MEDWIN PUBLISHERS
Committed to Create Value for Researchers

International Journal of Forensic Sciences
ISSN: 2573-1734

Improved Intrusion Detection and Response System for Wireless Sensor Network

Kathirvel A* and Subramaniam M

Department of Computer Science and Engineering, SRM Institute of Science and Technology, India

***Corresponding author:** Professor Kathirvel A, Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani campus, Chennai, India, Email: kathirva@srmist.edu.in; ayyakathir@gmail.com

Review Article

Volume 5 Issue 4

Received Date: September 29, 2020

Published Date: November 02, 2020

DOI: 10.23880/ijfsc-16000203

Abstract

Wireless sensor network (WSN) is highly sophisticated than ad hoc wireless network. Ad hoc wireless network is mostly affected by different resources such as high processing energy, storage capabilities and battery backup and etc. Due to the open nature, poor infrastructure, quick deployment practices, and the conflict environments, make them susceptible to a wide range of attacks. Recently, the network attack affects the performance of networks such as network lifetime, throughput, delay, energy consumption, and packet loss. The conventional security mechanisms like intrusion detection system (IDS) of network security are not enough for these networks. In this thesis, we introduce an enhanced intrusion detection and response (EIDR) system using two tire processes. The first contribution of proposed EIDR system is optimal cluster formation and performed by the chaotic ant optimization (CAO) algorithm. The second contribution is to calculate the trust value of each sensor node using the multi objective differential evolution (MODE) algorithm. The computed trust value is used to design the intrusion response action (IRA) system, which offers additional functions and exhibit multiple characteristics of response to mitigate intrusion impacts. The simulation results display that the proposed EIDR system has a better detection rate and false positive rate without affecting network performance.

Keywords: WSN; EIDR; CAO; MODE; IRA; IDS

Abbreviations: Wireless Sensor Network; Enhanced Intrusion Detection and Response; Chaotic Ant Optimization; Multi Objective Differential Evolution; Intrusion Response Action; Intrusion Detection System.

Introduction

WSNs are distributed volatile sensors to monitor the physical or environmental conditions like temperature, pressure, sound and synchronize their data with the network. Due to the continued development of wireless sensor networks, the need for more effective security mechanisms is also increasing. The security issues of the sensor network should be addressed by the beginning of the design of the system because the sensor networks interact with sensitive data and generally work in hostile unpredictable environments. Wireless Sensor Network requires a detailed understanding of the capabilities and limitations of each basic technology for secure work. At each end of the WSN, the design should be designed to provide the main sources of synchronization of the combined topology package, which is strict energy consumption. The protection of the connection to the group that requires the delivery of packages from one or more of the senders is a major objective [1-3].

An intrusion detection system (IDS) attempts to detect

[4] insecure conditions of networks due to the malicious attacks. Intrusion is a set of events that can lead to unofficial access or change of wireless networking system. IDS methods can detect cruel intruders from those anomalies and to monitor the system's behavior, to identify the existing intrusions in the network, and to alert the users after the intrusion has been identified, to re-enter the network if this is possible [5]. Generally, the neighbors of a malicious node are the first to learn those abnormal behaviors. Therefore, it is easy to let every node control its neighbors in such a way that the IDS mechanism can be activated as soon as possible [6]. IDS observe and analyze the maximum security problems in the network system, track unusual events and it is used to monitor the network. The principal approaches for IDS are classified into two: misuse detection and anomaly detection. Misuse detection technique compares the behavior observed with known attack signatures. Action patterns that cause security threats should be defined and stored in the system. The advantage of this technique is that it can detect instances of known attacks accurately and efficiently, but it does not have the ability to detect unknown type of attack [6]. Anomaly detection [7] is based on the general behavior of a system and it compares normal activities against the events observed for identifying important deviations.

In recent years, many IDS are proposed for WSN. IDS employed as a second line of defense are mandatory to provide a high security information system and it can effectively identify intruders and thus provides intensive security [8]. The intrusion detection models are single-sensing detection and multi-sensing identification used to detect intrusion in both homogeneous and heterogeneous WSN by showing the probability of intrusion detection with distance and network parameters [9].

An enhanced intrusion detection and response (EIDR) system is proposed using two tier processes are optimal clustering and trust computation. The IDS module classifies the type of malicious present in the network and the IRS module is responsible to make the response action of particular malicious problem in data transmission path. The main objective is to maximize the detection rate and minimize false positive rate without affecting the network performance such as network lifetime, throughput, end-to-end delay, energy consumption, and packet loss.

The remainder of the paper is organized as follows. Above Section briefly reviews the recent papers related to our contributions. In Section 2, problem methodology of IDS system and system model of proposed solution is presented. The brief discussion of proposed EIDR system is given in Section 3 with proper mathematical models. The simulation results are analyzed in Section 4. Finally, the paper concludes in Section 5.

Problem Methodology and Network Model

Problem Methodology

Security is a key issue for each and every one of the structures of affiliation and foundations at the present time and each and every one of the checks are attempting in ways that actuating access to the data design of these affiliations. IDS is an inside and out new advancement of the structures for dangerous unmistakable assertion procedures that have made starting late. The run some bit of IDS is to help PC structures with planning and deal with the framework ambushes. Interference ask for limits wires checking and executing both customer and structure works out, withdrawing system setups and vulnerabilities, looking over structure and record unfaltering quality, ability to see plans ordinary of ambushes, examination of atypical change cases and following customer procedure encroachment. The goal of impedance zone is to screen manage focal obsessions for see sporadic lead and abuse in regulate. Jin, et al. [10] has proposed IDS using a multi-agent system and a node trust value (MTID). The multi-official display structure is made in both the bundle heads and standard sensor centers to perform impediment unmistakable proof. Customary obsession point trust properties are delineated and pull back hypothesis is used to judge whether these characteristics are standard.

Starting late, by far most of the IDS are secured to arranging layer essentially, regardless it can be moved to see aggregated sorts of strikes at different structures association layers as well [1-9,11-21]. Two or three sees just interference and some achieve more like getting more information e.g. sort of ambushes, regions of the gatecrasher et cetera. Regardless of the way that a partner with number of IDS instruments are used yet not an enormous measure of them can be fitting for WSN with their slant slants [22]. From existing works Han, et al., Lin, et al., Pintea, et al., Huang, et al., Zhang, et al., Mrugala, et al., Sedjelmaci, et al., Guo, et al., Santoro, et al., Alsaedi, et al., Jin, et al. [23-32,10], IDS are not speaking to shield WSN from Inside and Outside aggressors. None of them are done case most by a wide edge of the strategies offer social affair frameworks without picking how they will be kept and by what procedure will they continue with rest of the structure. In context of their open nature and nonattendance of structure, security for WSNs has changed into a confounding issue than the security in various frameworks. The standard security frameworks of guaranteeing wired structure are not appealing for these structures. Thus, proposed EIDR system overcome those problems by two tire process such as clustering and trust evolution. The main contribution of proposed EIDR system is summarized as follows:

1. In EIDR system, the chaotic ant optimization (CAO) algorithm is used to form the cluster using the sensor

node constraints such as position and velocity, which provides stable and energy efficient clusters.

2. The multi objective differential evolution (MODE) algorithm is used to compute the trust of each sensor node, which used to make routing between source-destination with the help of basic low-energy adaptive clustering hierarchy (LEACH) protocol. Then, perform IRA using the computed trust value with the actions are no punishment (NP), punishment (P) and isolation (I).
3. The proposed EIDR system is tested with high density nodes in network simulator (NS-2) with three different network attacks are selective forwarding, denial of service (DoS) and flooding attacks.

Network Model

In EIDR system, we assume network consists of randomly distributed high density nodes and malicious nodes without movement. The sensors present in the network have same transmission range and unique ID for user identification. The routing pattern is followed by the basic LEACH protocol with the help of our computed trust values. That is to say, the sensed information's from each sensor are forward to next node that is selected by trust value.

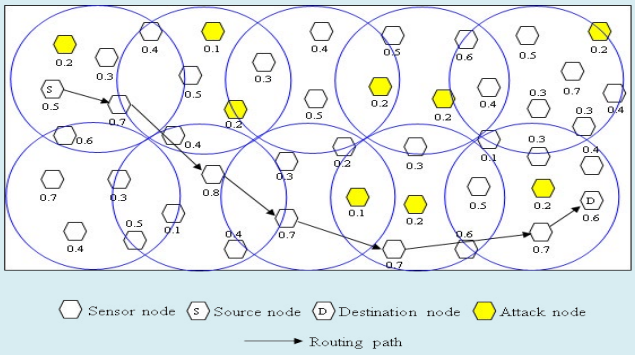

Figure 1: EIDR systems with example trust values and attacks.

The routing implies that nodes only directly communicate with their highest trust neighbor nodes. Also, the information's forwarded between neighbor nodes are depends on the trust value, which cannot only transfer the packets from source nodes to destination nodes, but also process the packets based on specific requirements. The assumed network model of proposed EIDR system is shown in Figure 1 with example trust values and attacks.

Enhanced Intrusion Detection and Response System

The IDS used to detect the attacks. Even if the system cannot prevent the attacks from getting into the network, noticing the intrusion will provide the security officer with valuable information. The detailed description of proposed Enhanced Intrusion Detection and Response (EIDR) system is present in the following section. EIDR consists of two algorithms namely clustering using CAO (Chaotic Ant Optimization) algorithm and Trust computation using MODE (Multi Objective Differential Evolution) algorithm.

Clustering using Chaotic Ant Optimization (CAO) Algorithm

Deif and Gadallah [22] proposed Ant colony optimization (ACO) is a metaheuristic figuring for combinatorial change issues. The key idea of ACO figuring is the mix of from the earlier data about the structure of a promising plan with a posteriori data about the structure of formally got staggering systems. Metaheuristic estimation are checks which, with a specific common made obsession to escape from neighborhood optima, drive some enormous heuristic: either a central heuristic begin from an invalid method and adding bits to store up an OK entire one, or a near to ask for heuristic begin from a total approach and iteratively changing some of its parts to accomplish a typical one. The metaheuristic part interfaces with the low-level heuristic to secure plans superior to anything those it could have accomplished alone, paying little regard to whether iterated. The controlling piece is pro either by influencing or by randomizing the philosophy of close neighbor answers for considers in neighborhood look or by joining parts taken by various structures. The standard key thought, everything considered began by the lead of veritable ants, is that of a parallel range for after in excess of a not a lot of computational strings in setting of neighborhood issue information and on a dynamic memory structure containing data on the probability of early got result. The aggregate direct moving out of the relationship of the specific demand strings has shown standard in controlling combinatorial streamlining issues.

Here, the central ACO computation is invigorated by chaotic manner i.e. chaotic ant optimization (CAO) count to make best faultless squeezing. Exactly when ants see assistance, they attempt to keep up a proportionate edge with the light to fly in straight line. Here, the game-plan of ants is tended to in a structure. For each and every one of the ants, there is a get-together to secure the looking regards. The second parts in the estimation are foods tended to in a structure F, and a social gathering for securing the looking regards. The CAO algorithm starts with the initialization process, which approximates the global optimal of the optimization problems and defined as follows:

$$MFO = (P, S, T) \quad (1)$$

Where P represents the function of random population $P \to \{X, X_a\}$, S represents the moth's movement around search space $S \to X$, T represents the termination criteria $T \to \{\text{True}, \text{False}\}$. After the instatement, S function is iteratively keeping running until the T point that the minute that the cutoff returns outstanding kept. For the refinement in reflecting the direct of ants, the condition of every underground offensive irrelevant creature restored concerning sustenance as takes after:

$$X_i = s(X_i, F_i) \quad (2)$$

Where s represents the spiral function, i and j represents the i-th moth, j-th food respectively. Spiral's initial point should begin from the underground bug and end at the last point ought to be the condition of the sustenance. Change of the level of winding pound the intrigue space. A logarithmic spiral is defined for the CAO algorithm as follows:

$$s(X_i, F_i) = \left|F_j - M_i\right| e^b \cos(2\pi r) + F_j \quad (3)$$

Where $\left|F_j - M_i\right|$ indicates the distance of the i-th ant for the j-th food, b, r represents the shape of the logarithmic spiral, and random number respectively. From this condition, the running with position of an underground bug is portrayed concerning a help. The parameter in the winding condition depicts how much the running with position of the moth ought to be near the sustenance. With a specific extraordinary obsession to collect the sensible approach of individuals against troublesome joining and enable the mixing speed, we enhance the CAO check by the Levy-flight. It has the unmistakable properties to cover away the not dazzling get-together of masses, innovatively, which can make this appropriately ricochet out of the zone wrap up. The new position of ants is updated as follows:

$$X_i^2 = X_i^1 + u \; sign\left[r - 0.5\right] \oplus \text{Levy}(\ddot{\text{I}}) \quad (4)$$

Where t, u is a random parameter which conforms to a uniform distribution, $sign\left[r - 0.5\right]$ is take as 1, 0, and −1.

