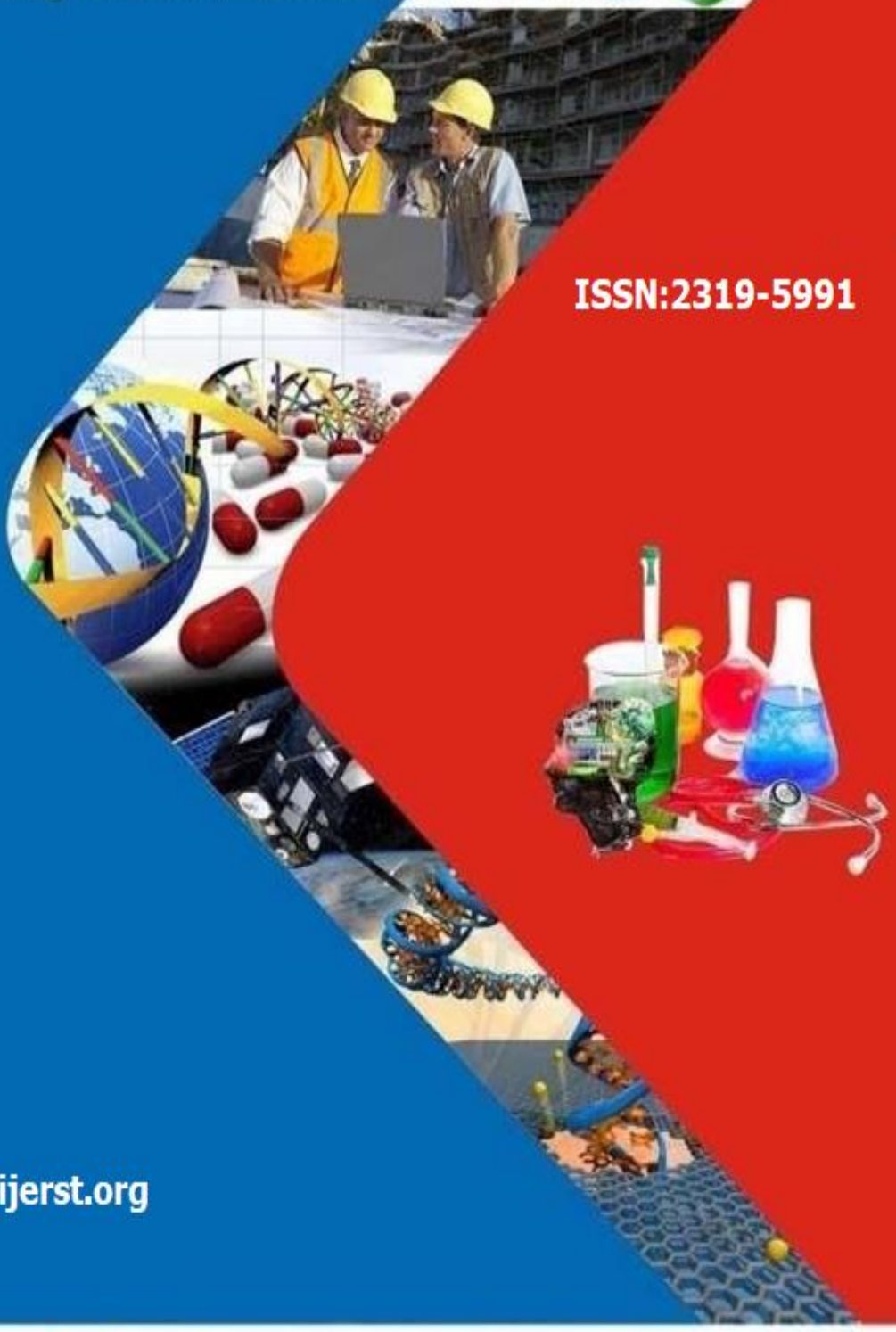
International Journal of Engineering Research and Science & Technology

IJERST

ISSN:2319-5991



www.ijerst.org

E-mail: editor@ijerst.org or ijerst.editor@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

ALENHANCESERCURITY: ROBUSTDATATRANSMISSION IN AD-HOC NETWORK

Mr.E.NAGARAJU[1], SHAIK.ABDULRAWOOF [2]

[1] Assistant professor, Department of Master of Computer Applications, SRK Institute of Technology, Vijayawada, Andhra Pradesh

[2] MCA Students, Department of Master of Computer Applications, SRK Institute of Technology, Vijayawada, Andhra Pradesh

