Proceedings of the International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT 2023)
IEEE Xplore Part Number: CFP23CV1-ART; ISBN: 978-1-6654-7451-1

2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) | 978-1-6654-7451-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/IDCIoT56793.2023.10053398

Machine Learning based Secure Data Transmission and Improvement in MANET through Internet of Things (IoT)

G Dinesh[1]
Department of Computational Intelligence, School of Computing, SRM Institute of Science and Technology,
Chennai, Tamil Nadu, India.
dineshg@srmist.edu.in

Yogesh Shivaji Pawar[2]
Department of Electrical Engineering, Bhabha University
Bhopal, Madhya Pradesh, India.
ysp.logmieer@gmail.com

P Dinshi[3]
Department of Computer Science Engineering, Koneru Lakshmaiah Educational Foundation,
Guntur, Andhra Pradesh,India
dinshidinu@gmail.com

Soundararajan S[4]
Department of Computer Science and Engineering, Velammal Institute of Technology,
Chennai, Tamil Nadu, India.
soundar07@gmail.com

S Syed Husain[5]
Department of Electronics and Communication Engineering, K.Ramakrishnan college of Engineering,
Tiruchirappalli, Tamil Nadu, India
apsyedhusain@gmail.com

Ch. Venkata krishna reddy[6]
Department of Electrical and Electronics Engineering, Chaitanya Bharathi Institute of Technology,
Hyderabad,Telangana, India.
Chkrishnareddy_eee@cbit.ac.in

***Abstract*—The term MANET stands for Mobile Ad hoc Network. MANET is a structure of wireless communication network that is combined with various nodes that are movable in various directions in the network. They are accompanied with the absence of infrastructure which helps the nodes to interconnect with the neighboring one in a random fashion. They are highly dynamic in nature. The internet of things device have the ability to communicate with the various heterogeneous networks. These IoT nodes helps to communicate with each other without the need of infrastructure. The cloud helps to store the data and tends to transmit through the nodes in the network. The secure data transmission includes the intrusion detection system, neglecting malicious attacks and selfish nodes in the network. The secure data transmission system without any constraints helps in the improvement of overall efficiency of the system. This is done through the machine learning accompanied with genetic algorithm. These biologically inspired algorithms helps to obtain exact optimum solutions helps to provide secure data transmission.**

Keywords—Mobile Ad hoc network (MANET), wireless communication system, heterogeneous network, selfish nodes, Internet of Things (IoT), machine learning, genetic algorithm

I. INTRODUCTION

The MANET is composed of mobile nodes which are interconnected with each other through wireless medium in the absence of infrastructure [1]. They are used in versatile applications such as military, navy and medical applications. This helps to obtain bidirectional communication system. This does not influenced by any other pre-existing infrastructure or any other form of wireless network. In these systems the nodes itself acts as a routers and the host system in the network [2].

These absence of infrastructure does not communicate on the wired network. The information in the networking system are done through the nodes which are transmitted through the neighboring nodes in the network. The nodes carry information and leads to transfer through the neighboring nodes in the system [3]. These information are sensed through the sensors in the network. They are done through gathering and processing the data in the system [4]. These systems are independent in nature. The MANET is composed with no access points which are aligned themselves in the systems. These MANETS are highly movable and mobile in nature [5]. The malicious attacks cause various constraints in the system due to various flexibility in the networking system. The various constraints in the system leads to decrease in the overall efficiency of the networking system [6]. To enhance secure data transmission in the communication network, Intrusion Detection System (IDS) is implemented. This tends to detect the malicious attacks in the network that lends to enhance the secure data transmission in the network. It does not consist of any form of datasets [7]. The further classification and rectification is done through the control room which records the transfer of information in the networking system. The neglecting process of malicious attacks in the networking system leads to increase the efficiency of the system [8].

The malicious attacks include grey hole attack, black hole attack and wormhole attack. The various disturbances in the communication network are termed as the attacks in the networking system. They are more common that occurs in the system. These constraints are need to be neglected in order to avoid various consequences in the networking system and to improve the performance of the system [9]. The most frequent attack happens in the network are the grey hole attack. The dropping of packets in the malicious nodes are termed as the attacks in the network. The consequences in the networking system are needed to be solved in a particular period of time so that to improve the performance of the networking system without any interruption [10].

