International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Detection of Multiple Attackers and Provide Security for UAV Networks

P. Jenifa, S. Gomathi, V. Perathuselvi

Abstract: ***Remote controlled aerial vehicle networks haven't received right smart analysis attention. Specifically, security problem area unit is a serious concern as a result of such networks that carry very important data square measure at risk of numerous attacks. In our projected system to style and implemented a novel Location –Aided Delay Tolerant Routing Protocol(LADTR) with intrusion detection and response scheme, that operates at the UAV(Unmanned Aerial Vehicle)and ground station level, to find spiteful anomalies that menace the network. And conjointly UAV networks to be used in post-disaster operation, which combined with Store Carry Forward (SCF) techniques. During this theme, a group of detection and response techniques square measure projected to observe the UAV behaviors and reason them into appropriate list (normal, abnormal, suspect, malicious) in keeping with the detected cyber attack. Our simulation result make sure that the projected theme performs well in terms of attack detection even with an oversized range of UAVs and attackers since it exhibits a high detection rate , an occasional range of false positives, and prompt detection overhead and conjointly improve the packet delivery magnitude relation, network time period.***

Keywords: UAV, intrusion, cyber, detection, anomaly.

I.INTRODUCTION

A vehicle which can be used to take images and videos from the criminal areas without using human as a pilot in that vehicle but it can be controlled by remote is an Unmanned Aerial Vehicle (UAV). Here the UAV are used to capture data from the criminal areas and then send the data to the ground station controller, the controller receives the data from the UAV. When UAV transmit the data, due to wireless communication the data are corrupted from other because of some attacks are available in UAV networks. For that purpose we create security mechanism for protecting the data and also all UAVs are delivers the data to the ground station controller correctly. Security mechanism is based on two types: one is cryptography and the other is intrusion detection mechanism. Cryptography is based on the security for protecting the data for only if the user and receiver know the secret code. But intrusion detection is software application which can be used to monitoring the networks and automatically provides the alert to the system admin if someone may disrupt the network.

Revised Manuscript Received on March 30, 2020.
***** Correspondence Author
P. Jenifa, P.G. Student, Computer Science and Engineering, Francis Xavier Engineering College, Tamilnadu, India.
E-mail: jenijey96@gmail.com
Dr. S. Gomathi, Associate Professor, Computer Science and Engineering, Francis Xavier Engineering College, Tamilnadu, India.
Mrs. V. Perathuselvi, Assistant Proffesor, Computer Science and Engineering, Francis Xavier Engineering College, Tamilnadu, India.

So here when UAV transmit the data to the system admin some of the attacks are found and those attacks can be removed by using intrusion detection security mechanism. In recent years, the researchers found the attacks and provide the security for the networks and also transmit the data without disruption. Our proposed system is to deliver the data to the ground station controller within a period of time and also increase the high detection rate and very less number of false positive communications. The related work are mentioned in the bellowed section II that can explained how the UAV transform the information without any disturb in the network and also see how the author provide security to those networks.

II.BACKGROUND AND RELATED WORK

In this phase we discussed about the network architecture that we provides the secure communication for UAV networks and also discussing the detection techniques which can classified as two subsection: one is anomaly detection method whereas the other is rules based detection method are summarized in the following below section. The above figure 1 shows how the UAVs are get connected together by forming a network. Through this, some of the attacks are found so that the author is used to identify the attack and provides only the clear communication between the UAV and ground stations. Some of the possible attacks are gray hole attack, jamming attack, false dissemination attack, black hole attack and GPS Spoofing attack. Here can reduce the possible attack by seeing how they implemented. The analysis of encoding and encoding is done in the following diagram it will hide the secret key for that purpose the information is not hacked by others. So the controller can easily find all those type of information and then take action.

