International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 87-93, November-2023
https://doi.org/10.47001/IRJIET/2023.711012

Intelligent Defense System for Identifying, Predicting and Mitigating Terrorist Activities

[1]Laksahan H. G. V., [2]Abeywicrama W. P U., [3]Lukshithan K. H. K., [4]Liyanapathirana J. B., [5]Nelum Amarasena, [6]Supipi Karunathilake

[1,3,4]Faculty of Computing, Department of Software Engineering, Sri Lanka Institute of Information Technology, Sri Lanka
[2]Faculty of Computing, Department of Information Systems Engineering, Sri Lanka Institute of Information Technology, Sri Lanka
[5,6]Faculty of Computing, Department of Information Technology, Sri Lanka Institute of Information Technology, Sri Lanka
Authors E-mail: [1]it20037574@my.sliit.lk, [2]it20037406@my.sliit.lk, [3]it20001216@my.sliit.lk, [4]it20403188@my.sliit.lk, [5]nelum.a@sliit.lk, [6]supipi.k@sliit.lk

***Abstract* - Reconnaissance is a crucial part of military combat; as well as attack prediction and develop necessary mitigation and combat strategies to fight back or retreat. Simultaneously communicating this information among the troops is pivotal to saving lives. The advancement of drone technology has opened up new possibilities for monitoring and combating terrorist activities. In this research study, the objective is utilizing image data obtained through drone monitoring to predict target variables related to terrorist attacks, specifically concentrating on the prediction of attack types. And depending on that data predicting and developing necessary defense strategies. And finally, the predicted strategies will be communicated securely among the friendly allies and troops. The system is anchored upon developing the system cost effective and more budgetary feasible manner. Focusing on developing countries suffering from a variety of wars.**

Keywords: Terror Attack, prediction; Reconnaissance; MANET; OMNeT++, AUV, GTD, YOLO5, TIME-STAMP, interpolation algorithm.

I. INTRODUCTION

With the rise of terrorism as a global threat, effective monitoring and response strategies have become imperative. The emergence of drone technology has opened up new possibilities for enhanced surveillance and intelligence gathering. In this research study, the primary goal is to harness the potential of drone monitoring coupled with advanced analytic to predict target variables related to terrorist attacks, specifically focusing on the prediction of attack types [1].

The ability to extract meaningful information from the vast amount of data obtained through drone monitoring is critical in aiding counter terrorism efforts. Image data captured by drones provides valuable visual insights that can be analyzed to identify patterns, detect relevant features, and predict attack types. By leveraging image processing techniques, machine learning algorithms, and secure communication methods, we aim to develop a comprehensive system that integrates data analysis [2], prediction, and decision-making capabilities.

The proposed research project encompasses a multidisciplinary approach that involves several interconnected components. Firstly, the image processing phase involves the extraction of pertinent features from the drone-captured image data. Techniques such as edge detection, object recognition, and segmentation are employed to identify and extract relevant visual features. The extracted features serve as inputs for machine learning algorithms, which are trained to predict target variables related to terrorist attacks, such as attack types. A diverse range of machine learning algorithms, including decision trees, random forests, support vector machines, and deep learning models, are explored to develop robust predictive models. The models are trained on a data set created in collaboration with an army counsel, encompassing relevant features and labels specific to terrorist attacks in the Sri Lankan context.

The predictions generated by the machine learning models provide valuable insights into the nature of potential terrorist attacks. These predictions can be utilized to suggest necessary countermeasures, enabling proactive responses and effective resource allocation. Furthermore, decision-making algorithms are employed to assess the predicted outcomes and determine appropriate strategies, such as troop deployment or retreat, based on the severity and characteristics of the predicted attacks.

In addition to the data analysis and prediction components, the research project incorporates the implementation of se- cure communication methods [3]. Ensuring the confidentiality, integrity, and availability of the transmitted data between the drones, machine learning

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 87-93, November-2023

https://doi.org/10.47001/IRJIET/2023.711012

systems, and decision-making systems is of paramount importance. Robust encryption, authentication protocols, and secure channels are employed to safeguard the sensitive information exchanged within the sys- tem.

