Secure and Energy Efficient Trust Aware Routing Protocol in IoT using the Optimized Artificial Neural Network: SEETA-IoT

Balwinder Kaur Dhaliwal, Rattan K Datta

Abstract**:** ***Nowadays, Internet of Things (IoT) has been widely used in many areas such as surveillance of battlefield, controlling of industry, pipeline monitoring, ecological monitoring, healthcare and medical science, defense and military affairs, etc. To make better IoT based applications, secure routing plays an imperative responsibility for Device-to-Device (D2D) data packet transmission. The most essential inventiveness behind this research is to design a Secure and Energy Efficient Trust Aware (SEETA) routing protocol in terms of detecting the fail/malicious nodes by utilizing the Artificial Neural Network (ANN) using Particle Swarm Optimization (PSO) Algorithm. To discover a secure and energy-efficient route, the trust-based approach is integrated with GOA and ANN. Therefore, this research focuses on the security enhancement of the IoT network using the concept of trust-based route maintenance mechanism. In IoT networks, communicating sensor nodes have limited energy resources and a rapid energy reduction of communicating nodes leads to the creation of energy holes in the network. To overcome this problem, an energy-efficient mechanism of trust aware approach is also one of the essential objectives of IoT routing protocols. To avoid unnecessary network failure and extra energy consumption rate, we had designed a model using the concept of PSO based ANN with a novel fitness function and for involvement in the routing process, sensor nodes should fulfill the fitness criteria; otherwise, the system considers as affected communicating nodes. From the experiments conducted, it is proved that the proposed SEETA routing protocol using the PSO and ANN, achieves significant performance improvement over the existing schemes in terms of security, energy efficiency and packet transmission rate. Besides, SEETA routing protocol also reduces the number of intermediates nodes in D2D route discovery mechanism for IoT networks which helps to decrease the energy consumption rate and also offers a proficient approach to discover secure routing support with maximum routing capacity and end to end data transmission rate. The QoS performance parameter of our routing protocol is analyzed with standard and existing work with several routing protocols and the experimental results validating the concept of optimized ANN. The experimental results indicate that the introduced SEETA routing protocol provides 8.74% less energy consumption rate and high data delivery rate and data delivery rate is improved by 92% as compare to exiting works.***

Keywords: Internet of Things, Secure and Energy Efficient Trust Aware, Device-to-Device Communication, Particle Swarm Optimization Algorithm, Artificial Neural Network, Quality of Service (QoS).

Revised Manuscript Received on August 30, 2019.

* Correspondence Author

Balwinder kaur*, Assistant Professor B.tech(I.T),M.Tech(CSE) and now pursuing Ph.D from Sant Baba Bhag Singh University. India.

Dr Rattan K Datta, Ph.D from IIT-Delhi on "Monsoon Dynamics & Atmospheric Modeling". India.

I. INTRODUCTION

Nowadays, the utilization of the Internet has moved toward a basic need of the regular day to day existence. The spirit of an exhaustive systems administration stage dependent on the correspondence of the brilliant article has officially made a major jump forward. The alleged Internet of Things (IoT) [1] innovation develops into prerequisites for contemporary society, where people and things are coordinated. This advancement will prepare for the improvement of new applications and administrations, which will probably use the availability of physical and virtual substances.The IoT model relies on accessible communication technologies such as Wi-Fi, Bluetooth, Zig-Bee, etc, just to name a few [2]. However, configuring an acceptable and desirable IoT network, based on these various technologies, seems a laborious and difficult challenge. The regularity of the IoT network is crucial in providing advanced interoperability for all tiny sensor devices, which also require security supervision structure. Also, IoT network security and data packets confidentiality raises major issues. Last but not least, efficient energy and route maintenance systems are required; with intend to secure IoT networks. The entire challenges require to be addressed according to the adopted type of routing mechanisms. Although several studies have been conducted concerning the secure communication in IoT networks, none of them deals with the secure and trusted routing mechanism for IoT network layer. More specifically, a promising routing protocol for supporting wide-area Device-to-Device (D2D) communication [3] in IoT networks (figure 1) based on sensor devices are presented in this research with focus on the security mechanism utilizing the concept of artificial intelligence technique with ANN and PSO.

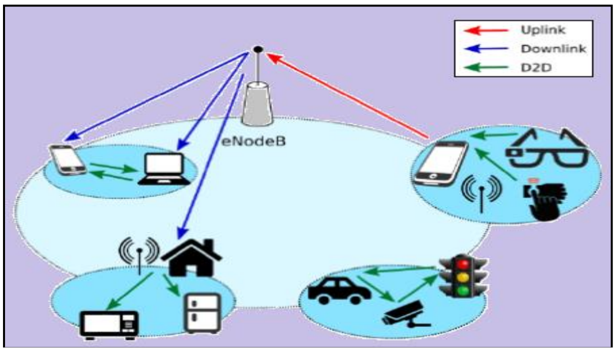


Figure 1: D2D Communication in IoT Networks

In IoT network, direct data packets transmission connecting devices is demanding task in the IoT networks because of its great scale, dynamic and assorted environment. In D2D routing, sensor devices may not communicate

over the core network but can route data for each other separately [4]. So D2D routing mechanism requires novel strategies that can make use of efficient optimization techniques. The success of IoT networks depends on the efficient and intelligent use of network resources [5].

The most important intend of proposed research is precisely to discuss the remuneration introduced by D2D technologies in IoT network for secure and trust aware routing that may be suitably exploited within ecosystems operating within future IoT systems. Security is a prime issue in IoT networks due to a large number of sensor nodes, feeble connectivity and energy source constraints [6]. Therefore, IoT networks are more prone to attacks than other types of infrastructural networks. Establishing secure communication route in an IoT network is predominantly challenging assignment because of

- IoT is a communal wireless transmission medium
- Transmission depends on the broadcasting
- Transmitted data packets pass through in a hop-by-hop approach so W
- Natures of IoT networks are dynamic
- Sensor nodes are constrained in terms of energy computation and battery power

Motivation of Research: In IoT networks, routing mechanism can be divided into different types like clustering based routing, D2D routing and locality based routing depending on the IoT network structure. From these types of routing protocols; D2D routing is the most excellent and secure routing protocol due their trust worthy nature [7]. In D2D routing, communicating sensor nodes will play different roles in the IoT network. The main aim of D2D routing is to efficiently maintain the energy consumption of communicating sensor nodes by involving them in multi-hop communication. This paper presents a SEETA routing protocol for IoT network using the concept of Particle Swarm Optimization (PSO) and Artificial Neural Network (ANN) as classifier to detect the fail/malicious/attacks [8] and their comparison with existing trends. Specifically, in section 2, we present the literate survey (Related Work) of existing work for IoT communication using different routing protocols and algorithms. The working of proposed work is described in the section 3 with trust model. The analysis of experimental result is cover in section 4 by comparing existing routing protocols and the conclusion with discussions on current challenges with future trends is described in section 5

