A Survey on Different Types of Attacks in UAV Network

K.Shanthini Smilin[1], Dr.S.Raja Ratna[2]
[1]ME Student, [2]Associate Professor
[1,2] Department of CSE, V V College of Engineering, Tisaiyanvilai,India

***Abstract* - Unmanned Aerial Vehicles (UAV) for traditionally exhausting and dangerous manned missions has become more feasible. Security issues are a major concern in the UAV network. This paper focus on the most lethal cyber-attacks that can target an UAV network, namely, GPS spoofing, jamming, black hole and grey hole attacks. The aim of this paper is to provide a general overview of various detection techniques for different attacks in UAV networks. This study covers the related works, the possible attacks in UAV networks and various detection techniques. The comparative analysis of various attack detection techniques is also highlighted.**

***Keywords*-** Anomaly, cyber, detection, Intrusion, UAV.

I. INTRODUCTION

Unmanned aerial vehicles (UAVs) or drones are flying entities that can be controlled remotely or autonomously without a human on board. In recent years, they have been widely investigated in different fields, not only for military use as well as in civilian applications such as research and rescue missions, target detection, remote sensing and surveillance tasks.

Unmanned aerial vehicle is a flying machine without a human pilot on board and a type of unmanned vehicles. It comprise a large part of the warfighting capability of modern militaries. Likewise, they are emerging in civilian applications such as surveillance for law enforcement, situational awareness for emergency services, content for news outlets, and information accumulation for researchers. While they pose the same risk as piloted aircraft, he operator is removed from the vehicle in time and space which calls for enhanced automated security systems to guarantee the safe operation.

There are three kinds of aircraft, excluding missiles that fly without pilots; they are unmanned aerial vehicles (UAVs), remotely piloted vehicles (RPVs), and drones. UAVs used in military that have autopilots and navigation systems which are used to maintain attitude, altitude, and ground track automatically. An unmanned aerial vehicle (UAVs) has been limited to military use for the past decade. Nowadays, UAVs are additionally used in civil functions to explore inaccessible zones (e.g., disaster areas) and deliver information to and from areas with no network infrastructure (3G, 4G, etc.).

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.

This paper focuses on the survey of different detection techniques used in various attacks in UAV networks. The paper proceeds as follows. Section 2 explains the different types of attacks in UAV Network and Section III describes the literature survey. Finally Section 4 concludes the paper.

II.TYPES OF ATTACKS IN UAV NETWORK

The possible attacks in UAV networks are jamming attack, GPS Spoofing attack, Black hole attack, and Grey hole attack.

2.1 Jamming attacks

Jamming attack are introduced by emitting radio frequency signals, such attacks are not easily preventable by regular security measures. In nutshell, jamming works by denying service to authorized users [2]. In jamming, legal Packets are jammed by the large frequencies of illegal traffic. Jamming is used for lowering network performance. Jamming is just one of many ways to compromise the network. an Attacker is aware of implementation details of network protocols [4]. By using this knowledge, jammer targets the packets of high priority. Ideal jamming attacks are hard to detect, efficient, resistant to anti-jamming measures.

2.2 GPS spoofing attack

The Global Positioning System (GPS) is comprised of a network of satellites that continually broadcast time stamped messages describing their locations in space [7]. GPS receivers use these time stamped messages to determine how long it took for the signals from each satellite to reach the receiver. Multiplying this time by the speed of light gives the distance between the receiver and each satellite [9]. Transmitting false GPS signals to receivers may cause them to lock onto the false signals instead of the authentic satellite signals. This is called GPS spoofing.

2.3 Black hole attack

A black hole node that attracts all the packets by falsely claiming that it has valid route to 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]. At the point when the source node transmits data packets through the black hole, the attacker disposes of them without sending back a RERR message.

2.4 Grey hole attack

Grey-hole is an attack that can switch from behaving genuine to sinkhole. Because it can act as normal node switch over to malicious node it becomes too typical to identify the state whether it us normal node or malicious node [11]. In the ad-hoc on demand distance vector (AODV) routing process every node carry a routing table having ultimate destination and next hop information. This information is used to discover route from source to destination [15]. Here, every node check routing table to know whether the route is available or not. In case of indirect communication it forward packets to next hop node to forward packet to destination.