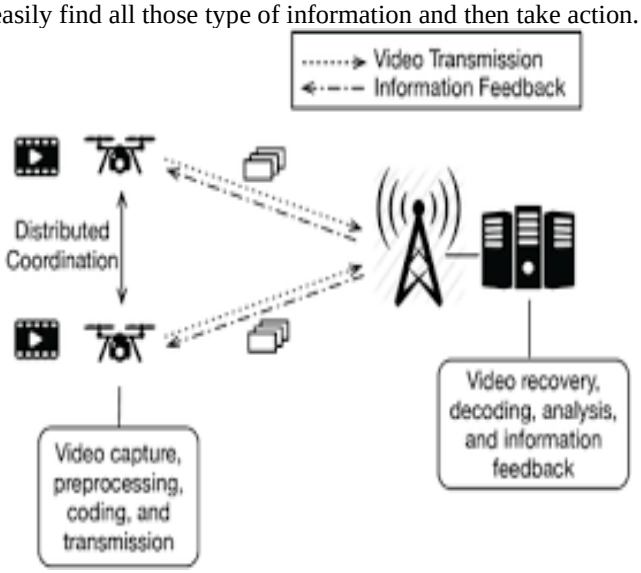

Fig.1.The UAV network architecture

A. Network architecture

This architecture is based on civilian or military application which can be used to transmit the critical information to the controller. The formation of network is either between the UAV to UAV or UAV to ground station controller. The above figure shows that the UAV collect the data in critical areas and forwards the data to another UAV by using greedy forwarding algorithm and it will transmit the data to the ground station controller through the wireless network communication. In case when UAV is neither found another UAV nor ground station controller it stores the message for a period of time. It can be measured as Ts. If the time is elapsed when UAV are not found the another UAV or ground station then the message is automatically removed from the UAV. Unmanned Aerial Vehicle(UAV) is used to control signal due to wireless communication and also used to control spoofing attack i.e., which is used to determine whether the controlled signal is comes from the ground station doesn't share secret key to handle the problem by using the framework as Generalized Log Likelihood Radio(GLLR) test.

B. Detection techniques

The detection method can be classified into two ways: one is anomaly detection and the other is rules based detection. Let see how these detection methods are performed.

i. Anomaly detection

Anomaly detection method which can be uses support vector machine learning algorithm for detecting anomalies in UAV networks. This detection method never detecting the previous attack available in the monitored node but it can detect only the new attack which can cause immediately on the monitoring node.

ii. Rules based detection

The behavior of monitored node and the known attack can be compared by the rules based detection method. This method has a basic set of rules to monitor the node if any of the attacks are available or not. So here the author provides some rules to protect the information shared by UAV to ground station.

III.PROPOSED SYSTEM

➢ Hierarchical intrusion detection

The hierarchical scheme is used to protect the cyber attack which can be possible in UAV networks are jamming attack, false information, GPS spoofing and grey and black hole attacks.

- *Jamming attack*

Jamming attack are a subset of Denial Of Service (DOS) attacks that malicious node are getting blocked communication by causing intentional between the networks. So, here the author decreasing the Signal to Noise Ratio (SINR) for the transmission of radio signal which disrupt the communication. Jamming attack consists of three types: spot, sweep and barrage. Spot jamming is occurred when jammer focuses only on all of its power in a single frequency. Sweep jamming occur when all of its power is shifted. Barrage jammer is occurred when multiple frequencies is jammed at once.

- *GPS Spoofing attack:*

GPS receiver receives the message by a fake GPS. A spoofing attack is when the message is theft by another person and that person may operate the whole system successfully. This attack may used to find out the receiver where they found and provides the global positioning of the system to identify the position where the message is comes from the destination. By using the GPS locator we used to find the location of where the information being shared. And here the dataset can be classified as the following ways; these data classification are used to find whether the condition is correct or incorrect prediction. By using this we have to identify the accurate value of each of the following section so that we can easily identify whether there is an attack founded or not. For that we have to easily neglect all the attacks which are founded in the node.

Table. 1. Data classification

True positive(TP)	Correct positive prediction
False Positive(FP)	Incorrect positive prediction
True Negative(TN)	Correct negative prediction
False Negative(FN)	Incorrect positive prediction

The above table shows that the data classification which is able to find whether the information comes from the source is to be true or else to be false it can be used for the controller to identify the attacks easily.