II. RELATED WORK

In this section, we present the survey of existing IoT networks using different routing protocols and others algorithms to discover a secure transmission route. *Tie Qiu et al [1]* had designed an IoT network with efficient routing protocol for emergency response which is known as Emergency Response IoT based on Global Information Decision (ERGID). They proposed ERGID routing protocol to improve the performances of reliable data packet transmission and efficient urgent situation reply in IoT network. Specifically, they presented a Delay Iterative Method (DIM) mechanism, which is based on delay estimation, to resolve the predicament of ignoring applicable and valid routes in the networks. Moreover, to balance the load of IoT network, Residual Energy Probability Choice (REPC) is proposed by focusing on the residual energy of communicating sensor nodes. Simulation results and analysis of proposed IoT network show that designed ERGID routing protocol is better than EA-SPEED and SPEED in terms of QoS parameters such as end to end (E2E) delay, packet loss and energy consumption. s information routing decisions often lead to the blindness of secure route selection so that energy consumption is high for large data packets. *Saptarshi Debroy et al [2]* developed a simulator for D2D communication in IoT and talked about the difficulties of dynamic based auxiliary routing protocol for IoT network. They proposed SpEED routing mechanism with a range mindful, vitality effective multi-channel multi-jump directing method among IoT electronics gadgets with sensor nodes. A transmission power control based particular flooding procedure is proposed in this work to spread the course demands in the system without causing system wide transmission overhead. They investigated the network condition among IoT gadgets utilizing such techniques. Besides, there may investigate the presentation of their proposed plan both hypothetically and tentatively for various essential conditions and IoT organizes as far as operational range, essential transmission qualities, range attributes, and heterogeneous optional IoT gadget correspondence mode/capacities. But they don’t work on security mechanism and transmission time. *Meng Shiuan Pan and Shu-Wei Yang [3]* in 2017 presented a lightweight and distributed geographic-based multicast routing protocol for IoT applications. Their main goal is to reduce the number of transmission links and shorten path lengths in the constructed multicast paths. The proposed scheme contains a request phase, a reverse update phase, and a modify phase. In the request phase, nodes locally find the minimum number of next hop nodes to reach dsestination nodes. Then, in reversed update phase and modify phases, multicast paths can further be trimmed and merged by the designed schemes. The simulation and experiment results indicate that the proposed scheme can effectively reduce the number of transmission links and transmission delays but, they can be modify their scheme to support node mobility and their security. *Ishino et al [4]* in 2014 exhibited a lightweight and disseminated geographic-based multicast steering convention for IoT application. They proposed the adaptable steering engineering utilizing Bloom Filters for the IoT applications, and after that have cleared up the viability of our directing design. Thus, they have demonstrated that their steering engineering can decrease the extent of filters to roughly when required bundle conveyance rates are around 0.9. Furthermore, they can want to address the examination questions like how to stifle overheads to refresh steering data. Moreover, these sensor nodes are not compatible to existing routing protocol due to which a new set of routing protocols are developed to cater the requirements of the IoT networks.

To design or improve a secure and energy efficient framework for authentication, identity management, and a flexible trust management for secure and compatible IoT communication using sensor nodes. These types of problem always faced by the researcher in the field of IoT based communication and to solve out these problems better option is the selection of optimized classifiers for routing mechanism as a routing protocol using PSO with ANN.

After study of above mentioned existing research we conclude some important point which helps to short out existing secure routing problem. To solve the existing problem, we are summarizing the most important contributions in this research for proposed model as follows:

♦ ***Security from malicious/fail/ nodes:*** In the proposed SEETA scenario, only those nodes are participating in route discovery mechanism which has high residual energy which is use to prevent the network from fail nodes. The hybridization of PSO and ANN is sued detect the malicious nodes during D2D communication in IoT network.

♦ ***Energy Consumption Minimization:*** To achieve this goal, we are adding energy efficient trust aware based secure routing protocols and select only appropriate nodes in route as intermediate nodes.

♦ ***To maintain route in IoT Network:*** The proposed PSO based ANN is used to maintain the route in IoT network. To discover route within the network, fitness function of PSO helps for selection of intermediate route nodes.

Our experimental results show that SEETA routing protocol with PSO-ANN mechanism can further improve the routing performance by removing the unauthorized nodes from route then consider in the routing table for trust awareness. To validate the performance, we comprehensively evaluate the effectiveness, efficiency and the generalization capability of the proposed SEETA model with another author research work. Our proposed model can be easily generalized to other challenging routing protocol problems and also improve the energy consumption rate with high data transmission rate and flowchart is shown in figure 2.

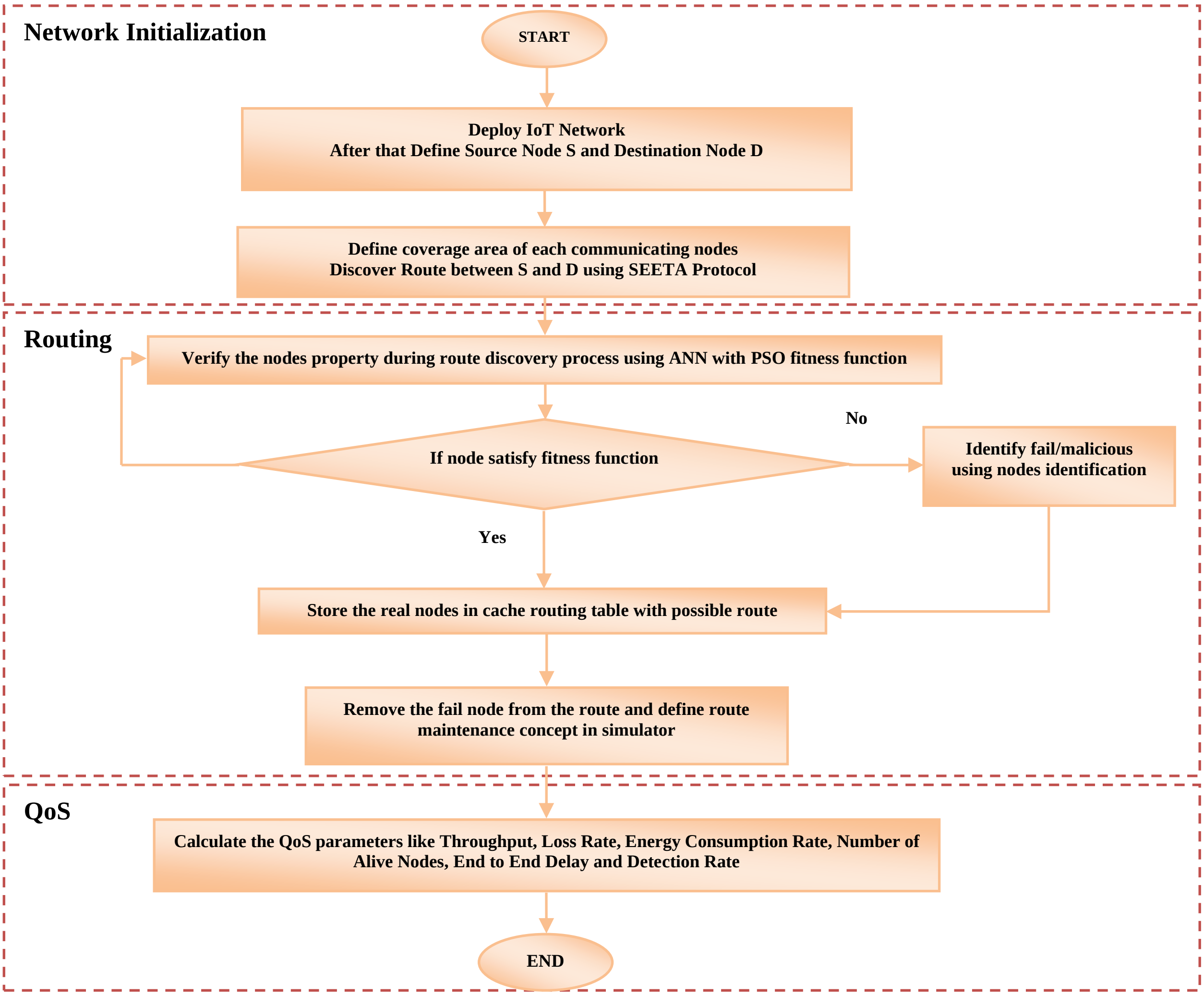

Network Initialization
START
Deploy IoT Network
After that Define Source Node S and Destination Node D
Define coverage area of each communicating nodes
Discover Route between S and D using SEETA Protocol
Routing
Verify the nodes property during route discovery process using ANN with PSO fitness function
If node satisfy fitness function
No
Identify fail/malicious
using nodes identification
Yes
Store the real nodes in cache routing table with possible route
Remove the fail node from the route and define route
maintenance concept in simulator
QoS
Calculate the QoS parameters like Throughput, Loss Rate, Energy Consumption Rate, Number of
Alive Nodes, End to End Delay and Detection Rate
END

Figure 2: Flow of GOA-ANN based SEETA Routing Mechanism

III. WORKING OF PSO-ANN BASED SEETA

The proposed IoT network with PSO-ANN based SEETA routing mechanism consists of several steps. The procedures of proposed IoT network are defined as follows:

A. IoT Network Architecture

First of all, we design an IoT simulator using the concept of Matlab based-Graphical User Interface (GUI) for simulation of proposed PSO-ANN based SEETA routing mechanism for secure and trusted establishment of communication link.