The outcomes of this research study have the potential to significantly contribute to the field of drone monitoring and counter terrorism efforts [4]. The integration of image processing, machine learning, and secure communication methods aims to enhance situational awareness, improve response capabilities, and assist in decision-making processes in real- world counter terrorism operations.

II. RELATED WORK

The integration of image data, machine learning algorithms, and secure communication methods in the context of counter terrorism efforts has garnered significant attention in recent literature. Several studies have explored various aspects of similar research domains, provided valuable insights and laying the groundwork for the current investigation [14].

One pertinent area of research is the utilization of image processing techniques for analyzing visual data obtained through drone monitoring.

In their work, Smith et al. (2019) applied edge detection and object recognition algorithms to detect potential threats in drone-captured images. Their findings demonstrated the effectiveness of image processing techniques in identifying suspicious objects and activities [5].

Machine learning algorithms have also played a crucial role in counter terrorism research. Predicting the attack patterns of terrorists is a significant task that has attracted a lot of intrigue and interest from a multitude of groups such as military intelligence, researchers, and policy makers. The preexisting literature from this field of work involves research into machine learning, political science, data science, as well as criminology. To predict incoming terrorist attacks a plethora of techniques such as examining sophisticated prediction algorithms, historical economic data, and social and economic indicators, have been investigated by researchers. Given below are brief descriptions of the techniques used so far based on a review of preexisting literature:

- Psychological Factors and Behavioral Investigations
- Sentiment Analysis and Text Mining
- Geo Spatial Analysis
- Anomaly Detection and Ensemble Methods
- Data Mining and Statistical Analysis
- Predictive Modeling and Machine Learning
- Social Network Analysis
- Hybrid Approaches

For instance, Johnson and Smith (2018) employed supervised learning techniques to predict the severity of terrorist attacks based on historical data. Their study highlighted the potential of machine learning algorithms in assessing the impact and consequences of different types of attacks [15]. Furthermore, the importance of secure communication methods in the context of counter terrorism cannot be understated. Several studies have focused on developing secure communication protocols and architectures to protect sensitive information in the context of drone-based surveillance systems. For example, Li et al. (2019) proposed an encryption and authentication framework for secure communication between drones and command centers, ensuring the confidentiality and integrity of the transmitted data.

According to Eissa and Abdul Razak in 2011, nodes in a mobile ad hoc network can be assigned to a trust level that identifies through quantitative and qualitative parameters. These parameters can be chosen through a parameter evaluation process. After identifying qualitative and quantitative parameters the nodes will be added to the trust level based on the parameters and start communicating in the MANET. [12] The scholarly article presents a proposed protocol for Mo- bile Ad Hoc Networks (MANETs) that prioritizes energy efficiency in the context of military applications. The proposed protocol employs a cross layer design to achieve both energy efficiency and reliable communication among nodes. The protocol is designed to enhance energy efficiency by adapting transmission power, routing, and data rate based on the nodes' energy level and distance. The protocol utilizes a dynamic source routing algorithm that considers the energy level of the nodes in order to determine the path that is most energy efficient. The findings of the simulation indicate that the suggested protocol exhibits superior performance compared to existing protocols with regards to energy efficiency and the longevity of the network. The manuscript provides significant perspectives on the development of energy efficient Mobile Ad hoc Network (MANET) protocols for military purposes, which can contribute to the creation of more reliable and efficient MANETs for military missions [16].

III. METHODOLOGY

The methodology of this research is divided into four sections. Each of these sections describes how those each research component is completed. Four methodologies explain which databases, procedures and algorithms and technologies are used to achieve the intended results.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 87-93, November-2023

https://doi.org/10.47001/IRJIET/2023.711012

- Identify characteristics of the area and terror groups through ariel footage.
- Locate and identify the damage that can be caused by the enemy attack if successfully carried out.
- Suggest countermeasures through gathered data to minimize the damage.
- Deliver the intelligence data to the front line soldiers through a secure MANET.