Levy-flights are a kind of random walk in which the steps are determined by the step lengths, and the jumps conform to a Levy distribution as follows.

$$\text{Levy}(\ddot{\text{I}}) \approx \frac{\left[\dfrac{\Gamma(1+O) \times \sin\left(\pi \times O/2\right)}{\Gamma\left(\left((1+O)/2\right) \times O \times 2^{(O-1)/2}\right)}\right]^{1/O}}{|\nu|^{1/O}} \times \mu \quad (5)$$

Where μ, ν represents the standard normal distributions, $\text{O} = 0.5$, Γ represents the standard Gamma function. To show up, global search cutoff of this figuring upheld utilizing remarkable stroll around Levy-flight, it is being gotten in neighborhood smallest is adjusted, and it to the degree anyone knows gives more triumphs especially to strike and multimodal benchmark limits. The planning improvement of proposed CAO estimation is given in Algorithm-1.

Input: X← population size, F← number of design variables, termination criterion **Output:** cluster formation	
1	Initialize the position and distance of populations.
2	Compute initial solution using equation (3), and identify best and worst solution in the population.
3	Modify the population solution using equation (4).
4	Update the new solution if is better than old, otherwise maintain old one.
5	Stop the process if termination reached.
6	**Return:** Cluster formation

Algorithm 1: Cluster formation using CAO algorithm.

Trust Computation using Multi Objective Differential Evolution (MODE) Algorithm

Differential evolution (DE) algorithm [23] is branch of transformative program for reestablish issues over pleasing spaces. The upsides of DE are its sensible structure, solace, speed and power. DE is striking harm from other fundamental effect suggests coordinating issues with the colossal encircled to respected domains. DE is a procedure contraption of gigantic utility that is in an inconsequential minute open for satisfying applications. DE has been utilized as a touch of two or three science and building applications to find influencing reactions for sensibly unmanageable issues without join as one with star information or complex strategy estimations. In the event that a structure is obliging to being continually analyzed, DE can give the best way to deal with oversee manage sort out expelling the best execution from it. DE utilizes change as a demand structure and choice to amass the power toward oversaw regions in the possible locale. Here, to vivify the consistent DE figuring by multi-objective DE (MODE) estimation utilizing the moving focuses, for example, criticalness utilize, got hail quality, administer lifetime and stop up rate. The detailed description of each constraint as follows.

Energy Model: The way that most energy models considered are made in light of estimations made on utilitarian liberal fixations, and these models change just to the parts used as a touch of the executed contraption setup and working rely on that kind of focuses, these models are not traditionalist, and can be used only for reenactment and evaluation of sensor pack for which they were made. For WSN applications are to an inconceivable degree collected, and possible applications

are unending, so it is crucial to execute a general enormity appear, nonexclusive and all the more little. The monstrosity use amidst conditions of rest and dynamic states can be intervened after some time. For a node to operate autonomously sense the average energy scavenged must be greater than or equal to the energy consumed by the node. The average energy (E_a) consumption defined as follows:

$$E_a = n T_a P_a + m T_s P_s \quad (6)$$

Where P_a is the power consumed by the node in its active state during T_a and n is the rate of occurrence, and P_s that is the power consumed by the node in its inactive state and has the occurrence rate m and lasts for a period equal to T_s . Given the diversity of energy collection methods, and the wide range of application profiles it is not possible to create a generic model, however, the essential criterion is that the energy stored (E_s) in the node must be at least equal with the energy used for its operation in the time interval $T_2 - T_1$.

$$E_s = \int_{T_1}^{T_2} (P_c - P_s)dt \quad (7)$$

Where P_c the power is consumed by the sensory node in the time interval $T_2 - T$ and P_s is the power collected and stored power in the same timeline. General working of sensor bases expected a particular power supply, which for the periods in which handset and sensor are not utilized, when they are either wrapped up by electronic switches, or set into rest state, it is in a perfect world to be set to affect a lower to yield voltage through part vapor sorption system in light of the way that the criticalness sound judgment of the microcontroller will increment amidst these seasons of rest states. The total energy consumed by sensor node will be represented as follows:

$$E_{node} = \sum_{k=0}^{T} \frac{E_{\mu c}(t) + E_{trns}(t) + E_{sns}(t)}{E_{\eta_{DC-DC}}} \quad (8)$$

Where $E_{\mu c}(t)$, $E_{trns}(t)$, $E_{sns}(t)$, and $E_{\eta_{DC-DC}}$ is the energy consumption due to control unit, communication unit, sensor unit, and DC-DC converter respectively.

Received Signal Strength: The received signal strength represents the most major and the basic metric to assess the bit between the sensor living spaces for the restriction objectives. In the got flag quality based block structures, the signal strength received at the sensor focus point is mapped into divisions by systems for certain channel show up. The received power (P_R) at the sensor nodes employing the log normal shadowing model is represented as follows:

$$P_R = P_T - 10 \log P_{Loss}\left(\frac{r}{r_0}\right) + \delta \quad (9)$$

The mathematical equation for the path loss function evaluated and expressed in decibel is represented as follows:

$$P_{Loss}(dB) = \overline{P_{Loss}}(r_o)(dB) + 10\gamma \log_{10}\left(\frac{r}{r_o}\right) + \delta(dB) \quad (10)$$

Where r is the distance between sending and receiving nodes, r_o denotes the near earth reference distance γ corresponds to the path loss index δ signifies the zero-mean Gaussian random noise. The path loss function represented in terms of the transmitter and receiver is furnished by as follows:

$$P_{Loss}(dB) = 10 \log\left(\frac{P_T}{P_R}\right) \quad (11)$$

Where P_T and P_R denotes the transmitted and receiver signal power respectively. The value of path loss index is invariably dependent on the environment or the transmission scenario. The distance r_o is considered as one meter for the sake of easy evaluation. The basic edition of equation (10) may be expressed with respect to the received power as follows:

$$\left[\frac{P_R(r_o)}{\overline{P_R}(r)}\right] = \left[\frac{r}{r_0}\right]^{\gamma} + \delta \quad (12)$$

Network Lifetime: The network lifetime (NL) is the weighted whole of whatever is left of the lifetime of individual sensors of the baffling number of sensors in the sensor plot. The straggling stays of the lifetime of individual sensor is depicted as the made holding up criticalness out of the sensor at minute. In the preparing of the sensor manage, the centrality is depleted when the sensor gets or passes on something specific. By uprightness of the wobbly remote correspondence in WSN, the bundle might be retransmitted to ensure the right transport. The criticalness of each inside and their condition in like way used to pick remaining lifetime of the entire sensor make. We consider the straggling bits of the lifetime of the entire sensor regulate as the aggregate of the weighted extra lifetime of all sensors in the sensor network. Thus, the remaining lifetime of the whole sensor network (NL) as follows:

$$NL = \sum_{y=1}^{n} w_y L(y) \quad (13)$$

Where W_y represents the weight factor of each sensor node counts. Weight factor is the nearer the sensor to the CH, the more important it is. The weight of each sensor represented by,

$$w_y = c \frac{1}{d_{s-bs}^2} \quad (14)$$

Where c represents the constant. The weighted sum of remaining lifetime of individual sensors computed as follows:

$$N = \max\left(1 - \sum_{y=0}^{n}\left(E_{node} - P_R\right)\right) \quad (15)$$

Congestion Rate: The congestion rate (CR) is utilized to study the store of sensor focus. Every wide enchanting fixation can adaptively watch the event of cripple and a short cross later impact the parent focuses to reduce the bundle transport rate as appeared by the blockage level. The bare rate of each node is calculated as follows:

$$R = v_i = \frac{\sum_{i=1}^{N} P\left(P_i\right) - P\left(P_i\right)}{\sum_{i=1}^{N} P\left(P_i\right)} \quad (16)$$

Where the bare rate of the node i is v_i and $V = \{v_i, 1 \le i \le m\}$; $P\left(P_i\right)$ is the node importance index, which computes a quantitative indicator. It can be defined as,

$$P\left(P_i\right) = \sum_{n_i \in L_j^m} C\left(n_i\right) \quad (17)$$

Where $C\left(n_i\right)$ represents the connectivity degree describes how close the node is to neighbors. A coverage probability to represent the connectivity degree and obtained as,

$$C\left(n_i\right) = \left|\sigma_j\left(n_k\right)\right| \quad (18)$$

Where $\sigma_{ij}\left(n_k\right)$ represents the edge number from n_i to n_k on node L_{ij} .

MODE depends on individuals and goes for overhauling general multi-specific motivations driving limitation. It utilizes the change manager as to give the trading of data among a few blueprints. It utilizes three developmental parameters and significant errands, for example, increment, subtraction, examination, and its execution is proportionate or even beats other transformative or heuristic estimations. The immediate purpose of joining of MODE is to registers the general immaculate of a most pivotal over eager space. In particular, and without loss of generality, this problem can be reduced to finding the minimum of a function:

$$\text{minimize } f\left(r\right) = f\left(r_1, r_2, \ldots, r_n\right) \quad (19)$$

Where n is D dimensional vector and f is a real function of real-valued arguments.

Differential evolution algorithm requires just three parameters, for example, mutt and change sharpens that are everything seen as continued, scaling some piece of the refinement of two people and masses size to make the developmental technique for D-dimensional issue. The check begins with introduction process considering parameter respects that are particularly scattered between the pre-shown disengage down beginning parameter bound $r_{n,low}$ and the upper initial parameter bound $r_{n,high}$ as follows:

$$r_{n,m} = r_{n,low} + rand\left(0,1\right) \cdot \left(r_{n,high} - r_{n,low}\right) \qquad n = 1,2,\ldots D; m = 1,2,\ldots N_p$$

(20)

In order to generate a trial vector, first changes the objective vector $r_{n,tar}$, from the present individuals by including the scaled multifaceted nature of two vectors from the present masses with the mutant vector M_i . Records s_1 and s_2 are subjectively picked with the condition that they are surprising and have no relationship with the iota report by any structures (i.e. $s_1 \neq s_2 \neq n$). The change scale factor F is a positive superior to normal encompassed number, however a mind blowing bit of the time as could sensibly be common short of what one. The process of mutant vector generation is given as follows:

$$M_n = r_{tar} + F \cdot \left(r_{n,s_1} - r_{n,s_2}\right) \qquad s_1, s_2 \in \{1,2,\ldots N_p\}$$

(21)

In order to increase the diversity of the parameter vector, the crossover operation is applied to the mutant vector M_n and the original individuals $r_{n,m}$. The result is a trial vector $T_{n,m}$, which is computed as follows:

$$T_{n,m} = \begin{cases} M_{n,m} & \text{if } rand(0\ 1) \le R \\ r_{n,m} & \text{Otherwise} \end{cases} \quad (22)$$

The crossover parameter $\left(0 \le R \le 1\right)$ controls the bit of parameters that the mutant vector is adding to the last trial vector. In like way, the trial vector dependably gets the mutant vector parameter as appeared by the subjectively picked record. This MODE check is utilized to figure the trust in estimation of each inside point. Here, our devotion is to pick require level of each inside; the standard DE [33] performs just with two-dimensional factors yet MODE tally handle D-dimensional vectors and it can particularly sensible to figure confide in an enlivening power as important and perfect way.

Simulation Experiments

We use a simulation model based on NS2 in our evaluation. Our performance evaluations are based on the simulations of 200 wireless sensor nodes that form a wireless sensor network over a rectangular (1000×1000 m) flat space. The MAC layer protocol used in the simulations was the Distributed Coordination Function (DCF) of IEEE 802.11. The performance setting parameters are given in Table 1.

