Reliable routing with Hierarchical Detection and Response System in UAV Networks

P. Jenifa[1], Dr.S.Gomathi[2]
[1]PG Student, [2]Associate Professor
Computer Science and Engineering, Francis Xavier Engineering College, Tamilnadu, India.
[E-mail: jenijey96@gmail.com]

***Abstract*- Unmanned Aerial Vehicles (UAVs) have been used in military applications for committed in air-to ground combats, surveillance, and target tracking in hostile environments.UAV network are more prone to various attacks than other networks. Networked UAVs are vulnerable to malicious attacks over open-air radio space and accordingly Intrusion Detection Systems (IDSs) have been naturally derived to deal with the vulnerabilities and/or attacks. This project focus on the lethal cyber attacks that target an UAV network. Possible attacks in UAV networks are false information dissemination, GPS spoofing, jamming, and black hole and gray hole attacks. The main objective is to identify different types of attacks in UAV Network and to achieve high detection rate and low false positives in UAV network and also to obtain an attack free environment.**

***Keywords*- UAV, detection, Intrusion, Cyber, Anomaly**

I. INRODUCTION

Unmanned Aerial Vehicle (UAV) is a flying device is used to capture the images and videos data from the disaster area and then transfer the data to the ground station.uav is a military application for committed in air to ground station, surviving, and to tracking information in hostile environment. Surveillance is the process of observing the critical information in critical areas and then tracking is the process of monitoring (suspected person or vehicles)their behaviors. Nowadays UAV are also used in civil application to explore in disaster areas and sending data from that area to the ground station controller with no network infrastructure. UAV is wireless adhoc network (WAN) that transfer the information for environmental monitoring, disaster assistance, emergency occurrence through the network from UAV to UAV, and UAV to ground station controller. UAV is very difficult to setting up of an adhoc network because this network may differ from the vehicular adhoc network and mobility adhoc network. Due to mobility node, a delay tolerant network should be based on store-carry and forward mechanism. This may need to store the information in a node and carries a message until the next node is available , hereafter founded the next node then it forwards the message to that node.

Due to wireless characteristics and relevant information handled by UAV has the major challenging is security issues. For that, security has two major mechanism such as cryptography mechanism and intrusion detection mechanism. Cryptography is a method of protecting information by the use of codes so that only the user can read the information correctly and process it and it can be use to prevent external intruder to pierce the network. And the second one is intrusion detection mechanism; it can be used to analyze the misbehavior of a monitored node. Here cryptography is used to prevent the network only from the external intruder but Intrusion Detection System (IDS) is used to prevent the network from both the internal and external intruder so IDS is more effective for preventing the network. Moreover, IDS depending

on two major detection techniques namely anomaly detection and rules based detection techniques.

Anomaly detection technique is used to find only the new attacker. It cannot be detect the information which is previously observed by the system and the computation of this technique is costly. This technique be always uses a learning algorithm such as Support Vector Machines (SVM) and neural networks to find the behavior of monitored node.
Rules based detection is a technique used to compare the behavior of monitored node in opposition to the set of rules which is related to the behavior of monitored node.

UAV network is challenging because the attackers are required on permanent basics so it is difficult for IDS node to monitor the behavior of node which can spread across demarcated. Here detection and response techniques could be run at two layers such as UAV and ground station. At early cryptography based is applied to UAV networks for ensuring message privacy and node authentication. Especially, Strohmeier et al [9] and Wesson et al [10] proposed to ensure the message privacy by the (ADS-B) automatic dependent surveillance broadcast component which is one of the component parts of the UAV system. In UAV network detecting attack is not well defined in literature. To the best of knowledge, Mitchel [12] has designed intrusion detection techniques which can be used for protecting such networks. In this paper, rules based detection methods have been used to model the normal behavior of UAV and to detect malicious anomalies by the exchange of behaviors with their neighbors. According to the simulation result the system includes the high positive rates because of high communication. Without using UAV network requirements such as mobility node and energy constraints it can directly applied the MANET which is proposed in intrusion detection techniques to the UAV networks. Therefore, in this paper, we propose a reliable routing with hierarchical detection and response scheme in UAV networks. The main aim is to detect the cyber attack that has a goal on UAV networks such as false positive, GPS spoofing, jamming, gray hole attack and black hole attack.

