International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 8 (2018) pp. 5722-5735

Trust based Genetic Neuro-Fuzzy System for Intrusion Detection and Self Adaptive Firefly integrated Particle Swarm Optimization Algorithm for Secure Routing in MANET

Ramireddy Kondaiah [1] and Dr. Bachala Sathyanarayana[2]

[1]*Research Scholar ((PP COMP.SCI-053), Department of Computer Science, Rayalaseema University, Kurnool, Andhra Pradesh, India.*

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

Abstract

Mobile Ad hoc Network (MANET), which is comprised of a number of self-organized and battery equipped mobile nodes, is used widely in various applications, including military and private sectors. However, security is a major issue in MANET routing, as the network is prone to attacks. This paper introduces the intrusion detection scheme for establishing the secured path in MANET. Here, the presence of intruder in network is identified with the use of genetic neuro-fuzzy system, and various trust factors. Then, the possible paths between the source and the destination through the trust nodes are generated. The work aims to identify the secured paths from the possible paths through the proposed Self Adaptive Firefly based Particle Swarm Optimization (SA-FPSO) Algorithm. Finally, the secured paths are generated between the source and the destination for data communication. Simulation environment for implementing the proposed scheme is developed with the NS2 simulator, and evaluated by introducing network attacks, such as black hole, flooding, and selective packet drop attack. Simulation results reveal that the proposed SA-FPSO scheme outclassed existing works with the values of 0.04319 sec, 0.691, and 0.769 for delay, detection rate, and throughput, respectively, while the MANET is under black hole attack.

INTRODUCTION

MANET has the dynamic topology and the nodes present in the network do not provide proper structure to the network, and thus, it may suffer from various network attacks [1]. MANET contains several nodes freely distributed over the wireless medium. The data is passed from the source node to the destination node through various set of intermediate nodes, and the communication between the nodes can be referred as hopping. Based on the communication, the MANET comes under two categories; they are single hop network, and multi hop network [3]. Various routing algorithms come in handy for establishing the routing path between the source and the destination for data transmission.

The MANET nodes have large separation distance and limited battery life. Thus, establishing the routing path helps in improving the speed and efficiency of communication. One of the major factors affecting the path establishment is the network attacks [4]. Network attacks affect both the routing mechanism and the security mechanism. Further, it comes under the category of passive attack and active attack. Passive attack does not pose a greater threat to the network, whereas the active attacks change the data transfer [10]. Handling the security threats occurring in MANET can be done through Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). IDS identify the malicious nodes in network, whereas the IPS prevents the system from security threats and allows secured data transmission [1]. Formerly, IDS detects the malicious activity in the node through anomaly detection and misuse detection. IDS can be defined as the reactive defence mechanism, which offers defence to MANET through early detection of network attacks [15] [16]. IDS helps in providing secured nodes for routing protocol and thereby, establish a secured path between the source and the destination [11].

IDS design parameters, such as routing nature of the protocols, mobility of the nodes, lack of centralized control and limited bandwidth act as factors for the presence of malicious nodes in MANET [1]. DoS attack specifies the isolation of node from the network, which results in packet dropping, by modifying the data packets transferred between source and destination. DoS attacks result in route disruption, data rejection, and data depletion. DoS attacks in the MANET come under different categories, namely wormhole attack, blackhole attack, and greyhole attack, respectively [13] [14]. Wormhole attack happens when two or more malicious nodes establish a private channel between them [4]. The black hole attack [17] attracts the traffic by providing false routing information, and upon data reception, it drops the data packets. The black hole attack drops most of data and hence, referred as full data dropping attack. The greyhole attack [18] is similar to the black hole attack, but drops partial data. Greyhole attack is also referred as partial data dropping attack [12]. Sybil attacks create identity of physical device to launch a coordinate attack on the network, and this weakens the detection process [10].

In several literature schemes, both the qualities of IDS and IPS are utilized, to develop the Intrusion Detection and Prevention Scheme (IDPS) [1]. Recently, developed routing algorithms have neglected the IDS and thus, failed to provide secured routing path. As the security is one of the important design parameters, inclusion of IDS scheme along with the routing algorithm improves the overall efficiency of the MANET [2]. Several works used the classification scheme for classifying the normal nodes from the malicious nodes. In [6], SVM scheme

was incorporated to identify the flooding attacks happening in the MANET. Here, SVM classifies the normal node by detecting the nodes affected by flooding attacks. Using fuzzy based system for classifying has gained more popularity in recent years since, it provides improved decision making than other standard classifiers. In [8], Fuzzy Inference System (FIS) has been deployed for controlling the attacks in the MANET. FIS uses the rule based logic to define the fuzzy score for each node in MANET, and based on the fuzzy score, the node can be declared as normal or abnormal. In [9], DoS attacks are mitigated by using the Open Link State Routing (OLSR) protocol.

This paper introduces the IDPS for the MANET and hereby, establishes a secured routing path between the MANET nodes. The IDPS is established in MANET by identifying the malicious nodes, and developing a secured routing path between source and destination. Accordingly, Self-Adaptive Firefly based Particle Swarm Optimization (SA-FPSO) algorithm is newly developed by adjusting the acceleration coefficients in the update rule of the Firefly and PSO algorithms, to make it self-adaptive. The intruders available in MANET make the path establishment difficult and hence, require valid network for detection. This work utilizes the genetic neuro-fuzzy system for differentiating the intruders from normal one. The overall procedure of the proposed IDPS can be explained as follows: Initially, the trustworthy of each node in the MANET is computed based on the trust factors, to establish the paths between the source and the destination. Then, the intruders in the network are identified using the genetic neuro-fuzzy system, which utilizes the fuzzy neural network with the Genetic Algorithm (GA). Once the intruders are identified, the possible paths are established, and the proposed SA-FPSO algorithm establishes optimal path between source and destination.

The contribution of this work is the development of the SA-FPSO algorithm for selecting the optimal path, ensuring security in the MANET. The proposed SA-FPSO algorithm modifies the existing PSO algorithm with the fractional theory and makes the PSO to be self adaptive.

The organization of this paper is as follows: Section 1 gives introduction to the intrusion detection scheme suitable in MANET model. Section 2 reviews recent works related to intrusion detection, and secure routing. Section 3 gives a brief description to the proposed genetic neuro-fuzzy system and SA-FPSO algorithm for helping in intrusion detection. Simulation results achieved by genetic neuro-fuzzy system and SA-FPSO algorithm are described in section 4, and conclusion is given in section 5.

MOTIVATION

Literature Survey

Various algorithms have been developed for resolving the issues related to IDS and few of them are described here, Singh, O. et al. [1] proposed the Intelligent Intrusion Detection and Prevention System (IIDPS) for preventing the nodes from various attacks. The IIDPS model tackled various attacks by integrating the trust manager, which assigned trust value to each node in MANET. Also, it used predefined threshold and risk factor conditions for ensuring the security to the nodes. Babu, M.R. and Usha, G.et al. [2] proposed the Novel Honeypot Based Detection and Isolation (NHBADI) scheme for securing the MANET from different attacks. The scheme mainly concentrated in mitigating the black hole attacks. The use of honeypot technique ensured reduced network overhead. Finally, the model isolated the path from nodes affected by black hole attacks, and ensured security. The scheme neglected other network attacks during the path formulation. P. Joshi, et al. [3] proposed the Enhanced Adaptive ACKnowledgment (EAACK) scheme for detecting and preventing malicious attacks. The scheme handled the packet dropping and hacking issues prevailing in the MANET. The system ensured security by defining priority to each node for path establishment. Even though the model ensured improved security in MANET, all the weakness arising due to the watchdog was not handled efficiently. Khan, F.A., et al. [4] proposed the Detection and Prevention System (DPS) for handling the security alerts arising due to network attacks. The model employed some special nodes for monitoring the normal nodes in the MANET. If a change in normal operation was detected, then the special node declares the node to be suspicious. As the special node employed in the scheme does not involve in data transfer, it had enhanced battery life, but increases the network cost.

