A Trust Aware Based Predictive Model using Hybrid Convolutional Neural Network for Mobile AD HOC Network in Internet of Things

Balwinder Kaur Dhaliwal, Rattan K Datta

Abstract: ***Mobile ad-hoc networks (MANETs) are inescapable independent Wireless Sensor Networks (WSNs) that will assume a fundamental job in upcoming trends of Internet-of-Things (IoT) communication, somewhere sharp-witted gadgets will a tendency to associated in a totally scattered manner. The IoT is a type of wireless heterogeneous network of different types such as WSNs, MANETs, Zig-Bee, WI-FI, and RFID. So a trust based routing in MANET based IoT network is a difficult task for better Device to Device (D-2-D) communication. Be that as it may, because of the absence of framework and the nonappearance of concentrated administration in MANETs, networks are covered with different security threats. Some inward mobile sensor nodes in these positive feature based obliged wireless networks may bargain the routing mechanism in order to attacks to do unmistakable sorts of the data packet sending mischievous activities.***

Methods: In order to address this type of IoT communication issue, in our previous research paper, we devised a routing protocol in IoT based on the secure and energy efficient trust aware approach using the Particle swarm based (PSO) Optimized Artificial Neural Network (ANN), it is used to classify the packet dropping adversaries before the transmission by supervising the intermediates communicating sensor nodes nature to discover route and their maintenance period. But the achieved result should be better by using the concept of Convolutional Neural Network (CNN) with PSO instead of ANN. In this paper, we perform sensitivity analysis of IoT communication using Secure and Energy Efficient Trust Aware (SEETA) routing mechanism with PSO based optimized CNN and it is used to identify the unlike parameters variation in distinctive scenarios in the existence of data packet dropping attacks or malicious nodes. Also the proposed work recapitulates the trusted route discovery mechanism with their maintenance process where routing is based on our existing SEETA protocol with the purpose of countering the certain attack or malicious patterns along with optimized CNN.

Results: Simulation is conducted with MATLAB based network simulator which indicates the correct choices of parameter values for proposed IoT network scenarios. When the QoS constraints of IoT network is calculated and compared with various existing approaches, the proposed PSO based CNN with SEETA routing mechanism achieves the better performance of 99.31% in terms of data delivery rate with reduction of 16.76% in energy consumption rate as compare to exiting works.

Conclusion: During simulation of proposed IoT network based on different network conditions, we observed that the achieved performance is best in terms of Energy Consumption with Throughput and Loss Rate. After that we also obtained the achieved transmission delay is less and Alive Nodes Count is more with maximum Detection Rate.

KEYWORDS: — Mobile ad-hoc networks, Internet of Things, Secure and Energy Efficient Trust Aware (SEETA), Particle Swarm Optimization (PSO) Algorithm, Convolutional Neural Network (CNN), Quality of Service (QoS.)

I. INTRODUCTION

After the accomplishment of Zig-Bee, Cellular network and Wi-Fi technologies in the communication field in preceding two consecutive decades, Internet-of-Things (IoT) network [1], [2] & [3] based wireless communication has been converted into a well-liked approach to communication in people's everyday existence. Ad-Hoc networks [4] have developed in a substantial and quick route because of expanded need of taking out fixed framework, topographical reliance and multifaceted nature of organization for basic applications, for example, IoT, military activities, fiasco alleviation the executives, sea communications, wise transportation frameworks, untamed life observing, wellbeing checking and some more. Mobile ad-hoc networks (MANETs) based IoT for Device to Device (D-2-D) communication [5] is shown in the figure .

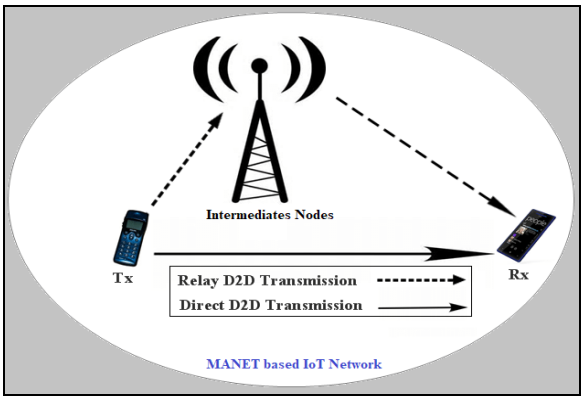


Figure 1: MANET based IoT Network

A MANET based IoT network is such a self-directed and centralized distributed network of mobile sensor nodes that hold up the communication without any wired medium (wireless medium) in the environment with geographical self-determination and spontaneous deployment [6]. An IoT network is formed from such a MANET which accede to the virtues of wireless communication standard alike litheness, well-organized power resource exploitation and enhanced discovered route manageability.

Revised Manuscript Received on July 22, 2019.

Balwinder kaur , Assistant Professor in Lyallpur Khalsa college for women.
Jalandhar panjab india.
Dr Rattan K. Datta, Adviser,DST, Govt. of India

Designed network can provide wireless utility by excessive utilizing the available power resources in the mobile sensor nodes.

At individual level, whereas wireless technologies are altering the digital communication globe with high level protection, has still remained as a major concern for cyber protection. Owing to the intrinsic and selfness nature of MANETs with dynamic routing topology, power resource constraints, and restricted communication choice get an innovative protection challenges for IoT based applications together with additional challenges alike quality-of-service (QoS) enhancement [7], power resource supervision, dependability and scalability with trusted routing concept [8]. Secure routing mechanism in MANET based IoT networks has been one of the most important concerns for academic as well communicational researchers like the conservative routing protocols intended for these networks imagine cooperative trusted setting amid the mobile sensor nodes.

