

A Trustable Security Solutions using XAI for 5G-Enabled UAV

S. B. Goyal^{1,*}, Anand Singh Rajawat², Ram Kumar Solank², Dipak Patil³, Amol Potgantwar⁴

¹ Faculty of Information Technology, City University, Petaling Jaya, 46100, MALAYSIA

² School of Computer Science & Engineering, Sandip University Nashik, INDIA

³ Sandip Institute of Engineering and Management, Nashik, INDIA

⁴ Sandip Institute of Technology, & Research Centre, Nashik, INDIA

drsbgoyal@gmail.com (Corresponding author)

Abstract. It has been challenging to establish stable data transfer and information exchange in 5G UAV networks. This is because UAVs are frequently vulnerable to attack, which can slow data transmission and compromise security. We believe that an Explainable Artificial Intelligence (XAI)-based Trustworthy Security Solution (TSS) for 5G-enabled UAVs would be an effective method for resolving this issue. Our TSS-XAI technique employs XAI to monitor and analyze 5G-enabled UAV network traffic in order to identify attacking nodes. By comparing our TSS-XAI strategy to the previous approach to data detection, we were able to determine its efficacy. Our research indicates that our method can locate attacking nodes at least 98.4 percent of the time. By comparing our TSS-XAI method to AI/DL-based methods, we were able to determine its efficacy. Our results indicate that our method is superior to AI/DL-based methods. Overall, our TSS-XAI method is an effective way to enhance the security of 5G-based UAV networks. It can help ensure the stability and security of data transfer and information exchange.

Keywords: 5G, XAI, Unmanned aerial vehicle, Restricted Boltzmann machine, Reinforcement learning.

1. Introduction

As computer network architectures and 5G-enabled communication (Guo, W., 2020) technologies change quickly, it becomes harder to use traditional security tools and methods to find flaws in 5G-enabled UAV networks' security for route planning and detecting data that is being used to attack. Older cryptographic systems are based on mathematical principles and theoretical limits on how much a computer can do. When sensitive information needs to be sent over a channel that might not be secure, these techniques are widely used. In traditional cryptography, it's hard to figure out how to share encryption keys. All cryptographic algorithms can be roughly put into two groups: those with symmetric keys and those with asymmetric keys. In symmetric key cryptosystems, both encrypting and decrypting use the same key. But the Asymmetric Key Cryptosystem needs not just one key, but two: a key to encrypt and a key to decrypt. Challenges include, but are not limited to, insufficient network monitoring, a lack of attack data or patterns, and the complexity of software and hardware infrastructure. The UAV security system keeps a log, keeps an eye on the network, and does some serious analysis to see if any of the approved systems are being attacked. Both the misuse detection model and the anomaly detection model need data from network logs. The quality of this data is very important to how well these security and prevention systems for 5G-enabled UAVs work. We plan our routes using discrete points that match grids on the map of the search area so that we can find attacks as they happen. As the UAV moves from grid to grid, its speed stays the same (the next one). The amount of time you spend travelling depends on how many grids you go through. The paths of the UAVs will always cross, no matter what. We can rule out a crash because the UAVs aren't in the same place at the same time. But a collision avoidance algorithm is needed to finish the path planning and attack data detection. The biggest problems that none of the models we have right now can solve are finding problems and predicting collisions caused by attacks. Traditional models also couldn't predict the new shortest routes because there were so many problems with navigation. The proposed XAI model (Dazeley et al., 2021) makes it easier for a UAV network with 5G to monitor and analyse traffic for attacking nodes using new shortest distance measures. When putting AI models into production, XAI is a must-have for a 5G-enabled UAV. The proposed method has the system collect important information about the environment before it dynamically checks for obstacles. Next, 5G-enabled UAV nodes use dynamic attack data classification and path reconstruction techniques to find random obstacles between the origin and the destination. These proposed XAI are used to get around obstacles of any shape found in an analysis of traffic patterns (Hodge et al., 2021). Also, a top-of-the-line A Reliable Security Solution for 5G that uses XAI. Due to the 5G network's low latency and high capacity, XAI processing can be spread out across the device, the edge cloud, and the central cloud. This gives users a wide range of new and improved ways to interact with systems. Figure 1 shows that an adaptive 5G-enabled UAV (Zhang et al, 2020; De Dutta & Prasad, 2019) makes the right trade-offs in network security, leading to better network efficiency, easier deployment, and better service quality.

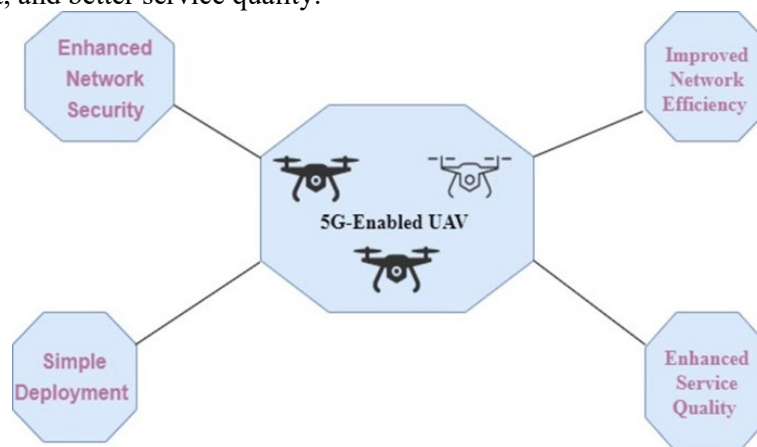


Fig. 1: Basic Service Model For 5G-Enabled UAV

The following sections provide significant contributions to this paper: Section II related work, Section III XAI Basics and the need for XAI in a secure UAV network, Section IV proposed model and algorithm and analysis results, and Section V conclusion and future work.

