DS Journal of Cyber Security
Volume 2 Issue 2, 9-19, Apr - Jun 2024
ISSN: 2584-0665 / https://doi.org/10.59232/CYS-V2I2P102

Original Article

Appraise the Desideratum of Cyber Security for Armed Drone

Udaya Kumar Giri[1], Shrish Kumar Tiwari[2]

[1,2]*Department of Strategic Technologies, School of National Security Studies, Central University of Gujarat, Gujarat, India.*

[2]drshrishkumartiwari@gmail.com

Received: 07 April 2024; Revised: 09 May 2024; Accepted: 31 May 2024; Published: 13 June 2024;

Abstract - Industrial and technological advancement has paved the way for the emergence of highly sophisticated and modernized arms and ammunition in the defence sector. Unmanned aerial vehicles, popularly known as drones, emerged as a force multiplier technology that makes intelligence, surveillance, and target acquisition easier. The technological processes that include the airframe, propulsion system, embedded computing system, ground control system, and autopilot systems of drones can run through networking or by connecting the GPS systems. That makes drone technology vulnerable because its networking and dispersed physical systems located in remote places make it easier for cyber-attacks on control loops. For instance, GPS spoofing, fuzzing attacks, hijacking, immobilization, and gain scheduling attacks are most common for cyber attackers, which cannot deny the operability of the UAVs but pose security threats to the host countries. So, in this premise, this paper examines the necessity and role of cyber security for unmanned aerial systems or armed drones. Further, this paper analyses various methods to protect armed drones from cyber-attacks.

Keywords - Cyber-attack, Armed drone, Spoofing, Hijacking, Information corruption.

1. Introduction

In the 21st century, digitalized world security in cyberspace has become a live blood for the smooth running and sustentation of a nation. Any threat in cyberspace leads to an unrecognized and uncertain threat towards the security and survivability of a nation. The technological advancement and modernization in the defence sector pave the way for the advancement and use of drone technology by developed and developing nations. At the same time, the capability of drones as a force multiplier and their role in ISRT operation became another factor for its advancement and use in critical situations like warfare. For instance, in the Armenia-Azerbaijan conflict, the multifaceted role of armed drones makes it easy for the nation to win in warfare. On the one side, there is the growing importance of the advancement of drones and their use, and on the other hand, there is the emergence of cyber threats on armed drones. This is because the technological processes that include the airframe, propulsion system, embedded computing system, ground control system, and autopilot systems of drones can run through networking or by connecting the GPS systems. That makes drone technology vulnerable because its networking and dispersed physical systems located in remote places make it easier for cyber-attacks on control loops.

For instance, in 2018, a predator drone of the USA flew on top of the World Trade Organization, and a Chinese cyber attacker hacked and jam the ground control system; as a result, the predator drone lost its connectivity and fell on the World Trade Organization. In this scenario, there is a plethora of research conducted on the theme of advancement and use of drones, how AI is used in drones and what is its relevance for the present world. There is less amount of research taking place that highlights the cause, consequences and needs of cyber security for armed drones and suggests mitigative measures in order to get rid of the cyber threats which is the main aim of this paper. So this paper highlights three major themes: firstly role and relevance of armed drones in the 21st century digitalized world. Secondly, to examine the cause and consequence of cyber threats and security for armed drones, and lastly, what will be the mitigative measure to minimize these cyber related threats.

Drones are cyber-physical systems that primarily rely on the close connection of systems like aircraft systems, Ground Control Stations (GCS) and computing elements like flight management computers and data links to complete their mission. These systems incorporate various components, including computing, networking, propulsion, physical structure (airframe), embedded computers (including ground-based control station, autonomous system, virtualized radio link, multiple payloads, launch, and retrieval systems) and propulsion system (Sihag et al., 2023). Drones rely extensively on cyber networks and embedded computational systems for their functionality. It is increasingly recognized as an intelligent sensor that provides situational awareness and reconnaissance to operators. In military operations, UAVs are employed for Net-Centric Operations (NCO) tasks like relentless Intelligence gathering, aerial Reconnaissance and Surveillance (ISR), and Acquiring Targets (TA). It is argued that with the development of armed drones, the nature of modern-day warfare has changed. This is because the armed drone provides unprecedented capabilities for surveillance, precision strikes and intelligence gathering. On the other side, with the high demand and huge use of armed drones, it becomes an indispensable tool in military operations that enables forces to engage targets remotely and with minimal risk to the personnel. Also, with the increase in reliance on armed drones, cyber security threats have become familiar, so there is also a need for robust cybersecurity measures to protect these sophisticated systems from any myriad threats.

