IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 2, Ser. 5 (Mar. – Apr. 2025), PP 25-34
www.iosrjournals.org

A Comprehensive Review Of Cyber Security In Unmanned Aerial Vehicles (UAVS)

Reecha Sharma, Lakshmi Shankar, Munaem Bin Salim Seam, Sushmoy Dey
Department Of Electronics And Communication Engineering, Punjabi University Patiala, India
Department Of Mechanical Engineering, Punjabi University Patiala, India

Abstract:
Various industries, such as agriculture, surveillance, transportation, and environmental monitoring, are seeing substantial changes due to the swift advancement of unmanned aerial vehicles (UAVs) and unman. The application of these technologies significantly affects sectors reliant on unmanned systems by offering transformative autonomy and operational efficiency.
The increasing integration of unmanned aerial vehicles (UAVs) into critical operations presents substantial cybersecurity challenges that must be resolved to ensure the secure and reliable functioning of these vehicles.
This paper examines the cybersecurity risks associated with unmanned aerial vehicle (UAV) systems, focusing specifically on vulnerabilities in hardware, software, and communication channels.
This study examines various cyberattacks, including ssurveillance attack assaults, Denial of Service (DoS) attacks, and Command Injection attacks, as well as their consequences for the integrity and confidentiality of unmanned aerial vehicle (UAV) operations.
This study evaluates various mitigation options, including distributed real-time systems, multi-agent system designs, redundancy, and encryption methods.
The research highlights the efficacy of these strategies in safeguarding unmanned aerial vehicle (UAV) systems against potential cyber threats.
Distributed systems and redundancy are significant since they ensure uninterrupted availability and mitigate the effects of hardware or software problems that may arise during cyberattacks. The capability of multi-agent systems to provide decentralized control markedly enhances the system's ability to react in real time to possible threats.
Moreover, the implementation of encryption and authentication methods enhances data security and access control, thereby safeguarding conversations against compromise.
The study underscores the importance of integrating cybersecurity protections from the initial design phase of unmanned aerial vehicle (UAV) systems to ensure their resilience and reliability.
The study underscores the essential function of these methods in mitigating risks and facilitating the successful implementation of autonomous unmanned systems across many operational contexts by evaluating the efficacy of these strategies.

Keywords: *Unmanned Aerial Vehicles (UAVs), Unmanned Surface Vehicles (USVs), UAV System Design, Cyberattacks, Security Vulnerabilities, Encryption Technique, Mitigation Strategies.*

Date of Submission: 13-04-2025 Date of Acceptance: 23-04-2025

I. Introduction:

The concept of fully autonomous robots has been around for a while. Trials of unmanned aircraft occurred during World War I, and in 1925, a radio-controlled automobile was displayed in New York City.[1] The goal of fully autonomous and unmanned vehicles has made great strides in recent years, thanks to advancements in robotics and artificial intelligence. It is especially thrilling to see developments in two main types of autonomous and unmanned vehicles: driverless cars and unmanned aerial systems (UAS).[2]

Unmanned Aerial Vehicles (UAVs) and Unmanned Surface Vehicles (USVs) are emerging as transformative technologies across various sectors, offering new dimensions of autonomy, adaptability, and operational efficiency. UAVs, or drones, have become essential in sectors such as agriculture, surveillance, transportation, and environmental monitoring due to their ability to explore hard-to-reach areas and collect real-time data with minimal human intervention. [3] Similarly, unmanned surface vehicles (USVs), which operate on the water's surface, are progressively utilized in coastal and marine activities, encompassing military applications, environmental monitoring, and oceanographic study. [4] The integration of UAVs with USVs facilitates multi-domain operations, hence enhancing operational scope and enabling the expedited execution of complex missions compared to previous eras. [5]

However, the integration of these unmanned systems into critical operations has introduced numerous cybersecurity challenges. Primarily reliant on wireless communication, autonomous decision-making algorithms, and cloud-based data storage—all susceptible to cyberattacks—UAVs and USVs are System integrity may be jeopardized by threats such as GPS spoofing, data interception, command injection, and denial-of-service (DoS) attacks, hence threatening missions and potentially public safety. The development and implementation of robust cybersecurity frameworks are essential not just from a technical perspective but also as a critical element for the secure and sustainable operation of increasingly complex and autonomous systems in both civilian and military domains.

II. Unmanned Aerial Vehicles:

Unmanned Aerial Vehicles have garnered significant interest recently. Generally, UAVs are unmanned aerial vehicles operated without a human operator. Sensors, microprocessors, and various electrical equipment enable autonomous operation. [6] illustrates the communication of UAVs through connections with satellites, ground control systems (GCS), smartphones, and computers, so exemplifying a conventional UAV system architecture. The remote control and operation of a UAV is executed by a human operator. When human participation is difficult or hazardous, UAVs can execute autonomous operations.[7] Currently, UAVs serve as a highly effective instrument for logistics. The civilian market for UAVs exhibits a distinct growth. The primary applications of UAVs encompass remote missions such as search and rescue, catastrophe monitoring, environmental surveillance, and the transportation of airmail, medical supplies, and freight. Despite increased attention, human-operated remote controllers predominantly govern UAV operations. The characteristics, designs, and mechanics of UAVs are often determined by their application, speed, weight, and operation. Although there is increased focus, UAVs are often operated under human-assisted remote control. The application, speed, weight, and operation typically dictate the characteristics, designs, and mechanisms of UAVs. [8]