The area of proposed IoT network is defined by using given formula:

$$\boldsymbol{Area\ of\ IoT\ Network, A = H\ X\ W} \ \ldots\ldots\ (1)$$

Where, H and W are height and width of network that is considered as 1000m. So the total simulation area of IoT network is 1000m^2 which is sufficient for simulation. The designed frame work with some number of sensor nodes is show in figure 3. The IoT network deployment algorithm is given as:

Algorithm 1: IoT Network Architecture

```
Input Attributes: Number of Sensor Nodes (N), Height (H) and Width (W)
Output Attributes: Created IoT Network
Start:
Define height, H ← 1000
Define width, W ← 1000
Calculate area (A) of IoT network using equation 1
for i in N do
    X-Position (i) ← AX Random
    Y-Position (i) ← AX Random
    Deploy-Sensor (i) ← Coordinate (X-Position (i), Y-Position (i))
    Labeled sensor node name ← $N_1, N_2, N_3 \ldots N_n$
    $T_x$ (Source) ← Random ($N_1, N_2, N_3 \ldots N_n$)
    $R_x$ (Destination) ← Random ($N_1, N_2, N_3 \ldots N_n$)
    If $T_x$ == $R_x$ then (Check similarity)
        $T_x$ (Source) ← Random ($N_1, N_2, N_3 \ldots N_n$)
        $R_x$ (Destination) ← Random ($N_1, N_2, N_3 \ldots N_n$)
    Else
        $T_x$ (Source) ← $T_x$ (Source)
        $R_x$ (Destination) ← $R_x$ (Destination)
    End
    Design IoT Network
        Deploy Sensor in network
        Mark $T_x$ as a source node
        Mark $R_x$ as a destination node
    End
End
Return: Architecture of IoT Network
End
```

The designed IoT network with sensor nodes N_1, N_2, $N_3 \ldots N_n$ is shown in figure 3.

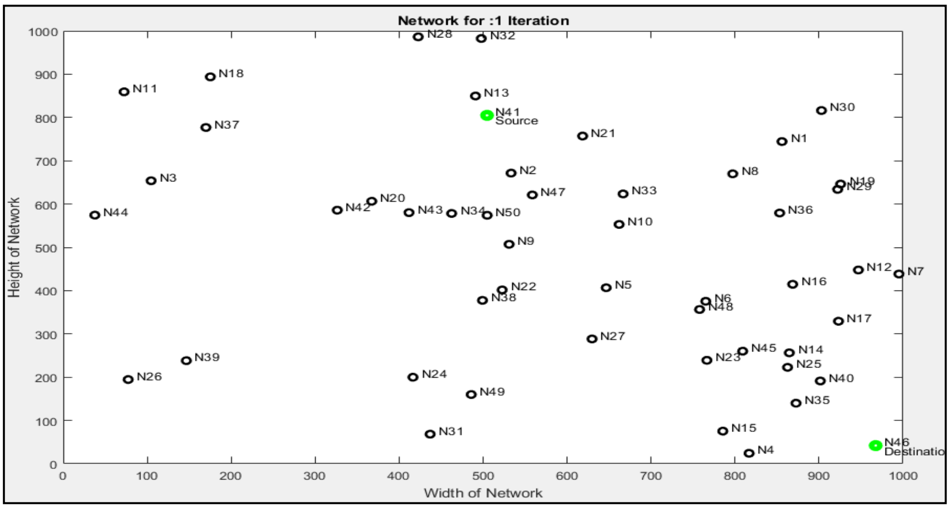


Figure 3: Flow of GOA-ANN based SEETA Routing Mechanism

B. Process for Coverage Limit Calculation

Define the coverage area for each node which helps to establish the route from source node to destination node using inter and intra communication process. The algorithm of coverage set calculation is given as:

Algorithm 2: Coverage Set of Nodes

```
Input Attribute: Number of sensor nodes (N), Area of IoT Network (A)
Output Attribute: Coverage list of communicating sensor nodes ($C_{List}$)
Start:
Characterize coverage limit of sensor nodes using equation (2) and it is 25% of IoT network area
    $Coverage_{Limit}, (C_L) = \frac{(25 \times A)}{100}$.... (2)
Initialize a setup for coverage list
for i in N do
    for j in N do
        If $i \neq j$ then
            Compute distances from one sensor node to other sensor node using distance formula in equation (3)
            $Dist = \sqrt{((X_j - X_i)^2 + (Y_j - Y_i)^2)}$.... (3)
        Else
            No need to calculate distance
        End
        If Dist < $C_L$ then
            $C_{Set}$ (i, j) ← Distance of nodes
            $C_{List}$ (i, j) ← Sensor nodes number
        End
    End
Return: $C_{List}$ as coverage list of sensor nodes
End
```

C. SEETA Routing Mechanism

To discover a secure route from source (T_x) node to destination (R_x) node using SEETA routing protocol for the D2D communication in IoT network The SEETA routing protocol algorithm is written follows:

Algorithm 3: SEETA Routing Protocol

```
Input Attribute: Source Sensor Node (SSN), Destination Sensor Node (DSN) Coverage list of communicating sensor nodes ($C_{List}$)
Output Attribute: Route from SSN to DSN (R)
Start
Initialize Route as empty and broadcast RREQ
Set Destination Found Flag (DFF) ← not founded (0)
While DFF ← 0 do searching continue
    R (1) ← SSN and receive RREP
    R (2) ← Region nearest node which have maximum energy using algorithm 2
    R (3) ← Consider next sensor node
Repeat process until DFF ← 1
Next Node in R ← Coverage (Route (3))
If R (any) ← DSN
    DFF←1
    R (last) ← DSN
Else
    Process continue
End
Return: R as a Route from SSN to DSN
End
```

The route discovery through proposed SEETA routing is show in figure 4.

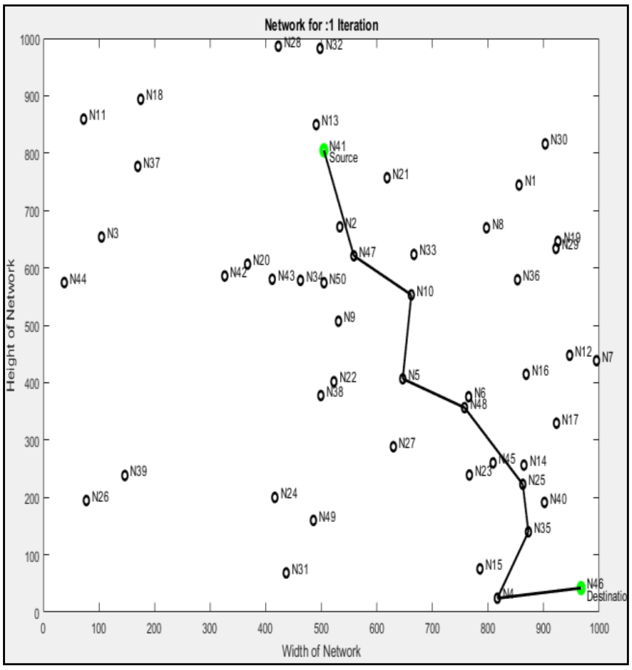


Figure 4: Flow of GOA-ANN based SEETA Routing Mechanism

SEETA is a secure energy efficient routing which helps in D2D communication scheme in IoT network. Discovery of a secure route is started when an IoT device directs a route request to the associated sensor nodes in the region of IoT network. SEETA routing protocol employed by the sensor node seeks to improve two key aspects in the route construction: route request broadcasting and reply of neighbouring selected node to minimize energy and end-to-end data rate maximization. It is similar to reactive routing protocol but to adopt the trust concept, PSO and ANN is used. In SEETA routing protocol, a secure route from sensor source node to destination sensor can be of two kinds reliant on their next of locations: intra-domain and inter-domain. When the communication under the purview of the identical region then it is entitled intra-domain and when under different region it is inter-domain.