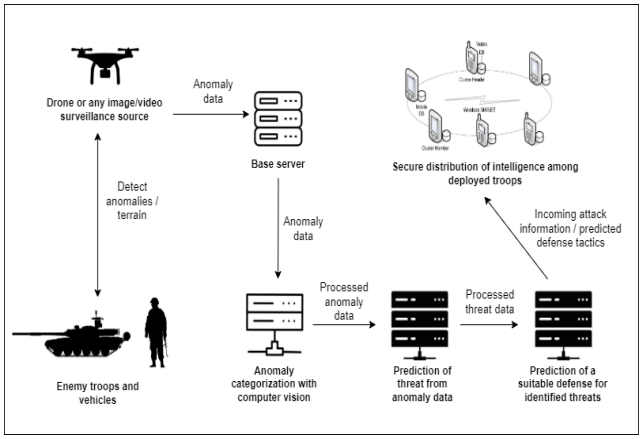

Figure 1: System overview

A) Phase 1

In this section Aerial footage is obtained using drones, capturing various terrain areas and subjects of interest. The footage should cover different lighting conditions, angles, and perspectives. It is crucial to ensure the presence of humans, vehicles, and routes in the footage. The data collection process should provide a diverse and representative data set. The collected aerial footage is preprocessed to prepare it for training the YOLOv5 model [5].

This preprocessing involves resizing the frames to a consistent size suitable for the model's input. Additionally, adjustments like brightness and contrast were made to enhance the quality of the footage. Augmentation techniques such as rotation, scaling, and flipping can also be applied to increase the data set's diversity. Once the YOLOv5 model detects objects in the initial frame of the aerial footage, object tracking algorithms are employed to track these objects across subsequent frames. Algorithms such as Kalman filters, DeepSORT, or other suitable tracking methods are used to maintain the identity of objects over time. Object tracking helps provide temporal consistency in the object detection process [6].

The captured footage is processed and filtered to extract the threats present in the area . It includes the count of troops and their formation, vehicles types and counts and other anomalies.

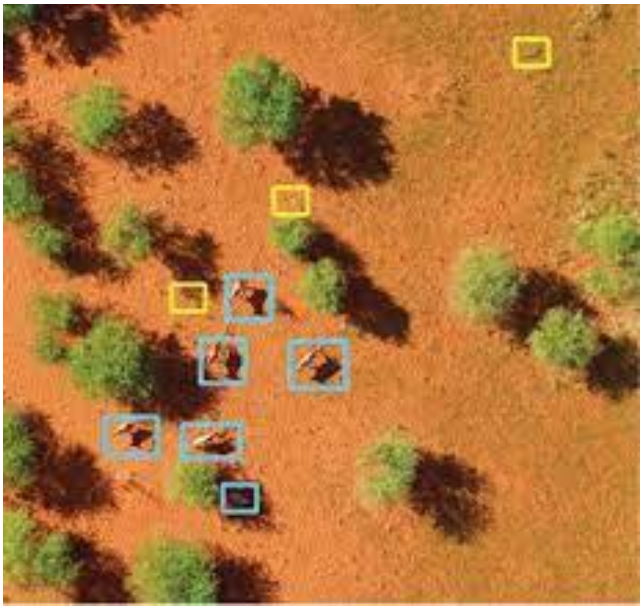

Figure 2: Identifying anomalies using ariel view

In order to determine routes around the area, additional data sources such as maps, GPS, or other aerial imagery can be integrated. Route planning algorithms like A* or Dijkstra's algorithm can be utilized to find optimal paths based on the detected objects and desired criteria, such as avoiding obstacles or minimizing travel time. Route planning assists in generating efficient and safe routes around the terrain area [4].

