TRUST FACTOR AND FUZZY-FIREFLY INTEGRATED PARTICLE SWARM OPTIMIZATION BASED INTRUSION DETECTION AND PREVENTION SYSTEM FOR SECURE ROUTING OF MANET

Ramireddy Kondaiah[1] and Bachala Sathyanarayana[2]

[1]Research Scholar, Department of Computer Science, Rayalaseema University, Kurnool ,A.P,India.& Associate Professor, Dept of CSE, PBRVITS, Kavali, Andhra Pradesh , India.
[2]Professor in Computer Science &Technology ,Sri Krishnadevaraya University, Anantapur, A.P, India.

ABSTRACT

Mobile Ad hoc Networks (MANET) is one of the rapidly emanating technologies, which has gained attention in a wide range of applications in the fields of military, private sectors, commercials and natural calamities. Securing MANET is a dominant responsibility, and hence, a trust factor and fuzzy based intrusion detection and prevention system is proposed for routing in this paper. Based on the trust values of the nodes, the fuzzy system identifies the intruder, such that the path generated in the MANET is secured. Moreover, an optimization algorithm, entitled Fuzzy integrated Particle Swarm Optimization (Fuzzy-FPSO), is proposed by the concatenation of the Firefly Algorithm (FA) and Particle Swarm Optimization (PSO) for the optimal path selection in order to provide secure routing. The simulation of the proposed methodology is NS2 simulator and analysis is carried out considering four cases, like without attack, flooding attacks, black hole attack and selective packet drop attack concerning throughput, delay and detection rate. The remarkable evaluation measures of the proposed Fuzzy-FPSO are the maximal throughput of 0.634, minimal delay of 0.044 , maximal detection rate of 0.697 and minimal routing overhead of 0.24550 And the evaluation measure for the case without any attacks are the maximal throughput of 0.762, minimal delay of 0.029 ,maximal detection rate of 0.805 and minimal routing overhead of 0.11511.

KEYWORDS

MANET, Routing, Trust, Fuzzy system, Firefly Algorithm, Particle Swarm Optimization.

1. INTRODUCTION

The wireless communication network is available in many modes with the hasty technology evolution. Because of the omnipresent existence of remarkable factors, like scalability and mobility, the wireless networks [1] are preferred compared to the wired network. One of the crucial applications of the wireless network is the Mobile Ad-hoc Network (MANET), which has uninterrupted self-configuration, self-maintenance and framework-less network for mobile gadgets interlinked without wires [2]. A MANET is a collection of heterogeneous, self-organized and battery powered mobile nodes with varying availability of resources and computation capacity [5]. The communication of data between these nodes is established with the help of neighbors either directly or indirectly without utilizing the support of any central coordinator or permanent framework [6]. MANET is extensively used when the components or mobile nodes are not within the similar transmission range. Single-hop network and multi-hop network are the two types of networks; A network which provides direct communication between nodes existing within the same range is named single-hop network. It doesn't require any intermediate node,

DOI: 10.5121/ijcnc.2018.10102

whereas the multi-hop network provides indirect communication between the nodes by employing intermediate nodes. Owing to the non-availability of the central point of control, it expands to the incorporation of a malicious node into the network leading to various attacks [11] [4]. The enforcing procedure is tough because of the lack of infrastructure; such rare traits make the utilization of MANET in several fields [2]. The vigorous and distributed attribute of MANET makes them applicable in various applications, like monitoring of the environment, reclamation activity at emergencies, military processes, and human-urged hazards [5].

Network security is also a dominant application of MANET since it is an open medium, which is highly vulnerable to malicious attack by several attackers. Such malicious attacks in the MANET [12] are mainly due to the poor physical security measures. Since the MANET is tremendously vulnerable to easy interpolation of non-cooperative nodes and malicious nodes by attackers, a routing table is perpetuated in the network. Because of the distributed architecture in MANET with none of the controlling equipment, like access points or routers, it is troublesome to centralize the monitoring process [2]. The MANET has various routing protocols for providing assurance about the network cooperation, non-availability of the malicious node and routing the packets from source to destination [3]. The recent routing algorithms [25] are not constructed to overcome the malicious attacks, whereas the newly designed routing protocols are readily susceptible to react to the security hazards in the MANET [3]. Even though the networking technology has evolved to a greater extent in the last decade from fixed to wireless communication, the Intrusion Detection and Prevention (IDP) is still confessed as the primitive layer of defense. But in MANET, the IDP is declared as the elemental layer of defense since the implementation of the firewall is complicated [14] [9].

The malfunctionality of network gadgets, congestion in the network, active attack and intrusions are the major causes of the abnormality in MANET. An acute aberration, which spoils the availability and service integrity of a network, is the Intrusion [8]. Since the standard security measures like authentication and security don't assure complete network protection, the IDP mechanisms are extensively employed to protect the MANETs [9]. This IDP secures the nodes in the network from routing attacks. The two major Intrusion Detection (ID) schemes are Knowledge-Based Intrusion Detection (KBID) and Anomaly-Based Intrusion Detection (ABID). The KBID predicts only the attacks, whose signatures are already in the database. It has probably low false detection rate, whereas ABID exploits even the fresh and abrupt attacks, providing warning alarms for other expected intrusions. But KBID is highly prone to produce false positives compared to ABID [15]. Intrusion Detection Systems (IDSs) are employed to inspect the movements and destructive offensive actions within the network [14]. IDSs [26] investigate the unapproved operation of system and aggression in the network architecture. The IDS consideration is important because of the technology advancement and high chances of threats on the internet [13] [10]. Intrusion Prevention Systems (IPSs) are usually used to identify and protect the network from abominable traffic and the malicious attack consequences. Hence, an Intelligent Intrusion Detection and Prevention System (IIDPS) with the cooperation of trust management and a detection algorithm for the attack is proposed for identifying the malicious node [10].

This research intends to design an IDPS with the assistance of trust management and attacker's detection algorithm. The major goal of this proposed IDPS system is to provide the nodes with the secured path rather than the shortest path. This scheme explores all the feasible paths from the source node to a destination node on the basis of their trust modeled based on four trust factors, such as direct, indirect, recent and historic trust. From these feasible paths, the best optimal path is selected by the utilization of the newly devised FPSO algorithm, constructed by the incorporation of the FA and PSO optimization algorithms. The optimized path with the maximum trust is conferred as the best secure path for routing. It also discovers and protects the nodes from malicious attacks by enhancing the detection rate, throughput, and delay.The major contribution of this research is developing a trust-based optimization algorithm, FPSO, by the integration of FA and PSO for the optimal path selection and thereby, combining the algorithm with the fuzzy logic, to develop fuzzy-FPSO, for the secured data communication in MANET.

The Organization of the rest of the paper is : the literature survey is discussed in Section 2, here the related works of IDSs are reviewed, the sytem setup together with the trust model are explained in section 3, the proposed IDPS scheme for protecting nodes from attacks and providing a secured routing path is elaborated in Section 4, the simulation results of the proposed work is available in Section 5 and finally, the conclusion of the research is made in Section 6.

2. Motivation

2.1 Related Works

This section elaborates the algorithms and techniques used in the priorly existing systems for the IDP in MANETs to gather some knowledge for the proposed IIDPS implementation Opinder Singh *et al.* [10] proposed an Intelligent IDPS (IIDPS), for protecting the ad-hoc network from malicious attacks. It was comprised of a central network administrator for malicious node detection and a trust manager to classify the network trust into various categories. This methodology enhances the performance of networks in MANET, but it is not convenient for detecting several types of attack in data mining.

Rajesh Babu and Usha [2] presented a Novel Honeypot Based Detection and Isolation Approach (NHBADI) that supported in detection and isolation of black hole attacks in MANET. Along with the detection of the malicious nodes, the approach had isolated the black hole prone nodes in the network. It improved the network security by minimizing the packet drop ratio, network overhead and normalized routing load. One of the considerable drawbacks is it doesn't track or solve the intruder activity of indirect interaction.

Poonam Joshi *et al.* [3] developed an Enhanced Adaptive ACKnowledgment (EAACK) technique for detection of malicious behavior. It is a powerful attack controlling mechanism guaranteeing data security, but it cannot handle the attacks like black hole attack or even spoofing.

Farrukh Aslam Khan *et al.* [4] presented a Detection and Prevention System (DPS) technique to identify and thwart the malicious nodes in MANETs. For continuous monitoring of the nodal behavior some special nodes, named DPS nodes, were employed. When the DPS node had predicted some abnormal nodal behavior, the technique could assign that node as a wormhole, broadcasting the message to the other nodes to terminate the control and data messages to the particular node. The main advantage was it minimized the total number of dropped packets due to the malicious nodes with a minimum false positive rate. However, the technique is not suitable to modify the DPS system to prevent the network from other similar attacks.

Basant Subba *et al.* [5] developed a Bayesian game theory based MANET IDS scheme to address the rapid depletion of battery life of node. The scheme comprised of an election process based on cluster leader and hybrid IDS. The election process with respect to cluster leader had elected the cluster leader for intrusion detection service by utilizing Vickrey–Clarke–Groves scheme. The hybrid IDS consisted of a lightweight module based on a threshold and a heavyweight module based on the powerful anomaly. The scheme reduces the power consumption along with the achievement of maximum detection rate and minimum false alarm rate but doesn't target on minimizing false positive rate and enhancing the detection rate of hybrid MANET IDS heavyweight and lightweight modules.

