ENSURING RESILIENT AND CONFIDENTIAL DATA TRANSMISSION WITH ARTIFICIAL INTELLIGENCE IN AD-HOC NETWORKS

Gudala Karunakar[1], A. Yogitha[2], A. Shruthi[2], Ch. Sindhuta[2] , Ch. Sowmya[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science Engineering
[1,2]Malla Reddy Engineering College for Women, Maisammaguda, Dhulapally, Kompally, Secunderabad-500100, Telangana, India

ABSTRACT

Ad-hoc networks are dynamic, decentralized networks formed spontaneously by a collection of wireless devices. They play a crucial role in scenarios where traditional infrastructure-based networks are unavailable or impractical. However, due to their dynamic nature and potential security vulnerabilities, ensuring resilient and confidential data transmission in ad-hoc networks is a challenging task. Traditional methods for securing ad-hoc networks may involve cryptographic techniques, secure routing protocols, and intrusion detection systems. While effective to some extent, these methods may not adapt well to dynamic network conditions and may not provide sufficient resilience and confidentiality. The primary challenge is to develop a system that employs artificial intelligence (AI) techniques to enhance the resilience and confidentiality of data transmission in ad-hoc networks. This involves designing algorithms that can dynamically adapt to changing network conditions and secure data transmission against potential threats. Therefore, the need of Ad-hoc networks are widely used in various applications, including emergency response, military operations, disaster recovery, and IoT environments. It's critical to ensure that data transmitted within these networks is not only reliable and resilient to disruptions but also kept confidential to prevent unauthorized access or tampering. This project, "Ensuring Resilient and Confidential Data Transmission with Artificial Intelligence in Ad-Hoc Networks," aims to revolutionize the security and reliability of data transmission in ad-hoc networks by integrating artificial intelligence techniques. By leveraging AI for adaptive routing, threat detection, and encryption, this research endeavors to develop a system capable of autonomously and accurately ensuring both the resilience and confidentiality of data transmission. AI algorithms can dynamically respond to changing network conditions and security threats, making them a powerful tool for enhancing the security of ad-hoc networks. This advancement holds great promise for improving the reliability and security of data transmission in critical scenarios where ad-hoc networks play a pivotal role.

Keywords: AD_DOC Nrtworks, Artificial Intelligence, Confidential Data Transmission.

1. INTRODUCTION

Overview

Naval mines represent a formidable threat to maritime activities, spanning naval operations, shipping, and offshore infrastructure. Safeguarding vessels and ensuring secure maritime environments necessitates the accurate detection and classification of these mines. One promising avenue for achieving this is the utilization of sonar technology, which has long served as a pivotal tool in underwater surveillance.

The historical backdrop of naval mine warfare traces its roots to ancient times, but it gained prominence during the 19th and 20th centuries, evolving into more sophisticated and elusive forms with technological advancements. Traditional methods for mine detection, such as visual inspection and magnetic detection, encounter limitations, particularly in challenging environments like murky or deep waters. Sonar technology emerged as a viable solution to overcome these challenges.

The contemporary challenge lies in the precise classification of underwater objects identified by sonar systems, with a specific focus on distinguishing between mines and natural formations like rocks. This task is inherently complex due to the variability in the acoustic signatures of different objects and the imperative for real-time decision-making to avert potential threats.

Conventional mine detection systems often integrate various sensors, including sonar, for identifying underwater objects. However, interpreting sonar signals traditionally relies on intricate signal processing algorithms and rule-based systems. These conventional approaches may struggle to adapt to the dynamic and diverse underwater environment, resulting in either false positives or missed detections.

The impetus for sonar signal classification arises from the recognized limitations of traditional systems in grappling with the intricacies of underwater environments. Sonar signals, serving as a rich source of information about underwater object characteristics based on their acoustic reflections, offer valuable insights. Leveraging connectionist networks, notably neural networks, stands as a promising approach to enhance the discrimination between mines and rocks. These networks possess the capacity to learn intricate patterns and relationships within sonar data, thereby improving the accuracy and efficacy of mine classification.