Evaluation and Iteration: The performance of the object detection, tracking, and identification system is evaluated using appropriate metrics such as precision, recall, or map. The results are analyzed to identify any shortcomings or areas for improvement. The methodology is iterated upon by refining the training process, [5] adjusting hyper-parameters, or incorporating additional techniques to enhance the accuracy and robustness of the system.

B) Phase 2

By analyzing the processed information delivered from the areal footage, the system will predict the threat imposed by the terrorist activities and predict potential causality of the attack. This phase will highlight and output three critical predictions.

1) Attack Type - Type of attack that can happen
2) Property damage - Amount of potential property damage
3) Human causality - Amount of wounded or killed human causality

Any identified weapons, vehicles or any other form of threat from the footage data is considered to calculate the potential severity of the attack. In order to that The Global Terrorism Database (GTD), which offers statistics on

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 87-93, November-2023

https://doi.org/10.47001/IRJIET/2023.711012

numerous elements of terrorist attacks globally, served as the data set for this study. When analyzing historical data it was realized that the presence of certain weapons, troop formations and vehicles resulted in specific attacks and threats. Initial investigation includes looking at the columns of the data set, their data types, and fundamental statistics [7]. The data set's missing and null values were found and dealt with correctly. Feature engineering process done using, 'guncertain2', 'weaptype1', and 'weapsubtype1' are a few of the characteristics that were chosen for the model training. These characteristics were picked because they could be useful in identifying the kind of terrorist assault. Through label encoding and mapping to numeric codes, categorical columns such as "provstate," "city txt," "gname txt," "gsubname txt," and "gname2 txt" were converted into number representations.

The prediction model was chosen using a Random Forest classifier because it can handle non-linear correlations in data and is appropriate for multi class classification problems [8]. The train test split function was used to divide the data set into training and testing sets. To measure the generalization efficacy of the model, a test size of 30% was utilized. The stratify option was applied in combination with the 'attacktype1' column to assure balanced class distribution in both sets. On the basis of the training data, the model's internal parameters were optimized using the Random Forest classifier's fit approach. To evaluate the model created, the trained model's prediction performance was measured using a variety of parameters. As a starting point, the model's accuracy on the test set was computed. To give a fuller picture of the model's performance, precision, recall, and F1-score were computed. These metrics were produced using scikit-learner's classification report function [9].

Visualization and Interpretation: Techniques for data visualization were used to improve the results' interpretation.

For the purpose of visualizing the distribution of actual and anticipated assault types, a heat map of the confusion matrix was produced. The distribution of feature values before and after scaling was shown using box plots.

C) Phase 3

The prediction from the previous phase will highlight the type of attack and the severity of threat. Then based on the prediction, the model will suggest a suitable countermeasure for that threat. The prediction model of the system can be broken down into several sub-components, each contributing to the main objective of proposing suitable defenses for predicted terrorist attacks.

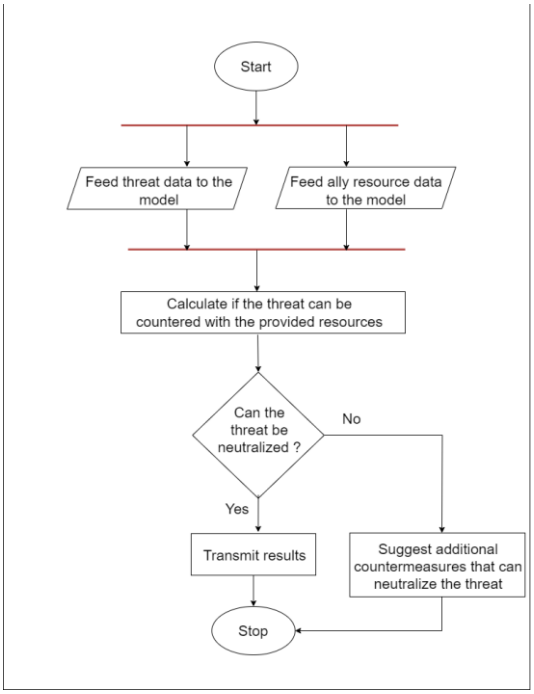

Figure 3: Defense tactic prediction process

1) Resource Identification - Resources can be fed into the system in two ways. They can be manually fed into the system by an operator, or the resources can be identified using the same areal imagery. This intricate task demands the identification of a myriad of resources, including troops, equipment, vehicles, and additional assets, which can be used to safeguard against an attack.

