ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

Cyber Security Methods for Vehicle Networks Challenges and Solution Using UAVs Networks

Murugesan S, Dr. Nithya.,B.E.,M.E.,Ph.D., R.Bharanidharan,M.E.,(Ph.D),

Dept. of Computer Science & Engg., VMKV Engineering College, Salem, India

Professor & Head of the Department, Dept. of Computer Science & Engg., VMKV Engineering College, Salem, India

Assistant Professor, Dept. of Computer Science & Engg., VMKV Engineering College, Salem, India

ABSTRACT: Unmanned aerial vehicles (UAVs) networks have not yet received considerable research attention. Specifically, security issues are a major concern because such networks, which carry vital information, are prone to various attacks. Cyber Physical Systems (CPS) play an important role in providing critical services in industries such as: autonomous vehicle systems, energy, health, manufacturing, etc., by integrating computation, physical control, and networking. Most of these systems are not only cyber-physical, but also operate in a safety-critical application where a failure or malfunction could result in damage or even loss of life. An Unmanned Aerial System (UAS) meets the requirements of a CPS and safety-critical system with its dependence on wireless communication, sensors, and algorithms that work synergistically to perform its functionality. Innovation technology has followed the paradigm of enhancing performance as a main priority, with security as either an afterthought or not considered at all, causing a lack of security against cyber-attacks in most UAVs. In the past UAVs have expensive, heavy, and most commonly used by the military, however, cost, size, and weight have decreased drastically, while their capabilities, attributed to technology, have increased substantially.

I. INTRODUCTION

Technological advances are rapidly increasing in unmanned systems and secure solutions must keep-up with the technology to maintain safety and assurance. The increased interest in UAS due to semi and fully autonomous flight has benefited the civilian and military community and lead to increased efforts to incorporate UASs into industry [1] [2]. The shift of control from a human pilot to an automated, computerized autopilot has tremendous advantages; however, the dependence on embedded electronics exposes UASs to new threats of cyber-attacks. The cyber threats to UASs are becoming more evident and research in the area of securing safety-critical CPSs is increasing [3] [4]. Current research is focused on creating attack assessments and discovering vulnerabilities [5] [6], but has not significantly addressed detection and prevention of cyber-attacks on UASs, and more specifically the UAS Flight 3 Control System (FCS). Information for environmental monitoring, emergency, rescue and recovery operations, and disaster assistance. Setting upan ad-hoc network consisting of UAVs is very challengingbecause they differ from mobile ad-hoc networks (MANETs)and vehicular ad-hoc networks in terms of mobility, connectivity, routing, services, and applications. A survey has been conducted on cyber-attack vulnerabilities and defenses for flight control systems [7].

II. BACKGROUND AND RELATED WORK

2.1 Vulnerabilities of a generic CPS

A vulnerability can be defined as a weakness or flaw in the system which an exploit can take advantage of to perform malicious activity. The vulnerabilities of a CPS can vary depending on the application. To characterize the vulnerabilities that exist in a CPS, a taxonomy of vulnerabilities was developed as shown in Figure 1. Although it is not a complete taxonomy listing all vulnerabilities in a CPS, it can be generalized to apply to most systems. The taxonomy does not differentiate between deliberately and non-deliberately created vulnerabilities, as it demonstrates where a vulnerability is created in a general manner. Who created the vulnerability and for what purpose can be considered irrelevant for the purposes of this work.

