Model Checking Based Unmanned Aerial Vehicle (UAV) Security Analysis

Eman Shaikh
College of Computer Engineering and Science,
Prince Mohammad Bin Fahd University (PMU),
Al Khobar, Saudi Arabia.
emanshaikh26@gmail.com

Nazeeruddin Mohammad, Shahabuddin Muhammad
Cybersecurity Center,
Prince Mohammad Bin Fahd University (PMU),
Al Khobar, Saudi Arabia.
nmohammad,smuhammad@pmu.edu.sa

***Abstract*—For the past few years, there has been an increase in the use of Unmanned Aerial Vehicles (UAVs). Referred popularly as drones, this technology was initially developed to perform military operations. Later they were used in different civilian sectors like agriculture, environment, disaster management, etc. It has been predicted that by the end of the year 2036, the UAV industry would soar up to $30 billion. However, an increase in the use of UAVs meant that there would be a rise in the risk of security. This paper talks about the different security attacks that UAVs suffer. It also proposes and implements a Probabilistic Model Checking (PMC) model for these attacks. The proposed model can be used to study the probability of success, cost, and attempts required for a variety of UAV attacks.**

***Index Terms*—UAV, Drone, Attacks, Security**

I. Introduction

Unmanned Aerial Vehicles (UAVs) have been increasingly deployed around the world. The Federal Aviation Administration (FAA) has estimated that currently, a total of seven million UAVs operate in the United States alone [1]. By the end of 2036, it has been anticipated that the total revenue of UAVs would add up to $30 billion [2]. They facilitate smooth operation without the need for a human pilot present on board. Due to this, they can easily navigate in areas that are risky for human life. They are also able to fly at high altitudes for long hours effectively. They have minimal cost and are lightly weighted as compared to an ordinary manned aircraft. This is why they stand out in the market and have a high demand. They were initially developed as a means of carrying out military operations like monitoring dangerous areas, deploying armed weapons, acquiring critical information, airstrikes, and others [3]. They have also gained a major impact in civil sectors to perform activities like the shipment of products, monitor illegal activities, manage wildlife and environment to prevent natural calamities, climate observation, management of wildlife, and a variety of other uses [4].

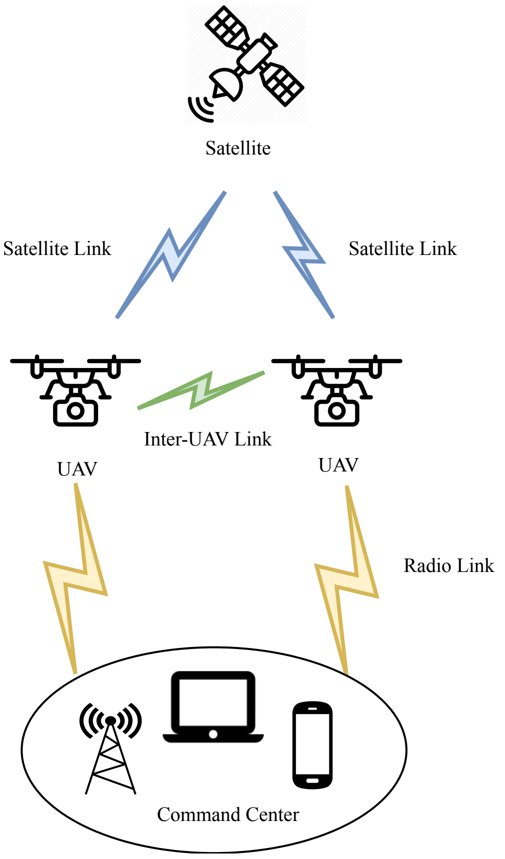

Fig. 1. Basic UAV system.