Thus the machine learning with biologically extracted genetic algorithm are helpful in neglecting the constraints and helps in secure data transmission in the networking system [11]. They are formulated through the human intelligence which leads the machine to perform as

similar to humans by training and testing process. They are done through analyzing the data through processing them in the hidden nodes which leads to produce the exact optimum solution.

II. PROPOSED SYSTEM

In the wireless communication system, the data transmission must be done through secure way without any interruptions. The interruptions in the communicating system leads to decrease in the overall performance of the networking system. The cloud storage system helps to store the overall data for further references.

The occurrence of various attacks leads to various collapse in the system. They are obtained through a trust management system. The prior threshold values helps to implement the trust management system. The various constraints in the system are avoided through the machine learning process. This helps to obtain an optimum solution through training and evaluation of the data in the network. This includes numerous input to process in the hidden layer to produce the exact output. This is implemented through the genetic algorithm. It helps to transmit the information in the networking system through secure data transmission through neglecting the malicious behavior. Thus the major objective of the system is to improve the performance of the system by neglecting the constraints occurred in the malicious nodes in the system.

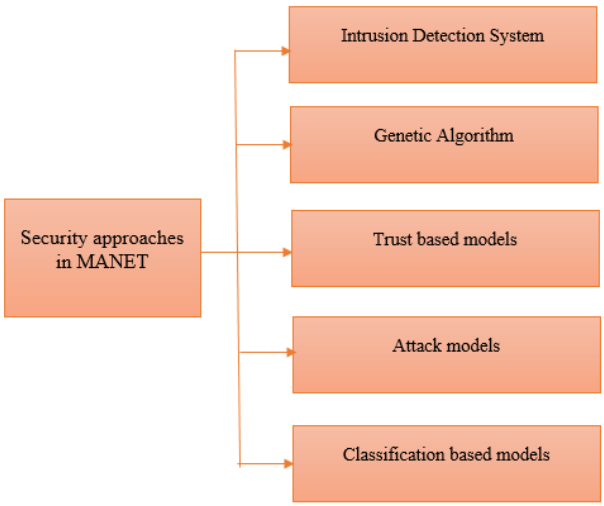

Fig 1: Security approaches in MANET

The figure 1 represents the security approaches in MANET. This involves the Intrusion Detection System (IDS), genetic algorithm, trust based models and attack models.

(i) Intrusion detection System (IDS)

The crowd in the networking system is detected through the Intrusion Detection System (IDS). This indicates the suspicious activities in the network. The malicious behaviour of the nodes in the networking system are referred in the intrusion detection software system. This helps to analyze the harmful attacks in the system. The event management system represents the overall functioning of the system. The input parameter is integrated with the output parameter through filtering for the odentification of malicious activities in the networking system.

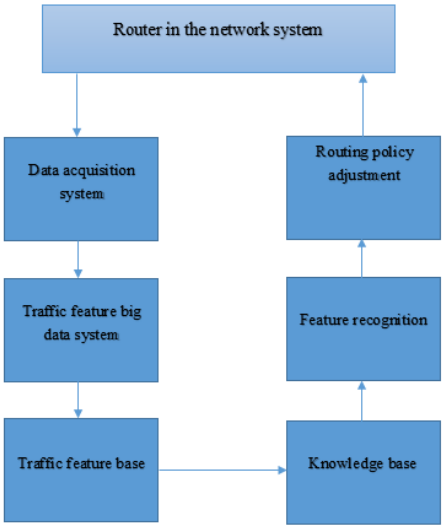

Fig 2: Intrusion Detection System (IDS)

The figure 2 represents the Intrusion Detection System (IDS). This is a depicted as a defense mechanism system that helps to identify and monitor the suspicious activities in the networking system. This helps to analyze the various constraints caused by the malicious attacks in the nodes in the networking system. These malicious attacks are caused due to the nature of the infrastructure which are highly movable in nature [12]. Due to highly flexible infrastructure, various attacks are done. Thus the intrusion detection system software is need to integrated with the networking system so that to filter the unlicensed access in the system. This is done through the machine learning accompanied with the genetic algorithm. The machine learning helps to identify various threats in the networking system [13].