ABSTRACT

A cluster of wireless devices may spontaneously establish a dynamic, decentralized network called an ad hoc network. When more conventional network infrastructure is either not accessible or not feasible, they step in to fill the void. As a result of their inherent instability and security flaws, ad hoc networks make it difficult to guarantee secure and private data transfer. Security measures for ad hoc networks have traditionally included cryptography, encrypted routing protocols, and intrusion prevention systems. These approaches function, but they may not be resilient enough or give enough privacy, and they might not be able to adjust to changing network circumstances. The main obstacle is creating an AI-powered system that can improve the security and privacy of data transfer in ad hoc networks. This necessitates the development of algorithms capable of securely transmitting data while simultaneously adapting to evolving network circumstances. Emergency response, military operations, disaster recovery, and Internet of Things (IoT) settings are just a few of the many applications that rely on ad hoc networks. It is of the utmost importance to guarantee the security of data transferred across these networks, making sure it can withstand interruptions and remains private to avoid manipulation or unauthorized access. Data transmission in ad-hoc networks is vulnerable and unreliable; this project, "Ensuring Resilient and Confidential Data Transmission with Artificial Intelligence in Ad-Hoc Networks," seeks to change that by incorporating AI methods. This project aims to construct a system that can automatically and correctly ensure the resilience and secrecy of data transmission by employing AI for adaptive routing, threat detection, and encryption. Ad-hoc network security may be greatly improved with the help of AI algorithms due to their ability to adapt on the fly to new security threats and network circumstances. This development shows a lot of potential for making ad-hoc networks more secure and reliable for data transfer in important situations.

KEYWORDS: Internet of Thing, Cryptography, Emergency Response.

1. INTRODUCTION

1.1 Overview

In the modern digital era, the demand for wireless communication has expanded rapidly, resulting in increased attention toward the development and deployment of mobile ad-hoc networks (MANETs). These networks are composed of autonomous nodes that communicate

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

with each other using wireless links, without relying on any fixed infrastructure or centralized control. The flexibility, scalability, and rapid deploy ability of ad-hoc networks make them suitable for various critical applications such as military operations, disaster relief, vehicular networks, and remote sensing.

However, the dynamic topology, open wireless medium, and lack of centralized monitoring make ad-hoc networks vulnerable to various security threats and transmission failures. Nodes can frequently join or leave the network, links can break, and the network structure can change unpredictably. These challenges can severely impact the performance, reliability, and security of data transmission within the network.

To address these issues, there is a growing interest in integrating Artificial Intelligence (AI) techniques into ad-hoc networks. Al algorithms can enhance the intelligence of routing protocols, detect intrusions, optimize network paths, and adaptively respond to network changes. In particular, machine learning methods like Artificial Neural Networks (ANN), Support Vector Machines (SVM), and met heuristic optimization algorithms like Artificial Bee Colony (ABC) have shown promise in improving network robustness and securing data transmission.

This project, titled "Robust and Secure Data Transmission Using Artificial Intelligence in Ad-Hoc Networks," aims to design and implement a system that employs Al-based models for improving the reliability and confidentiality of data transmission. By integrating these models with traditional routing protocols like AODV (Ad hoc On-Demand Distance Vector), the project seeks to build an adaptive and secure communication framework suitable for real-time and mission-critical applications.

1.2ProblemStatement

Ad-hoc networks are inherently unstable due to their decentralized and dynamic nature. Nodes in such networks act both as hosts and routers, forwarding data packets for others in the absence of fixed infrastructure. This leads to several critical challenges, particularly when it comes to secure and reliable data transmission.

These challenges include:

- Frequent route failures due to node mobility and topology changes.
- Limited bandwidth and power constraints, making efficient communication essential.
- Vulnerability to various attacks, including black hole, wormhole, and denial-of-service (DoS).
- Lack of centralized security management.

Traditional solutions such as static routing algorithms, manual configuration, and encryption-based methods offer limited adaptability and scalability. They often fail to address real-time threats or dynamically optimize network performance. Moreover, these approaches do not effectively differentiate between legitimate and malicious behavior in ever-changing network conditions. Thus, there is a pressing need for systems that can not only detect and

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

mitigate threats in real-time but also ensure continuous and reliable data transmission under fluctuating conditions. This project addresses this need by incorporating Al-driven algorithms with routing protocols to: Detect anomalies and threats in the network traffic. Adapt routing paths dynamically based on the network state. Improve data delivery ratio, throughput, and reduce latency. Secure data against unauthorized access and manipulation.