Property	Values
Simulation Time	600 seconds
Propagation Model	Two rays Ground Reflection
Antenna	Omni Antenna
Initial Energy	14.3
Transmission Energy	0.395
Receiving Energy	0.660
Traffic Type	CBR (UDP)
Payload Size	512 Bytes
Number of Flows	10 / 20 flows
Node Placement	Random
Transmission Range	200 meters
Radio Bandwidth	2 Mbps

Table 1: Parameter Settings.

Before the simulation we randomly selected a 40% of the network population as generic malicious behavior nodes. Each flow did not change its source and destination for the lifetime of a simulation run. We had kept the simulation time as 600s, so as to enable us to compare our results with that of ETUS.

Simulation studies have been done using NS2. We have carried out our focus attention on four parameters – packet delivery ratio, false negatives probability, false positives probability and control overhead when node density and percentage of malicious nodes vary. We have undergone two investigations namely investigations – I and investigations – II.

The performance evaluations for investigations – I are based on the simulations of 200 sensor nodes that form a WSN over a rectangular (1000 X 1000 m) flat space discussed in this section. Next section 4.2 discuss about investigations – II. Parameters setting are given in Table 6.

Investigations – I

Before the simulation we randomly selected a certain fraction, ranging from 0 % to 40 % of the network population as malicious nodes. We considered only two attacks – modifying the hop count and dropping packets. Each flow did not change its source and destination for the lifetime of a simulation run.

Throughput: In the world of MANET, packet delivery ratio has been accepted as a standard measure of throughput. Packet delivery ratio is nothing but a ratio between the numbers of packets received by the destinations to the number of packets sent by the sources. We present in Table 2 the packet delivery ratios of EIDR with node density varying between 50 to 200.

Node density	Percentage of Malicious nodes				
	0 %	10 %	20 %	30 %	40 %
50	99.48	99.59	99.58	99.48	90.54
75	99.16	99.48	97.41	96.45	83.44
100	98.38	98.60	95.91	96.15	78.42
150	97.19	97.77	93.95	93.24	72.64
200	97.40	95.96	93.44	91.33	65.57

Table 2: EIDR Throughput in varying node density.

From Table 2 and Table 3 the following conclusions can be drawn:

i. In general packet delivery ratio decreases as node density and percentage of malicious nodes increase.
ii. We find that EIDR yields a much higher packet delivery ratio compared to generic ETUS, IDSEM and ETUS in the presence of 40% malicious nodes. It is found that with EIDR, there is a higher packet delivery ratio ranging from 10.21% (ETUS, 50 node density) to 15.3 % (ETUS, 200 node density).

Failure to Deduct (False Negatives) Probability: False Negatives Probability can be defined as:

$$\text{False Negatives Probability} = \frac{\text{Number of malicious nodes left undetected } N_{LU}}{\text{Total number of malicious nodes } T_{MN}}$$

Table 3 Presents failure to deduct probability as a function of node density and percentage malicious nodes.

Node density	Percentage of Malicious nodes				
	0 %	10 %	20 %	30 %	40 %
50	0	0.0934	0.1415	0.1425	0.1598
75	0	0.0933	0.1215	0.1239	0.1047
100	0	0.0531	0.0517	0.0622	0.0630
150	0	0.0639	0.0724	0.0729	0.0737
200	0	0.0731	0.0839	0.0799	0.0841

Table 3: EIDR False Negatives in varying node density.

The above definition requires some elaboration. We can think of two groups of malicious nodes that are left undetected. In the first group are those nodes, which never played a part in the network operation; they were probably traveling along the boundaries and never had a chance to participate in the network activity.

Table 3 and Table 4 presents failure to detect probability as a function of node density and percentage of malicious nodes of generic ETUS, IDSEM and ETUS, respectively. We have calculated the failure to detect probability by taking into consideration only those nodes that took part in the network activity. Other researchers have also adopted the same approach. A false-negative probability, which is the chance that umpires fail to convict and isolate a malicious node, can be defined as the ration of the number of malicious nodes left undetected to the total number of malicious nodes. From Table 4, we can see that the false negative probability has decreased in EIDR compared to ETUS.

False Accusation (False Positives) Probability: False accusation probability (refer Table 4) is the chance that umpires incorrectly convict and isolate a legitimate node. In other words, this is the probability of wrongly booking innocent nodes. Table 5 presents false accusation probability as a function of node density and percentage of malicious nodes for EIDR and ETUS, respectively. We find a similar decrease in false accusation probability at all other combinations of malicious node percentages and node density values with ETUS. We find that false-positive probability increases with increasing percentage of malicious nodes and increased node density. We present a comparison of false- positive probability values between generic ETUS, IDSEM, EIDR and ETUS of 40% malicious nodes in Figure 5. It is seen that with EIDR, false-positive probabilities decrease slightly.

Node density	Percentage of Malicious nodes				
	0 %	10 %	20 %	30 %	40 %
50	0	0	0	0	0
75	0	0.0021	0.0057	0.0064	0.0078
100	0	0.0067	0.0104	0.0113	0.0311
150	0	0.0087	0.0216	0.0245	0.0438
200	0	0.0079	0.0381	0.0318	0.0471

Table 4: EIDR False Positives in varying node density.

Communication Overhead: In the Table 5, Communication overhead for EIDR is given below. Table 6 Communication overhead for GETUS, plain AODV, ETUS, IDSEM and EIDR in presence of 40 % of malicious nodes.

Node density	Percentage of Malicious nodes				
	0 %	10 %	20 %	30 %	40 %
50	12151	15137	18764	20274	22174
75	12357	15934	18969	20386	22889
100	12554	17835	20061	21395	23898
150	12947	18042	21172	21563	24889
200	13534	18069	21789	22984	25541

Table 5: EIDR Communication overhead in varying node density.

i. In general communication overhead increases as node density and percentage of malicious nodes increase.
ii. We find that EIDR yields a much lower communication overhead compared to generic ETUS, and ETUS in the presence of 40% malicious nodes as shown in Table 6. It is found that with EIDR, there is a lower communication overhead ranging from 18% (ETUS 50 node density) to 38.75% (ETUS 200 node density).

Investigations – II

In this section 4.2, we evaluate the performance of proposed an enhanced intrusion detection and response (EIDR) system and the network simulation (NS-2) results are compared with existing multi-agent trust-based intrusion detection (MITD) scheme.

Simulation Parameter and Setup: The proposed EIDR system is simulated by the NS-2 tool with the sensor nodes deployed in a 600m x 600m square region for 500 seconds simulation time. The simulated traffic source is Constant Bit Rate (CBR). The overall monitoring radius is 100 units distance, monitoring depth is 500 units distance. All sensor nodes have the same transmission range of 40 units distance. The initial energy of a sensor node is 104W. The energy cost to transmit one unit of data is 10W and receive one unit of data is 3W. The average data packet length is 128 bits. The average transmission power is 1mW. Similar to Jin, et al. [10], the MAC layer protocol used was IEEE802.15.4, and the routing protocol used was LEACH. The performance of proposed EIDR system is analyzed by two different testing scenarios is single attack and multiple attacks with fixed number nodes as 100 and 200. For the single attack case, we use the flooding attack to observe the results and for multiple attack case, we use the three different attacks such as a selective forwarding attack, a DoS attack, and a flooding attack. The simulation parameters and setups are summarized in Table 1 and 2 respectively.

Parameters	Values
Number of nodes	100 and 200
Number of attacks	0-20 (variable)
Packet size (bytes)	128
MAC layer protocol	IEEE 802.15.4
Routing protocol	LEACH
Simulation area	600 m X 600 m
Initial transmission power	1 mW
Traffic source	Constant bit rate (CBR)
Simulation time	500 seconds

Table 6: Simulation Parameters.

Test scenario	Number of nodes	Number of attacks	Attacks in details
1	100	0-20	Flooding attack
		0-20	Selective forwarding, DoS and flooding attacks
2	200	0-20	Flooding attack

Table 7: Simulation Setup.

The performance of our proposed an enhanced intrusion detection and response (EIDR) system is compared with existing multi-agent trust-based intrusion detection (MITD) scheme [10] in terms of delay, packet loss rate, energy consumption, network lifetime, throughput, detection rate and false positive rate.

- Delay is the average time, in seconds taken for a data packet to travel from the source to destination.
- Packet loss rate is the ratio of number of packets dropped and the total number of packets transmitted.
- Energy consumption is the amount of energy consumed by the nodes for the data transmission.
- Network lifetime is the operational time of the network during which it is able to perform the dedicated tasks.
- Throughput is the amount of packets moved successfully from one place to another in a given time period.
- Detection rate is the ratio of number of malicious nodes detected and the total number of malicious nodes in a network [10].
- False positive rate is the proportion of the number of nodes that are mistakenly identified as malicious nodes to the total number of nodes detected [10].

Case-1: Node Density-100: In this test, we analyze the performance of EIDR with the fixed network size as 600×600 m^2 area, node as 100 and varying the malicious nodes as 0, 5, 10, 15 and 20 for both single and multiple attacks.
The simulation time of this test is set as 500 seconds and compute performance metrics.

➢ **Single Attack:** Figure 2 shows the delay for both two schemes and it clearly depicts the delay of the proposed EIDR system is very lower than existing MITD scheme for different number of malicious nodes.

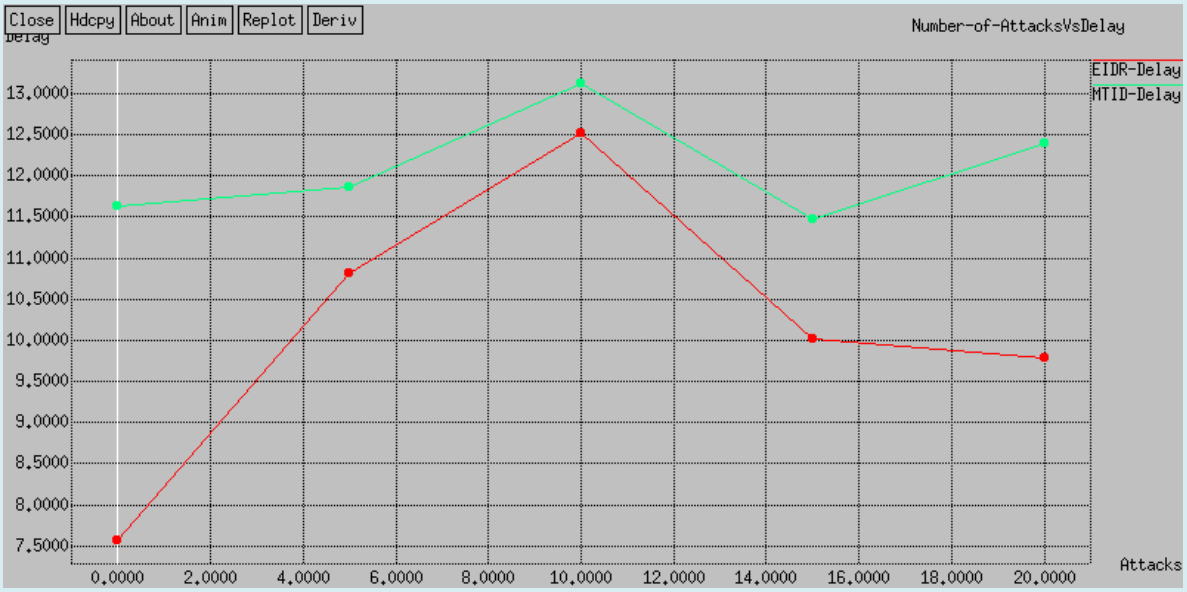

Figure 2: Delay comparisons with varying malicious nodes (single attack).

Figure 3 shows the packet loss ratio for both two schemes and it clearly depicts the loss ratio of the proposed EIDR system is lower than existing MITD scheme for different number of malicious nodes.