N. Marchang, et al. [5] proposed the IDS for detecting the malicious nodes in MANET by reducing the overall active time of IDS. The model ensured secure data transmission over network even though the active time of IDS was reduced. The model ensured secure transmission in homogenous platform, but has failed in heterogeneous network. Shams, E.A. and Rizaner, A. [6] proposed the IDS based on SVM framework. The framework was specially trained to identify the effects arising due to the DoS type attacks. As the SVM architecture had simple structure, the scheme detected the attacks with less computation time. The scheme removed malicious nodes from the system, and established the secured routing path. Gurung, S. and Chauhan, S. [7] introduced special nodes, namely Flooding-Intrusion Detection System (F-IDS) for eliminating the effects of flooding attacks. The special nodes deployed with MANET nodes ensured the detection and prevention of flooding attacks. The impact of address spoofing that raised during flooding was not addressed in the scheme. Bisen, D. and Sharma, S. [8] proposed the Fuzzy Based Secure

Architecture (FBSA) for detecting the malicious activity in MANET. Here, the fuzzy detector was employed for the detection of malicious nodes. However, the scheme mitigated the effects of only less number of network attacks, and hence, provided less performance in challenging environments.

Challenges

Various challenges involved in detecting the intrusions prevailing in the MANET nodes are enlisted below,

- MANET has limited resources with small battery life, and hence, running IDS all the time may reduce the capacity of MANET. This can be avoided by reducing the active time of MANET without compromising the effectiveness [5].

- Detecting the selective flooding attack is more challenging, as it behaves as normal node sometimes. Several schemes adopted constant threshold value for detecting the selective flooding attack, and suffer under high mobility environment [7].
- Sybil attack offers combined or coordinated attack on the defense, and hence, avoiding the Sybil attacks is necessary. Nodes in MANET transfer both the control and data packets simultaneously and hence, when the node is under Sybil attack, both the control and data can be affected [10].
- IDS scheme need to compensate between the energy consumption and scalability of nodes, as it influences the network performance [11].

PROPOSED INTRUSION DETECTION SCHEME FOR SECURED PATH ESTABLISHMENT

This section presents the proposed intrusion detection scheme for the MANET, and identifies the secured routing path between the source and the destination nodes. Figure 1 presents the architecture of IDS for detecting the malicious nodes, and secured path establishment.

The MANET depicted in the figure 1 has numerous nodes placed randomly all over the network. In the initial stage, four trust factors, such as direct trust, indirect trust, recent trust, and historical trust are calculated and provided to the genetic neuro-fuzzy system. It generates the fuzzy score for each node and declares the node as 'trust node' or 'malicious node' based on a predefined threshold value. After obtaining the trustworthy nodes through genetic neuro-fuzzy system, the possible paths in MANET with trust nodes that are suitable for data transmission are identified. Here, the SA-FPSO algorithm is proposed to identify the optimal paths among the possible paths and data transmission is done through the optimal paths. The trust value alters during the data transmission, repeating the process. The proposed scheme aims in establishing the secured routing path between the source and the destination nodes by eliminating the malicious nodes from the path estimation procedure. The entire process can be subdivided into two major processes, 1) Differentiating the trust node, and malicious node, and 2) Establishing the secured path between the source and the destination through the trust nodes. MANET contains the collection of self configured sensor nodes placed randomly throughout the network.

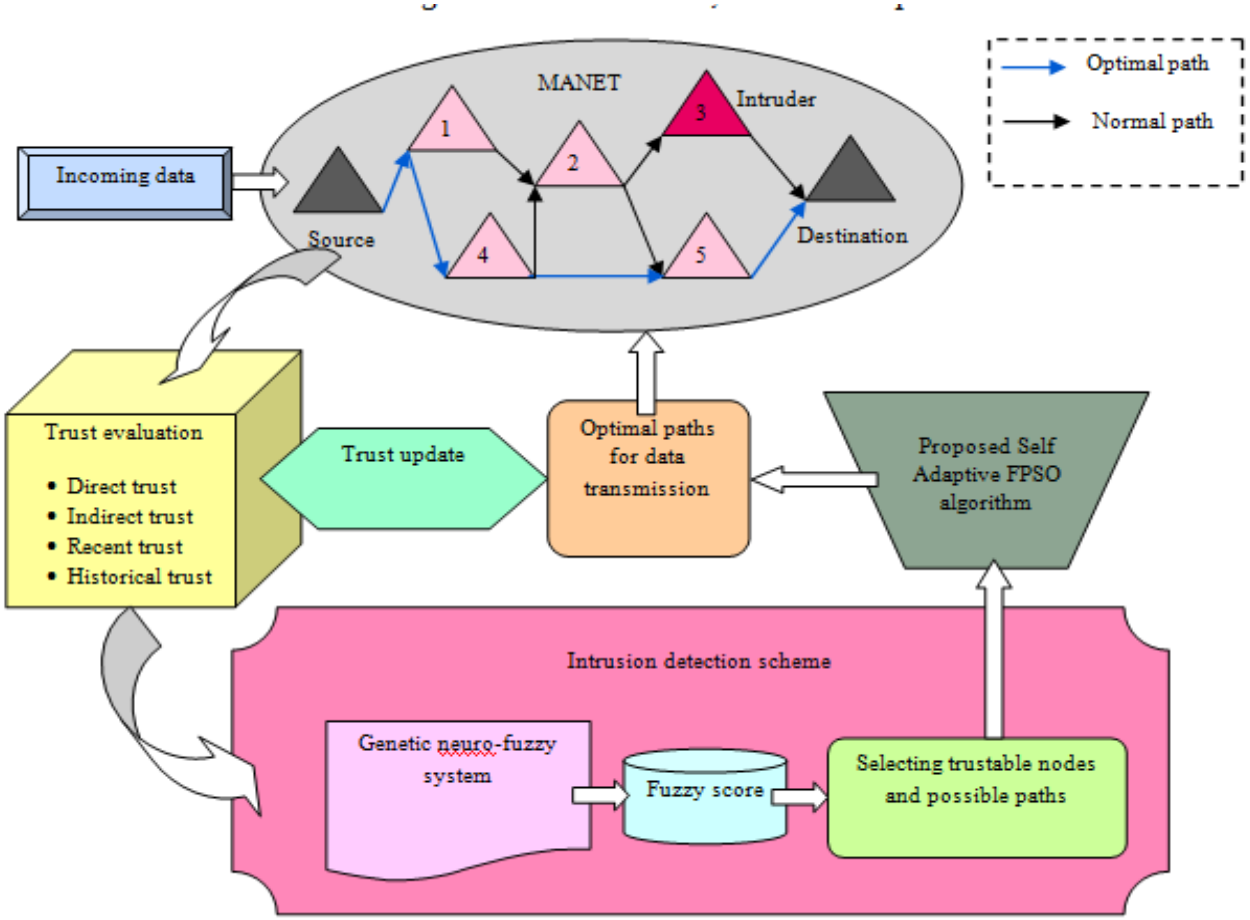


Figure 1. Block diagram of the IDS with Genetic Neuro-Fuzzy classifier and proposed SA-FPSO Algorithm

Consider the MANET network with B nodes, and the nodes in the network are expressed as $J = \{J_1, \cdots, J_x, \cdots, J_B\}$. Here, B refers to the total nodes in the MANET environment. The nodes in the MANET are located at random position and the location of the x^{th} node in MANET is specified as (d_x^1, d_x^2). The communication between the nodes occurs through hopping, and it starts from the source node, and ends at the destination node. The source node and the destination node in the network are referred as J_S and J_D, respectively. The communication path established between the source and the destination can be found by using the routing protocol. Also, the secured routing path neglects the malicious nodes from the routing path. The intrusion detection algorithm identifies the intruder in the MANET and helps in establishing the secured routing path.

Trust evaluation

The MANET considered for secured routing merely depends on the trust factors. This work considers basic trust model as defined in [20]. Here, four trust factors, namely direct trust, indirect trust, recent trust, and neighbouring trust, are considered. The trust factors used for determining the validity of nodes against various attacks are described below:

Direct trust: As the name implies, this trust depends on direct data transmission between the nodes and its neighbors. The direct trust, also referred as local trust, relates the data packets sent and received between two neighbor nodes, and the expression for direct trust is stated below:

$$Z_{x,y}^{direct}(t) = \frac{Q_{x,y}^{u}(t)}{Q_{x,y}^{v}(t)} \quad (1)$$

where, $Z_{x,y}^{direct}(t)$ indicates the trust between the nodes x and y, $Q_{x,y}^{v}(t)$ and $Q_{x,y}^{u}(t)$ indicate the total data packets sent and received between the nodes for the time limit t.