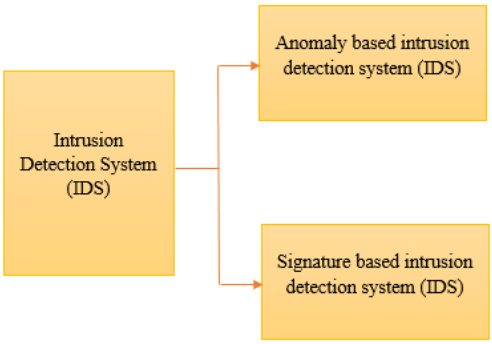

Fig 3: Classification of IDS

The figure 3 demonstrates the classification of Intrusion Detection System (IDS). This includes the anaomaly and signature based intrusion detection system. This helps to monitor the packets in the network that helps to detect the malicious attacks in the networking system. The overall performance is detected and send as a notification to the security service panel system [14]. This helps to identify the malicious attacks in the networking system to improve the performance of the system. The attack is referred as the abnormal behaviour in the system

are are indicated through the intrusion detection system (IDS) software in the networking system.

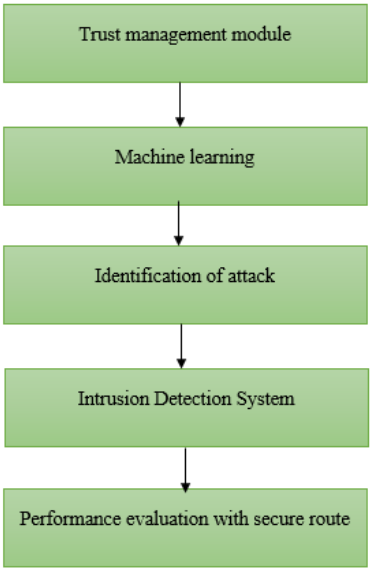

Fig 4: Intrusion Detection System (IDS)

The figure 4 represents the intrusion detection system mechanism.

(ii)Grey hole attack

The improper security solutions in the network are denoted as the grey hole attack. In this phase, the malicious nodes acts as a normal functioning node. The advancement of the black hole attack in the metworking system are referred as grey hole attack. This causes the dropping of packets in the communicating network through selective forwarding attack [15]. The dropping of packets are occurred with certain probabilistic situations. The grey hole attack causes to decrease the complete performance and functioning of the system.

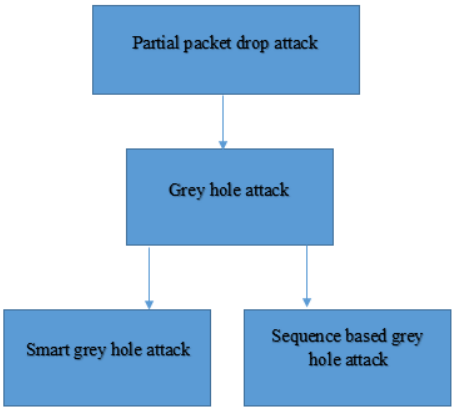

Fig 5: Grey hole attack

The figure 5 represents the grey hole attack in the networking system. These are neglected through the machine learning process.

III. METHODOLOGY

Machine learning is a subset of the artificial neural network. The machine learning is adopted through the human intelligence [16].

This shows the tendency of the machines to perform the functions as similar to that of the human intelligence. They are adopted to perform complex problems to adopt the exact optimum solutions. They are based upon the function through the testing and training process. The machine learning helps to obtain the optimum solutions with higher accuracy and precision [17]. This is done through the process of representation, evaluation and optimization techniques. The optimization techniques used here are genetic algorithm.

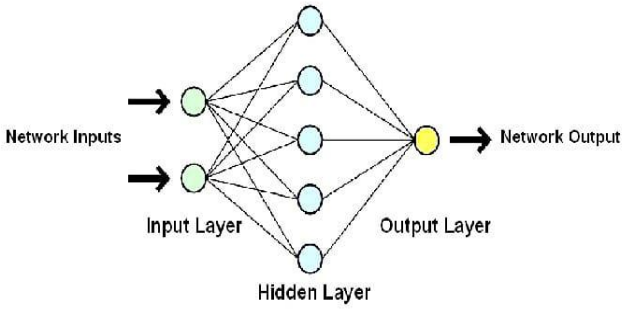

Fig 6: Machine learning

The figure 6 represents the machine learning. This includes the numerous inputs that are processed in the hidden layers to produce the desired output. This is done through seven stage which includes data collection, preparation of data, model choosing with training the model and evaluation of the models [18]. They are represented as supervised and semi-supervised machine learning algorithms.