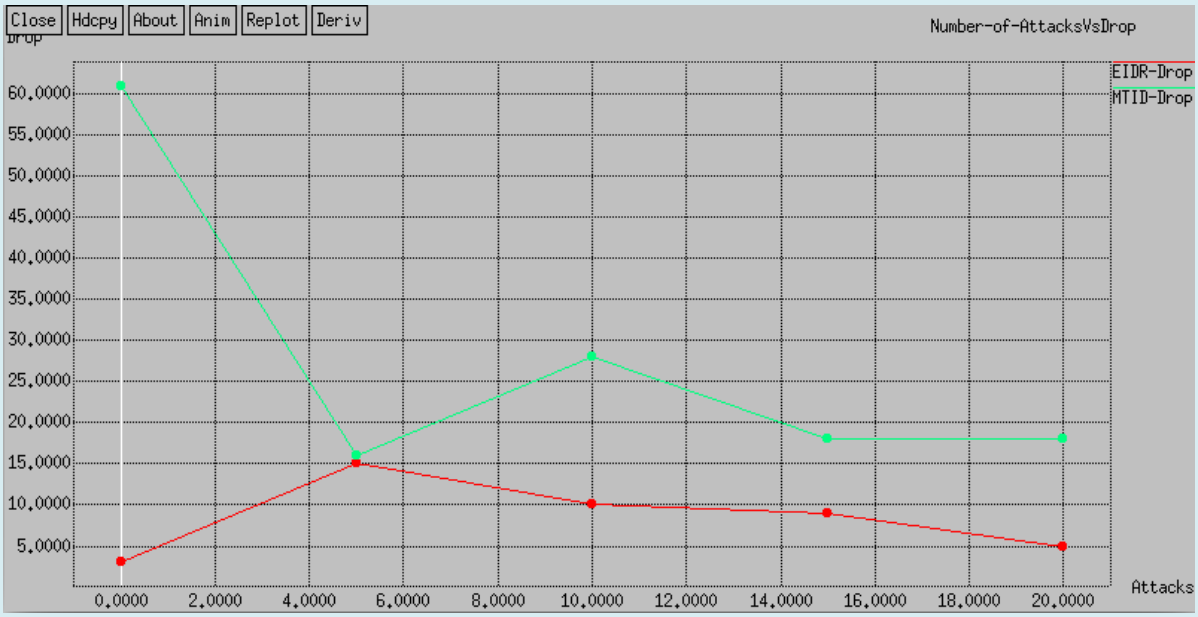

Figure 3: Packet loss rate comparisons with varying malicious nodes (single attack).

Figure 4 shows the energy consumption for both two schemes and it clearly depicts the energy consumption of the proposed EIDR system is very lower than existing MITD scheme for different number of malicious nodes.

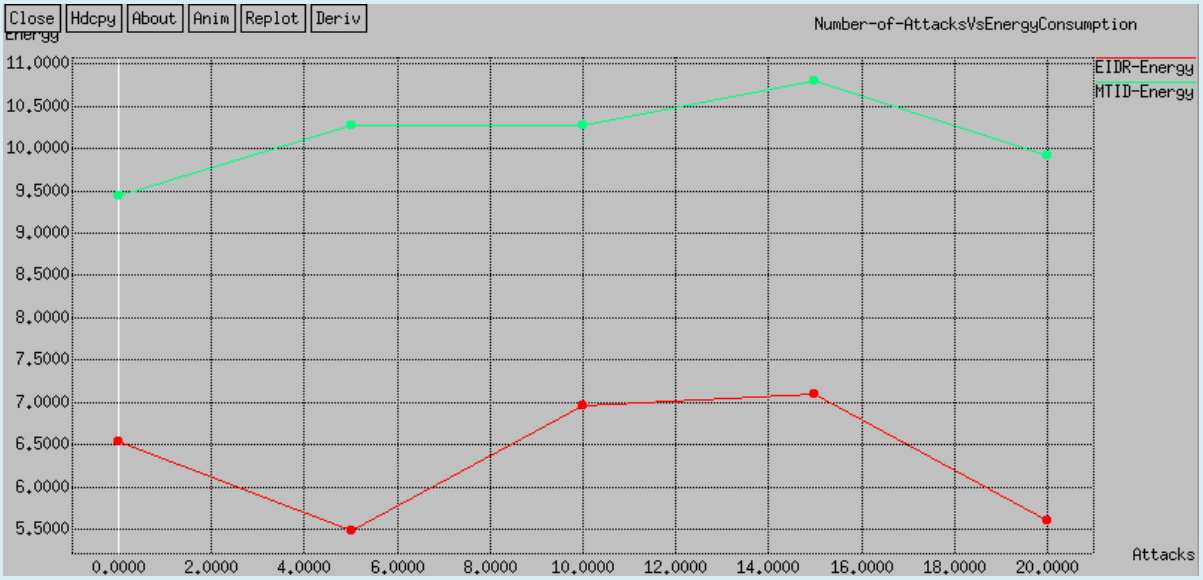

Figure 4: Energy consumption comparisons with varying malicious nodes (single attack).

Figure 5 shows the network lifetime for both two schemes and it clearly depicts the network lifetime of the proposed EIDR system is very higher than existing MITD scheme for different number of malicious nodes.

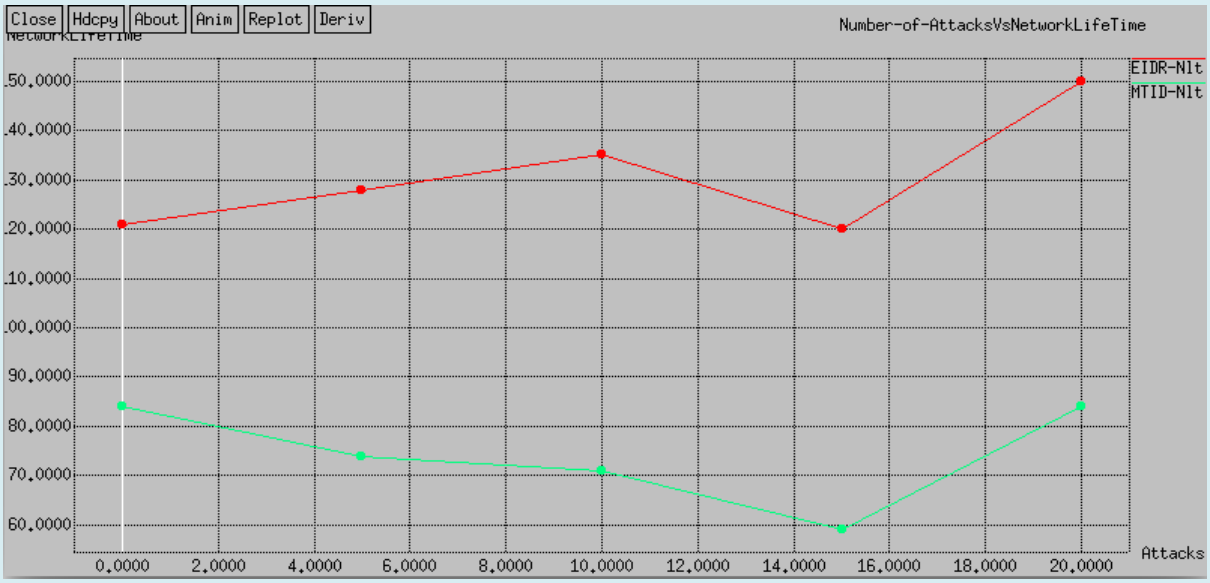

Figure 5: Network lifetime comparisons with varying malicious nodes (single attack).

Figure 6 show the throughput for both two schemes and it clearly depicts the throughput of the proposed EIDR system is very higher than existing MITD scheme for different number of malicious nodes.

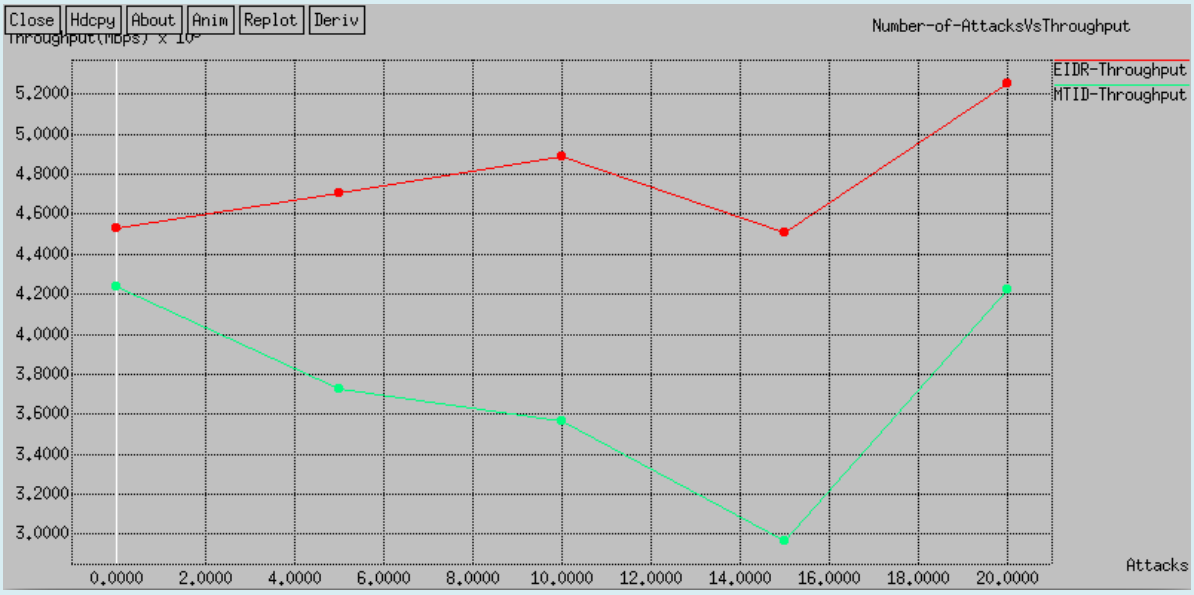

Figure 6: Throughput comparisons with varying malicious nodes (single attack).

Figure 7 shows the detection rate for both two schemes and it clearly depicts the detection rate of the proposed EIDR system is very higher than existing MITD scheme for different number of malicious nodes.

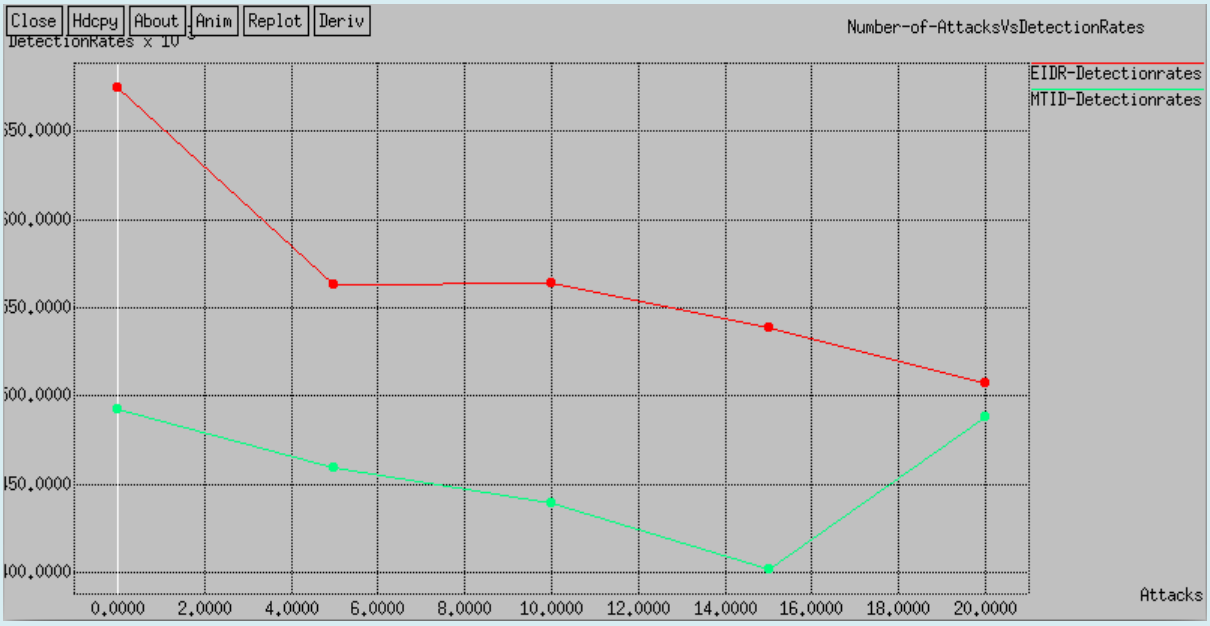

Figure 7: Detection rate comparisons with varying malicious nodes (single attack).

