International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Logistic Regression Based Malicious UAV Tracking in WSN

S.V.R Vara Prasad[1],Gulla Sulochana[2],Kunibilli Jaswanth[3],Akula Leela Prasanna[4],Bevara Sowmya Laxmi[5]

[1]*Assistant Professor,* [2-6] *BTech Student, LIET*
[1,2,3,4,5] Computer Science and Information Technology, Lendi Institute of Engineering and Technology, Vizianagaram

---

ABSTRACT

In recent years, Unmanned aerial vehicles (UAV) assisted WSNs have had a major impact on wireless communication. The sensor nodes are deployed for efficient and effective data collection by considering UAVs as mobile sinks in WSN. Due to the deployment and wide range of access, UAVs are focused on academia and industry UAV-assisted communication includes UAV-assisted relaying, dissemination, coverage extension, and data collection. UAV-based WSN permits only the cluster head to communicate with UAV. UAVs are applicable in several domains due to their attributes such as flexibility, mobility, and adaptability to different environments. For wireless communication systems, UAV offers services as aerial base stations. While compared with the traditional base stations, energy resources, reliability, and coverage are restricted. However, the UAV components are not modeled with the security approaches. Insufficient security and drone movement causes problems including excessive latency, high energy usage, and unauthorized access. In our proposed system we implemented a Linear Regression system for malicious UAV tracking in WSN.

Key Words: UAV, LR, Malicious UAV

1.INTRODUCTION

A Wireless Sensor Network (WSN) is a combination of various sensors integrated for different tasks and purposes and are rendered or separated by distance or location. The architecture of WSN. Sensor nodes are used for information gathering and also for the transfer of the considered packet back to the destination in the network. The base station is the node which is a bit different from the rest of the nodes as it has high energy-related resources, high computational power, and also strong communication power, following proper information processing and collection. WSN is used in several other sectors, Such as in applications for military, medical, landslide detection, and many more. Malicious UAVs are those that either carry restricted explosive payload or collect audiovisual data from restricted private geographic territory. Moreover, a UAV can be considered malicious when it loses control and enters the nonflying zone. The low-altitude flight of a malicious drone enables it to violate the security measures of a restricted zone, as shown in Figure 1. Restricted areas protect sensitive locations, such as prisons and nuclear facilities. The official definition of such a restricted area is “an airspace of defined dimensions above the land areas or territorial waters of a State within which the flight of aircraft is restricted under certain specified conditions”.

Intrusion of malicious drones:

There is a need for a technology that can detect and disarm such malicious UAVs promptly. Recently, various techniques for UAV detection have been reported in the literature, relying on audio, video, thermal, and radio frequency signals. Each scheme has its advantages and limitations. The video- and thermal-based detection techniques fail in adverse weather conditions. The sound of a UAV’s motor fan and its images are useful to differentiate the amateur UAV from other objects. The audio-based detectors are cost-effective as they require only an array of microphones to capture the sounds and classify them in their respective class. However, environmental noise can degrade the performance of sound-based detection.

We propose a machine-learning-influenced audio and vision-based UAV detection method. The proposed scheme is capable of detecting UAVs with higher accuracy, even in a noisy environment. The proposed hybrid method consists of acoustic and image processing algorithms for the precise detection of amateur drones. The classification accuracy obtained using a handcrafted and deep neural network is compared with the proposed framework. Various handcrafted feature extraction methods for image description, such as Local Binary Pattern, Histogram of Oriented Gradient, Locally Encoded Transform Feature Histogram, Gray Level Co-occurrence Matrix,

Completed Joint-scale Local Binary Pattern, Local Tetra Pattern, and Non-Redundant Local Binary Pattern, have been employed to detect objects based on their texture. Moreover, several handcrafted feature extraction methods for audio have been proposed, such as Linear Predictive Cepstral Coefficients, and Mel Frequency Cepstral Coefficients. The deep neural network models such as Alex Net, ResNet-50, VGG-19, Inceptionv3, and GoogLe Net have also been utilized for image feature extraction. The support vector machine, along with various kernels, has been employed to classify the extracted feature vectors. The proposed scheme is cost-effective as well as highly accurate, even with a small dataset. The proposed scheme integrates the handcrafted sound descriptor with deep features extracted from the image to detect the malicious drone. This hybrid method has provided better accuracy even in adverse weather conditions.