In essence, the historical narrative underscores the enduring threat posed by naval mines and the evolution of technology-driven solutions to address this challenge. The contemporary focus on sonar signal classification, empowered by neural networks, reflects a commitment to advancing capabilities in underwater mine detection and ensuring the safety and security of maritime activities.

2. LITERATURE SURVEY

Shahabi et al. [23] designed a novel routing algorithm in addition to AODV to secure a network from BHA. Using this strategy, the malicious nodes are identified based on the node's behavior. If any are detected that node is deleted from the route. The experiments also show better Packet Delivery Rate (PDR) with reduced delay. Baadache and Belmehdi [24] presented an acknowledgment-based routing approach by which the communicating nodes send acknowledgment whenever the nodes receive the data packet. The algorithm suffers from high routing overhead as each node sends an acknowledgment message to the prior node. In addition to the above problem, Kumari and Paramasivan [25] developed a routing mechanism of trust where the behavior of nodes is analyzed based on the dropping rate of packets, but this protocol also suffers from high overhead because of the additional use of control packets. Gurung and Chauhan [26] used the approach of mitigating a Gray Hole Attack (GHA) that takes the help of other nearby nodes, known as the nodes of the Intrusion Detection System (IDS), to monitor the performance of other communicating nodes. In the appearance of any malicious node, the packet drop value of the node is higher. In this case, the important message ("ALERT") is transferred among the networks to intimate other nodes to separate attacker nodes. As the algorithm works on the defined threshold, proper positioning of special nodes is required. Mohanapriya and Krishnamurthi [14] designed a new approach source node that imitates the destination node of the total amount of packets transmitted from all expected routes. Query request is transmitted by the destination node, particularly in the case where the node cannot obtain the desired packets. In response to this query reply, a message is sent back to the node that is about two-hop counts in contrast to the destination node. Once the message of query reply is received, the destination node compares its prior-received data with the recently received data. In case an error appears, consider that node as the suspected node and add it to the list of malicious nodes. Keerthika and Malarvizhi [27] presented a combined trust-based bee approach to secure the network against BHA. ABC is used for the detection of a secure route. A new solution is generated based on the fitness function of bees. The designed algorithm shows enhancement in the PDR and end-to-end delay.

Merlin and Ravi [28] presented a new trust-based approach that works on energy-aware routing for MANET. The BHA has been detected for single as well as for multiple routes formed during the data communication process. Rezaei et al. [29] presented a mechanism in which the source node transmits the route response data packet after processing the node's information, which is later used for BHA detection. Whether the node is genuine or malicious is decided by the intermediate node. On the other hand, Yasin et al. [30] used a timer and baiting-based method for BHA detection in MANET. Monica Sood et al. [31] used a deep learning model for traffic flow prediction based on attention for inventory automation using a Wireless Sensor Network.