D. Improvisation of Routing Mechanism

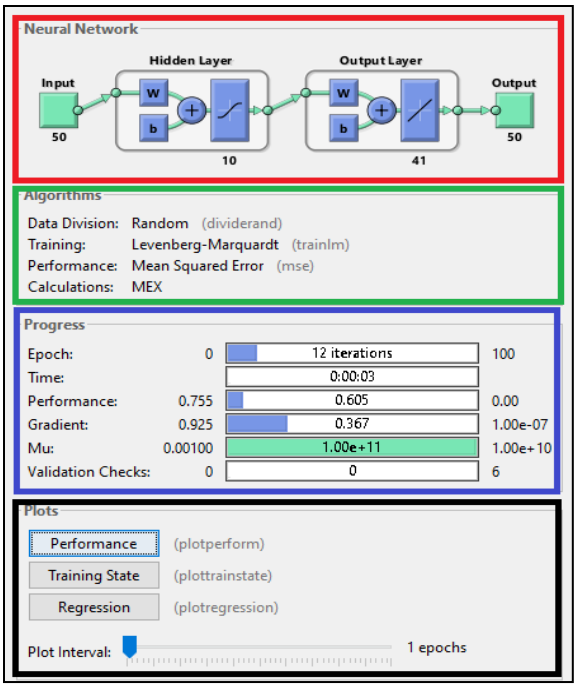
If performance in terms QoS of IoT network is degraded, then ANN with PSO is used to identify the fail/malicious node in IoT network during the data packets transmission. The combined hybrid algorithm of ANN with PSO which helps to make secure and trusted route is written follows:

Algorithm 3: Hybridization of PSO with ANN

```
Input Attributes: Number of nodes (N), Route (R) and Nodes Properties
Output Attributes: Secure and trusted route from SDN to DSN
Start:
1. Setup and call PSO initiator in simulator
2. Define basis parameters of PSO like
    Swarm size (S)
    Iterations (T)
    Lower Bound (LB)
    Upper Bound (UB)
    Fitness function
    Number of property selection (N)
3. Records ← IoT Network Sensor Node Properties
4. Fs ← Selected property value from the Records
5. Ft ←Threshold property value from the Records (Average of record's properties)
6. Define fitness function of GA using give equation (4)
    $Fit(f) = \begin{cases} True\ (1) & if\ fs \geq ft \\ False\ (0) & else \end{cases}$.... (4)
7. No. of variables ← N
8. for i in R's element do
9. F/M_Node (i) ← PSO (Fit (f), T, LB, UB, N)
10. End
11. Save the intermediate sensor nodes in the list of trusted table
12. for i in N do
13. Initialize ANN with parameters
    Epochs (E)
    Neurons (N)
    Performance parameters: MSE, Gradient, Mutation and Validation Points
    Training Techniques: Levenberg Marquardt (Trainlm)
    Data Division: Random
14. for each set of T
15. Group ← Categories of Training Data
16. End
17. Initialized the ANN using Training data and Group
18. Net ← Newff ($T, G, N$)
19. Set the training parameters according to the requirements and train the system
20. Net ← Train (Training Data, Group, Neurons) Classify the attackers
21. End
22. If properties of R (n) == true then
23.     Node considers in the route and trusted table and create a secure and trusted route
24. Else
25.     Node not considers in the route and trusted table
26. End
27. Calculate QoS parameters of IoT network
28. Return: Secure and trusted route from SDN to DSN with better QoS parameters
29. End
```

The ANN structure of proposed IoT model is shown in the figure 5 with their algorithms, progress and their graphical representations. After loading all node basic properties, training is performed using ANN algorithm. For all iteration, the sensor nodes properties is loaded and passed to the intermediate hidden layer and the weight of the nodes is adjusted as per the need, and then the property of nodes is passes to the output layer, where we obtained 2 number of output each corresponding to the different nodes attributes. The performance of ANN is examined on the basis of the following parameters.

- Mean Square Error (MSE)
- Gradient
- Mutation
- Validation


Neural Network
Hidden Layer
Output Layer
Input
Output
W
b
W
b
50
10
41
50

Algorithms

Data Division: Random (dividerand)
Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Calculations: MEX

Progress

Epoch:	0	12 iterations	100
Time:		0:00:03	
Performance:	0.755	0.605	0.00
Gradient:	0.925	0.367	1.00e-07
Mu:	0.00100	1.00e+11	1.00e+10
Validation Checks:	0	0	6

Plots

Performance (plotperform)
Training State (plottrainstate)
Regression (plotregression)

Plot Interval: 1 epochs

Figure 5: Training Architecture using ANN

Figures: 6 represent the training performance of ANN and figure: 6 (a) represents the plotting of the training based on mean square error as a performance parameters. Basically above figure: 6 (b) represents three types of graph used by ANN which is known as training state. In figure: 6 (b), first is gradient value of training which is presented by the blue color line, second is mutation of training data which is represented by the green color line and last is the used to adjust the input data according to the target of ANN. The best validation of data is represented by circle which is obtained after 12 iterations in figure: 6 (b) basically it is the validation fails during the training of IoT system. The minimum validation fails is 0 and the maximum validation fails is 6 in ANN and both gradient and validation fails represents the training status with respect to the epochs/iterations and there is total 12 iteration is used by ANN.

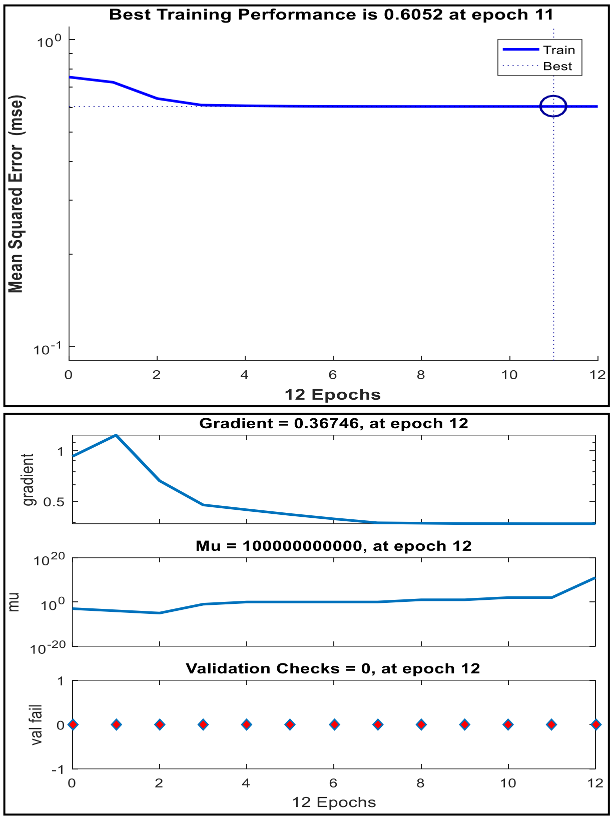


Figure 6: (a) Performance and (b) Training State

Identify nodes in discovered a secure and trusted route with detection of the fail/malicious node which is not able to communicate or misbehave in route with other nodes. If the fail/malicious nodes eliminated within the route, the consumed energy is reduces using the based on the PSO fitness function with ANN. At last of IoT network simulation, the QoS parameters of proposed work will be calculated and compare with exiting work in terms of Throughput, Loss Rate, Energy Consumption Rate, Number of Alive Nodes, End to End Delay and Detection Rate.

IV. SIMULATION RESULTS AND ANALYSIS

In this section, the simulation results of proposed IoT network with an optimized ANN for energy aware trust based secure routing protocol is discussed and the efficiency of proposed work is compared with existing work [1]. The simulation environment of the proposed work is shown in the table and the simulation results are described in the below section.

