ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2021.0364

INVESTIGATION OF DEEP LEARNING OPTIMIZERS FOR FALSE WINDOW SIZE INJECTION ATTACK DETECTION IN UNMANNED AERIAL VEHICLE NETWORK ARCHITECTURE

N. Vanitha and G. Padmavathi
Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, India

Abstract

The Unmanned Aerial Vehicle (UAV) network plays a prominent role in this pandemic era. Nowadays UAVs are applied in various applications like military, civil etc. This article works on the Search and Rescue application part. UAV networks are applied in search and rescue operations in order to find the missing people in Hill areas. Due to false data dissemination attacks some UAVs in the network will lost the data so the rescue will become an issue. In order to detect those attacks this work uses Feed Forward Neural network with backpropagation algorithm. This work experiments chosen optimizers to get the accurate detection of attack and compares the results among the optimizers All the more explicitly this examination did in the Delay-Tolerant based Decentralized Multi-Layer UAV ad-hoc organization Assisting VANET (DDMUAV) design utilizing Opportunistic Network Environment (ONE) test system.

Keywords:

Unmanned Aerial Vehicle, Delay Tolerant, Neural Network, Optimizer, Simulation

1. INTRODUCTION

The DDMUAV architecture provides store - carry and forward mechanism which in turn reduces packet drops in search and rescue applications. The Fig.1 provides the DDMUAV architecture with U2U, U2V, V2U and U2G links for communications [3]. There are three groups of nodes in this architecture, they are ground station, backbone DTN UAVs, next layer DTN UAVs. There will be fully enabled VANET is always available with the architecture. Binary Spray and Wait with controlled replication protocol are used for routing packets, and for mobility this work employs random waypoint mobility model with high-speed interface [7] [13] [16].

Authors done a security analysis of cyber-attack classification for UAV networks and identified that False data Dissemination attack is most vulnerable in the article [18], and in this paper works on one of the False data Dissemination attack that is Low false Window Size injection attack.

1.1 FALSE WINDOW SIZE INJECTION ATTACK

False Window size injection attack is a sub class of False data Dissemination attack this will depicted in the Fig.2, where this work concentrates on Low False Window size injection attack [4] - [6].

1.1.1 High False Window Size Injection Attack:

The high false window size injection attack, the window size has been falsified by the attacker more than the connection can actually offer. So that, the link will be allocated with the added traffic information. It will cause overcrowding with highest delay and drops the packets [8].

1.1.2 Low False Window Size Injection Attack:

The low false window size injection attack, the window size has been falsified by the attacker less than the connection can actually offer, the link with low bandwidth data will produces underutilization and the throughput of the DDMUAV network will lessening [8].