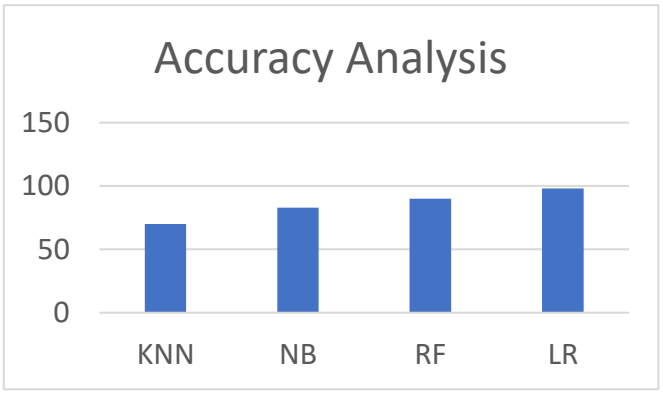
2. PROPOSED METHOD

UAV-based data communication in WSN is deployed with the sensor node, UAV, and base station (BS). The sensor node is located in a random area and it is responsible for collecting data and forwarding it to the UAV. In order to collect the data from SN, the UAV moves along the WSN cluster. The UAV collects information from the SN and sends it to the base station. During this communication, the sensor sends some data packets to the UAV. An adversary compromises with the UAV to launch an attack such as data modification, selective forwarding, and data injection. The process flow for detecting the malicious UAV is described as follows. Initially, the sensor starts transmitting data packets with the generation of authentication parameters and it is transmitted to BS through UAV. Each sensor generates a feedback packet for communicating through UAV.The feedback packet is encrypted before sending it to the base station. By using the incoming packet, the BS creates an authentication parameter by decrypting the feedback packet.

We propose a machine-learning-influenced audio and vision-based UAV detection method. The proposed scheme is capable of detecting UAVs with higher accuracy, even in a noisy environment. The proposed hybrid method consists of acoustic and image processing algorithms for the precise detection of amateur drones. The classification accuracy obtained using a handcrafted and deep neural network is compared with the proposed framework. Various handcrafted feature extraction methods for image description, such as Local Binary Pattern, Histogram of Oriented Gradient, Locally Encoded Transform Feature Histogram, Gray Level Co-occurrence Matrix, Completed Joint-scale Local Binary Pattern, Local Tetra Pattern, and Non-Redundant Local Binary Pattern, have been employed to detect objects based on their texture. Moreover, several handcrafted feature extraction methods for audio have been proposed, such as Linear Predictive Cepstral Coefficients, and Mel Frequency Cepstral Coefficients. The deep neural network models such as AlexNet, ResNet-50, VGG-19, Inceptionv3, and GoogleNet have also been utilized for image feature extraction. The support vector machine, along with various kernels, has been employed to classify the extracted feature vectors. The proposed scheme is cost-effective as well as highly accurate, even with a small dataset. The proposed scheme integrates the handcrafted sound descriptor with deep features extracted from the image to detect the malicious drone. This hybrid method has provided better accuracy even in adverse weather conditions.

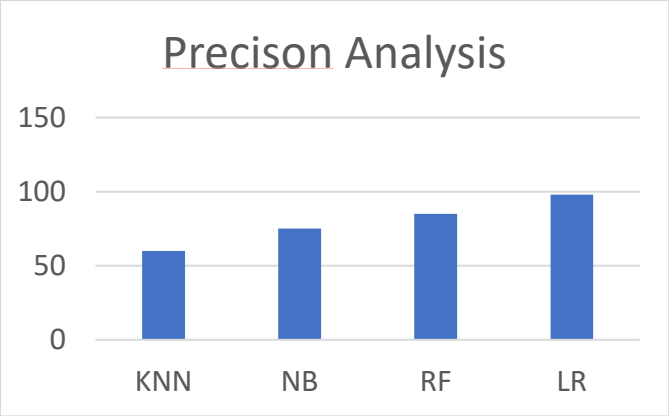
2.1 Graphical Analysis

In order to analyze the effectiveness of proposed study, the performance is compared with other existing studies. For comparison, different existing methods such as K-Nearest Neighbor (KNN), Naïve Bayes (NB), Logistic Regression (LR) and Random Field (RF) are utilized. The performance comparison over existing studies states the ability of proposed approaches. The below figure illustrates the accuracy performance comparison.