Marchang *et al.* [6] presented a Probabilistic model, which utilized the cooperation among the neighboring node IDSs for reducing the individual active time. The model aimed to decrease the active time duration of IDSs without affecting its effectiveness. The interactions between the IDSs were modeled as a multi-player cooperative game, which provided partially conflicting and partially cooperative goals, for the validation purpose. The model enhances the network lifetime significantly but is not suitable for heterogeneous networks.

G. Usha *et al.* [7] proposed a Honeypot Based Dynamic Anomaly Detection Using Cross-Layer Security (HBDADCS), for prediction and protection of the MANET from black hole attack. This technique enhanced the detection accuracy of attacks and provided better delivery of packets. However, due to the least percentage of black hole nodes, the network load is very low.

Erfan A Shams, and Ahmet Rizaner [8] developed a SVM-based IDS to predict the Denial of Service (DoS) type of attacks. The system had provided continuous monitoring of the network to predict and eliminate the malicious nodes in the MANET, in order to enhance its performance. It had intensified the network reliability and was independent of the network size, node mobility and network routing protocol. The system could detect and remove the network attacks within a short computing time, and high detection rate, but the packet delivery ratio shrinks when a malicious node is available in the system.

2.2 Challenges

Some of the perceived challenges from the above literature survey are stated as follows,

- The traditional routing protocols can't effectively predict and protect the MANET from various intruder attacks. One of the highly demanded aspects in MANET design is the evolution of a secure routing protocol [4].
- The Bayesian game theory based MANET IDS scheme [5] doesn't address several issues, like the prediction of selfish nodes in MANETs with high accuracy, reducing the computational overhead associated with the mechanism of cluster leader node selection.
- On implementation of SVM-based IDS [8], the packet delivery ratio decreases due to the availability of malicious nodes in the system. The end-to-end delay is maximum when malicious nodes attack the network. When the network is affected by a large number of malicious nodes, the effect becomes worse.

3. Network Model Of MANET

A MANET is a self-configured collection of wireless devices or nodes, which easily transmit and receive data with the support of MANET. The type of application decides the node density and the number of nodes for data transmission. Figure 1 displays the network model of a MANET with a number of nodes, expressed as $A = \{A_1, \cdots, A_v, \cdots, A_q\}$, where q is the total number of nodes in the MANET. Each node is located in the network at the location (a, b), such that the location of v^{th} the node is (a_v, b_v). The source node is denoted as A_S and the destination node is denoted as A_D. The data transmission within the network is done hop by hop because of the limited transmission range [17]. All the nodes that constitute a path are assumed to be within a transmission range, denoted as R. The routing between the source and the destination is carried out on the basis of trust computation value through trusted nodes. Here the nodes with maximum trust value are considered as secured nodes, whereas the nodes with minimum trust value are considered as intruder nodes. The sink used in the MANET, denoted as J acts as a server and manages the traffic and improves the lifetime of the network. There are multiple routes available between the source and destination and the optimal path for transmission is selected by employing FPSO algorithm.

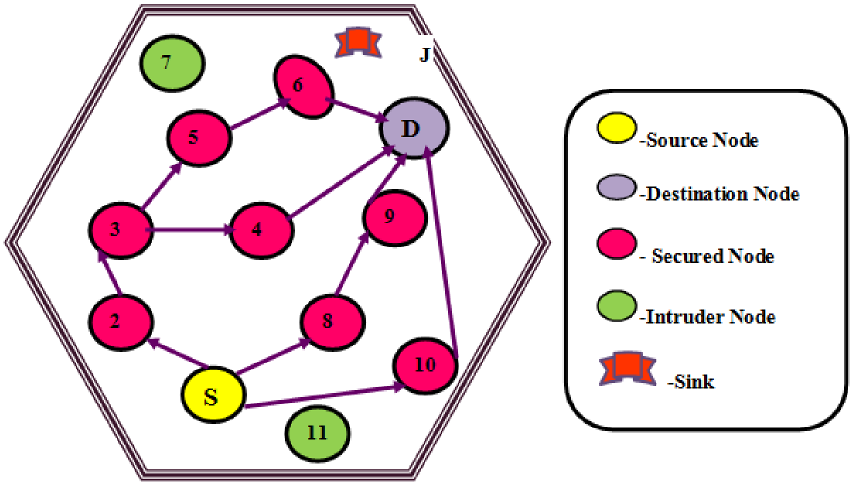


Figure 1. Network Model of MANET

3.1 Trust Computation Model

Trust computation plays an important role in exploiting the trust of agents in the existence of malicious nodes in a network. The main function of the trust model [18] is to gather, disseminate and accumulate the feedback of previous participant nodes. The trust is the relationship between two nodes in a network; trust computation classifies the nodes as trusted and non-trusted nodes. The trust computation value is quantified within the limit 1 to -1, where -1 indicates the non-trusted nodes, +1 indicates the trusted nodes, and 0 indicates the unknown nodes. The four trust computations chosen for predicting the trusted source and destination nodes are direct, indirect, recent and historic.

Direct trust: The direct trust is also called local trust; it indicates the trust portion, which a node calculates from its self-experience about the target nodes.

$$T_{v,w}^{\ direct}(t) = \frac{N_R^{v,w}(t)}{N_S^{v,w}(t)} \tag{1}$$

Where, $T_{v,w}^{direct}(t)$ indicates the direct trust at an instant t, $N_R^{v,w}(t)$ denotes the total number of packets received by A_v from A_w within the time t, i.e., from 1 to t, and $N_S^{v,w}(t)$ indicates the total number of packets sent by A_v to A_w within the time t.

Indirect trust: The indirect trust is also called as recommendation, and is calculated from the experience of neighbouring nodes about the target node.

$$T_{v,w}^{\ indirect}(t) = \frac{1}{n}\sum_{g=1}^{n} T_{g,w}^{direct}(t) \tag{2}$$

Where, $T_{v,w}^{indirect}(t)$ indicates the indirect trust at instant t, n denotes the number of neighbouring nodes of the w^{th} node, where w is the target node whose trust is to be computed, and $T_{g,w}^{direct}(t)$

denotes the direct trust value between the target node w and neighbouring node g, g value varies from $1 \leq g \leq n$.

Recent trust: The recent trust is the integration of direct and indirect trust; it considers the recent behaviours of the target node.

$$T_{v,w}^{recent}(t) = \beta * T_{v,w}^{direct}(t) + (1-\beta) * T_{v,w}^{indirect}(t) \tag{3}$$

Where, $T_{v,w}^{recent}(t)$ denotes the recent trust at instant t, and β represents the direct trust weight, which has the value given by $\beta = 0.5$

Historical trust: The historical trust is calculated by considering the past experiences and long-term behavioural pattern of the target node.

$$T_{v,w}^{historic}(t) = \rho * T_{v,w}^{historic}(t-1) + T_{v,w}^{recent}(t-1) \tag{4}$$

where, $T_{v,w}^{historic}(t)$ notifies the historic trust at instant t, ρ is the forgetting factor whose limit is given by $0 \leq \rho \leq 1$, the historic trust at $(t-1)^{th}$ instant is denoted as $T_{v,w}^{historic}(t-1)$, and the recent trust at $(t-1)^{th}$ instant is indicated as $T_{v,w}^{recent}(t-1)$.

4. Proposed IDPS Based On The Trust Factor And The Firefly Integrated Particle Swarm Optimization Algorithm

The Intrusion Detection and Prevention in MANET utilizing the proposed fuzzy-FPSO is discussed in this section. The primitive goal of this work is to construct a contemporary highly secure routing protocol by implementing trust factor and fuzzy based IDPS methodology. For the Intrusion Detection and Prevention, here a trust factor and Firefly integrated Particle Swarm Optimization (FPSO) algorithms are employed for predicting the secure route in the MANET. The four major phases of this research are i) Trust computation of the nodes, ii) Intrusion detection using fuzzy rule classifier, iii) Path generation, and iv) Selection of the secured path using the proposed FPSO Algorithm. In phase 1, the trust value of every node will be calculated on the basis of various trust factors, like direct trust, indirect trust, recent trust and historic trust. After the successful computation of trust value of nodes, the intrusion detection will be identified on the basis of Fuzzy rule classifier. The attackers intruding the network can be predicted by employing the proposed IDPS with fuzzy rule along with trust factors. Once the secure nodes are identified, the newly designed FPSO algorithm plays the vital role in the optimal path selection for secure routing.

The block diagram of the IDPS implementation using proposed fuzzy-FPSO is depicted in figure 2. The four main steps in the IDPS are intrusion detection, path prediction, optimal path selection, and finally the data transmission. Initially, all the nodes are initialized with trust=1, the intrusion node is detected by utilizing the fuzzy classifier. On the basis of the trust, the source node and the destination node are chosen for the transmission of data. All the paths between the source-destination nodes are predicted considering the trust level of the nodes. For determining the optimal path between source and destination, an integrated newly designed FPSO optimization algorithm is employed that predicts the path concerning the appropriate fitness function. Then, the data will be sent through the predicted optimal path. The upcoming sections elaborate the proposed methodology.