However, an increase in the popularity of UAVs has also given rise to a variety of security attacks encountered. The extent of the outcome of these attacks depends upon the motive of the attacker. Fig. 1 depicts a basic UAV system that consists of UAVs, satellites, various types of communication links and a command center (smartphones, remote controls, laptops, etc.). The communication channels between UAV and the command center use radio signals, which gives rise to a variety of attacks. Moreover, UAVs constitutes of various sensors onboard to collect and process information that is prone to be acquired by the attacker. These channels could also be injected with fraudulent information. The communication protocol that takes place between UAV-UAV communication is also vulnerable to different attacks. All of these attacks are further discussed in Section II.

The goal of this paper is to review key security threats for

978-1-7281-6535-6/20/$31.00 © 2020 IEEE

UAVs, propose and implement a Probabilistic Model Checking (PMC) solution for modeling the UAV attacks. This proposed model is used to study the probability of success, cost, number of attempts needed for different UAV attacks.

The remaining paper is organized as follows: Section II introduces the different types of cyber-attacks that a UAV can face, Section III talks about modeling details of UAV attacks, Section IV discusses the results acquired by the proposed model for the various attack and Section V concludes the paper with possible opportunities for future work.

II. UAV ATTACKS

Over the past few years, various cyber attacks have been launched on UAV systems. This is mainly because of the absence of security assessment and weak security countermeasures. In December 2009, the first case of cyber-attack was recorded. It was launched by a group of terrorists who tried to capture the live video feed of a UAV through the use of SkyGrabber software [5]. Later in 2011, a keylogger malware was detected after the insertion of an external hard drive to the Predator and Reaper ground control stations [6]. In December 2012, U.S. RQ-170 Sentinel UAV was hijacked and captured by the Iranian government [7]. In July 2012, the University of Texas partnered with the Department of Homeland Security to indicate how a military UAV can be hijacked by using a $1000 worth equipment. In this experiment, they tried to spoof the GPS and take control of the UAV [8]. Therefore, it is important to learn more about the different cyber attacks in order to combat them.

In this section, we have classified the major cyber attacks based on the impact they have on the UAV system as illustrated in Fig. 2. These attacks can result to several issues like the total charge of the UAV, to the landing of the UAV in a different location, or even crashing of the UAV to cause financial loss. Mentioned below are the different ways in which UAV attacks can take place:

A. UAV to UAV Coordination

For optimizing efficiency, multiple UAVs are often deployed to carry out certain tasks. However, the communication network present between them is vulnerable to different security attacks. The goal of the attacker in this type of attack is to disrupt the coordination between the UAVs. This can be achieved by making the UAV collide to one another, sending fake messages to the other UAVs present in the network, deleting or altering the current messages, etc. Examples of such attacks are described below:

1) Dispatch System Attack: The route of UAVs is often predestined in advance to complete the designated tasks. However, for applications that require the use of multiple UAVs like to deliver goods, a dispatch system is used to deploy multiple UAVs. In this case, the attacker would launch an attack on the dispatching system that would mislead the UAV or make it crash to other UAVs. By attacking the dispatch system, the attacker basically makes the system not follow the right allocated missions that were initially assigned to the UAVs. The most common way to launch this attack is to inject Trojans in the system [9].