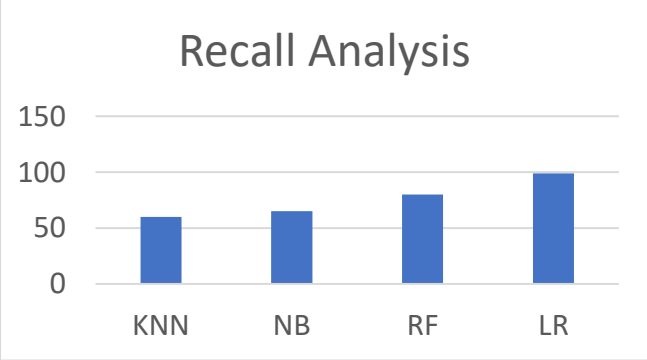


The accuracy performance of the proposed LR approach and varied existing techniques are illustrated in the above graphical representation. The simulation results

clearly shows that the proposed detection approach gained higher accuracy performance as compared with other techniques. The obtained accuracy of proposed LR is 98.61, KNN is 80.2%, NB is 84.2% and RF is 92.8%.The below Figure mentions the precision performance comparison.



The precision performance of proposed study is compared with other existing techniques such as KNN, NB and RF. By comparing with other techniques, the attained precision value of proposed approach is increased. The achieved precision performance of proposed LR is 98.65%, KNN is 80.21%, NB is 84.21%, and RF is 92.8%. The below figure illustrates the sensitivity performance comparison.



The above graphical representation exhibits the sensitivity performance comparison of both proposed and existing methods. The proposed approach obtained the sensitivity performance of 98.63%, KNN is 80.23%, NB is 84.21% and RF is 92.85%. The mentioned values represents that the existing methods attained reduced sensitivity performance due to its inability of detecting malicious UAVS. The below figure depicts the F-measure performance comparison.

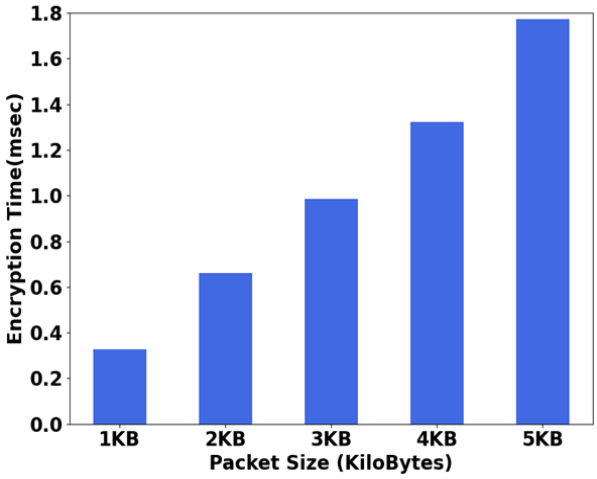


Fig: Encryption time

Measuring the encryption time is necessary to analyze the efficiency of proposed encryption scheme. the obtained encryption time is 1.32ms and at 5KB packet size, the time taken to complete the encryption operation is 1.773ms. Thus, the analyzed results exhibits that the proposed study obtain appropriate encryption time while varying the size of input packets.

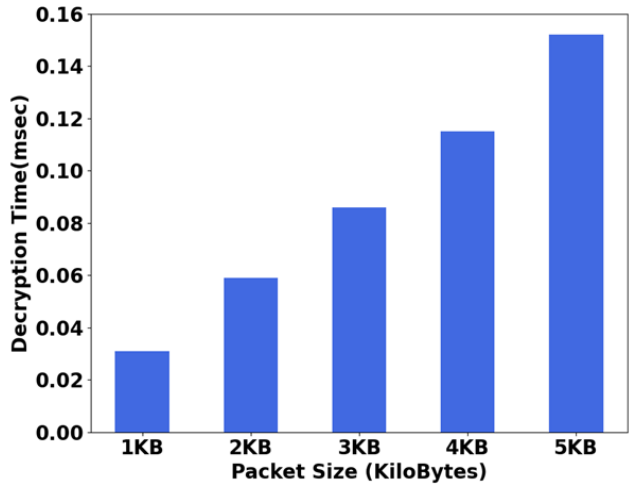


Fig: Decryption time

The decryption process is performed by retrieving the plain text data from the cipher text and the time taken to complete this process is measured. The above figure exhibits the obtained decryption time of proposed proxy re-encryption scheme. By varying the packet sizes, at 5KB packet size, the proposed encryption scheme takes 0.152ms to complete the decryption process. This analysis shows that the proposed scheme only takes reduced time for decrypting the input data. The figure below represents the packet delivery ratio of proposed WSN environment.