III. COMPARATIVE ANALYSIS OF ATTACK DETECTION TECHNIQUES IN UAV NETWORKS

Various attacks encountered in UAV networks are jamming attack [1]-[5], GPS Spoofing attack[6]-[10], Black hole attack [12]-[14], as well as Grey hole attack[11],[15],[16]. The existing detection techniques for various attacks are listed in the following tables.

3.1 Jamming Attack:

In jamming, legal Packets are jammed by the large frequencies of illegal traffic. Jamming attacks are not easily detectable by regular security measures. Various jamming detection techniques in UAV network are Kalman filter technique[1], Harmony search algorithm[2], policy hill climbing technique[3], Isaacs approach[4], Free space optical technique[5]. Different techniques are listed in Table 1.

TABLE 1 JAMMING ATTACK

Technique	Description	Advantage	Drawback
Kalman filter[1]	Estimate the probably direction of the jammer from loud perception of the jammer's position	Jammed nodes decreases up to 96.65% compared with legacy isotropic communication.	Computational expensive.
Harmony search algorithm[2]	Find helper node position that maximize the quantity of jammers expected to disrupt the network.	Robustness of wireless networks is improved.	Less security

Policy hill climbing[3]	Jamming in the dynamic UAV supported VANET game without the information of network model and jamming model.	Anti-jamming transmission performance is improved. Error bit rate is improved.	Shorter distance.
Isaacs approach[4]	Determine the necessary conditions to land at the equations governing the seat point strategies of the players.	Optimal controls for various terminal conditions.	Does not analyse multiple jammers and multiple UAVs.
Free space optical[5]	Prevents the transmitter and the receiver to properly communicate through the FSO interface and to utilize the network resources.	Recover the transmitted signal.	Shorter time period.

3.2 GPS Spoofing Attack:

The Global Positioning System (GPS) is comprised of a network of satellites that continually broadcast time stamped messages describing their locations in space. Various GPS spoofing detection techniques in UAV network are Machine learning and Neural network technique[6], MLAT and Spoofer localization technique[7], SLMR algorithm[8], Support Vector Machine algorithm[9], Sensor fusion technique [10]. Different techniques are listed in table 2.

TABLE 2 GPS SPOOFING ATTACK

Technique	Description	Advantage	Drawback
Machine learning, Neural network[6]	Detect GPS spoofing signals.	Maximize the accuracy.	Unlabled data.
MLAT, spoofer localization[7]	Measure the time and position.	Detection delay below two seconds.	Privacy issues.
SLMR algorithm[8]	Analyzing the variation in the front-end signal power recorded by the GPS recipients on-board a system of UAVs.	Locate multiple jammers.	Inability to track GPS signal.
Support Vector Machine[9]	Identification of GPS spoofing attack to unmanned aircraft vehicle.	Can detect any spoofing attack.	Undetected large position errors.

Sensor fusion algorithm[10]	Impact on UAVs is investigated, through a series of tests, in a simulation environment.	Low communication rate.	Cannot guarantee the security.

3.3 Black Hole attack:

A black hole node that attracts all the packets by falsely claiming that it has valid route to destination node. Various black-hole detection techniques in UAV network are detection and prevention algorithm[12], AODV protocol[13], Robust algorithm[14]. Different techniques are listed in table 3.

TABLE 3 BLACK HOLE ATTACK

Technique	**Description**	**Advantage**	**Drawback**
SPRT method[15]	Identifying black hole attack which causes loss of critical information on the network.	Effective and fast detection.	Does not use cluster sensor nodes.
DSR algorithm[16]	Define routes from source to destination.	Minimizes the number of route requests.	Does not locally repair a broken down links.
AODV routing protocol [11]	Build up routes to destinations on demand both unicast and multicast routing.	High processing demand.	Increase false positive detection.

3.4 Grey hole attack:

Grey-hole is an attack that can switch from behaving genuine to sinkhole. Because it can act as normal node switch over to malicious node it becomes too typical to identify the state whether it us normal node or malicious node. Various Grey hole detection techniques in UAV network are SPRT method[15], Dsr algorithm[16], AODV routing protocol[11]. Different techniques are listed in table 4.