2. Related Work

Y. Su, et al., (2020) – For 5G UAV communication systems, proposes a revolutionary trust-based security approach. Their proposed system enhances communication performance. Additionally, a trust evaluation scheme for unmanned aerial vehicles (UAVs) is being created to assess their reliability.

Vlahogianni, E.I., et al., (2021) – Deep learning is used to identify traffic conditions based on uncalibrated video recordings collected by unmanned aerial vehicles (UAVs).

Adrian Carrio et al., (2017) – The main issues with using deep learning in UAV-based techniques are discussed.

K. Xiao et al., (2019) – Normal behavior models provide a position used to detect abnormal UAV activities. According to the results of the studies, the proposed anomalous behavior detection technique has a high level of accuracy.

F. Fu et al., (2021) – In urban contexts, this article addresses U2V communications with several eavesdroppers on the ground.

Table 1: A Summary of the Methodology Used To Evaluate Ai/ML/DI Solutions For 5g-Enabled Uavs

S.N.	Citation	AI/ML/DL Solution	Security Level	Evaluation approach
1	Bithas, Petros S et al., (2019)	Machine Learning	Data analysis on 5G	UAV-based communications and security
2	Basim Mahbooba et al., (2021)	Explainable Artificial Intelligence	Large volumes of data reveal hidden patterns and weak signals.	Trust Management in IDS
3	Koumaras, H.; et al., (2021)	Artificial Intelligence	proof-of-concept 5G-enabled UAV	Energy-Efficient Opportunistic Networks
4	Gupta, Rajesh, et al., (2021)	Artificial Intelligence	5G Communications and blockchain	Secure Drone Networking
5	H. Kim, et al., (2020)	Artificial Intelligence	5G Virtual Emotion Applications	Secure Autonomous Vehicles, Drones, and Smart Devices

3. Proposed Methodology

System stability, robustness, and confidence – It should be required for the certification of Artificial Intelligence (AI) systems to thoroughly analyze the hazards of the Artificial Intelligence system's impacts on the environment. Consider the case of a self-driving automobile. The dangers involved are the road users who may be harmed or killed if the automated system makes a single incorrect choice. The task at hand is crucial, and the hazards involved are great. The accuracy of an XAI system is always used to certify its quality when performing a categorization task. Neighboring data collection on Real-time.

3.1. Trustable Security Solution

Even if the explain ability approaches can increase confidence, explanations inherently increase trustworthiness since they provide information that helps to comprehend the model and its predictions. While technological considerations might help with confidence and robustness, a user's trust can also be earned through methods other than objective measurements. A user's trust in an AI system can be

subjectively and objectively defined. Interactions between the user and the AI system could be crucial in establishing confidence between the automated system and the user. Users will not trust automated systems if they lack trust, especially while performing vital activities. For example, AI systems in drones suffer from a lack of customer trust in the 5G enabled UAV (Viana et al., 2021). Such systems may be plagued by a lack of feedback, explaining why the automated system took a specific action. In semi-automated systems, these interactions are particularly crucial. When the AI is working against a user or a business stakeholder, interactions are very critical. The user could look into why they does not agree with the AI prognosis. Figure 2 shows the 5G-Enabled UAV security layer model.

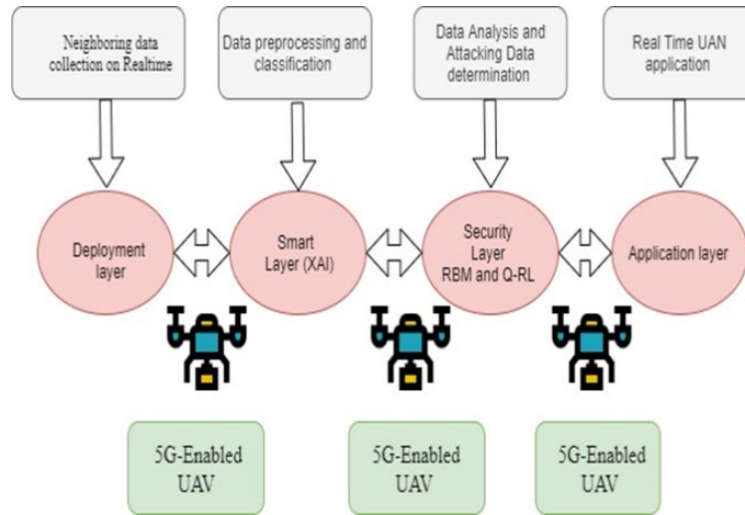


Fig. 2: 5G-Enabled UAV Security Layer Model

3.2. XAI Model for RBM And Reinforcement Learning (RL)

In this study, an original integrated authentication and security model is developed and deployed in XAI-based wireless networks to ensure safe data transfer between mobile, high-speed 5G-enabled UAV (Wang et al., n.a) networks. This was done in order to ensure the safety of the data transfer between these types of networks. During the process of conducting area and infrastructure monitoring, wireless traffic networks are established and then monitored as part of the process. It is necessary to implement an innovative security-based XAI path planning (Keneni et al., 2019) and attacking data detection model in order to defend dynamic UAV networks against attacks from the outside.