Indirect trust: Indirect trust depends on direct trust posed by the neighbor node on entire network. For the node x that has m number of neighbor nodes, the expression for indirect trust is,

$$Z_{x,y}^{indirect}(t) = \frac{1}{m}\sum_{j=1}^{m} Z_{j,y}^{direct}(t) \quad (2)$$

where, $Z_{j,y}^{direct}$ indicates the direct trust between the j^{th} neighbour node and the node y.

Recent trust: The trust factor depends on various behaviors of nodes. The node may behave different from time to time and it is necessary to consider the recent behavior of the nodes for trust evaluation. Thus, the recent trust depends on direct and indirect trust values, and it is formulated as,

$$Z_{x,y}^{recent}(t) = \alpha * Z_{x,y}^{direct}(t) + (1-\alpha) * Z_{x,y}^{indirect}(t) \quad (3)$$

where, α refers to the weight constant with the value of 0.5.

Historical trust: Historical trust refers to the trust defined to the target node at past, and it is expressed as,

$$Z_{x,y}^{historic}(t) = \beta * Z_{x,y}^{historic}(t-1) + Z_{x,y}^{recent}(t-1) \quad (4)$$

where, β indicates the forgetting factor under the limit of [0,1]. The terms $Z_{x,y}^{historic}(t-1)$ and $Z_{x,y}^{recent}(t-1)$ indicate the historical trust and recent trust at time $(t-1)$.

Intrusion detection using Genetic Neuro-Fuzzy system

This work uses the genetic neuro-fuzzy system [19] for identifying the number of intruder/malicious nodes in the MANET. Figure 2 presents the architecture of genetic neuro-fuzzy system for intrusion detection.

Establishing the secured routing path using the Proposed SA-FPSO

The important process after intrusion detection is the establishment of secured routing path between the source and the destination nodes. The genetic neuro-fuzzy system differentiates the trusted node and the malicious nodes by calculating the fuzzy score. After finding the trustable nodes in the MANET, it is necessary to establish the routing path between the source and the destination along the trust nodes.

Generating k paths based on trusted nodes

Feeding the trust values of each node to the genetic neuro-fuzzy system, it differentiates the trust nodes and the malicious nodes. Consider the genetic neuro-fuzzy system identifies a total of C trust nodes to be present in MANET. The target of routing algorithm is to establish the routing path between the source and the destination through trust nodes. Here, the possible paths that can be established between the source and the destination through the trust nodes are found. As depicted in figure 1, the path may choose different trust nodes as intermediate nodes between the source and the destination. Consider the communication between source J_S and destination J_D through C trust nodes can follow k number of paths. The paths for data communication can be expressed as $\{U_1, \ldots U_r, \ldots U_k\}$.

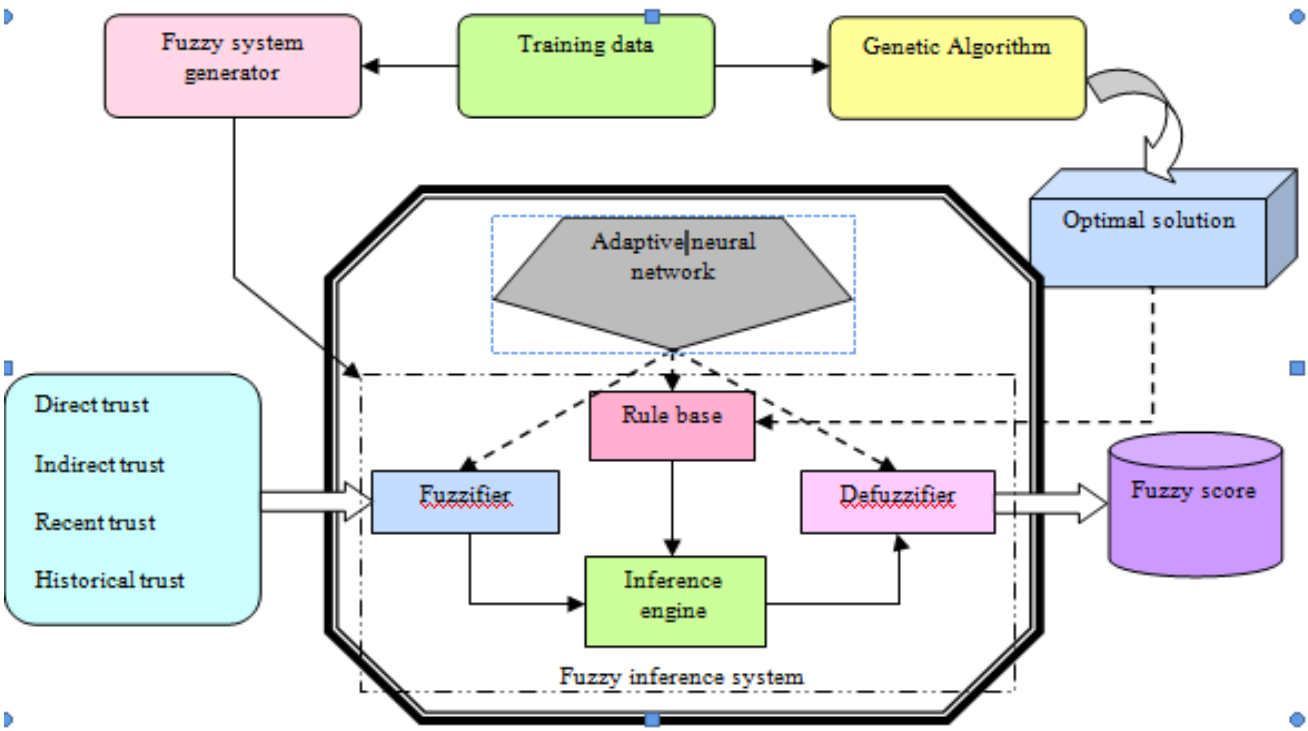


Figure 2. Architecture of Genetic Neuro-Fuzzy system

This work develops the SA-FPSO algorithm by integrating the PSO [21], and FA [22] for establishing the secured routing path in MANET. Also, the algorithm is made self adaptive in nature by choosing different values for weight constants of PSO. Since, there are k paths between the source and the destination, the proposed SA-FPSO chooses p secured paths among k paths through the optimization procedure. The secured path selection depends on distance and trust factors between the trusted / optimal nodes.

Solution encoding for SA-FPSO

The proposed SA-FPSO finds the p optimal secured paths among k paths generated between the source and the destination. Thus, the solution of the proposed SA-FPSO has p optimal paths represented as, $P = \{P_1, \ldots P_i, \ldots P_p\}$. Here, the solution space gets updated based on the fitness criterion.

Fitness for deriving the optimal path

The proposed SA-FPSO algorithm uses the fitness function to regulate the optimization, and it is derived to be a maximization function. For developing the fitness criterion, the distance between the nodes and the trust possessed by the node is considered as the parameter. The expression for the fitness is given as follows,

$$Fitness = \frac{1}{p}\sum_{i=1}^{p} 0.5\left(Z_{path}^{i} + \left[1 - Y_{path}^{i}\right]\right) \quad (5)$$

where, Z_{path}^{i} indicates the trust of the i^{th} optimal path and Y_{path}^{i} indicates the distance of the path. The expression for the trust of the path is expressed as,

$$Z_{path}^{i} = \frac{1}{a^2}\sum_{q=1}^{a-1}\sum_{w=q+1}^{a} Z_{q,w} \quad (6)$$

where, $Z_{q,w}$ indicates the trust between the q^{th} and w^{th} node in i^{th} path, and a indicates the total number of trust nodes in the i^{th} path. The value of the trust $Z_{q,w}$ can be computed as

$$Z_{q,w} = \frac{1}{4} * \left[Z^{direct} + Z^{indirect} + Z^{recent} + Z^{historic}\right] \quad (7)$$

The next major factor in fitness is defining the distance of the path, and it can be computed as,

$$Y_{path}^{i} = \frac{1}{a^2}\sum_{q=1}^{a-1}\sum_{w=q+1}^{a} Y_{q,w} \quad (8)$$

where, a indicates the number of nodes in the i^{th} path. The term $Y_{q,w}$ indicates the distance between the q^{th} and the w^{th} node in the i^{th} path. The distance depends on the

Euclidean distance and simulation area of the MANET and it is expressed as,

$$Y_{q,w} = \frac{E(q,w)}{M} \quad (9)$$

where, $E(q,w)$ indicates the Euclidean distance between the nodes q and w, and M indicates the simulation area of MANET, and it has the dimension of 100×100.