3. PROPOSED SYSTEM

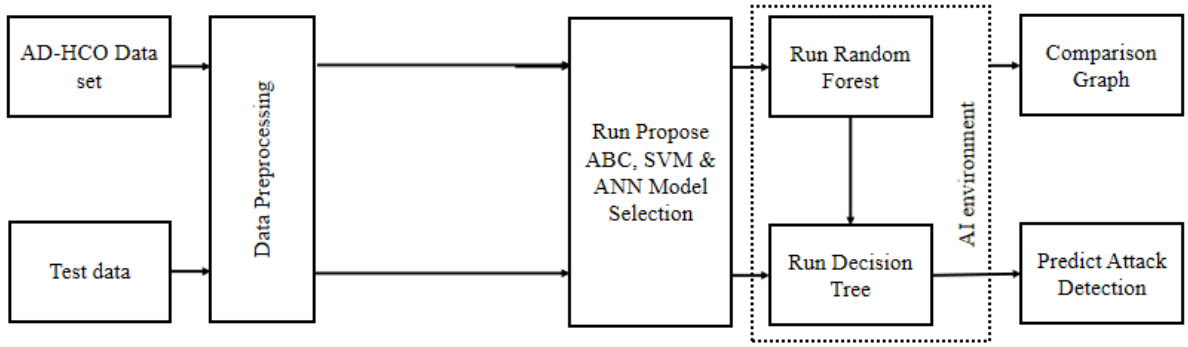

Fig. 1: Block diagram of proposed system.

Overview

The Python script demonstrates a comprehensive approach to an ad-hoc networks project, encompassing data loading, preprocessing, model training, and evaluation.

Below is a detailed explanation of each step in a human-readable manner:

Dataset Upload: The research begins with the importation of necessary libraries and the loading of the dataset. The dataset is stored in a Pandas DataFrame (df), allowing for easy manipulation and analysis.

Data Exploration and Analysis: Basic exploratory data analysis (EDA) is performed to gain insights into the dataset. Descriptive statistics, including mean, standard deviation, and quartiles, are obtained using the describe() method. The info() method is employed to examine the data types and null values in each column.

Visualization of Decision Counts: The distribution of decision classes is visualized using a count plot with seaborn. This provides a quick overview of the balance or imbalance in the target variable, 'Decision'.

Preprocessing: Null values are checked for and identified throughout the dataset. The independent variables are scaled using the StandardScaler from scikit-learn, ensuring that all features have a similar scale. This is crucial for models that are sensitive to the magnitude of input features.

Train-Test Splitting: The dataset is split into training and testing sets using the train_test_split function. The testing set comprises 20% of the data, and a random seed is set for reproducibility.

Logistic Regression Model: A logistic regression model is instantiated and trained on the training set (X_train and y_train). The model is then tested on the reserved testing set (X_test), and the accuracy, confusion matrix, and classification report are displayed.

Artificial Neural Network (ANN) Model: An ANN model is constructed using the Keras library. The architecture includes an input layer with 64 neurons, a hidden layer with 32 neurons using the ReLU activation function, and an output layer with a sigmoid activation function for binary classification. The model is compiled using binary cross-entropy loss and the Adam optimizer.

Model Training and Evaluation (ANN): The ANN model is trained on the resampled training set (X_train_smote and y_train_smote) using the Synthetic Minority Over-sampling Technique (SMOTE) for handling imbalanced data. The model is then evaluated on the original testing set, and accuracy, classification report, and confusion matrix are displayed.

ROC Curve Analysis: Receiver Operating Characteristic (ROC) curves are generated for both the logistic regression and ANN models. The curves visually represent the trade-off between true positive rate and false positive rate, with the area under the curve (AUC) serving as a performance metric.

Dataset Splitting

In machine learning data pre-processing, we divide our dataset into a training set and test set. This is one of the crucial steps of data pre-processing as by doing this, we can enhance the performance of our machine learning model. Suppose if we have given training to our machine learning model by a dataset and we test it by a completely different dataset. Then, it will create difficulties for our model to understand the correlations between the models.

If we train our model very well and its training accuracy is also very high, but we provide a new dataset to it, then it will decrease the performance. So, we always try to make a machine learning model which performs well with the training set and also with the test dataset. Here, we can define these datasets as:

Training Set: A subset of dataset to train the machine learning model, and we already know the output.

Test set: A subset of dataset to test the machine learning model, and by using the test set, model predicts the output.

