Secured Monitoring of Unauthorized UAV by Surveillance Drone Using NS2

Priti Mandal[1[0000-0002-6697-8613]], Lakshi Prosad Roy [2[0000-0003-4670-5666]] and Santos Kumar Das[3[0000-0002-8788-6152]]

[1, 2, 3] National Institute of Technology, Rourkela, 769008, Odisha, India
[1]pritimandal2310@gmail.com, [2]royl@nitrkl.ac.in,
[3]dassk@nitrkl.ac.in

Abstract. Rapid increase in the Unmanned Aerial Vehicles (UAVs) or drones led to its wide application in all the sectors. This makes the situation critical and demands a proper monitoring system to keep an eye on the UAVs in the particular area. In this paper, work is taken up on monitoring/tracking of unauthorized UAV by the surveillance drone using proposed tracking algorithm in NS2 platform. In addition to this, a cryptographic algorithm is proposed to transferred the data of the tracked UAVs to the ground basestation with proper routing protocol.

Keywords: Monitoring system, Unauthorized UAV, Cryptography.

1 Introduction

Enormous application of UAVs makes it suitable for both civilian as well non-civilian sector [1]. For any emerging technology, along with its advantages disadvantages are also needed to be dealt. Easy accessibility and low cost create an alarming situation of using UAV inappropriately. So, a proper monitoring system is required towards the unauthorized UAV. In order to do so, swarm of UAVs could be used to determine the presence of unauthorized UAV in particular area.

There are several research works in which network simulator is used to analyse the performance of the Flying Ad hoc Network (FANET). FANET can be deployed in different environment for both air-to-air communication and air-ground communication [2]. While communicating proper routing protocol is to be used. In [3], different routing protocols such as Ad hoc on Demand Distance Vector (AODV) and Destination-Sequenced Distance-Vector (DSDV) are analysed using NS2 platform. For the swarm of UAVs, particular topologies are to maintained for proper communication. Different topologies are based on the mobility model of the FANET. In [4], different mobility model such as random way-point mobility model, random movements, Gauss-Markov, etc., are explained briefly.

Like other networks, while communicating or exchange of information within the aerial nodes in FANET security is to be ensured. The data should be secured from the attacks such as hacking, spoofing, etc. In order to have a proper monitoring system for unauthorised UAV in a specific area, data is to be encrypted for secured information transmission. There are different traditional cryptographic techniques [5] such as AES, DES, Blowfish, Two-fish, etc. For the high-speed processing of the UAVs, novel cryptographic technique is required with much more efficiency.

So, here in this paper, work is taken up on continuous tracking of unauthorised UAV after detection and transmitting the information to the ground base-station securely in NS2 platform.

The important advantages of the proposed method in secured monitoring of intruder UAV are summarized as follows:

- After detecting the unauthorized UAV, continuous location of it is tracked using proposed tracking algorithm and send to the ground base-station for further processing.
- Transmitted Data includes the location of the unauthorized UAV, which are securely transferred with a newly proposed cryptographic technique.

The rest of the paper is arranged as follows. Section 2 contains the description of the system model. In section 3, proposed methodology is explained to track the unauthorized UAV with proper routing protocol along with the proposed encryption and decryption algorithm for transmitting the packets securely using secret key. Section 4, contains the simulation results of the proposed technique in the NS2 platform. Finally, in section 5 concludes the work.