Algorithmic representation of the proposed SA-FPSO algorithm

The proposed SA-FPSO algorithm updates the solution space in adaptive way for change in iteration. In PSO algorithm, the solution update depends merely on velocity and position of current iteration, which acts as a base for the movement of fireflies as depicted in FA [22]. Also, making the solution space adaptive to iteration improves the convergence and also, helps in finding the optimal paths suitable for data transfer. PSO can be made self adaptive by modifying the weight parameters based on iteration count, and the adjustment to inertia parameter is done as specified in self adaptive PSO [24]. Here, the algorithmic steps involved in proposed SA-FPSO algorithm are presented below:

1) Initialization of solution space: The initial step in the proposed SA-FPSO scheme is the initialization of population. As the solution for the proposed SA-FPSO tries to identify p optimal paths from k paths, the solution vector randomly initializes p parameters in solution space.

$$P = \{P_1, P_2, \ldots, P_i, \ldots, P_p\}; 1 \le i \le p \quad (10)$$

where, P_i refer to the i^{th} solution in the population, and the total size of population is set as p.

2) Fitness evaluation: Here, the fitness of the solution determines the feasibility of the path. The fitness of solution depends on the trust and the distance factor, and for the proposed SA-FPSO algorithm, the fitness is declared to be the maximization function as expressed in (5). While calculating the fitness of the solution vectors, it takes the value as 0 (Worst solution) or 1 (Best solution).

3) Solution update based on proposed SA-FPSO algorithm: The position of the solution vector in the search space is updated based on the proposed SA-FPSO algorithm. The PSO algorithm updates the solution space by calculating the velocity, at which the parameter changes its position. The expression for the position update, specified by PSO is given as follows,

$$P_i(T+1) = P_i(T) + V_i(T+1) \quad (11)$$

where, $P_i(T)$ indicates the position of the solution at time instant T and $V_i(T+1)$ indicates the velocity of i^{th} solution at time $(T+1)$. Several factors influence the movement of the particle, and the following expression provides the velocity at time $(T+1)$,

$$V_i(T+1) = WV_i(T) + g_1 h_1 (A_L(T) - P_i(T)) + g_2 h_2 (A_G(T) - P_i(T)) \quad (12)$$

where, $V_i(T)$ refers to the velocity of the i^{th} particle at time duration T, the term W indicates the inertia weight factor chosen between [0,1], the terms g_1 and g_2 indicate the acceleration constants and h_1 and h_2 indicate the random vectors, $A_L(T)$ and $A_G(T)$ indicate the local best and global best solutions. Here, the value of the inertia weight factor W is chosen to be self adaptive. As specified in [24], the PSO was made self adaptive by choosing the value of W as,

$$W = W_{min} + (W_{max} + W_{min}) \exp\left(-\frac{1}{1 + \left(1 + \frac{T}{T_{max}}\right)} \right) \quad (13)$$

where, W_{max} and W_{min} refer to the maximum and minimum value provided for making the algorithm to be self adaptive, and T_{max} indicates the maximum iteration count. While changing the value of W as specified in (13), it adopts a linearly decreasing strategy, and thus, makes the algorithm as self adaptive in nature. Now, the PSO equation is modified as,

$$P_i(T+1) = P_i(T) + W_{min} + (W_{max} + W_{min}) \exp\left(-\frac{1}{1 + \left(1 + \frac{T}{T_{max}}\right)} \right) V_i(T) + g_1 h_1 (A_L(T) - P_i(T)) + g_2 h_2 (A_G(T) - P_i(T)) \quad (14)$$

Rearranging the above equation,

$$P_i(T+1) = P_i(T)[1-g_1h_1-g_2h_2]+(W_{\max}+W_{\min})\exp\left(-\frac{1}{1+\left(1+\frac{T}{T_{\max}}\right)}\right)V_i(T)+g_1h_1A_L(T)+g_2h_2A_G(T) \quad (15)$$

Here, the solution update of the FA algorithm described in [22], is integrated with the PSO. As the PSO and FA have similar properties, the integration improves the convergence of solution space. The solution update of FA is expressed as follows,

$$\mathbf{P_i(T+1) = P_i(T) + \delta_0 e^{-\eta\, n^2}(P_f(T) - P_i(T)) + \omega \in_i} \quad (16)$$

where, $P_f(T)$ indicates the position of f^{th} firefly, which acts as the neighbor to the i^{th} firefly, the term δ_0 indicates the attractiveness achieved at $n=0$, and η indicates the light absorption coefficient, and it has the fixed value. The term ω indicates the random parameter with value between [0,1], and $\in_i$ specifies the parameter in Gaussian distribution. Now, find the value of $P_i(T)$ from expression (16) and it is given as,

$$P_i(T) = \frac{1}{1-\delta_0 e^{-\eta\, n^2}}\left[P_i(T+1) - \delta_0 e^{-\eta\, n^2} P_f(T) - \omega \in_i\right] \quad (17)$$

Now, substitute the value of $P_i(T)$ in the solution update specified by self adaptive PSO. The expression for proposed SA-FPSO is given as,

$$P_i(T+1) = \frac{1}{1-\delta_0 e^{-\eta\, n^2}}\left[P_i(T+1) - \delta_0 e^{-\eta\, n^2} P_f(T) - \omega \in_i\right][1-g_1h_1-g_2h_2]+$$
$$(W_{max}+W_{min})\exp\left(-\frac{1}{1+\left(1+\frac{T}{T_{max}}\right)}\right)V_i(T)+g_1h_1A_L(T)+g_2h_2A_G(T) \quad (18)$$

Rearranging the above equation yields the required solution update of SA-FPSO, and it is expressed as,

$$P_i(T+1) = \frac{1-\delta_0 e^{-\eta\, n^2}}{1-\delta_0 e^{-\eta\, n^2}-(1-g_1h_1-g_2h_2)}\left[\begin{array}{l}(W_{max}+W_{min})\exp\left(-\frac{1}{1+\left(1+\frac{T}{T_{max}}\right)}\right)V_i(T)+g_1h_1A_L(T)+g_2h_2A_G(T)\\ -\left(\frac{1}{1-\delta_0 e^{-\eta\, n^2}}(\delta_0 e^{-\eta\, n^2} P_f(T)+\omega \in_i)\right)[1-g_1h_1-g_2h_2]\end{array}\right] \quad (19)$$

The above equation indicates the expression for the proposed SA-FPSO algorithm. Incorporation of FA in PSO improves the effectiveness of algorithm in finding the p optimal paths, and self adaptive nature makes the algorithm to achieve high speed convergence.

4) Identifying the best solution: Here, the best solution is identified by evaluating the fitness of the solutions. As presented in expression (5), the fitness for the proposed SA-FPSO algorithm is designed as the maximization function. Thus, the solution providing high fitness function is declared to be best solution, and it replaces the global best in solution update.

5) Termination: At the end of iteration T_{max}, the optimal p paths found by optimization procedure are retained and the data transfer is done.

Flow diagram of the proposed intrusion detection scheme

The proposed scheme aims in establishing the secured routing path between the source and the destination nodes. For this purpose, the malicious nodes in the network are identified with genetic neuro-fuzzy system. Figure 3 presents the flow diagram of various processes involved in proposed intrusion detection scheme.