Table 1: Requirements of Proposed IoT Network

Number of Sensor Nodes	**50-200**
Area of IoT Network	**1000m^2**
Simulation Tool	**Communication Toolbox in MATLAB Software**
Routing Protocol	**Secure and Energy Efficient Trust Aware (SEETA)**
Optimizer	**Particle Swarm Optimization (PSO)**
Classifier	**Artificial Neural Network (ANN)**
Authentication Parameter	**Delay of transmission and Energy Consumption**
Evaluation Parameter	**Throughput, Loss Rate, Energy Consumption Rate, Number of Alive Nodes, End to End Delay and Detection Rate**

In this paper, swarm based algorithm optimize ANN is used as classifier to classify the malicious/fails nodes based on the optimized properties of communicating wireless sensor nodes in IoT network. In this section, the simulation results of proposed IoT network for D2D communication using SEETA routing protocol and optimized ANN for energy aware trust based secure routing protocol is discussed and the efficiency of proposed IoT network is compared with existing work [1] on the basis of energy consumption, loss rate and end to end delay. An IoT model with efficient routing protocol for emergency response is proposed in [1] and they used the concept of emergency based routing protocol to improve the performances of IoT network. The simulation environment of the proposed work is shown in the table and the simulation results are described in the below section. On the basis of the above mentioned scenario, the simulation results of proposed work with existing work [1] are given as:

Table 2: Throughput comparison of IoT Network

NO OF ROUNDS	EXISTING WORK [1]	PROPOSED WORK
1	86.64	98.62
2	84.80	97.06
3	83.12	95.16
4	82.96	93.53
5	80.44	91.72
6	74.92	89.38
7	60.64	83.05
8	69.85	69.56
9	55.72	61.92
10	41.59	54.24

In the perspective of optimized IoT networks, throughput is the complex measurement of the maximum amount of information data packet that may be transferred between T_x sensor node to R_x sensor node over a secure or trusted route.

Retrieval Number F8928088619/2019©BEIESP
DOI: 10.35940/ijeat.F8928.088619
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

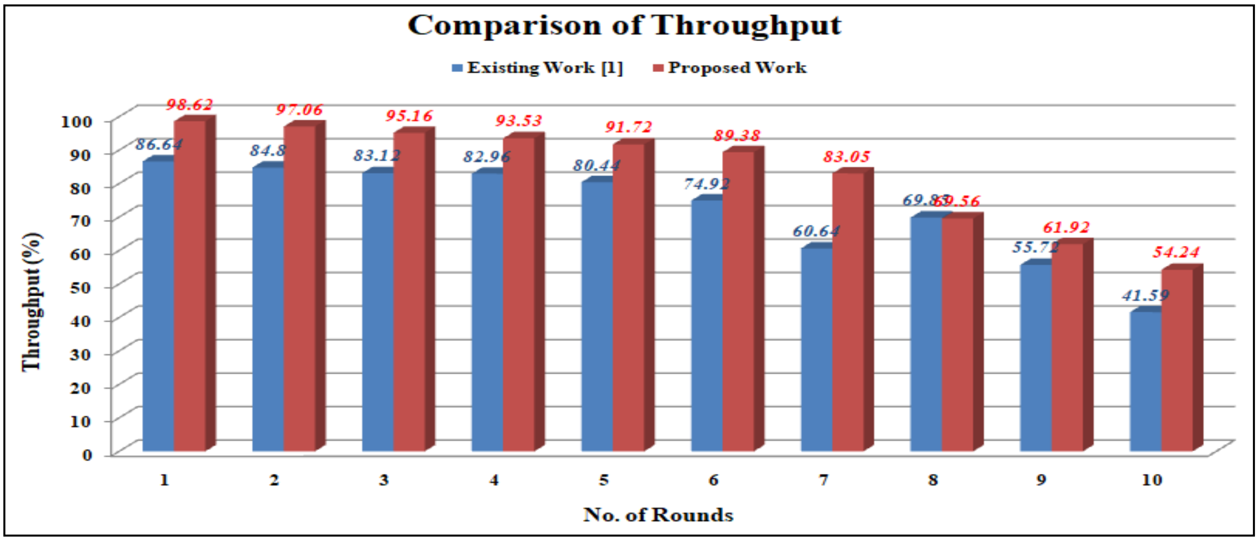


Figure 7: Comparison of Throughput for IoT Network

To calculate the throughput value given equation (6) is used for designed IoT network using SEETA routing protocol based on the optimized ANN.

$$\boldsymbol{Throughput} = \frac{\sum_{i=1}^{Sensor\ node}(DP_{Successful\ delivered})\times(DP_{AverageSize})}{DP_{SentTime}} \ldots\ldots (5)$$

Where, $DP_{\text{Successful delivered}}$ is the successful data packet with respect to each communicating nodes, $DP_{\text{AverageSize}}$ is average data packet size and DP_{SentTime} is total time taken by nodes to sent data packets. The obtained throughput of the designed IoT network is shown in figure 7 with the comparison table 2 between proposed and existing work [1]. In the figure, x-axis defines the number of simulation rounds and Y-axis defines the obtained throughput values measured for improved ERGID routing protocol. Red line represents the obtained throughput value measured of proposed IoT network. From the above comparative graph it is clear that the throughput value measured for the IoT network with proposed SEETA routing protocol is higher than existing technique and it is possible by integrating the PSO based ANN as classifier.

Table 3: E2E Delay comparison of IoT Network

No of Rounds	Existing Work [1]	Proposed Work
1	6.866	3.759
2	7.746	4.353
3	8.755	4.356
4	8.755	5.742
5	9.754	6.013
6	10.663	6.753
7	10.764	7.653
8	12.75	8.564
9	13.76	9.55
10	15.27	10.664

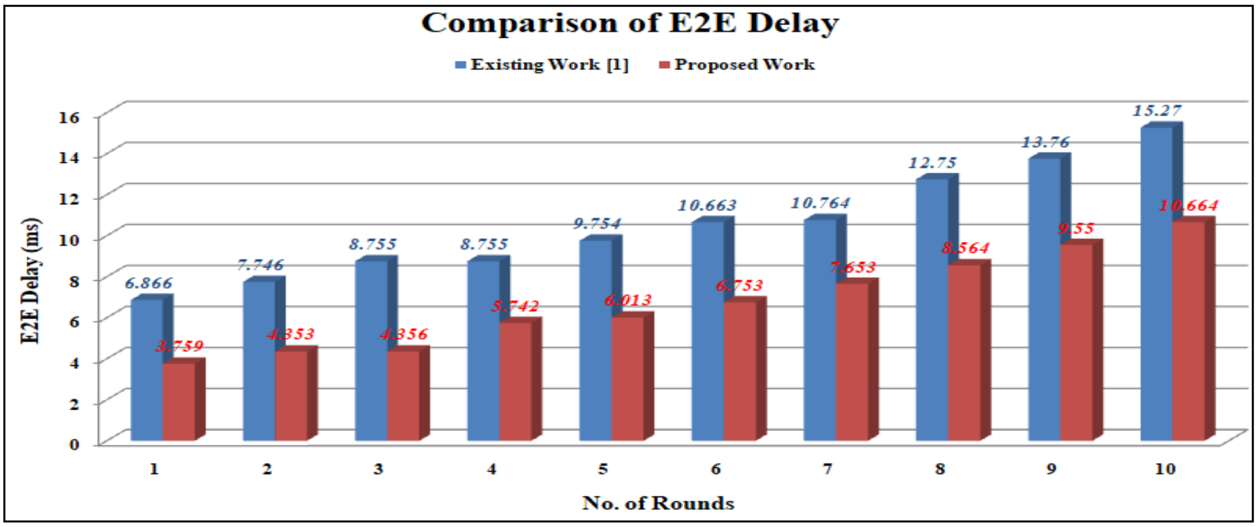


Figure 8: Comparison of E2E Delay for IoT Network

The end to end delay value of proposed IoT network is the summation of each and every one types of time consumption for the duration of the packet data transmission. To calculate the end to end delay value of proposed work given equation is used.

$$\boldsymbol{E2E - Delay = \sum_{i=1}^{Sensornode} T_t + R_t + W_t} \; ..... (6)$$

Where, T_t is the time consumed by nodes during packet data transmission time, R_t is the time consumed by nodes packet data receiving and W_t is the waiting time for each nodes. The end to end delay for packet data transmission in the proposed IoT network is shown in figure 8 with comparison table 3 between proposed and existing work [1]. In graph, the blue and red line defines the obtained value of end to end delay for existing and improved SEETA routing protocol. The end to end delay by using improved SEETA with the hybridization of PSO and ANN is less than of existing routing protocol.