Armed drones come up with highly complex and integrating advanced technologies such as AI, real-time data processing and satellite communications that make the drone highly effective and, at the same time, create multiple attack vectors for cyber adversaries. It is noticed that any cyber-attack leads to catastrophic damage in the form of loss of sensitive information, unintended military engagements or disabling critical military assets. A cyber-attack on a UAV could lead to loss of control, data theft, or malicious manipulation of its mission and payload. Safeguarding UAVs against cyber threats involves implementing secure communication protocols, encrypted data transmission, and ensuring the integrity of flight control systems. Additionally, protecting the ground control stations and the networks used to operate UAVs remotely is crucial to prevent unauthorized access and control. Manufacturers and operators of UAVs must prioritize cyber security in the design, development, and operation of these devices to mitigate potential risks and enhance the safety and trustworthiness of UAV operations. As the military continues to integrate drones into operations, and there is a continuous cyber threat on armed drones, there is the necessity to understand the cybersecurity challenges and to develop robust defense mechanisms become crucial (Krishna & Murphy, 2017). The future of warfare will increasingly depend on our ability to secure these advanced systems against cyber threats, making cybersecurity an integral component of military drone operations. Thus, this paper tries to examine the role of cyber security for armed drones and find out some mitigative measures to minimize cyber threats in armed drones.

2. Delineation of Theme

This paper wants to highlight three major themes first one is what is the importance of cyber security in the 21st-century digitalized world, the second one is to analyze what is unmanned aerial systems and their importance, and the last highlights how cyber threats on UAS put security threats and how cyber security can be maintained. So, the major theme of the paper is discussed as follows.

2.1. Unmanned Aerial System (UAS)

Federal Aviation Administration (FAA) defined UAS as “A device used or intended to be used for flight in the air that has no on-board pilot. This includes all classes of airplanes, helicopters, airships, and translational lift aircraft that have no onboard pilot". Traditional balloons are not considered to be unmanned aircraft because they are unable to navigate in three axes. A UAV, or drone, is a flying machine in the absence of a human pilot or any passengers (Labib et al., 2021). It is a pilotless aircraft. Unmanned aircraft can either have on-board or off-board (remote control) control mechanisms. Markus Wrangler rightly defined the term UAV as "An unmanned aerial vehicle is an aircraft without a human operator on-board and is commonly referred to as a 'drone', but also as a Remotely Piloted Vehicle (RPV), Remotely Piloted Aircraft (RPA), Remotely Operated Aircraft (ROA) or, in the case of UAVs with specific combat roles, as an unmanned aerial combat vehicle". A motorized vehicle without a human driver that can be controlled remotely or autonomously, can carry an extremely dangerous or nonlethal payload, and can be expendable or recoverable, ballistic or semi-ballistic items, such as cruise missiles, artillery missiles, submarines, mining operations, satellites, or unattended sensors, are not considered unmanned vehicles. (without a propulsion system). According to the U.S. DOD, "an unmanned aerial vehicle is a powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or non-lethal payload".

2.1.1. Communication Mechanism for the UAV System

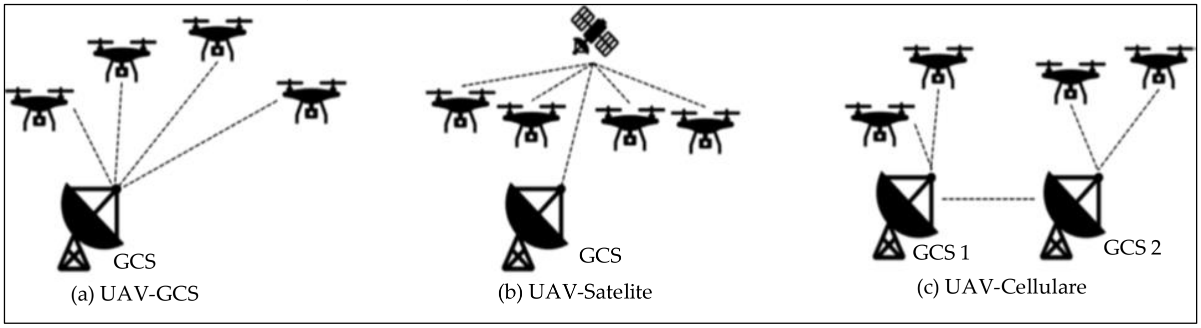


Fig. 1 Communication system for UAV

As per the communication mechanism of UAVs is concerned, UAVs are communicated through three means: ground control system, satellite communication system, and last one is circular system. In the ground control system UAVs, a bunch of drones are connected with one ground control system. In satellite communication systems, drones are connected to the satellite and operated by a human pilot through ground control systems. In the cellular system, a bunch of UAVS are connected with more than one ground control system.