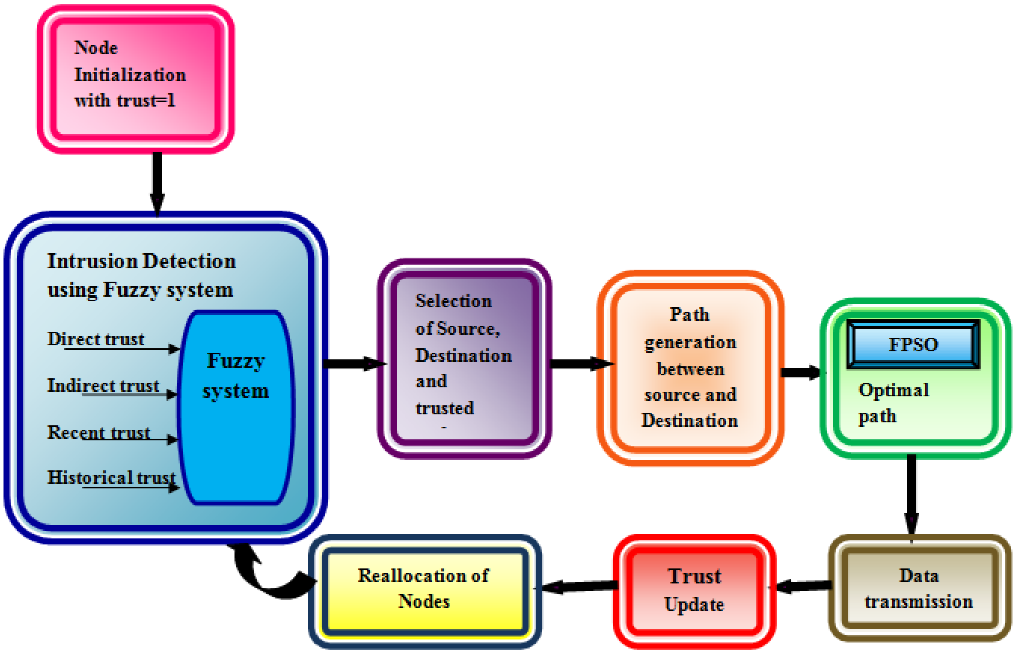

Node Initialization with trust=1
Intrusion Detection using Fuzzy system
Direct trust
Indirect trust
Recent trust
Historical trust
Fuzzy system
Selection of Source, Destination and trusted
Path generation between source and Destination
FPSO
Optimal path
Data transmission
Trust Update
Reallocation of Nodes

Figure 2. Block diagram of IDPS implementation using proposed fuzzy-FPSO

4.1 Fuzzy Based Intrusion Detection In MANET

The similarity between the MANET and the fuzzy system is that both deals with uncertainty. The uncertain mobility of nodes makes the communication in MANET vulnerable. The fuzzy system is adaptable, and it can modify its fuzzy rule set and membership functions, its block diagram is depicted in figure 3. The mathematical pattern representation of the fuzzy set is called as the mathematical function. This fuzzy system [19] is employed to predict the intrusion nodes in a data communication system on the basis of trust computation values. The four main modules [20] for the intrusion detection system using the fuzzy system are i) extraction of trust based parameter module, ii) Inference module of fuzzy, iii) Threshold-based decision module, and iv) Response module. Initially, the extracted trust based parameters are fed to the fuzzy system as the input. The fuzzification is the process of conversion of the input or output value to their semantic level in order to determine its membership function. The relationship between the input and output value is supervised by a set of rules. After the generation of all the rules the resultant control surface is denoted as the constraint output, this mechanism is termed as inference. The process of conversion of fuzzy data into crisp data is said to be defuzzification. In the inference module, the membership functions and the fuzzy rules are applied on the input trust parameters to determine the level of fidelity in each node. In the threshold based decision module, the fidelity level of nodes is compared with the threshold value to predict the behavior of the node. The response module is initiated concluding that, if the fidelity level of a node is greater than the threshold, it is a secured node, whereas if the fidelity level is lesser than the threshold, it is an intruder node.

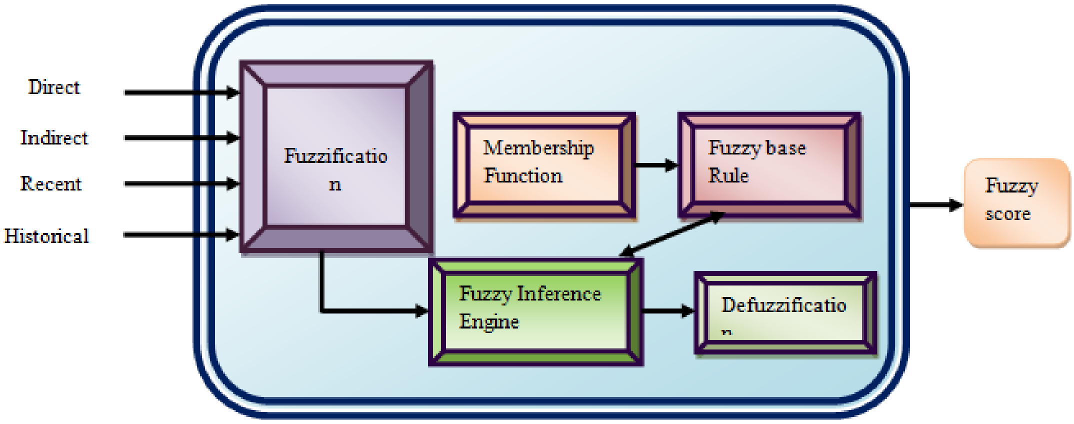


Figure 3. Block Diagram of the Fuzzy System

4.2 Path Generation Between Source And Destination

After the prediction of the secured nodes and intruder nodes using the fuzzy system, the next step is the generation of paths between the source and the destination through the trusted nodes. Thus, all the possible number of paths between the source node, A_S, and the destination node, A_D, are generated for the transmission of packets. Some of the possible paths from the source to the destination in figure 1 can be interpreted as $S \to 8 \to 9 \to D$, $S \to 10 \to D$, $S \to 2 \to 3 \to 4 \to D$, and so on. From the generated paths, the optimal 'p' paths are to be selected by implementing the newly developed FPSO optimization algorithm, based on the objective function, which will be discussed in section 4.3.

4.3 Proposed FPSO For The Selection Of Optimal Path

The important research field, which is based on the collective behaviour of decentralized and self-organized systems, is the Swarm Intelligence (SI). The Firefly Algorithm (FA) is incorporated with the PSO for the optimal path selection. FA [21] [22] is a recently evolved SI, which is a type of nature-inspired, stochastic, meta-heuristic algorithm employed to deal with the hard optimization issues. FA was promoted by the inspiration of firefly's flashing light and was incorporated for determining the optimal path by trial and error method. Initially, it produces new solutions within the search space and then chooses the optimal path for efficient data transmission. Every search process is inveigled by the balance between exploration and exploitation, exploration focuses on the methodologies for the generation of varying solutions within the search space and exploitation denotes the search process within the proximity of optimal solution. The main advantages of FA are it posses multi-nodal characteristics and so, it can easily solve the multi-nodal issues, providing faster convergence. Moreover, it can solve both local and global problems. Particle Swarm Optimization (PSO) algorithm [16], [23] is also a stochastic Optimization algorithm based on SI, imitating the social behaviour of animals, like herd, birds, fishes and insects. Each particle is defined as the promising solution for the search space's optimal problems by memorizing the position and velocity of the swarm. For every generation, the information of particles is merged together for altering the dimension's velocity, which is used for computing the new particle position. In the search space of multi-dimension, there is a constant alteration in the particle state, until the optimum or balanced state is reached. The fitness functions are utilized for creating an exclusive connection between the varying dimensions in the problem space. The major advantages of PSO are faster convergence, simple and easy, robust, applicable to the varying environment with minimal modifications and provide better performance on hybridization with other algorithms. The above-discussed FA is incorporated with the PSO in order to select the optimal p-paths from the generated paths. The optimal path is selected for the data transmission to provide effective communication by minimizing the intrusion.

4.3.1 Solution Encoding

The simplest representation of the algorithm's procedure is given by the solution encoding. The encoding method for prediction of the optimal path by the proposed FPSO is mentioned here. From the generated paths, the optimal path via non-intruded nodes is chosen by using the proposed FPSO algorithm. Let 'P' be the number of paths generated between the source and the destination. Let the population representing P number of solutions or the solution set be $G = \{1,2,\cdots,P\}$. By utilizing the fitness function the binary valued solution is obtained. For the secure transmission of packets during routing, the fitness function is developed by considering the distance and trust, as its main objective functions. From the generated P solutions, the proposed FPSO chooses the maximum fitness valued solution, i.e. 'p' paths, for the optimal path selection.