Figure 8 shows the false positive rate for both two schemes and it clearly depicts the false positive rate of the proposed EIDR system is very lower than existing MITD scheme for different number of malicious nodes.

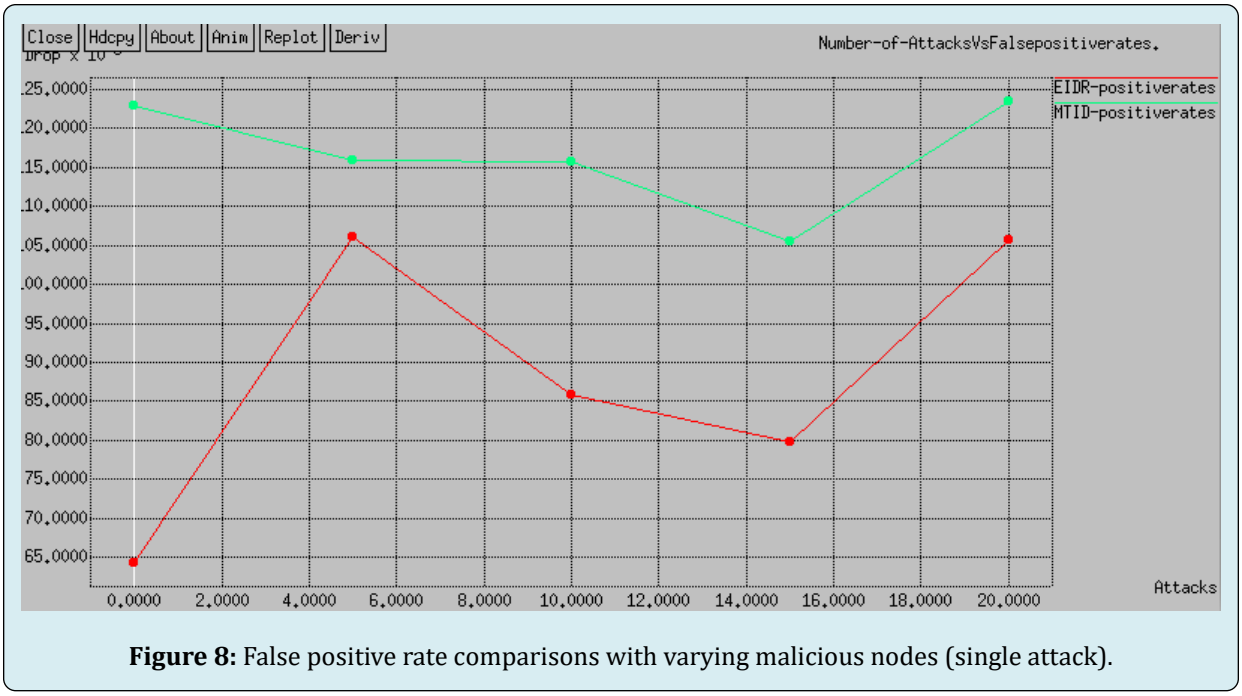

Figure 8: False positive rate comparisons with varying malicious nodes (single attack).

- **Multiple Attacks:** Figure 9 shows the delay for both two schemes and it clearly depicts the delay of the proposed EIDR system is very lower than existing MITD scheme for different number of malicious nodes.

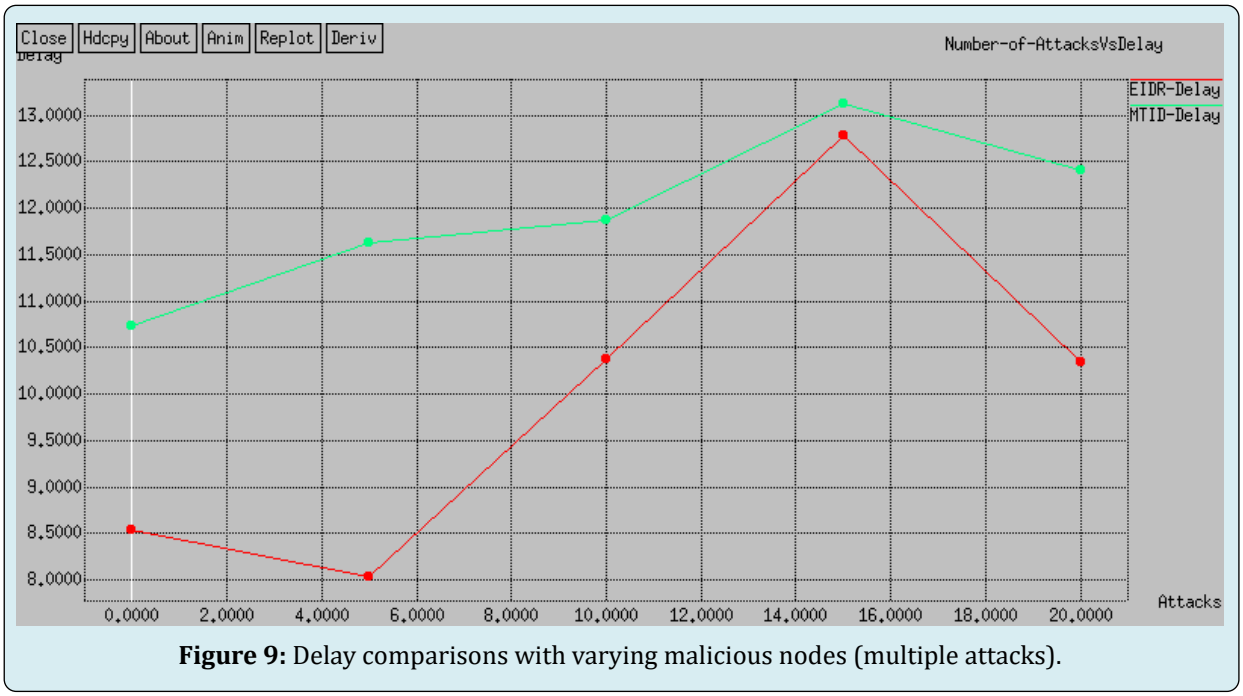

Figure 9: Delay comparisons with varying malicious nodes (multiple attacks).

Figure 10 shows the packet loss ratio for both two schemes and it clearly depicts the loss ratio of the proposed EIDR system is lower than existing MITD scheme for different number of malicious nodes.

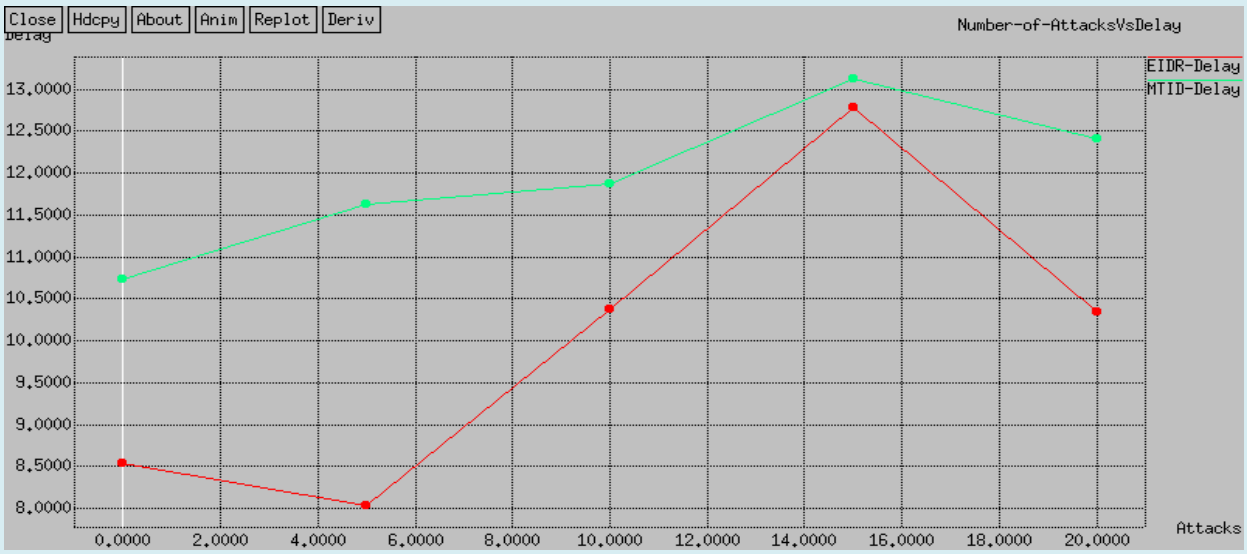

Figure 10: Packet loss rate comparisons with varying malicious nodes (multiple attacks).

Figure 11 shows the energy consumption for both two schemes and it clearly depicts the energy consumption of the proposed EIDR system is very lower than existing MITD scheme for different number of malicious nodes.

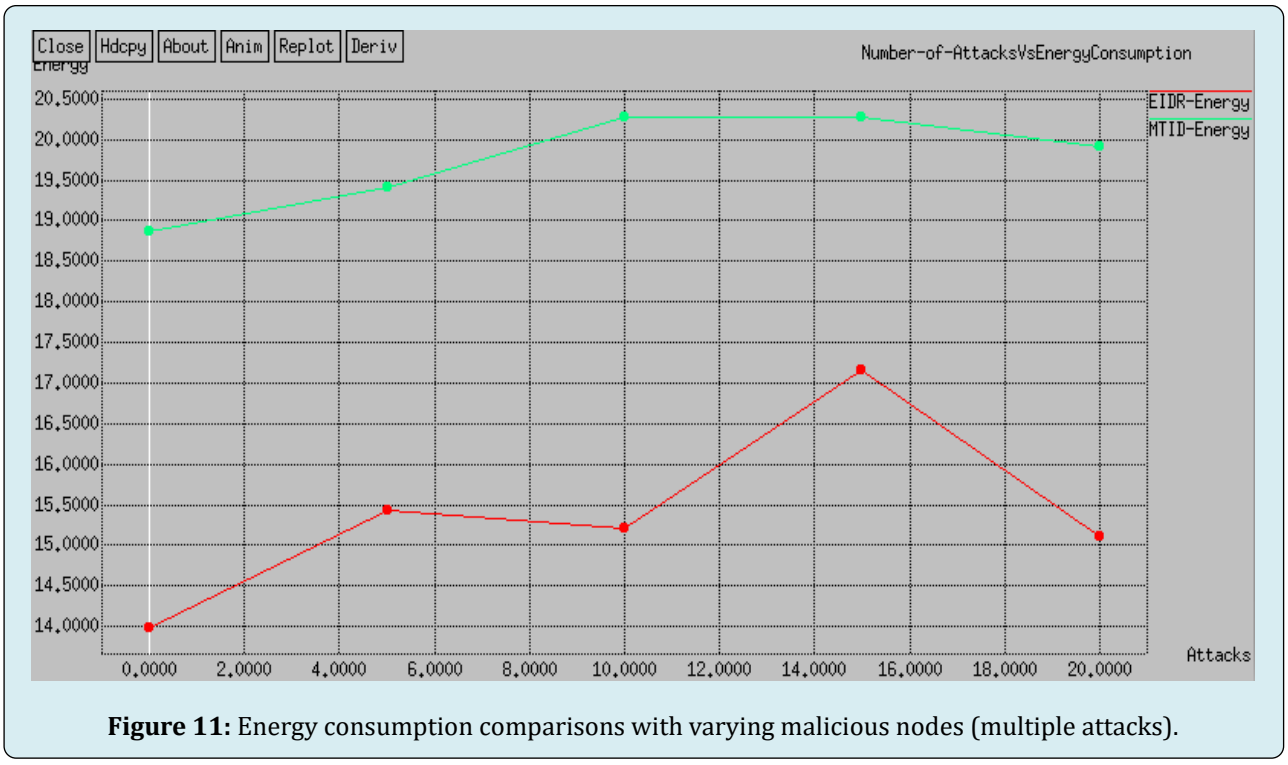

Figure 11: Energy consumption comparisons with varying malicious nodes (multiple attacks).

Figure 12 shows the network lifetime for both two schemes and it clearly depicts the network lifetime of the proposed EIDR system is very higher than existing MITD scheme for different number of malicious nodes.