2 System Model

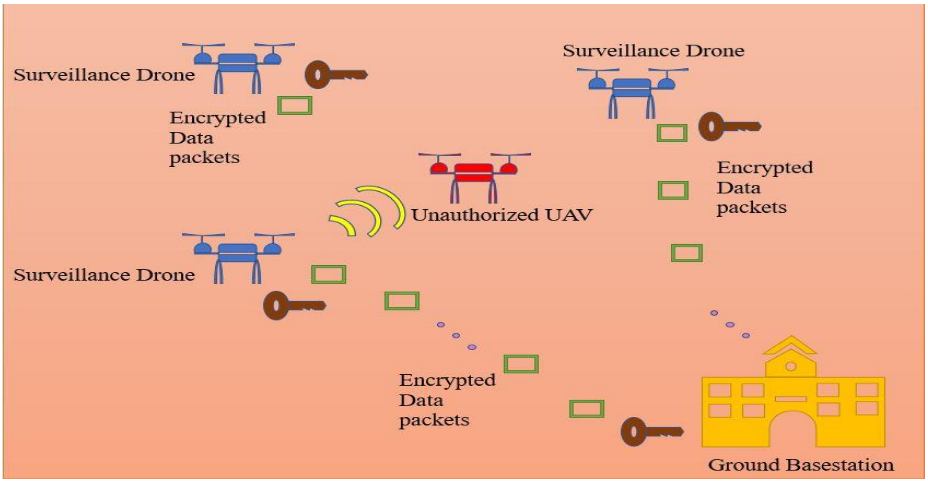


Fig. 1. Proposed System Model

Proposed system model is depicted in Fig. 1. It comprises of aerial UAV nodes and ground basestation. Proposed algorithm is used to track the unauthorized UAV and proper routing protocol is used to transfer data among the swarm of UAVs and to the ground station. After detection of unauthorized UAV, its location is continuously sent to the base-station for further processing and action. The packets are encrypted with the secret key which is explained in section 3.

3 Proposed Methodology

The proposed methodology consists the explanation of the proposed tracking method used along with the proposed encryption and decryption techniques with proper routing protocol.

3.1 Proposed tracking method

The monitoring of UAV in general is done with camera, radar, LiDAR, etc [6]. In this work, for monitoring an algorithm is proposed by considering the continuous hovering and movement of the UAV. It is assumed in Kalman filter [7] that the present state is evolved from the previous state. The present state could be represented as,

$$\boldsymbol{Y}_t = \boldsymbol{A}\boldsymbol{Y}_{t-1} + \boldsymbol{w}_t \tag{1}$$

where, $\boldsymbol{A}$ is the state transition matrix, t is the current state and $(t-1)$ is the previous state, $\boldsymbol{w}_t$ is the system noise. The observation state measured from the sensor is represented as,

$$\boldsymbol{Z}_t = \boldsymbol{G}\boldsymbol{Y}_t + \boldsymbol{u}_t \tag{2}$$

where, $\boldsymbol{G}$ is the measurement matrix and $\boldsymbol{u}_t$ is the measurement noise.
For estimation the priori state and covariance matrix can be represented as,

$$\boldsymbol{Y}_{t/t-1} = \boldsymbol{A}\boldsymbol{Y}_{t-1} + \boldsymbol{w}_t \tag{3}$$

$$\boldsymbol{C}_{t/t-1} = \boldsymbol{A}\boldsymbol{C}_{t-1} + \boldsymbol{M}\boldsymbol{Q}_{t-1}M^T \tag{4}$$

where, $\boldsymbol{M}$ is the total number of predicted value and $\boldsymbol{Q}$ is the noise covariance. The gain of the filter can be represented as,

$$\boldsymbol{K}_t = \boldsymbol{C}_{t/t-1}\boldsymbol{G}^{\boldsymbol{T}}(\boldsymbol{G}\boldsymbol{C}_{t/t-1}\boldsymbol{G}^T + \boldsymbol{R})^{(-1)} \tag{5}$$

The updated state can be represented as,

$$\boldsymbol{Y}_{t/t} = \boldsymbol{Y}'_{t/t-1} + \boldsymbol{K}_t(\boldsymbol{Z}_t - \boldsymbol{G}\boldsymbol{Y}_{t/t-1}) \tag{6}$$

where,

$$\boldsymbol{Y}'_{t/t-1} = \boldsymbol{Y}_{t/t-1} + \Delta\boldsymbol{Y}_{t/t-1} \tag{7}$$

$\Delta\boldsymbol{Y}_{t/t-1}$ determines the direction of the UAVs movement which follows the principle of Dragonfly Algorithm [8].