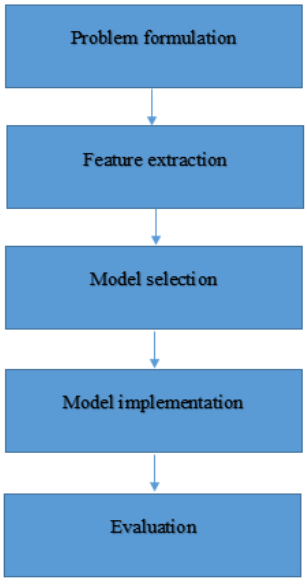

Fig 7: Stages in machine learning

The figure 7 demonstrates the various stages in the machin elearning process. This includes the problem formulation, feature extraction, selection of model, implementation of model and eveluation through the

training and testing the models. The problem formulation is the first step in the analysis of the type of defect in the networking system. This helps to detect the attacks and tends to proceed further. The feature extraction is defined as the process of converting the raw data into a desired data form [19].

This helps to analyze the obtained data in the system. This is further proceeded to the model selection and evaluation process. This is done through the genetic algorithm [20].

Fig 8: Genetic algorithm

The figure 8 represents the functioning of genetic algorithm with gene, chromosome and population.

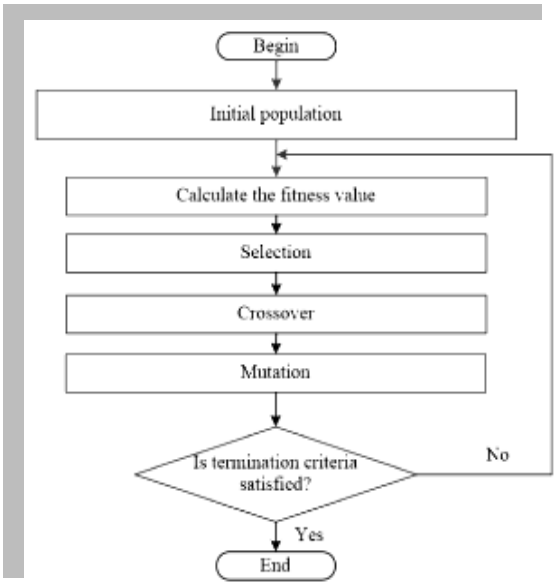

Fig 9: Genetic algorithm

The figure 9 represents the flowchart of genetic algorithm. This is initialised through the calculation of the fitness value. Then selection of the individual and crossover process. The process of crossover is defined as the combination of two genetic information that are used to obtain a newer genetic information [21]. The mutation id defines as a small random function to obtain the optimum solution in the system. The overall process is done through the satisfication of the termination criteria. If it satisfies the terminating criteria, the optimum solution is obtained. This helps to solve the problem with the exact solution [22].

IV. Software Implementation and Results

The secure data transmission through the machine learning with genetic algorithm is implemented through the matlab Simulink. This helps to identify the malicious attacks in the networking system through the training and testing process. This optimization techniques helps to identify the attack at an early stage in order to rectify the defects in the networking system.

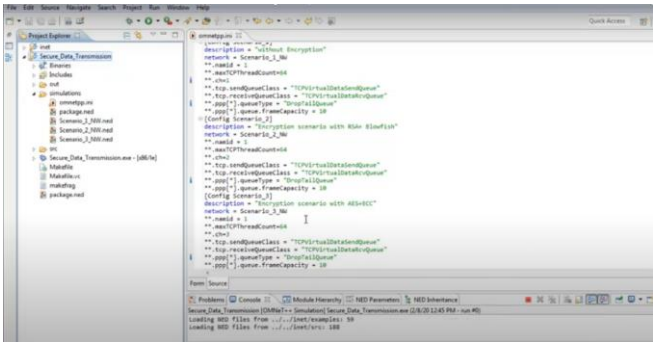

Fig 10: Matlab implementation

The figure 10 demonstrates the matlab implementation through code generation.