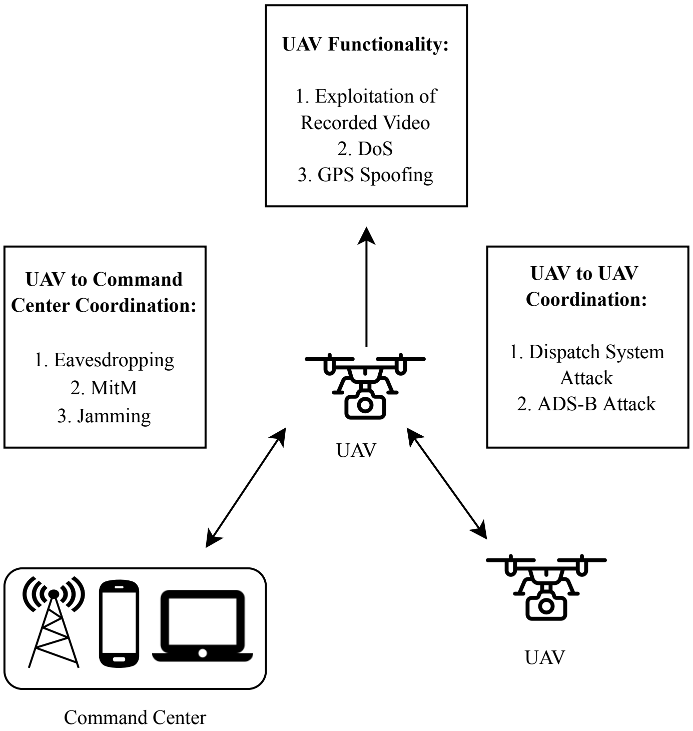

Fig. 2. Classification of cyber-attacks on UAV.

2) ADS-B Attack: The Automatic Dependent Surveillance-Broadcast (ADS-B) technology is implemented in UAVs to ensure collision-free and smooth navigation. It also provides a general overview of the air traffic, so that collisions can be avoided by manned and unmanned air crafts flying within the same network. In terms of a UAV network, this can be achieved by fetching the current location of the UAV and then broadcasting it with other information of the UAV such as altitude, speed, unique identifier, etc. This data is also sent to both air crafts (manned or unmanned) and the command center. However, the ADS-B messages are sent via WiFi in plain text format [10]. This makes the messages vulnerable to a variety of attacks. Some of them are described below:

- *Message Elimination:* An attacker in this attack erases few messages of the original aircraft and prevents other air crafts from acquiring these messages as well as detecting the original aircraft itself. This attack can be achieved through the execution of two major approaches called constructive interference and destructive interference [11]. In constructive interference, the attacker purposely injects bit errors in the ADS-B message to make the recipient drop the message as the message collected would seem like it has been manipulated. Whereas, in the case of the destructive interference, the attacker develops an inverse of the original ADS-signal. This results in the complete or partial destruction of the ADS-B signal.

- *Message Infusion:* The ADS-B network is prone to this attack since it does not provide any means of authentication in the network [12]. The motive of the attacker for this attack is to inject malicious messages to air traffic communication. This can be easily achieved through the use of commercially available devices present in the market [13]. This attack can also be achieved by the means of two major methods: Aircraft Target Ghost injection and Command center Ghost Injection. The purpose of these attacks is to broadcast illegitimate ADS-B messages that are similar in characteristics as that of the legitimate ADS-B messages. The only difference in both methods is that the first one targets the aircraft while the latter targets the command center. Nevertheless, in both methods, the reliability of the information received is questioned as they output the appearance of a fake aircraft on the screen.
- *Message Fabrication:* Fabrication of messages is done via three methods: overshadowing, bit flipping or by a combination of message insertion and removal. Overshadowing is a type of message fabrication attack in which the attacker broadcasts high powered ADS-B signal to substitute parts or the entire legitimate message. In bit flipping, the attacker would superimpose the manipulated signal by flipping the bits from 0 to 1 or 1 to 0. In both of these methods, malicious information is inserted in secret either completely or at least partially. Lastly, the fabrication of a message can also be achieved by a combination of removing information from the message or inserting malicious information to the message [14].

3) TCAS Induced Collision: Traffic collision avoidance system (TCAS) is a system that is designed to avoid collisions in both manned and unmanned air crafts. However, the issue of TCAS is that it cannot predict the long term effect of the advisory it produces. This can give rise to a problem called TCAS Induced Collision. This problem can mainly occur in a heavy network environment as there might some instances that can result in a situation where collision avoidance is not an option. An attacker can hence easily take advantage of such situations by altering the traffic data and forcing conditions that lead to a TCAS Induced Collision. For instance, the author in [15] provided a scenario that depicted this issue. The scenario consisted of four UAVs in which UAV 1 and UAV 2 are initially operating in a collision path. To combat this, the TCAS produces a collision avoidance advisory for both the UAV 1 and UAV 2 to change their altitude respectively (UAV 1 descends and UAV 2 climbs). Now at a lower level altitude, UAV 3 and UAV 4 might face the same situation that was initially faced by the other two UAVs. The TCAS again produces an advisory for UAV 3 and UAV 4, which causes UAV 4 to go at a higher altitude. Now UAV 1 and UAV 4 are on the same collision path. So in this way, even though the TCAS produced successfully advisories for the four UAVs, but the new advisory is no longer useful since there is not much time to implement a new path before the collision can occur.