$$\Delta\boldsymbol{Y}_{t/t-1} = s\boldsymbol{S_i} + v\boldsymbol{V}_i + e\boldsymbol{E}_i + f\boldsymbol{F}_i \tag{8}$$

where, $\boldsymbol{S}$ represents the separation between the drones while monitoring the unauthorized drone to avoid collision among themselves, $\boldsymbol{V}$ represents the tuned velocity of the swarm of UAVs to work in alignment towards the task, $\boldsymbol{E}$ and $\boldsymbol{F}$ represents the distance which is to be maintained by the UAVs to find the unauthorized UAV. The updated covariance can be represented as,

$$\boldsymbol{C}_{t/t} = (\boldsymbol{I} - \boldsymbol{Y}_t \boldsymbol{G})\boldsymbol{C}_{t/t-1} \tag{9}$$

Algorithm 1 Proposed tracking method

```
Initialize Parameters: $\boldsymbol{Y}_0$, $\boldsymbol{C}_0$, $\boldsymbol{A}$, $\boldsymbol{H}$, $\boldsymbol{Q}$, $\boldsymbol{R}$, $\boldsymbol{M}$
Repeat each cycle $t$
    Estimate current state $\boldsymbol{Y}_{t/t-1}$ at $t$ based on previous state $t-1$
    Estimate the error covariance $\boldsymbol{C}_{t/t-1}$ based on previous covariance
    Compute the filter gain
    Correct the state using (5)
    Update the state using $\boldsymbol{Y}'_{t/t-1}$
    Update the error in covariance using (9)
    Replace the previous information with the updated information of
    the unauthorized drone
Until $t = timeout$
```

Next sub-section explains about the routing protocol used for entire process.

3.2 Routing Protocol

Based on the system model it could be observed that different kind of interaction between the nodes are to be maintained, interaction among the UAV nodes in the sky and UAV nodes to ground basestation. Ground basestation is fixed in this scenario which works as a reliable backbone of the entire system. It indicates heterogeneous routing is required to adapt. Le *et al.* [9] proposed a technique Load Carry and Deliver Routing (LCAD) which is used to enhance the connectivity between the UAV and the ground basestation. It uses Disruption Tolerant Network (DTN) in the sky while for the ground base-station Ad hoc On Demand Distance Vector (AODV).

3.3 Proposed Encryption and Decryption Algorithm

The proposed encryption algorithm is the improved and more secured version of traditional AES algorithm. In the proposed algorithm initially the data to be encrypted is considered as plain text of 128-bits. Then, the plain text is divided into four blocks and 4 × 4 state matrix. The add round key is obtained by 128-bits of state XOR with the Round Key which is a transformation of the Cipher Key. Followed by the substitution of the bytes which are arranged randomly and the order is stored in the look-up table i.e., S_{box}. The next step is to Shift Rows. As 128-bits of plain text is placed in 4 × 4 matrix then the shift operation is performed for the 4 rows. First row remains intact, second row of the matrix moved circularly towards left once, third row is circularly shifted towards left twice and the fourth row is circularly relocated towards left three times. In the Mix Column state, the 4 columns are combined in a reversible way which could be accessed back. This could be considered as the matrix multiplication. The steps are repeated for N − 1 times i.e., here N = 10 as plain text is considered to be 128 bits. This may vary according to the number of bits. In the last round i.e., Nth round Mix Column step is not considered only three steps are there as shown in the Fig. 2. After the AddRound Key in the last stage, the bits are crossover with the random crossover key and the output is further mutate after a constant number of bits. The remaining bits after the crossover of the AddRound Key output and crossover key is consider as the secret key. This secret key makes it more secured and robust. This proposed encryption technique makes it secured than the symmetric encryption method and faster than the asymmetric method.