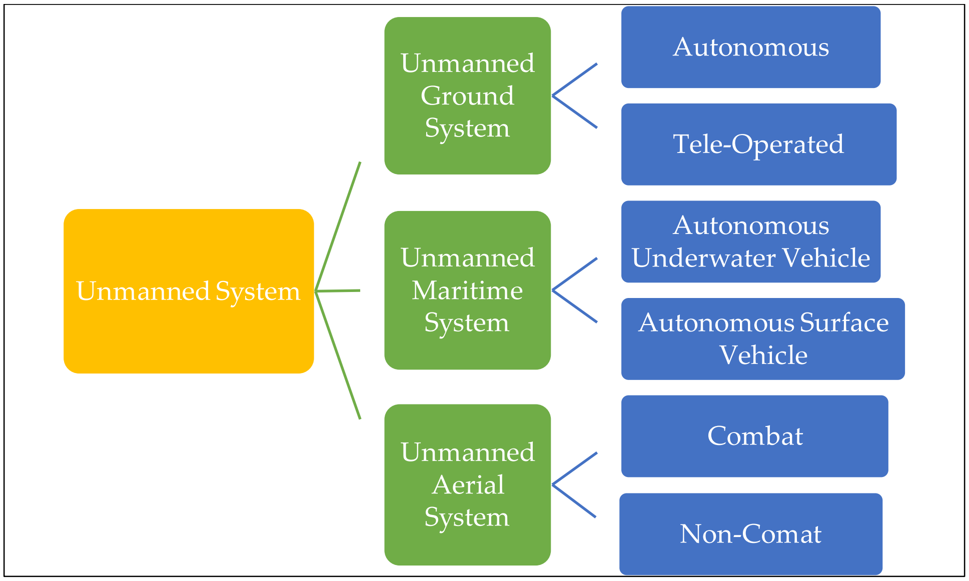


Fig. 2 Types of UAS system

2.2. Use of Artificial Intelligence in UAV

Artificial intelligence is defined as a combination of computer science and robot systems that can be applied to a particular problem and enable problem-solving. It also encompasses subfields of artificial intelligence that are widely used in conjunction with machine learning and deep learning. It refers to the capability of a machine that can perform the task as like human being where human intelligence is core in performing certain tasks. However, the use of artificial intelligence in UAVs enables the UAV to cover a larger area and perform tasks more efficiently. For instance, UAVs are deployed for border surveillance, and with the help of artificial intelligence, UAVs can do surveillance autonomously and provide real-time surveillance data (Kariri, 2022). UAVs are used to analyze the data that are collected through surveillance by using AI algorithms. For instance, UAVs are deployed for border surveillance, and with the help of artificial intelligence, UAVs can do surveillance autonomously and provide real-time surveillance data (Kariri, 2022). In a nutshell, AI can be used to automate the controls of drones including their navigation and movement. Images and videos are captured during surveillance to learn more about the targets (Kariri, 2022). Scientists, as well as companies are using automated surveillance more frequently, which enables them to evaluate video material more accurately.

With the emergence of the fighter and high-altitude long-endurance category of unmanned aerial vehicles, the role of artificial intelligence has doubled. It is because of doing precision strikes and conducting SEAD and DEAD operations that artificial intelligence is highly essential. For instance, the use of the unmanned aerial system for anti-terror operations, especially in areas where both civilians and terrorists are living together. So, it will be difficult for a machine like UAV to differentiate between civilians and terrorists and attack the exact target (Johnson, 2019). However, with the help of artificial intelligence and by applying facial recognition technology, UAVs can differentiate between civilian and terrorist and limit the cause of civilian death and collateral damage.