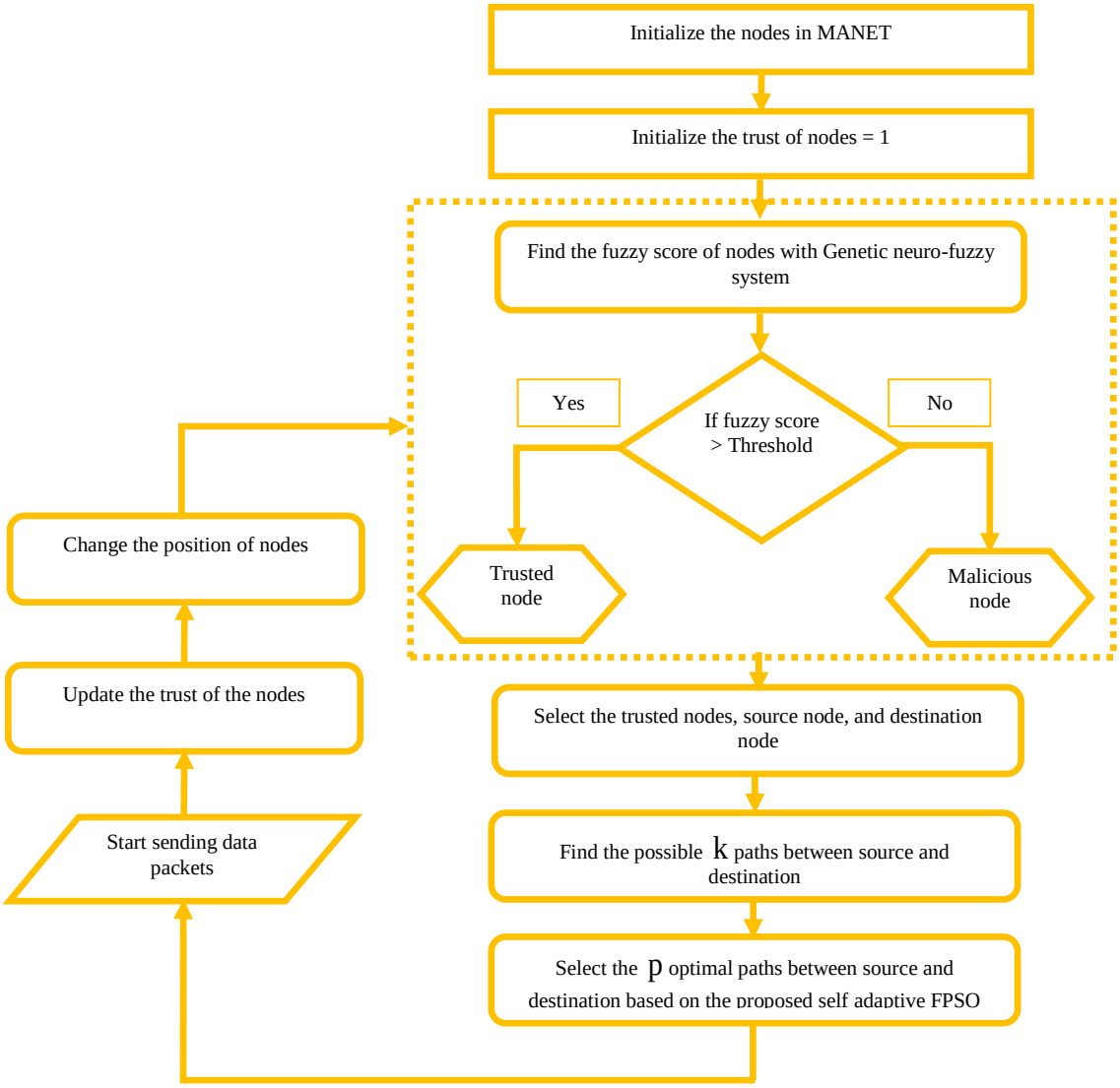


Figure 3. Flow diagram of IDPS scheme with the proposed SA-FPSO and Genetic Neuro-Fuzzy system

The operation of the proposed IDS scheme is described as follows: Initially, the number of nodes, source node, and destination node are initialized. Before the path establishment, the nodes will not be under attack; hence the trust for each node can be initialized as 1. During the data transfer, the trust of the nodes comes under scrutiny as the network attacks influence the data transfer. For detecting the nodes under attack, the fuzzy score of the nodes are determined with the help of genetic neuro-fuzzy system. The node having fuzzy score above threshold is declared to be trusted node and other as the malicious nodes. Then, genetic neuro-fuzzy system declares the number of trusted nodes in entire MANET. Elimination of malicious nodes from the system creates possible k paths between the source and the destination. The paper proposes SA-FPSO algorithm to identify the optimal p paths among k paths through the optimization process. Whenever, new data enters the system, the trust of the nodes gets updated based on equations (1), (2), (3), and (4), respectively, and the fuzzy score is recalculated. The process repeats for each data entry, and the use of SA-FPSO algorithm makes the process to be suitable in real time.

RESULTS AND DISCUSSION

This section discusses the results achieved by the proposed intrusion detection scheme. Here, the performance of Genetic Neuro-Fuzzy system and the SA-FPSO classifier are analyzed.

Experimental setup

The simulation of the proposed intrusion detection scheme is implemented in NS2 tool, with the PC having configurations of Ubuntu16.04, 4 GB RAM, and Intel I3 processor. For the experimentation of the proposed scheme, few parameters are utilized and it is expressed in table 1.

Algorithmic parameters: Population size p =25, Maximum iteration T_{max} =100.

Table 1. Parametric values

Parameters	Value
Radio-propagation model	Propagation/TwoRayGround
MAC type	Mac/802_11
Network interface type	Phy/WirelessPhy
Interface queue type	Queue/Drop Tail/PriQueue
Link layer type	LL
Antenna model	Antenna/OmniAntenna
Routing protocol	AODV
Max packet in ifq	500
Packet Size	512
Rate	250kbps
X-axis	700
Y-axis	300
Number of Nodes	100
Simulation Time	50sec

Evaluation metrics

Evaluation of IDS scheme with the proposed SA-FPSO algorithm with other comparative techniques is done with the metrics, such as throughput, delay, and detection rate. The expression for the evaluation metrics is defined below:

Throughput: It defines the ratio of the total number of data packets delivered between the source and the destination in stipulated time interval, and the expression is given as,

$$\text{Throughput} = \frac{R_b}{X} \tag{20}$$

where, R_b refers to the total data packets delivered in simulation time X.

Delay: Delay refers to the sum of delays posed by total nodes during the data reception and transmission, and it is expressed as,

$$Delay = \frac{\sum \left(c^{tr} - c^{re} \right)}{B} \tag{21}$$

where, c^{tr} and c^{re} indicates the time taken by the nodes for transmission and reception of data.

Detection rate: The IDS detects the malicious nodes for establishing the secured routing path, and high detection rate indicates improved performance. Detection rate defines the ratio to total number of malicious node detected by IDS out of total nodes in MANET, and it is expressed as,

$$\text{Detection Rate} = \frac{K}{B} \tag{22}$$

where, K indicates the total number of malicious nodes detected by IDS in MANET.

Comparative techniques

For comparative analysis, this work utilized several existing works, such as Fuzzy integrated Particle Swarm Optimization (Fuzzy-FPSO), Hybrid Intrusion Detection System (HIDS) [1], Support Vector Machine Intrusion Detection System (SVM-IDS) [6] and Intelligent Intrusion Detection and Prevention System (IIDPS) [23]. These works while implemented in same platform as proposed SA-FPSO algorithm show varying results. Description to the comparative models used in this work is given below:

Fuzzy-FPSO: Fuzzy FPSO integrates the fuzzy theory and firefly optimization approach with the PSO algorithm for detecting the malicious nodes in network. After detecting the malicious nodes, the algorithm establishes secured path along the secured nodes.

HIDS: HIDS module develops IDS scheme by hybridizing novel light weight and heavy weight module. The threshold based scheme reduces the network traffic and hereby, achieved low power consumption.

SVM-IDS: SVM-IDS technique develops IDS scheme along with SVM for differentiating malicious nodes from normal node.