4.3.2 Fitness Formulation

The fitness function included in the optimization scheme makes the decisions based on the solution quality. The major aim of the fitness function of FPSO with distance and trust as its objective is to maximize the fitness value. The distance between the nodes taking part in routing must be in minimum for an efficient route. Trust level is computed between the node and its neighboring nodes for ensuring security in the network. The nodes with the maximum trust level will be only chosen as the intermediate trusted nodes for data transmission. The maximum fitness valued solution is considered as the optimal path of a system. The formulation of fitness function is given below,

$$Fitness = \frac{1}{P}\sum_{k=1}^{P} 0.5\left(T_{path}^{k} + \left[1 - D_{path}^{k}\right]\right) \qquad (5)$$

where, P denotes the considered number of multipaths, T_{path}^{k} indicates the Path trust of the k^{th} path, D_{path}^{k} represents the Path distance of the k^{th} path. The T_{path} value must be maximum in an effective system; it is computed based on the trust of the nodes in the particular path by using the below equation (6).

$$T_{path}^{k} = \frac{1}{m^2}\sum_{c=1}^{m-1}\sum_{d=c+1}^{m} T_{c,d} \qquad (6)$$

where, m denotes the total number of nodes in the particular path, and $T_{c,d}$ indicates the trust value between c^{th} node and d^{th} node in the path k.

The computed path distance value D_{path}^{k} must be in minimum for effective intrusion detection. $T_{c,d}$ and D_{path}^{k} is calculated by using the following equations (7) and (8),

$$T_{c,d} = \frac{1}{4} * \left[T^{direct} + T^{indirect} + T^{recent} + T^{historic}\right] \qquad (7)$$

$$D_{path}^{k} = \frac{1}{m^2}\sum_{c=1}^{m-1}\sum_{d=c+1}^{m} D_{c,d} \qquad (8)$$

Where, the distance between the c^{th} node and d^{th} node is denoted as $D_{c,d}$, and it is formulated as shown in equation (9),

$$D_{c,d} = \frac{ED(c,d)}{SA} \tag{9}$$

where, $ED(c,d)$ denotes the Euclidian distance between c^{th} node and d^{th} node and SA is the Simulation Area of dimension 100×100.

4.3.3 FPSO ALGORITHM

The proposed FPSO was constructed by incorporating FA [21] and PSO [23] algorithm, for the detection and prevention of malicious nodes in MANET, assuring secured data communication. The steps associated with the FPSO algorithm are discussed below,

Step I: Initialization

Initialization of the swarm population is the basic step of the algorithm. The population for the proposed FPSO is expressed as

$$H = \{H_1, H_2, \ldots, H_i, \ldots, H_L\}; 1 \le i \le L \tag{10}$$

Where, L is represented as the population size, and H_i is the i^{th} solution of the population.

STEP II: FITNESS COMPUTATION

The fitness value for each solution is computed using the equation (5), the maximum fitness valued solution is considered as the optimal path for data communication. The node's positions are updated based on the iterative generation of fitness value of the solutions. The optimal path prediction and reallocation of node's location is discussed in the remaining steps.

STEP III: UPDATING POSITION WITH THE INTEGRATED FA

The PSO algorithm was evolved by imitating the animal social behavior of leaderless swarm or group. The best surveillance condition for the animal is achieved by simultaneous communication with the other members already surviving in better circumstances. Finally, the best condition (optimal solution) is achieved by continuous exchange of information between its members [24]. Here every node is considered as a member and the distance and trust level are the information parameters. This PSO is accelerated to provide better results and solves problems of varying diversity when some modifications are included. In this research, the provided modification for PSO is the integration of PSO with FA.

Let the particle position be $H_i(z)$ at time instant z, the position of the particle is updated by adding velocity since the velocity influences the particle position,

$$H_i(z+1) = H_i(z) + U_i(z+1) \tag{11}$$

where, $H_i(z+1)$ is represented as the particle position at $z+1^{th}$ instant and $U_i(z+1)$ is denoted as the particle velocity at $z+1^{th}$ instant and its formula is given by,

$$U_i(z+1) = Fu_i(z) + h_1 s_1 (B_l(z) - H_i(z)) + h_2 s_2 (B_g(z) - H_i(z)) \tag{12}$$

where, $u_i(z)$ is indicated as the velocity at z^{th} instant , F is mentioned as the weight whose value ranges from 0 to 1, the acceleration coefficients are denoted as h_1 and h_2, the random vectors are indicated as s_1 and s_2, the local best solution is denoted as $B_l(z)$, and the global best solution is denoted as $B_g(z)$.

The formulation of position update equation of PSO is shown in the upcoming equations (13), (14) and (15) as follows,

$$H_i(z+1) = H_i(z) + Fu_i(z) + h_1 s_1 (B_l(z) - H_i(z)) + h_2 s_2 (B_g(z) - H_i(z)) \tag{13}$$

$$H_i(z+1) = H_i(z) - h_1 s_1 H_i(z) - h_2 s_2 H_i(z) + Fu_i(z) + h_1 s_1 B_l(z) + h_2 s_2 B_g(z) \tag{14}$$

$$H_i(z+1) = H_i(z)\left[1 - h_1 s_1 - h_2 s_2\right] + Fu_i(z) + h_1 s_1 B_l(z) + h_2 s_2 B_g(z) \tag{15}$$

In the proposed FPSO, FA is employed to improve the performance of PSO for the optimal path selection. Using FA [21], the firefly population is randomly initiated, and the initial parameter value is altered by the inclusion of alpha new function. Based on the fitness value, the best population (optimal solution) is identified, and finally the reallocation of the position of fireflies is done.

$$H_i(z+1) = H_i(z) + \beta_0 e^{-\gamma r^2} (H_j(z) - H_i(z)) + \alpha \in_i \tag{16}$$

where, $H_i(z+1)$ is the firefly position at $z+1^{th}$ instant, $H_i(z)$ is the firefly position at z^{th} instant, j and i are the fireflies considered for position update, β_0 is indicated as the attractiveness at $r = 0$, γ is mentioned as the fixed light absorption coefficient, r is represented as the distance between the two fireflies j and i, α is indicated as the randomization parameter within the limit $[0,1]$ and $\in_i$ is denoted as the random number drawn from Gaussian distribution.

$$H_i(z+1) = H_i(z) + \beta_0 e^{-\gamma r^2} H_j(z) - \beta_0 e^{-\gamma r^2} H_i(z) + \alpha \in_i \tag{17}$$

$$H_i(z+1) = H_i(z)\left[1 - \beta_0 e^{-\gamma r^2}\right] + \beta_0 e^{-\gamma r^2} H_j(z) + \alpha \in_i \tag{18}$$

$$H_i(z) = \frac{1}{1 - \beta_0 e^{-\gamma r^2}} \left[H_i(z+1) - \beta_0 e^{-\gamma r^2} H_j(z) - \alpha \in_i\right] \tag{19}$$

The formulation of position update of FPSO is explained in the upcoming equations by substituting equation (19) in equation (15),

$$\begin{aligned} H_i(z+1) = {} & \left(\frac{1}{1 - \beta_0 e^{-\gamma r^2}} \left[H_i(z+1) - \beta_0 e^{-\gamma r^2} H_j(z) - \alpha \in_i\right]\right)\left[1 - h_1 s_1 - h_2 s_2\right] + \\ & Fu_i(z) + h_1 s_1 B_l(z) + h_2 s_2 B_g(z) \end{aligned} \tag{20}$$

$$\begin{aligned} H_i(z+1) = {} & \left(\frac{H_i(z+1)}{1 - \beta_0 e^{-\gamma r^2}} - \frac{1}{1 - \beta_0 e^{-\gamma r^2}} \left[\beta_0 e^{-\gamma r^2} H_j(z) - \alpha \in_i\right]\right)\left[1 - h_1 s_1 - h_2 s_2\right] + \\ & Fu_i(z) + h_1 s_1 B_l(z) + h_2 s_2 B_g(z) \end{aligned} \tag{21}$$

$$H_i(z+1)=\frac{H_i(z+1)}{1-\beta_0 e^{-\gamma r^2}}\left[1-h_1s_1-h_2s_2\right]-\left(\frac{1}{1-\beta_0 e^{-\gamma r^2}}(\beta_0 e^{-\gamma r^2}H_j(z)+\alpha\in_i)\right)\left[1-h_1s_1-h_2s_2\right]+ \\ Fu_i(z)+h_1s_1B_l(z)+h_2s_2B_g(z) \qquad (22)$$

$$H_i(z+1)\left[1-\frac{1-h_1s_1-h_2s_2}{1-\beta_0 e^{-\gamma r^2}}\right]=-\left(\frac{1}{1-\beta_0 e^{-\gamma r^2}}(\beta_0 e^{-\gamma r^2}H_j(z)+\alpha\in_i)\right)\left[1-h_1s_1-h_2s_2\right]+ \\ Fu_i(z)+h_1s_1B_l(z)+h_2s_2B_g(z) \qquad (23)$$

$$H_i(z+1)\left[\frac{1-\beta_0 e^{-\gamma r^2}-(1-h_1s_1-h_2s_2)}{1-\beta_0 e^{-\gamma r^2}}\right]=-\left(\frac{1}{1-\beta_0 e^{-\gamma r^2}}(\beta_0 e^{-\gamma r^2}H_j(z)+\alpha\in_i)\right)\left[1-h_1s_1-h_2s_2\right]+ \\ Fu_i(z)+h_1s_1B_l(z)+h_2s_2B_g(z) \qquad (24)$$

$$H_i(z+1)=\frac{1-\beta_0 e^{-\gamma r^2}}{1-\beta_0 e^{-\gamma r^2}-(1-h_1s_1-h_2s_2)}\left[Fu_i(z)+h_1s_1B_l(z)+h_2s_2B_g(z)-\left(\frac{1}{1-\beta_0 e^{-\gamma r^2}}(\beta_0 e^{-\gamma r^2}H_j(z)+\alpha\in_i)\right) \left[1-h_1s_1-h_2s_2\right]\right] \qquad (25)$$

