Review of Computer Engineering Research
2024 Vol. 11, No. 1, pp. 45-57
ISSN(e): 2410-9142
ISSN(p): 2412-4281
DOI: 10.18488/76.v11i1.3636
© 2024 Conscientia Beam. All Rights Reserved.

Cyber attacks on UAV networks: A comprehensive survey

Ashish Mahalle[1+]
Sarika Khandelwal[2]
Abhishek Dhore[3]
Vishwajit Barbudhe[4]
Vivek Waghmare[5]

[1]*Department of Computer Science and Engineering, GHRCE, Nagpur, India.*
Email: mahalle.ashish04@gmail.com
[2]*Department of Computer Science and Engineering, G H Raisoni College of Engineering, Nagpur, India.*
Email: sarikakhandelwal@gmail.com
[3]*Department of CSE, MITSOC, MIT ADT University, Pune, India.*
Email: abhishekdhore811@gmail.com
[4]*Department of Artificial Intelligence and Data Science, Sandip Institute of Technology and Research Centre, Nashik, India.*
Email: vishwajit.barbudhe@sitrc.org
[5]*Department of Computer Science & Engineering, Walchand College of Engineering, Sangli, India.*
Email: dr.vnwaghmare@gmail.com

(+ Corresponding author)

Article History
Received: 14 June 2023
Revised: 18 October 2023
Accepted: 5 January 2024
Published: 9 February 2024

Keywords
Cyber-attacks
Security
Threats
UAV networks
Vulnerabilities
Countermeasures.

ABSTRACT

New technologies are constantly emerging in the modern world and changing the way we live our everyday lives. Although technology has many useful applications, there are various ways it can potentially be abused. Unmanned aerial vehicles (UAVs) are one of the most rapidly developing technologies, with potentially far-reaching consequences. A new focus on UAV applications has fueled rising concerns with regards to security, specifically around networked UAVs. UAVs may be managed from a remote place with relative ease. Essential operations involving the use of military tactics and weapons involve employing them in a variety of situations, such as reconnaissance, surveillance, and offensive, defensive, and civilian capacities. Message insertion, message manipulation, jamming, and GPS spoofing are the most commonly used cyber-attacks against these systems. Ensuring the security of electronics and communications in systems that employ several UAVs is of utmost importance to guarantee their safety and dependability in military and civilian activities. Many technological methods have been developed over the past decade for securing UAVs from cyber-attacks. This paper attempts to summaries the problems that can arise with unmanned aerial vehicles (UAVs), cyber-attacks, and the countermeasures used to protect against them. This is the first paper that details all of the past cyber-attacks on unmanned aerial vehicles (UAVs).

Contribution/Originality: We highlight the various security flaws, attack vectors, and attack types. We provide a fresh classification system for cyber threats. Countermeasures for different cyber-attacks are presented with up-to-date analysis.

1. INTRODUCTION

In today's society, new technologies are continually developing and changing the way we do things. Although there are a lot of useful uses for technology, there are also a lot of ways to misuse it. Unmanned aerial vehicles, or UAVs, are also adopting similar practices. UAV usage is growing in popularity for both personal and business

© 2024 Conscientia Beam. All Rights Reserved.

applications. Guided surveillance [1], weather monitoring [2], unmanned attacks [3], covert intrusions [4], enemy reconnaissance [5], cargo transport, disaster relief [4], rescue operations [5], search operations [6], tracking operations [1], etc. all benefit from this technology.

A new set of security and safety threats, however, has been unwittingly invited with the wider introduction of UAVs to the civilian market for law enforcement, research, and entertainment. Concerns that remain unanswered pertain to attributing drone actions to their human controllers; protecting against drones that have already been hacked, intercepted, or otherwise compromised; and regaining control of hostile or adversarial drones. The lack of defense against electronic attack, hacking, or hijacking on civilian UAVs makes each of these problems much more challenging and increases the likelihood of their unauthorized use or interception. The likelihood of hijacking or interception increases the risk of abusive and dangerous use by cyber attackers, which further complicates the attribution issue. The ramifications are pertinent to every aspect of UAV operations, from military to civilian to law enforcement to even recreational uses.

Most civilian UAS networks, in contrast to military and federal UAS networks, use non-secure communication protocols, such as the transmission of Global Positioning System (GPS) and Automatic Dependent Surveillance–Broadcast (ADS-B) signals, without encryption or authentication. Because of this, cyber-attacks can easily compromise the confidentiality and security of UAS communications with other network entities over wireless channels. Cybersecurity research on such civilian networks has been limited thus far. In particular, the effects of attacks on airspace and civilian security, as well as the systems that can be attacked within a UAS network, remain unclear. There are hardly any systematic studies that thoroughly examine assaults on the communications of civilian UAS. As a result, in this paper, we provide a much-needed overview and analysis of these kinds of attacks. We classify the attacks by the methods they use. In addition, this paper differs from the aforementioned reviews in that it focuses primarily on discussing the most recent developments in detection and countermeasure methods.

1.1. Contributions

The main contributions of this paper can be summarized as follows:

- We highlight the various security flaws, attack vectors, and attack types.
- We provide a fresh classification system for cyber threats.
- Countermeasures for different cyber-attacks presented

The paper is structured as such to achieve these goals. In Section 2, we classify the various kinds of attacks that can be launched against the network connections between UAVs and other nodes. In Section 3, we present types of cyber-attacks; in Section 4, we cover attacks and countermeasures involving data interception. DE authentication, GPS spoofing, ADS-B attacks, and Denial of service attacks, such as jamming, are described along with possible countermeasures. In Section 6, we present a conclusion and further discussion.

2. BACKGROUND AND OVERVIEW

In the twenty-first century, our society is rapidly revolutionizing the way that we approach interactions. Because of the combination of quickly advancing communication technology and a rising interest in and trust for autonomy, humanity is making a quantum leap ahead in its evolution towards the delegation of difficult tasks to non-human entities. From search and rescue robots to Mars rovers, we've seen this trend of overcoming human limitations by replacing personnel with cyber-physical systems that can perform dangerous, repetitive, physically difficult, or economically unfeasible tasks.