1.3 Research Motivation

The primary motivation behind this project is to harness the capabilities of Al to overcome the limitations of traditional network routing and security mechanisms in ad-hoc networks. Al-based systems can analyze historical and real-time data to make predictive decisions, learn from patterns, and continuously adapt to new conditions. This ability is especially valuable in the context of ad-hoc networks, which operate in highly unpredictable environments.

Several factors drive the motivation for this research:

1. Dynamic Adaptability: Al algorithms, particularly machine learning

Models can learn and evolve based on ongoing data patterns, making them well-suited for networks with changing topologies and usage patterns.

2. Threat Detection: Al techniques can identify deviations from normal network behavior, helping detect intrusions or malicious activity more effectively than rule-based systems.

3. Optimized Routing: Algorithms like ANN and ABC can find optimal or near-optimal paths for data transmission, thereby reducing packet loss, delay, and energy consumption.

4. Automation and Scalability: By reducing the need for manual

Intervention, Al-powered systems can operate autonomously and scale efficiently to large and complex networks.

5. Real-world Relevance: The practical significance of robust ad-hoc

Networks are immense in sectors like emergency services, defense, and smart infrastructure. Enhancing their reliability and security has direct societal and economic benefits.

6. Academic and Technological Advancement: The integration of Al into

Networking is a growing area of research. This project contributes to that field by proposing and evaluating a hybrid model that can be further extended or adopted in future systems.

2.LITERATURESURVEY

In addition to dsr vs. protect of one infrastructure and butyrate hydroxyl, Shahabad donc ibn. [23] Built a narrative routing protocol. And use this strategy; the same hacker group has been identified just by the behavior of the nodes. Upon examination, it seems that the aforementioned base station has been disconnected from the road. Good received packets speed (pdr) to reduced latency is also shown in these tests. In a packet forwarding technique proposed by

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

baadache and belmehdi [24], the interacting source node formally acknowledges the receipt of datagram's from any module. This automated system also has trouble with the once-high-altitude packet forwarding, when each node sends a positive affirmation text to the base station that came before it. In addition to the issue mentioned earlier, Krishna and paramasivan [25] developed a routing algorithm based on the belief that data is available at the packet level and on the behavior patterns of all endpoints. However, these guidelines are currently facing challenges due to the significantly increased use of datagram's. It seems that many other close single nodes, often referred to as this same source node of intrusion detection and prevention (ids), helped kaur [26] minimize a single sinkhole strike (gha) and observe the achievement of many other interacting endpoints. Inside the character of any malicious node, the endpoint's average packet advantage would be enhanced. In this case, a crucial message ("alert") has been sent over certain connections between these source nodes and certain attacker destinations. A specific, one-of-a-kind node is required, even if the algorithm only works on predetermined thresholds. The novel approach source and destination, devised by Mohanapriya and Krishnamurthy [14], pretends to be a destination network for data packets of final quantities sent along all anticipated channels. The application in issue has been sent, but only to the point where the receiving device may potentially reach the necessary packet level via its base station. In response to a request like this, a single text message was sent to an endpoint; the message concerned two things in relation to the destination device. That after receiving text such as an inquiry remark, the receiving device compares it to its own previously received data. If a type error occurred, consider the specified nucleus as the endpoint and add it to the identify after all nodes. The introduction of one blended confidence butterfly reach between safeguarding an infrastructure group and keerthika and malarvizhi [27] was a significant development. Error verification of a protected route will be done by the firm. A novel solution would need preliminary assessment of its optimization procedure, following all pollen. Both the suggested technique and the final result benefit from this well constructed approach. Using efficient energy quality assurance and enhancement tools such mobile ad hoc networks, a new faith technique was launched by Disney Theme and Felix [28]. It has come to light that a key component, like a tune or alternative pathways identified in the processes of the communication system, has been intercepted. [29] Rezaei et al. introduced a system whereby node 1 releases its datagram handling technology within a week after receiving a node's knowledge, which is then used for butylated hydroxyl error checking. The decision of whether an endpoint is genuine or malignant is made by the node. Then again, hussain, etc.

[30] Formerly, mobile ad hoc processes like material identification and timeouts based on baiting were in use. Michelle Yadav or perhaps IBN. [31] Was using a wireless sensor network-based automated test that relied on a learning algorithm, such as a macro-level traffic flow-predicted forward emphasis on inventory.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

3. PROPOSED SYSTEM

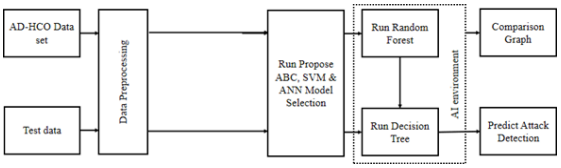


Fig. 1: Block diagram of proposed system.