Table IV: Loss rate comparison of IoT Network

No of Rounds	Existing Work [1]	Proposed Work
1	2.9	2.6
2	3.4	2.9
3	4.8	2.95
4	4.2	3.1
5	5.2	3.9
6	5.3	4.1
7	6.1	4.8
8	7.3	5.3
9	8.3	6.6
10	9.2	6.9

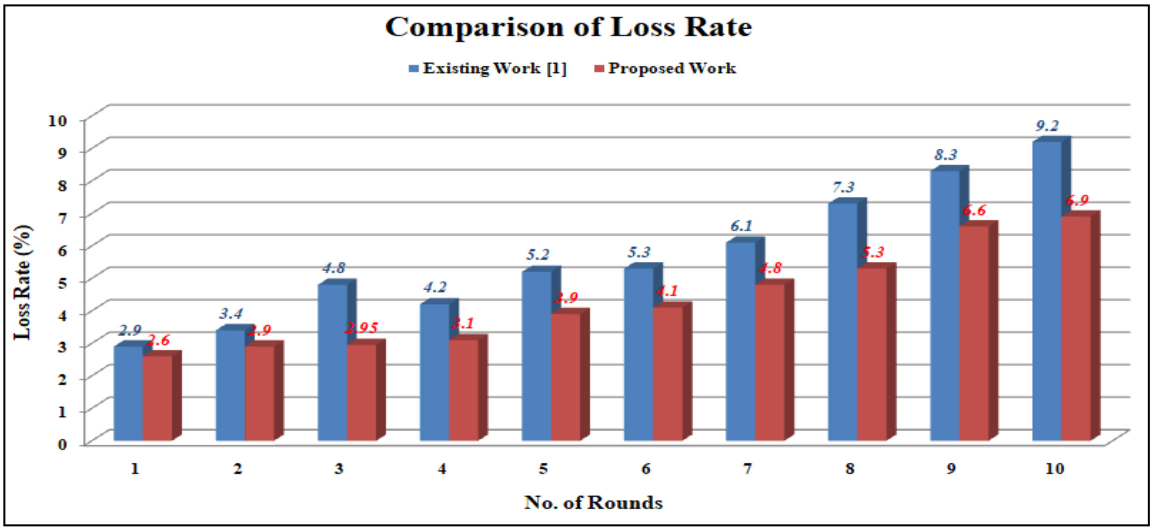


Figure 9: Comparison of Loss Rate for IoT Network

Loss rate is the result of two sensor nodes on the same network attempting to transmit a data packet at closely the same instance. The IoT network become aware of the "collision of sensor nodes" for the two transmitted data packets and discards them both. Loss rate is a usual incidence in any IoT network. The loss rate value of the proposed IoT network is shown in figure 9 with comparison table 4 between proposed and existing model [1]. In graph, two types of bar first is blue and second is red which defines the loss rate value measured for existing work and improved SEETA routing protocol using the combination of PSO and ANN. The loss rate of IoT network by using proposed algorithm is reduces and it is a great improvement.

Table 5: Energy consumption comparison of IoT Network

No of Rounds	Existing Work [1]	Proposed Work
1	62	38
2	141	69
3	211	84
4	481	116
5	911	765
6	2411	2054
7	2631	2422
8	3911	3818
9	4811	4455
10	5211	5132

Retrieval Number F8928088619/2019©BEIESP
DOI: 10.35940/ijeat.F8928.088619
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

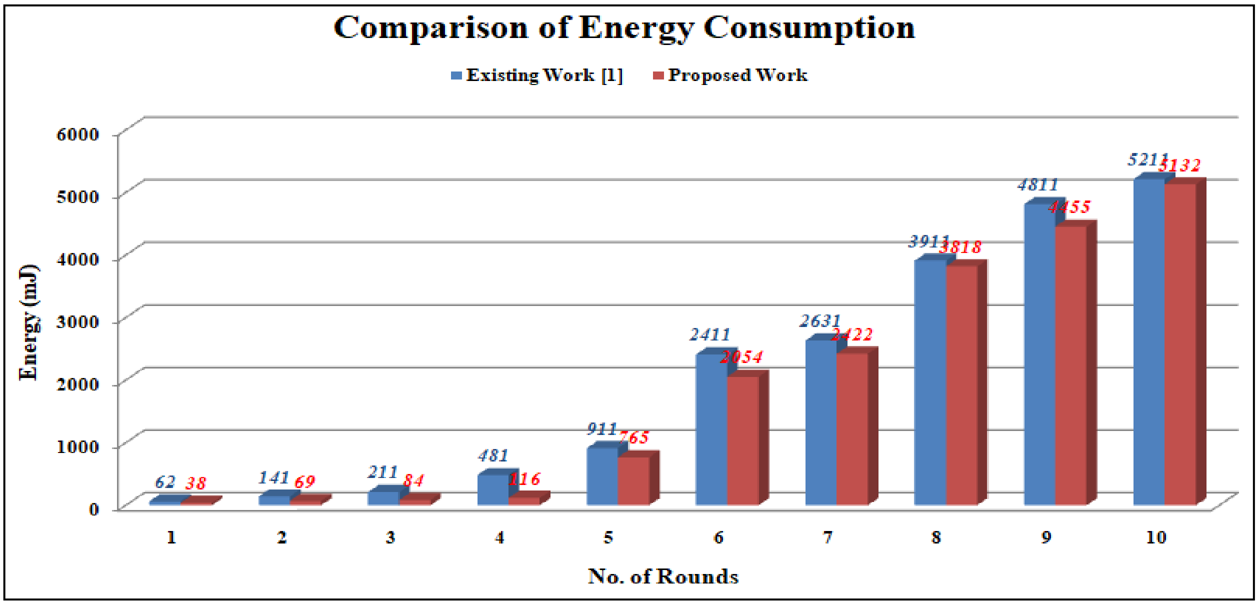


Figure 10: Comparison of power consumption

Above mentioned parameters evaluates the energy efficiency of our proposed SEETA routing protocol. It is calculated as totality energy consumed in an IoT network per data packet successfully delivered to destination sensor node and formula of energy/power consumption is written as:

$$\boldsymbol{E_C} = \sum_{i=1}^{Sensornode} \boldsymbol{T_E} + \boldsymbol{R_E} + \boldsymbol{W_E} \text{ .... } (7)$$

Where, T_E is the whole summation of energy consumed by sensor node during the packet transmission in IoT network, R_E is the total amount of energy consumption by sensor node during the packet receiving by receiver sensor node and W_E is the waiting energy consumption rate which consumed by sensor nodes during waiting to receive a data packets. Figure 10 represents the comparison of energy consumption rate by the sensor nodes in IoT network during the transmission of data packets from source to destination sensor node with comparison table 5 between proposed and existing work [1]. From the above figure, we observe that the rate of energy consumption is reduce by 8.74% using SEETA protocol using the hybridization of PSO and ANN is less as compared to the existing routing protocol. The QoS performance comparison of proposed IoT network with SEETA routing mechanism based on the PSO and ANN as a classifier is described in below section with simulation results. In this comparison we assumed three different routing mechanisms such as ERGID (Emergency Response IoT based on Global Information Decision), SPEED (Spectrum aware energy efficient routing for device-to-device), EA-SPEED (Spectrum aware energy efficient routing for device-to-device) and SEETA

Table 6: Comparison Of Delay Based On Different Routing Algorithms

NO OF ROUNDS	SPEED	EA-SPEED	ERGID	SEETA
1	11.716	9.289	6.866	3.759
2	12.814	10.387	7.746	4.353
3	13.405	10.978	8.755	4.356
4	13.907	11.481	8.755	5.742
5	14.906	12.479	9.754	6.013
6	15.815	13.388	10.663	6.753
7	15.916	13.489	10.764	7.653
8	17.902	15.475	12.75	8.564
9	18.912	16.485	13.76	9.55
10	20.152	17.725	15.27	10.664