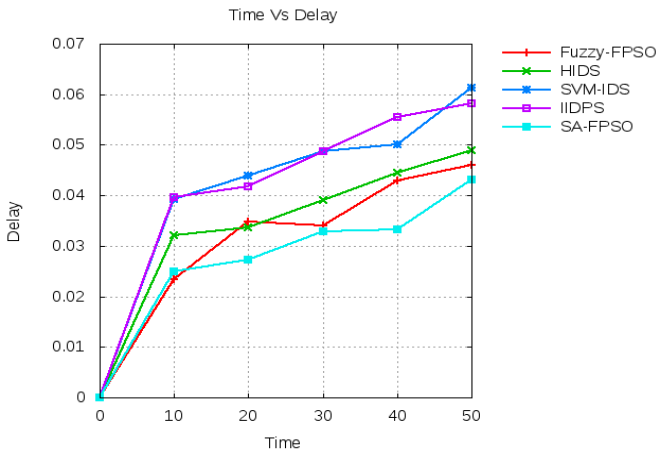
IIDPS: The IIDPS includes both detection and prevention scheme by having trust manager and attacker detection module.

Comparative analysis

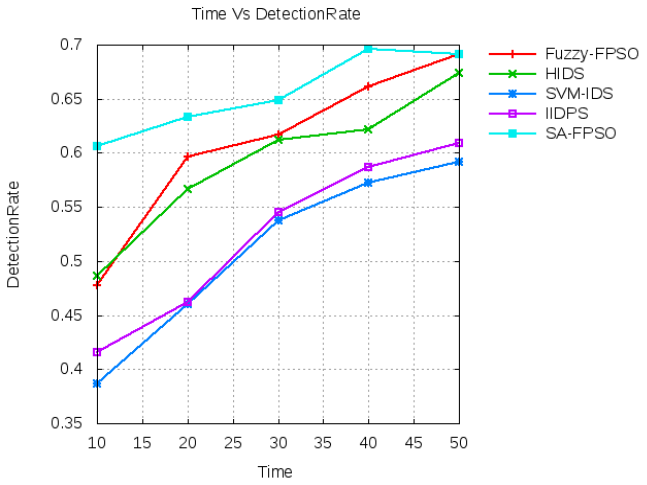
The performance of the proposed scheme is analyzed by introducing different attacks, namely flooding attack, black hole attack and selective packet dropping attack, and robustness against attacks is measured.

Comparative analysis under the black hole attack

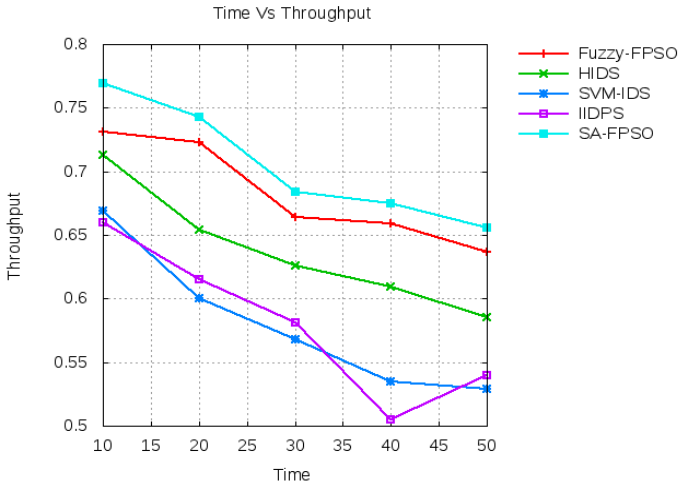
Here, the performance of comparative models when the MANET is under black hole attack is explained. Under the influence of black hole attack, the network may undergo packet loss, and delay in communication. Figure 4 presents the comparative performance of techniques in MANET under black hole attack. Performance of models based on delay as depicted in figure 4.a suggests that, the proposed SA-FPSO model achieved less delay in entire operating time. The proposed SA-FPSO achieved less delay value of 0.04319 sec at time = 50 sec, while other techniques, such as Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS achieved delay value of 0.04597 sec, 0.04900 sec, 0.06136 sec, and 0.05822 sec, respectively. Figure 4.b depicts the performance of models against detection rate while MANET faces the threat under black hole attack. The proposed SA-FPSO algorithm achieved increase in detection rate for increase in time, and at time = 50 sec, the scheme achieved detection rate of 0.691. Other existing models, such as Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS models have low detection rate of 0.691, 0.674 0.592, and 0.609, respectively, at 50 sec. Figure 4.c presents the performance of models based on throughput metric, while the MANET is attacked from black hole attack. The comparative models, Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS achieved throughput value of 0.637, 0.585, 0.529, and 0.540, respectively, at 50 sec. The proposed SA-FPSO algorithm has high throughput value of 0.656 during time = 50 sec.



(a)



(b)



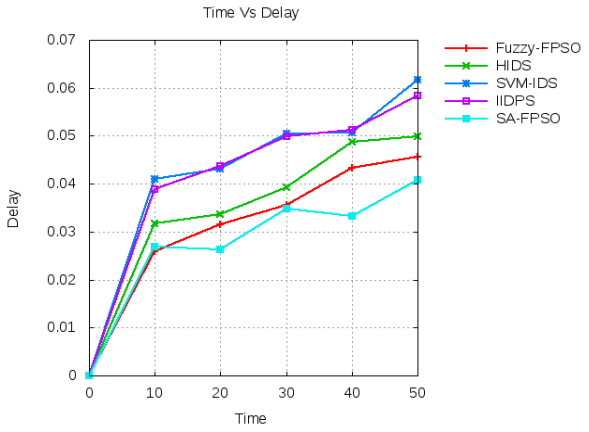
(c)

Figure 4. Comparative analysis of techniques when system is under black attack based on (a) delay, (b) detection rate, and (c) throughput

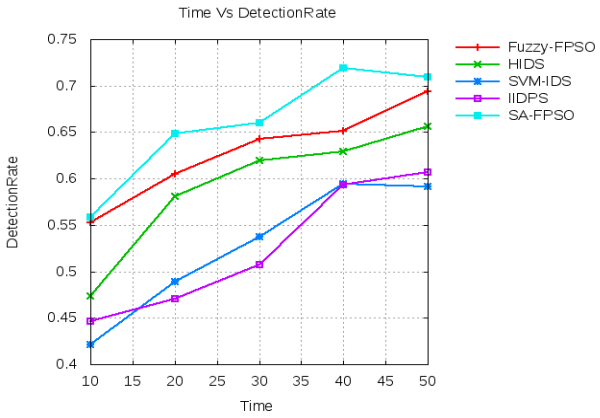
Comparative analysis under the flooding attack

Here, performance of models while MANET is under the influence of flooding attack. Figure 5 presents the comparative performance of techniques based on delay, detection rate, and throughput, and the effects of flooding attacks are analyzed. Figure 5.a presents the performance of comparative models based on delay metric. The proposed SA-FPSO achieved less delay value of 0.0408 sec at time = 50 sec, while other techniques, such as Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS achieved delay value of 0.0456 sec, 0.0499 sec, 0.0616 sec, and 0.0584 sec respectively. Figure 5.b depicts the performance of models against detection rate, while MANET faces the threat under flooding attack. The proposed SA-FPSO algorithm achieved increase in detection rate for the increase in time, and at time = 50 sec, the scheme achieved detection rate of 0.709. Other existing models, such as Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS models have the low detection rate of 0.694, 0.674, 0.591, and 0.607,

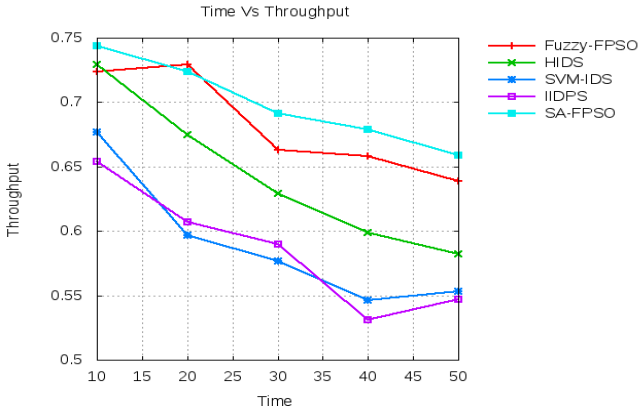
respectively, at time = 50 sec. Figure 5.c presents the performance of models based on throughput metric under the influence of flooding attack. The comparative models, Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS achieved throughput value of 0.639, 0.582, 0.553, and 0.547, respectively, at time = 50 sec. The proposed SA-FPSO algorithm has high throughput value of 0.659 during time = 50 sec.