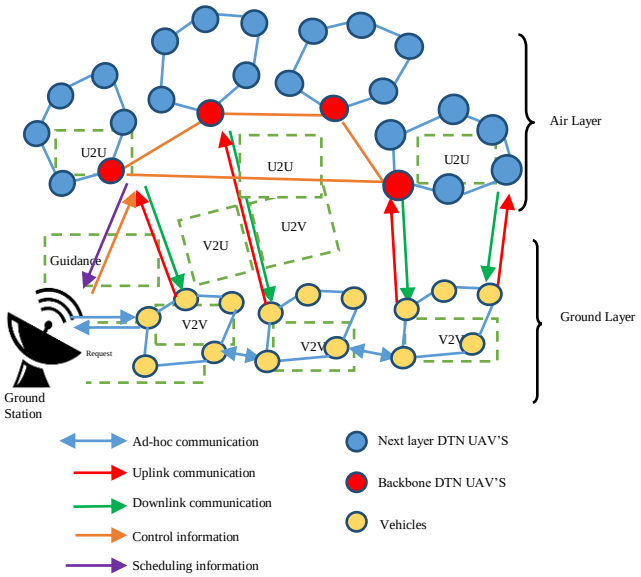

Fig.1. DDMUAV Architecture

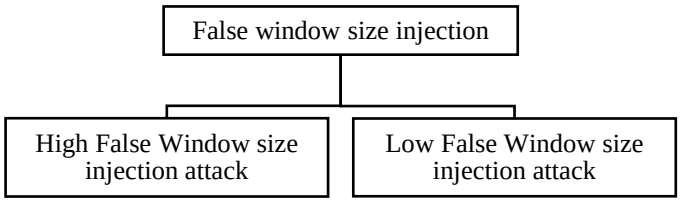

Fig.2. Classification of False Window size injection attack

1.2 OBJECTIVE OF THE WORK

The primary objective of this article is to find the best optimizer on DFFNN with Backpropagation to detect false window size injection attack on DDMUAV network architecture to get best detection rate.

2. BACKGROUND STUDY

Brandon et al. [10], through simulation analysed the behaviour of post-attack in the autopilot system and they have analysed the cyber-attack exposures in Unmanned Aerial Vehicles.

Sedjelmaci et al. [2] based on Belief approach a threat estimation model is projected by the authors, and promptly detecting these attacks, cyber detection mechanism was introduced, since categorizing a genuine vehicle as an attacker and attacker as a genuine vehicle might compromises the efficacy of the safety system while diminishing false negatives and positive rates is a main problem.

Sedjelmaci et al. [3] proposed attack identification and responding methods for UAV networks, applied mutual monitoring techniques to classify the attacks.

Abbaspour et al. [1], in sensors of an UAV networks, authors detected the injected faults and used adaptive neural network. In order to update the weight, the authors used an embedded Kalman filter (EKF). Results good detection rate.

Wu et al. [17] in order to detect the attacks authors used the methods in Deep Learning and compared the results with the currently available methods and finally discusses a performance improvement method of the attack detection in deep learning methods.

Weiy et al. [14] demonstrated the impact of wrong data injection attacks and using NS-2 simulator tool, simulated wrong data injection attacks in UAV networks. The Table.1 provides the background study of the work.

Vanitha et al. [18] shown a security analysis of cyber-attack classification for UAV networks and identified that False data Dissemination attack is most vulnerable. Vanitha et al. [19] applied the EDFFNN method to detect the wrong bandwidth injection attack in Centralised UAV communication network architecture.

Table.1. Background Study

Techniques used	Outcomes
Examined the Cyber Attack Weaknesses for UAVs [10]	Through simulation, analyze the post-attack behaviors.
SVM based technique against Cyber – Attacks [2]	Identification pace of 93 % and false positives rates become low.
A Bayesian Game-Theoretic Methodology for IDE frame work [3]	Results in Low false positive rates and communication overhead with High detection rate of attacks.
Simulated wrong data injection attacks in UAV networks using Network Simulator tool [14]	Wrong bandwidth injection attack on performance of the UAV network has been proved.
Deep neural network model for network IDS has been built [5]	From KDD-NSL dataset, authors chosen 6 features form 41 features. Conducted experiment in SDN environment, flow-based anomaly discovery.
embedded Kalman filter (EKF) is used to update the weight [1]	Detection rate is good

This article presents various wrong data injection attacks on DMUAV network architecture specifically Low window size injection attack, then the networks traffic is monitored and analysed using the Deep Feed Forward Neural Network with backpropagation procedure with various optimizers. The best optimizer is identified and compared the results with other optimizers [15].

3. MATERIALS AND METHODS

This work utilizes the Deep feed forward neural organization with a backpropagation strategy for preparing and furthermore distinguishing the False window Size injection attack [9][17].

3.1 THREAT MODEL

UAVs are considered for rich applications like search and rescue. False data injection, message corruption like cyber-attacks can root solemn consequences and disturb the projects upheld by DDMUAVs in the operations of search and rescue. In this article, the writers have made a dangerous model that injects the low false window size in the packet of TCP header window size [19]. The nodes with buffer size less than 100 packets are termed as low window size injected node in this simulated network.

3.2 PREPARING DFFNN WITH BPNN PROCESS

Step 1: Set the number of layers, inputs, Hidden neurons and the yield in the architecture

Step 2: Choose a learning rate η and set small random values to all weights and biases, naturally $\in$ [-1, 1].