Inspiration & Contributions: MANET based IoT network is the evolution of internet pretentiousness enormous challenges in wireless network and their analysis with distribution towards a more security in use of information transmission in order to improve the quality of communication. The concept of MANET based IoT involves the management of sensors nodes or electronics devices distributed around the communicating network [9], so as to recognize and notify abnormal users instantly in networks. So, existing IoT network faced a major problem of trust in routing mechanism for secure and fast data transmission within the network. From these types of challenging routing task, we present a trust aware model for MANET in IoT network utilizing hybridization of Particle Swarm Optimization (PSO) based Convolutional Neural Network (CNN). In simple words, this research forms the ensuing offering.

- We used Secure and Energy Efficient Trust Aware (SEETA) routing mechanism for data packet transmission in IoT network.
- We developed a hybrid routing mechanism using the PSO based optimized CNN to manage and maintain network security with maximum trust.
- In addition, to train the designed MANET based IoT network, PSO based CNN classifier is used which helps to classify the attackers or malicious nodes in the network.
- At the end phase of simulation, a relative study is done to authenticate the QoS execution parameters of network based on earlier and presented work.

To the best of our knowledge, SEETA is the first routing scheme to manage trust in MANET based IoT network which attempts to classify the attack or malicious nodes during the route discovery procedure. The used scenario of IoT network is useful in various IoT based applications which are shown in the figure 2.

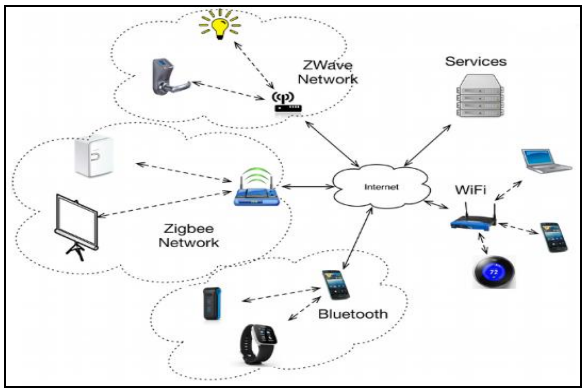


Figure 2: Application of IoT Network

The rest of this research paper is planned in the following sequences:

In Section II, further we discuss routing mechanism in the existing MANET based IoT network.

In Section III, we summarize the IoT network implementation methodology based on the SEETA routing protocol using optimized CNN.

In Section IV, we present the simulation results of IoT network and their analysis based on the QoS performance parameters such as loss rate with consumption of energy, throughput, number of alive nodes, delay and detection rate of attack or malicious nodes.

In Section V, Finally, the conclusion and future scope will discuss.

II. BACKGROUND SURVEY

In this segment, we introduce the analysis of presented routing mechanism for IoT network based on artificial intelligences. ***Balwinder Kaur Dhaliwal and Rattan K. Datta [1]*** had proposed secure and vitality proficient trust mindful steering convention in IoT utilizing the upgraded counterfeit neural. To locate a safe and essentialness beneficial course, we proposed a trust-based approach with PSO with ANN. In this investigation, we focused on the security improvement of the IoT framework using trust-based course upkeep part. The Quality of Service execution parameter of our controlling show is examined using previously presented work with a couple of coordinating shows and the exploratory results affirming improved ANN. The test outcomes demonstrate that the exhibited SEETA coordinating show gives 8.74 percent take away imperativeness use pace and tall data transport datum and pace movement pace is enhanced by 92% like diverge from leaving workings anyway the blend of upgrade computations with CNN, fitting for speedy sporadic direct of centers inside the framework for secure and trusted in correspondence. ***Tie Qiu et al. [2]*** had organized an IoT associate with beneficial guiding show for emergency response which is known as Emergency Response IoT reliant on Global Information Decision (ERGID). They proposed ERGID directing show to enhance the displays of strong data package conduction and powerful desperate condition answer in IoT arranges. Particularly, they introduced a Delay Iterative Method (DIM) framework that relies upon concede assessment, to decide the issue of disregarding material as well as considerable courses within the systems.