Examples of this revolution include Unmanned Aerial Vehicles (UAVs). There has been a meteoric rise in the use of tactical UAVs for surveillance, transport, and combat operations in military and intelligence theatres since the early 2000s. Meanwhile, small and medium-sized UAVs' manufacturing and operations costs are steadily decreasing, giving rise to a rise in civilian use of UAVs. Cost reductions in these UAVs have also sparked increased

© 2024 Conscientia Beam. All Rights Reserved.

curiosity about using fleets of them to accomplish goals like crop monitoring and border security. However, there are many obstacles standing in the way of this vision, all of which must be overcome before such systems can be used reliably and safely in civilian and military settings. Since UAVs typically operate in inaccessible environments, their onboard cyber-physical components must shoulder the bulk of the command-and-control workload. Recent years have seen a rapid expansion of the literature on this topic [1], in part as a result of major cyber-attacks on UAVs [6]. In order to ensure the protection of unmanned aerial vehicles (UAVs) from potential threats, it is crucial to establish rigorous standards and frameworks. These measures should cover all aspects of UAVs, including their mechanical components, central processing units, and communication networks, to effectively safeguard them against any form of malicious interference.

2.1. UAV System

Varieties of Unmanned Aerial Vehicles (UAVs) with enhanced communication capabilities have advanced rapidly in recent years. Several unmanned aerial vehicle (UAV) systems are needed for other applications, such as wide-area monitoring in risky environments. While single-UAV systems have been in use for decades thanks to the ease of operating and developing a single large UAV, there are a number of benefits to using a fleet of smaller UAVs instead. Each UAV in a single UAV system functions as a standalone node, able to exchange data only with the ground node. That's why the UAV communication system relies solely on UAV-to-infrastructure communication; UAVs can talk to each other via the network. When compared to the benefits offered by a network of UAVs, the capabilities of a single UAV system quickly become inadequate. To begin, the overall cost of a mission is reduced when multiple UAVs are used. Additionally, UAVs working together can boost system efficiency. Additionally, in a multi-UAV system, the operation can continue with the other UAVs if one UAV fails during a mission, and missions are typically completed faster and more efficiently with multi-UAV systems.

Multiple UAVs can be utilized to complete missions successfully and efficiently due to their capabilities, flight times, and payload limitations [7]. Communication and networking are necessary for facilitating collaboration, coordinating many UAVs, and realizing autonomous UAV networks. As an alternative, UAVs can connect to one another via ad hoc networks to exchange data. Even though only a portion of the UAVs in an ad hoc UAV network are physically connected to the ground station, the entire network functions as a single unit. UAVs can communicate with the ground control station and one another using this network. Unmanned aerial vehicle (UAV) ad hoc networks can be compared to a mix of mobile ad hoc networks (MANETs) and vehicular ad hoc networks (VANETs). UAV networks, on the other hand, have several special characteristics not present in conventional Ad hoc networks. Nodes in UAV networks are extremely mobile. UAVs are airborne, in contrast to the ground-based or human-based nodes in a VANET or MANET. Due to the rapid mobility of UAVs, the network topology is more dynamic than in a MANET or VANET. Furthermore, creating peer-to-peer links is the main goal of both VANET and MANET. Peer-to-peer connections are necessary in UAV networks as well, so that the UAVs can communicate and cooperate. The majority of the time, a UAV's main job is to acquire data and send it to a Ground Control Stations (GCS). Therefore, it is essential to ensure UAV-to-UAV (U2U) and UAV-to-Infrastructure (U2I) communication. Therefore, peer-to-peer communication and converging cast traffic must both be made available on UAV networks at the same time. Additionally, distances between UAVs are substantially wider than gaps between MANET and VANET nodes. In order to create reliable communication linkages between the UAVs, the communication range of the UAVs must be increased. Figure 1 presents the overview of unmanned aircraft systems.

© 2024 Conscientia Beam. All Rights Reserved.