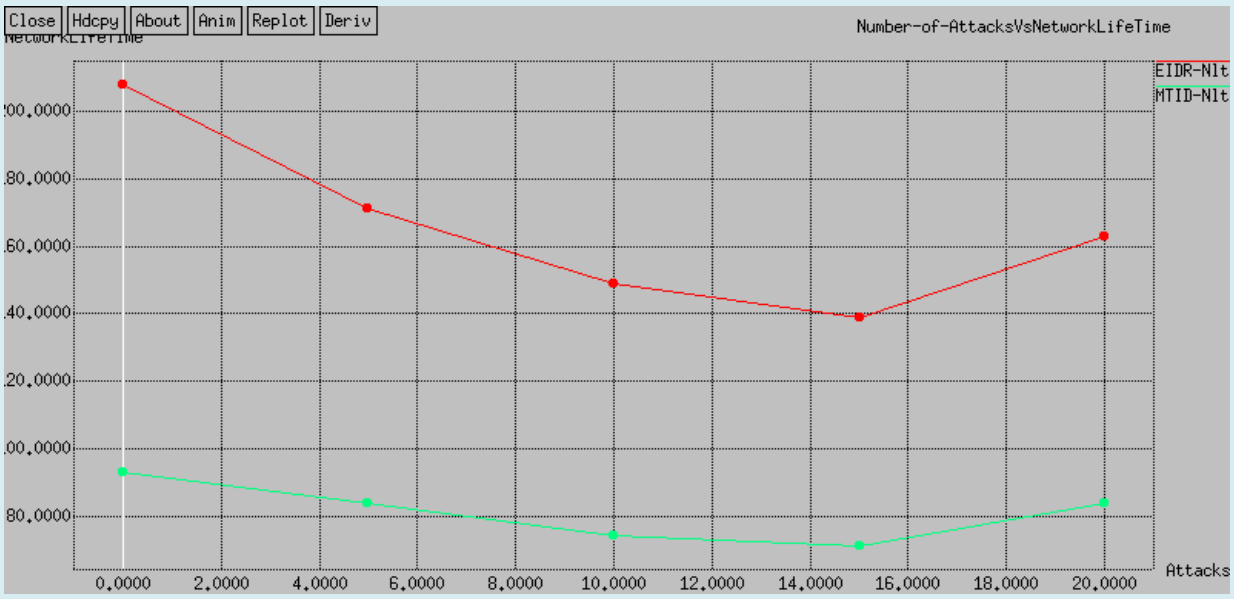

Figure 12: Network lifetime comparisons with varying malicious nodes (multiple attacks).

Figure 13 show the throughput for both two schemes and it clearly depicts the throughput of the proposed EIDR system is very higher than existing MITD scheme for different number of malicious nodes.

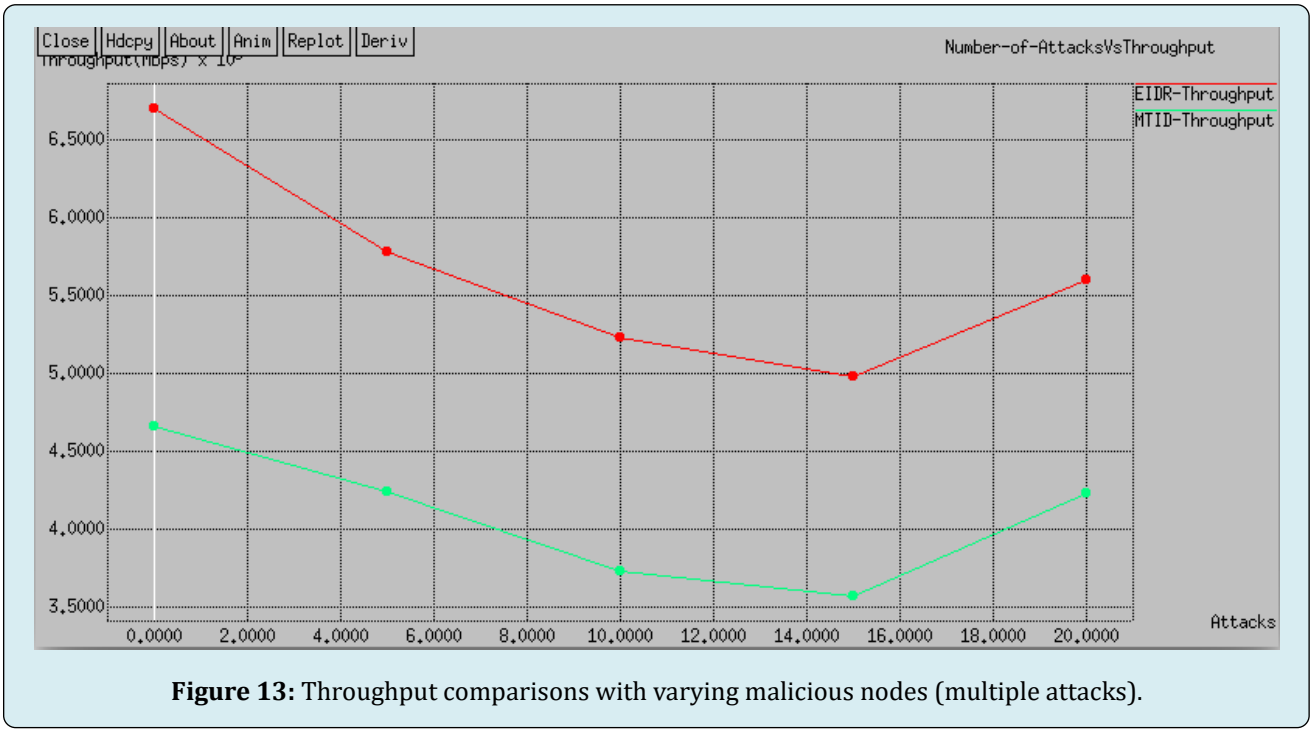

Figure 13: Throughput comparisons with varying malicious nodes (multiple attacks).

Figure 14 shows the detection rate for both two schemes and it clearly depicts the detection rate of the proposed EIDR system is very higher than existing MITD scheme for different number of malicious nodes.

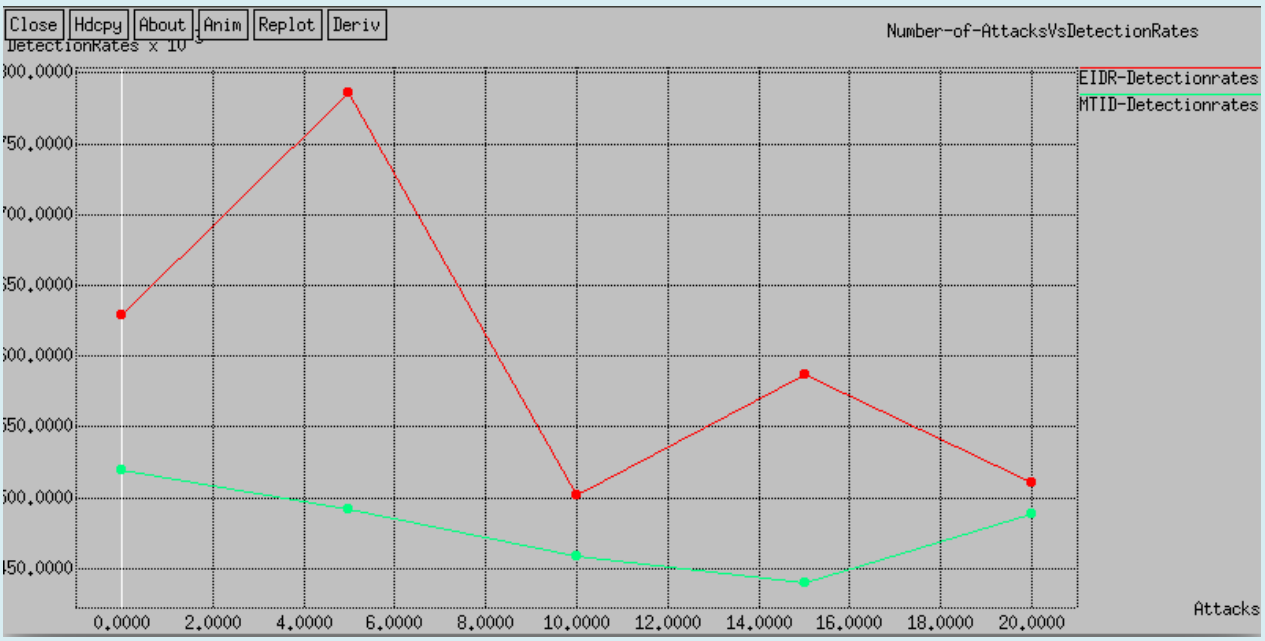

Figure 14: Detection rate comparisons with varying malicious nodes (multiple attacks).

Figure 15 shows the false positive rate for both two schemes and it clearly depicts the false positive rate of the proposed EIDR system is very lower than existing MITD scheme for different number of malicious nodes.

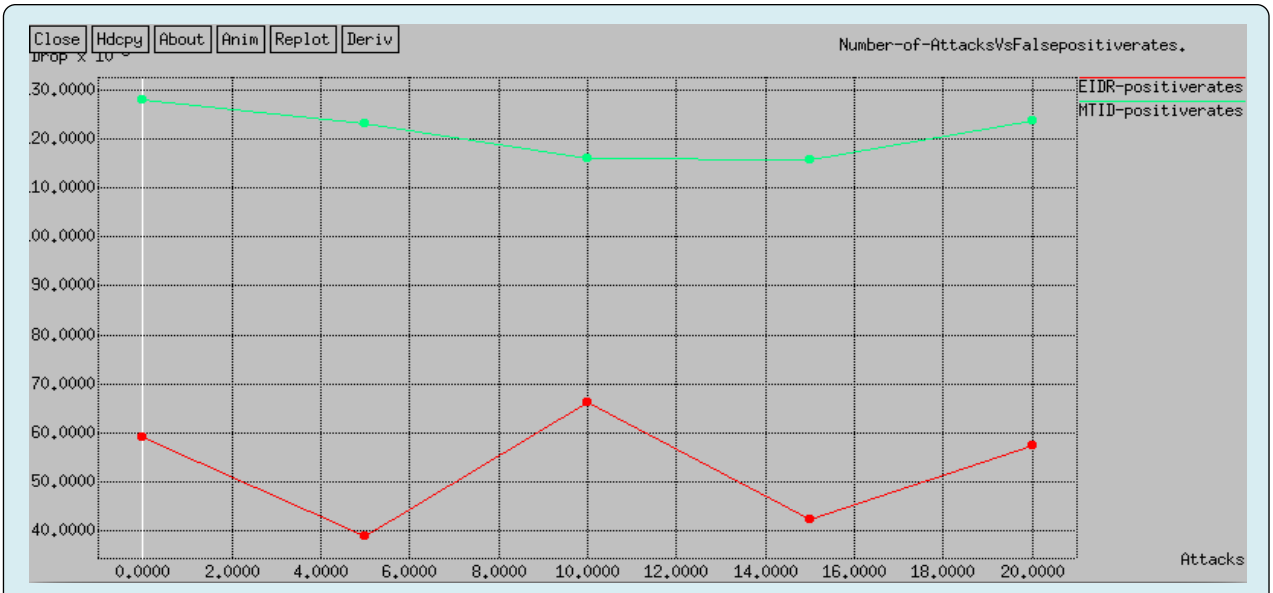

Figure 15: False positive rate comparisons with varying malicious nodes (multiple attacks).

Case-2: Node Density-200: In this test, we analyze the performance of EIDR with the fixed network size as 300×300 m^2 area, node as 200 and varying the malicious nodes as 0, 5, 10, 15 and 20 (single attack). The simulation time of this test is set as 100 seconds and compute performance metrics. Figure 16 shows the delay for both two schemes and it clearly depicts the delay of the proposed EIDR system is very lower than existing MITD scheme.