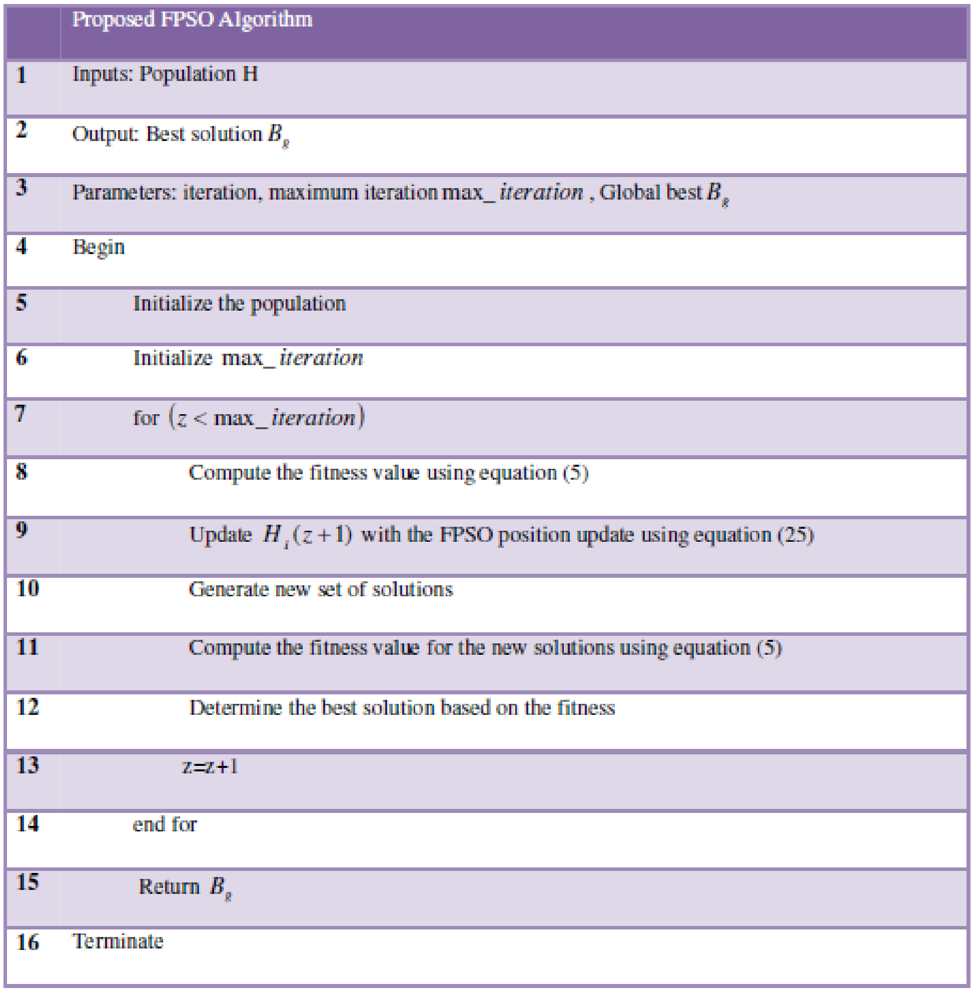
Equation (25) is the finally obtained position update equation by using the proposed FPSO algorithm. Using the above equations the optimal ‘p’ path prediction and the reallocation of nodes in the MANET is done successfully, for routing.

STEP IV: DETERMINATION OF BEST SOLUTION

After the position update of the nodes using equation (25), the fitness value is computed utilizing the fitness function in equation (5). The solution with the maximum fitness value is considered as the best solution.

STEP V: TERMINATION

For the maximum number of iterations, the above steps are iteratively repeated. Finally, the proposed Fuzzy-FPSO optimization algorithm determines the optimal path for secured data transmission within the MANET. The pseudo code for the proposed Fuzzy-FPSO is given below in figure 4.



```
Proposed FPSO Algorithm
Inputs: Population H
Output: Best solution $B_g$
Parameters: iteration, maximum iteration $\max\_iteration$ , Global best $B_g$
Begin
    Initialize the population
    Initialize $\max\_iteration$
    for $(z < \max\_iteration)$
        Compute the fitness value using equation (5)
        Update $H_i(z+1)$ with the FPSO position update using equation (25)
        Generate new set of solutions
        Compute the fitness value for the new solutions using equation (5)
        Determine the best solution based on the fitness
        z=z+1
    end for
    Return $B_g$
Terminate
```

Figure 4. Pseudo code of the Proposed Fuzzy-FPSO Algorithm

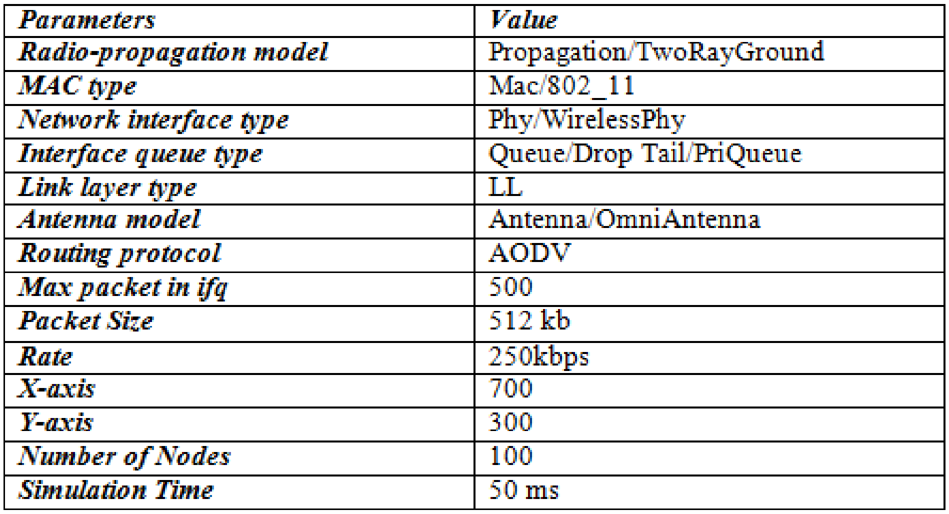
5. Results And Discussions

The results of the proposed Fuzzy-FPSO for optimal path selection in MANET for IDPs are elaborated in this section. The upcoming sections discuss the experimental setup and the simulation along with its performance analysis.

5.1 Experimental Setup

The experimentation is done in a computer configured with OS-Ubuntu-16.04, processor- Intel core i-3, CPU with network adapter frequency as 2.16 GHz and RAM of 2 GB. NS2 Simulator is the software tool utilized for the IDPS of MANET utilizing the proposed Fuzzy-FPSO with various parameters shown in Table 1.

Table 1. Simulation Parameters



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 kb
Rate	250kbps
X-axis	700
Y-axis	300
Number of Nodes	100
Simulation Time	50 ms

5.2 Methods Chosen For Comparison Analysis

The performance analysis of the proposed Fuzzy-FPSO is compared with the other three existing schemes like, Hybrid Intrusion Detection System (HIDS) [5], Support Vector Machine Intrusion Detection System (SVM-IDS) [8] and Intelligent Intrusion Detection and Prevention System (IIDPS) [10]. IIDPS includes a trust manager and attacker detection algorithm for categorizing the network's trust and detect the malicious node. The HIDS includes a threshold based lightweight module and anomaly-based heavyweight module for reducing the IDS traffic and overall power consumption. Meanwhile, the SVM-IDS use a simple structure for detecting the DoS attacks within a short time. The effectiveness of the proposed scheme can be determined by the comparative analysis with the existing approaches.

5.3 Evaluation Measures

The three evaluation metrics considered for the comparative performance analysis are throughput, delay and detection rate, which are defined below,

Throughput: This is a measure used for acknowledging the data packet delivery between the source and the destination in the network. It is expressed as the ratio of the delivered number of data packets to the simulation time.

$$Throughput = \frac{N_d}{T_s} \tag{26}$$

where, the total number of packets delivered is denoted as N_d and the Simulation time is indicated as T_s.

Delay**:** The network's transmission delay is defined as the ratio of the sum of delays in every node to the total number of available nodes. It is expressed as shown in equation (27),

$$Delay = \frac{\sum\left(T^t - T^r\right)}{q} \tag{27}$$

where, the time taken for transmitting the packets is indicated as T^t , the time taken for receiving packets is denoted T^r and the total number of available nodes is denoted as q.