Furthermore, to modify heap of IoT sorts out, Residual Energy Probability Choice (REPC) is projected by centering upon the waiting imperativeness of passing on the sensor center points. Multiplication results as well as assessment of proposed IoT framework show that organized ERGID guiding show is superior than anything EA-SPEED and SPEED with respect to QoS parameters, for instance, from beginning to end (E2E) delay, bundle hardship and imperativeness usage. Limited information guiding decisions regularly lead to the visual impedance of secure course decision with the objective that essentialness uses is far above the ground for gigantic data groups. ***Saptarshi Debroy et al. [3]*** improved a test framework for destination to destination correspondence in IoT as well as examined the obstacles of vibrant based partner controlling show for IoT organize. They proposed SpEED controlling part through a variety cautious, vivacity ground-breaking multi-channel multi-skip organizing system amongst IoT equipment contraptions with center points of sensor. A power control based conduction explicit inundating approach is projected within this work to widen the course difficulty inside the system with no causing structure wide conduction overhead. They look into the framework situation amongst IoT devices utilizing these types of techniques. Moreover, there may analyze the donation of their projected course of action in cooperation theoretically and likely for different essential circumstances and IoT deals with like outfitted range, fundamental conduction traits, expand properties, and assorted elective IoT device association method/limits. In any case, they do not wear down safety instrument along with conduction time. ***Meng Shiuan Pan and Shu-Wei Yang [3]*** in 2017 showed a insubstantial and scattered geographic-centered multicast controlling show on behalf of IoT applications. Their essential target had to lessen the amount of communication associates along with condensed path lengths in the created multicast ways. The planned arrangement holds a requesting stage, a turnaround bring up to date organizes, plus a change organizes. within the requesting stage, center points locally find the base number of next skip centers to touch base at objective centers. By then, in pivoted renovate phase and change stage, multicast customs can more cut and met through the arranged procedure. The multiplication plus preliminary outcomes exhibit that the planned arrangement can enough reduce the amount of program associations and program hinders simultaneously, they can be alter their arrangement on the way to aid core adaptableness and their safety. ***Ishino et al. [4]*** in 2014 showed a lightweight and spread geographic-centered multicast controlling show on behalf of IoT applications. They planned the versatile controlling structure utilizing the Bloom Filters in favor of the IoT applications, moreover later than that has cleared up the reasonableness of our planning structure. In like manner, they had demonstrated that their coordinating structuring is able to trim down the level of channels to by and large once requisite gathering development rates are around 0.9. These sorts of issue continually looked as a result of the researcher in the area of IoT centered correspondence in addition to deal with out these issues better option is the decision of improved classifiers meant for coordinating segment as a directing show using PSO with ANN.

From the above analysis, we concluded the most recent and accurate CNN as classifier is the best option. So, SEETA routing protocol with PSO-CNN mechanism is used for improvement in routing by withdrawing not permitted attacker or malicious nodes from route then regard as in the routing table intended for trust awareness which show that our experimental results is better. To corroborate the effectiveness of proposed model based on their efficiency, the concept of SEETA protocol of proposed model is compare with another author research work as well as our previous work.

III. WORKING MANET BASED IoT

PSO-CNN based SEETA routing mechanism is proposed in this research which consists of several steps. Below section define the procedures to implement an IoT network for the simulation of model and procedural steps are:

A. Architecture of MANET based IoT

With the help of the MATLAB based-Graphical User Interface (GUI), we create a MANET based IoT simulator which is considered as a platform for simulation of proposed SEETA routing mechanism with PSO based CNN as a classifier for secure and trusted route establishment. The area of proposed MANET based IoT network is considered by utilizing specified equation:

$$Area\ of\ MANET\ based\ IoT\ Network,$$
$$\mathcal{A} = \mathcal{H}\ X\ w \quad \ldots\ldots. (1)$$

Where, Height of network is consider as $\mathcal{H}$, Width of network is w

In the model, $\mathcal{H}$ and w is considere as 1000m. Therefore, total communication area fof network is $1000m^2$ that is satisfactory scenario for manipulating purpose. IoT framework with MANET structure which is designed for simulation using few number of sensor nodes is demonstrate in figure 3.