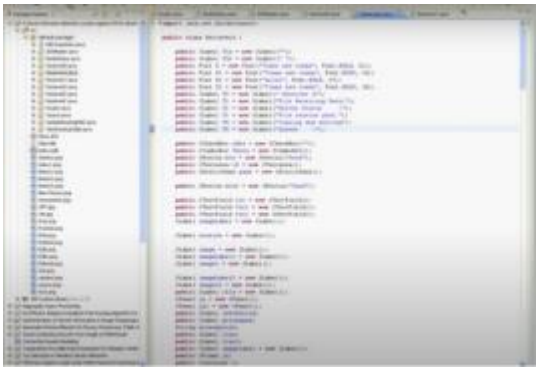

Fig 11: Trace file

The figure 11 represents the generation of trace file code in the matlab simulink.

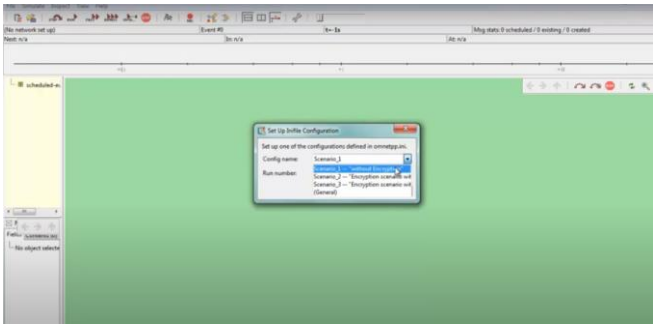

Fig 12: Infile configuration

The figure 12 demonstrates the infile configuration

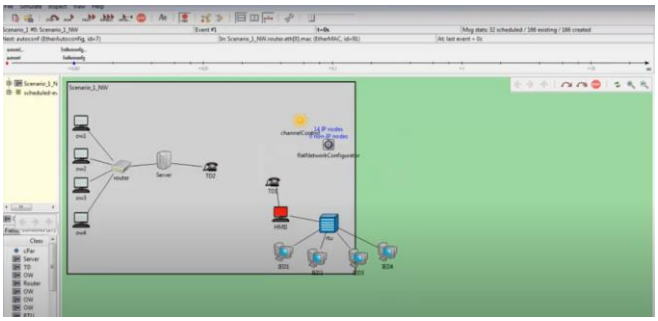

Fig 13: Mobile Ad hoc Network (MANET)

The figure 13 represents the mobile ad hoc network. This shows the routing protocols. The nodes are interconnected with each other in a random fashion in the system.

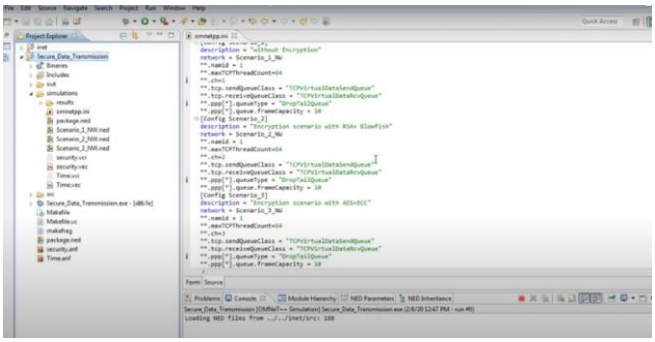

Fig 14: Code Implementation

The figure 14 shows the implementation of code in matlab. This helps in analysing the fitness function.

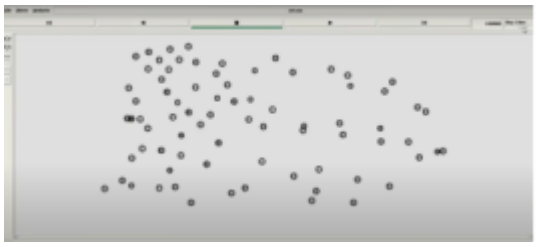

Fig 15: Packet Implementation

The figure 15 represents the packet implemetation in MANET. They communicate with the neighbouring nodes for the transfer of information.