Methods from RBM (Decelle & Furtlehner, 2021) and RL (Parak & Matousek, 2021) are utilised in the XAI research field of DDoS attack detection, which is a subfield of the field of study known as XAI. It is possible to determine the probability of the hidden layer given the inputs for the visible layer by using a conditional probability distribution. The same distribution can also be used to determine the probability of the visible layer given the inputs in the hidden layer. This XAI can be utilised in a wide variety of contexts, such as for dimensionality reduction, feature learning, classification, collaborative filtering, and topic modelling. When compared to other learning methods for neural networks, RBM's intralayer connections are more restricted. As a result, RBM's training is more effective, and the learning process is completed more quickly. The RBM incorporates both an open module and a closed module into its design. The visible layer is responsible for the training of the input features, while the hidden layer is responsible for the processing of the inputs. In RBM, the bias-weighted connections between the visible and hidden units are represented by a weight matrix that has binary values. This matrix contains the weights of the connections. The weight matrix is subject to change in accordance with the dynamic behaviour of the network. The softmax classifier located in the hidden layer is responsible for assigning categories to the network traffic based on the target class. The RBM methodology can be applied to goals that have either continuous or discrete value sets. Inputs such as traffic flow features

and their respective threshold values are fed into an RBM's visible layer neurons from reliable network measurements. These inputs come from the RBM's visible layer. The RBM's hidden layer performs independent analysis of incoming traffic flows in a dynamic network environment, learning from the inputs that are provided. Because of the restrictions on intra-layer connectivity, training and learning for traffic flow detection that uses non-standard threshold values can take place more quickly and efficiently. For the purpose of this study, RBM was applied to the task of determining the dynamics of an attack's traffic flows.

This network, as far as RBM can tell, consists of two different nodes. In this particular scenario, we are interested in "L" Evident units $EU = (EU_1, \dots, EU_L)$ and "M" Hidden units $HU = (HU_1, \dots, HU_M)$. The weight matrix between hun and eul is denoted by $WM = (WMLM)$, and a_i and b_j represent the bias weights for the evident units and the hidden units, respectively.

Where, ENERGY (EU, HU) is the RBM deployed network's energy configuration.

Weight matrix between two network nodes. = WLM

Bias unit of visible and hidden layers (a_m, b_n). vm = The network's visible unit.

M = The network's hidden unit.

$$ENERGY(EU, HU) = \sum_{i=1}^L \sum_{j=1}^M W_{M,L} HU_M EU_L - \sum_{i=1}^L a_m EU_L - \sum_{j=1}^M b_m EU_M$$

The following table provides a presentation of the probability distribution for both the visible and the hidden layers of the structure. LPF is an abbreviation for "layer partition function," which describes the layer in question. The constrained connections that exist between the intra layers make it possible to use a speedier learning method when

$$Predicate \frac{HU}{EU} = \prod_{j=1}^m \text{sinmoid}(b_m + EU^T W_m)$$

compared to energy-based models that were used in the past. This is because the intra layers are constrained. This is the function of the predicate

$$P(V, H) = \frac{1}{Z} e^{-(V,H)}$$

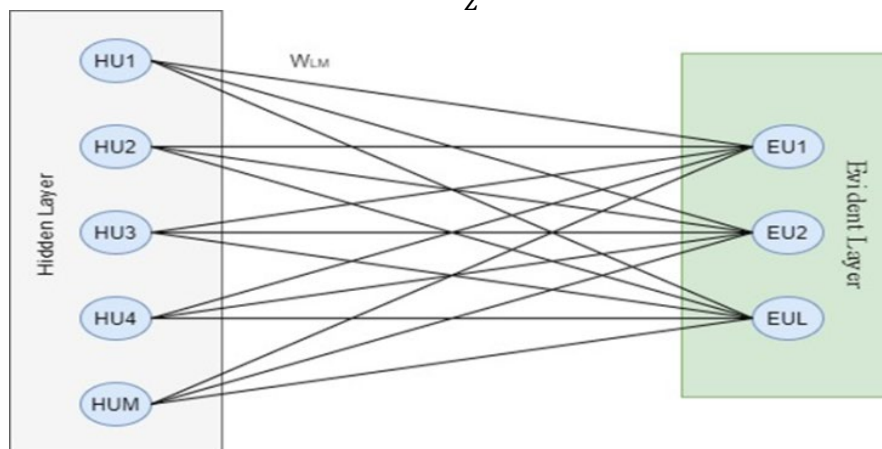


Fig. 3: RBM Structure The Following Is An Illustration of The Probability Distribution of Both The Visible And The Hidden Layers

$$Predicate(EU, HU) = \frac{1}{LPE^{-\langle EU, HU \rangle}}$$

3.3. Q-Reinforcement Learning (QRL)

A trust performance indicator that is updated based on feedback tells the environment what the most rewarding result is for any given observation (performance). This way of learning can be seen as a mix of supervised and unsupervised training that indirectly controls prior knowledge of how a system should work best, even though there isn't any direct training data that goes along with the results that are wanted. Along with QL and Markov decision-making, RL is often used to solve, organise, and manage problems. From inside a 5G-enabled UAV, a representative can connect to each service station to improve QoS and find the best scheduling parameters. Advanced learning applications like power control and optimization can be used in the physical layer of communication networks. We show how to change the transmission power for model-free distributed strengthening learning by using Channel State Information (CSI) and QoS indicators. To figure out the best way to use cutting-edge mapping techniques.

$$\pi: States \rightarrow Actions$$

What is it that the agent tries to optimize?

$$V^\pi(States_t) = R_t + \gamma R_{t+1} + \gamma^2 R_{t+2} + \dots = \sum_{t=1}^{\infty} \gamma^i R_{t+1} \quad 0 \leq \gamma < 1$$

The present benefit is more treasured than future rewards. Could you repeat that would happen if the gamma labyrinth were set to 0? – a value function. Assume we have access to the optimum value function,

$$\pi(States) = ARGMAX \times [R(States, Actions) + \gamma V(\delta(States, Actions))]$$

We assume that we know what the reward will be if we perform action “a” in state “s”: $R(States, Actions)$

We also assume we know what the next state of the world will be if we perform action “a” in state

$$States_{t+1} = \delta(States_t, Actions)$$

Q-Function: One approach to RL is then to try to estimate

$$V(States). \\ V(States) \leftarrow \max [R(States, Actions) + \gamma V(\delta(States, Actions))]$$

However, this approach requires you to know $R(States, Actions)$ and $\delta(States, Actions)$.