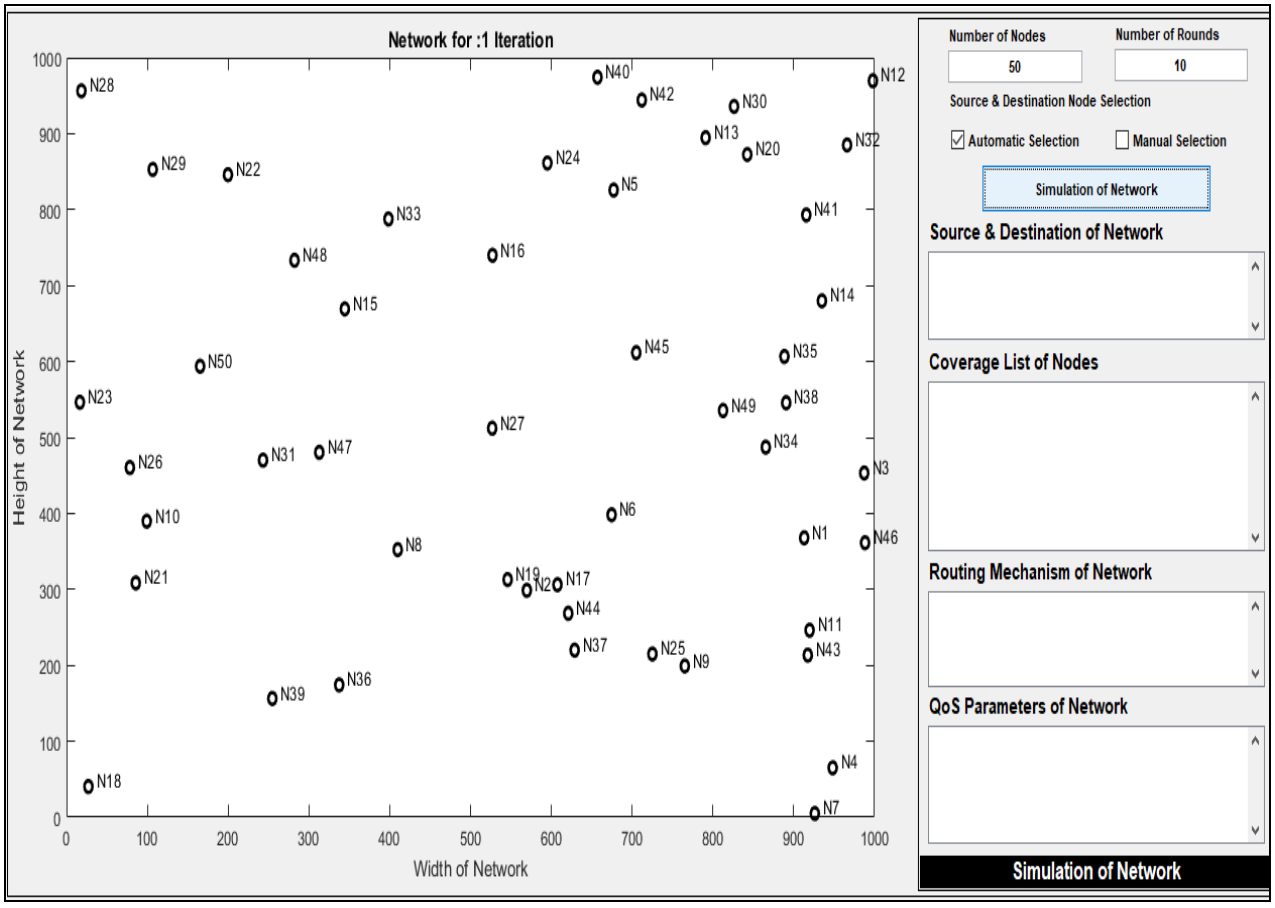


Figure 3: Designed MANET based IoT Network

Above figure represents the designed model of MANET based IoT network which is implemented in MATLAB software using the GUI concept. In the figure, we deploy total 50 numbers of nodes for the simulation purpose and after that a route is created using the SEETA routing mechanism for secure and trustworthy data transmission from source to destination nodes and the MANET based IoT network deployment algorithm is written as:

1st Algorithm: Deployment of MANET based IoT Network

Input-Attributes: N — Sensor Nodes
H — Height of N/W
W — Width of N/W

Output-Attributes: Deployed MANET based IoT Network for simulation purpose

Start:
Define N/W Height, 1000 ← H
Define N/W Width, 1000 ← W
Compute total IoT network area (A) utilizing equation 1

1. for each N do
2. X-coordinate ← Random multiple of A
3. Y- coordinate ← Random multiple of A
4. Sensor Deployment ← Coordinate (X- coordinate, Y-coordinate)
5. Assign name for nodes ←N where N = N_1, N_2, N_3…N_n
6. Source node as T_X ← Select (N_1, N_2, N_3…N_n)
7. Destination node as R_X ← Select (N_1, N_2, N_3…N_n)
8. **Check similarity, if T_X == R_X then**
9. Source node as T_X ← Repeat again step 6
10. Destination node as R_x ← Repeat again step 7
11. **Else**
12. Source node as T_X ← T_X
13. Destination node as R_X ← R_X
14. **End**
15. **Construct MANET based IoT Network**
16. Deploy N in N/W
17. **End**
18. End
19. Return: Deployed MANET based IoT Network for simulation purpose
20. End

The deployed MANET based IoT Network for simulation purpose with source T_X and destination R_X sensor nodes is shown in figure 4.

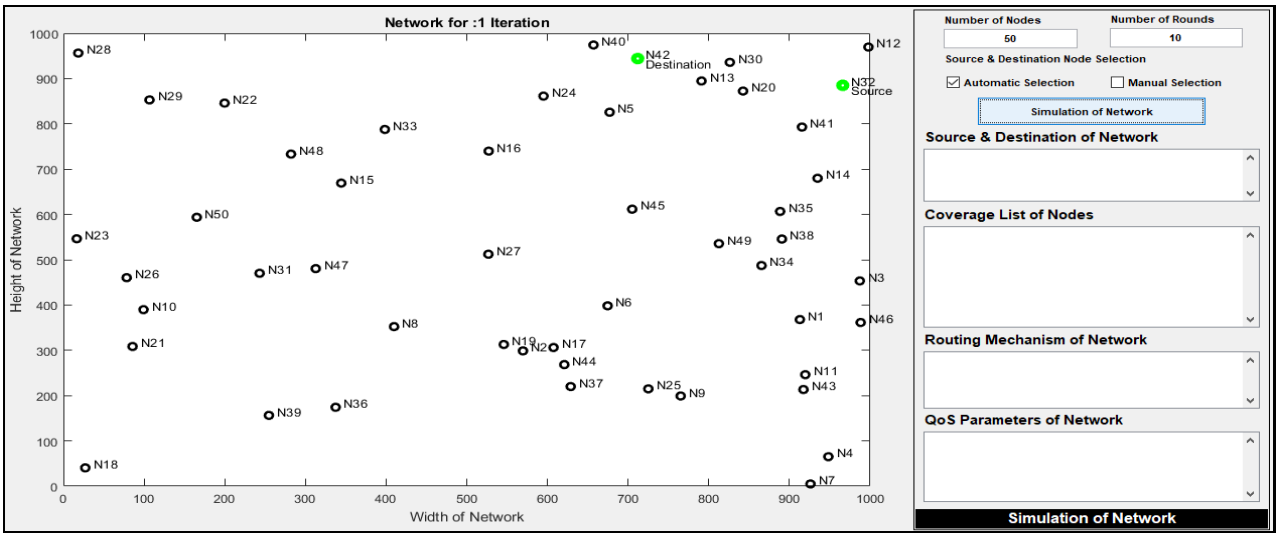


Figure 4: Designed MANET based IoT Network with T_X and R_X node

B. Coverage limit determination of nodes

After the IoT network deployment, we calculate the coverage area with their limited transmission range for each sensor node for the establishment of route from source node (T_X) to destination node (R_X) utilizing SEETA routing mechanism with PSO and CNN. The coverage area determination algorithm is written as:

2nd Algorithm: Coverage Area Determination

Input-Attribute: N — Sensor Nodes
A — Area of IoT Network
Output-Attribute: C_{List} — Coverage area with nodes as list of communication

Start:

1. Set Limit:

$$Coverage_{Limit}, (C_L) = \frac{(25 \times A)}{100} \ldots. (2)$$

2. for each N do with respect to i
3. for each N do with respect to j
4. If N(i) ≠ N(j) then
5. Using distance formula in equation (3)

$$N2N - Dist = \sqrt{((X_j - X_i)^2 + (Y_j - Y_i)^2)} \ldots. (3)$$

We calculate limit of coverage of nodes
6. End
7. If N2N-Dist < C_L then
8. C_{Set} (i, j) ← N2N-Dist
9. C_{List} (i, j) ← N
10. End
11. End
12. Return: C_{List} as output
13. End

C. Routing Mechanism: SEETA

After the coverage limit and set calculation, a secure route is required for data transmission, so SEETA routing protocol is used for the D-2-D communication in MANET based IoT network. Basically in our previous paper we mentioned SEETA routing mechanism is a better manner and also in this paper we explain the algorithm of SEETA routing protocol is written follows:

3rd Algorithm: Routing Protocol SEETA

Input-Attribute: SSN — Source Sensor-Node
DSN — Destination Sensor-Node
C_{List} — Coverage area with nodes as list of communication
Output-Attribute: R — SSN to DSN Route

Start

1. Consider a variable for Route (R) as an empty array and broadcast RREQ
2. Define DFF ← not founded (0) // as a destination found flag
3. Start routing: While DFF ← 0 do
4. R (1st) ← SSN which transmit RREQ
5. R (2nd) ← Region nearest N which have maximum energy using algorithm 2
6. R (3rd) ← Next N
7. Do again until 1←DFF
8. Next N in R ← Coverage Range (R (3rd))
9. If R (N) ← DSN, (Check)
10. DFF←1
11. R (Last N) ← DSN
12. Else
13. Continue searching
14. End
15. Return: R as an output
16. End

Based on the above mentioned route discovery algorithm SEETA we construct a route which is show in figure 5 with a route from T_X to R_X.

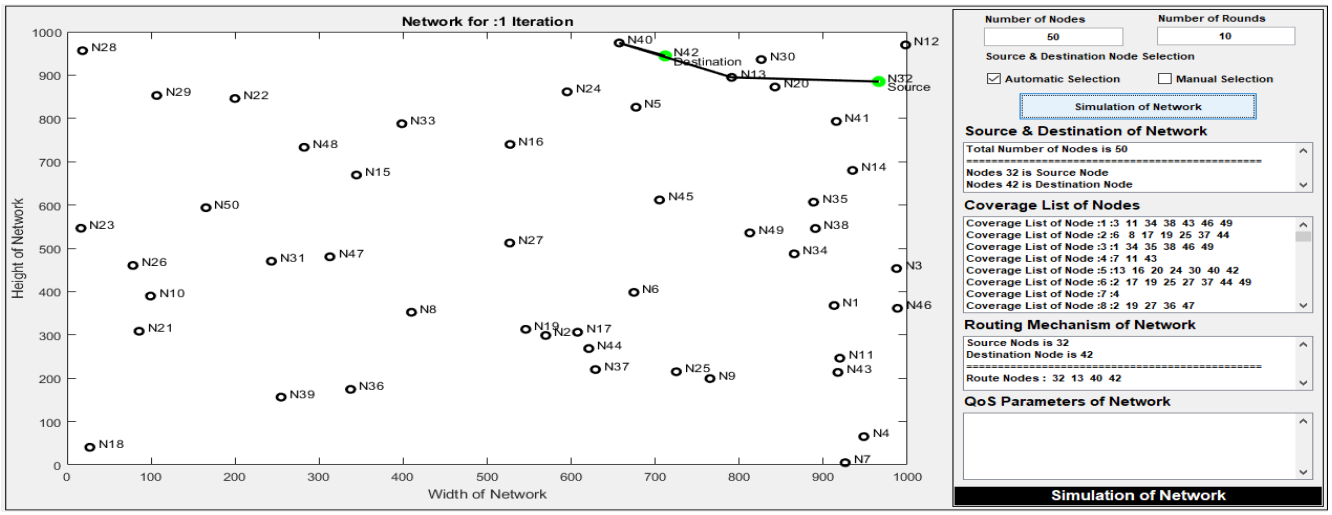


Figure 5: T_X to R_X Route using SEETA Routing Mechanism

D. Routing Optimization

After the simulation of IoT network using SEETA routing mechanism tf presentation in terms QoS is degraded, then we apply CNN with hybridization of PSO as a optimization approach to improve the network efficiency as compared to the our previous work. Optimized CNN is utilized to make out the attack/malicious nodes in MANET based IoT network during the T_X to R_X packets transmission. The route optimization algorithm is written as:

4th Algorithm: Hybridization of CNN with PSO

Input-Attributes: N — Sensor Nodes & Properties
R — SSN to DSN Route
Output-Attributes: ST-R — Secure and trusted route

Start:

1. PSO initialization
2. PSO operators are defined like
- S← Size Particle Swarm
- T← Searching Iterations
- LB←Define a bound for lower data
- UB← Define a bound for upper data
- FF← Fitness/Objective function
- N← Feature selection count