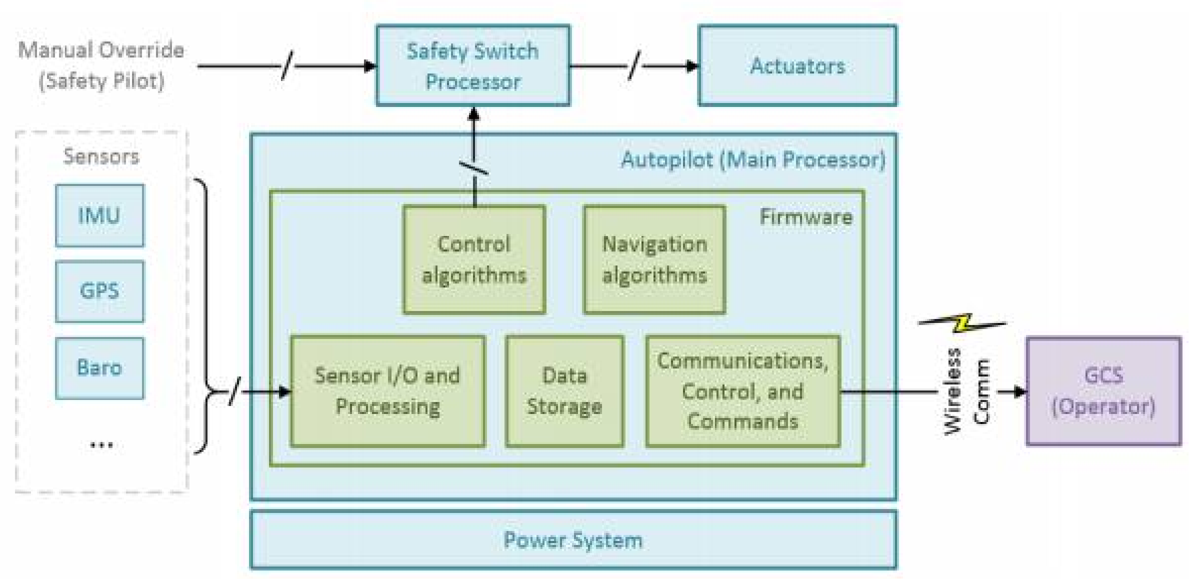


Figure: 1 manual diagram of Cyber-Attacks in UAV Networks

2.2 Network Attacks

UASs typically use wireless communications links for command, control, and communications (C3). The C3 link allows a GCS operator to send navigational commands to change the vehicles flight path, altitude, airspeed, and etc. as well as receiving system status and health information from the vehicle. The data communications link, if applicable, allows the real-time transmission of data gathered by the vehicle (e.g. video) to be sent to the operator or other entities. Usually, the data communications link does not affect the operation of the vehicle meaning that it is not safety-critical, although interrupting it may effectively cause a Mission Envelope Failure. Small, low-cost, COTS UASs were not historically designed with the consideration that the wireless communication channel would be a vulnerability since they were considered to be used as a hobby. It has become evident, however, that the vulnerabilities in UAS communication links can be exploited. With UASs becoming more popular, the use of new, low cost, small, lightweight, and fast encryption capabilities will reduce the probability of wireless security problems.

III. PROPOSED METHOD

3.1 Detected cyber-attack

- **GPS Spoofing**

Interest in detecting GPS spoofing has increased in the past decade, leading to the development of techniques applied to GPS signal characteristics, including the position solution, Doppler shift, and SNR. A method is developed in that uses a reference receiver to compare the cross-correlation of the C/A and P(Y) codes. By isolating the P(Y) code, a large correlation can be observed in a non-spoofed signal.