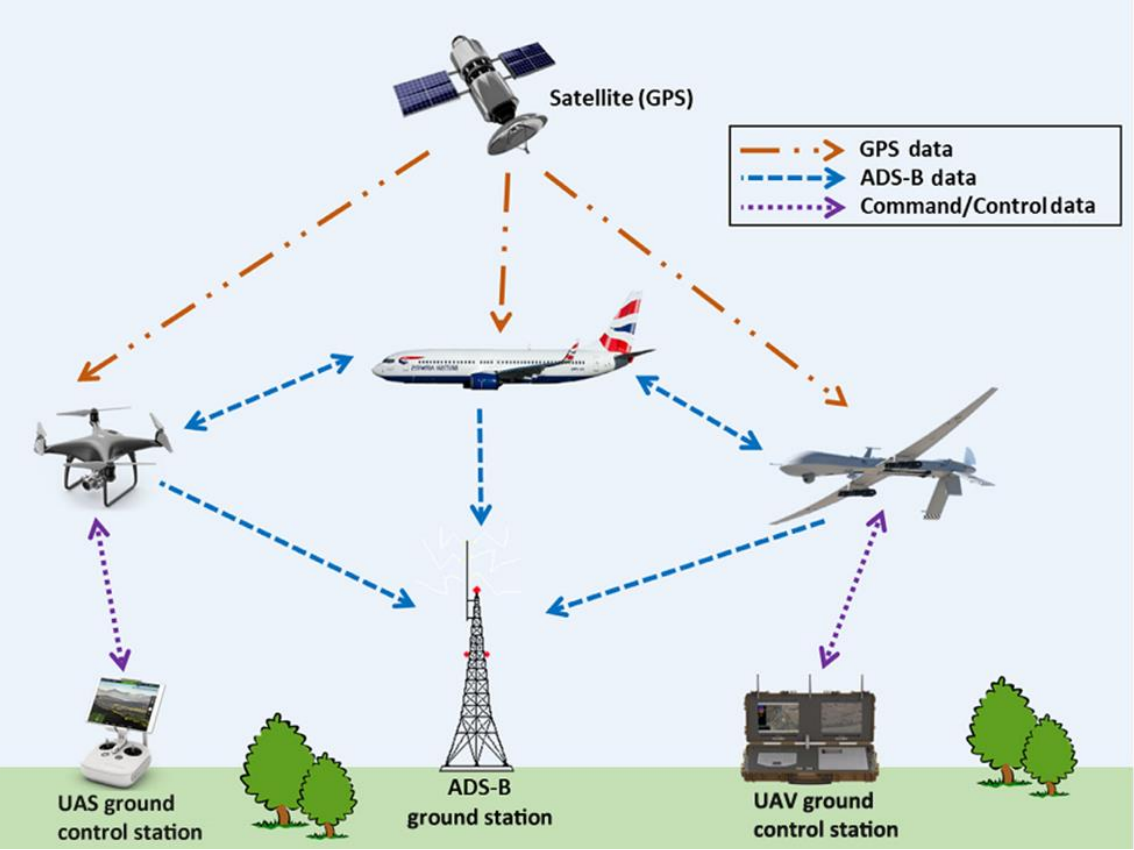

Figure 1. Oversight of an unmanned aircraft system.

2.2. Cyber Attacks

A cyberattack on a UAV can be carried out in a number of different ways. Theft of passwords is the first concern, and this can be accomplished in several ways. Different kinds of dictionary attacks use different combinations of words, digits, and symbols to guess a password. Brute-force attacks on short passwords are possible if every possible combination is tried [8]. In order to determine if a word guess from a byte is correct, statistical methods, like Air cracking, use statistical data. The attackers will gather the necessary information from "leaks" in the configuration vectors of the target entity, then look for the basic keys in order to rely solely on brute force [9].

Second, a man in the middle (MITM) attack occurs when a third party listens in on a conversation between two parties and has access to (and can modify) private information without the knowledge of either party involved. There are a wide variety of man-in-the-middle (MITM) attacks [8], including covert eavesdropping and tampering with URLs, third, Denial-of-Service (DoS). It grants the intruder complete control over the compromised system or network. The attack consumes application resources like processing time and memory by sending a barrage of requests to the system. A de-authentication application could be used in an attack on a UAV to quickly sever all lines of communication with the aircraft [10, 11]. The fourth issue is GPS spoofing and jamming. When an unmanned aerial vehicle (UAV) is unable to receive accurate GPS coordinates, it can be exploited in the same covert way that GPS jamming and spoofing are. The attacker generates a GPS-jamming signal, which disrupts legitimate GPS signals and causes the GPS receiver in the UAV to fail. The attacker sends a false message that may alter the UAV's direction via GPS spoofing, a similar but more sophisticated attack [12].

Not a hacking system at all, but rather a cyberattack tool employing a technique known as reverse engineering. To reverse engineer a device and figure out how to change or steal its data, one must disassemble or examine it closely. Using reverse engineering techniques [13] derived from a higher-level programming language, the original binary programme is recreated.

© 2024 Conscientia Beam. All Rights Reserved.

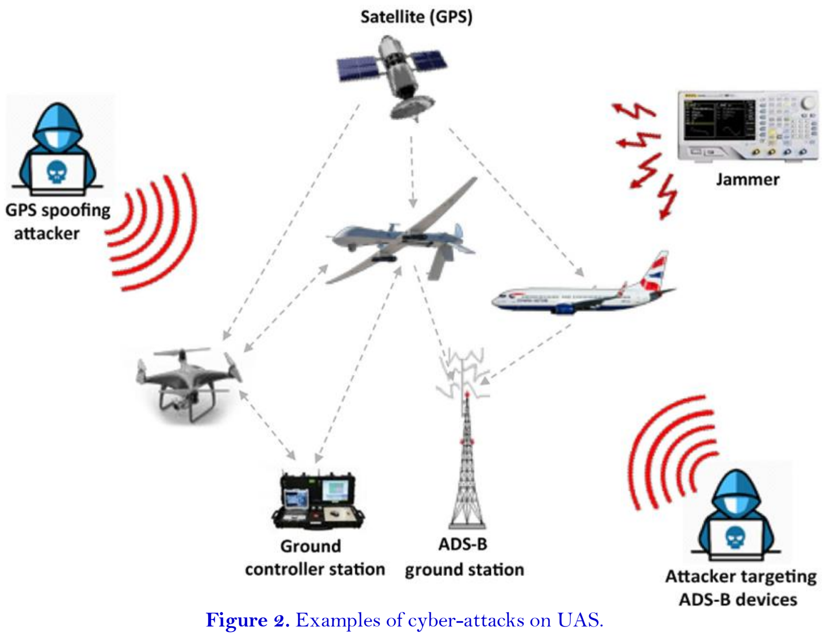

Figure 2. Examples of cyber-attacks on UAS.

3. TYPE OF CYBER ATTACKS

The type of attack that can be carried out on a UAV is determined by the specific vulnerability that is being exploited. The UAV transceiver, the communication channel, and the control center are the three primary points of attack in a UAV system, and any one of these could be compromised at any given time. There are two broad types of attacks that can be carried out. Figure 2 presents an example of cyber-attacks on UAS.

3.1. Active Attacks

The Ethical Hacking framework includes penetration testing for precisely this kind of attack. The primary goal of such attacks is to cause a service disruption or data breach without worrying about the impact on the initial transmission. These kinds of assaults happen in the here-and-now, or at time t = 0, and they wrap up as soon as the necessary information or goal has been attained.

3.2. Passive Attacks

Network monitoring, port listening, and packet sniffing are common methods of attack in this category. Such attacks typically involve the attacker remaining on the network unnoticed by the user, allowing the original transmission to continue unhindered. An attacker can obtain sensitive data, such as encryption keys or digital certificate algorithms, by intercepting and analyzing specific packets.