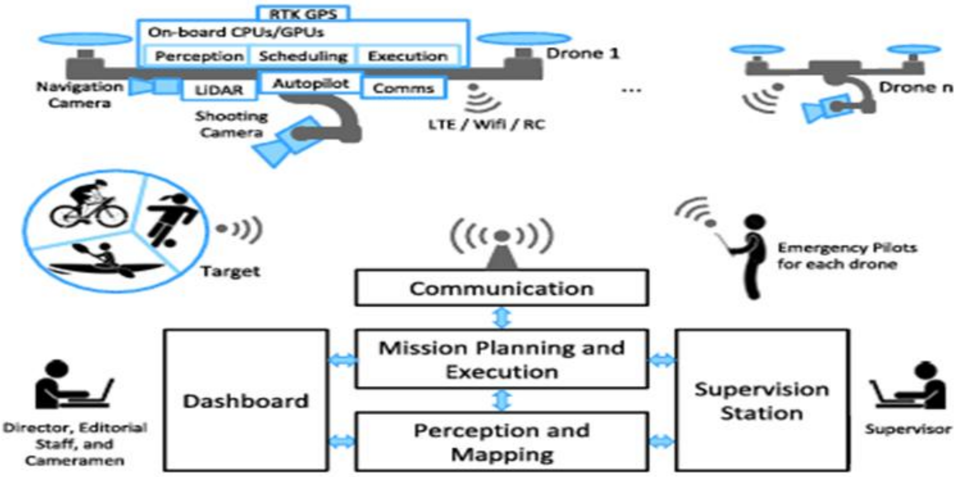

Figure: 1 UAV architecture [9]

III. Unmanned Surface Vessels:

Unmanned Surface Vessels (USVs) are mostly navigated by automated onboard decision-making systems, while remaining under the oversight of a remote operator stationed onshore. They are also referred to as autonomous surface craft (ASC). They eliminate the operators from the platform and permit novel operational methods, as the phrase

implies. Unmanned Surface Vessels (USVs) have advanced in capability due to the increased compactness, efficiency, and affordability of global positioning systems (GPS). Affordable, long-range, high-bandwidth wireless data systems are also crucial for the rapid proliferation of USVs across various applications. Currently, academic laboratories, commercial enterprises, and governmental entities have developed and exhibited unmanned surface vehicles (USVs). The displayed projects encompass scientific endeavors, hydrographic surveying, defense applications, and general robotics research.[10] Scientific research is another domain where surface and subsurface vehicles are utilized. Underwater vehicles that can navigate without human intervention are employed in the Catlin Sea View Survey Project to explore the mesopelagic zone, at depths ranging from 30 to 100 meters. In the absence of human physiology, AUVs can autonomously explore coral reefs for hours, collecting samples, delivering gear to divers, or conducting reconnaissance.[11,12] They utilize depth, temperature, direction, tilt, and altitude sensors, with an GIS system with an extremely short baseline (USBL), such that precise underwater GPS fixes can be obtained. The US government has efforts aimed at the growth of

autonomy. Investigate the increasing prevalence of illegal drug smuggling operations utilizing submarines. [13,14] A USV's location near the air-sea interface enables it to broadcast audio signals underwater and radio frequency communications in the air. Consequently, they constitute a crucial element of the US Navy's conceptualization of the interconnected battle environment. [15,16] Recent demonstrations have utilized USVs to promote the advancement of long baseline navigation for UUVs. [17,8] While several military applications have focused on conventional requirements and capabilities such as harbor protection or mine sweeping, others have advanced Unmanned Surface Vessels (USVs) into intricate networks and behaviors.
These programs assist in safeguarding humanity from danger. [10]

IV. Classification Of UAVS:

UAVs are characterized by varying standards, equipment, dimensions, ranges, and configurations. UAVs are available in the market with differing numbers of propellers or rotors. [18] Various engines and wing layouts have been integrated into UAVs. Short-range and long-range wireless technologies facilitate communication among UAVs, which are categorized as nano, micro, or large based on their intended use. Due to continuous and progressive advancements, there are significant prospects for providing cellular service. Drones are equipped with First Person View (FPV) goggles, a Global Positioning System (GPS), sensors, stabilizers, and cameras. This research identifies four main types of UAVs: fixed-wing, fixed-wing hybrid, single rotor, and multirotor. [19] Fixed-wing aeronautical vehicles The fundamental components of UAVs are wings, fuselage, motor, and propeller. Despite its ability to maintain vertical stability in the air for nearly sixteen hours, these UAVs are incapable of reversing, hovering, or rotating; proficient operational abilities are essential for their use. Consequently, they are unhelpful for several occupations, including aerial photography. [20] UAVs are frequently employed for aerial mapping and power line inspections. In contrast, fixed-wing UAVs are ineffective for forward flying and hovering; they rely on automation and manual gliding. [21] Moreover, expensive single rotor UAVs rely on proficient training for operation. These UAVs exhibit mechanical intricacy and are susceptible to vibrations, among other factors.[22] Furthermore, multirotor UAVs are the most economical and easily manufactured UAVs. Typical applications for these UAVs include video surveillance and imaging. Multirotor UAVs may be classified as hexacopters, octocopters, tricopters, or quadcopters. The most often utilized unmanned aerial vehicles (UAVs) are quadcopters. In addition to their simplistic design, affordability, and compact dimensions, quadcopters have garnered interest because to their vertical landing, rapid maneuverability, exceptional agility, and takeoff proficiency. [23]

Drone:

A Drone, classified as a "Unmanned Aerial Vehicle" or Flying Robot [24], is engineered using microcontrollers to operate in concert with sensors, communication systems, and GPS technology. It can be remotely controlled or autonomously navigate using pre-programmed software flight plans. The term and concept of drone, initially employed for military applications through hot air balloons, developed during World Wars I and II. Drones are currently highly versatile and employed at various periods depending on the platform and the nature of the given mission.