TABLE 4 GREY HOLE ATTACK

Technique	Description	Advantage	Drawback
Detection and prevention algorithm[12]	Detection and prevention of Black hole attack in WSN.	Low throughput.	High end to end delay.
AODV protocol[13]	Removes malicious node by isolating it to make safe and secure communication.	Easier to breach the security.	Increase false positive rate.
Robust algorithm[14]	Detect colluding attackers.	Low false positive.	Continuously drop message.

IV. CONCLUSION

Security issues are a major concern in the UAV network. This paper surveyed the different types of attacks, its vulnerability, and classification of its detection techniques. Four different attacks in UAV network and their detection techniques, their advantage and disadvantage are compared and discussed in this paper.

REFERENCES

[1] Suman Bhunia, Shamik Sengupta, “Distributed adaptive beam nulling to mitigate jamming in3D UAV mesh networks”, International conference on networking and communication, 2017.

[2] Jixin Feng, Warren E. Dixon, and John M. Shea, “Positioning helper nodes to improve robustness of wireless mesh networks to jamming attacks”, IEEE conferences on GLOBECOM, 2017.

[3] Xiaozhen Lu, Dongjin Xu, Liang Xiao, Lei Wang , Weihua Zhuang, “Anti-Jamming Communication Game for UAV-aided VANETs”, IEEE conferences on Global Telecommunications,2017.

[4] Sourabh Bhattacharya, Tamer Basar, “Game-theoretic analysis of an aerial jamming attack on a UAV communication network”, Proceedings of American Control Conference, PP 818-823, 2010.

[5] Maha Sliti, Walid Abdallah, and Noureddine Boudriga, “Jamming Attack Detection in Optical UAV Networks”, International Conference on Transparent Optical Network, 2018.

[6] Mohsen Riahi Manesh, Jonathan Kenney, Wen Chen Hu, Vijaya Kumar Devabhaktuni, and Naima Kaabouch, “Detection of GPS Spoofing Attacks on Unmanned Aerial Systems”, IEEE Conference on Annual Consumer Communications & Networking, Jan 2019,

[7] Kai Jansen, Matthias Schafer, Daniel Moser, Vincent Lenders, Christina Popper and Jens Schmitt, “Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks”, IEEE Symposium on Security and Privacy,2018.

[8] Sriramya Bhamidipati, Grace Xingxin Gao, “Locatong Multiple GPS Jammers Using Networked UAVs”, IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1816 – 1828, 2019.

[9] G. Panice, S. Luongo, G. Gigante, D. Pascarella, C. Di Benedetto, A. Vozella, “A SVM-based detection approach for GPS spoofing attacks to UAV”, International Conference on Automation and computing, Sep 2017.

[10] Daniel Mendes, Naghmeh Ivaki, Henrique Madeira. “Effects of GPS Spoofing on Unmanned Aerial Vehicles”, Pacific Rim International Symposium on Dependable Computing, 2018.

[11] Durgesh Kshirsagar, Ashwini Patil, “Blackhole Attack Detection and Prevention by Real Time Monitoring”, International conference on Computing, Communications and Networking Technologies,2013.

[12] Mohammad Wazid, Avita Katal, Roshan Singh Sachan, R H Goudar and D P Singh, "Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network", International Conference on Communication and Signal Processing, PP. 576-581, 2013.

[13] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks", International Conference on Advanced Computing & Communication Technologies, 2012.

[14] Thi Ngoc Diep Pham and Chai Kiat Yeo, "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks", IEEE Transactionon Mobile Computing ,vol. 15, no. 5, May 2016.

[15] Maryam Motamedi, Nasser Yazdani, "Detection of Black Hole Attack in Wireless Sensor Network Using UAV", 7th International Conference on Information and Knowledge Technology, 2015.

[16] Prachee N.Patil, Ashish T.Bhole, " Black holeattack prevention in mobile Ad Hoc networks using route caching" 10th International Conference on wireless and Optical Communication Networks, 2013.

[17]