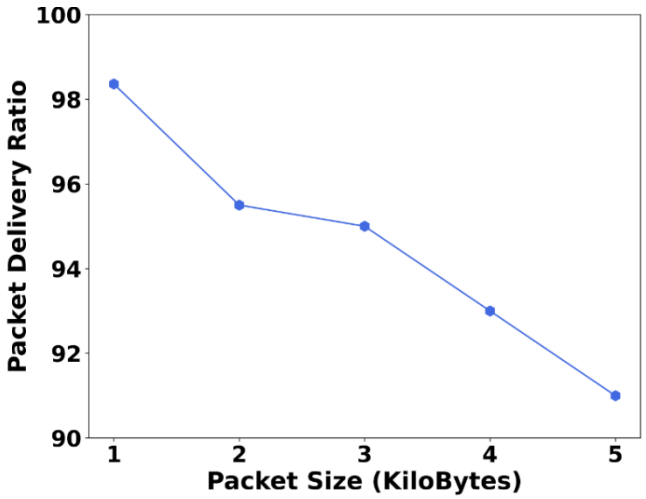


Fig: Attained packet delivery ratio

3. CONCLUSIONS

This paper presents machine learning-based malicious UAV detection in a WSN environment through an effective encryption scheme. Initially, the sensor nodes are randomly deployed in the WSN platform. These sensor nodes are responsible for gathering environmental data such as temperature, humidity, and pressure. After collecting the data, the sensor nodes transmit these data along with an authentication parameter to the nearest UAV.

Because the sensor nodes have no ability to communicate with the UAV. Hence, a feedback packet (authentication parameter) is generated and forwarded to the UAV with the collected environmental data. The UAV faces several malicious attacks which may highly degrade the performance of the entire network system. Thus, to secure the sensed input data, the authentication parameter gets encrypted through a proxy re-encryption scheme.

Whereas, LR is employed to optimally tune the hyperparameters of LR and hence the performance of LR is gets enhanced. The simulation analysis shows that the proposed approaches gained higher performance as compared with other existing methods. The proposed study obtained the accuracy of 98.61%, sensitivity of 98.63%, precision of 98.65% and F-measure of 98.62%. In future, optimal key selection process will be performed to enhance the efficiency of encryption scheme. The proposed study only performs binary classification (attack or non-attack) so that the future study will be extended to detect and classify multiple UAV attacks in WSN platform.

ACKNOWLEDGEMENT

We would like to thank the Department of Computer Science and Information Technology, Lendi Institute of Engineering and Technology, Vizianagaram for helping us to carry out the work and supporting us all the time.

REFERENCES

1. D. Papademetriou and E. Collett, A new architecture for border management, Management Policy Institute, Washington, DC-USA, MAR 2011.
2.G.Loney, Border intrusion detection: thinking outside the perimeter, 41st Annual IEEE International Carnahan Conference on Security Technology, pp. 0106, Oct 2007.
3.E.Systems,Unattended ground sensors network (USGN),http:/defenseupdate.com/newscast/0608/news/news1506 ugs.htm, Copyright 2016 Defense-Update.
4.T.Damarla, A. Mehmood, and J. Sabatier, Detection of people and animals using non-imaging sensors, 14th International Conference on Information Fusion, Chicago-Illinois, USA, vol. 09, no. 03, pp. 468 477, Jul 5-8 2011.
5. K. K.B.Madhavi and G. RishikeshM, Border security using wins, International Journal of Advanced Trends in Computer Science and Engineering, vol. 03, no. 01, pp. 112116, Feb 2014.
6. R. Ramzi Bellazreg, N. Boudriga, K. Trimche, and S. An, Border surveillance : A dynamic deployment scheme for wsn-based solutions, Wireless and Mobile Networking Conference (WMNC), 6th Joint IFIP, vol. 01, pp. 2325, Apr 2013.
7. J. Robert and P. Gervasio, An unattended ground sensor architecture for persistent border surveillance, Proc. SPIE 6980, Wireless Sensing and Processing III, vol. 6980, pp. 69 800A69 800A8, Apr 2008.
8. S. Babu Nr, A. Swaminathan, and D. C. JoyWinnieWise, Boarder analysis with ensora and doa using wireless sensor networks, Sixth International Conference on Emerging trends in Engineering and Technology, pp. 7683, 16-18 Dec 2013.
9. J. Blazakis, Border security and unmanned aerial vehicles, Congressional Research Service, Report for Congress, vol. RS21698, pp. 0106, Jan 2004.
10. C. Haddal and J. Gertler, Homeland security: unmanned aerial vehicles and border surveillance, Congressional Research Service, Report for Congress, vol. RS21698, pp. 0110, JUL 2010.