ANN Classifier

Although today the Perceptron is widely recognized as an algorithm, it was initially intended as an image recognition machine. It gets its name from performing the human-like function of perception, seeing, and recognizing images. Interest has been centered on the idea of a machine which would be capable of conceptualizing inputs impinging directly from the physical environment of light, sound, temperature, etc. — the "phenomenal world" with which we are all familiar — rather than requiring the intervention of a human agent to digest and code the necessary information. Rosenblatt's perceptron machine relied on a basic unit of computation, the neuron. Just like in previous models, each neuron has a cell that receives a series of pairs of inputs and weights. The major difference in Rosenblatt's model is that inputs are combined in a weighted sum and, if the weighted sum exceeds a predefined threshold, the neuron fires and produces an output.

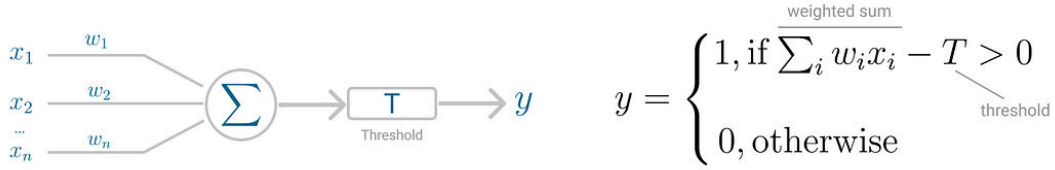

Fig.2: Perceptron neuron model (left) and threshold logic (right).

Threshold *T* represents the activation function. If the weighted sum of the inputs is greater than zero the neuron outputs the value 1, otherwise the output value is zero.

Advantages

Comprehensive Data Analysis: The reserch begins with a thorough exploration and analysis of the dataset, providing descriptive statistics and visualizations. This step aids in understanding the characteristics and distribution of the data.

Preprocessing for Model Readiness: Null value checks and preprocessing techniques, such as standard scaling, are applied to the dataset. This ensures that the data is suitable for training machine learning models by addressing missing values and normalizing feature scales.

Visualization of Decision Classes: The use of a count plot to visualize the distribution of decision classes enhances the understanding of the dataset's class balance or imbalance. This insight is crucial for selecting appropriate modeling techniques, particularly in the context of imbalanced datasets.

Logistic Regression Model: The inclusion of a logistic regression model provides a baseline for binary classification. Logistic regression is a simple yet effective algorithm for such tasks, making it suitable for comparison with more complex models.

Artificial Neural Network (ANN) Model: The research introduces an ANN model, a more sophisticated and flexible approach capable of capturing complex patterns in the data. ANNs are well-suited for tasks with non-linear relationships between features and outcomes.

4. RESULTS AND DISCUSSION

Dataset description:

This dataset has the information of network switches and their ports, particularly focusing on network traffic and operational metrics.

Here's a brief description of each column:

- Switch ID: This column represents the unique identifier for a network switch.
- Port Number: This column contains information about the port number on the switch.
- Received Packets: Indicates the number of packets received on the specified port.
- Received Bytes: Represents the total number of bytes received on the specified port.
- Sent Bytes: Represents the total number of bytes sent from the specified port.
- Sent Packets: Indicates the number of packets sent from the specified port.

Results description:

- This figure 3 depicts the main interface of the application, providing an overview of the tool for ad-hoc network framework. It include various features and options for users to interact with the application.
- The figure 4 represents the confusion matrix and performance metrics, focusing on the Decision Tree algorithms.
- The figure 5 provides a comprehensive comparison of the performance metrics across multiple machine learning models, including the proposed algorithms, Random Forest, and Decision Tree.

— The figure 6 illustrates the predictions generated by the chosen machine learning models on the selected test dataset. It provides insights into how well the models generalize to new, unseen data

Figure 3: Main GUI application of ensuring resilient and confidential data transmission with artificial intelligence in ad-hoc networks.