***Detection rate*:** The ratio of the exactly detected number of malicious nodes to the total number of available nodes in the network is called as the detection rate.

$$Detection\ Rate = \frac{N_q}{n} \tag{28}$$

where, the total number of exactly detected malicious nodes is indicated as N_q.

5.4 Comparative Analysis

The comparative analysis of the proposed scheme with other existing schemes for the four cases considered such as, black hole attack, flooding attack, and selective packet dropping attack, and without attacks based on the three evaluation metrics.

5.4.1 Analysis Based On Throughput

Figure.5 displays the comparative analysis plot of throughput for the four cases, like black hole attack, flooding attack, selective packet dropping attack and without attack. Here, in the below plots, the throughput is plotted against the simulation time. In figure 5.a, the throughput measure of black hole attack at initial time 10 sec, is 0.732 for Fuzzy-FPSO, 0.702 for HIDS, 0.654 for SVM-IDS, 0.660 for IIDPS. Similarly, at the final time 50 sec, the throughput values of different approaches are, 0.634 for Fuzzy-FPSO, 0.59 for HIDS, 0.52 for SVM-IDS, and 0.543 for IIDPS. In figure 5.b, the throughput value of flooding attack at initial time instant 10 sec, is 0.740 for Fuzzy-FPSO, 0.691 for HIDS, 0.676 for SVM-IDS, 0.659 for IIDPS. Likewise, at the final time instant 50 sec, the throughput values are as follows: 0.627 for Fuzzy-FPSO, 0.575 for HIDS, 0.523 for SVM-IDS, and 0.559 for IIDPS. In figure 5.c, the throughput measure of selective packet dropping attack at initial time 10 sec is 0.725 for Fuzzy-FPSO, 0.729 for HIDS, 0.651 for SVM-IDS, and 0.672 for IIDPS. Similarly, at the final time 50 sec, the throughput values of different approaches are, 0.626 for Fuzzy-FPSO, 0.588 for HIDS, 0.527 for SVM-IDS, and 0.508 for IIDPS. In figure 5.d, the without attack throughput measure, at initial time 10 sec, for the different approaches are, 0.875 for Fuzzy-FPSO, 0.849 for HIDS, 0.813 for SVM-IDS, and 0.829 for IIDPS. Likewise, at the final time 50 sec, the throughput values of different schemes are, 0.762 for Fuzzy-FPSO, 0.737 for HIDS, 0.668 for SVM-IDS, and 0.684 for IIDPS. The obtained values deliberate that the throughput measure of all the schemes has decreased with the increase in the simulation time. The maximum throughput value is attained by the proposed Fuzzy-FPSO in all the considered four cases compared to the other existing methodologies. The upholding of maximum throughput declares the newly devised scheme as the dominant methodology.

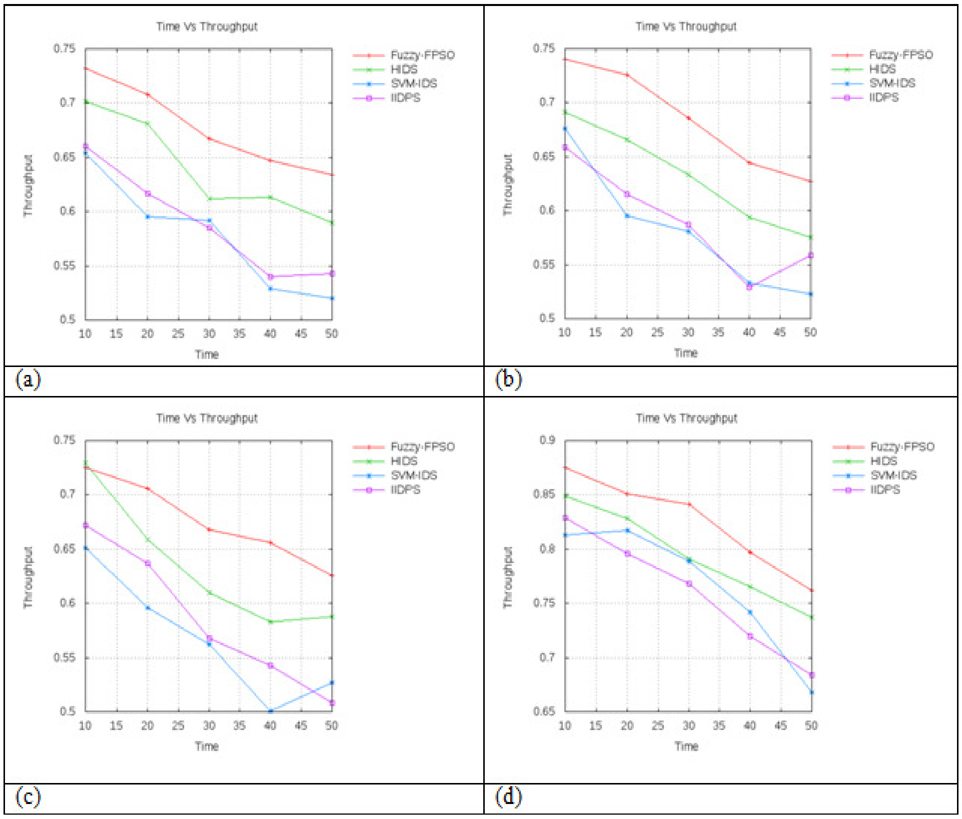


Figure 5. Comparative analysis plot of throughput for (a) Black Hole attack, (b) Flooding attack, (c) Selective Packet Dropping attack and, (d) without attack.

5.4.2 Analysis Based On Delay

The comparative analysis of delay plotted against the simulation time for the four cases, such as black hole attack, flooding attack, selective packet dropping attack and without attack is depicted in figure.6. In figure 6.a, the delay of the schemes for black hole attack at simulation time 10 sec, for Fuzzy-FPSO is 0.023, HIDS is 0.031, SVM-IDS is 0.038, and IIDPS is 0.039. Similarly, the delay at simulation time 50 sec for Fuzzy-FPSO is 0.044, HIDS is 0.049, SVM-IDS is 0.057, and IIDPS is 0.057. In figure 6.b, the delay of the approaches for flooding attack at simulation time 10 sec, for Fuzzy-FPSO is 0.025, HIDS is 0.031, SVM-IDS is 0.041, and IIDPS is 0.039. Likewise, the delay, at simulation time 50 sec, for Fuzzy-FPSO is 0.044, HIDS is 0.049, SVM-IDS is 0.063, and IIDPS is 0.059. In figure 6.c, the delay of the schemes for selective packet drop attack, at simulation time 10 sec, for Fuzzy-FPSO is 0.025, HIDS is 0.034, SVM-IDS is 0.038, and IIDPS is 0.041. Correspondingly, the delay at simulation time 50 sec, for Fuzzy-FPSO is 0.044, HIDS is 0.049, SVM-IDS is 0.059, and IIDPS is 0.058. In figure 6.d, the delay of without attack case, for different schemes, at simulation time 10 sec, for Fuzzy-FPSO is 0.014, HIDS is 0.019, SVM-IDS is 0.025, and IIDPS is 0.033. Similarly, the delay at simulation time 50 sec, for Fuzzy-FPSO is 0.029, HIDS is 0.031, SVM-IDS is 0.052, and IIDPS is 0.051. The yielded delay measure conveys that the delay increases with the increasing simulation time. In all the four cases, the proposed Fuzzy-FPSO has the minimum delay compared to the other three schemes summarizing the effectiveness of the proposed scheme.