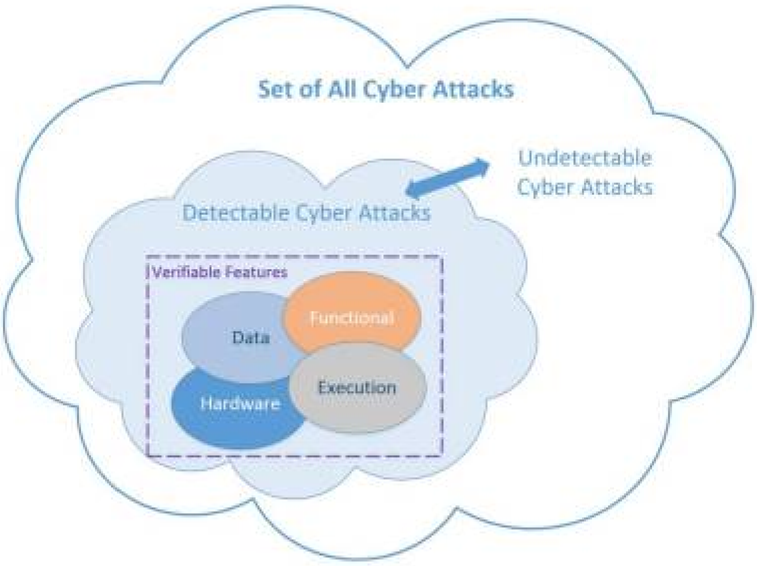


Figure: 2 set of cyber attacks

- In Proposed System, a set of detection and response techniques are proposed to monitor the UAV behaviors and categorize them into the appropriate list (normal, abnormal, suspect, and malicious) according to the detected cyber-attack.
- I focus on the most lethal cyber-attacks can target an UAV network, namely, false information dissemination, GPS spoofing, jamming, and black hole and gray hole attacks.
- Extensive simulations confirm that the proposed scheme performs well in terms of attack detection even with a large number of UAVs and attackers since it exhibits a high detection rate, a low number of false positives, and prompt detection with a low communication overhead.

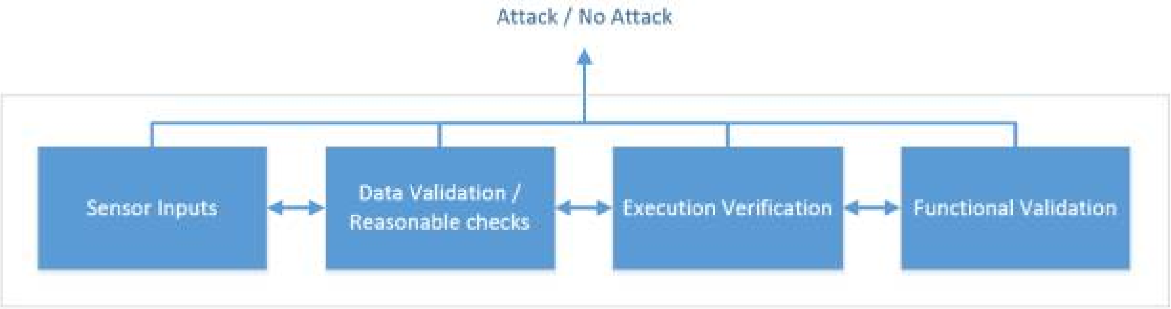


Figure: 3 display of Security Monitor

Attack detection even with a large number of UAVs and attackers. It exhibits a high detection rate, a low number of false positives, and prompt detection with a low communication overhead.

DOI: 10.15680/IJIRCCE.2018.0605093

IV. RESULT AND DICUSSION

Which satisfies the requirement of delay-sensitive applications. Such efficiency is attributed to community of trusted UDAs: all the UAVs, in the hierarchical scheme, have the ability to run an intrusion detection agent (UDA) and monitor their neighbors. However, when the UAV is suspected to be malicious, it cannot play the role of UDA. Therefore, only a community of trusted UDAs carry out the intrusion monitoring and detection, thus reducing the time.

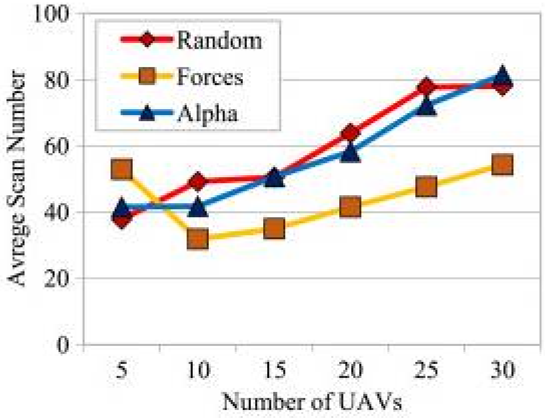
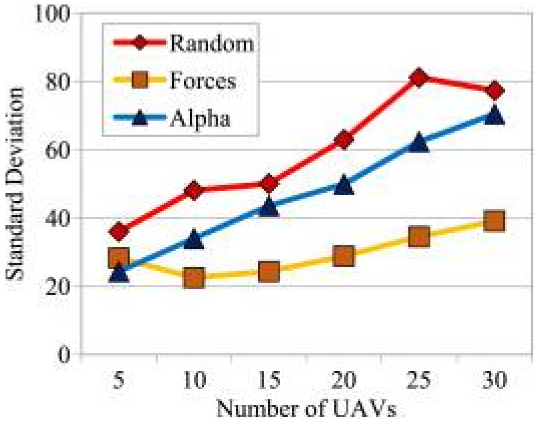