We have to apply a function that directly teaches good state action pairings, i.e., which actions should we perform in this state. This is what we refer to as Q. $(States, Actions)$. Executing the best policy is now a piece of cake with Q, without knowing and delta

$$\pi(States) = ARGMAX \times Q(States, Actions)$$

$$V(States) = maxQ(States, Actions)$$

Q-Learning

$$Q(States, Actions) = R(States, Actions) + \gamma V(\delta(States, Actions))$$

$$R(States, Actions) + \gamma maxQ(\delta(States, Actions) Asctions)$$

$R(States, Actions)$ and delta are always important Consider what happens if the drone explores its surroundings and tries new approaches. It obtains an “R” reward at each stage and monitors the surroundings change to a new condition before taking action. How can we use these observations to learn a model?

$$Q(States, Actions) \leftarrow R + \gamma maxQ(States, Action)_{States' = Satates_{t+1}}$$

This equation constantly estimates Q’s state for a single step, specifically time difference, according to Q’s estimates (TD). Since it’s closer to the aim, it is more “confidence-inspiring.” The update of estimations based on other estimates is known as bootstrapping. We make an update after each action pair. Figure 4 shows the major advantages of 5G technologies enabled security modules.

Exploring pairs of activities tells us something useful. These are usually the most beneficial because they are most likely to be found again.

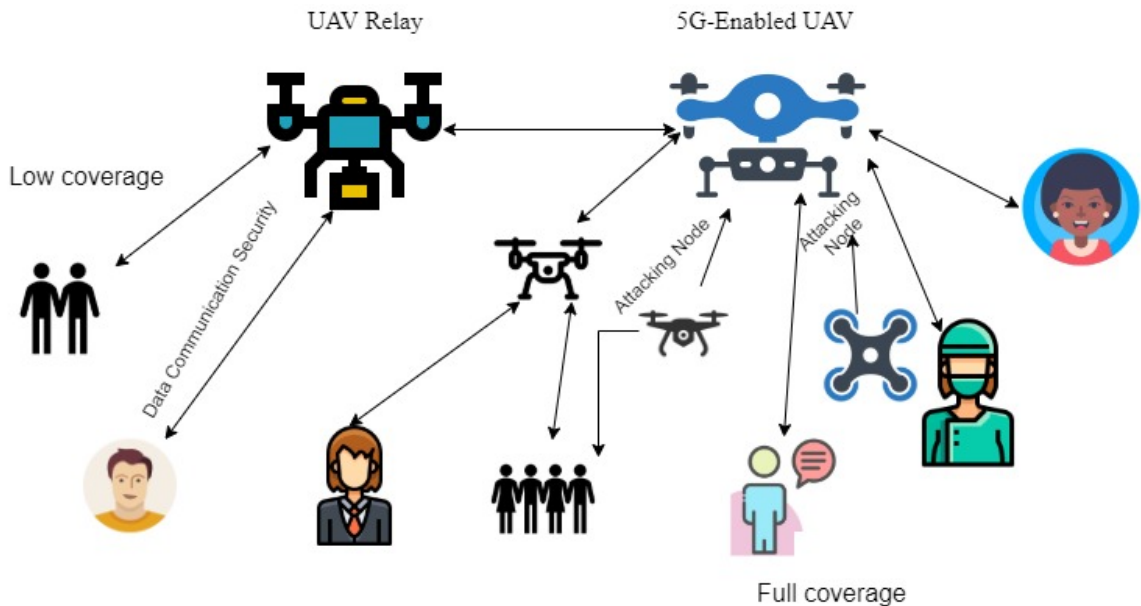


Fig. 4: Major Advantages of 5G Technologies Enabled Security Modules

3.4. Classification of Sensors Data

5G-Enabled UAV (Ning et al., n.a) is already in use in various applications, including smart industry catastrophe prediction, traffic control, and home and city intelligence monitoring. In today’s modern environment, 5G-Enabled UAV devices would be much more in demand and visible. Different agencies will increase their investments in data centers to save and analyze large volumes of data generated (Wu et al., 2020) by 5G-Enabled UAVs. Companies can increase profit and capitalize on client preferences

by integrating and adjusting to customized data. On a bigger scale, massive data and 5G-Enabled UAV can be coupled with the government, and smart cities can be adopted to ensure improved lifestyles, time consumption, finance, and energy use. In today’s living trends, everything is infused with technology. Every organization, especially the government, has its own data center for storing traffic and criminal data. It must be updated daily. When we examine traffic numbers closely, we see that it is significantly more difficult. Figure 5 shows the Traffic analysis is a big issue in 5G-Enabled UAVs. The data center’s technology combines traffic data (Garg et al., 2021) to keep the database up to date. To obtain a clear image of the map. Massive amounts of data from a variety of 5G-Enabled UAVs and data are processed in the same way.