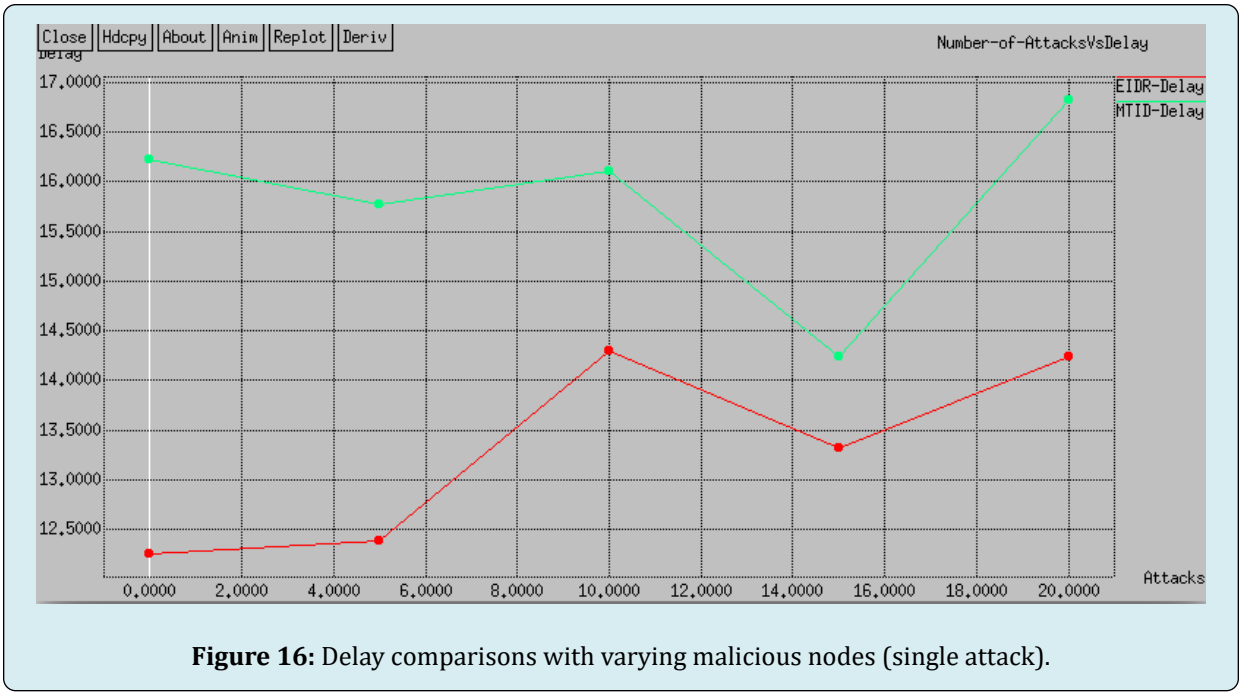

Figure 16: Delay comparisons with varying malicious nodes (single attack).

Figure 17 shows the packet loss ratio for both two schemes and it clearly depicts the loss ratio of the proposed EIDR system is lower than existing MITD scheme.

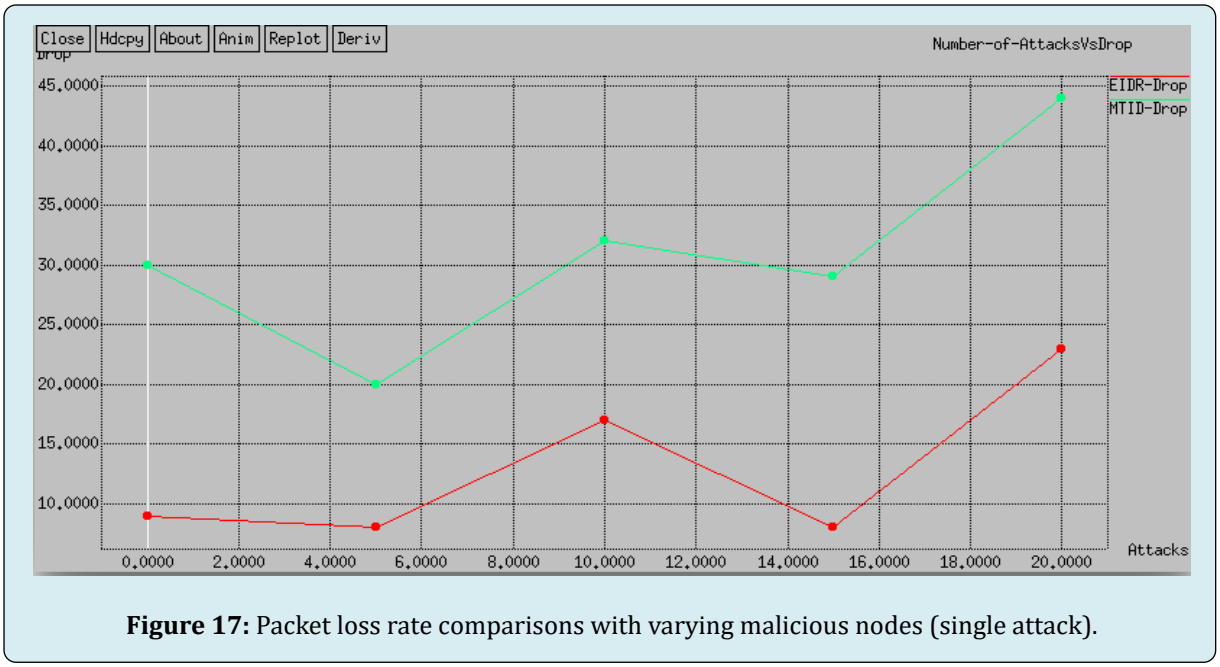

Figure 17: Packet loss rate comparisons with varying malicious nodes (single attack).

Figure 18 shows the energy consumption for both two schemes and it clearly depicts the energy consumption of the proposed EIDR system is very lower than existing MITD scheme.

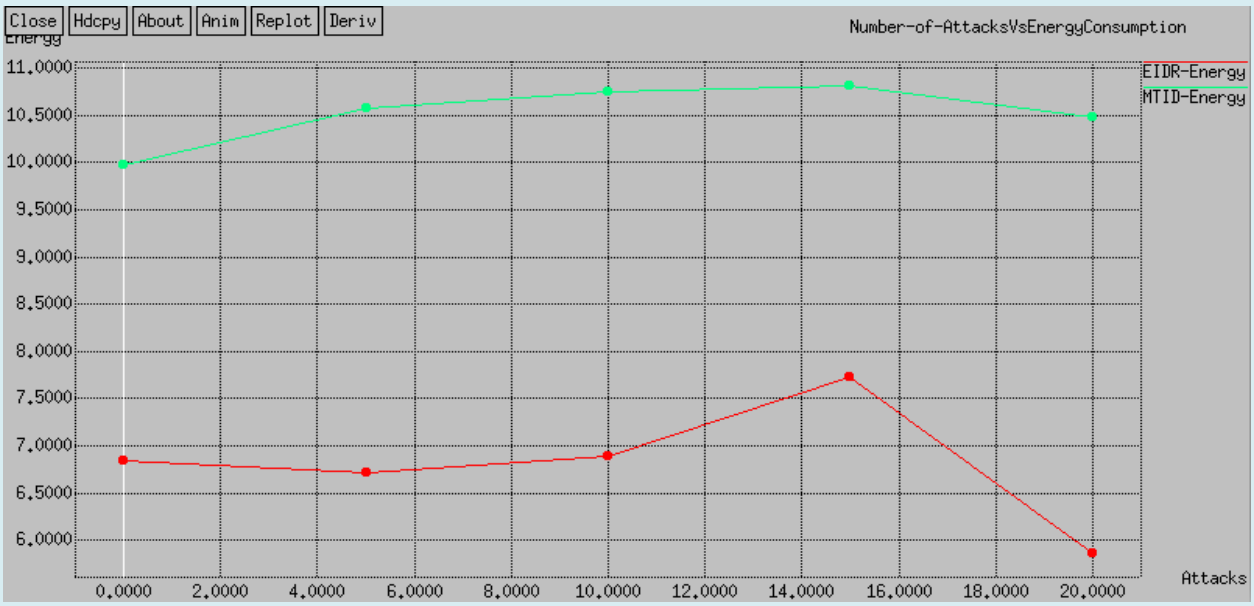

Figure 18: Energy consumption comparisons with varying malicious nodes (single attack).

Figure 19 shows the network lifetime for both two schemes and it clearly depicts the network lifetime of the proposed EIDR system is very higher than existing MITD scheme.

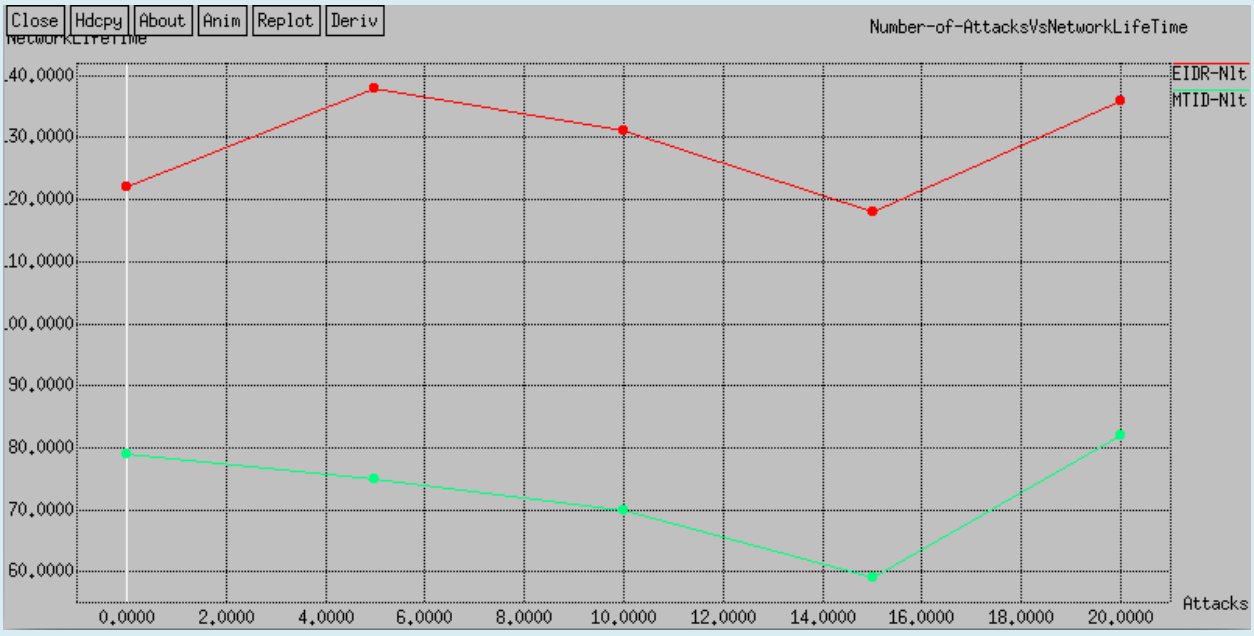

Figure 19: Network lifetime comparison with varying malicious nodes (single attack).

Figure 20 show the throughput for both two schemes and it clearly depicts the throughput of the proposed EIDR system is very higher than existing MITD scheme for different number of malicious nodes.

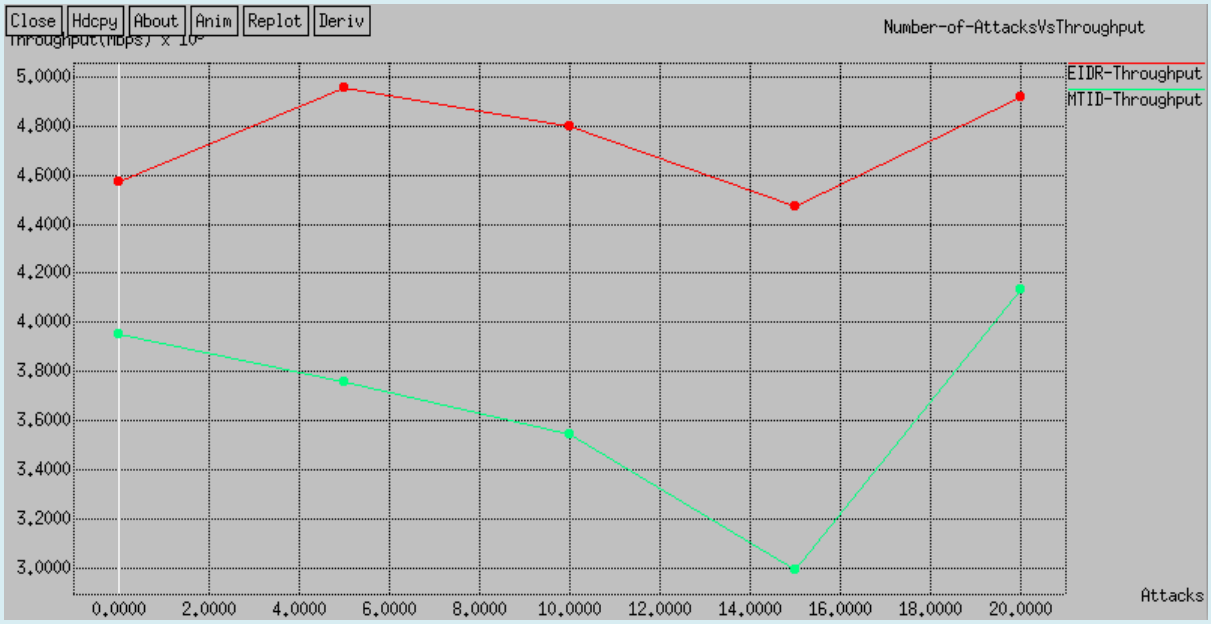

Figure 20: Throughput comparisons with varying malicious nodes (single attack).