B. UAV to Command Center Coordination

The command center is a critical part of the UAV network. This is because it is responsible to perform a variety of operations like payload control, mission planning, and air vehicle control [16]. These operations are executed on the UAV via radio or a wireless link that is not secure in nature [17]. Thus, the communication links are vulnerable to various cyber-attacks. The goal of the attacker in this attack is to disrupt the coordination between the UAV and the command center.

1) Eavesdropping: In this attack, the attacker gains unauthorized access to listen to broadcast transmissions that are not encrypted in nature. The attack also allows the attacker to gain a copy of the required data. The goal of the adversary is to attack the weakly encrypted communication channel between the UAV and other network entities [18]. Although the eavesdropping can be used for several beneficial methods like keeping a record of commercial airplanes, data obstruction, legal obstruction of aircraft, etc., it can also be used as an initial step for launching even more complicated and dangerous active attacks. In terms of UAV, the attacker would eavesdrop to learn the way the packets in the network are designed and then use this knowledge to launch a harmful active attack [19].

2) MITM: Also known as a Man-in-the-Middle attack. In this attack, the attacker takes complete control over the communication between the UAV and the command center. Furthermore, the attacker also secretly collects confidential data. This collected data is then used by the attackers to behave as though they are legitimate users. The attacker can also pose as a legitimate user by issuing an authentication command to the UAV [20].

3) Jamming: It is a type of attack where packets are intentionally transmitted to restrict the communication network to send or receive information. To execute this attack in a UAV system, the jammer would constantly send out packets to restrict the system to receive or send information from other nodes present in the same network. This loss of control signal makes the UAV to enter into a lost link state. In this case, the UAV normally enables the command center to call out for a lost link protocol [21]. But, because of this attack, the protocol thinks that the call for the lost link protocol was done due to an error in the data link present in the UAV. Furthermore, it also assumes that the UAV can navigate its way to the base via the GPS signals. However, in this attack, the jammer would also jam the GPS signals. Thus, this would allow the jammer to take complete control of the UAV.

4) WiFi Attack: This type of attack only occurs to UAVs that operate on a WiFi signal. In this attack, the attacker tries to disrupt the communication link between the UAV and the command center and then take full charge of the UAV. For instance, the authors in [22] demonstrated a way to launch a WiFi attack by following three steps. First, they target and monitor a particular WiFi network. Then, they try to gain the authorization of the network by launching a de-authentication attack. Finally, the password of the system is cracked and the

UAV is hijacked. One way to avoid this attack is to use a remote control with a radio signal rather than WiFi.

C. UAV Functionality

Some of the cyber attacks launched in the UAV has a major impact on the way the UAV behaves. The main motive of the attacker in this attack is to take full control of the UAV and perform tasks according to their respective goals. These types of attacks can either target the components present in the UAV or the communication network present in the UAV system itself. Described below are examples of such attacks:

1) Exploitation of Recorded Video: This attack is performed exclusively on small-scale UAVs that use its camera to perform smooth navigation without any collisions. For this to be executed effectively, the flight controller first requests the recorded video from the kernel via system calls [23]. However, an attack can be launched, provided that the attacker has an idea of the system specifications and can access the flight controller to obstruct the system calls issued to the kernel and also replace the original video with a manipulated one. The outcome of this attack is to make the land drone intentionally to a different location as compared to the designated one.