3. Records ← N Properties
4. Fs ← Selected Records
5. Ft ←Threshold Records (Mean of record's Features)
6. Define FF of PSO using give equation (4)

$$FF(f) = \begin{cases} 1\ (True) & if\ fs \geq ft \\ 0\ (False) & else \end{cases} \quad \ldots (4)$$

7. No. of variables ← N
8. for each R do with respect to i
9. Attack/Malicious_N (i) ← PSO (FF (f), T, LB, UB, N)
10. End
11. Accumulate the intermediary N in the catalog of TT (Trusted Table) as Training Data (T)
12. for i in N do
13. CNN is initialized with parameters
- Training Epochs (E)
- Training Neurons (N)
- Training Performance parameters: Cross entropy, Gradient and Validation
- Training Techniques: Scaled Conjugate Gradient (Trainscg)
- Training Data Division: Randomly

14. for each set of T with respect to j
15. G (j) ← T Categories
16. End
17. CNN training parameters setting using T and G
18. IoT-Net ← Patternnet (N)
19. Set the CNN parameters in proportion to network necessities
20. IoT-Net ← Train (T, G, N) and categorize the attackers
21. End
22. If properties of R (N) == 1 then
23. ST-R = R (N)
24. Else
25. ST-R = X
26. End
27. Determine QoS parameters of MANET based IoT network
28. Return: ST-R with better QoS parameters as an output
29. End

The architecture of CNN-Structure which is used in proposed MANET based IoT model is publicized in the figure 6 with their used training algorithms

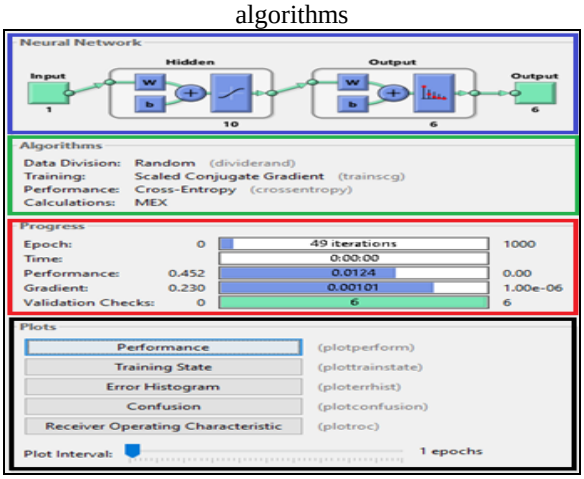


Figure 6: CNN Training Architecture

The performance of PSO based CNN is examined on the basis of the following parameters which is shown in below figures.

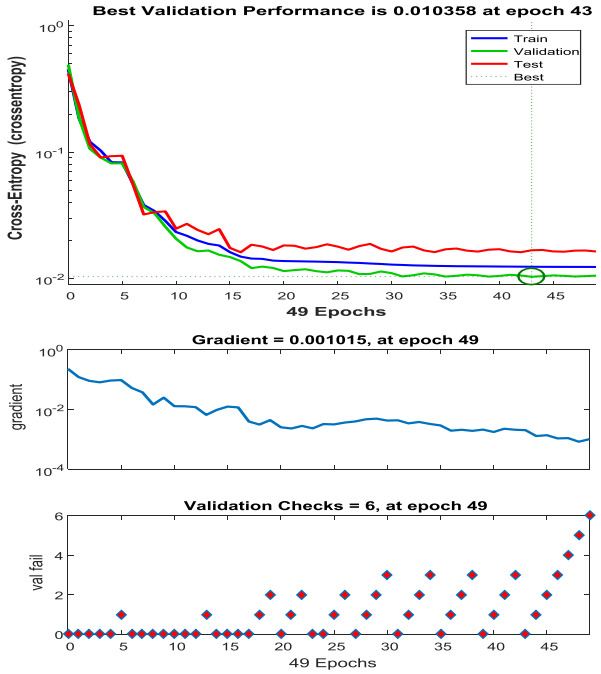


Figure 7: (a) Training Cross-Entropy and (b) State of Training

Above figure 7 (a) and (b) represents the training performances of PSO based CNN and Training Cross-Entropy of CNN is shown in figure (a) where figure (b) shows that training state with gradient and validation fails represented during the training of IoT network in terms of graphically representation.

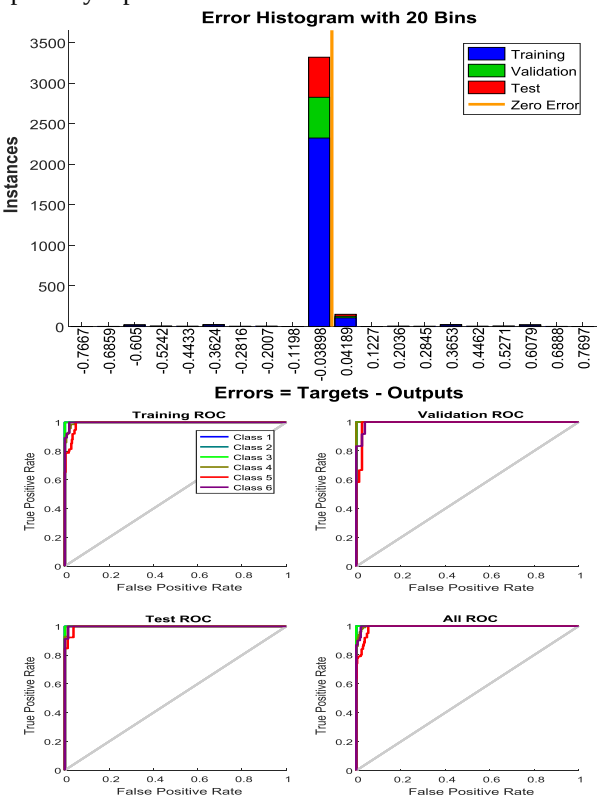


Figure 8: (a) Error Histogram and (b) ROC

Figure 8 (a) speaks to the histogram error containers and the absolute mistake that has been estimated for the PSO based CNN during analysis is lies between - 0.7667 (furthest left receptacle) to 0.7697 (furthest right canister). Where, figure 8 (b) speaks to the ROC bend with four unique information types, for example, preparing, testing, approval and blend of all.