This paper work based on UAV military application where UAV that need to collect information and transfer the critical information to the remote ground station. Here can achieve high accuracy we have used both the anomaly detection and rules based detection method. We can develop a new response scheme with the help of these techniques that can classify into appropriate list (normal, abnormal, suspect and malicious) according to their behaviors. Intrusion detection has the following characteristics,
IDS gather information from a network system and analyze it in order to determine elements which violate security policies of computer and networks. An Intrusion Detection System (*IDS*) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

The rest of this paper can be explained by the following ways: in section II describes about network model and in section III described about the proposed system of detection and response scheme and in section IV described about the simulation results. And finally we completed with the conclusion and discussed about the future work of the project.

II. RELATED WORK

NETWORK MODEL AND SECURITY

This section can be classified into two ways: network model and the different types of attackers aim to identify, respectively.

A) Network Model

This paper is based on military application where UAV are carried to collect and transmit the critical information about the detecting events and forward it to the remote control station. The communication is either between the UAV to UAV or UAV to ground stations. In this paper, our aim is to find information in disaster areas (e.g.., tsunami, volcanic eruption, etc) that all are time sensitive application. In time sensitive application "store-carry and forward" mechanism used to decrease the loss of packets like ho -by- hop manner. This "store-carry and forward mechanism is used when data forwarding where nodes are need to be store, carry and then forward packets to the destination nodes.

Data Transfer Node (DTN) have been proposed to improve the delay of networks in communication [14] [15]. In this paper we proposed to use the ground station as a relay node when the next hop UAV is not available.

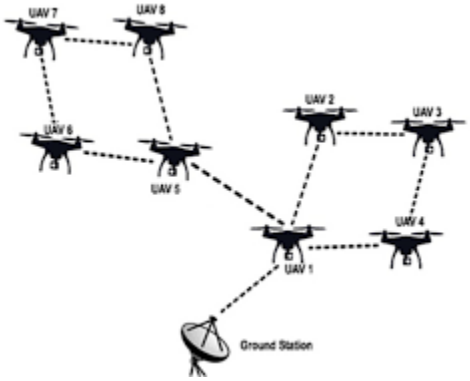

Fig.1 .UAV and ground station deployment

Here discussed about UAV and ground station deployment of how the data can be forwarded through DTN. At first, ground station deployment is achieved with the help of graph based model. As in [14] and because all UAVs U = {u1, u2, u3,...}follow the shortest path, the degree of vertex vi ∈ V is defined as:

(1)

For safety purpose ground station cannot be deployed everywhere in disaster areas…,

$$LIV = vi \in V\ Di < TR \quad (2)$$

And the second one is data forwarding which means it forward the data packets to the destination area that means control station. And the second one is data forwarding, when the UAV finds the critical area it forwards the message to the destination. This forwarding is done by using hop by hop greedy forwarding mechanism. Suppose there neither UAV nor ground station is available, it carries and stores the message for the period of time.

B) ***Common UAVs Cyber Attack***

In this paper, we focused on two types of cyber attack: integrity attackand DOS (Denial Of Service) attack.

1) ***Integrity attack***

This attack aims to contain false information attack GPS spoofing attack.

a) GPS Spoofing Attack:

Leading to a false estimate of drone areas, GPS receiver of a UAV can be spoofed by an attacker. Recently, Wesson [21] on a civilian UAV he has detailed given the procedure for GPS spoofing attack: 1) The satellite at the target node GPS signal with the authenticate signal is generated; 2) To get the control of target node gradually increase the counterfeit signal; 3) From the authentication we slowly move the counter signal.

b) False Dissemination attack:

False information could be disseminated by another kind of attack (i.e..,) ADS-B attack. This ADS-B attack is to broadcast a false position of a GPS coordinates of a target node. A malicious intrusion detection method may also used to provide the false information to degrade the network performance.

2) ***DOS attack***

The major DOS attack in this malicious node is to exhaust energy of UAV and routing protocol. Jamming and gray hole and black hole are the major lethal cyber attack.

a) Jamming attack

The main aim of Jamming attack is to jam the communication between the UAV and controller. Deceptive and random are the two main different types of jamming attack.

b) Gray hole and black hole attacks

A black hole is a node that attracts all the packets by falsely information that can be stored and transmit the data packets to the destination node [12]. It disturbs the routing protocol by deceiving other nodes about the routing information. The source node sends data packets to the black hole instead of the destination node [14]. When the source node transmits data packets through the black hole, the attacker discards them without sending back a RERR message.