(a)



(b)

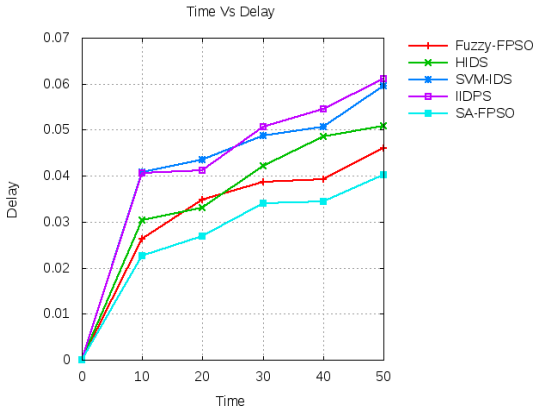


(c)

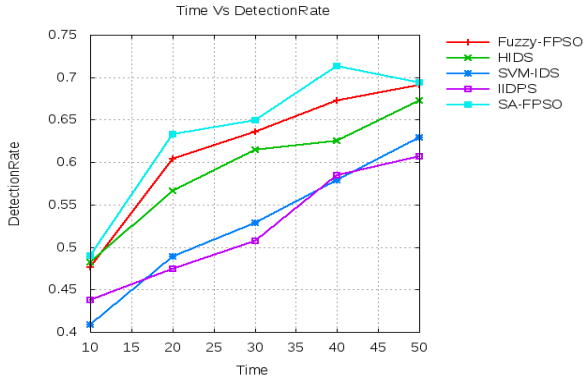
Figure 5. Comparative analysis of techniques when system is under flooding attack based on (a) delay, (b) detection rate, and (c) throughput

Comparative analysis under the Selective packet drop attack

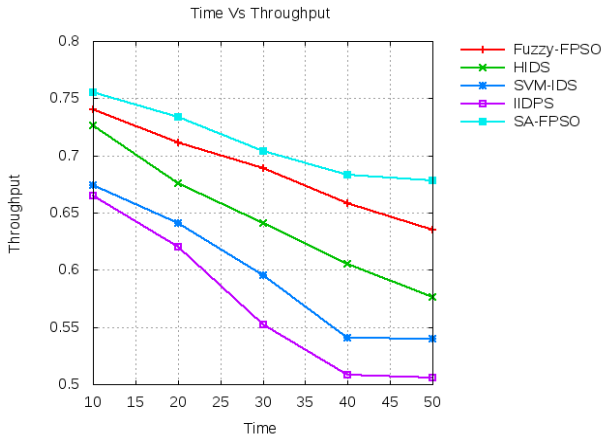
Selective packet drop attack indulges communication between the source and the destination and makes it difficult to establish secured routing path.



(a)



(b)



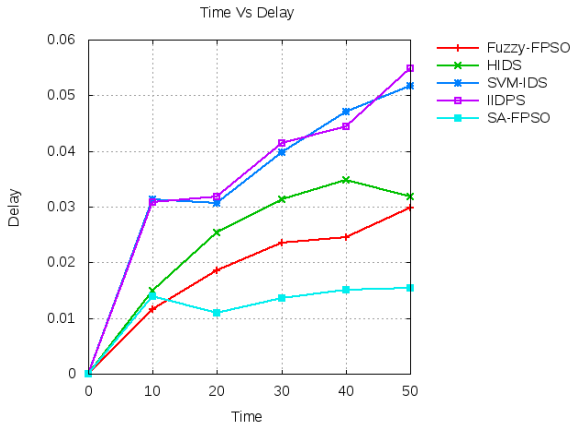
(c)

Figure 6. Comparative analysis of techniques when system is under selective packet drop attack based on (a) delay, (b) detection rate, and (c) throughput

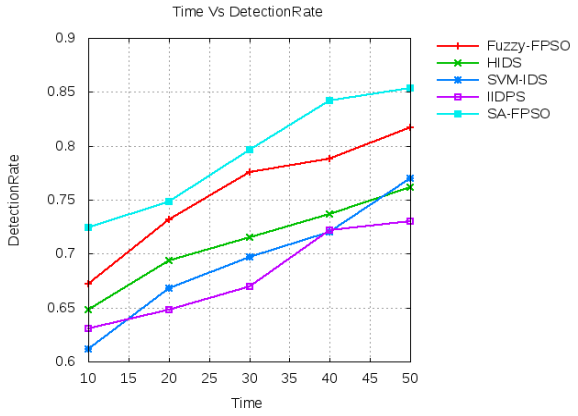
Figure 6 presents the performance of comparative models against the effect of selective packet drop attack. Delay performance as depicted in figure 6.a, suggests that the proposed SA-FPSO model achieved less delay in entire operating time. The proposed SA-FPSO achieved less delay value of 0.04028 sec at time = 50 sec, while other techniques, such as Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS achieved delay value of 0.04595 sec, 0.05079 sec, 0.05959 sec, and 0.06105 sec, respectively. Figure 6.b depicts the performance of models against detection rate while MANET faces the threat under selective packet drop attack. The proposed SA-FPSO algorithm achieved increase in detection rate for increase in time, and at time = 50 sec, the scheme achieved detection rate of 0.694. Other existing models, such as Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS models have low detection rate of 0.691, 0.673 0.692, and 0.607, respectively, at time = 50 sec. Figure 6.c presents the performance of comparative models based on throughput metric when the MANET is attacked from selective packet drop attack. The comparative models, Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS achieved throughput value of 0.635, 0.576, 0.540, and 0.506 respectively at time = sec. The proposed SA-FPSO algorithm has high throughput value of 0.678 during time = 50 sec.

Comparative analysis under without attack

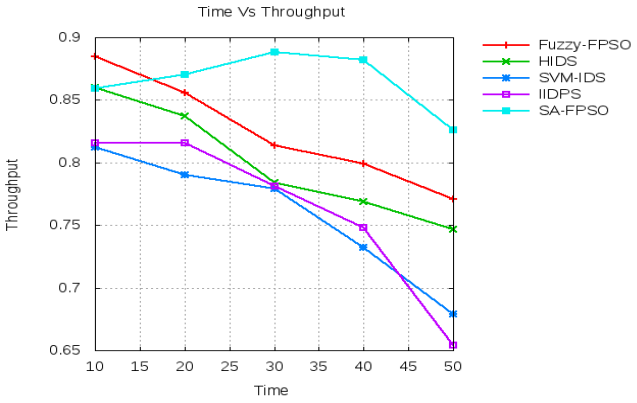
This analysis states the performance of comparative models under the ideal case, where the MANET faces no threat from any kind of attacks. Basically, the performance of comparative models is better while MANET faces no threat. Figure 7 depicts the comparative performance of models against the evaluation metrics for varying time duration. Figure 7.a depicts the performance of models based on delay, and the proposed SA-FPSO model achieved less delay in entire operating time. The proposed SA-FPSO achieved less delay value of 0.01548 at time = 50 sec, while other techniques, such as Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS achieved delay value of 0.02979, 0.03180, 0.05164, and 0.05481, respectively. Figure 7.b depicts the performance of models against detection rate while MANET faces no threat. The proposed SA-FPSO algorithm achieved increase in detection rate for increase in time, and at time = 50 sec, the scheme achieved detection rate of 0.854. Other existing models, such as Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS models have low detection rate of 0.817, 0.762 0.770, and 0.730, respectively, at time=50 sec. Figure 7.c presents the performance of models based on throughput metric when the MANET is free from network attacks. The comparative models, Fuzzy-FPSO, HIDS, SVM-IDS, and IIDPS achieved throughput value of 0.771, 0.747, 0.679, and 0.654, respectively, at the final simulation time. The proposed SA-FPSO algorithm has high throughput value of 0.826 during time = 50 sec.