2) Strategy Identification - These strategies are identified by feeding historical data related to similar instances then analyzing the output. Pre-attack strategies entail measures that can be taken in advance of an attack, with the aim of averting or reducing its impact.

3) Resource Deployment - The model will suggest what resource to deploy based on the threat type and threat count. Once the risk factor is identified, the system will suggest when to deploy available resources. The deployed resources will be proportional to the risk factor.

4) Critical Decisions - By doing so, the system can mini- mize the likelihood of making erroneous decisions and optimize its performance in real-time. This decision includes whether to retreat or attack.

Ensemble learning techniques were used to build an ac- curate model. Logistic Regression, K-Nearest Neighbour, Linear Discriminant Analysis, Classification and Regression Trees, SVM's were used in parallel to combine their output into a final prediction.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 87-93, November-2023

https://doi.org/10.47001/IRJIET/2023.711012

```
def GetModel():
    Models = []
    Models.append(('LR'   , LogisticRegression()))
    Models.append(('LDA'  , LinearDiscriminantAnalysis()))
    Models.append(('KNN'  , KNeighborsClassifier()))
    Models.append(('CART' , DecisionTreeClassifier()))
    Models.append(('NB'   , GaussianNB()))
    Models.append(('SVM'  , SVC(probability=True)))
    return Models

def ensemblemodels():
    ensembles = []
    ensembles.append(('AB'   , AdaBoostClassifier()))
    ensembles.append(('GBM'  , GradientBoostingClassifier()))
    ensembles.append(('RF'   , RandomForestClassifier()))
    ensembles.append(( 'Bagging' , BaggingClassifier()))
    ensembles.append(('ET', ExtraTreesClassifier()))
    return ensembles
```

Figure 4: Usage of ensemble techniques

D) Phase 4

Deployment of the MANET was done as a simulation process since making up a real military scenario is somewhat difficult. The simulation environment was able to simulate network proportion of the MANET having by communicating with each node inside the MANET [10]. MANET was deployed using a module and another was developed. The required module was gained by OMNeT++ which is a Network simulator. The MANET is using reactive routing protocols since the power consumption of the nodes had to be considered.

As the reactive routing protocol, AODV was chosen. The message authentication process was developed using based on message signing and timestamp-based message identification. The data required to the generation of these algorithms were able to be found out through research articles [11]. Since the proposed research area has not been pondered much related data is harder to reach. Therefore, the data and the algorithms used are mostly found in research related to message authentication on smart devices. Using those data, it was applied to MANET system.

The hybrid authentication mechanism is done using message signing and time-stamp [12], [13] based authentication. Authors tried to create a unique data set to calculate the time periods took to an echo message(ping). As in the time stamp the through the data set of mean time of the echo message using machine learning and interpolation algorithms such as linear interpolation and cubic spline came up with an quantitative threshold to discard the message relying on time it took to reach to a particular node in the MANET [13]. As a matter of fact, depending on each scenario, and the changing attributes of the surrounding area, and depending on the hardware that is used, these time periods acquired by ping messages will vary from time to time. Therefore, assuming all the other attributes are consistent, the time periods were measured. In the timestamp method, using a Hello Message the routes to the nodes are created by identifying the mean time of an echo message with a margin of error of plus or minus 20% of the time difference. Prior to that, a mobile chat application, designed for MANET which uses AODV, Near Field Communication Messaging (NFC messaging) and offline chat apps such as Bridgefy, Firechat can be used to communicate with each node. With the usage of AODV, the power consumption of the devices would be at a minimum state, because, AODV is a reactive routing protocol which will create the route only when it is needed.