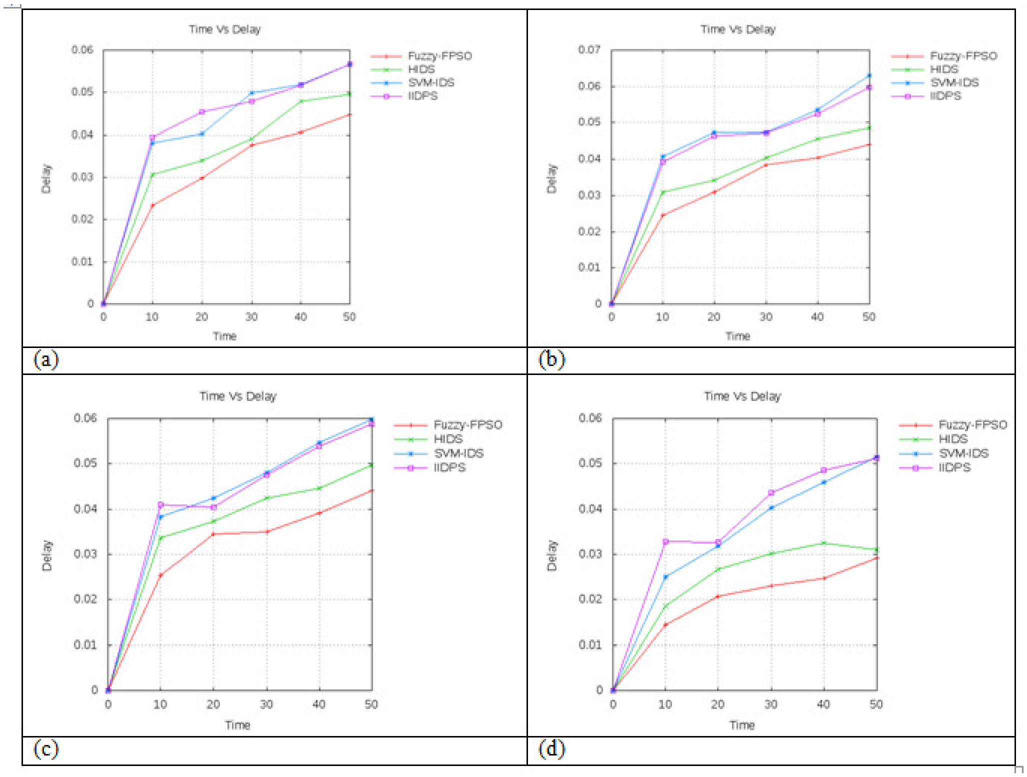
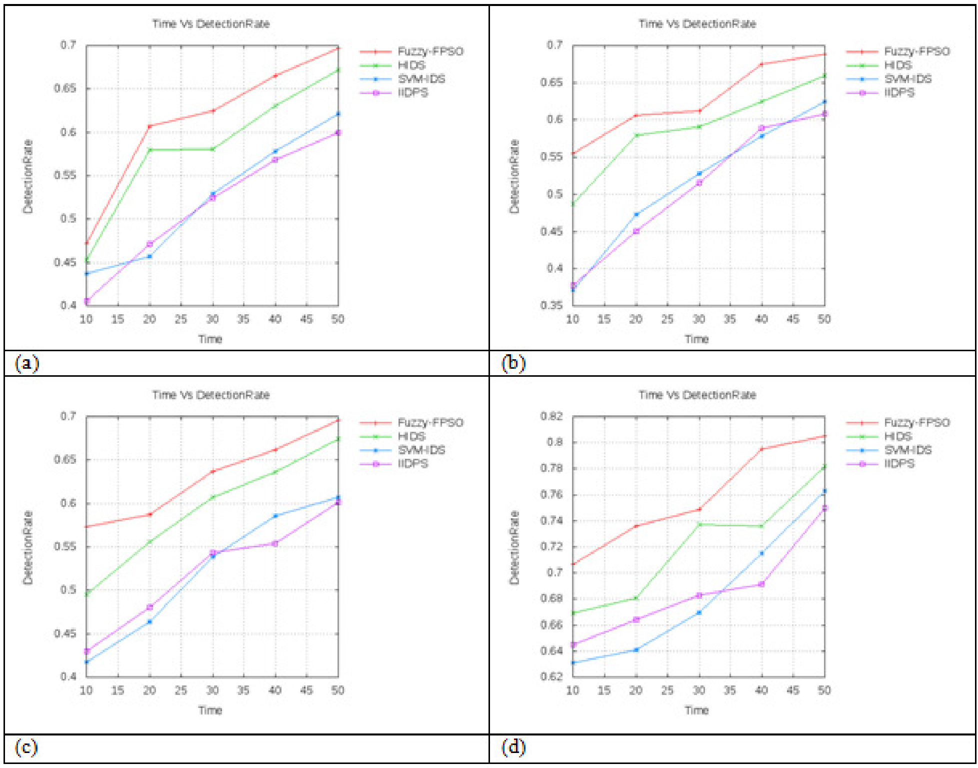


Figure 6. Comparative analysis plot of delay for (a) Black Hole attack, (b) Flooding attack, (c) Selective Packet Dropping attack and (d) without attack.

5.4.3 Analysis Based On Detection Rate

The comparative analysis of detection rate is carried out concerning simulation time for black hole attack, flooding attack, selective packet dropping attack and without attack is pictured in figure.7. In figure 7.a, the detection rate of the methodologies with black hole attack at simulation time as 10 sec, for Fuzzy-FPSO is 0.472, HIDS is 0.453, SVM-IDS is 0.437, and IIDPS is 0.406. Correspondingly, the detection rate at simulation time 50 sec, for Fuzzy-FPSO is 0.697, HIDS is 0.672, SVM-IDS is 0.621, and IIDPS is 0.6. In figure 7.b, the detection rate of the approaches for flooding attack at simulation time 10 sec, for Fuzzy-FPSO is 0.555, HIDS is 0.487, SVM-IDS is 0.371, and IIDPS is 0.378. Likewise, the detection rate, at simulation time 50 sec, for Fuzzy-FPSO is 0.688, HIDS is 0.659, SVM-IDS is 0.625, and IIDPS is 0.608. In figure 7.c, the detection rate of the schemes, for selective packet drop attack, at simulation time 10 sec, for Fuzzy-FPSO is 0.573, HIDS is 0.495, SVM-IDS is 0.417, and IIDPS is 0.430. Correspondingly, the detection rate, at simulation time 50sec, for Fuzzy-FPSO is 0.696, HIDS is 0.674, SVM-IDS is 0.607, and IIDPS is 0.601. In figure 7.d, the detection rate for without attack case in different schemes at simulation time 10 sec, for Fuzzy-FPSO is 0.707, HIDS is 0.669, SVM-IDS is 0.631, and IIDPS is 0.645. Similarly, the detection rate at simulation time 50 sec, for Fuzzy-FPSO is 0.805, HIDS is 0.782, SVM-IDS is 0.763, and IIDPS is 0.750. The determined detection rate measure reveals the fact that the detection rate increases with the increase in simulation time. And the maximum detection rate is achieved by the proposed Fuzzy-FPSO in comparison with the other existing approaches justifying the proposed scheme as a productive one.



(a)

(b)

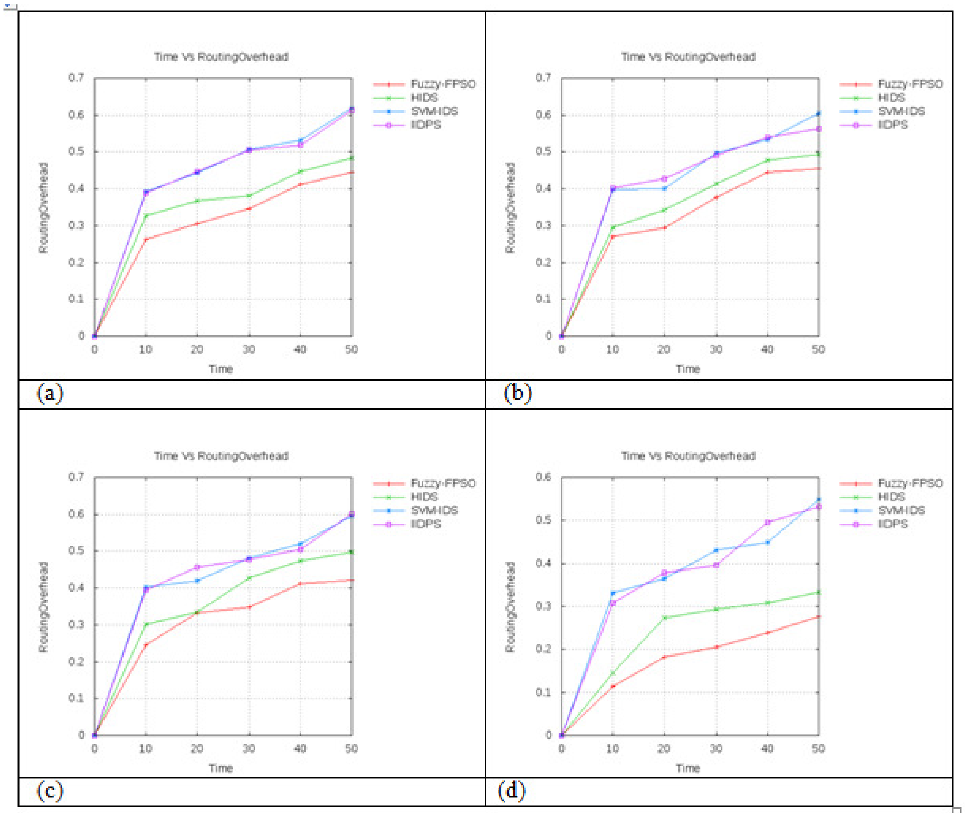
(c)

(d)

Figure 7. Comparative analysis plot of detection rate for (a) Black Hole attack, (b) Flooding attack, (c) Selective Packet Dropping attack and (d) without attack.