➢ Security for UAV Network

Cyber attacks are securing by using intrusion detection method which is used to find the spiteful node and getting alert to the controller that can be provides false positive and false negative decreasing. The process of which containing 21 UAVs are presented nearby UAVs when the single UAV collect the information, it started search for nearby UAV and sends the message to that UAV and then that UAV send to the ground station. Here the author provides 21 neighbors for easily find out the UAV for transmitting information.

- *True positive*

True positive may used to identifying the correct values from the observed sources. This can be calculated from the true positive plus the true negative is getting divided by the true positive.

- *False positive*

False positive may used to identify the positive values from the observed sources but it provides false information. This can be calculated as adding false positive and false negative is getting divided by the false positive.

The result shows how the attacks are occurred and how to detect those types of attacks and decreasing the false negative and false positive by providing these in the following results. Unmanned Aerial Vehicle (UAV) is used to control signal due to wireless communication and also used to control spoofing attack i.e., which is used to determine whether the controlled signal is comes from the ground station doesn't share secret key to handle the problem by using the framework as Generalized Log Likelihood Radio(GLLR) test. The proposed system is to improve the true negative ratio compared to the existing system. This ratio reduces the false detection ratio in number of nodes detection ratio and to produce the better performance compared to the existing method.

This proposed system is to improve the detection accuracy compared to the existing system. The network contains multiple UAV and single access point in the node creation Each and every node transferred the data to the destination node through the predicting route. If IDS detect the node behavior as malicious then automatically isolate the node into the network. Jamming attack are a subset of Denial Of Service (DOS) attacks that malicious node are getting blocked communication by causing intentional between the networks. So, here the author decreasing the Signal to Noise Ratio (SINR) for the transmission of radio signal which disrupt the communication. Jamming attack consists of three types: spot, sweep and barrage. Spot jamming is occurred when jammer focuses only on all of its power in a single frequency. Sweep jamming occur when all of its power is shifted. Barrage jammer is occurred when multiple frequencies is jammed at once. The attackers are used to find by the detection method and it can be reduced by the following true positive ratio of the above graph and it may need to contain the accurate value for that node.

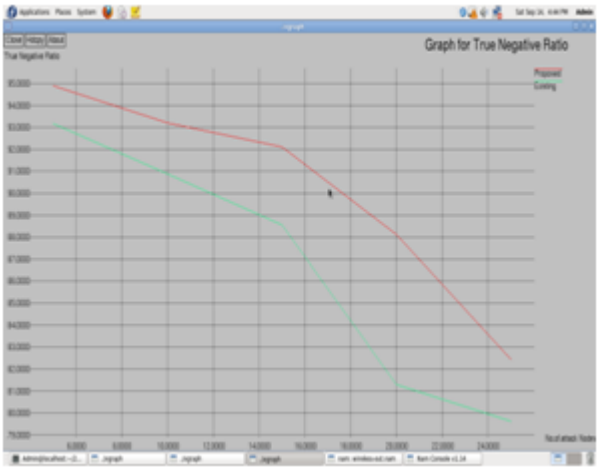

Fig. 2. True negative graph

IV.RESULT ANALYSIS

When comparing with existing part the true negative ratio will be improved in the proposed areas. The above screen shows how the UAV get connected with other UAV by network communication. By coloring each node it is easily to find what are the attacks are available in nodes.

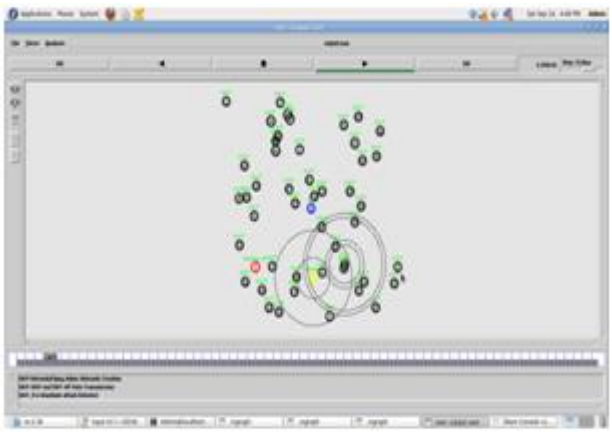

Fig. 3. Network formation

The nodes which is detected is reduces the false negative ratio. The behavior of monitored node and the known attack can be compared by the rules based detection method. This method has a basic set of rules to monitor the node if any of the attacks are available or not. So here the author provides some rules to protect the information shared by UAV to ground station. After the analysis of this figure the UAV is easily identify the other UAV for transmitting the information without any disturbing in the network. Multiple attacks are to be detected by finding the attacks in the above scenario.