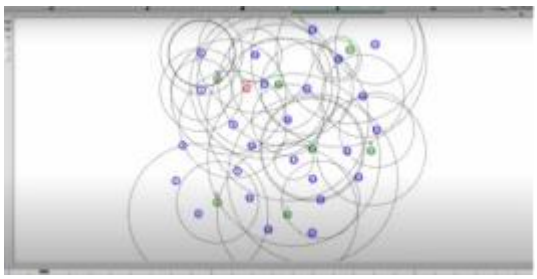

Fig 16: Packet drop in malicious node

The figure 16 represents the packet drop in the malicious nodes. The performance are initiates to the control room for rectification of the performance of the system. This is done through the genetic algorithm to obtain secure pathway.

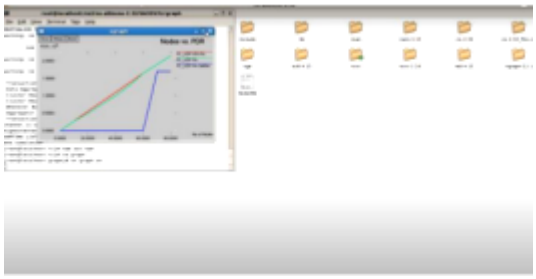

Fig 17: Retransmit output

The figure 17 represents the packet retransmit output in the system.

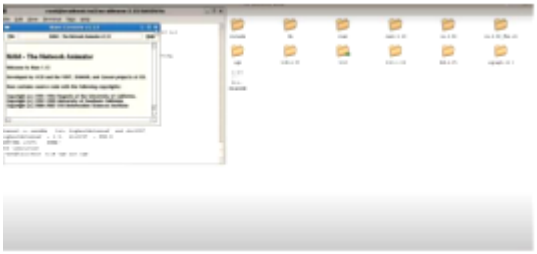

Fig 18: Implementation of NS2 simulator

The figure 18 demonstrates the implementation of NS2 simulator. This helps to enhance a secure pathway through neglecting the malicious nodes.

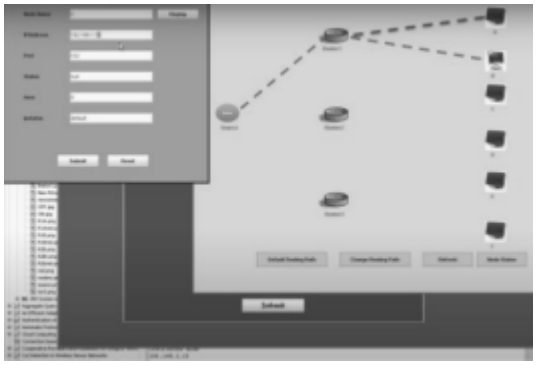

Fig 19: Web application structure

The figure 19 demonstrates the web application structure with the transmission of data through the nodes. They are formed with absence of infrastructure hence they are highle flexible in nature. This is the result of occurrence of the attack in the network.

Fig 20: Network attack layer

The figure 20 represents the network attack layer. This indicates the malicious behaviour in the networking system. This is neglected through the genetic algorithm.

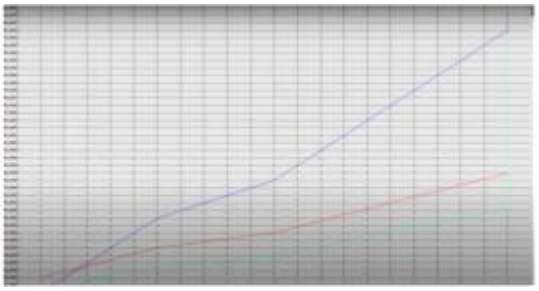

Fig 21: Delay ratio

The figure 21 represents the average delay ratio in the system. The packet delivery ratio is used to identify the ratio of packets in the networking layer before the detection of the malicious nodes in the network.

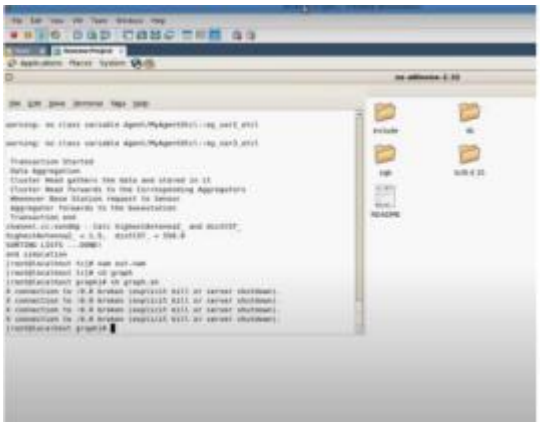

Fig 22: AODV routing protocol

The figure 22 demonstrates the AODV routing protocol in the networking system.