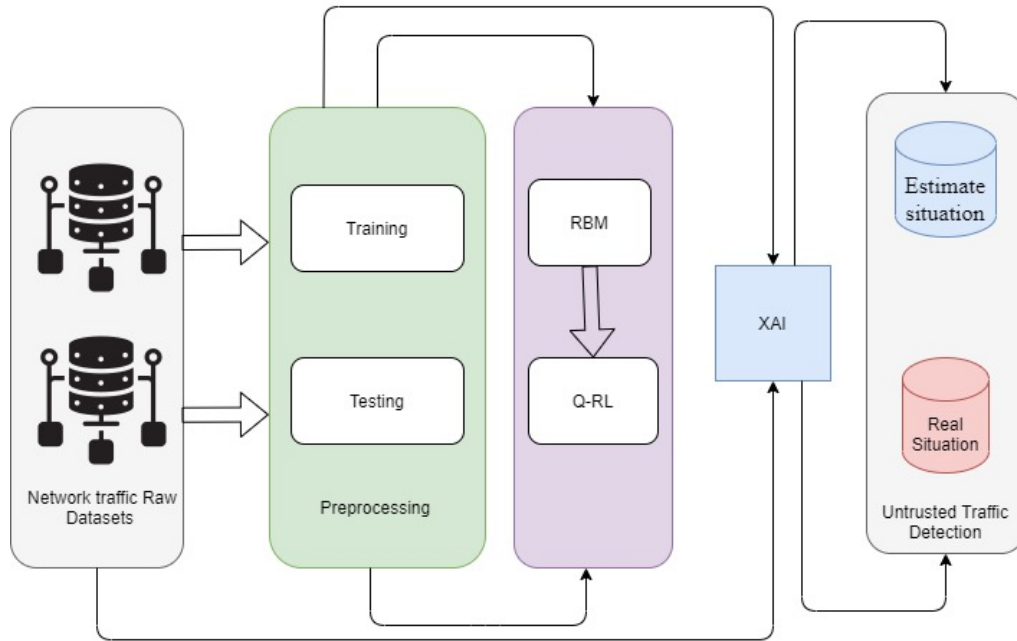


Fig. 5: Working of Proposed Model

In meticulous the probability distributions (PD) of UAV data. Data received from the “i” UAV

$$PD = \{PD_n\} \{N i = 1\}$$

The probability of density function will be $f(C)$ from

$$f\{PD_n\} \{N i = 1\}$$

If you look closely at distributed and parallel data processing, you can see how data approaches can be used in data centers. All of the entities in a decentralized ad hoc network are shown here. So, when the 5G-Enabled UAV, the goal remains the same.

$$\min_{UV} f(UV) = \sum_{X=1}^N f_X(A)$$

The arguments are X^{th} , and “UV” is an unknown variable. And the function is the local variable, and JV is the joint variable(JV). Equation 3 can be expressed as follows:

$$\min UN_1 \dots UN_N, JV = \min_{UV} f(UV) = \sum_{X=1}^N f_X(A_X) \text{ therefor } A_X = JV, X = 1 \dots N$$

Now that you know how 5G-Enabled UAV analysis works let's look at how different types of 5G-Enabled UAV data sets are used in real-world applications.

The following fields can be found in the data of most devices:

- T Information on location, grouping, or proximity
- Temperature, voltage and output, rpm, speed, torque, and other device readings
- Timestamp

In the first instance, a single device is monitored, displayed, and alerted (Rojat et al., 2021). The proprietors of a gadget are the subject of this application case.

Proposed Algorithm

1. Set all state-action pairs in the Q-table to zero.
2. Set the exploration rate (alpha), the learning rate (alpha), and the discount factor (gamma) (epsilon)
3. Define the state representation of the UAV's environment by taking into account things like location, speed, and nearby obstacles.
4. Specify the action representation that will be used by the UAV, such as moving in a variety of directions or carrying out various tasks.
5. Describe the function of the reward that gives Define the reward function that tells the agent what to do next based on how well obstacles were found and the level of security reached.
6. Follow these steps to train the Q-learning agent:
 - a. Check out the current state (or states) of the UAV's surroundings.
 - b. Choose (a) based on the epsilon-greedy policy (with a chance of random exploration)
 - c. First, carry out the act (a), then record both the subsequent state (s') and the payoff (r) that you get.
 - d. Using the Bellman equation, bring the Q-value of the (s, a) pair up to date as follows:
 $Q(s, a) = Q(s, a) + \alpha * [r + \gamma * \max(Q(s', a')) - Q(s, a)]$
 - e. Transfer information from the current state to the next state's.
 - f. Iterate through steps b to e until convergence is reached or until a predetermined number of times has passed.
7. Implementing Trustworthy Security Solutions with XAI for Unmanned Aerial Vehicles That Have 5G Connectivity:
 - a. Develop a model for obstacle detection and avoidance using XAI techniques
 - b. Make sure the XAI model can justify its choices in a way that humans can understand.
 - c. Integrate the XAI model with the Q-learning agent to enhance decision-making in security-critical scenarios
 - d. Keep the XAI model up-to-date with fresh data and user feedback to ensure its continued credibility.
8. Test the trained Q-learning agent with the integrated XAI model:
 - a. Deploy the UAV in a simulated environment or controlled real-world setting
 - b. Evaluate the performance of the agent in detecting obstacles and maintaining security levels
 - c. Information about the agent's reasoning and the justifications given by XAI models should be gathered.
9. Continue the process of investigation and enhancement:
 - a. Examine the rationales provided by the XAI model to learn more about the UAV's actions and choices.
 - b. Determine if there are any holes in the security measures or ways they can be improved.
 - c. Q-learning and XAI can be made more trustworthy and effective through iterative model refinement.