Figure 21 shows the detection rate for both two schemes and it clearly depicts the detection rate of the proposed EIDR system is very higher than existing MITD scheme.

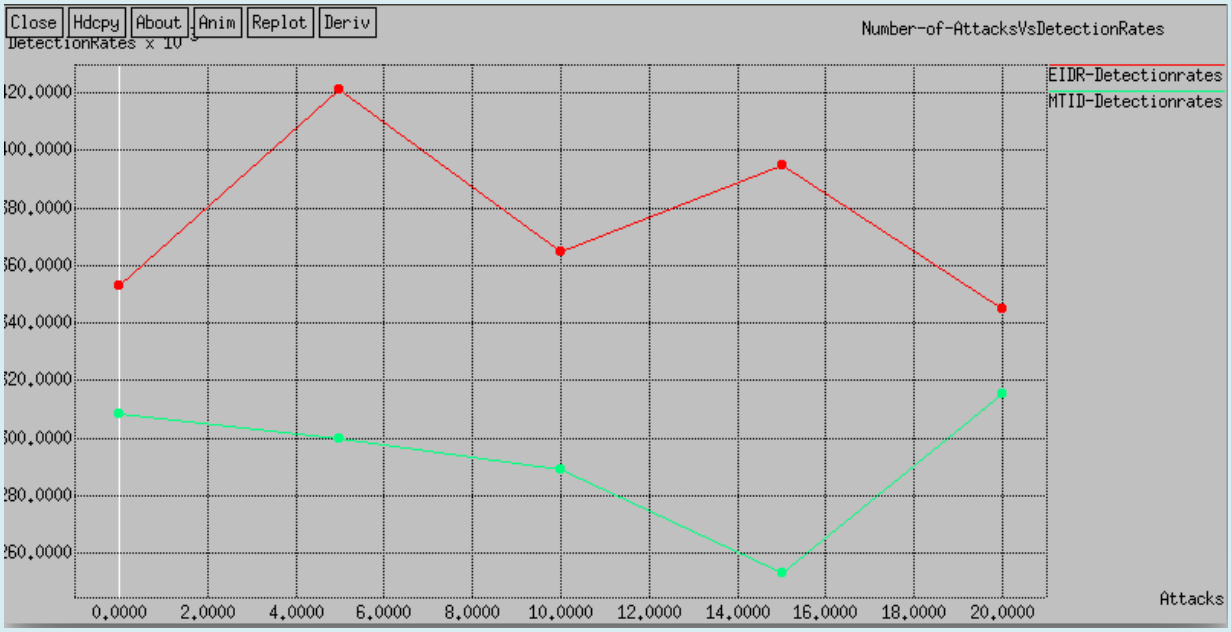

Figure 21: Detection rate comparisons with varying malicious nodes (single attack).

Figure 22 shows the false positive rate for both two schemes and it clearly depicts the false positive rate of the proposed EIDR system is very lower than existing MITD scheme.

Figure 22: False positive rate comparisons with varying malicious nodes (single attack).

Conclusion

We have proposed an enhanced intrusion detection and response (EIDR) system using the combination of clustering and trust model. In EIDR, chaotic ant optimization (CAO) algorithm is utilized to form the optimal clustering with balanced network and multi objective differential evolution (MODE) algorithm is utilized to compute the trust value of each node. Then, perform the intrusion response action (IRA) system using the computed trust values. The simulation result shows the effectiveness of proposed EIDR system in terms of delay, loss ratio, energy consumption, network lifetime, throughput, detection rate and false positive rate.

References

1. Bleda A, Fernandez Luque F, Rosa A, Zapata J, Maestre R (2017) Smart Sensory Furniture Based on WSN for Ambient Assisted Living. IEEE Sensors Journal 17(17): 5626-5636.

2. Wu J, Ota K, Dong M, Li C (2016) A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities. IEEE Access 4: 416-424.

3. Jokhio S, Jokhio I, Kemp A (2013) Light-weight framework for security-sensitive wireless sensor networks applications. IET Wireless Sensor Systems 3(4): 298-306.

4. Valeur F, Vigna G, Kruegel C, Kemmerer R (2004) Comprehensive approach to intrusion detection alert correlation. IEEE Transactions on Dependable and Secure Computing 1(3): 146-169.

5. Mishra A, Nadkarni K, Patcha A (2004) Intrusion detection in wireless ad hoc networks. IEEE Wireless Communications 11(1): 48-60.

6. Ye N, Chen Q, Borror C (2004) EWMA Forecast of Normal System Activity for Computer Intrusion Detection. IEEE Transactions on Reliability 53(4): 557-566.

7. Erbacher R, Walker K, Frincke D (2002) Intrusion and misuse detection in large-scale systems. IEEE Computer Graphics and Applications 22(1): 38-47.

8. Hoyle B, Rau M, Paech K, Bonnett C, Seitz S, et al. (2015) Anomaly detection for machine learning redshifts applied to SDSS galaxies. Monthly Notices of the Royal Astronomical Society 452(4): 4183-4194.

9. Sun B, Osborne L, Xiao Y, Guizani S (2007) Intrusion detection techniques in mobile ad hoc and wireless sensor networks. IEEE Wireless Communications 14(5): 56-63.

10. Jin X, Liang J, Tong W, Lu L, Li Z (2017) Multi-agent trust-based intrusion detection scheme for wireless sensor networks. Computers & Electrical Engineering 59: 262-

273.

11. Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang, Agrawal D (2008) Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks. IEEE Transactions on Mobile Computing 7(6): 698-711.

12. Shin S, Kwon T, Jo G, Park Y, Rhy H (2010) An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks. IEEE Transactions on Industrial Informatics 6(4): 744-757.

13. Bu S, Yu F, Liu X, Tang H (2011) Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks. IEEE Transactions on Wireless Communications 10(9): 3064-3073.

14. Bao F, Chen I, Chang M, Cho J (2012) Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection. IEEE Transactions on Network and Service Management 9(2): 169-183.

15. Wei M, Kim K (2012) Intrusion detection scheme using traffic prediction for wireless industrial networks. Journal of Communications and Networks 14(3): 310-318.

16. Chen J, Li J, Lai T (2013) Energy-Efficient Intrusion Detection with a Barrier of Probabilistic Sensors: Global and Local. IEEE Transactions on Wireless Communications 12(9): 4742-4755.

17. Abduvaliyev A, Pathan A, Jianying Zhou, Roman R, Wai Choong Wong (2013) On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks. IEEE Communications Surveys & Tutorials 15(3): 1223-1237.

18. Sun B, Shan X, Wu K, Xiao Y (2013) Anomaly Detection Based Secure In-Network Aggregation for Wireless Sensor Networks. IEEE Systems Journal 7(1): 13-25.

19. Matyas V, Kur J (2013) Conflicts between Intrusion Detection and Privacy Mechanisms for Wireless Sensor Networks. IEEE Security & Privacy 11(5): 73-76.

20. Moosavi H, Bui F (2014) A Game-Theoretic Framework for Robust Optimal Intrusion Detection in Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security 9(9): 1367-1379.

21. Han G, Rodrigues J, Jiang J, Shu L, Shen W (2013) IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks. IET Information Security 7(2): 97-105.

22. Deif D, Gadallah Y (2017) An Ant Colony Optimization Approach for the Deployment of Reliable Wireless Sensor Networks. IEEE Access 5: 10744-10756.

23. Han G, Li X, Jiang J, Shu L, Lloret J (2014) Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack in Wireless Sensor Networks. The Computer Journal 58(6): 1280-1292.

24. Lin K, Xu T, Song J, Qian Y, Sun Y (2016) Node Scheduling for All-Directional Intrusion Detection in SDR-Based 3D WSNs. IEEE Sensors Journal 16(20): 7332-7341.

25. Pintea C, Pop P, Zelina I (2015) Denial jamming attacks on wireless sensor network using sensitive agents. Logic Journal of IGPL 24(1): 92-103.

26. Huang K, Zhang Q, Zhou C, Xiong N, Qin Y (2017) An Efficient Intrusion Detection Approach for Visual Sensor Networks Based on Traffic Pattern Learning. IEEE Transactions on Systems, Man, and Cybernetics: Systems 47(10): 2704-2713.

27. Zhang Z, Zhu H, Luo S, Xin Y, Liu X (2017) Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks. IEEE Access 5: 12088-12102.

28. Mrugala K, Tuptuk N, Hailes S (2017) Evolving attackers against wireless sensor networks using genetic programming. IET Wireless Sensor Systems 7(4): 113-122.

29. Sedjelmaci H, Senouci S, Ansari N (2017) Intrusion Detection and Ejection Framework against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology. IEEE Transactions on Intelligent Transportation Systems 18(5): 1143-1153.

30. Guo Q, Li X, Xu G, Feng Z (2017) MP-MID: Multi-Protocol Oriented Middleware-level Intrusion Detection method for wireless sensor networks. Future Generation Computer Systems 70: 42-47.

31. Santoro D, Escudero Andreu G, Kyriakopoulos K, Aparicio Navarro F, Parish D, et al. (2017) A hybrid intrusion detection system for virtual jamming attacks on wireless networks. Measurement 109: 79-87.

32. Alsaedi N, Hashim F, Sali A, Rokhani F (2017) Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS). Computer Communications 110(15): 75-82.

33. Harno H, Petersen I (2015) Synthesis of Linear Coherent Quantum Control Systems Using a Differential Evolution Algorithm. IEEE Transactions on Automatic Control

60(3): 799-805.

Authors Biography

Dr. Kathirvel Ayyaswamy, acquired, B.E.(CSE), M.E. (CSE) and Ph. D (CSE.) from Anna University. He has served in various positions at Deemed Universities, Autonomous Institution and Anna University affiliated colleges from 1998 to till date.

He is currently working as Professor, Dept of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus at Chennai. He has worked as Lecturer, Senior Lecturer, Assistant Professor, Professor, and Professor & Head in various institutions.

He is a studious researcher by himself, completed 18 sponsored research projects worth of Rs 103 lakhs and published more than 110 articles in journals and conferences. 4 research scholars have completed Ph. D and 3 under progress under his guidance. He is working as scientific and editorial board member of many journals. He has reviewed dozens of papers in many journals. He has author of 12 books. He has also published a research monograph from the LAP Lambert Academic Publishing GmbH & Co., Germany, Europe based on his Ph.D thesis titled "Umpiring Security Model and Performance improvement on MANETS", costing 110.35 Euros. His other two books are Introduction to GloMoSim and Prevention of Attacks using Umpiring Security Model for MANETS, LAP Lambert Academic Publishing GmbH & Co., Germany. Europe. His research interests are protocol development for wireless ad hoc networks, security in ad hoc network, data communication and networks, mobile computing, wireless networks and Delay tolerant networks.

His biography was published in 29th edition of Marquis's Who's Who in the World in 2012 issue. He has also guided more than 3 dozen projects (B.E/B.Tech/M.E/M.Tech/MCA) in various engineering colleges. He has given many keynote/ invited talks/ plenary lecturers in various national and international conferences and chaired many sessions.

He is a Life member of the ISTE (India), Senior Member IACSIT (Singapore), Life Member IAENG (Hong Kong), Member ICST (Europe), IAES, Member IEEE and ACM. He has given a number of guest lecturers/expert talks and seminars, workshops and symposiums. He has visited Dubai, Abu Dhabi and Oman for presentation of his research papers in various international conferences.