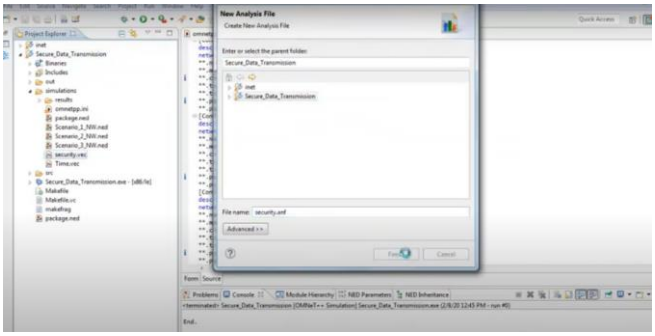

Fig 23: Secure data transmission

The figure 23 represents the secure data transmission in the network. This is done through the machine learning and genetic algorithm.

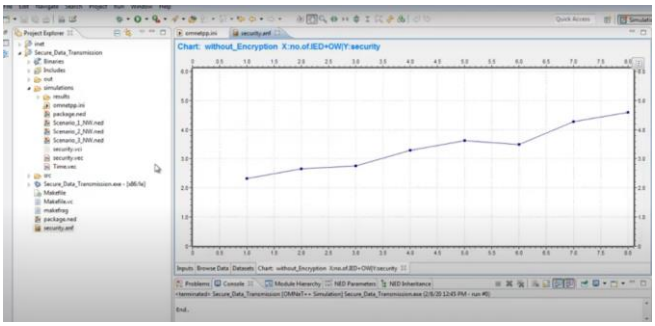

Fig 24: Data transmission without encryption

The figure 24 demonstrates the data transmission without encryption techniques. This causes various consequences. The encrypted data is obtained through the optimization of the obatined information in the nodes.

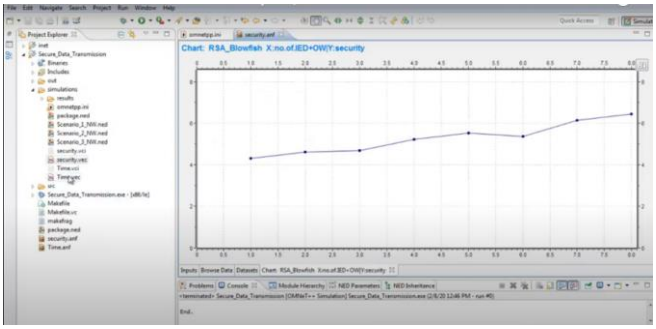

Fig 25: Data transmission with encryption

The figure 25 shows the data transmission with encryption techniques.

VIII. CONCLUSION

The major purpose of the proposed system is to enhance secure data transmission and improvement through machine learning with genetic algorithm. This helps to reduce the security threats. These are done through machine learning based IDE, models through trust based systems and attack detection models. This helps to enhance the energy efficiency in the network. This biologically inspired genetic algorithm helps in obtaining desired solution.

REFERENCES

[1] Cai R.J., Li X.J., Chong P.H.J. An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs. *IEEE Trans. Mob. Comput.* 2019;18:42–55. doi: 10.1109/TMC.2018.2828814

[2] Kumar M., Mukherjee P., Verma K., Verma S., Rawat D.B. Improved Deep Convolutional Neural Network based Malicious Node Detection and Energy-Efficient Data Transmission in Wireless Sensor Networks. *IEEE Trans. Netw. Sci. Eng.* 2021 doi: 10.1109/TNSE.2021.3098011

[3] Hussain A., Nazir S., Khan F., Nkenyereye L., Ullah A., Khan S., Verma S., Kavita A Resource Efficient hybrid Proxy Mobile IPv6 extension for Next Generation IoT Networks. *IEEE Internet Things J.* 2021 doi: 10.1109/JIOT.2021.3058982

[4] Rani P., Kavita, Verma S., Nguyen G.N. Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm with Artificial Neural Network. *IEEE Access.* 2020;8:121755–121764. doi: 10.1109/ACCESS.2020.3004692