(a)



(b)



(c)

Figure 7. Comparative analysis of techniques when system is without attack based on (a) delay, (b) detection rate, and (c) throughput

Comparative discussion

Table 2 discusses the results achieved by the proposed SA-FPSO algorithm, and the effectiveness of proposed scheme against intrusion detection is measured against metrics, such as delay, detection rate and throughput. Here, the methods are evaluated by introducing various attacks on MANET model. For establishing a secured routing path, delay of algorithm

must be less with high detection rate and throughput. As depicted in the table 2, the proposed SA-FPSO algorithm achieved better performance than existing models with the values of 0.04319 sec, 0.691, and 0.769, respectively, for delay, detection rate, and throughput when the MANET faces threat from black hole attack. Among the existing methods, the Fuzzy-FPSO model achieved values of 0.04597 sec, 0.691, and 0.731 for delay, detection rate, and throughput, respectively. Under the influence of flooding attack in MANET, the proposed SA-FPSO system achieved better performance than other models with the values of 0.0408 sec, 0.709, and 0.744, for delay, detection rate, and throughput, respectively. Similarly, the performance of proposed SA-FPSO algorithm achieved better performance with the values of 0.04028 sec, 0.694, and 0.755 for delay, detection rate, and throughput during the selective packet drop attack. Analysis of proposed scheme during the MANET attacks suggests that the SA-FPSO algorithm successfully mitigates the network attacks. During the state of no attack in MANET, the performance of proposed scheme achieved high performance with the values of 0.0154 sec, 0.854, and 0.859 for delay, detection rate, and throughput, respectively.

Table 2. Best performance under the influence of various attacks

Attack on MANET	**Evaluation metrics**	**Comparative models**				
		Fuzzy-FPSO	**HIDS**	**SVM-IDS**	**IIDPS**	**SA-FPSO**
Black hole attack	**Delay (sec)**	0.04597	0.0490	0.06136	0.05822	**0.04319**
	Detection rate	0.691	0.674	0.592	0.609	**0.691**
	Throughput	0.731	0.713	0.669	0.660	**0.769**
Flooding attack	**Delay (sec)**	0.04565	0.04997	0.0616	0.05843	**0.0408**
	Detection rate	0.694	0.656	0.591	0.607	**0.709**
	Throughput	0.724	0.729	0.677	0.654	**0.744**
Selective packet drop attack	**Delay (sec)**	0.04595	0.0507	0.0595	0.061	**0.04028**
	Detection rate	0.691	0.673	0.629	0.607	**0.694**
	Throughput	0.740	0.726	0.674	0.665	**0.755**
Without attack	**Delay (sec)**	0.02979	0.03180	0.0516	0.0548	**0.01548**
	Detection rate	0.817	0.762	0.770	0.730	**0.854**
	Throughput	0.885	0.747	0.812	0.816	**0.859**

CONCLUSION

This work develops the IDS based secured routing scheme for secured data transmission in MANET. As the nodes in MANET comes under varying attacks, it is necessary to identify the trust nodes for path establishment. For this purpose, the genetic neuro-fuzzy classifier is employed, and it identifies the trust node based on various trust factors. Now, the secured path between the source and destination are generated as the optimization problem. The proposed SA-FPSO algorithm selects the optimal paths through the optimization. The proposed SA-FPSO algorithm is newly developed by integrating the properties of PSO and FA along with self adaptive nature. Finally, the communication between the source and destination is done through the secured routing path generated by proposed SA-FPSO. Simulation of the proposed SA-FPSO algorithm is done in NS2 simulator, by developing a MANET setup under various attacks. Simulation environment evaluates the performance of proposed scheme under the black hole, flooding and selective packet drop attack. From the simulation results, it is evident that the proposed SA-FPSO algorithm achieved better performance than comparative models with the value of 0.0154 sec, 0.854,

REFERENCES

[1] Singh, O., Singh, J. and Singh,S R., “An Intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks against Malicious Nodes,” Indian Journal of Science and Technology, vol. 10, no. 14, pp. 1-12, 2017.

[2] Babu, M.R. and Usha, G., “A Novel Honeypot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black Hole Attacks in MANET,” Wireless Personal Communications, vol. 90, no. 2, pp.831-845, 2016.

[3] P. Joshi, P. Nande, A. Pawar, P. Shinde and R. Umbare, "EAACK - a secure intrusion detection and prevention system for MANETs," In proceedings of International Conference on Pervasive Computing (ICPC), pp. 1-6, Pune, 2015.

[4] Khan, F.A., Imran, M., Abbas, H. and Durad, M.H., “A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks,” Future Generation Computer Systems, vol. 68, pp.416-427, 2017.

[5] N. Marchang, R. Datta and S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 66, no. 2, pp. 1684-1695, Feb. 2017.

[6] Shams, E.A. and Rizaner, A., "A novel support vector machine based intrusion detection system for mobile ad hoc networks," Wireless Networks, pp.1-9, 2017.

[7] Gurung, S. and Chauhan, S., "A novel approach for mitigating route request flooding attack in MANET," Wireless Networks, pp.1-16, 2017.

[8] Bisen, D. and Sharma, S., "Fuzzy Based Detection of Malicious Activity for Security Assessment of MANET," National Academy Science Letters, pp.1-6, 2017.

[9] Bhuvaneswari, R. and Ramachandran, R., "Denial of service attack solution in OLSR based manet by varying number of fictitious nodes," Cluster Computing, pp.1-11, 2018.

[10] 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.

[11] Thivakaran, T.K. and Sakthivel, T., "GUARD: an intrusion detection framework for routing protocols in multi-hop wireless networks," Wireless Networks, pp.1-18, 2017.

[12] Gurung, S. and Chauhan, S., "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET," Wireless Networks, pp.1-14, 2017.

[13] Pragya, M., Arya, K.V. and Pal, S.H., "Intrusion Detection System Against Colluding Misbehavior in MANETs," Wireless Personal Communications, pp.1-13, 2017.

[14] Chen, M., Wang, N., Zhou, H. and Chen, Y., "FCM technique for efficient intrusion detection system for wireless networks in cloud environment," Computers & Electrical Engineering, 2017.

[15] Singh, O., Singh, J. and Singh, R., "Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET," Cluster Computing, pp.1-13, 2017.

[16] Mechtri, L., Tolba, F.D. and Ghanemi, S., "An optimized intrusion response system for MANET," Peer-to-Peer Networking and Applications, pp.1-17, 2017.

[17] Shahabi, S., Ghazvini, M. and Bakhtiarian, M., "A modified algorithm to improve security and performance of AODV protocol against black hole attack," Wireless Networks, vol. 22, no. 5, pp.1505-1511, 2016.

[18] Mohanapriya, M. and Krishnamurthi, I, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," Computers & Electrical Engineering, vol. 40, no. 2, pp.530-538, 2014.

[19] Huang, M., Ma, Y., Wan, J. and Chen, X., "A sensor-software based on a genetic algorithm-based neural fuzzy system for modeling and simulating a wastewater treatment process," Applied Soft Computing, vol. 27, pp.1-10, 2015.

[20] Anupam Das and M. Mahfuzul Islam,"SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multi-Agent Systems", IEEE Transactions on dependable and secure computing, vol.9, no.2, 2012

[21] Y. Harold Robinson and M. Rajaram, "Energy-Aware Multipath Routing Scheme Based on Particle Swarm Optimization in Mobile Ad Hoc Networks", Scientific World Journal, Hindawi Publishing Corporation, vol. 2015, pp. 1-9, 2015.

[22] Iztok Fister, IztokFisterJr, Xin-SheYang and JanezBrest, "A comprehensive review of firefly algorithms," Swarm and Evolutionary Computation, vol.13, pp.34-46, December 2013.

[23] Basant Subba , Santosh Biswas, and Sushanta Karmakar, "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation," Engineering Science and Technology, an International Journal, vol. 19, no.2, pp. 782-799, 2016.

[24] Wang, X.M., Guo, Y.Z. and Liu, G.J., "Self-adaptive particle swarm optimization algorithm with mutation operation based on K-means," In Advanced Materials Research, vol. 760, pp. 2194-2198, 2013.