Classification of Drone Vehicles According to Propeller Number

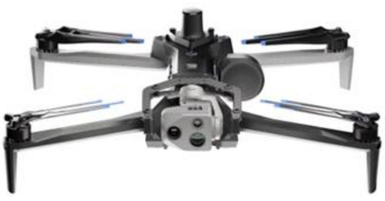

Figure 2: Quadcopter Drone [43]

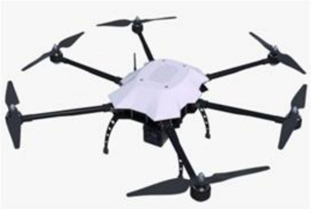

Figure 3: Hexacopter Drone [44]

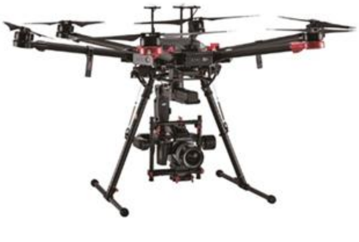

Figure 4: Octocopter Drone [45]

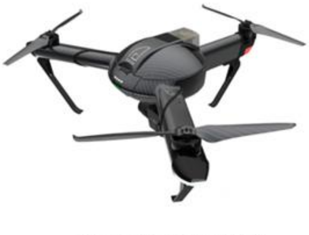

Figure 5: Tricopter [46]

V. General Structure Of The UAV:

Unmanned combat aerial vehicles (UCAVs) have surged in prominence in recent years owing to advancements in their mechanical, electronic, and software systems. These gadgets comprise a chassis, electrical circuitry, propellers, speed and flight control mechanisms, a remote access module, GPS, and a power source. Supplementary components comprise sensors, transceiver antennas, data storage devices, cameras, and weapon systems. Additional mobile devices, such as PCs, tablets, and smartphones, may also be incorporated into these components.

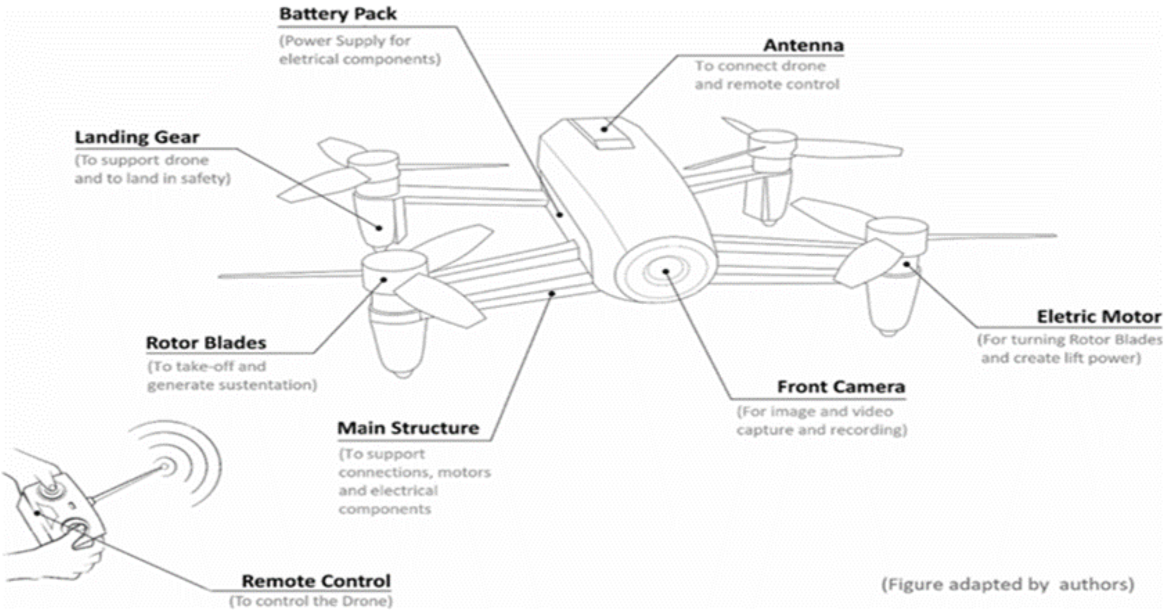
Battery Pack
(Power Supply for eletrical components)
Antenna
To connect drone and remote control
Landing Gear
(To support drone and to land in safety)
Eletric Motor
(For turning Rotor Blades and create lift power)
Rotor Blades
(To take-off and generate sustentation)
Front Camera
(For image and video capture and recording)
Main Structure
(To support connections, motors and electrical components
Remote Control
(To control the Drone)
(Figure adapted by authors)

Figure: 6 Scheme of the main physical parts of drones in general [26]

UAV systems utilizing wireless network architecture implement the principles established by Private Dynamic Networks (Ad-Hoc), which are networks founded on the collaboration of mobile nodes communicating without a centralized and fixed structure. Diverse network architectures can be implemented within Ad-Hoc architecture for UAV systems, including Mobile Ad-hoc Network (MANET), Vehicle Ad-hoc Network (VANET), and Wireless Sensor Networks (WSN).

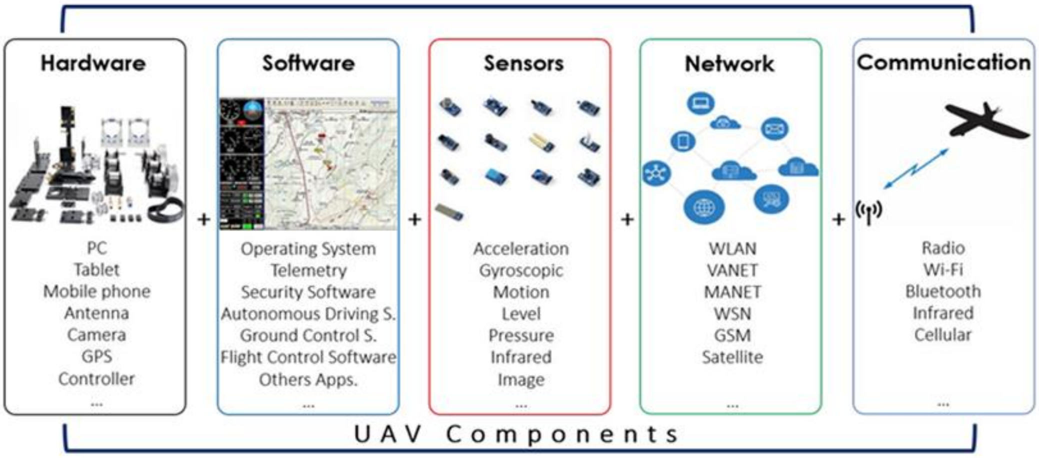

Figure:7 Parts that are fundamental to the UAV[27]