Step 3: Perform training repeat until expiry criteria fulfilled and throughout the network increase it (Forward movement) and the actual output has been calculated.

- **a.** Take Inputs, multiplied by weights, summated
- **b.** Sigmoid activation function used for compress.
- **c.** Individual neuron in subsequent layer, output is passed, after the output layer adjust weights and waged back (backward movement) using chosen optimizer.

The Eq.(1)-Eq.(5) shows the formula for calculating activation, output, derivative, error and updating weight,

$$activation\_function = sum(weight * input_i) + bias \quad (1)$$

$$output = 1/(1+e^{-activation\_function}) \quad (2)$$

$$transfer\_derivative = output * (1-output) \quad (3)$$

$$error = (expected - output) * transfer\_derivative(output) \quad (4)$$

General weight updation formula is shown in Eq.(5),

$$update\_weight = weight + learning\ rate * error * input \quad (5)$$

This work makes use of adaptive optimizers to update weights. The following section provides the detail explanation of optimizers. The Fig.3 shows the work flow of the training of the proposed algorithm. Pictorial representation of the algorithm is available in Fig.3.

3.3 OPTIMIZER

In deep learning model, reduce the cost function optimizer algorithms were used. By assessing the gradient of nodes, the process typically accomplished and minimizes it iteratively. The various optimization algorithms in the deep learning arena, Adam is the most popular in Deep Learning methods. Still, there are

plenty of optimizers to choose. This article chooses Adam, Adagrad and RMSprop to compare detection accuracy that receive from each optimizer. The Fig.4 shows the optimizers chosen for weight updation [2].

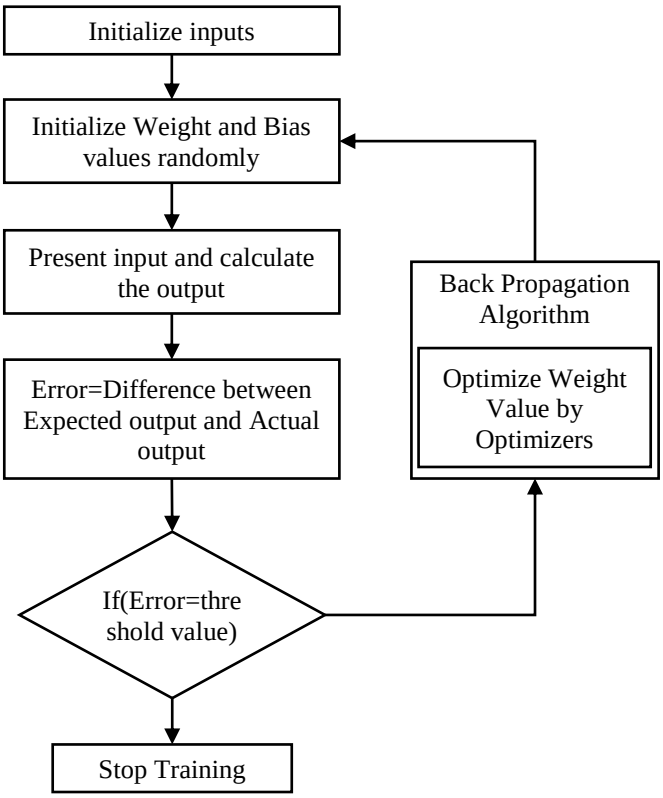

Fig.3. DFFNN with Backpropagation with Optimizers

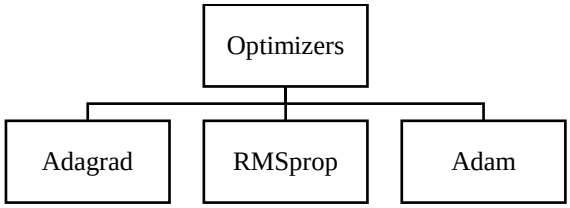

Fig.4. Optimizers for Deep Learning

3.3.1 Adagrad:

Adagrad is termed as adaptive gradient. This optimizer changes the learning rate η for each update. Each and every weight has its individual cache value, till the present point, that gathers the squares of the gradients. Cache is calculated using below Eq.(6):

$$cache_{new} = cache_{old} + \left(\frac{\partial (Loss)}{\partial (W_{old})} \right)^2 \quad (6)$$