5.4.4 Analysis Based On Routing Overhead

The comparative analysis of routing overhead plotted against the simulation time for the four cases, such as black hole attack, flooding attack, selective packet dropping attack and without attack is depicted in Figure.8. Figure 8.a shows the routing overhead of the schemes for black hole attack at simulation time 0, 10, 20, 30, 40, and 50 sec. At simulation time of 10 sec, the routing overhead of Fuzzy-FPSO is 0.26376, HIDS is 0.32585, SVM-IDS is 0.39176, and IIDPS is 0.38773. Similarly, the routing overhead at simulation time 50 sec for Fuzzy-FPSO is 0.44468, HIDS is 0.48398, SVM-IDS is 0.61945, and IIDPS is 0.61384. Figure 8.b shows the routing overhead of the schemes for flooding attack at simulation time 0, 10, 20, 30, 40, and 50 sec. At simulation time of 10 sec, the routing overhead of the Fuzzy-FPSO is 0.27128, HIDS is 0.29508, SVM-IDS is 0.39832, and IIDPS is 0.40236. Likewise, the routing overhead, at simulation time 50 sec, for Fuzzy-FPSO is 0.45453, HIDS is 0.49319, SVM-IDS is 0.60460, and IIDPS is 0.56270. Figure 8.c shows the routing overhead of the schemes for selective packet drop attack at simulation time 0, 10, 20, 30, 40, and 50 sec. At simulation time of 10 sec, the routing overhead of the Fuzzy-FPSO is 0.24550, HIDS is 0.30169, SVM-IDS is 0.40317, and IIDPS is 0.39508. Correspondingly, the routing overhead at simulation time 50 sec, for Fuzzy-FPSO is 0.42143, HIDS is 0.49683, SVM-IDS is 0.59616, and IIDPS is 0.60166. Figure 8.d shows the routing overhead of schemes without attack case at simulation time 0, 10, 20, 30, 40, and 50 sec. In all the four cases, the proposed Fuzzy-FPSO has the minimum routing overhead compared to the other three schemes summarizing the effectiveness of the proposed scheme.



(a) (b) (c) (d)

Figure 8. Comparative analysis plot of routing overhead for (a) Black Hole attack, (b) Flooding attack, (c) Selective Packet Dropping attack and (d) without attack.

5.5 Discussion

A comparative discussion of the proposed scheme with the existing scheme considering the three evaluation metrics is made and shown in the below Table.2.

Table 2. Performance comparison of Fuzzy- FPSO with other existing schemes

Evaluation Metrics	Attacks	Methodology			
		Proposed Fuzzy-FPSO	HIDS	SVM-IDS	IIDPS
Throughput	Black hole Attack	0.634	0.590	0.520	0.543
	Flooding	0.627	0.575	0.523	0.559
	Selective Packet Drop	0.626	0.588	0.527	0.508
	Without attack	0.762	0.737	0.668	0.684
Delay	Black hole Attack	0.044	0.049	0.057	0.057
	Flooding	0.044	0.049	0.063	0.059
	Selective Packet Drop	0.044	0.049	0.059	0.058
	Without attack	0.029	0.031	0.052	0.051
Detection Rate	Black hole Attack	0.697	0.672	0.621	0.600
	Flooding	0.688	0.659	0.625	0.608
	Selective Packet Drop	0.696	0.674	0.607	0.601
	Without attack	0.805	0.782	0.763	0.750
Routing Overhead	Black hole Attack	0.264	0.326	0.312	0.388
	Flooding	0.271	0.295	0.398	0.402
	Selective Packet Drop	0.246	0.302	0.403	0.395
	Without attack	0.115	0.145	0.331	0.308

The simulation results justify that the proposed scheme has the enhanced performance over the existing HIDS, SVM-IDS, IIDPS schemes with maximum throughput, minimum delay and maximum detection rate.

6. CONCLUSION

This research work contemplates to develop an IDPS for the threats in MANET by the reinforcement of trust management and based on the proposed Fuzzy-FPSO detection algorithm. All the secured feasible paths from source node to destination node are discovered based on trust computation, and the optimal path is chosen by employing the proposed FPSO having trust and distance as its objective function. The proposed scheme is implemented in a NS2 simulator, and the performance is evaluated in terms of the four evaluation metrics, like throughput, delay, detection rate and routing overhead. The three major attacks considered for performance evaluation are flooding attack, selective packet dropping attack and black hole attack. The simulation results of the proposed Fuzzy-FPSO provides the maximum throughput and detection rate along with minimized delay and minimum routing overhead on contrasting with the existing approaches like HIDS, SVM-IDS, and IIDPS.

REFERENCES

[1] M. Nekovee, and R. S. Saksena,“Simulations of large-scale Wi-Fi-based wireless networks,” Interdisciplinary challenges and applications, Future Generation Computer Systems, vol. 26, no. 3, pp. 514–520, 2010.

[2] Poonam Joshi, Pooja Nande, Ashwini Pawar, Pooja Shinde, and Rupali Umbare, "EAACK-A Secure Intrusion Detection And Prevention System For MANETS," in proceedings of IEEE International Conference on Pervasive Computing (ICPC), pp. 1-6, 2015.

[3] Babu, M. Rajesh, and G. Usha, "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.

[4] arrukh Aslam Khan, Muhammad Imran, Haider Abbas, and Muhammad Hanif Durad, "A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks," Future Generation Computer Systems, vol. 68, pp. 416-427, 2017

[5] 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.

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

[7] Usha, G., M. Rajesh Babu, and S. Saravana Kumar, "Dynamic anomaly detection using cross layer security in MANET," Computers & Electrical Engineering, pp.1-11, 2016.

[8] Erfan A Shams, and Ahmet Rizaner, "A Novel Support Vector Machine Based Intrusion Detection System For Mobile Ad Hoc Networks," Wireless Networks, pp. 1-9, 2017.

[9] Nadeem, Adnan, and Michael P. Howarth, "A survey of MANET intrusion detection & prevention approaches for network layer attacks," IEEE communications surveys & tutorials, vol. 15, no. 4, pp. 2027-2045, 2013.

[10] Opinder Singh, Jatinder Singh, and Ravinder Singh, "An Intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks against Malicious Nodes," Indian Journal of Science and Technology, vol. 8, no. 1, pp. 1-12, 2017.

[11] Hamed Janzadeh, Kaveh Fayazbakhsh, Mehdi Dehghan, and Mehran S. Fallah, ”A secure credit-based cooperation stimulating mechanism for MANETs using hash chains,” Future Generation Computer Systems, vol. 25, no. 8, pp. 926-934, 2009.

[12] Soni M, Ahirwa M, and Aggarwal S, “A Survey on Intrusion Detection in MANET,” in proceedings of International Conference on Computational Intelligence and Communication Networks, pp. 1027-1032, 2015.

[13] Djahel S, Farid N, and Zhang Z, “Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges,” IEEE communications surveys and tutorials, vol. 13, no. 4, pp. 658-672, 2011

[14] H. Debar, M. Dacier and A.Wespi, “A Revised Taxonomy for Intrusion Detection Systems,” Annals of Telecommunications, Vol.55, No.7, pp 361-378, July 2000.

[15] Adnan Nadeem, and Michael Howarth, "A generalized intrusion detection and prevention mechanism for securing MANETs," in proceedings of ICUMT09 International Conference on Ultra Modern Telecommunications and Workshops, pp. 1-6, 2009.

[16] 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, Article ID 284276, pp. 1-9, 2015.

[17] Vikas Gupta , Ashok Verma, Ajay Lala and Ashish Chaurasia, "Scenario Based Performance and Comparative Simulation Analysis of Routing Protocols in MANET," IJCSNS International Journal of Computer Science and Network Security, Vol.13, No.6, June 2013.

[18] 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

[19] A. Sharma and P.K. Johari, "Eliminating Collaborative Black-hole Attack by Using Fuzzy Logic in Mobile Ad-hoc Network,” International Journal of Computer Sciences and Engineering, Vol.5, No.5, pp. 2347-2693, May 2017.

[20] Mohammed Abdel-Azim, Hossam El-Din Salah and Menas Ibrahim, "Black Hole attack Detection using Fuzzy based IDS," International Journal of Communication Networks and Information Security (IJCNIS), Vol.9, No.2, August 2017.

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

[22] Xin-She Yang, "Firefly Algorithm, Nature-Inspired Metaheuristic Algorithms," Computers, Luniver Press, pp.79–90, 2008.

[23] Dongshu Wang, Dapei Tan and Lei Liu, "Particle Swarm Optimization Algorithm: An overview," Soft Computing, pp.1–22, January 2017.

[24] Dian Palupi Rini, Siti Mariyam Shamsuddin and Siti Sophiyati Yuhaniz, "Particle Swarm Optimization: Technique, System and Challenges," International Journal of Computer Applications, Vol.14, No.1, January 2011.

[25] Mahmood K. Ibrahem , Ameer M. Aboud, "A Secure Routing Protocol for MANET," International Journal of Computer Science Engineering and Technology(IJCSET), Vol.4, No.7, July 2014.

[26] Nisha Soms and P.Malathi, "Evolution of Intrusion Detection System in MANETs – A Survey," International Journal of Innovations & Advancement in Computer Science(IJIACS), Vol.6, No.5, May 2017.

AUTHORS

Mr.Ramireddy Kondaiah received his B.Sc Degree in Mathematics, Physics and Chemistry from Sri Venkateswara University,Tirupti, A.P , India in 1996, Master of Computer Applications from Sri Krishna Devaraya University Campus College affiliated to Sri Krishna Devaraya University in 2000.Now He is pursuing Ph.D. from Rayalaseema University,Kurnool ,AndhraPradesh,India. His research areas Include Computer Networks/MANET Routing with Intrusion Detection.

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.