In MANET architecture, each device functions as a node, however possesses the autonomy to traverse freely, resulting in the loss of routing data packets, security vulnerabilities in network communications, and deficiencies in access control. The VANET design facilitates wireless connections among autonomous mobile devices and connecting devices equipped with sensors, whereas WSN constitutes an Ad-Hoc network formed by several sensors, which suffers from significant drawbacks due to high energy consumption. [27]

VI. Cyber Dangers And Attacks On Unmanned Aerial Vehicles:

Cyber attacks on UAV systems can occur in various components, including hardware, software, network, sensor, and communication. Each component requires a separate architecture, resulting in potential security vulnerabilities. Critical decision-making components may also be affected by these threats. Cyber attacks aim to compromise the confidentiality, integrity, and accessibility of information. [42]. The vulnerability exploited by the assailant will dictate the kind of strikes a UAV can do. The extensive UAV system comprises three main components: the UAV transceiver, the communication channel, and the control center; hence, one or several vulnerabilities may be present at any time. Available hits can be classified into two principal categories.

Active Attacks

The section on penetration testing within the Ethical Hacking system encompasses this type of assault. The primary objective of such attacks is to induce a breach or disrupt services, disregarding the disruption in the initial transmission. These attacks conclude immediately upon achieving the requisite data or objective; they transpire in real-time, at t = 0.

Passive Attacks

This type of attack is encompassed inside the penetration testing module of the Ethical Hacking system. The primary objective of these assaults is to induce a breach or disrupt services, irrespective of the disruption occurring during transmission. At t = 0, these assaults transpire in real time and conclude immediately upon the attainment of the requisite data or objective.

VII. Assaults And Their Associated Risk Factors

The three primary forms of assaults that can be executed against a UAV are command injection, denial of service, and man-in-the-middle attacks.[31] Each assault will yield a certain form of loss. The loss may represent either a security threat or a minor setback in the sector. The subsequent part clarifies the causes and risks associated with attacks that can be conducted using a UAV system.

Surveillance Attack

It may adopt either a passive or aggressive approach to this assault. During this assault, the assailant manipulates data or does reconnaissance by intercepting communications between the authorized sender and the recipient. This attack may result in damage to data integrity or a data breach. The CIA trinity depends on the safeguarding of data integrity. Intercepting essential communications during the connection process can initiate this attack. A multitude of techniques, such as IP spoofing, ARP poisoning, DNS poisoning, ARP spoofing, DNS spoofing, SSL hijacking, and HTTPS spoofing, can be employed to execute this attack. The subsequent image illustrates a fundamental Man-in-the-Middle attack, which entails diverting the communication from its initial sender to the attacker and subsequently returning it to the original recipient..[32] (Figs. 5 and 6).

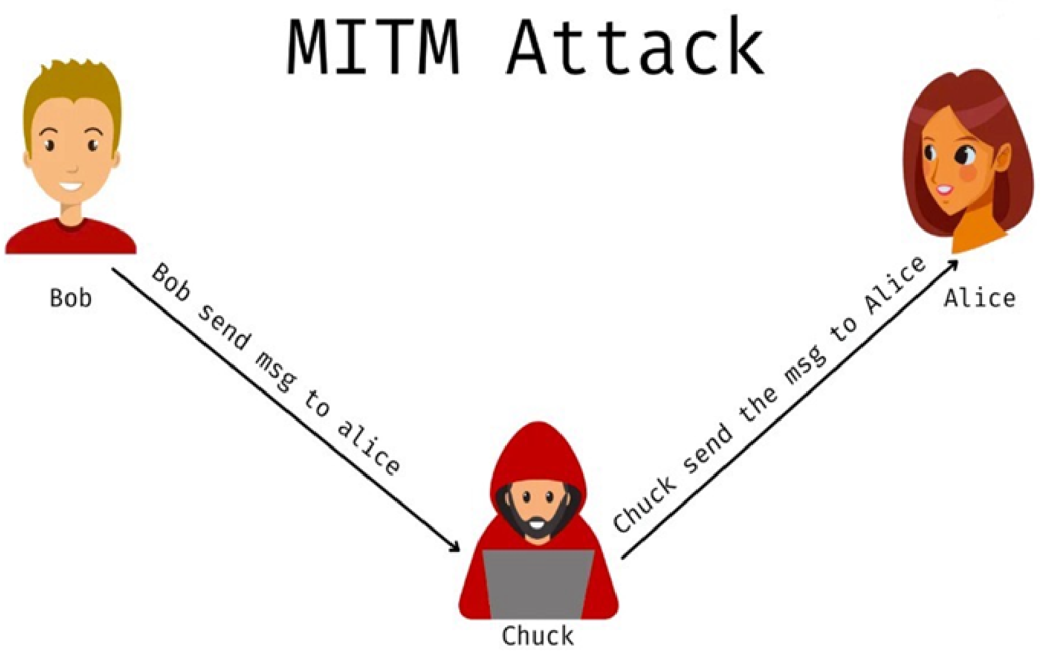

Figure: 8 Surveillance Attack [33]