III PROPOSED METHODOLOGY AND DISCUSSION

HIERARCHICAL INTRUSION DETECTION AND RESPONSE SCHEME:

We proposed an efficient hierarchical intrusion and response scheme for protecting UAV networks. The main aim of this efficient hierarchical detection is to prevent the most lethal cyber attack that could target an UAV networks such as GPS Spoofing, jamming, black hole and gray hole attack and false information. By using hierarchical we can classified as two ways, an intrusion detection mechanism which can be running at UAV node and intrusion response mechanism which can be running at the ground station level.

A) Intrusion Detection Mechanism

Intrusion Detection System has been classified into two types. There are rules based intrusion detection and anomaly intrusion detection. Security is another major challenging issue due to the wireless medium characteristics and the relevant information handled by UAVs. Cryptography and Intrusion Detection System (IDS) are two major security mechanisms. On one hand, cryptography is used to ensure message privacy and node authentication, and is used to prevent external intruders to penetrate the network. IDS use special agents to analyze the misbehavior of a monitored node. IDS are effective in protecting the network against both internal and external intruders. Furthermore, the IDS rely mainly on two detection techniques: Anomaly detection and Rule based Detection. Here the author can use the rules based detection system because anomaly detection can be used detect only the normal behavior of the node. But rules based detection can be used to compare the behavior of monitored node and behavior of specific known attack by the rules. So here we need to find the behavior of specific known attacks by the comparison of behavior of monitored node by the rules based detection method.
Feasibility study is carried out to check the economic impact that the system will have on the organization. The expenditures must be justified. The vehicular adhoc network is used for intelligent transportation. In our proposed system can reduce the communication overhead. In our developed project is used for reduce the communication overhead and improve the network performance. In this proposed system will check by the user. In this system is providing accurate result. The newly developing system is checked by the user, which is intelligently transmitting the message about the traffic to the RSU. The output of the system was reduced the communication overhead and improve the network performance.

B) Intrusion Response method

The response mechanism is embedded in the ground station to evaluate the UAV's behavior and categorize each UAV according to its perceived threat into the appropriate list. UAV categorization into a well or bad behaved node and permanent exclusion of a malicious UAV can only be done by a trust entity (i.e., ground station) to decrease the false positives and negatives. Thereby each UDA broadcasts to the ground station located within its radio range an Intrusion Report message, which includes the suspected UAV's information. The ground station stores into its database the id of this suspected UAV, the ids of UDAs that detect the suspected UAV as an intruder and also the ids of UDAs (neighbor of suspected UAV) that do not detect it as an

intruder. Afterward, the ground station executes the verification, node assessment, and Monitored UAVs' Categorization processes.

IV. EXPERIMENTAL RESULT

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.