4. CYBER ATTACKS ON UAVS

UAVs are vulnerable to hacking and could be used as weapons. As a result, UAV surveillance is an important issue that needs fixing. Some examples of UAV attacks are as follows: I. In 2009, it was discovered that a terrorist organization had used SkyGrabber (free software for capturing satellite videos) to record an unencrypted UAV video feed [14]. In 2011, Iran's Cyber Unit successfully took control of US Army drones and gathered classified data from them. Weak security measures on the drones also allowed this to happen [15]. Third, a Chinese drone was compromised in 2017. The United States' Cyber Security Response Team did this, and they discovered a wide variety of flaws in the aircraft. On August 5, terrorist organizations used two drones to attack the President of Venezuela. These unmanned aerial vehicles carried explosives. The primary cause for alarm is the drones' proximity to the President. Figure 3 shows the classification of cyber-attacks on UAVs.

© 2024 Conscientia Beam. All Rights Reserved.

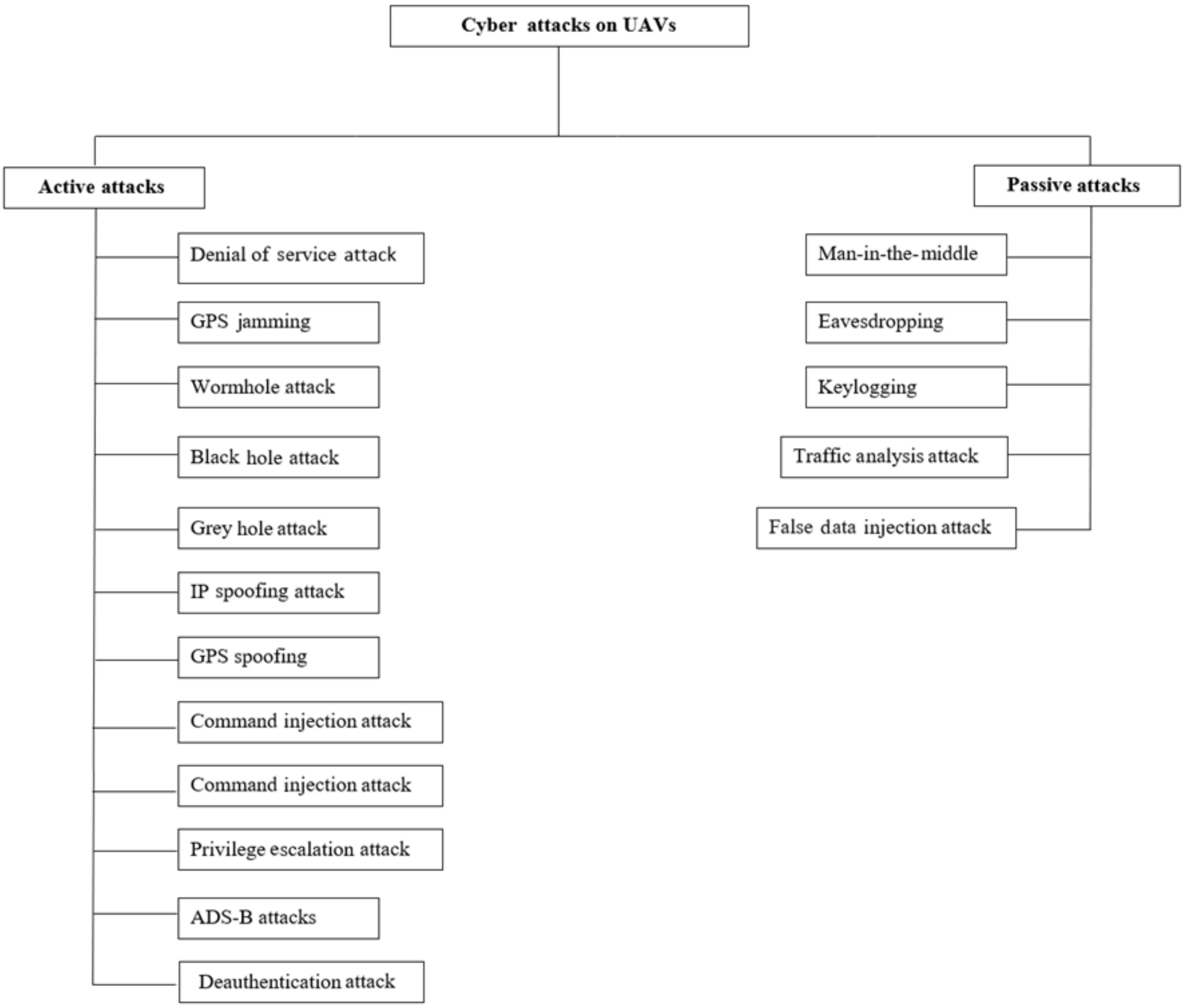

Figure 3. Classification of cyber-attacks on UAVs.

4.1. Denial of Service Attack

This is an aggressive assault method. The attacker sends a barrage of packets to the target in order to overwhelm its defenses. These packets represent multiple requests made to the target, which causes the target to fail if it is unable to keep up. These datagrams may be Transmission Control Protocol sides-synchronize (TCP SYN) packets or standard ping datagrams. There is also a more sophisticated form of this attack called a Distributed Denial of Service attack (DDoS). In this attack, the adversary makes use of multiple sources under his control to flood the target with packets. Zombies are the name given to these types of information providers. The Zombie Net, a group of zombies, carried out a planned attack.

In Figure 3, DDoS is defined. In the event of a Distributed Denial of Service attack, the server will be unable to respond to requests from its actual users. As a result, the UAV and the control center might lose contact if a DDoS attack were launched against the UAV transceiver or the control center via the UAV communication channel. This can lead to the loss of the UAV and the potential corruption or deletion of sensitive data packets [16].