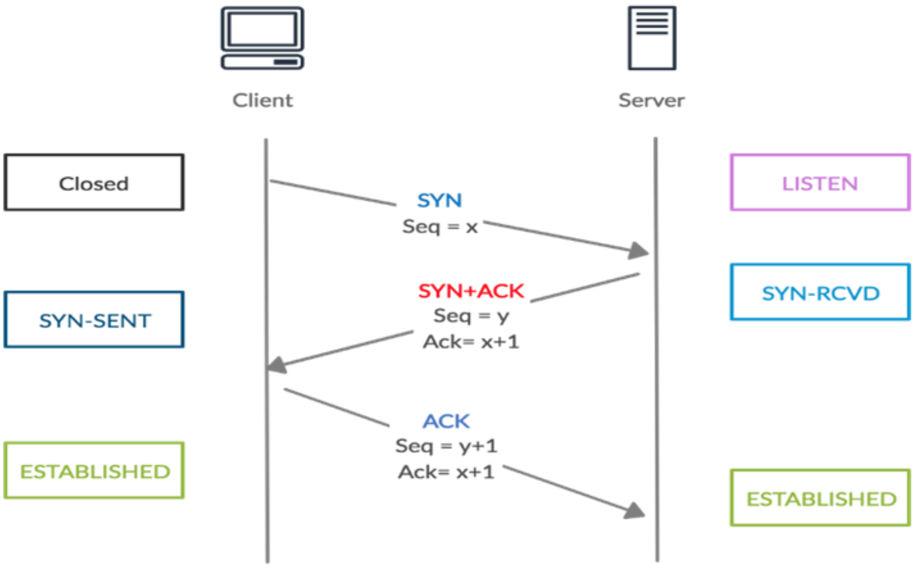

Figure: 9 Multiple TCP handshakes in MITM attack [34]

A surveillance attack on the UAV communication channel may result in compromised monitoring, session hijacking, illegal activities, attacks—particularly involving military UAVs—erroneous data, change of UAV projectiles, and more repercussions.

Denial of Service Attack

This signifies a proactive attack. The assailant overwhelms the target with numerous packages in this assault. These packets function as many requests to the destination, which falters when it is unable to manage the amount of demands. These packets may consist of either TCP SYN packets or ordinary ICMP echo request packets. The Distributed Denial of Service (DDoS) attack is an advanced version of this assault. The aggressor utilizes many controlled sources to inundate packets in this attack, rather than relying on a singular source. The name "zombies" refers to these beings.
Zombie refers to the extensive network of zombies utilized to carry out the assault.

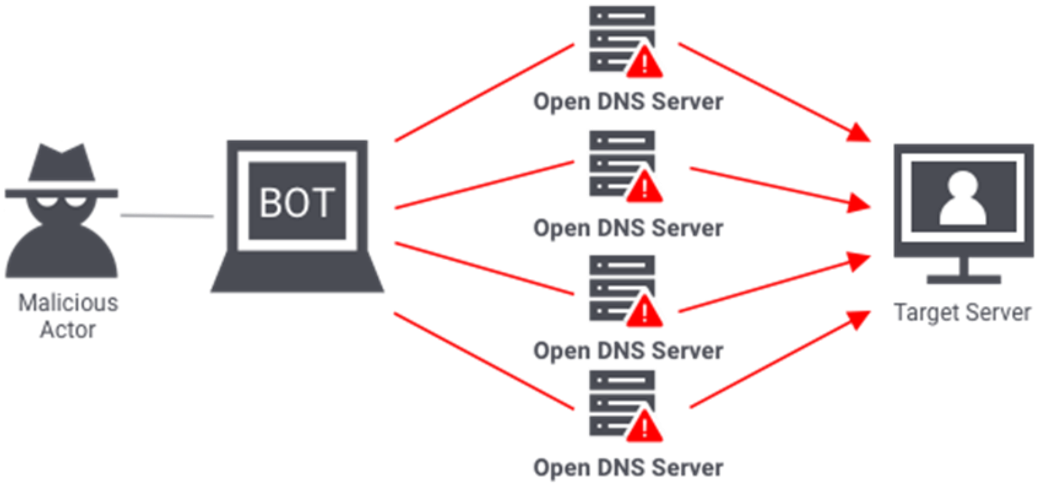

Fig. 10 Representation of distributed denial of service attack [35]

Consequently, as a result of DDoS attacks, the server will be unable to accommodate the needs of legitimate users. A distributed denial of service (DDoS) attack on the control center or the UAV transceiver through the UAV communication channel may disrupt communication between the two entities. Consequently, the UAV may be susceptible to hacking, potentially resulting in the loss of packets containing critical data. [36]

Command Injection Attack

This demonstrates a forceful attack. This approach involves placing a code fragment into an HTML-based application to facilitate unauthorized access. The tendency to Cyber Attacks has a script that might facilitate unwanted access and data tampering. The added code is inherently harmful and runs the script. Should a command injection vulnerability exist in either the UAV control center or the UAV drone, the whole system becomes subject to external compromise and takeover.

Privilege Escalation Attack

This is a kind of aggressive assault. In this assault, the user obtains access from a superior authority to execute actions that are unauthorized for them. This transpires due to the use of default credentials in administrative systems or the presence of insufficient access control mechanisms.

IP Spoofing Attack

This represents a violent attack. This type of attack use IP spoofing to deceive the system into believing the request originated from a legitimate source. It involves substituting the genuine IP address with a fictitious one to conceal it. Consequently, this strategy may be employed to infiltrate the UAV system if its firewall permits access from designated fixed IP addresses.

DJI Parrot Bebop 2 and Phantom 4

Changing two drone models, DJI's Phantom 4 Pro and Parrot's Bebop 2 echo how safe UAV is nowadays. They are easy targets for various kinds of assaults.
Consequently, Phantom 4 Pro has two combined risks: GPS Spoofing and DJI SDK. [37]