[5] M. Zolanvari, M.A. Teixeira, L. Gupta, K.M. Khan, R. Jain Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things IEEE Internet Things J., 6 (4) (2019), pp. 6822-6834

[6] W. Wu, S. Pirbhulal, H. Zhang, S.C. Mukhopadhyay Quantitative Assessment for Self-Tracking of Acute Stress Based on Triangulation Principle in a Wearable Sensor System IEEE J. Biomed. Heal. Informatics, 23 (2) (2019), pp. 703-713

[7] Y.K. Saheed, M.O. Arowolo Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms IEEE Access, 9 (2021), pp. 161546-161554

[8] Arulkumar, V., Sridhar, S., Kalpana, G., & Guruprakash, K. S. (2022). Real-Time Big Data Analytics for Improving Sales in the Retail Industry via the Use of Internet of Things Beacons. In Expert Clouds and Applications (pp. 111-126). Springer, Singapore.

[9] H.H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, K.-K. Choo A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks IEEE Trans. Emerg. Top. Comput., 7 (2) (2019), pp. 314-323

[10] C. Hu, J. Yan, and C. Wang, "Advanced Cyber-Physical Attack Classification with Extreme Gradient Boosting for Smart Transmission Grids," *IEEE Power Energy Soc. Gen. Meet.*, vol. 2019-Augus, 2019, doi: 10.1109/PESGM40551.2019.8973679

[11] Husain, A. Salem, C. Jim, and G. Dimitoglou, "Development of an Efficient Network Intrusion Detection Model Using Extreme Gradient Boosting (XGBoost) on the UNSW-NB15 Dataset," *2019 IEEE 19th Int. Symp. Signal Process. Inf. Technol. ISSPIT 2019*, 2019, doi: 10.1109/ISSPIT47144.2019.9001867

[12] M. Al-Qatf, Y. Lasheng, M. Al-Habib, K. Al-Sabahi Deep Learning Approach Combining Sparse Autoencoder with SVM for Network Intrusion Detection IEEE Access, 6 (2018), pp. 52843-52856

[13] S.M. Kasongo, Y. Sun A deep learning method with filter based feature engineering for wireless intrusion detection system IEEE Access, 7 (2019), pp. 38597-38607

[14] S.U. Jan, S. Ahmed, V. Shakhov, I. Koo Toward a Lightweight Intrusion Detection System for the Internet of Things IEEE Access, 7 (2019), pp. 42450-42471

[15] Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," IEEE Communications Surveys Tutorials, vol. 20, pp. 3453–3495, Fourthquarter 2018

[16] L. Hu, H. Wen, B. Wu, F. Pan, R. F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in internet of things," IEEE Internet of Things Journal, vol. 5, pp. 219–228, Feb 2018

[17] H. B. Salameh, S. Almajali, M. Ayyash, and H. Elgala, "Spectrum assignment in cognitive radio networks for internet-of-things delaysensitive applications under jamming attacks," IEEE Internet of Things Journal, pp. 1–1, 2018

[18] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "Sdn-based data transfer security for internet of things," IEEE Internet of Things Journal, vol. 5, pp. 257– 268, Feb 2018

[19] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiotnetwork-based detection of iot botnet attacks using deep autoencoders," IEEE Pervasive Computing, vol. 17, pp. 12–22, Jul 2018

[20] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for iot: Towards universal and resilient systems," IEEE Communications Surveys Tutorials, pp. 1–1, 2018

[21] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, "Information security model of block chain based on intrusion sensing in the iot environment," Cluster Computing, Mar 2018

[22] Matukumalli, V., Naga Sasidhar Maddi, S., Krishna Angirekula, K., Reddy Pulicherla, V., Senthil kumar, A. M., Maridurai, T., … Kasinathan, D. (2021). Augment reality chatbot using cloud. Materials Today: Proceedings, 46, 4254–4257. doi:10.1016/j.matpr.2021.03.058 10.1016/j.matpr.2021.03.058

[23] Enireddy, V., Finney Daniel shadrach, S., Shobha rani, P., Anitha, R., Vallinayagam, S., Maridurai, T., … Balakrishnan, E. (2021). Prediction of human diseases using optimized clustering techniques. Materials Today: Proceedings, 46, 4258–4264. doi:10.1016/j.matpr.2021.03.068 10.1016/j.matpr.2021.03.068