4.2. GPS Jamming

A well-known and well-respected attack that has the potential to completely disable GPS navigation and all other forms of communication. In order to disable all communication receivers in the area, jamming involves sending out both high- and low-power noise signals. Although several anti-jamming techniques have been proposed, neither narrow band nor wide band interference can be completely eliminated at this time. The use of GPS Jamming is discussed in this section.

© 2024 Conscientia Beam. All Rights Reserved.

4.3. Wormhole Attack

Attacks by WH on UAVs pose a serious hazard. In WH assaults, an adversarial node intercepts data packets at a certain UAV position before tunneling them to an additional adversarial node at a different location, which then manages the distribution of the packets to its neighboring nodes. A strong transmission, an encrypted packet, or an out-of-band channel can all be used to create this tunnel. Tunneled packets use these techniques to reach their destination significantly faster or with fewer hops than conventional packets, which are sent via a multi-hop path. This technique gives the appearance that the tunnel's two termini are near one another [17]. In order to achieve this, the hostile nodes are positioned as dummy nodes halfway between the source and destination nodes, giving them the ability to carry out nefarious operations such as packet dropping and modification. Figure 4 exhibits the working of a wormhole attack.

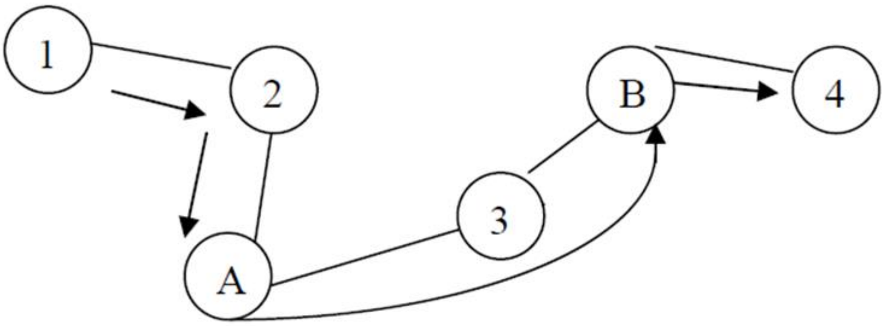

Figure 4. Wormhole attack.

4.4. Black Hole Attack

A BH node will send back a phony Route Reply (RREP) in response to a Route Request (RREQ) packet it receives, even if the routing table does not include the claimed shorter and legitimate route to the destination. A path is constructed through the malicious intermediate node after the bogus RREP packet reaches the source node, causing the source node to disregard any legitimate RREP signals coming from other intermediate and destination nodes. As a result, the BH node is effective in tricking the source node into sending data traffic to that location. The BH node then chooses not to forward any incoming data packets. The BH node forges a transmission route with a very high number of destination sequences and a very low hop count in order to increase the likelihood of acceptance at the source node. A BH attack can be initiated from the source node, poisoning the routing tables of both the intermediate and final hops, by fabricating field-source sequence numbers in RREQ packets and hop counts [18]. Figure 5 exhibits the workings of a black hole attack.

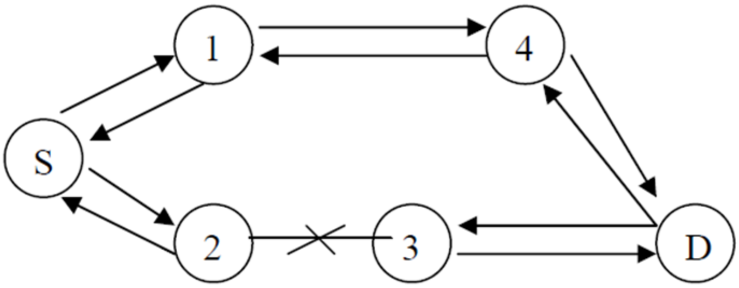

Figure 5. Blackhole attack.

4.5. Grey Hole Attack

By broadcasting erroneous routing data, malicious nodes disrupt legitimate network traffic in grey hole attacks. The grey hole attack is an extension of the BH attack because the malicious nodes' origins are unknown. A node can

© 2024 Conscientia Beam. All Rights Reserved.

perform normal and malicious roles. This attack reduces throughput and packet delivery ratios by interfering with the route discovery process [19].

4.6. IP Spoofing Attack

That's an aggressive tactic, too. Internet Protocol (IP) spoofing is used in this attack to make it appear as though the requests are coming from a trusted source. To mask one's IP address means to replace it with a fictitious one. This attack can be used to compromise a UAV system if its firewall is set up to permit connections only from a limited set of static IP addresses.

4.7. FID Attack

When an adversary sends out a bogus GPS signal to divert a drone's intended flight path, they are committing a Fake information dissemination (FID) attack. In order to reduce the accuracy of the drone's estimated location, an attacker can broadcast interference between the drone and the pilot. Several methods have been proposed to counter a FID attack in wireless communications research [20] to disseminate information; however, such regulations are largely ineffective in preventing data from being intercepted by unauthorized parties.

4.8. Command Injection Attack

Another form of active assault. A malicious piece of code is inserted into the HTML-based application during this attack. The injected code is malicious and launches a script that can facilitate data manipulation and access bypass. The entire system can be compromised and taken under external control if a command injection vulnerability exists in the UAV control center or the UAV Drone.

4.9. Privilege Escalation Attack

Another form of active assault. In this type of attack, the user impersonates a higher-level user in order to carry out actions outside of his or her normal scope of authority. This happens as a result of administrators frequently using weak passwords or ones that come with the system.

4.10. ADS-B Attacks

U.S. law prohibits the use of aircraft not equipped with automatic dependent surveillance-broadcast (ADS-B) systems, which is a common form of attack. By continuously broadcasting the identity, position, and velocity of the aircraft carrying this system to nearby aircraft and ground stations via global navigation satellite systems, ADS-B creates an accurate air picture. In order to comply with FAA regulations, ADS-B messages must be sent via unencrypted wireless datalinks. Recent studies, however, have shown that ADS-B messages can be easily compromised with readily available, low-cost hardware and software. Some network entities can have their communications disrupted or otherwise hampered if an attacker is able to intercept and alter their ADS-B messages using such devices [21].