VIII. Possible Measures To Protect Against Cyber Dangers

- Methods for encrypting data provide excellent means to mitigate privacy protection concerns; nevertheless, professionals must include robust mechanisms to thwart attackers from simply deciphering encrypted data. Techniques based on policy and cryptography are useful mitigation strategies against integrity threats. Furthermore, the data must be maintained in an encrypted format. Additionally, if necessary, the data must be sent to the command center using an encrypted communication protocol. [38]
- Redundancy in systems denotes the duplication of components or functions. [39] A single component failing as a consequence of a potential cyberattack might cause the entire unmanned aircraft to crash, hence the concept must be considered during the initial design phase of the vehicle.
- Reliable sensors have to constantly examine the surroundings of autonomous vehicles. We need precise information on a thing's velocity and range close to the unmanned vehicle. Sound navigation and range, radio detection and ranging (RADAR), Under usual circumstances, SONAR and Light Detection and Ranging (LIDAR) provide exact quantitative data about ambient objects. [40] These sensors assist an autonomous vehicle in detecting and comprehending the motions of nearby objects, hence facilitating the avoidance of potential accidents. Consequently, both isolated and personal sensor systems may aid in detecting such threats. A prudent precaution is to compare data acquired from many sensors; sensors affected by a potential cyberattack may communicate erroneous data components. [41]
- Unmanned vehicles include several subsystems, namely systems of systems. The subsystems of unmanned vehicles include GNSS, communication equipment, and video cameras. It is possible to construct a "multi-agent system" on several unmanned vehicles. Software agents may be very effective at identifying potential hazards. [2]
- Solid-state storage devices surpass hard drive-based storage for the data requirements of unmanned vehicles. [41]
- Unmanned vehicles may be used in difficult circumstances. Hard-drive-based storage may be adversely impacted by vibration, directional forces, or magnetic fields, potentially resulting in data loss. Strategies for ensuring reliable operation must be developed to counter potential cyberattacks and breakdowns of hardware or software components. Consequently, distributed programming tools and methodologies have to be used in unmanned vehicles. [2]

IX. Compares The Efficacy Of Various Mitigation Measures:

Mitigation Strategy	Primary Focus	Contribution To Uav Safety	Example
Using Reliable Distributed Programming	Distributed Systems	Ensures Continuous Availability By Preventing Unforeseen Hardware Or Software Failures And Disruptions Caused By Cyberattacks.	Distributed Real-Time Systems For Uav Control With Redundancy In The Event Of Subsystem Failure

Including Cyber-Security In Requirement Phase	Requirement Engineering	Ensures The Prompt Identification Of Cyber-Security Requirements (Confidentiality, Integrity, Availability), Hence Mitigating Vulnerabilities In Subsequent Design Phases.	Preliminary Analysis Of Security Requirements For Uav Control Systems, Prioritizing Data Integrity And Availability.
Implementing A System With Multi-Agents	System Architecture	Facilitates Decentralized Intelligent Governance Through Flexible Software Agents That React To Environmental Fluctuations And Mitigate Security Threats..	Multi-Agent Systems That Ensure Communication Pathways Against Cyber-Attacks And Provide Real-Time Updates For Uav Subsystems.
Redundancy	Fault Tolerance	Ensures Multiple Systems Or Components Are Established To Manage Failures Or Cyberattacks Without Compromising Vehicle Performance, So Averting Loss Of Control.	In Dual-Control Systems, The Failure Of One Subsystem, Such As Communication, Does Not Compromise Vehicle Control.
Diversity	Fault Tolerance	Employs Several Techniques To Prevent Assailants From Infiltrating Redundant Systems, So Ensuring That Breakdowns Are Detected And Contained	Redundant Systems Employing Voting Logic Ensure The Vehicle Remains Operational Even If A Single Component Fails.
Defense-In-Depth	Cyber-Defense	Implements Multiple Layers Of Security To Detect And Prevent Cyberattacks, Including Unauthorized Access And Subsequent Efforts To Breach The System.	Following An Initial Breach, Anomalous Activity Has Been Observed By Intrusion Detection Systems.
Authentication	Access Control	Blocks Entry By Unapproved Users To The Uav System, Ensuring That Both Devices And Individuals Are Properly Authenticated Prior To System Interaction.	Digital Signatures And Authentication Codes Facilitate The Validation Of Users And Components Within Uav Systems
Using Micro-Kernel	Embedded Software	Minimizing The Attack Surface Of The Operating System Ensures That Only Essential Actions Are Permitted For The Kernel, Hence Enhancing Security.	Microkernel-Based Embedded Systems Restrict Device Drivers And Other Non-Essential Functions From Affecting The Primary Operations Of The Uav.[2]

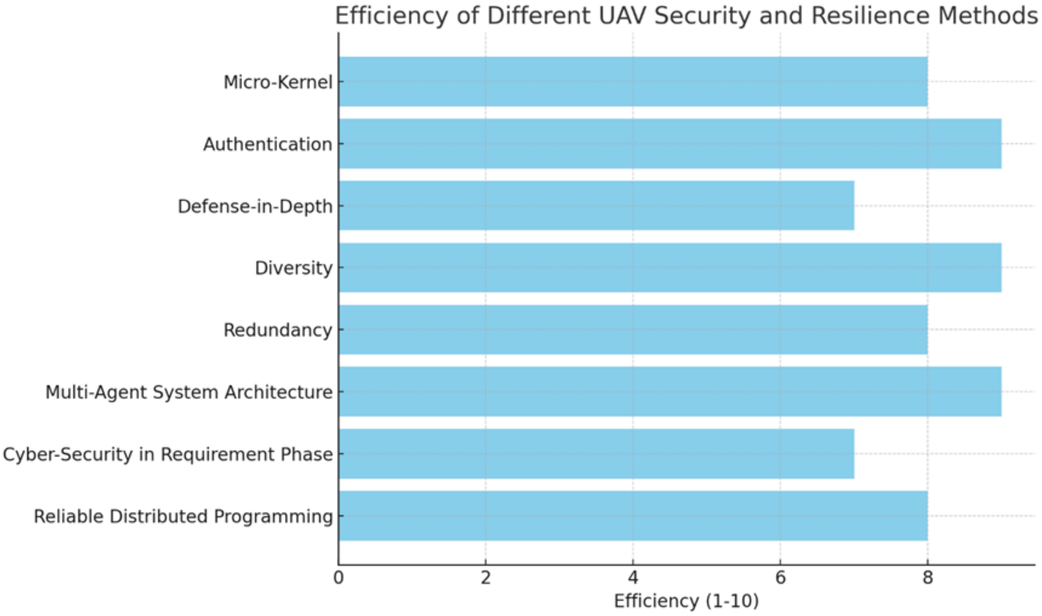

Figure: 11 Efficiency Of Different Uav Security And Resilience Methods [28-30]