As the training growths, the cache will remain to rise in rate. The weight update method is as tracks:

$$W_{new} = W_{old} + \frac{\eta}{\sqrt{cache_{new}} + \varepsilon} * \frac{\partial (Loss)}{\partial (W_{old})} \quad (7)$$

The learning rate (η) continuously changes throughout the training. In order to avoid division by zero, ε is used. The learning rate of each weight will ultimately be lessening to a very small rate till training does not occur pointedly is the problem.

3.3.2 RMSProp:

In RMSProp works on the cache updating plan. Formula for updating cache is available in Eq.(8), presents a new parameter, the decay rate (γ).

$$cache_{new} = \gamma * cache_{old} + (1-\gamma) * \left(\frac{\partial (Loss)}{\partial (W_{old})} \right)^2$$

The γ value is about 0.99 or 0.9. The square of gradients gets added at a very deliberate rate compared to adagrad, for each and every update. The weight is updated similar to adagrad, but eventually the learning rate does not falloff rapidly, so allow training to last for lengthier.

3.3.3 Adam:

Adam is a combination of RMSProp with Momentum. By using the cache, adam performs gathering the gradients by calculating momentum and changing the learning rate. Calculate momentum (m) value, at the current point. The Eq.(9) represents the adam momentum update formula,

$$m_{new} = \beta_1 * m_{old} + (1-\beta_1) * \frac{\partial (Loss)}{\partial (W_{old})} \quad (9)$$

Next, compute the gathered cache calculation in Eq.(10), it is accurately the equal as it is in RMSProp:

$$cache_{new} = \beta_2 * cache_{old} + (1-\beta_2) * \left(\frac{\partial (Loss)}{\partial (W_{old})} \right)^2 \quad (10)$$

Now the final weight update formula is in Eq.(11),

$$W_{new} = W_{old} - \frac{\eta}{\sqrt{cache_{new}} + \varepsilon} * m_{new} \quad (11)$$

For training neural networks model, Adam achieves better results than any other optimizer. In this article for Adam, the suggested constraints are$1e^{-8}$ for ε, 0.9 for β_1 and 0.99 for β_2.

3.4 EVALUATION METRICS

The proposed model has been evaluated using the confusion matrix and the results are tabulated in the table. The following are the components of confusion matrix,

- *True Positives (TP)*: Correctly classified malicious packets count.
- *True Negatives (TN)*: Correctly classified normal packets count.
- *False Positives (FP)*: Count of the regular packets erroneously classified as malicious.
- *False Negatives (FN)*: Count of the malicious packets incorrectly classified as normal.

This work measures the true positive rates and the false positive rates to estimate the classification performance. Here are the pre-owned assessment measurements: The True Positive Rate (*TPR*), False Positive Rate (*FPR*) and Detection Rate (*DR*). Eq.(12)-Eq.(14) shows the formula for calculating the metrics,

$$TNR = \frac{TP}{TN + FP} * 100 \quad (12)$$

$$DR = \frac{TP}{TP + FN} * 100 \quad (13)$$

$$FPR = \frac{FP}{TN + FP} * 100 \quad (14)$$

The classifier suggests 0 or 1, if it is 0 then the result is normal packet or it is the attack packet.

4. EXPERIMENT RESULTS AND DISCUSSIONS

To simulate the Secure and Communication Efficient Delay Tolerant based decentralized multi-layer UAV assisting VANET (DDMUAV) architecture Opportunistic Network Environment (ONE) Simulator is used. Simulation parameters are displayed in the Table.2. The results of proposed DFFNN with backpropagation algorithm using different optimizers will be compared. This work computes the FPR, TPR, DR. The Fig.6 shows the sample dataset.