4.11. Message Injection

Because there is no authentication in ADS- B networks, attackers can compromise air traffic communications by inserting fake messages that look like they came from a legitimate source. Both ground-based (via "Ghost Injection") and airborne (via "Aircraft Injection") targets are vulnerable to "message injection" attacks. To execute a Ground Station Target Ghost attack, for instance, an adversary broadcasts sham ADS-B messages that mimic the characteristics of real ones (velocity, position, identification number, etc.). Both pilots and air traffic controllers could see dummy planes on their screens if this happened [22].

© 2024 Conscientia Beam. All Rights Reserved.

4.12. Message Deletion

In this scenario, the attacker deletes some messages sent by a legitimate aircraft to avoid detection by other aircraft. Both constructive interference and destructive interference can be used to delete messages. By using constructive interference, an attacker can introduce bit errors into an ADS-B transmission, leading to the message's dismissal by the receiver as corrupted. By generating a synchronized signal at the right time that is the inverse of the ADS-B signal, an attacker can destroy the ADS-B signal within the transmission, either completely or in part. Both scenarios result in the unmanned aerial system (UAS) with the deleted messages being undetectable by other aircraft, increasing the potential for air traffic disruption and the risk of aircraft collisions.

4.13. Message Modification

An attack that alters the messages of trustworthy nodes in the network is the most challenging to launch. The three techniques for carrying out a message modification attack are overshadowing, bit flipping, and combined message deletion and injection. By sending out powerful ADS-B signals, overshadowing aims to substitute for or change legal communications. By superimposing a fake signal, an attacker tries to convert any number of 0s to 1s or 1s to 0s when performing a bit flip. When message deletion and message injection assaults are combined, it is feasible for a freshly updated message to show up on the network. However, the first two techniques are riskier since they permit a genuine communication to be changed in the midst for recipients to still accept it as genuine.

4.14. Deauthentication Attack

Communication between a UAS and its ground control station must first be authenticated and then initiated using management packets. The control stream between the UAS and its controller is vulnerable to a deauthentication attack if management packets are not encrypted. This attack involves sending deauthentication frames to both nodes in an effort to break their connection to one another. After that, the attacker can impersonate a safe ground controller and take over the UAV with a replay attack or message injection. Encryption is the best defense against this kind of attack, but it can be broken by a brute force attack if the encryption key is poorly chosen.

4.15. Man-in-the-Middle Attack

This assault may take the form of a passive or active strategy. The attacker spies on the communication between the sender and the recipient, then modifies or alters the data. This attack could seriously jeopardize the integrity of the data. The most crucial aspect of the Confidentiality, integrity, and Availability (CIA) triad is data integrity, which must be protected at all costs. By eavesdropping on the exchange of keys during connection establishment, an attacker can launch this type of attack. IP spoofing, Address Resolution Protocol (ARP) poisoning, Domain Name System (DNS) poisoning, ARP spoofing, DNS spoofing, Secure Sockets Layer (SSL) hijacking, Hyper Text Transfer Protocol Secure (HTTPS) spoofing, and many other techniques can also be used to achieve this attack. See how traffic is rerouted from sender to attacker and back to the receiver in this illustration of a basic Man-in-the-Middle attack. (Figures 6 and 7). The key idea underlying this attack is the establishment of multiple TCP handshakes [23]. A man-in-the-middle (MITM) attack on a UAV's communication channel can compromise surveillance, session hijacking, unauthorized activities, unauthorized attacks (in the case of military UAVs), incorrect data, and the alteration of the UAV's projectile, among other things. Figures 6 and 7 present the workings of the man-in-the-middle (MITM) attack.

© 2024 Conscientia Beam. All Rights Reserved.

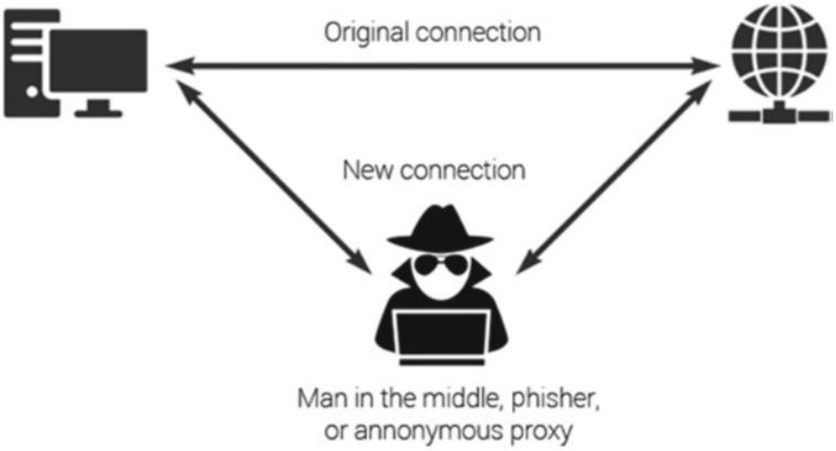

Figure 6. Man-in-the-Middle attack

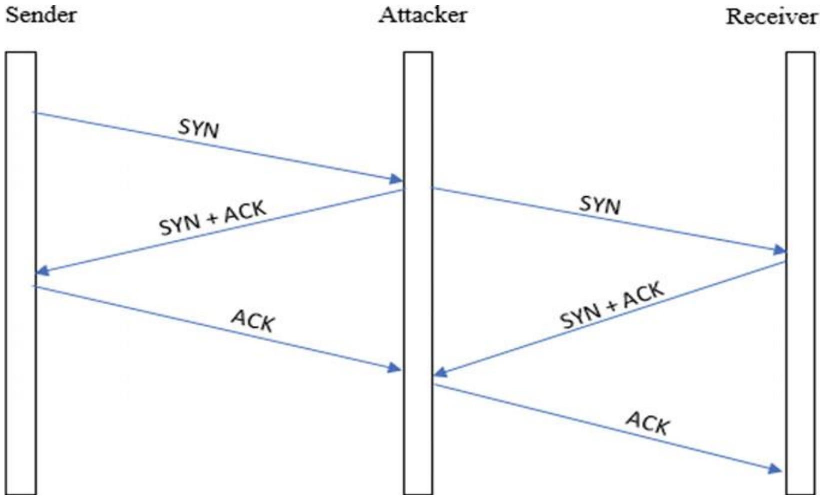

Figure 7. Multiple TCP handshake in MITM attack.