X. Conclusion:

The rapid development and integration of Unmanned Aerial Vehicles (UAVs) into environmental monitoring, surveillance, and agriculture has generated cybersecurity concerns. Surveillance attacks, Denial of Service (DoS), and Command Injection attacks were examined, along with UAV hardware, software, and communication channel vulnerabilities. These threats threaten UAV availability, integrity, and secrecy, threatening public safety and mission success. To address these risks, the research examined distributed real-time systems, multi-agent topologies, redundancy, encryption, and authentication. Multi-agent systems enable distributed control and real-time threat response, while distributed systems and redundancy provide ongoing operation amid component failures or cyberattacks. UAV communications are protected against eavesdropping and tampering using encryption and authentication. The results show that cybersecurity should be included in the first UAV system design to increase reliability and resilience. These mitigation methods will let UAVs function safely and sustainably in multiple uses. Future research should focus on adaptive security and innovative technologies to address autonomous system cyber threats.

Future of Autonomous Cybersecurity in UAVs (Industry 5. O):

The future of autonomous cybersecurity in UAVs will be influenced by sophisticated technologies such as AI-driven threat detection, blockchain-secured communications, and quantum-resistant encryption to combat emerging cyber threats. Blockchain ensures immutable data integrity and decentralized authentication; artificial intelligence will facilitate real-time anomaly detection and autonomous recovery capabilities. Digital twins will provide proactive vulnerability assessments, while swarm intelligence will enhance the coordination of defences inside UAV networks. Zero Trust Architecture will necessitate ongoing authentication as UAVs become increasingly integrated into. Industry 5.O ecosystems; regulatory frameworks will establish standardized security protocols.

These advancements will transform UAVs into robust, self-protecting systems capable of autonomous danger mitigation. The integration of artificial intelligence, quantum cryptography, and distributed security models will ensure that UAVs operate safely in increasingly complex environments, from smart cities to defence applications. As UAVs undertake ever-sophisticated roles, the necessity for cybersecurity that aligns with technological advancements and emerging threat vectors becomes imperative.

References:

[1] Yeomans, P. 5–6 (2014).

[2] Yağdereli, E., Gemci, C. & Aktasx, A.Z. A Study On Cyber-Security Of Autonomous And Unmanned Vehicles. J. Def. Model. Simul. Appl. Methodol. Technol. 12, 369–381 (2015). Https://Doi.Org/10.1177/1548512915575803

[3] Zhang, X., Yang, J. & Lu, W. Applications Of Uavs In Environmental Monitoring. Environ. Sci. Technol. 56, 3435–3444 (2022).

[4] Smith, J., Robinson, D. & Zhao, L. Unmanned Surface Vehicles For Marine Operations: A Review. Mar. Technol. Soc. J. 54, 56–68 (2020).

[5] Johnson, P., Lee, K. & Baker, S. Synergy Between Uavs And Usvs: A Potential Framework For Future Maritime Operations. Ieee Trans. Autom. Control 66, 6789–6799 (2021).

[6] Nourmohammadi, A., Jafari, M. & Zander, T.O. A Survey On Unmanned Aerial Vehicle Remote Control Using Brain–Computer Interface. Ieee Trans. Hum.-Mach. Syst. 48, 337–348 (2018).

[7] Kanellakis, C. & Nikolakopoulos, G. Survey On Computer Vision For Uavs: Current Developments And Trends. J. Intell. Robot. Syst. 87, 141–168 (2017).

[8] Ucgun, H., Yuzgec, U. & Bayilmis, C. A Review On Applications Of Rotary-Wing Unmanned Aerial Vehicle Charging Stations. Int. J. Adv. Robot. Syst. 18, 17298814211015863 (2021).

[9] Mademlis, I. Et Al. A Multiple-Uav Software Architecture For Autonomous Media Production. Eurasip Eur. Signal Process. Conf. (Eusipco) (2019).

[10] Manley, J.E. Unmanned Surface Vehicles, 15 Years Of Development. Proc. Oceans 2008, Mts/Ieee, Quebec City, Canada (2008).

[11] Catlin Sea View Survey Project. Http://Catlinseaviewsurvey.Com/ (Accessed September 10, 2014).

[12] Hagen, P.E., Fossum, T.G. & Hansen, R.E. Applications Of Auvs With Sas. Proc. Oceans 2008, Mts/Ieee, Quebec City, Canada (2008).

[13] Kushner, D. Drug-Sub Culture. N. Y. Times April 23 (2009). Http://Www.Nytimes.Com/2009/04/26/Magazine/26drugs-T.Html (Accessed September 10, 2014).

[14] Carter, M. Network Integrated Robotics At Spawar Systems Center Pacific. 2nd Annu. C4isr, Cyber Secur., Robotic Platf. Sens. Conf., San Diego, Ca (2009).

[15] Ferreira, H. Et Al. Swordfish: An Autonomous Surface Vehicle For Network Centric Operations. Proc. Oceans Europe'07 Conf., Ieee Oes, Aberdeen, Scotland (2007).

[16] U.S. Navy. The Navy Unmanned Surface Vehicle (Usv) Master Plan. Www.Navy.Mil/Navydata/Technology/Usvmppr.Pdf (Accessed September 29, 2014).

[17] Curcio, J. Et Al. Experiments In Moving Baseline Navigation Using Autonomous Surface Craft. Proc. Oceans 2005, Mts/Ieee, Washington, Dc (2005).

[18] Different Types Of Drones. Https://Dronepedia.Xyz/5-Different-Types-Of-Drones/ (Accessed April 1, 2022).

[19] Tahir, A., Boling, J., Haghbayan, M.H., Toivonen, H.T. & Plosila, J. Swarms Of Unmanned Aerial Vehicles—A Survey. J. Ind. Inf. Integr. 16, 100106 (2019).