The Fig.5 shows the simulated experiment of the network architecture and Fig.6 shows the traffic data from simulated experiments and of the simulated experiments [11] [12].

Table.2. Simulation Parameters

Parameter name	Value
Simulator tool used	ONE Simulator
Simulation area size	5000×5000 m^2
Simulation time	1000 secs
Mobility model used	Random waypoint mobility model
UAV number	15
Speed/Velocity	50 to 100 km/h
Link Layer configuration	802.11 b
Type of the Protocol	TCP
Routing technique	DTN routing (Binary Spray and Wait with controlled replication)
Transmission range	100 m
Packet Size	256 bytes
Buffer size	100 packets
Total packets	500 Packets

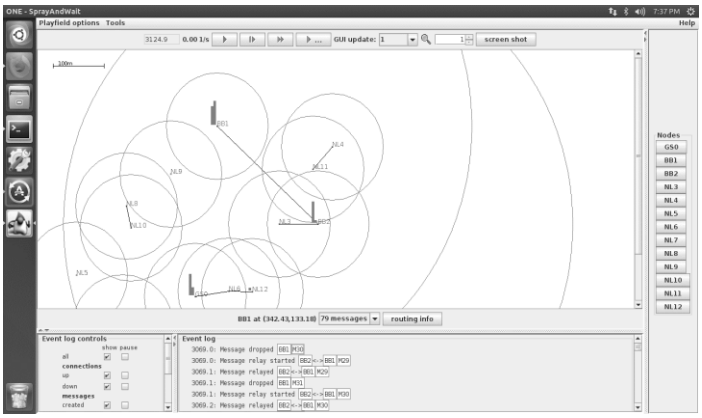

Fig.5. Traffic analysis with Low bandwidth injection attack

time	ID	size	fromHost	toHost	TTL	BufferSize	Attack
32	M1	902834	GS0	NL8	300	100	0
58	M2	629931	NL4	BB1	300	0	1
86	M3	947923	GS0	BB2	300	100	0
120	M4	418337	BB2	NL8	300	100	0
149	M5	886241	NL11	NL7	300	0	1
177	M6	348208	NL9	NL8	300	0	1
203	M7	910475	NL4	NL11	300	0	1
235	M8	452401	NL4	NL3	300	0	1
263	M9	811700	BB1	NL9	300	100	0
291	M10	980040	GS0	NL11	300	100	0
319	M11	949927	NL5	BB2	300	0	1
351	M12	918471	NL7	BB1	300	0	1
384	M13	651571	BB1	NL5	300	100	0
410	M14	426872	NL9	NL7	300	0	1
436	M15	520565	BB2	NL9	300	100	0
470	M16	562902	BB1	NL4	300	100	0
498	M17	691290	NL6	NL11	300	0	1
528	M18	584463	BB2	NL3	300	100	0
559	M19	427680	NL6	NL8	300	0	1