V.CONCLUSION AND FUTURE WORK

UAV networks has to be protected by providing security is basically based on the attacking mechanism. The author proposing cyber attacks which is related to each set of detection rules. The accuracy may provide the correct values for identifying the attackers which is present in the UAVs. For detecting these types of attack it will provide only the true positive values. The author future work is directly based on implementing the above process into the real time and also used to comparing the exploratory values with the simulation results.

REFERENCES

1. T. Yang, C. H. Foh, F. Heliot, C. Y. Leow and P. Chatzimisios, "Self-Organization Drone-Based Unmanned Aerial Vehicles (UAV) Networks," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6.
2. T. C. Mallick, M. A. I. Bhuyan and M. S. Munna, "Design & implementation of an UAV (Drone) with flight data record," 2016 International Conference on Innovations in Science, Engineering and Technology (ICISET), Dhaka, 2016, pp. 1-6.
3. Jeongeun Kim, Seungwon Kim, Chanyoung Ju, Hyoung Il Son, "Unmanned Aerial Vehicles in Agriculture: A Review of Perspective of Platform Control and Applications", *Access IEEE*, vol. 7, pp. 105100-105115, 2019.
4. Michał Okulski, Maciej Ławryńczuk, "Development of a High-Efficiency Pitch/Roll Inertial Measurement Unit Based on a Low-Cost Accelerometer and Gyroscope Sensors", *Methods and Models in Automation and Robotics (MMAR) 2019 24th International Conference on*, pp. 657-662, 2019.
5. Alaukik Joshi, Amritanshu Tripathi, R. N. Ponnalgu, "Modelling and Design of a Hybrid Aerial Vehicle Combining VTOL Capabilities with Fixed Wing Aircraft", *Instrumentation Control and Automation (ICA) 2019 6th International Conference on*, pp. 47-51, 2019.
6. Jacob. D. Bushaw, Kevin. M. Ringleman, " Application of Unmanned Aerial Vehicle to survey mesocarnivores", https://doi.org/10.3390/drones3010028
7. Tkáč, M. & Mésároš, P. (2019). Utilizing drone technology in the civil engineering. *Selected Scientific Papers - Journal of Civil Engineering*, 14(1), pp. 27-37. Retrieved 24 Feb. 2020, from doi:10.1515/sspjce-2019-0003.
8. A. Deleforge, D. Di Carlo, M. Strauss, R. Serizel and L. Marcenaro, "Audio-Based Search and Rescue With a Drone: Highlights From the IEEE Signal Processing Cup 2019 Student Competition [SP Competitions]," in IEEE Signal Processing Magazine, vol. 36, no. 5, pp. 138-144, Sept. 2019.

AUTHORS PROFILE

P. Jenifa is presently studying M.E in the Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli . She has completed her B.E degree in the department of computer science and engineering from Jayaraj Annapackiam C.S.I College of Engineering in the year 2018. She attended the conference and publishing her paper in journal also. Her areas of interest are Networks, Intrusion detection system.

Dr. S. Gomathi, is presently working as an Associate Professor in the Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. She has completed her B.E degree from National Engineering College in the year 2003 and M.E from Anna University in the year 2005. She has also completed her Ph.D in Grid Computing, Anna University, Chennai in the year 2015. She has 13 years of experience in teaching as Assistant professor and Associate Professor in Francis Xavier Engineering college. She participated in 16 training programs in various colleges and also she published 9 International Journals and 9 international conferences. Her area of interests are Networks, Intrusion detection system and grid computing system.

Mrs. V. Perathuselvi, is presently working as an Assistant Professor in the Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. Her areas of interest are Operating systems, Software testing, Object oriented analysis and design, Ad hoc and sensor networks. She attended 2 conference and 2 seminar and four workshops. And also she published twenty four publications.