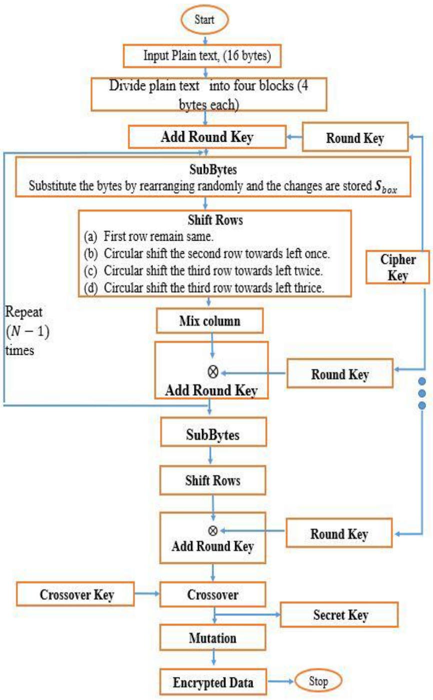

Start
Input Plain text, (16 bytes)
Divide plain text into four blocks (4 bytes each)
Add Round Key
Round Key
SubBytes
Substitute the bytes by rearranging randomly and the changes are stored S_{box}
Shift Rows
(a) First row remain same.
(b) Circular shift the second row towards left once.
(c) Circular shift the third row towards left twice.
(d) Circular shift the third row towards left thrice.
Cipher Key
Repeat
$(N-1)$
times
Mix column
⊗
Add Round Key
Round Key
SubBytes
Shift Rows
⊗
Add Round Key
Round Key
Crossover Key
Crossover
Secret Key
Mutation
Encrypted Data
Stop

Fig. 2. Proposed Encryption Technique Flowchart

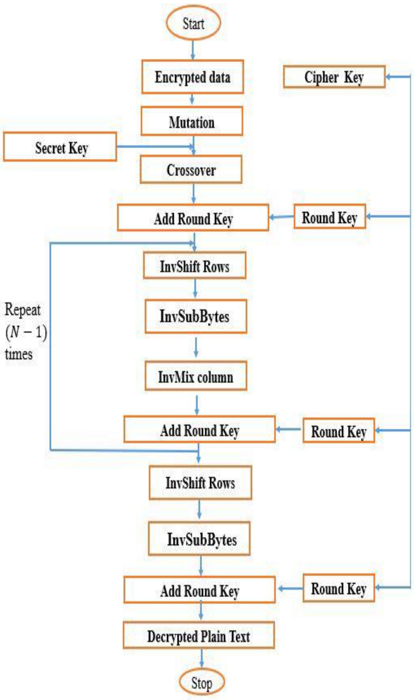


Fig. 3. Proposed Decryption Technique Flowchart

The decryption method is depicted in Fig. 3. In this the encrypted text is first de-mutate for the particular bits. Then using the secret key crossover is performed. Similar to the encryption technique four stages - Inv Shift Rows, Inv SubByte, Inv Mix Column, and AddRound Key are performed for N − 1 times using the round key as shown in the flowchart. In the last round Inv Mix Column stage is not considered. Finally, the plain text is obtained.

4 Simulation Results

In this section, proposed algorithm is analysed in the NS2 environment. For tracking the unauthorised drone protocol is used. For continuously updating the location of the drones in the basestation, information is sent in the packets securely. The parameters for the simulation are as follows: Number of nodes = 4, Wireless channel, LCAD protocol, Directional Antenna, 3J of node energy, 0.175W transmission and reception power with Random-Way point movement model.

Monitoring of nodes and data transfer in the NS2 platform can be observed in NAM file as depicted in Fig. 4. The surveillance drones are represented in green colour and unauthorized/intruder UAV is represented in red colour with ground basestation in blue. Fig. 5 depicts the intruder UAV position and speed using proposed tracking algorithm in NS2. The data of the intruder UAV is encrypted and transferred and then decrypted using the proposed algorithm depicted in Fig. 6.

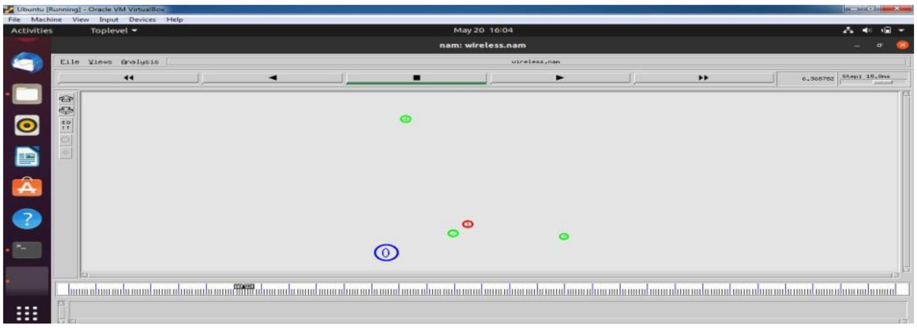
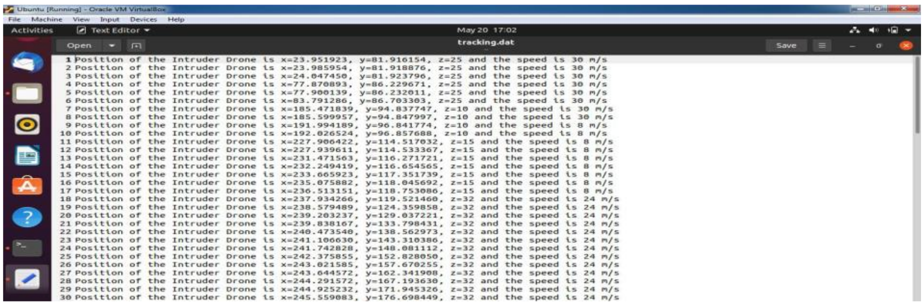