2.3. Cyber Security

Until recently, security analysis mostly focused on state security, viewing it as a result of the seriousness of risks that states confront from other states as well as the strategy and effectiveness of those responses. Following the conclusion of the Cold War, academics shifted their focus away from the state-centric perspective of security and broadened the term to include individual security. Around the same time, internal state conflicts brought on by civil wars, environmental degradation, economic hardship, and human rights violations began to pose a greater threat than external invasion (Pyzynski & Balcerzak, 2021). In this context, national security started to cover issues besides territorial security, such as poverty, economic inequality, educational troubles, environmental dangers, human trafficking, and other issues. The digital era has brought hitherto unrecognized threats to national security to the attention of the national security community. Cyber risks are, therefore, developing and growing quickly in the second decade of the twenty-first century. To secure the bioelectrical environment, as well as the data it keeps and sends, from all imaginable threats, a variety of technological and non-technical activities and procedures are together referred to as cyber security (Pyzynski & Balcerzak, 2021).

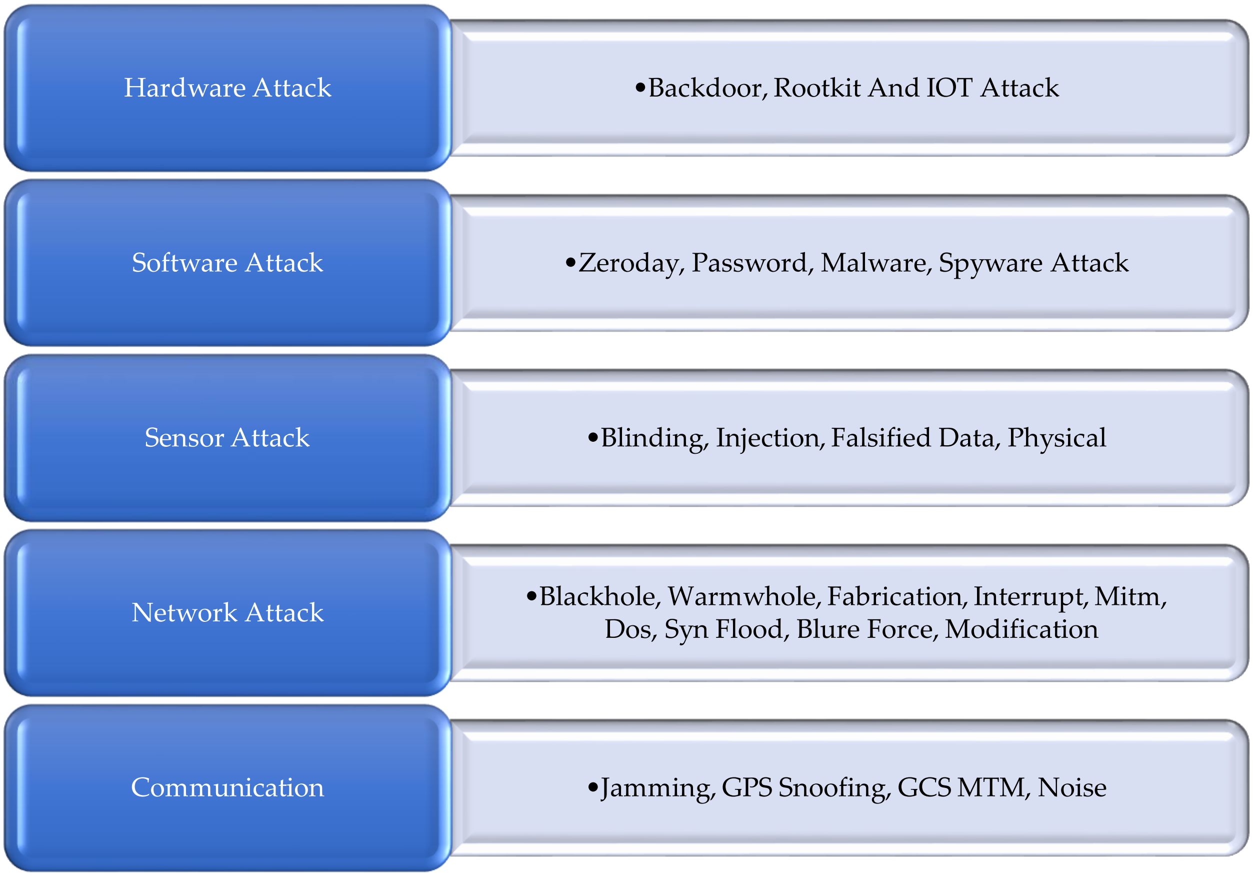
3. Methodology

This paper tries to examine how cyber threats became vulnerable to emerging technology like unmanned aerial systems and tries to find out what type of cyber threat took place on UAS systems. This paper also tries to highlight security threats that occur due to the cyber threats on UAS systems and lastly, suggests some mitigative measures to minimize cyber threats. To attain the above goal this paper took the help of descriptive, analytical methods and was based purely on qualitative research design. This paper uses a systematic approach to the literature review to reflect the current state of the field best. Data are gathered from secondary sources, including books, journal articles, newspaper articles, and periodicals. Different search engines like DTU Findit, Google Scholar, Semantic Scholar, and Scopus data are used. This paper contains three major sections first section deals with the introduction, the second major theme of this paper, the third is methodology, and the last one is a discussion that contains core arguments.

4. Discussion

4.1. Cyber-Attack on Unmanned Aerial Systems

The cyber attack on the UAV can be divided into various categories as per the nature of the attack, such as hardware attacks, software attacks, sensor attacks, network attacks, and communication, out of which communication attacks are most vulnerable. In a hardware attack, the nature of the attack is like a backdoor, rootkit, and IOT attack. Software attack includes password hacking, malware to the communication channel, and spyware attacks. The sensor is vital for the smooth running of a drone mechanism, and cyber threats took place in the form of blinding the data of UAVS and falsifying the communication data from the UAS to the pilot. Nowadays most of the cyber-attacks on the UAS took place. It takes various forms like blackhole attacks, wormholes, denial of service attacks, blur force attacks, etc. Lastly, communication cyber threats include jamming, GPS spoofing, GCS MTM, and noise.