Fig.6. Sample Traffic Data

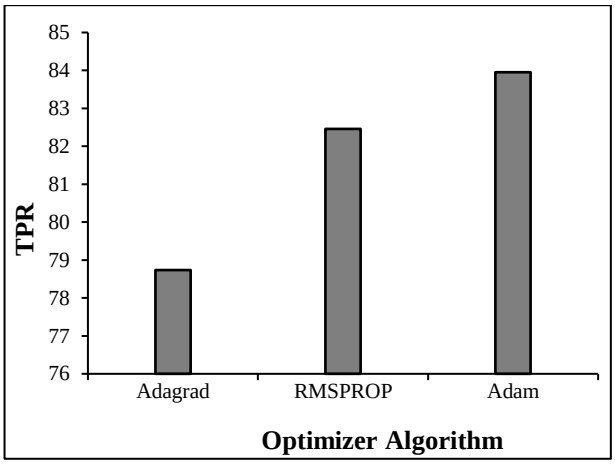

Fig.7. True Positive Rate

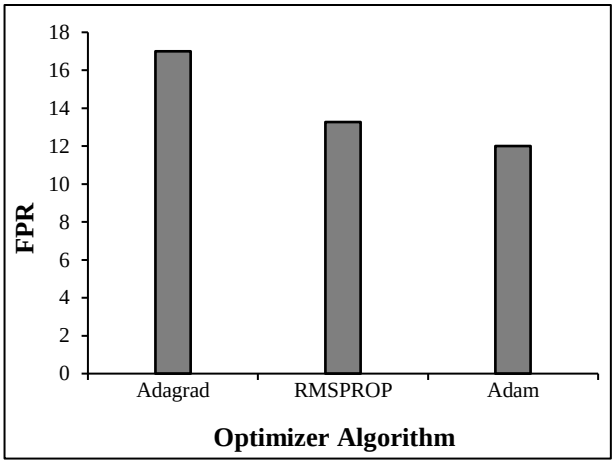

Fig.8. False Positive Rate

It is observed that the detection of attacks through DFFNN back propagation algorithm with Adam optimizer is respectable and it provides decent outcomes in detection rate, true positive rate and true negative rate. Adam optimizer provides 1.77% of improvement in true positive rate, 9% of improvement in false positive rate and 4.157% of improvement in detection rate

compared to RMSprop optimizer. The results from Table.3 shows that Adam optimizer is the best optimizer for updating weights in detecting false window size injection attack.

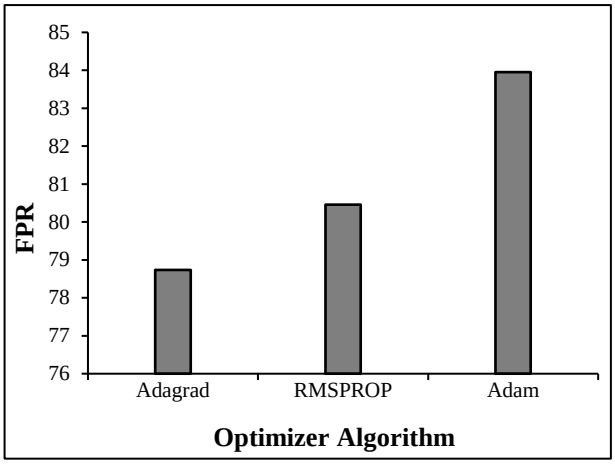

Fig.9. Detection Rate

The Fig.7-Fig.9 show that, in the case of detection rate the adam optimizer provides highest rate and adagrad provides lowest rate and the RMSprop provides moderate rate. In the case of TPR adam optimizer provides 83.95% and RMSprop and adagrad provides 82.46%, 78.74% respectively. The best optimizer which provides lowers FPR, from our experiment it is proved that adam optimizer is the best with the lowest FPR compared to other two optimizers adagrad and RMSprop.

5. CONCLUSION

Due to the cyber-attacks like false data dissemination attacks, the Unmanned Aerial Vehicle (UAV) network got into trouble in search and rescue like operations. In order to avoid those attacks, detection of the attacks at the earliest with accuracy is important. This work employs Feed Forward Neural network with backpropagation algorithm with the chosen optimizers, in order to identify the best optimizer for attack detection. This work experiments chosen optimizers to get the accurate detection of attack and compares the results among the optimizers. More specifically this investigation carried out in DDMUAV architecture using ONE simulator. The experiment result shows that among the picked streamlining agents Adagrad, RMSprop, and Adam, Adam is the best enhancer which gives a great detection rate, true positive rate, and low false-positive rates.

REFERENCES

[1] Alireza Abbaspour, Kang K. Yen, Shirin Noei and Arman Sargolzaei, "Detection of Fault Data Injection Attack on UAV Using Adaptive Neural Network", *Procedia Computer Science*, Vol. 95, pp. 193-200, 2016.

[2] A. Alsarhan, A.R. Al-Ghuwairi and I.T. Almalkawi, "Machine Learning-Driven Optimization for Intrusion Detection in Smart Vehicular Networks", *Wireless Personal Communications*, Vol. 117, pp. 3129-3152, 2021.