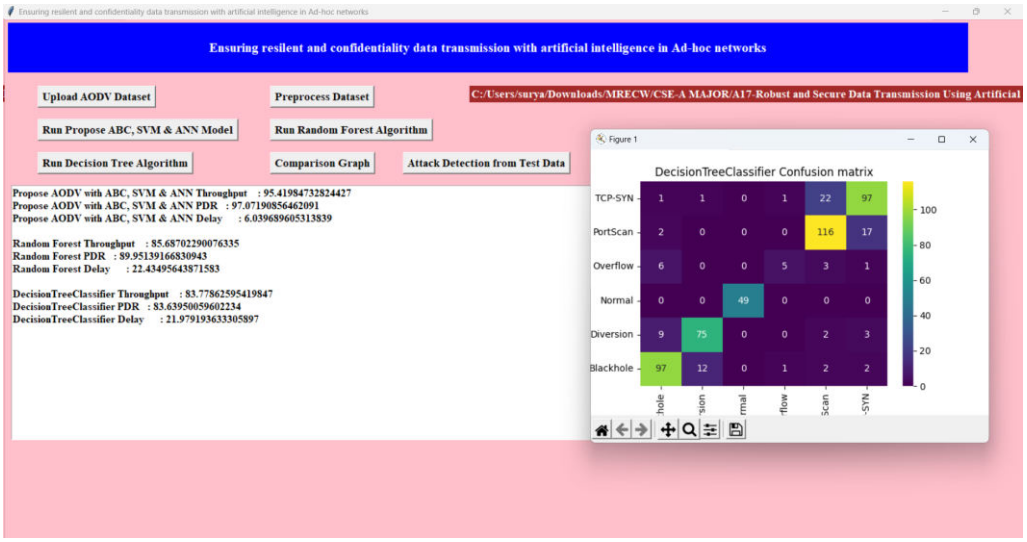

Figure 4: Displays the confusion matrix and Throughput, Pdr, Delay Decision Tree algorithms.

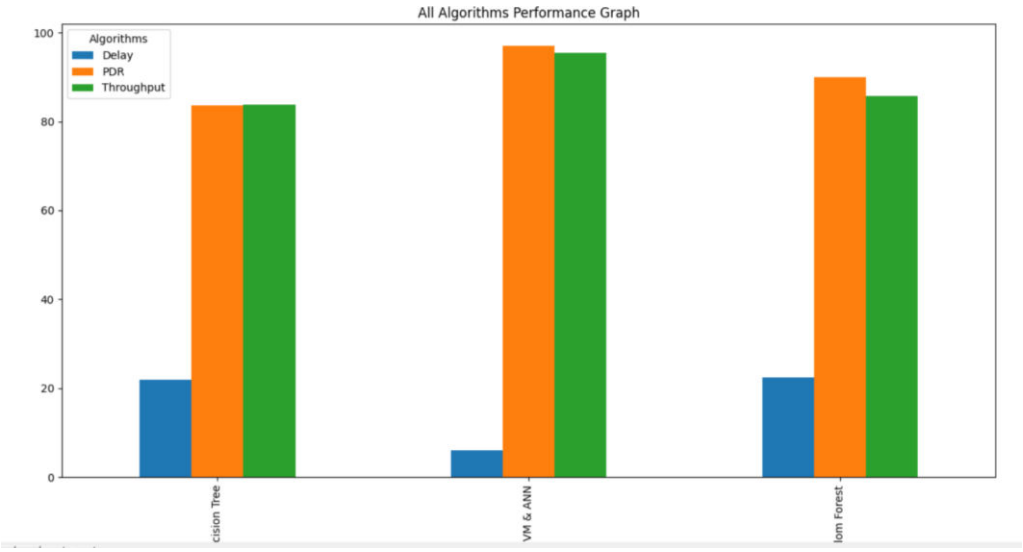

Figure 5: Displays the comparison plot for all the ml models performance metrics.