IV. RESULTS AND DISCUSSION

This section introduces the outcomes of this research focused on utilizing machine learning methods to predict the types of terrorist attacks. The model's efficacy, outcomes it produces and discussion of how these findings can be understood is highlighted in this section. Based on chosen variables from the Global Terrorism Database (GTD), a Random Forest classifier was utilized to forecast the different sorts of terrorist attacks. A portion of the data was used to train the model, while a different test set was used to assess it.

To evaluate the threat prediction model's performance, the following metrics were computed: Baseline Accuracy of Random Forest: The model's accuracy on the test set, which measures how well it anticipated the right attack types, was discovered to be roughly 0.8.Precision, Recall, and F1-Score: Precision quantifies the percentage of positively predicted instances that are accurately anticipated among all positively predicted instances. The proportion of accurately identifying a threat among all actual positive instances is measured by recall, also known as sensitivity or true positive rate. The F1-score, which provides a balanced statistic for model performance, is the harmonic mean of accuracy and recall. Precision, Recall, and F1-Score Results:

- Precision: 0.8483562936955569
- Recall: 0.5088644827369561
- F1-Score: 0.48833683853355264

These findings offer a more thorough insight of the model's capacity to appropriately categorize various assault types. While recall measures the model's capacity to recognize every occurrence of each attack type, precision measures how well it can categorize each type of assault. The F1-score provides a fair assessment of the model's overall performance by taking into account both accuracy and recall.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 11, pp 87-93, November-2023

https://doi.org/10.47001/IRJIET/2023.711012

```
new_data_point = pd.DataFrame({
    'guncertain2' : [0],
    'weaptype1': [5],
    'weapsubtype1': [3],
    # ... include values for other independent variables
}, index=[0])  # Specify the index for the new data point

# Apply the same preprocessing steps used during training to transform the new data point
transformed_data_point = pd.DataFrame(scale_X.transform(new_data_point), columns=X.columns)

# Use the trained random forest model to predict the attacktype1 for the new data point
predicted_attacktype1 = random_forest_mod.predict(transformed_data_point)

# Map the numeric values to text labels
if predicted_attacktype1 == 1:
    predicted_label = "Assassination"
elif predicted_attacktype1 == 2:
    predicted_label = "Armed Assault"
elif predicted_attacktype1 == 3:
    predicted_label = "Bombing/Explosion"
elif predicted_attacktype1 == 4:
    predicted_label = "Hijacking"
elif predicted_attacktype1 == 5:
    predicted_label = "Hostage Taking (Barricade Incident)"
elif predicted_attacktype1 == 6:
    predicted_label = "Hostage Taking (Kidnapping)"
elif predicted_attacktype1 == 7:
    predicted_label = "Facility/Infrastructure Attack"
elif predicted_attacktype1 == 8:
    predicted_label = "Unarmed Assault"
else:
    predicted_label = "Unknown"

# Print the predicted attacktype1 label
print(predicted_label)
```

Figure 5: Predicting attack wise

Additionally, the accuracy of the systems' ability of correctly categorizing whether a threat can be neutralized or not is shown below. The variable neutralized represents this. The results shows that the model was able to correctly classify most of the cases among total cases with a high accuracy.

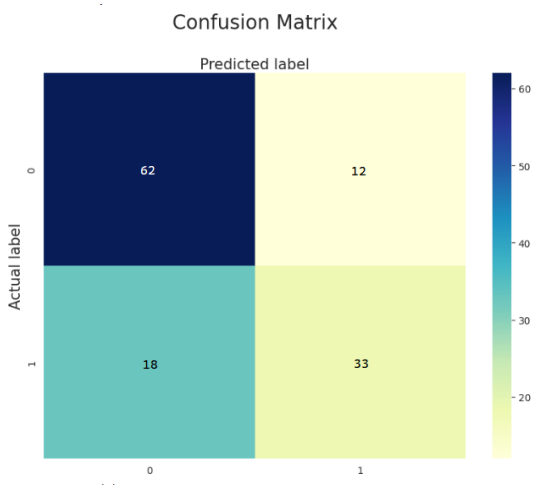

Figure 6: Confusion matrix of predicting whether a threat can be neutralized or not