4.16. Keylogging

The original purpose of keyloggers was to spy on typed text. For example, they are used to monitor children's online behaviour, to ensure that sensitive data is not being typed by employees, and to keep tabs on criminals by law enforcement. Keyboard sniffers, tracking software, computer activity monitoring software, snoopware, and keystroke monitoring systems are all examples of this type of software available today. Recently, keyloggers have become a major issue because they are often undetectable by antivirus software. Screen activity, file manipulation, and Internet use are just some of the things they can monitor on a computer. In contrast to viruses, worms, and Trojans, keyloggers coexist with legitimate software and remain on the system for as long as the hacker requires access to the stolen data. Both classified and unclassified information was compromised in 2011 when malicious keylogging software was installed on the Predator and Reaper ground control stations via a removable hard drive.

4.17. Eavesdropping

Eavesdropping, or secretly listening in on a network's communications, is one of the simplest security threats there is. If there is insufficient or nonexistent encryption in the UAS network, eavesdropping attackers will be able to intercept communications between aircraft and other network nodes. Since the beginning of ADS-B and GPS development, the possibility of eavesdropping has been a major concern. Data interception via eavesdropping can be used to launch complex attacks like GPS spoofing and ADS-B message injection, despite the fact that several services, such as tracking commercial aero planes, intercept air- craft data legally. Some nations, including the United Kingdom, have passed legislation punishing accidental listeners.

© 2024 Conscientia Beam. All Rights Reserved.

4.18. Traffic Analysis Attacks

More frequent traffic analysis attacks are possible because robotic systems are still reliant on open wireless communications or communications with basic security measures. One way to do this is to eavesdrop on the communication going on between the robots and their controllers. As a result, this compromises the security of data and robotic systems and may open the door to additional attacks in the future.

4.19. False Data Injection Attacks

Attacks that intercept and modify the payload of a robot's communication in order to plant false information in it are known as false data injection attacks [24]. In order to accomplish this objective, it is necessary to first intercept the current communication between the robots and then manipulate it by introducing fabricated data and information. This manipulation can either lead the robots to diverge from their planned tasks or force them to reply at a slower pace than anticipated.

5. DISCUSSION AND CONCLUSION

UAS/UAV communication security has recently received a lot of interest from academic and industrial researchers. The numerous types of cybercrime that can impair UAS communications were covered in this research. Data interception, data manipulation, and denial of service assaults are the three basic categories of these attacks. We also looked into the suggested defenses against intrusion on UAS networks. Although the need for protecting UAS and UAV data is becoming more widely recognized, not much has been done in this regard. Security issues and several significant impediments are still open for discussion. One of the challenges is the creation of extremely efficient detection methods with a high detection probability and very low false alarm and miss-detection percentages. There are severe problems with detecting technology as it stands today. Numerous difficulties arise since the majority of the suggested solutions involve changing the UAS network infrastructure and communication protocols that are currently in place. Furthermore, the majority of these methods have high false alarm rates rather than high detection rates.

The fact that the detection process doesn't take place in real time further reduces the methods' effectiveness. To get over these limitations, new methods of detection are needed. Similar to how detection approaches are unfeasible, most proposed methods to counteract and neutralize UAS cyber-attacks call for changes to the current communication and infrastructure protocols. Because the FAA requires that ADS-B messages be broadcast as plaintext over unencrypted data links so that they can be freely accessible by every receiver in the network, encryption-based techniques, for instance, are unworkable. As a result, it will be challenging to create countermeasure techniques that can handle a variety of threats while still operating in conjunction with the existing infrastructure and protocols. A UAS, as is widely known, heavily relies on GPS for both operating and navigation. Due to this dependence, navigating a UAV in a location without access to GPS can be quite difficult. If the GPS signal is lost or jammed, the unmanned aerial system (UAS) cannot fulfill its task, could jeopardize people's lives and its operational airspace, and/or could be hijacked. A few ideas based on image/video processing have been put forth for UAS navigation. However, these methods are ineffective since a UAS can only identify its flight route through picture analysis. As a result, better techniques must be created to guarantee the UAS's safe navigation in locations devoid of GPS. Beyond GPS and ADS-B, another concern that hasn't gotten enough attention is the impact of cyberattacks on the various UAS subsystems. Radars, processing units, autopilot, drive units, and power subsystems are examples of UAV sensors that fit within this category. These parts are attackable, which could lead to the UAS's operation failing. The battery will run out more quickly, for instance, if an attack forces the UAS's processing units to do additional processing cycles. Data from sensors that has been altered may also cause issues, resulting in crashes or a change in the flight path. It is crucial to carefully investigate potential threats and how they can affect these subsystems in order to design detection and mitigation strategies to deal with them.

Communication within UAS networks is more challenging than communication inside other networks due to the greater complexity, disparity in systems, dynamic nature of networks, and diversity of data flows (commands/video/audio/image). UAS networks have distinctive qualities that call for a different strategy for security than traditional networks. Therefore, it is ineffective to safeguard UAS networks using the same techniques as other wireless systems. These challenges point to new directions for research, such as the development of security solutions that take into account the unique security requirements of UAS. Another issue is that the majority of current UAS networks fall within the category of self-organizing networks.