3.5. Results Analysis

The experiment is conducted using Python, Scala, and the XAI technology based on H2O. Learning libraries will be utilised to aid in the development and experimentation of the venture. This strategy will utilise IBM Watson Studio, Anaconda Python, and the Scala and Python libraries. On NVIDIA GPUs, probabilistic demonstrating and deep learning strategies for UAV Datasets will be practised. The dashboard will continuously display data as graphs, lines, and tables, and Apache Zeppelin will retrieve the data from the database. Using the framework architecture proposed, UAV screen data can be continuously analysed.

After the experimental evaluation of new and established methodologies yielded fruitful results, numerous findings for a broad range of parameters were reported. Earlier sections of the performance evaluation examined the impact of operation and XAI state variables. The method achieved all UAV dataset detail output metric targets, and the proposed structure was positive. However, the suggested

solution was approximately 91 percent accurate. The proposed method, after a predetermined amount of time, determines the faith of the remaining nodes. To this end, we proposed a D-ESN-based XAI model for real-time optimization of multiple cellularly-connected UAV trajectories with minimal latency and interference. We do not extract these features from the RBM in order to keep things simple; instead, we use an input vector that specifies the positions and routes of nearby ground BSs and other UAVs. In the presence of connectivity constraints, cellular-connected UAVs with Reinforcement Learning (RL)-based path planning achieved more reliable wireless connectivity and lower latency. Figure 6 depicts an evaluation of the proposed algorithm's performance for a range of UAV counts.

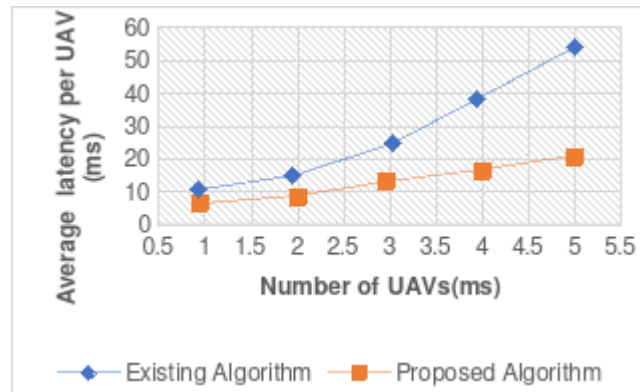


Fig. 6: Varying Numbers of UAVs, Performance Evaluation of The Proposed Model

We evaluate the performance of the proposed Reinforcement Learning (RL) -based path planning method for a variety of UAV densities in terms of the average rate per ground user equipment (UE). We compare this method to the shortest path technique, which is the standard method for path planning.

Table 2 presents a comparison of the outcomes produced by a number of different algorithms. In order to generate a comprehensive non-UAV dataset, we combined two primary data sources. This dataset includes both live and non-live video traffic from popular services such as Google Hangouts, Zoom, Skype, and YouTube. Second, the information is compiled with the assistance of a mobile application that provides the user with the ability to create their own one-of-a-kind motion sequences. Next, we gathered encrypted Wi-Fi data from a campus Wi-Fi network, which typically supports a wide variety of traffic types including video streaming, social networking apps, VoIP, email, and web browsing.

The data that we gathered came from a campus Wi-Fi network. Our approach ought to be able to differentiate between UAV traffic and other types of traffic on the campus in the event.

Table 2: Performance Comparison of Different Algorithm

Model	Execution time(m/s)	Accuracy
Proposed Model (XAI)	341	94.31%
Q-RL	561	90.32%
RL	682	90.39%
RBM	820	87.12%
BPNN	1,320	86.64%
FFNN	1,420	85.65%

That a UAV identification system is installed there. In order to record network traffic, Wireshark must first be started in the promiscuous mode. Before the controller can release the command, Wireshark has to be stopped, and the collected traffic has to be saved and labelled in accordance with the command. This process is repeated until sufficient data traffic has been collected for each mode of operation. Various modes of operation are described below.

On the other hand, the proposed solution keeps the XAI for the entire network, which makes it challenging. Introduces situations for probabilistic authentication systems in which all techniques may decide which node is trusted and identify the correct node.

Some of the approaches discussed in this survey were developed for A Trustable Security Solutions using XAI for 5G-Enabled UAVs. XAI techniques for RBM and Reinforcement Learning (RL) were developed for attacking data classification. 5G-Enabled UAV data must have unique (Vargas-Muñoz et al., 2018) characteristics that can be leveraged to develop explainable methodologies particular to RBM that are uniquely tailored to the attacking data classification field.

During classification (Chiba et al., 2016), most of the methods discussed in this survey indicate which the model gives specific parts of the input data special attention. They don't give the model any credibility and address its flaws (Zempoaltecatl-Piedras et al., 2013). It could, however, be one method to provide some explanations and boost system trust. Indeed, if a user or developer knows that the model focuses on the essential bits of the input for a certain prediction, they can have more faith in the system. As this research work illustrates, several explainable procedures can be used to Reinforcement Learning (RL) in a model by providing insights (Shaikh & Sita, 2020). The goal of XAI is to gather attacking network traffic information and gain a better knowledge of the model to establish confidence.