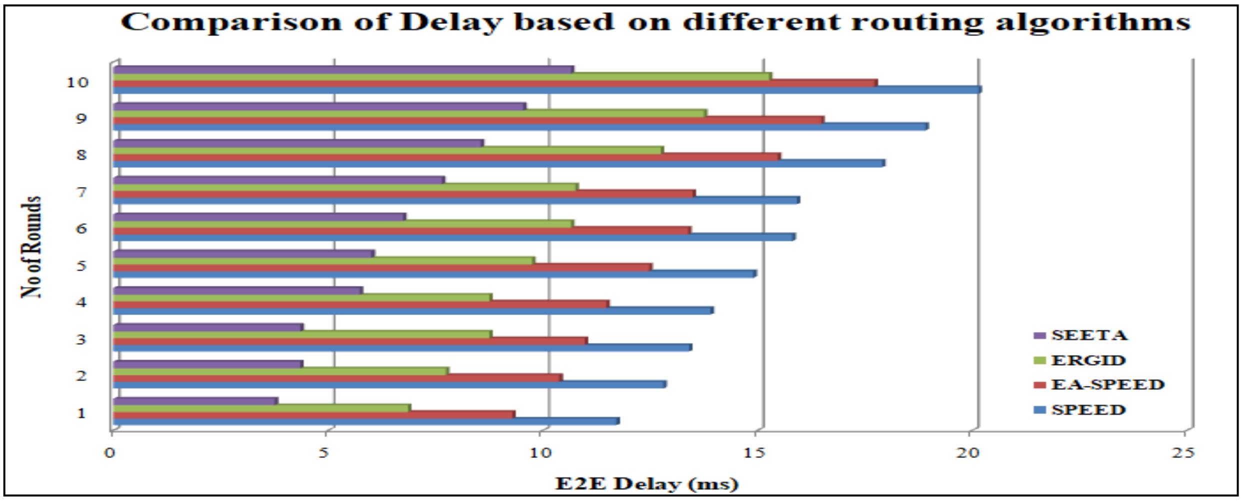


Figure 11: Comparison of Delay based on different routing algorithms

In the figure 11 with table 6, the comparison of existing routing protocol with proposed SEETA routing mechanism is given and from the figure it is clear that the delay for data packets transmission is less by using the concept of ANN along with PSO algorithm as compare to the others.

Table 7: Comparison of loss rate based on different routing algorithms

NO OF ROUNDS	SPEED	EA-SPEED	ERGID	SEETA
1	7.235	7.142	2.9	2.6
2	8.939	8.657	3.4	2.9
3	10.835	9.549	4.8	2.95
4	12.856	10.567	4.2	3.1
5	12.996	11.497	5.2	3.9
6	13.667	11.848	5.3	4.1
7	14.638	12.342	6.1	4.8
8	16.978	15.345	7.3	5.3
9	21.435	20.142	8.3	6.6
10	27.235	25.947	9.2	6.9

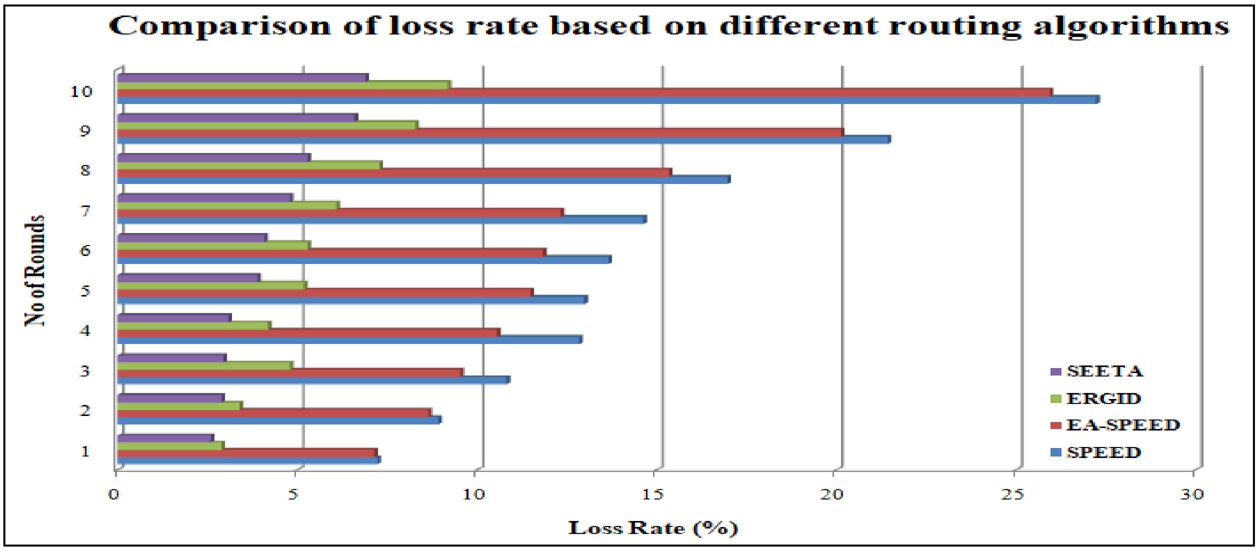


Figure 12: Comparison of Packets Receiving Rate based on different routing algorithms

In the figure 12 and table 7, the comparison of existing routing protocols with proposed SEETA routing mechanism is given and from the figure it is clear that the rate of packets loss is less by using the concept of ANN along with PSO algorithm as compare to others routing protocols like SPEED, EA-SPEED and ERGID.

Table 8: Comparison of Energy Consumption based on different routing algorithms

No of Rounds	SPEED	EA-SPEED	ERGID	SEETA
1	140	117	62	38
2	219	196	141	69
3	289	266	211	84
4	559	536	481	116
5	989	966	911	765
6	2489	2466	2411	2054
7	2709	2686	2631	2422
8	3989	3966	3911	3818
9	4889	4866	4811	4455
10	5289	5266	5211	5132

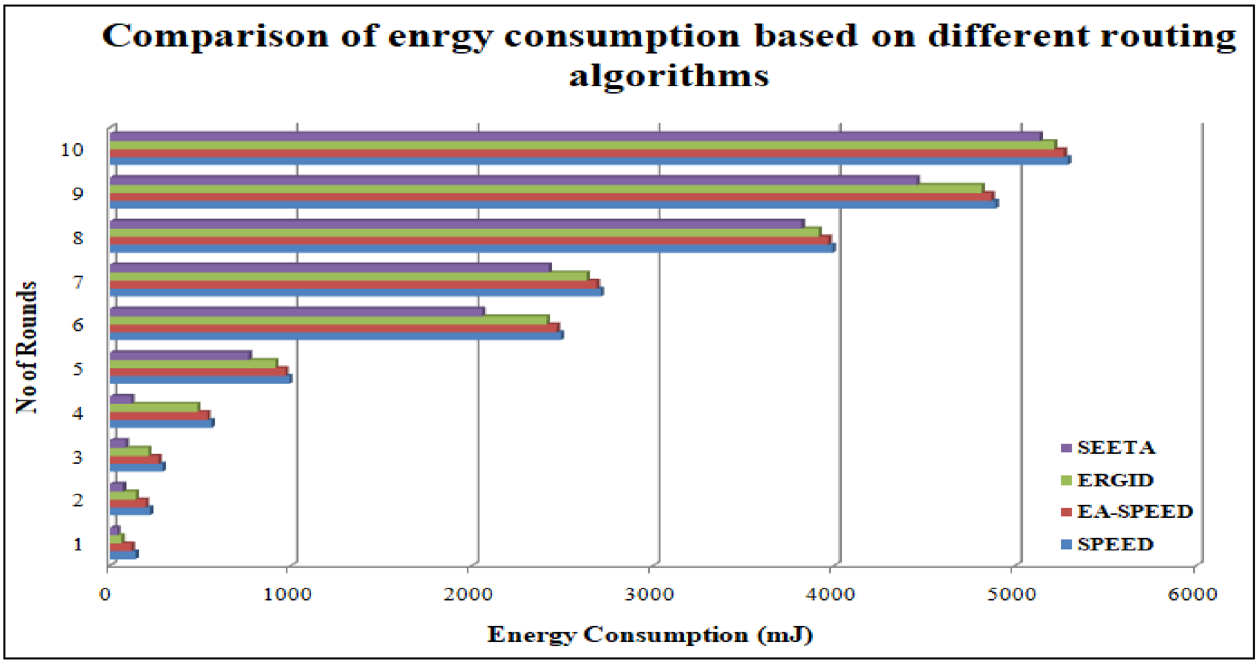


Figure 13: Comparison of Energy Consumption based on different routing algorithms

In the figure 13 and table 8, the comparison of energy consumption rate between existing routing protocol and proposed SEETA routing mechanism is given and from the figure it is clear that the energy consumption rate is less by using the concept of ANN along with swarm intelligence technique PSO algorithm as compare to others routing protocols.