[20] Mairaj, A., Baba, A.I. & Javaid, A.Y. Application Specific Drone Simulators: Recent Advances And Challenges. Simul. Model. Pract. Theory 94, 100–117 (2019).

[21] Gunarathna, J.K. & Munasinghe, R. Development Of A Quad-Rotor Fixed-Wing Hybrid Unmanned Aerial Vehicle. Proc. 2018 Moratuwa Eng. Res. Conf. (Mercon), Moratuwa, Sri Lanka (2018).

[22] Wen, S., Han, J., Lan, Y., Yin, X. & Lu, Y. Influence Of Wing Tip Vortex On Drift Of Single Rotor Plant Protection Uav. Trans. Chin. Soc. Agric. Mach. 49, 127–137 (2018).

[23] Mohsan, S.A.H. Et Al. Towards The Unmanned Aerial Vehicles (Uavs): A Comprehensive Review. Drones 6, 147 (2022). Https://Doi.Org/10.3390/Drones6060147

[24] Batth, R.S., Nayyar, A. & Nagpal, A. Internet Of Robotic Things: Driving Intelligent Robotics Of Future—Concept, Architecture, Applications And Technologies. Proc. 2018 4th Int. Conf. Comput. Sci. (Iccs), 151–160. Ieee (2018).

[25] Nayyar, A., Nguyen, B.L. & Nguyen, N.G. The Internet Of Drone Things (Iodt): Future Envision Of Smart Drones. Proc. 1st Int. Conf. Sustain. Technol. Comput. Intell. (Ictsci 2019), 563–580. Springer Singapore (2020).

[26] Falorca, J.F., Miraldes, J.P. & Lanzinha, J.C.G. New Trends In Visual Inspection Of Buildings And Structures: Study For The Use Of Drones. Open Eng. 11, 734–743 (2021).

[27] The Eurasia Proceedings Of Science, Technology, Engineering & Mathematics (Epstem) Issn: 2602-3199

[28] Zhang, L. Et Al. A Comprehensive Review Of Cyber Attack Defense Strategies For Uavs. Comput. Mater. Contin. 72, 123–138 (2023).

[29] Smith, J., Gupta, R. & Lee, K. Modeling And Simulation Of Cyber Attack Scenarios In Uav Networks. J. Cyber Secur. Priv. 4, 56–72 (2022).

[30] Chen, X., Zhao, H. & Yao, F. Real-Time Simulation Methods For Uav Cyber-Attack Analysis. Int. J. Unmanned Syst. 9, 201–215 (2021).

[31] Gudla, C., Rana, M.S. & Sung, A.H. Defense Techniques Against Cyber Attacks On Uavs. Int. Conf. Embedded Syst., Cyber-Phys. Syst. Appl. (Escs'18), 110–116 (2018).

[32] Secureboxpage. Https://Securebox.Comodo.Com/Ssl-Sniffing/Man-In-The-Middle-Attack/. (Last Accessed 2019/02/24).

[33] Man In The Middle Attack. Available Online: Man-In-The-Middle Attack | Different Types And Techniques - Cybervie

[34] Tcp 3 Way Handshake 2020. Available Online: Tcp 3 Way Handshake In Detail

[35] Denial Of Service Attack. Available Online: Denial-Of-Service Attack (Dos) Nedir? | Bulb

[36] Ddos Distributed Denial Of Service. Available Online: Ddos Distributed Denial Of Service Attacks: Protection, Prevention

[37] Dey, V., Pudi, V., Chattopadhyay, A. Et Al. Security Vulnerabilities Of Uavs And Countermeasures: An Experimental Study. Proc. 2018 31st Int. Conf. Vlsi Design & 17th Int. Conf. Embedded Syst. (Vlsid), 398–403. Ieee (2018).

[38] Madan, B.B., Banik, M. & Bein, D. Securing Unmanned Autonomous Systems From Cyber Threats. J. Def. Model. Simul. Appl. Methodol. Technol. 16, 119–136 (2019). Https://Doi.Org/10.1177/1548512916628335

[39] Lezoche, M. & Panetto, H. Cyber-Physical Systems, A New Formal Paradigm To Model Redundancy And Resiliency. Enterp. Inf. Syst. 14, 1150–1171 (2020). Https://Doi.Org/10.1080/17517575.2018.1536807

[40] Onori, D. Et Al. Coherent Radar/Lidar Integrated Architecture. Proc. 2015 Eur. Radar Conf. (Eurad), 241–244. Ieee, Paris, France (2015). Https://Doi.Org/10.1109/Eurad.2015.7346282

[41] Hartmann, K. & Steup, C. The Vulnerability Of Uavs To Cyber Attacks– An Approach To The Risk Assessment. 5th Int. Conf. Cyber Conflict (Cycon 2013), 1–23. Ieee, Tallinn, Estonia (2013).

[42] Cosar, M. & Kiran, H.E. Verification Of Localization Via Blockchain Technology On Unmanned Aerial Vehicle Swarm. Comput. Inform. 40, 428–445 (2021). Https://Doi.Org/10.31577/Cai_2021_2_428

[43] Drone Types And Uses: A Comprehensive Guide For Drone Pilots. Available Online: Drone Types And Uses: A Comprehensive Guide For Drone Pilots

[44] Global Defense News. Available Online: Russia Creates Mis-35 Hexacopter Drone That Comes Back When Communication Is Lost

[45] World's First 100-Million-Pixel Drone Launched By Dji And Hasselblad. Available Online: World's First 100-Million-Pixel Drone Launched By Dji And Hasselblad: Digital Photography Review

[46] This Drone Three Propellers Xiaomi Forward A Powerful Camera Action: 4k At 60 Images Per Second. Available Online: This Drone Three Propellers Xiaomi Forward A Powerful Camera Action: 4k At 60 Images Per Second | Improtec Inc