Fig. 4. Tracking of unauthorized UAV in NS2 NAM file

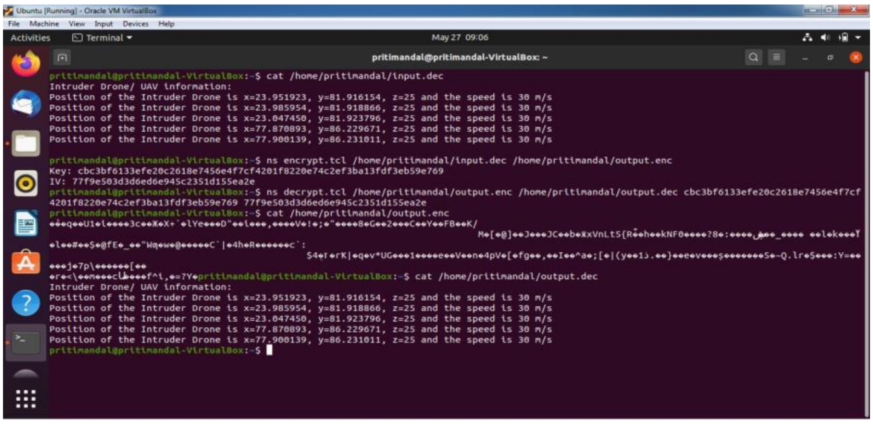

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Text Editor
May 20 17:02
tracking.dat
Open
Save

```
Position of the Intruder Drone is x=23.951923, y=81.916154, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=23.985954, y=81.918876, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=24.047450, y=81.923796, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=77.870893, y=86.229671, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=77.900139, y=86.232011, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=83.791286, y=86.703303, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=185.471839, y=94.837747, z=10 and the speed is 30 m/s
Position of the Intruder Drone is x=185.599957, y=94.847997, z=10 and the speed is 30 m/s
Position of the Intruder Drone is x=191.994189, y=96.841774, z=10 and the speed is 8 m/s
Position of the Intruder Drone is x=192.026524, y=96.857688, z=10 and the speed is 8 m/s
Position of the Intruder Drone is x=227.906422, y=114.517032, z=15 and the speed is 8 m/s
Position of the Intruder Drone is x=227.939611, y=114.533367, z=15 and the speed is 8 m/s
Position of the Intruder Drone is x=231.471563, y=116.271721, z=15 and the speed is 8 m/s
Position of the Intruder Drone is x=232.249419, y=116.654565, z=15 and the speed is 8 m/s
Position of the Intruder Drone is x=233.665923, y=117.351739, z=15 and the speed is 8 m/s
Position of the Intruder Drone is x=235.075882, y=118.045692, z=15 and the speed is 8 m/s
Position of the Intruder Drone is x=236.513151, y=118.753086, z=15 and the speed is 8 m/s
Position of the Intruder Drone is x=237.934266, y=119.521460, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=238.579489, y=124.359858, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=239.203237, y=129.037221, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=239.838167, y=133.798431, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=240.473540, y=138.562973, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=241.106630, y=143.310386, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=241.742828, y=148.081112, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=242.375855, y=152.828050, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=243.021585, y=157.670255, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=243.644572, y=162.341908, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=244.291572, y=167.193630, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=244.925232, y=171.945326, z=32 and the speed is 24 m/s
Position of the Intruder Drone is x=245.559083, y=176.698449, z=32 and the speed is 24 m/s
```

Fig. 5. Unauthorized/ Intruder UAV position and speed from Proposed tracking algorithm

Fig. 7 depicts the distance error computation while tracking unauthorized UAV. Proposed hybrid method performs with much more accuracy as compared to the existing algorithm. The packets are transferred by encrypting it using proposed algorithm. The performance of the proposed algorithm analysed using throughput.