Overview

Data loading, preprocessing, model training and assessment are all part of the all-inclusive approach to an ad-hoc networks project shown by the Python script.

Here is a step-by-step guide written in a way that everyone can understand:

Loading the dataset and importing the required libraries are the first steps in conducting research. Data frames, or Pandas Data Frames, make it easier to work with and analyze datasets.

Data Exploration and Analysis: In order to obtain insights into the dataset, basic exploratory data analysis (EDA) is conducted. Mean, standard deviation, and quartiles are some of the descriptive statistics that may be generated by using the describe () function. Each column's data types and null values are examined using the info () function.

Count plot with Seaborn: A visual representation of the distribution of choice classes. This gives a high-level picture of the imbalance or balance in the 'Decision' target variable.

In the preprocessing step, the dataset is examined for and any null values are highlighted. For uniform feature scaling, we scale the independent variables using scikit-learn's Standard Scaler. This is of the utmost importance for models that take input feature magnitude into account.

To divide the dataset into two parts, one for training and one for testing, the train_test_split function is used. Twenty percent of the data is in the testing set, which uses a random seed to ensure repeatability.

The training set (X_train and entrain) is used to instantiate and train a logistic regression model. After that, the accuracy, confusion matrix, and classification report are shown after testing the model on the reserved testing set (X_test).

Simulation of an Artificial Neural Network (ANN): Using the Keras library, an ANN model is created. In this design, a 64-neur input layer, a 32-neur hidden layer trained using the ReLU function, and a sigmoid-activated binary classification output layer make up the architecture. Binary cross-entropy loss and the Adam optimizer are used to construct the model.

When dealing with unbalanced data, the Synthetic Minority Over-sampling Technique (SMOTE) is used to train the artificial neural network (ANN) model on the resample training set (X_train_smote y_train_smote). Then, the ANN model is evaluated. After that, the accuracy, classification report, and confusion matrix are shown after evaluating the model on the original testing set.

Analyzing Receiver Operating Characteristic (ROC) Curves: ANN and logistic regression models both produce ROC curves. As a performance statistic, the area under

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

the curve (AUC) shows how well the true positive rate (TPR) and false positive rate (FPR) are balanced out.

3.2 Dataset Splitting

Separating our dataset into a training set and a test set is an important step in pre-processing data for machine learning. If we want our machine learning model to work better, this is an important part of pre-processing the data. Just imagine we train our machine learning model on one dataset and then put it to the test on an entirely other one. That will make it harder for our model to deduce model-to-model relationships.

Even with excellent training and great accuracy, our model's performance will suffer when fed a fresh dataset. Therefore, it is our constant goal to construct a machine learning model that exhibits good performance on both the training set and the test dataset. It is possible to describe these datasets as follows:-+

A subset of the dataset used to train a machine learning model, with the result known in advance.

The machine learning model is tested on a subset of the dataset called the test set. The model then uses the test set to forecast the output.

3.3 ANN Classifier

Despite the Perception's current prominence as an algorithm, its original intent was to serve as a machine for picture recognition. The fact that it can see, perceive, and identify pictures in a way that is similar to a human gives it its name. There has been a lot of focus on the concept of a machine that could conceptualize inputs that come from the physical world, like light, sound, temperature, etc. — the "phenomenal world" that we're all familiar with — without any help from a human being to process and code the data. A fundamental building block of computing, the neuron was the basis of Rosenblatt's perception machine. A cell inside each neuron, like in earlier models, receives a sequence of inputs and weights. The key distinction in Rosenblatt's model is that inputs are integrated in a weighted total. When this sum above a certain threshold, the neuron is activated and an output is generated.

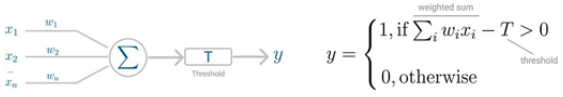


Fig.3.1: Perceptronneuronmodel (left) andthresholdlogic (right).

Binary Classification

The activation function controls the perception's discrete output, which defines a linear decision boundary and allows it to be utilized as a binary classification model.

By minimizing the distance between the decision border and misclassified locations, it discovers the separating hyper plane. The following is the definition of the perception loss function:

$$\underbrace{D(w,c)}_{\text{distance}} = -\sum_{i \in M} \overbrace{y_i}^{\text{output}} (x_i w_i + c)$$

misclassified observations

Perception employs stochastic gradient descent (SGD) as its optimization function to reduce this gap to a minimum. Assuming the data can be separated along linear lines, SGD will converge in a limited amount of steps. The activation function, which decides whether the neuron will fire or not, is the final component needed by Perception. The

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

sigmoid function was utilized by the first Perception models, and its form alone explains a lot! A non-linear function may be encoded using the sigmoid function, which transfers any actual input to a value of either 0 or 1. The neuron may take in negative integers as input and yet provide a positive or negative number as output.

