol in MANET. Energy 2015;4(11):82–90 .

[16] Oggier F , Fathi H . An authentication code against pollution attacks in network coding. IEEE/Acm Trans Network 2011;19(6):1587–96.

[17] Bahrami, M., Bozorg-Haddad, O. and Chu, X. (2018) Cat Swarm Optimization (CSO) Algorithm. In Advanced Optimization by Nature-Inspired Algorithms, pp. 9–18. Springer, Singapore.

[18] Jing, Q., Vasilakos, A.V., Wan, J., Lu, J. and Qiu, D. (2014) Security of the internet of things: perspectives and challenges. Wireless Netw., 20, 2481–2501. Comi,

[19] A., Fotia, L., Messina, F., Pappalardo, G., Rosaci, D. and Sarné, G.M.L. (2015) A Reputation-Based Approach to Improve QoS in Cloud Service Composition. In Proc. of IEEE 24th Int. Conf. on Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 15–17. IEEE, Larnaca, Cyprus.

[20] Das, A. and Islam, M.M. (2012) SecuredTrust: a dynamic trust computation model for secured communication in multiagent systems. IEEE Trans. Dependable Secure Comput., 9, 261–274.

[21] Mingquan Zhang, Xiaorong Cheng, Huawei Mei and Jujie Zhang, "Research of routing optimization based on improved PSO algorithm in power communication network," 2011 International Conference on Electric Information and Control Engineering, Wuhan, 2011, pp. 2494-2497.

[22] C. Hu, B. Hu and Y. Xiong, "Mobile agent routing using variable-dimension PSO algorithm based on chord-length parameterization," National Doctoral Academic Forum on Information and Communications Technology 2013, Beijing, 2013, pp. 1-8.

[23] K. Anbumani, R. Ranihemamalini and G. Pechinathan, "GWO based tuning of PID controller for a heat exchanger process," 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS), Chennai, 2017, pp. 417-421.