2) DoS: Also known as Denial of Service attack, is a type of that that is launched on small-scale drones, provided that the attacker has access to flight controller specifications. This access allows the attacker to disrupt the UAV system. The attack can be carried out by depleting the batteries, overloading the processing units, flooding the communication channels, etc. That is, the attack can alter the commands given by the flight controller by making the system land, crash, drift and also eventually shut down the UAV while the drone is still functioning [9].

3) GPS Spoofing: In this attack, a fake signal is generated. The signal can be artificially created from computers or it could be pre-recorded versions of past legitimate GPS signals. The attacker deceives the GPS receiver by successfully broadcasting the spoofed GPS signals from satellites that are higher in power than the legitimate GPS signals. This attack is commonly done to hijack civilian UAVs, as the GPS in military UAVs is more secure in nature [24]. This could even lead to the crashing of the UAV, provided that other UAVs within the same network perceive this fabricated signal.

III. UAV SECURITY MODELING

For this study, we are modeling attacks on UAV functionalities using Probabilistic Model Checking (PMC) [25]. For this study, we are considering that cyberattacks on UAV functionalities can be done in three different ways: direct access attacks, masquerading the command center communications, and denial of service (DoS) attacks. An attacker chooses one of these methods non-deterministically.

Direct access to drone hardware and software components is not easy, but nonetheless possible in various ways. For example, one method is with the help of installed malicious software (malware). Malware can be introduced into the drone during the firmware updates by exploiting the firmware update process or during the software updates by exploiting the operator machine. Another possibility is that an insider intentionally introduces malware.

When direct access is not possible, the drone functionality can be affected by interfering with the external inputs that drone depends on such as GPS signal and command and control center (CCC) instructions. In this context, Man-in-the-Middle (MITM) attacks are possible that manipulate the legitimate commands from CCC. Similarly, fake instructions can be given by masquerading the CCC. Similarly, interfering with GPS signals can result in false location information.

DoS attacks can be done by jamming the RF communication channels or by sending several unwanted commands that may result in energy depletion. In either case, drone functionality is greatly affected.

Once the attacker has chosen the type of attack, he retries different possible approaches for that attack for a maximum number of attempts. Once he reaches the maximum limit, he switches to another type until all the types are finished. In this case, the attack is considered unsuccessful. Conversely, when the attacker is successful the severity of the attack is determined by the type of attack. In this study, we consider the direct access attacks have the highest severity (3), the manipulation of external signals has a medium severity (2) and the DoS attacks have a low severity (1).

IV. TESTING AND DISCUSSION

The UAV attack model described in Section III is implemented in the popular probabilistic model checker PRISM. The probability of direct access attack, manipulation of external inputs, and DoS attacks is considered 1%, 10%, and 20% respectively. The cost (work required) of an attack is considered the same for all types of attacks and is chosen to be 3 units.

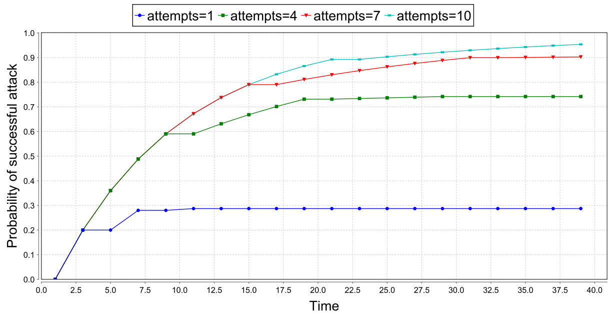

Fig. 3. Probability of attack success for different number of unsuccessful attempts that an attacker can make.