Nevertheless, the potential of the XAI field extends much further than simply the ability to promote credibility (Chu et al., 2019). It is essential to make use of these techniques because of the light they can potentially shed. Even the most difficult and abstract models have the potential to gain something from the implementation of new training practices and metrics that are motivated by the idea of explainability. There is still a significant distance between where we are now and a fully operational XAI system, despite the fact that we have made some headway in this direction. The XAI method does not take into account interactions with the user or the developer, which are essential in order for the AI system to be trusted

and utilized. At this time, the robustness of AI systems cannot be demonstrated through the use of objective methods (Guo et al., 2021). It may be helpful to use interactive systems that provide explanations and feedback in order to demonstrate to the user and the person making the decision that the AI system can be trusted both objectively and subjectively.

4. Conclusion

When 5G technology is used with UAVs, there are a lot of security and privacy issues. This makes the system vulnerable to a wide range of threats. It is now more important than ever to protect the 5G-enabled UAV ecosystem's foundations from these risks. As a solution to these problems, many encryption protocols have been made, such as those for "user authentication/device authentication," "access control/user access control," and "intrusion detection." To explain further, the study suggests combining integrity verification with a new model for detecting and avoiding obstacles that is based on XAI. By using Trustable Security Solutions and XAI (Explainable Artificial Intelligence) for 5G-Enabled UAVs, the research aims to make the system more resistant to possible threats. It's important to note, though, that the proposed method might not be able to handle the different integrity verification and data security constraints that come with running UAVs in real time. So, it is suggested that research be done on multi-level integrity verification and data security measures, which are meant to protect dynamic UAVs from different kinds of attacks. With more research and development, this model could be made to be able to classify the different kinds of obstacles that can be found in dynamic settings.

Researchers can make 5G-enabled UAVs safer and more private by constantly improving and fine-tuning them. This makes them safer, more efficient, and more resistant to new threats.

References

- Bithas, P. S., Michailidis, E. T., Nomikos, N., Vouyioukas, D., & Kanatas, A. G. (November 26, 2019). A survey on machine-learning techniques for UAV-based communications. *Sensors*, 19(23), 5170. <https://doi.org/10.3390/s19235170>.
- Carrio, A., Sampedro, C., Rodriguez-Ramos, A., & Campoy, P. (2017). A review of deep learning methods and applications for unmanned aerial vehicles. *Journal of Sensors*, 2017, article ID 3296874. <https://doi.org/10.1155/2017/3296874>.
- Chiba, Z., Abghour, N., Moussaid, K., omri, A. E., & Rida, M. (2016). A cooperative and hybrid network intrusion detection framework in cloud computing based on snort and optimized back propagation neural network. *Procedia Computer Science*, 83, 1200–1206. <https://doi.org/10.1016/j.procs.2016.04.249>. Accessed September 4, 2021.
- Chu, J., Wang, H., Meng, H., Jin, P., & Li, T. (2019). Restricted Boltzmann machines with Gaussian visible units guided by pairwise constraints. *IEEE Transactions on Cybernetics*, 49(12, December), 4321–4334. <https://doi.org/10.1109/TCYB.2018.2863601>. Accessed September 4, 2021.
- Dazeley, R., Vamplew, P., Foale, C., Young, C., Aryal, S., & Cruz, F. (2021), "Levels of explainable artificial intelligence for human-aligned conversational explanations," *Artificial Intelligence*, 299(October), 103525. <https://doi.org/10.1016/j.artint.2021.103525>
- De Dutta, S., & Prasad, R. (March 22, 2019), "Security for smart grid in 5G and beyond networks," *Wireless Personal Communications*, 106(1), 261–273. <https://doi.org/10.1007/s11277-019-06274-5>
- Decelle, A., & Furtlehner, C. (April 1, 2021). Restricted Boltzmann machine: Recent advances and mean-field theory. *Chinese Physics. Part B*, 30(4), 040202. <https://doi.org/10.1088/1674-1056/abd160>. Accessed September 4, 2021.
- Fu, F., Jiao, Q., Yu, F. R., Zhang, Z., & Du, J. (2021). Securing UAV-to-vehicle communications: A curiosity-driven deep Q-learning network (C-DQN) approach *IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021 (pp. 1–6). <https://doi.org/10.1109/ICCWorkshops50388.2021.9473714>.
- Garg, S., Aujla, G. S., Erbad, A., Rodrigues, J. J. P. C., Chen, M., & Wang, X. (January/February 2021). Guest editorial: Blockchain envisioned drones: Realizing 5G-enabled flying automation. In *IEEE Network*, 35(1), 16–19. <https://doi.org/10.1109/MNET.2021.9355047>.
- Guo, T., Jiang, N., Li, B., Zhu, X., Wang, Y., & Du, W. (2021). UAV navigation in high dynamic environments: A deep reinforcement learning approach. *Chinese Journal of Aeronautics*, 34(2), 479–489. <https://doi.org/10.1016/j.cja.2020.05.011>. Accessed August 10, 2020.
- Guo, W. (2020), "Explainable artificial intelligence for 6G: Improving trust between human and machine," *IEEE Communications Magazine*, 58(6, June), 39–45. <https://doi.org/10.1109/MCOM.001.2000050>. Accessed September 23, 2020.
- Gupta, R., Kumari, A., & Tanwar, S. (2021). Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. *Transactions on Emerging Telecommunications Technologies*, 32(1). <https://doi.org/10.1002/ett.4176>. Accessed September 3, 2021.
- Hodge, V. J., Hawkins, R., & Alexander, R. (2021), "Deep reinforcement learning for drone navigation using sensor data," *Neural Computing and Applications*, 33(6), 2015–2033. <https://doi.org/10.1007/s00521-020-05097-x>.