IV. SIMULATION RESULTS AND ANALYSIS

In this section, analysis of results for MANET based IoT network with an optimized CNN using PSO for secure and trust aware routing protocol is discussed and the efficiency of proposed work is compared with our previous existing work [1]. The MANET based IoT network simulation environment is defined in the table 1.

Table 1: MANET based IoT Requirements

Number of Sensor Nodes	**50-200**
IoT Network Area	**1000m^2**
Simulation Tool	**Curve fitting, Deep learning and Communication Toolbox in MATLAB Software**
Routing Mechanism	**Secure and Energy Efficient Trust Aware (SEETA)**
Optimization Algorithm	**PSO**
Classifier	**Convolutional Neural Network (CNN)**
Parameter fro Node Validation	**E2E Delay and Energy utilization for transmission**
Evaluation QoS Parameter	**Same as [1]**

In this research paper, we present a swarm based algorithm optimize CNN which is the improvement of our previous work to classify the attack/malicious nodes based in IoT network. The simulation results of IoT network for D-2-D communication using SEETA routing protocol with optimized CNN is discussed and the efficiency of proposed IoT network is compared with our previous work [1] which is better than the other existing work on the basis of energy consumption, loss rate and end to end delay. On the basis of the above mentioned scenario, the simulation results of proposed work with our previous work [1] are given as:

Table 2: IoT Network Throughput Comparison

No of Rounds	Previous Work [1]	Proposed Work
1	98.62	99.32
2	97.06	99.11
3	95.16	98.26
4	93.53	96.29
5	91.72	94.82
6	89.38	93.28
7	83.05	90.42
8	69.56	84.92
9	61.92	73.27
10	54.24	69.23

In the perspective of optimized MANET based IoT networks, throughput rate is the multifaceted capacity of the maximum amount of information data packet transmission rate between T_X to R_X over a secure or trusted route.

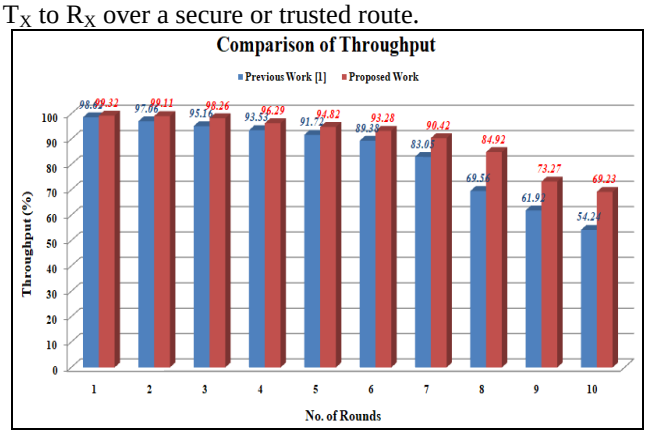


Figure 9: IoT Network Throughput Comparison

Above figure 9 represents the IoT network throughput comparison with the comparison table 2 between proposed and our previous work [1]. X-axis of figure 9 defines the number of simulation rounds where Y-axis defines the obtained throughput values measured for proposed and previous work. Red line represents the obtained throughput value measured of proposed MANET based IoT network. It is clear that the throughput of proposed MANET based IoT network is better as compare to our previous by integrating the PSO with CNN instead of ANN as classifier.

Table 3: IoT Network E2E Delay Comparison

No of Rounds	Previous Work [1]	Proposed Work
1	3.759	2.434
2	4.353	3.134
3	4.356	3.542
4	5.742	4.533
5	6.013	5.551
6	6.753	5.973
7	7.653	6.874
8	8.564	7.245
9	9.55	8.856
10	10.664	9.244

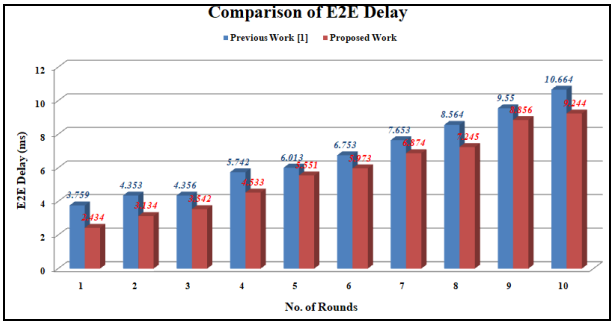


Figure 10: IoT Network Comparison of E2E Delay

The end to end delay for packet data transmission in the proposed MANET based IoT network is shown in figure 10 with table 3. The blue and red line defines the obtained value of end to end delay for our previous and proposed work in above graph. The end to end delay by using hybridization of PSO and CNN is less than of existing work with hybridization of PSO and ANN.