The majority of Deep Learning algorithms and articles published in the past ten years use the Rectified Linear Unit (Rely) as the activation function for their neurons. Reasons for ReLU's increased use include its capacity for more efficient computing, its ability to enable greater optimization using SGD, and the fact that its properties remain constant regardless of the input's magnitude. In response to inputs, the neurone randomly selects a starting set of weights. The activation function, ReLU, takes all of them into account when calculating the output value, which is a weighted sum.



Fig.3.2:Perceptronneuronmodel(left) andactivationfunction(right).

By using SGD, the perceptron is able to discover—or even learn—the weight set that minimizes the distance between the decision border and the misclassified points. After SGD converges, a linear hyper plane divides the dataset in half. The main complaint levelled against the Perceptron was that it was unable to depict the XOR gate, also known as exclusive OR, which only outputs 1 when the inputs are different. However, it was claimed that the Perceptron could represent any logic and circuit. This was shown over ten years later and it emphasizes that non-linear data cannot be processed using Perceptron, which only has one neuron.

3.3.2 ANN

To overcome this restriction, the ANN was created. A non-linear mapping from inputs to outputs characterises this neural network. Multiple stacked neurones make up an ANN's hidden layers, which are in addition to the input and output layers. In contrast to perceptrons, which require neurones to utilise threshold-imposing activation functions like ReLU or sigmoid, artificial neural networks (ANNs) allow neurones to use whatever activation function they wish. ANN is a kind of feedforward algorithm, similar to the Perceptron, in that it takes inputs, adds them up with the starting weights, and then applies the activation function. The key distinction, however, is the layer-by-layer propagation of each linear combination. The outcome of each layer's calculation, or its internal representation of the data, is passed on to the next layer. From the input layer to the output layer, this travels across all of the hidden levels. The algorithm would be unable to learn the weights that minimise the cost function if it only calculated the weighted sums in each neurone and communicated the results to the output layer. Learning would not occur if the algorithm just calculated one iteration. Backpropagation is useful in this situation.

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

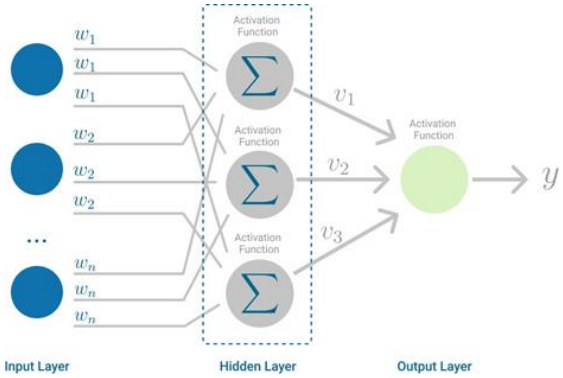


Fig.3.3: Architecture of ANN.

Backpropagation: The ANN is able to repeatedly alter the network weights by backpropagation, a learning technique, in an effort to minimise the cost function. Backpropagation can only be used correctly if one strict condition is met. Both the threshold function (like ReLU) and the function that mixes inputs and weights in a neurone (like the weighted sum) need to be differentiable. The usual optimisation function used in ANN is Gradient Descent, hence these functions must have a limited derivative. Each iteration begins by sending the weighted sums through each layer, and then, for each set of inputs and outputs, calculates the gradient of the Mean Squared Error. Then, in order to send it back, the gradient's value is used to update the first hidden layer's weights. That is the process by which the weights are sent back to the neural network's initialisation point. Here is a definition of one version of Gradient Descent:

$$\Delta_w(t) = -\varepsilon \frac{dE}{dw_{(t)}} + \alpha \Delta_{w(t-1)}$$

Bias, Error, Learning Rate, Gradient Current Iteration, Weight vector, Gradient Previous Iteration

Assessing and Contrasting Models:

In this study, we assess and contrast the two models' performance: logistic regression and artificial neural networks. By comparing the two, we can see whether the ANN model's increased complexity leads to noticeable gains in performance.

By incorporating confusion matrices and classification reports, we can get a full breakdown of the model's performance, including measures like F1-score, recall, and accuracy. To grasp the model's merits and shortcomings, this data is vital.