Fig. 8 represents the throughput of the proposed encryption algorithm. Greater throughput of the proposed algorithm represents its higher performance. Fig. 9 and 10 depicts the encryption and decryption time for various packet sizes. As the proposed



Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
May 27 09:06
pritimandal@pritimandal-VirtualBox: ~

```
pritimandal@pritimandal-VirtualBox:~$ cat /home/pritimandal/input.dec
Intruder Drone/ UAV information:
Position of the Intruder Drone is x=23.951923, y=81.916154, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=23.985954, y=81.918866, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=23.047450, y=81.923796, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=77.870893, y=86.229671, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=77.900139, y=86.231011, z=25 and the speed is 30 m/s

pritimandal@pritimandal-VirtualBox:~$ ns encrypt.tcl /home/pritimandal/input.dec /home/pritimandal/output.enc
Key: cbc3bf6133efe20c2618e7456e4f7cf4201f8220e74c2ef3ba13fdf3eb59e769
IV: 77f9e503d3d6ed6e945c2351d155ea2e
pritimandal@pritimandal-VirtualBox:~$ ns decrypt.tcl /home/pritimandal/output.enc /home/pritimandal/output.dec cbc3bf6133efe20c2618e7456e4f7cf
4201f8220e74c2ef3ba13fdf3eb59e769 77f9e503d3d6ed6e945c2351d155ea2e
pritimandal@pritimandal-VirtualBox:~$ cat /home/pritimandal/output.enc
��q��U1�l���3c��X�X+`�lYe���D"��l��,����V�!�;�"����8�G��2���C��Y��FB��K/
                                                                                 M�[�@]��J���JC��b�XxVnLt5{R��h��kNF0����?8�:����,�_����  ��l�k���Y
�l��#��$�@fE�_��"Wq�w�@�����C`|�4h�R������c`:
                                                              $4�r�rK|�q�v*UG���1������V��n�4pV�[�fg��,��I��^a�;[�|(y��1.��}���v���$�������S�~Q.lr�$���:Y=��
���j�7p\������[��
�r�<\��m���cL���f^i,�=?Y�pritimandal@pritimandal-VirtualBox:~$ cat /home/pritimandal/output.dec
Intruder Drone/ UAV information:
Position of the Intruder Drone is x=23.951923, y=81.916154, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=23.985954, y=81.918866, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=23.047450, y=81.923796, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=77.870893, y=86.229671, z=25 and the speed is 30 m/s
Position of the Intruder Drone is x=77.900139, y=86.231011, z=25 and the speed is 30 m/s
pritimandal@pritimandal-VirtualBox:~$ █
```