Figure: 4 detecting malicious UAVs.
(A) Average scan number



(b) Standard deviation

DOI: 10.15680/IJIRCCE.2018.0605093

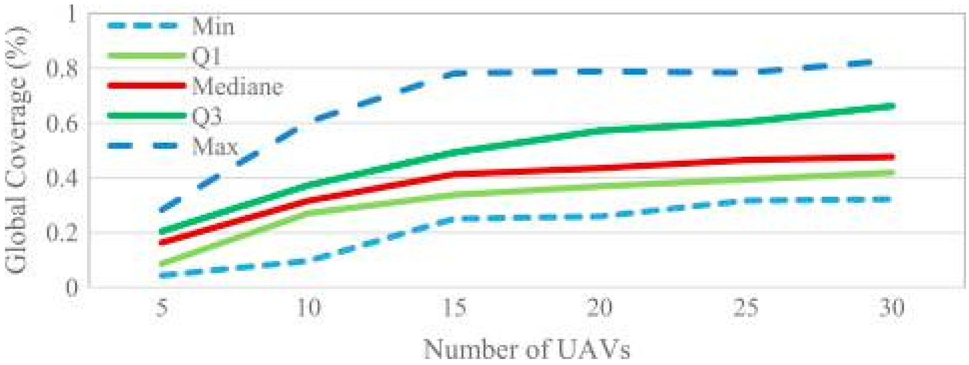


Figure: 5 Number of UAVs

Global Positioning System has slowly evolved to the point where it is the most widely used positioning system in the world. Aircrafts, Ships, Missiles, Cars and UAVs rely on the positioning provided by this system to make their next move. In a world where GPS is vital and in fact the most revolutionary positioning method

V. CONCLUSION

UAV that directs its weapon against a friendly resource, jamming, bad- and good-mouthing. In this detection framework, the authors proposed a set of rules related to the attacks to model a normal UAV behavior. According to their simulation results, their detection system exhibits a low false negative. However, the false positive is higher (equal to 7%).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. I have analyzed the performance of our scheme using NS-3, and showed that it exhibits a high-level of security with a high detection rate (more than 93%) and low false positive rate (less than 3%), and facilitates prompt detection with a low communications overhead, as compared to current state of the art. Our future direction is to embed our scheme in a fleet of a dozen of Parrot drones.

REFERENCES

[1] E. Yanmaz, R. Kuschnig, and C. Bettstetter, "Channel measurements over 802.11a-based UAV-to-ground links," in Proc. IEEE Globecom Wi-UAV Workshop, Houston, TX, USA, 2011, pp. 1280–1284.
[2] M. O. Cherif, S.-M. Senouci, and B. Ducourthial, "Efficient data dissemination in cooperative vehicular networks," Wireless Commun. Mobile Comput., vol. 13, no. 12, pp. 1150–1160, 2013.
[3] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1557–1568, Oct. 2007.
[4] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," in Proc. IEEE Veh. Technol. Conf. (VTC Fall), San Francisco, CA, USA, 2011, pp. 1–5.
[5] H. Sedjelmaci, S. M. Senouci, and M. Feham, "An efficient intrusion detection framework in cluster-based wireless sensor networks," Security Commun. Netw., vol. 6, no. 10, pp. 1211–1224, 2013.
[6] X. Haijun, P. Fang, W. Ling, and L. Hongwei, "Ad hoc-based feature selection and support vector machine classifier for intrusion detection," in Proc. IEEE Int. Conf. Grey Syst. Intell. Services, Nanjing, China, 2007, pp. 1117–1121.
[7] C. Callegari, S. Vaton, and M. Pagano, "A new statistical method for detecting network anomalies in TCP traffic," Eur. Trans. Telecommun., vol. 21, no. 7, pp. 575–588, 2010.