The study makes use of ROC curves and AUC analysis, which stand for Receiver Operating Characteristics. Particularly when considering the trade-off between the true positive rate and the false positive rate, these measures provide a visual depiction of the model's performance.

4. Results

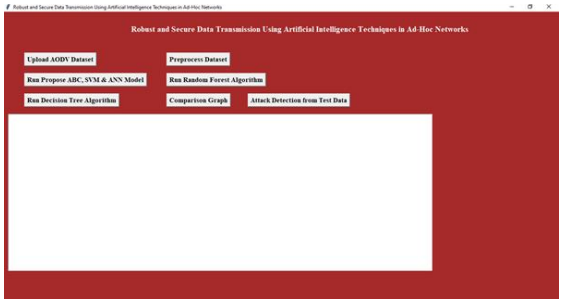


Figure1: Main GUI application of ensuring resilient and confidential data transmission with artificial intelligence in ad-hoc networks.

.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

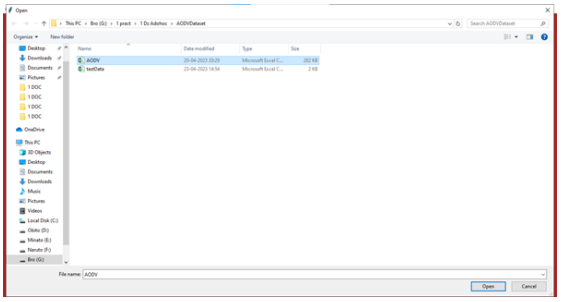


Figure2:Displays the selection of AODV Dataset.

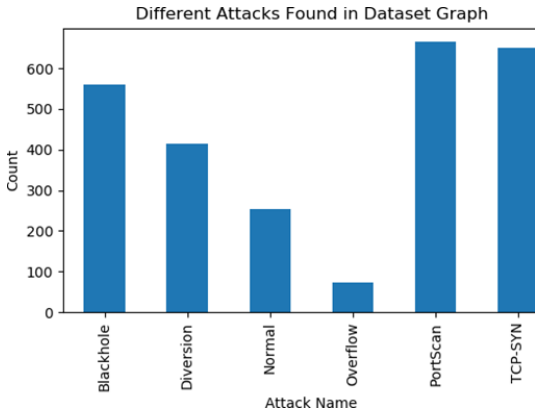


Figure3:Represents the sample data set and the count value of the label column.

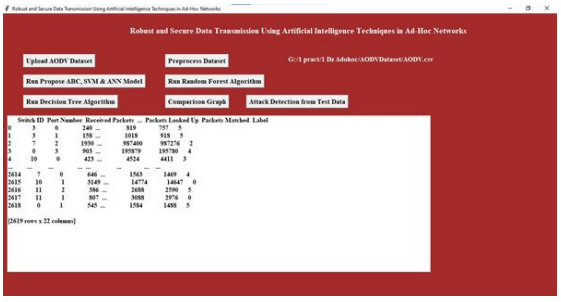
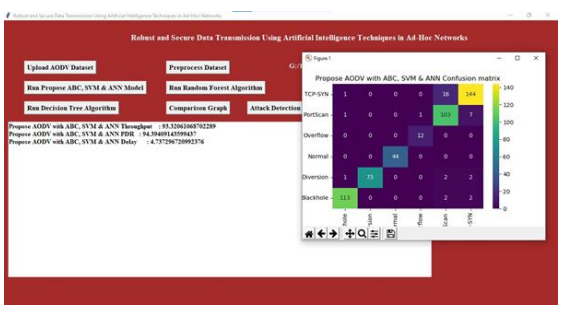


Figure4: Shows the pre-processed dataset.