Fig. 6. Output of proposed encryption and decryption algorithm

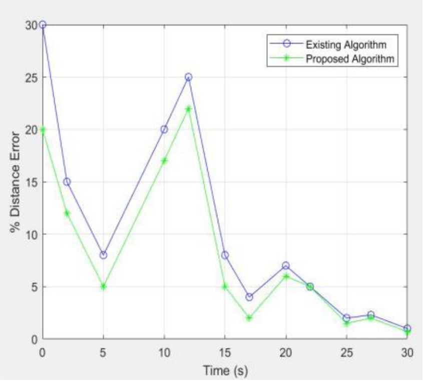


Fig. 7. Tracking Distance Error

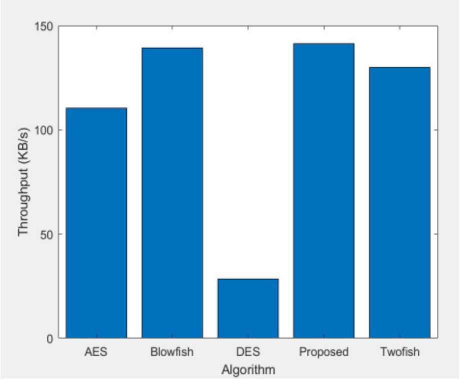


Fig. 8. Throughput Comparison

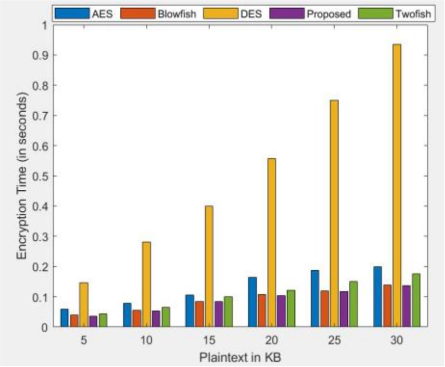


Fig. 9. Encryption Time Comparison

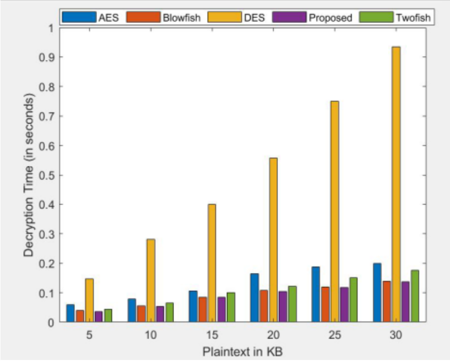


Fig. 10. Decryption Time Comparison

algorithm takes lesser time for encryption and decryption, it is more efficient than other algorithms. Proposed cryptographic algorithm outperforms as compared to the conventional methods.

5 Conclusion

In this paper, continuous monitoring of unauthorized drone using surveillance UAV is simulated in NS2 platform. The proposed monitoring algorithm performs better as compared to the existing algorithm which is analysed in terms of distance error. The information about the unauthorized/intruder drone is securely transmitted using newly proposed cryptographic algorithm which performs better in terms of throughput which makes it more efficient, secured and faster.

References

1. Mandal, P., Roy, L. P., Das, S. K.: Internet of UAV Mounted RFID for Various Applications Using LoRa Technology: A Comprehensive Survey. Internet of Things and Its Applications, pp. 369-380 (2022).
2. Azari, M., Sallouha, H., Chiumento, A., Rajendran, S., Vinogradov E., Pollin, S.: Key Technologies and System Trade-offs for Detection and Localization of Amateur Drones. In: IEEE Communications Magazine, vol. 56, no. 1, pp. 51–57 (2018).
3. Singh, K., Verma, A.K.: Experimental analysis of AODV, DSDV and OLSR routing protocol for flying adhoc networks (FANETs). IEEE International Conference on electrical, computer and communication technologies (ICECCT), pp. 1-4 (2015).
4. Mowla, M. M., Rahman, M. A., Ahmad, I.: Assessment of Mobility Models in Unmanned Aerial Vehicle Networks. 2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2), pp. 1-4 (2019).
5. Sohal, M., Sharma, S.: BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing. Journal of King Saud University-Computer and Information Science, vol. 34, 1, pp. 1417-1425 (2022).
6. Sie, N. J., Srigrarom, S., Huang, S.: Field Test Validations of Vision based Multi-camera Multi-drone Tracking and 3D Localizing with Concurrent Camera Pose Estimation. 2021 6th International Conference on Control and Robotics Engineering (ICCRE), pp. 139-144 (2021).
7. Nanda, S. K., Bhatia, V., Singh, A. K.: Performance analysis of Cubature rule based Kalman filter for target tracking. 2020 IEEE 17th India Council International Conference (INDICON), pp. 1-6 (2020).
8. Amaran, S., Madhan Mohan, R.: An Optimal Multilayer Perceptron with Dragonfly Algorithm for Intrusion Detection in Wireless Sensor Networks. 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), pp. 1-5 (2021).
9. Le, M., Park, J. S., Gerla, M.: UAV assisted disruption tolerant routing. In: Proceedings of the IEEE Conference on Military Communication (MILCOM), pp. 1–5 (2006).
10. Khan, U. S., Saqib, N. A., Khan, M. A.: Target tracking in wireless sensor networks using NS2. In: Smart Trends in Systems, Security and Sustainability, pp. 21-31, Springer, Singapore (2018).