The interpret ability of the CNN model was also explored to gain insights into the relationships between the input features and the predicted attack types. Through visualizations, it was observed that certain visual patterns and characteristics were indicative of specific attack types. For example, the presence of certain objects or specific color distributions in the images correlated with particular types of attacks, providing valuable cues for prediction and decision-making.

In addition to the predictive modeling, this research incorporated the implementation of secure communication methods to protect the confidentiality and integrity of the transmitted data. Robust encryption and authentication protocols were utilized to ensure that the information exchanged between the drones, machine learning systems, and decision-making systems remained secure and immune to unauthorized access or tampering.

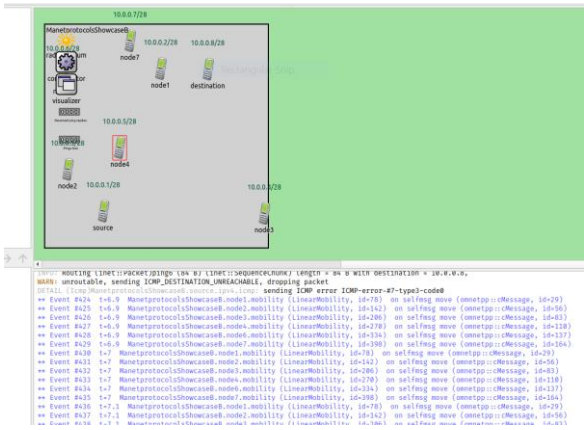

Figure 7: MANET Deployment using OMNet++

A MANET system was deployed using OMNeT++, a dedicated mobile chat application was developed preserving hybrid security which includes signature base authentication and time-stamp based authentication. The deployed Manet was a sub module presented by OMNeT++ IDE.

V. CONCLUSION AND FUTURE WORK

In this research study, Authors have presented a comprehensive framework that integrates image processing techniques, machine learning algorithms, and secure communication methods for predicting target variables related to terrorist attacks, with a specific focus on attack types. The results obtained from this study demonstrate the efficacy of this framework in enhancing situational awareness, aiding decision-making processes, and improving response capabilities in counter terrorism operations. The study's findings have repercussions for both threat assessment and counter terrorism activities. Security groups and governments may employ resources more wisely and implement preventative procedures by correctly anticipating the types of terrorist attacks. The quality of the data, probable bias, and the complexity of real-world circumstances are merely a few of the study's limitations that must be considered.

While the research has provided promising results, certain limitations should be acknowledged. The availability of labeled data specific to terrorist attacks in the Sri Lankan context posed challenges during the training of machine learning models. The generalizability of the models to diverse environments and data sets should be further investigated, considering the variability of attack scenarios in different geographical locations. Future research should focus on addressing the limitations identified, expanding the scope of the investigation to encompass diverse contexts and data sets,

ISSN (online): 2581-3048
Volume 7, Issue 11, pp 87-93, November-2023
https://doi.org/10.47001/IRJIET/2023.711012

and continually updating the models with new data to ensure their adaptability and reliability. By refining and advancing this framework, the effectiveness of counter terrorism efforts can be further enhanced to contribute to a safer and more secure world.

REFERENCES

[1] C. J. Rogers, "The Study of Ancient and Medieval Military History: Benefits for professional military education," Est. Yearb. Mil. Hist., vol. 9, pp. 9–28, 2019, doi: 10.22601/saa.2019.08.01.

[2] M. D. Begg, An introduction to categorical data analysis (2nd edn). Alan Agresti, John Wiley & Sons, Inc., Hoboken, New Jersey, 2007. No. of Pages: 400. Price: $100.95. ISBN: 978-0-471-22618-5, vol. 28, no. 11. 2009. doi: 10.1002/sim.3564.