The model is used to calculate the maximum probability of any of the attacks when the attacker has abundant time, but a limited number of attempts. The obtained results are plotted in Fig. 3. As anticipated, increasing the number of attempts increased the probability of success. However, the increase is not proportional to the total number of attempts. Increasing the ”attempts” from one to four has increased the probability of a successful attack by more than 40%. On the

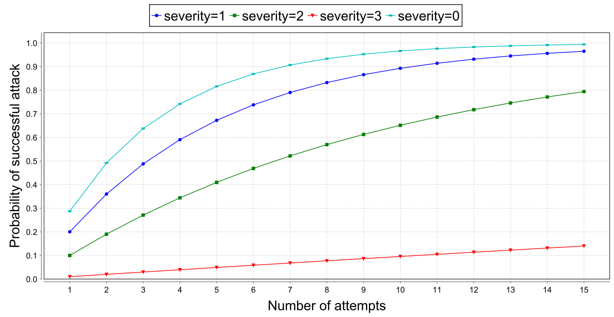

Fig. 4. Probability of attack success for different number of unsuccessful attempts without any time restrictions.

other hand, changing the "attempts" from seven to ten has increased the probability of success only 5%. Further, the probability remains constant regardless of available time for the attack. To check how many attempts are needed to make a successful attack, we calculated the attack success probability by changing the number of attempts without any restrictions on the time. The results are plotted in Fig. 4. The results show that at most 15 attempts are needed to have a successful attack of any impact level (represented as severity =0 in the figure). However, for high impact attacks the probability of success is very low (< 0.2) even after 15 attempts.

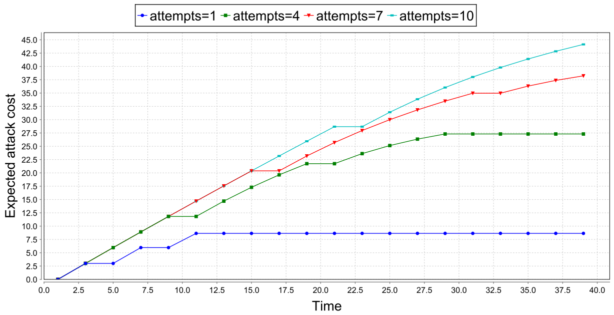

Fig. 5. Cost of attack for different number of unsuccessful attempts that an attacker can make.

The number of attempts increases the cost of the cyber attack on UAV. The model is used to calculate the attack overhead for a different number of attempts and results are plotted in Fig. 5. Similar to the probability of a successful attack, the cost also becomes constant after a certain time. In other words, once the maximum number of attempts is completed, the cost will not change. Since the cost of each attack attempt is chosen the same (3 units), the plot is mostly linear.

In the above results, the probability of success is calculated when any one of the attacks is successful. Fig. 6 shows the probability of a successful attack for individual attack types when the maximum number of retries is five. The results show that direct access attacks have less than 5% success possibility, while DoS attacks have more than 76% possibility. The possibility of any one of the attacks is also plotted for reference, and it has around 82% of success.

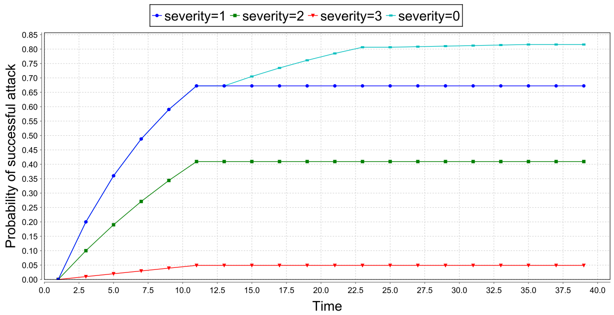

Fig. 6. Probability of attack success for different types of attacks.

V. Conclusion and Future Work

In the last few years, there has been widespread use of UAVs in both military and civil sectors. This is because they are affordable, portable, can fly long hours and most importantly that they do not require the presence of a human pilot onboard for its operation. Instead, they are operated remotely by pilots or autonomously via onboard computers. As the population of UAVs has been increasing at an enormous rate, so are the possibilities of different security attacks. In this paper, we have briefly talked about the key attacks that a UAV can face. We have modeled direct access attacks, masquerading, and denial of service (DoS) attacks using the PMC. We have also shown a glimpse of insights that can be obtained using PMC. As part of our future work, we intend to extend the model to include all types of major attacks on UAVs and study their risk under various practical scenarios.