[3] F. Nordemann and R. Tonjes, "Transparent and Autonomous Store-Carry-Forward Communication in Delay Tolerant Networks (DTNs)", *Proceedings of International Conference on Computing, Networking and Communications*, pp. 761-765, 2012.

[4] A. Shukla, G. Kalnoor and A. Kumar, "Improved Recognition Rate of Different Material Category using Convolutional Neural Networks", *Materials Today: Proceedings*, pp. 1-7, 2021.

[5] H. Sedjelmaci, S. M. Senouci and N. Ansari, "A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. 48, No. 9, pp. 1594-1606, 2018.

[6] V. Chang, B. Gobinathan and S. Kannan, "Automatic Detection of Cyberbullying using Multi-Feature based Artificial Intelligence with Deep Decision Tree Classification", *Computers and Electrical Engineering*, Vol. 92, pp. 1-18, 2021.

[7] Ilker Bekmezci, Ozgur Koray,Sahingoz and Samil Temel, "Flying Ad-Hoc Networks (FANETs): A Survey", *Ad-Hoc Networks*, Vol. 1, pp. 1254-1270, 2013.

[8] T. Karthikeyan, K. Praghash and K.H. Reddy, "Binary Flower Pollination (BFP) Approach to Handle the Dynamic Networking Conditions to Deliver Uninterrupted Connectivity", *Wireless Personal Communications*, Vol. 117, pp. 1-20, 2021.

[9] M.J. Kang and J.W. Kang, "Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security", *PLoS ONE*, Vol. 11, No. 6, pp. 1-14, 2016.

[10] Alan Kim, B. Wampler and H. Aldridge, "Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles", *Infotech Aerospace*, pp. 1-12, 2012.

[11] Kuldeep Singh and Karandeep Singh, "A Survey and Analysis of Mobility Models in Mobile Adhoc Network", *International Journal of Advances in Electronics and Computer Science*, Vol. 2, No. 1, pp. 29-33, 2015.

[12] S. Misra, B.K. Saha nd S. Pal, "A Developer's Guide to the ONE Simulator. In: Opportunistic Mobile Networks", *Proceedings of International Conference on Computer Communications and Networks*, pp. 53-88, 2016.

[13] S. Kitada, G. Hirakawa, G. Sato, N. Uchida and Y. Shibata, "DTN Based MANET for Disaster Information Transport by Smart Devices", *Proceedings of International Conference on Network-Based Information Systems*, pp. 26-31, 2015.

[14] Sixiao Wei, Linqiang Ge, Wei Yu, Genshe Chen, Khanh Pham, Erik Blasch, Dan Shen and Chao Lu, "Simulation study of Unmanned Aerial Vehicle Communication Networks Addressing Bandwidth Disruptions", *Proceedings of International Conference on Sensors and Systems for Space Applications*, pp. 1-8, 2014.

[15] Stephen George, "FAA Unmanned Aircraft Systems (UAS) Cyber Security Initiatives", *Federal Aviation Administration*, pp. 1-19, 2015.

[16] Yi Zhou, Nan Cheng, Ning Lu, and Xuemin Shen, "Multi-UAV-Aided Networks: Aerial-Ground Cooperative Vehicular Networking Architecture", *IEEE Vehicular Technology Magazine*, Vol. 10, No. 4, pp. 36-44, 2015.

[17] Yirui Wu, Dabao Wei and Jun Feng, "Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey", *Security and Communication Networks*, Vol. 2020, pp. 1-18, 2020.

[18] N. Vanitha and G. Padmavathi, "A Study on Various Cyber-Attacks and their Classification in UAV Assisted Vehicular Ad-Hoc Networks", *Proceedings of International Conference on Computational Intelligence, Cyber Security and Computational Models*, pp. 1-13, 2018.

[19] N. Vanitha and P. Ganapathi, "Traffic Analysis of UAV Networks Using Enhanced Deep Feed Forward Neural Networks (EDFFNN)", *Proceedings of International Conference on Research on Machine and Deep Learning Applications for Cyber Security*, pp. 219-244, 2020.