Keneni, B. M., Kaur, D., Al Bataineh, A., Devabhaktuni, V. K., Javaid, A. Y., Zaiantz, J. D., & Marinier, R. P. (2019). Evolving rule-based explainable artificial intelligence for unmanned aerial vehicles. In *IEEE Access*, 7, 17001–17016. <https://doi.org/10.1109/ACCESS.2019.2893141>.

Kim, H., Ben-Othman, J., Mokdad, L., Son, J., & Li, C. (November/December 2020). Research challenges and security threats to AI-driven 5G virtual emotion applications using autonomous vehicles, drones, and smart devices. In *IEEE Network*, 34(6), 288–294. <https://doi.org/10.1109/MNET.011.2000245>.

Koumaras, H., Makropoulos, G., Batistatos, M., Kolometsos, S., Gogos, A., Xilouris, G., Sarlas, A., & Kourtis, M.-A. (2021). 5G-enabled UAVs with command and control software component at the edge for supporting energy efficient opportunistic networks. *Energies*, 14(5), 1480. <https://doi.org/10.3390/en14051480>.

Mahbooba, B., Timilsina, M., Sahal, R., & Serrano, M. (2021). Explainable artificial intelligence (XAI) to enhance trust management in intrusion detection systems using decision tree model. *Complexity*, 2021, article ID 6634811. <https://doi.org/10.1155/2021/6634811>.

Ning, Z., Dong, P., Wen, M., Wang, X., Guo, L., Kwok, R. Y. K., & Poor, H. V. 5G-enabled UAV-to-community offloading: Joint trajectory design and task scheduling. In *IEEE Journal on Selected Areas in Communications*, 39(11), 3306–3320. <https://doi.org/10.1109/JSAC.2021.3088663>.

Parak, R., & Matousek, R. (June 21, 2021). Comparison of multiple reinforcement learning and deep reinforcement learning methods for the task aimed at achieving the goal. *Mendel*, 27(1), 1–8, 10.13164. Accessed July 3, 2021. <https://doi.org/10.13164/mendel.2021.1.001>.

Rojat, T., Puget, R., Filliat, D., Ser, J., Gelin, R., & D'iaz-Rodríguez, N. Explainable artificial intelligence (XAI) on TimeSeries data: A survey. *Arxiv [Abs.]/2104.00950* (2021): n. pag.

Shaikh, Mrs. M. A., & Dr Sita, D. D. (2020). Anomaly based intrusion detection system using deep learning methods. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3699870>. Accessed October 22, 2020.

Su, Y., Zhou, J., & Guo, Z. (2020). "A trust-based security scheme for 5G UAV communication systems." *IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCOM/CyberSciTech), 2020* (pp. 371–374). <https://doi.org/10.1109/DASC-PiCom-CBDCOM-CyberSciTech49142.2020.00072>.

Unlu, E., Zenou, E., Riviere, N., & Dupouy, P. (2019), "Deep learning-based strategies for the detection and tracking of drones using several cameras," *IPSN Transactions on Computer Vision and Applications*, 11(1), 7. <https://doi.org/10.1186/s41074-019-0059-x>

Vargas-Muñoz, M. J., Martínez-Peláez, R., Velarde-Alvarado, P., Moreno-García, E., Torres-Roman, D. L., & Ceballos-Mejía, J. J. (2018). Classification of network anomalies in flow level network traffic using Bayesian networks *International Conference on Electronics, Communications and Computers (CONIELECOMP), 2018* (pp. 238–243). <https://doi.org/10.1109/CONIELECOMP.2018.8327205>.

Viana, J., Cercas, F., Correia, A., Dinis, R., & Sebastião, P. (2021). MIMO relaying UAVs operating in public safety scenarios. *Drones*, 5(2), 32. <https://doi.org/10.3390/drones5020032>.

Vlahogianni, E. I., Del Ser, J., Kepaptsoglou, K., & Laña, I. (2021). Model free identification of traffic conditions using unmanned aerial vehicles and deep learning. *Journal of Big Data Analytics in Transportation*, 3(1), 1–13. <https://doi.org/10.1007/s42421-021-00038-z>.

Wang, J., Liu, Y., Niu, S., & Song, H. Extensive throughput enhancement for 5G enabled UAV swarm networking. In *IEEE Journal on Miniaturization for Air and Space Systems*, 2(4), 199–208.

<https://doi.org/10.1109/JMASS.2021.3067861>.

Wu, H., Hou, R., & Sun, B. Location information assisted mmWave hybrid beamforming scheme for 5G-enabled UAVs ICC 2020–2020 IEEE international conference on communications (ICC). (2020), pp. 1–6. <https://doi.org/10.1109/ICC40277.2020.9149027>.

Xiao, K., Zhao, J., He, Y., Li, C., & Cheng, W. (2019). Abnormal behavior detection scheme of UAV using recurrent neural networks. In *IEEE Access*, 7, 110293–110305. <https://doi.org/10.1109/ACCESS.2019.2934188>.

Zempoaltecatl-Piedras, R., Velarde-Alvarado, P., & Torres-Roman, D. (2013). Entropy and flow-based approach for anomalous traffic filtering. *Procedia Technology*, 7, 360–369. <https://doi.org/10.1016/j.protcy.2013.04.045>. Accessed September 4, 2021.

Zhang, Y., Mou, Z., Gao, F., Jiang, J., Ding, R., & Han, Z. (October 2020), "UAV-enabled secure communications by multi-agent deep reinforcement learning," *IEEE Transactions on Vehicular Technology*, 69(10), 11599–11611. <https://doi.org/10.1109/TVT.2020.3014788>