V. CONCLUSION AND FUTURE WORK

In this paper, a secure and energy efficient trust aware routing protocol in IoT using the optimized artificial neural network is proposed which is known as SEETA-IoT network. We have analyzed our proposed SEETA routing mechanism using the hybridization of PSO and ANN as classifier with respect to the other routing algorithms on different parameters IoT network. We focus on efficient security and trust based data dissemination issues and proposed an optimized SEETA routing protocol using of PSO and ANN with help of a novel fitness functions. Descriptive IoT network results point toward the proposed D2D routing scheme effectively improves the system performance in terms of QoS parameters. In addition, the proposed SEETA routing protocol helps to transmit data packets with secure and trusted route which achieves significant improvements in energy efficiency. Based on the experimental observations, we can conclude that energy consumption of ERGID routing protocol [1] is 8.74% more than proposed PSO-ANN based SEETA routing mechanism as routing protocol which is best among exiting work in the survey section.

Retrieval Number F8928088619/2019©BEIESP
DOI: 10.35940/ijeat.F8928.088619
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

In future work, the concept of deep learning will be used as a classifier to train IoT network based on encryption mechanism with optimization algorithms which may be applicable for fast random behavior of nodes within the network for secure and trusted communication.

REFERENCES

1. Qiu, Tie, et al. "ERGID: An efficient routing protocol for emergency response Internet of Things." Journal of Network and Computer Applications 72 (2016): 104-112.
2. Debroy, Saptarshi, et al. "SpEED-IoT: Spectrum aware energy efficient routing for device-to-device IoT communication." Future Generation Computer Systems (2018).
3. Pan, Meng-Shiuan, and Shu-Wei Yang. "A lightweight and distributed geographic multicast routing protocol for IoT applications." Computer Networks 112 (2017): 95-107.
4. Ishino, Masanori, Yuki Koizumi, and Toru Hasegawa. "A study on routing-based mobility management architecture for IoT devices." 2014 IEEE 22nd International Conference on Network Protocols (ICNP). IEEE, 2014.
5. Otermat, Derek T., Carlos E. Otero, and Ivica Kostanic. "Analysis of the FM radio spectrum for Internet of Things opportunistic access via cognitive radio." Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on. IEEE, 2015.
6. Huang, Jun, et al. "Multicast routing for multimedia communications in the Internet of Things." IEEE Internet of Things Journal 4.1 (2017): 215-224.
7. Hasan, Mohammed Zaki, and Fadi Al-Turjman. "Optimizing multipath routing with guaranteed fault tolerance in Internet of Things." IEEE Sensors Journal 17.19 (2017): 6463-6473.
8. Feng, Zhiyong, et al. "Priority-based dynamic spectrum management in a smart grid network environment." IEEE Journal on Selected Areas in Communications 33.5 (2015): 933-945.
9. Khan, Athar Ali, Mubashir Husain Rehmani, and Martin Reisslein. "Requirements, design challenges, and review of routing and MAC protocols for CR-based smart grid systems." IEEE Communications Magazine 55.5 (2017): 206-215.
10. H. Bogucka, P. Kryszkiewicz, A. Kliks, Dynamic spectrum aggregation for future 5g communications, IEEE Commun. Mag. 53 (5) (2015) 35–43.
11. L. Cheng, B.E. Henty, D.D. Stancil, F. Bai, P. Mudalige, Mobile vehicle-to-vehicle narrow-band channel measurement and characterization of the 5.9 GHz dedicated short range communication (DSRC) frequency band, IEEE J. Sel. Areas Commun. 25 (8) (2007) 1501–1516.
12. Z. Feng, Q. Li, W. Li, T.A. Gulliver, P. Zhang, Priority-based dynamic spectrum management in a smart grid network environment, IEEE J. Sel. Areas Commun. 33 (5) (2015) 933–945.
13. O. Younis, L. Kant, A. Mcauley, K. Manousakis, D. Shallcross, K. Sinkar, K. Chang, K. Young, C. Graff, M. Patel, Cognitive tactical network models, IEEE Commun. Mag. 48 (10) (2010) 70–77.
14. Sergey Balandin, Sergey Andreev, YevgeniKoucheryavy, Internet of Things, Smart Spaces, and Next Generation Networks and Systems: 15th International Conference, NEW2AN 2015, and 8th Conference, ruSMART 2015, St. Petersburg, Russia, August 26–28, 2015, Proceedings, in: Lecture Notes in Computer Science, Springer International Publishing, 2015.
15. Fujdiak, Radek, et al. "Using genetic algorithm for advanced municipal waste collection in Smart City." 2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP). IEEE, 2016.

a. Abbagnale, F. Cuomo, Gymkhana: A connectivity-based routing scheme for cognitive radio ad hoc networks, in: INFOCOM IEEE Conference on Computer Communications Workshops, March 2010, pp. 1–5.

16. Hodo, Elike, et al. "Threat analysis of IoT networks using artificial neural network intrusion detection system." 2016 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2016.
17. Geng Cheng, Wei Liu, Yunzhao Li, Wenqing Cheng, Spectrum aware on demand routing in cognitive radio networks, in: New Frontiers in Dynamic Spectrum Access Networks, DySPAN. 2nd IEEE International Symposium on 2007, pp. 571–574.
18. K.R. Chowdhury, M.D. Felice, Search: A routing protocol for mobile cognitive radio ad-hoc networks, Comput. Commun. J. 32 (18) (2009) 1983–1997.
19. Filippini, E. Ekici, M. Cesana, Minimum maintenance cost routing in cognitive radio networks, in: Mobile Adhoc and Sensor Systems, MASS. IEEE 6th International Conference on, 2009, pp.284–293.
20. Pefkianakis, S. Wong, S. Lu, SAMER: Spectrum Aware Mesh Routing in Cognitive Radio Networks, in: New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on, 2008, pp. 1–5.

AUTHORS PROFILE

Balwinder kaur has completed her B.tech(I.T),M.Tech(CSE) and now pursuing Ph.D from Sant Baba Bhag Singh University and working as Assistant Professor in Lyallpur Khalsa college for women.She has Published 9 paper in National and International Journals. Recently went to Canada for conference Women Deliver 2019 in Vancouver convention centre as a Delegate.She is also a cerified trainer of oracle.

[2]**Dr Rattan K Datta** had his Ph.D from IIT-Delhi on "Monsoon Dynamics & Atmospheric Modeling".
Dr Rattan K. Datta was Adviser,DST, Govt. of Indiaand During Monsoon Experiment (MONEX-79) he was the chief scientist to coordinate the scientific experimentation and data management.
He has contributed over 125 research papers. He was UN expert on data processing & Meteorological Advisor. He had been national president of CSI, Indian Meteorological Society andPresident IT section of ISCA.
Awards: Gold medal for best research paper in 1975, Life time achievement award by Ministry of Earth sciences on 9th Dec,2008& "The Lifetime Achievement Award" in the field of IT by Computer Society of India (CSI).