Acknowledgment

This research is partially supported by the Cybersecurity Center at Prince Mohammad Bin Fahd University.

References

[1] A. France-Presse, "Faa: Number of us drones will triple by 2020," Website, 3 2016. [Online]. Available: https://www.industryweek.com/technology-and-iiot/article/21972014/faa-number-of-us-drones-will-triple-by-2020

[2] "Unmanned aircraft systems (uas) represent a $30 billion opportunity for satcom and imaging," Website, 11 2018. [Online]. Available: https://www.nsr.com/unmanned-aircraft-systems-uas-represent-a-30-billion-opportunity-for-satcom-and-imaging/

[3] V. Boulanin and M. Verbruggen, *Availability and military use of UAVs*, 08 2017, pp. 121–132.

[4] D. Starovoytova, "Emerging technologies: Use of unmanned aerial systems in the realization of vision 2030 goals in the counties," *International Journal of Applied Science and Technology*, vol. 3, 01 2013.

[5] "Us drones hacked by iraqi insurgents," Website, 12 2009. [Online]. Available: https://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked

[6] "Exclusive: Computer virus hits u.s. drone fleet," Website, 07 2011. [Online]. Available: https://www.wired.com/2011/10/virus-hits-drone-fleet/

[7] "Hacking drones . . . overview of the main threats," Website, 06 2013. [Online]. Available: https://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/

[8] "How college students hijacked a government spy drone," Website, 07 2012. [Online]. Available: https://www.zdnet.com/article/how-college-students-hijacked-a-government-spy-drone/

[9] R. Altawy and A. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, pp. 1–25, 11 2016.

[10] M. Strohmeier, V. Lenders, and I. Martinovic, "Security of ads-b: State of the art and beyond," *IEEE Communications Surveys Tutorials*, vol. 17, 07 2013.

[11] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, Secondquarter 2015.

[12] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, "Realities and challenges of nextgen air traffic management: the case of ads-b," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 111–118, May 2014.

[13] A. Costin and A. Francillon, "Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," in *BLACKHAT 2012, July 21-26, 2012, Las Vegas, NV, USA*, Las Vegas, UNITED STATES, 07 2012. [Online]. Available: http://www.eurecom.fr/publication/3788

[14] M. R. Manesh and N. Kaabouch, "Cyber attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions," *Computers Security*, vol. 85, 05 2019.

[15] J. Tang, "Causal models for analysis of tcas-induced collisions," 2015.

[16] G. Natarajan, "Ground control stations for unmanned air vehicles," vol. 51, pp. 229–237, 07 2001.

[17] N. Rodday, R. de O. Schmidt, and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles," 04 2016.

[18] T. E. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps," 2012.

[19] M. Verup and M. Olin, "Security models and exploitations in theory and practice for unmanned aerial vehicles," Ph.D. dissertation, Master's thesis, Technical University of Denmark, 2016.

[20] C. Gudla, M. Rana, and A. Sung, "Defense techniques against cyber attacks on unmanned aerial vehicles," 10 2018.

[21] D. M. Marshall, R. K. Barnhart, S. B. Hottman, E. Shappee, and M. T. Most, *Introduction to unmanned aircraft systems*. Crc Press, 2016.

[22] Y. Zhi, Z. Fu, S. Xingming, and J. Yu, "Security and privacy issues of uav: A survey," *Mobile Networks and Applications*, 01 2019.

[23] E. Deligne, "Ardrone corruption," *Journal in Computer Virology*, vol. 8, 05 2012.

[24] A. Kerns, D. Shepard, J. Bhatti, and T. Humphreys, "Unmanned aircraft capture and control via gps spoofing," *Journal of Field Robotics*, vol. 31, 07 2014.

[25] N. Mohammad, "A multi-tiered defense model for the security analysis of critical facilities in smart cities," *IEEE Access*, vol. 7, pp. 152 585–152 598, 2019.