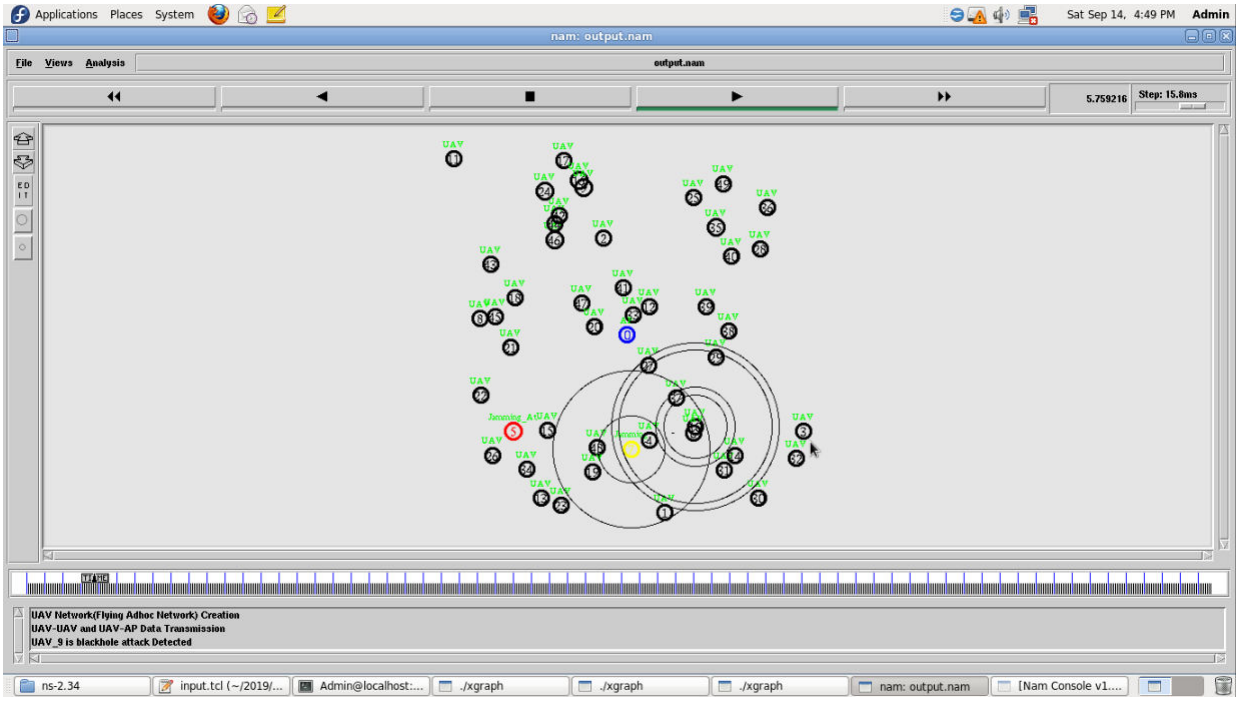

Fig 2: Network Communication

Predict the jamming attack, black hole and gray hole attack, spoofing attack, false information dissemination attack.

V. CONCLUSION

In this paper, we have taken the challenge of securing an UAV network by proposing a hierarchical intrusion detection and response scheme, which orchestrates the intrusion detection, decision, and categorization mechanisms cooperatively between UAVs and ground stations to detect and eliminate security threats that may disrupt the network. To model a normal UAV behavior, a set of detection rules related to each cyber-attack is proposed. Furthermore, at the ground station level, SVM-based anomaly detection is used to verify the attack detected by UAV agents; node assessment and UAV's categorization (normal, abnormal, suspect, and malicious) are developed. We have analyzed the performance of our scheme using NS-2, and showed that it

exhibits a high-level of security with a high detection rate and low false positive rate and facilitates prompt detection with a low communications overhead, as compared to current state of an art.

REFERENCES

[1]. R. Mitchell and I.-R. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," IEEE Trans.Syst., Man, Cybern., Syst., vol. 44, no. 5, pp. 593–604, May 2018.
[2].Liang Xiao, CaixiaXie, Minghui Min, Weihua Zhuang, "User-Centric View of Unmanned Aerial Vehicle Transmission Against Smart Attacks , " in Proc. IEEE Int. Conf. Unmanned Aircraft Syst., Orlando, FL, USA, 2017, pp. 383–388.
[3]. H. Sedjelmaci, S. M. Senouci, and M.-A. Messous, "How to detect cyber-attacks in unmanned aerial vehicles network?" in Proc. IEEE Globecom, Washington, DC, USA, Dec. 2017, pp. 1–6.
[4].Ke-Wen Huang, Hui-Ming Wang, " Combating the Control Signal Spoofing Attack in UAV Systems" in IEEE Trans. Mar 2018.
[5]. Shuhang Zhang, et al., "Cellular UAV-to-X Communications: Design and Optimization for Multi-UAV Networks" in IEEE Trans Jan 2019 .
[6]. Xiao Liu, Yuanwei Liu et al.," Trajectory Design and Power Control for Multi-UAV Assisted Wireless Networks: A Machine Learning Approach" in IEEE Trans. Jun 2019.
[7]. Fen Cheng, Shun Zhang et al., "UAV Trajectory Optimization for Data Offloading at the Edge of Multiple Cells" in IEEE Trans. Mar 2018.

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.

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 from JayarajAnnapackiam C.S.I College of Engineering in the year 2018. Her area of interests' are Networks, Intrusion detection system.