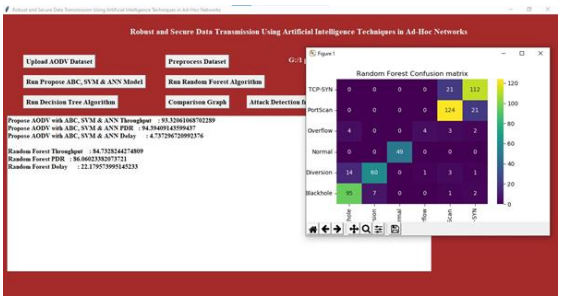


Figure5: Metrices of Proposed

Figure6: Metrics of the RF

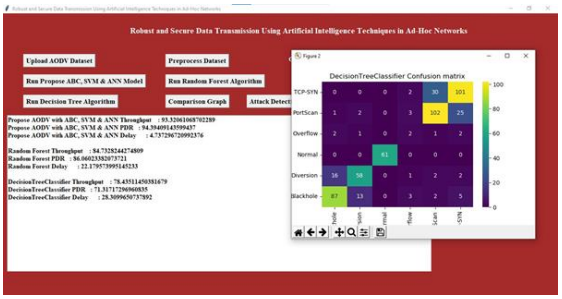


Figure7: Metrices of the DTC

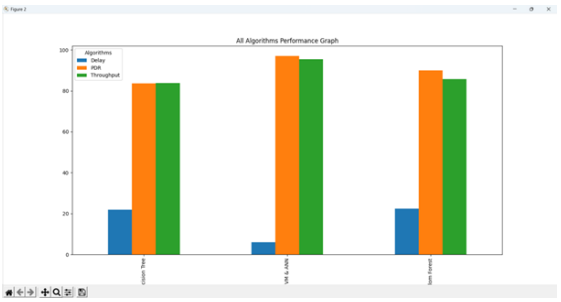


Figure8:Displaysthecomparisonplotf or allthemlmodelsperformancemetrics.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

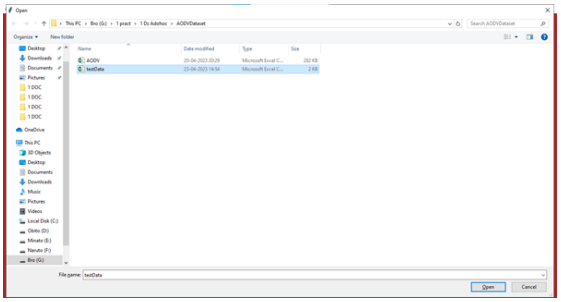


Figure9: Displays the selection of Test Dataset.

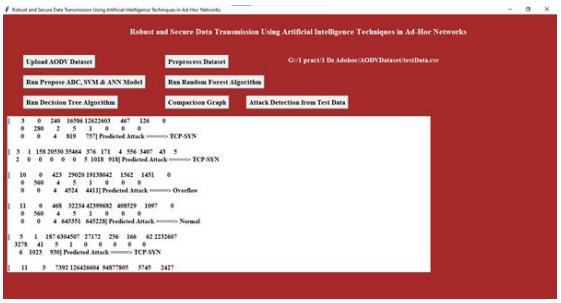


Figure10: Displaysthepredictionofthetestdata.

CONCLUSION

In conclusion, the integration of Artificial Intelligence in ad-hoc networks marks a significant leap forward in achieving secure, reliable, and intelligent wireless communication. This project sets out to design a model that not only addresses current challenges but also lays a foundation for future advancements in the field of intelligent networking systems.

REFERENCES

1. Alnumay, W.; Ghosh, U.; Chatterjee, P. A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things. Sensors 2019, 19, 1467.
2. Ghayvat, H.; Mukhopadhyay, S.; Gui, X.; Suryadevara, N. WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings. Sensors 2015, 15, 10350–10379.
3. Masek, P.;Masek, J.;Frantik, P.;Fujdiak, R.;Ometov,A.;Hosek, J.;Andreev, S.;Mlynek, P.; Misurec, J. A Harmonized Perspective on Transportation Management in Smart Cities: The Novel IoT-Driven Environment for Road Traffic Modeling. Sensors 2016, 16, 1872. Deng, Y.-Y.; Chen, C.-L.; T
4. Alnumay, W.; Ghosh, U.; Chatterjee, P. A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things. Sensors 2019, 19, 1467.
5. Ghayvat, H.; Mukhopadhyay, S.; Gui, X.; Suryadevara, N. WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings. Sensors 2015, 15, 10350–10379.
6. Masek, P.;Masek, J.;Frantik, P.;Fujdiak, R.;Ometov,A.;Hosek, J.;Andreev, S.;Mlynek, P.; Misurec, J. A Harmonized Perspective on Transportation Management in Smart Cities: The Novel IoT-Driven Environment for Road Traffic Modeling. Sensors 2016, 16, 1872. Deng, Y.-Y.; Chen, C.-L.; Tsaur, W.-J.; Tang, Y.-W.; Chen, J.-H. Internet of Things (IoT) Based Design of a Secure and Lightweight Body Area Network (BAN) Healthcare System. Sensors 2017, 17, 2919.
7. Tamilselvan, L.; Sankaranarayanan, V. Prevention of Co-operative Black Hole Attack in MANET. J. Netw. 2008, 3, 13–20.
8. Kang, B.-S.; Ko, I.-Y. Effective Route Maintenance and Restoration Schemes in Mobile Ad Hoc Networks. Sensors 2010, 10, 808–821.
9. Himral, L.; Vig, V.; Chand, N. Preventing aodv routing protocol from black hole attack. Int. J. Eng. Sci. Technol. (IJEST) 2011, 3, 3927–3932.
10. Panigrahi, R.;Borah,

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

S.;Bhoi,A.K.;Ijaz, M.F.;Pramanik, M.;Kumar,Y.;Jhaveri, R.H.A Consolidated Decision Tree-Based Intrusion Detection System for Binary and Multiclass Imbalanced Datasets. Mathematics 2021, 9, 751.