Everything about these networks, including setup, optimization, management, backup, and restore, is automated. These networks are susceptible to assaults, malevolent control, and unauthorized access since they usually lack basic security safeguards. This allows resources to be redirected towards developing standardized security measures for these kinds of networks. More research may be done on the effectiveness of multi-layer security frameworks, which employ a variety of methods to identify and stop assaults on UAS networks. The UAS may transport and broadcast private audio, video, and image data in addition to GPS, ADS-B, and command and control information. The former group of data may be the target of attacks on the UAS network's security. The latter group, however, is susceptible to assaults that seek to identify particular people and divulge their personal information. This work has already covered security vulnerabilities to UAS network operations and techniques for identifying and mitigating them. However, additional study is required on privacy issues.

Funding: This study received no specific financial support.
Institutional Review Board Statement: Not applicable.
Transparency: The authors state that the manuscript is honest, truthful, and transparent, that no key aspects of the investigation have been omitted, and that any differences from the study as planned have been clarified. This study followed all writing ethics.
Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

REFERENCES

[1] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber-attack vulnerabilities analysis for unmanned aerial vehicles," *In: AIAA Infotech@Aerospace*, 2012. https://doi.org/10.2514/6.2012-2438

[2] S. G. Gupta, D. M. Ghonge, and P. M. Jawandhiya, "Review of unmanned aircraft system," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 2, no. 4, pp. 1646-1658, 2013.

[3] G. Udeanu, A. Dobrescu, and M. Oltean, "Unmanned aerial vehicle in military operations," *Scientific Research & Education in the Air Force*, vol. 18, no. 1, pp. 199-206, 2016.

[4] W. Debusk, "Unmanned aerial vehicle systems for disaster relief: Tornado alley," *In AIAA Infotech@ Aerospace 2010*, p. 3506, 2010.

[5] S. Waharte and N. Trigoni, "Supporting search and rescue operations with UAVs," presented at the In: 2010 International Conference on Emerging Security Technologies, 2010.

[6] A. Javaid, W. Sun, V. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," presented at the In: 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, 2012.

[7] G. Chmaj and H. Selvaraj, "Distributed processing applications for UAV/drones: A survey," in *In Progress in Systems Engineering: Proceedings of the Twenty-Third International Conference on Systems Engineering, Springer International Publishing*, 2015, pp. 449-454.

[8] C. Rani, H. Modares, R. Sriram, D. Mikulski, and F. L. Lewis, "Security of unmanned aerial vehicle systems against cyber-physical attacks," *The Journal of Defense Modeling and Simulation*, vol. 13, no. 3, pp. 331-342, 2016. https://doi.org/10.1177/1548512915617252

[9] C. Devine and T. Otreppe, "Aircrack-ng," Retrieved: https://www.aircrack-ng.org/. 2018.

© 2024 Conscientia Beam. All Rights Reserved.

[10] C. Gudla, M. Rana, and A. Sung, "Defense techniques against cyber attacks on unmanned aerial vehicles," in *In Proceedings of the International Conference on Embedded Systems, Cyber-physical Systems, and Applications (ESCS)*, 2018, pp. 110–116.

[11] O. Westerlund and R. Asif, "Drone hacking with raspberry-Pi 3 and Wi-Fi Pineapple: Security and privacy threats for the internet-of-things," presented at the In 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS). IEEE, 2019.

[12] N. Shashok, "Analysis of vulnerabilities in modern unmanned aircraft systems," *Tuft University*, pp. 1-10, 2017.

[13] K. Thayer, "How does reverse engineering work?," Retrieved: https://insights.globalspec.com/article/7367/how-does-reverse-engineering-work. 2017

[14] D. He, S. Chan, and M. Guizani, "Communication security of unmanned aerial vehicles," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 134-139, 2016.

[15] S. Dahiya and M. Garg, "Unmanned aerial vehicles: Vulnerability to cyber attacks," in *Proceedings of UASG 2019, Springer International Publishing*, 2019.

[16] DoS, "DoS attacks," Retrieved: https://www.thewindowsclub.com/ddos-distributed-denial-service-attacks. 2023.

[17] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Networks*, vol. 84, pp. 124-147, 2019. https://doi.org/10.1016/j.adhoc.2018.10.002

[18] I. García-Magariño, R. Lacuesta, M. Rajarajan, and J. Lloret, "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain," *Ad Hoc Networks*, vol. 86, pp. 72-82, 2019. https://doi.org/10.1016/j.adhoc.2018.11.010

[19] S. Gurung and S. Chauhan, "A novel approach for mitigating gray hole attack in MANET," *Wireless Networks*, vol. 24, no. 2, pp. 565-579, 2018. https://doi.org/10.1007/s11276-016-1353-5

[20] S. N. Panda, "GPS hash table based location identifier algorithm for security and integrity against vampire attacks," in *In Cyber Security: Proceedings of CSI 2015, Springer, Singapore*, 2018, pp. 81-89.

[21] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78-87, 2011. https://doi.org/10.1016/j.ijcip.2011.06.001

[22] M. M. Riahi and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system," *International Journal of Critical Infrastructure Protection*, vol. 19, pp. 16-31, 2017. https://doi.org/10.1016/j.ijcip.2017.10.002

[23] A. Joseph, "Apparent attack in Venezuela highlights risk of drone strikes," Retrieved: https://www.reuters.com/article/us-venezuela-politics-drones/apparent-attack-in-ve-nezuelahighlights-risk-of-drone-strikes-idUSKBN1KQ0MG. [Accessed 2019/03/01], 2018.

[24] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," presented at the In: 2010 49th IEEE Conference on Decision and Control (CDC), IEEE, 2010.

Views and opinions expressed in this article are the views and opinions of the author(s), Review of Computer Engineering Research shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.

© 2024 Conscientia Beam. All Rights Reserved.