Table IV: Loss rate comparison of IoT Network

No of Rounds	Previous Work [1]	Proposed Work
1	2.6	1.2
2	2.9	2.2
3	2.95	2.3
4	3.1	2.7
5	3.9	2.9
6	4.1	3.3
7	4.8	4.2
8	5.3	4.8
9	6.6	5.3
10	6.9	5.9

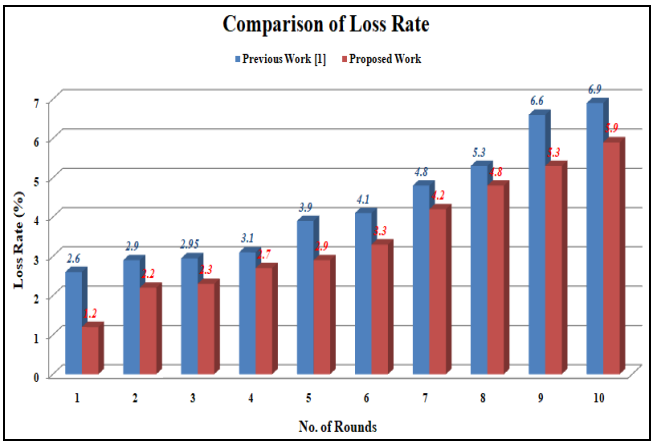


Figure 11: IoT Network Comparison of Loss Rate

The data packet loss rate comparison of the proposed MANET based IoT network is shown in figure 11 with table 4. In graph, comparison is shown with two types of bar first is blue and second is red which defines the loss rate value measured for our previous work proposed work using the combination of PSO and CNN. The loss rate of IoT network by using proposed algorithm is reduces and it is a great improvement.

Table 5: IoT Network Energy Consumption Comparison

No of Rounds	Previous Work [1]	Proposed Work
1	38	23
2	69	43
3	84	53
4	116	75
5	765	423
6	2054	1651
7	2422	2133
8	3818	2534
9	4455	4176
10	5132	4664

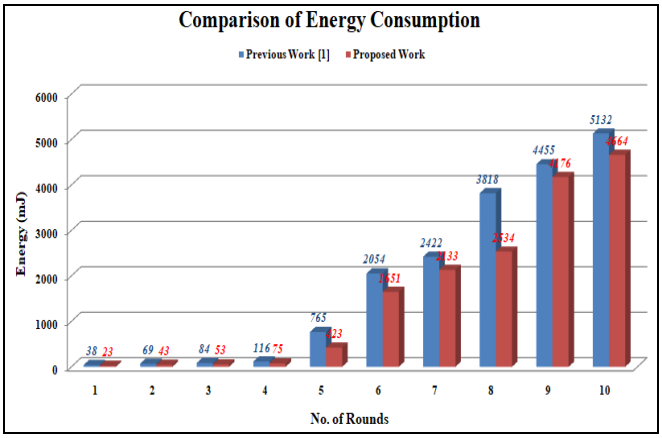


Figure 12: Comparison of power consumption

Figure 12 and table 5 represents the comparison of energy consumption rate by the sensor nodes in MANET based IoT network during the transmission of data packets from T_X to R_X. From the figure 12, we observe that the rate of energy consumption is reduce by 16.76% using SEETA protocol using the hybridization of PSO with CNN is less as compared to the our previous work.

V. CONCLUSION AND FUTURE WORK

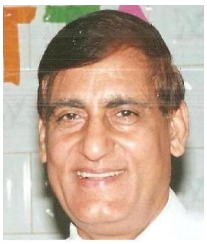
In this research manuscript, a trust aware based predictive model using hybrid CNN for MANET in IoT network is proposed and we use our previous routing mechanism which is known as SEETA. We have analyzed our proposed optimized CNN based SEETA routing mechanism with respect to our previous optimized ANN based SEETA routing mechanism routing on different QoS parameters of MANET-IoT network. Basically in this research we utilize the concept of deep learning instead of ANN with PSO because the training and classification capability of CNN is far better than ANN. We focus on security of IoT network with a trust based data dissemination issues using of PSO with CNN using a unique and novel fitness functions. Explanatory MANET based IoT network results point toward the proposed hybrid SEETA routing scheme effectively improves the network QoS performance in terms of energy consumption and data transmission. Based on the experimental observations after the simulation of IoT network, we concluded that energy consumption of proposed hybrid SEETA routing protocol is reduce by the 16.76% as compare to our previous work. In future work, the concept data encryption method could be used with deep learning to train IoT network with hybridization optimization algorithms.

REFERENCES

1. B. Kaur Dhaliwal and Rattan K. "Datta Secure and Energy Efficient Trust Aware Routing Protocol in IoT using the Optimized Artificial Neural Network: SEETA-IoT" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2252 – 8965, Volume-8 Issue-6, August, 2019.
2. 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.
3. Debroy, Saptarshi, et al. "SpEED-IoT: Spectrum aware energy efficient routing for device-to-device IoT communication." *Future Generation Computer Systems* (2018).
4. Pan, Meng-Shiuan, and Shu-Wei Yang. "A lightweight and distributed geographic multicast routing protocol for IoT applications." *Computer Networks* 112 (2017): 95-107.
5. 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.
6. 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.
7. Huang, Jun, et al. "Multicast routing for multimedia communications in the Internet of Things." *IEEE Internet of Things Journal* 4.1 (2017): 215-224.
8. 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.
9. 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.
10. 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.
11. H. Bogucka, P. Kryszkiewicz, A. Kliks, Dynamic spectrum aggregation for future 5g communications, IEEE Commun. Mag. 53 (5) (2015) 35–43.
12. 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.
13. 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.
14. 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.
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.
16. I. 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.
17. I. 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.
18. 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

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.



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).