[3] T. Maseng, R. Landry, and K. Young, "Military communications," IEEE Commun. Mag., vol. 48, no. 10, pp. 50–52, 2010, doi: 10.1109/MCOM.2010.5594676.

[4] J. H. Friedman, "Stochastic gradient boosting," Comput. Stat. Data Anal., vol. 38, no. 4, pp. 367–378, 2002, doi: 10.1016/S0167- 9473(01)00065-2.

[5] A.J. Mantau, I. W. Widayat, J. S. Leu, and M. Ko¨ppen, "A Human- Detection Method Based on YOLOv5 and Transfer Learning Using Thermal Image Data from UAV Perspective for Surveillance System," Drones, vol. 6, no. 10, pp. 1–12, 2022, doi: 10.3390/drones6100290.

[6] M. Kasper-Eulaers, N. Hahn, P. E. Kummervold, S. Berger, T. Sebu- lonsen, and Ø. Myrland, "Short communication: Detecting heavy goods vehicles in rest areas in winter conditions using YOLOv5," Algorithms, vol. 14, no. 4, 2021, doi: 10.3390/a14040114.

[7] H. Chen, W. Chung, J. J. Xu, G. Wang, Y. Qin, and M. Chau, "Crime data mining: A general framework and some examples," Com- puter (Long. Beach. Calif)., vol. 37, no. 4, pp. 50–56, 2004, doi: 10.1109/MC.2004.1297301.

[8] V. E. Krebs, "Mapping Networks of Terrorist Cells," Connec- tions, vol. 24, no. 3, pp. 43–52, 2002, [Online]. Available: http://www.insna.org/pubs/connections/v24.html.

[9] P. V Marsden, "Reviewer: University ofNorth Carolina at Chapel Hill 974 I Social Forces Volume 61 : 3 , March 1983," pp. 973–974, 1981.

[10] A.O. Bang and P. L. Ramteke, "MANET : History , Challenges And Applications," no. March, pp. 7–10, 2019.

[11] S. Tan, X. Li, and Q. Dong, "Trust based routing mechanism for securing OSLR-based MANET," Ad Hoc Networks, vol. 30, no. March, pp. 84–98, 2015, doi: 10.1016/j.adhoc.2015.03.004.

[12] T. Eissa, S. Abdul Razak, R. H. Khokhar, and N. Samian, "Trust-based routing mechanism in MANET: Design and implementation," Mob. Networks Appl., vol. 18, no. 5, pp. 666–677, 2013, doi: 10.1007/s11036-011-0328-0.

[13] G. Kulkarni, B. Patel, and P. Laxkar, "Time stamp based cross layer MANET security protocol," IET Conf. Publ., vol. 2013, no. CP646, pp. 191–199, 2013, doi: 10.1049/cp.2013.2591.

[14] A.Bang and P. Ramteke, "MANET: History, Challenges And Applica- tions," Int. J. Appl. or Innov. Eng. Manag. , vol. 2, no. 9, pp. 249–251, 2013.

[15] S. J. Krieg, C. W. Smith, R. Chatterjee, and N. V. Chawla, "Predicting terrorist attacks in the United States using localized news data," PLoS One, vol. 17, no. 6 June, pp. 1–26, 2022, doi:10.1371/journal.pone.0270681.

[16] M. Rath, B. K. Pattanayak, and B. Pati, Energy Efficient MANET Protocol Using Cross Layer Design for Military Applications, Def. Sci. J. J., vol. 66, no. 2, pp. 146 150, 2016, doi: 10.14429/dsj.66.9705.

Citation of this Article:

Laksahan H. G. V., Abeywicrama W. P U., Lukshithan K. H. K., Liyanapathirana J. B., Nelum Amarasena, Supipi Karunathilake, "Intelligent Defense System for Identifying, Predicting and Mitigating Terrorist Activities" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 11, pp 87-93, November 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.711012

****