11. Papadimitratos, P.; Haas, Z. Secure routing for mobile ad hoc networks. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), SanAntonio, TX, USA, 27–31 January 2002.

12. Cai, R.J.; Li, X.J.; Chong, P.H.J.An Evolutionary Self-Cooperative Trust SchemeAgainst Routing Disruptions in MANETs. IEEE Trans. Mob. Comput. 2019, 18, 42–55.

13. Djahel, S.; Nait-Abdesselam, F.; Zhang, Z. Mitigating Packet Dropping Problem in MobileAd Hoc Networks: Proposals and Challenges. IEEE Commun. Surv. Tutor. 2010, 13, 658–672

14. Gaur, L.;Singh, G.;Solanki,A.;Jhanjhi, N.Z.;Bhatia, U.;Sharma, S.;Verma, S.;Kavita; Petrovi´c, N.; Ijaz, M.F.; et al. Disposition of Youth in Predicting Sustainable Development Goals Using the Neuro-fuzzy and Random ForestAlgorithms. Hum.-Cent. Comput. Inf. Sci. 2021, 11, 24.

15. Gupta, P.; Goel, P.; Varshney, P.; Tyagi, N. Reliability factor-based AODV protocol: Prevention of black hole attack in MANET. In Smart Innovations in Communication and Computational Sciences; Springer: Singapore, 2019; Volume 851, pp. 271–279.

16. Mohanapriya, M.; Krishnamurthi, I. Modified DSR protocolfor detection and removalof selective black hole attack in MANET. Comput. Electr. Eng. 2014, 40, 530–538

17. Gurung, S.; Chauhan, S.Asurveyofblack-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability. Wirel. Netw. 2020, 26, 1981–2011.

18. Seyedi, B.; Fotohi, R. NIASHPT: A novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things. J. Supercomput. 2020, 76, 6917– 6940.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

19. Gaur, L.;Singh, G.;Solanki,A.;Jhanjhi, N.Z.;Bhatia, U.;Sharma, S.;Verma, S.;Kavita; Petrovi´c, N.; Ijaz, M.F.; et al. Disposition of Youth in Predicting Sustainable Development Goals Using the Neuro-fuzzy and Random ForestAlgorithms. Hum.-Cent. Comput. Inf. Sci. 2021, 11, 24.

20. Gupta, P.; Goel, P.; Varshney, P.; Tyagi, N. Reliability factor-based AODV protocol: Prevention of black hole attack in MANET. In Smart Innovations in Communication and Computational Sciences; Springer: Singapore, 2019; Volume 851, pp. 271–279.

21. Mohanapriya, M.; Krishnamurthi, I. Modified DSR protocolfor detection and removalof selective black hole attack in MANET. Comput. Electr. Eng. 2014, 40, 530–538

22. Gurung, S.; Chauhan, S.Asurveyofblack-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability. Wirel. Netw. 2020, 26, 1981–2011.

23. Seyedi, B.; Fotohi, R. NIASHPT: A novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things. J. Supercomput. 2020, 76, 6917– 6940.

24. Thebiga, M.; SujiPramila, R. A New Mathematical and Correlation Coefficient Based Approach to Recognize and to Obstruct the Black Hole Attacks in Manets Using DSR Routing. Wirel. Pers. Commun. 2020, 114, 975–993.

25. Lee, C.; Jeong, T. FRCA: A Fuzzy Relevance-Based Cluster Head Selection Algorithm for Wireless Mobile Ad-Hoc Sensor Networks. Sensors 2011, 11, 5383–5401.

26. Gurung, S.; Chauhan, S. A dynamic threshold based approach for mitigating black-hole attack in MANET. Wirel. Netw. 2018, 24, 2957–2971

27. Mohammadani, K.; Memon, K.A.; Memon, I.; Hussaini, N.N.; Fazal, H. Preamble time- division multiple access fixed slot assignment protocol for secure mobile ad hoc networks. Int. J. Distrib. Sens. Netw. 2020, 16, 1550147720921624.

28. El-Semary, M.; Diab, H. BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map. IEEE Access 2019, 7, 95197–95211.