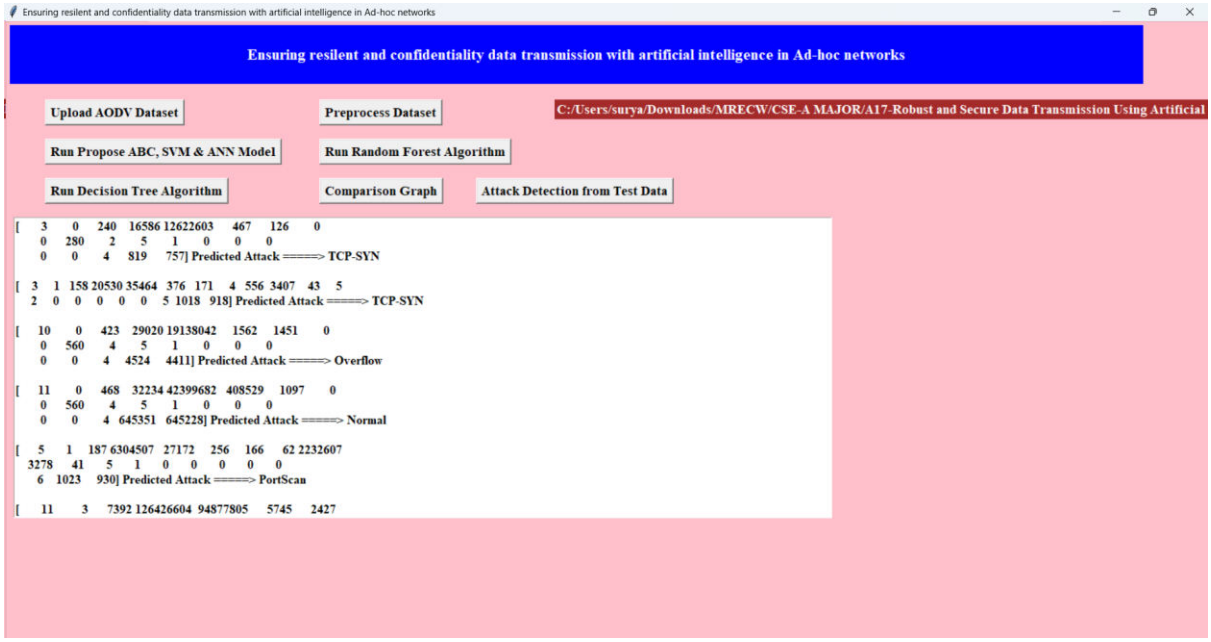

Figure 6: Displays the prediction of the test data.

5. CONCLUSION AND FUTURE SCOPE

The project focused on ensuring resilient and confidential data transmission in ad-hoc networks using artificial intelligence has successfully addressed critical challenges in the domain of secure communication. The integration of artificial intelligence into ad-hoc networks has shown promising results in enhancing the resilience and confidentiality of data transmissions. The project has contributed to the development of robust mechanisms that dynamically adapt to changing network conditions, ensuring reliable and secure communication in challenging environments.The artificial intelligence algorithms employed in the project have demonstrated their effectiveness in identifying and mitigating security threats, such as malicious nodes or eavesdropping attempts, in real-time. The incorporation of adaptive encryption and routing strategies based on AI-driven insights has significantly bolstered the security posture of ad-hoc networks.

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.; 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.

4. Tamilselvan, L.; Sankaranarayanan, V. Prevention of Co-operative Black Hole Attack in MANET. J. Netw. 2008, 3, 13–20.

5. Kang, B.-S.; Ko, I.-Y. Effective Route Maintenance and Restoration Schemes in Mobile Ad Hoc Networks. Sensors 2010, 10, 808–821.

6. Himral, L.; Vig, V.; Chand, N. Preventing aodv routing protocol from black hole attack. Int. J. Eng. Sci. Technol. (IJEST) 2011, 3, 3927–3932.

7. Panigrahi, R.; Borah, 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.

8. 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), San Antonio, TX, USA, 27–31 January 2002.

9. 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.

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

11. 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 Forest Algorithms. Hum.-Cent. Comput. Inf. Sci. 2021, 11, 24.

12. 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.