Hardware Attack	•Backdoor, Rootkit And IOT Attack
Software Attack	•Zeroday, Password, Malware, Spyware Attack
Sensor Attack	•Blinding, Injection, Falsified Data, Physical
Network Attack	•Blackhole, Warmwhole, Fabrication, Interrupt, Mitm, Dos, Syn Flood, Blure Force, Modification
Communication	•Jamming, GPS Snoofing, GCS MTM, Noise

Fig. 3 Cyber attack on drone

4.2. Types of Cyber Attacks on Armed Drones

4.2.1. RF Jamming

The establishment of communication between the satellites and the ground control system depends on radio frequency. Any breach in the communication link leads to the shutdown of the operation. Generally, 2.4 GHz to 5.8 GHz are the most common radio frequencies used in drones, making it easy for attackers to manipulate the radio frequency, which breaches communication links. The attackers easily identified the operating channel frequency, and in contrast to the signal from the target device, RF jammers produced powerful signals. The receiver was overpowered by the sender and attackers' combined signals (Sihag et al., 2023). Hence, the communication link breach from the GCS and drone can be operated by the jammer.

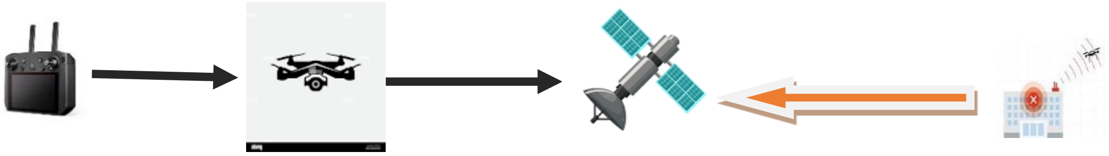


Fig. 4 Mechanism of RF jamming

4.2.2. Drone Cloning

Drones are most prominent for their ability to gather critical information through the means of ISR operations without putting any risk to the lives of pilots. For most of the critical situations, some programmed and specified drones are used and these drones contain some specific programs. The attackers develop the same drone by hacking the specific program of the drone and deploying it on the same mission. The cloned drone can then be employed to launch additional assaults (Sihag et al., 2023). The attacker controls the original drone, while the actual user pilots the drone's clone, giving the impression that he has complete control over it.

4.2.3. GPS Jamming

GPS is vital for building communication links between the ground control station with the satellite drone. GPS is utilized to determine the drone's location. GPS is an exclusive broadcast technology that uses spacecraft to monitor the drone and time the passage of data transmissions. GPS jamming is defined as a planned attack system in which the attacker can manipulate the data of the exact location of the drone and provide wrong information by jamming the communication link between the drone and the satellite. It may be simple to use GPS jamming to separate the receiver from the real satellite (Tu & Piramuthu, 2023). Example: 46 UAVS recently crashed to the ground during a demonstration above Victoria Harbour because of a GPS jamming attack.

4.2.4. Software Based Attack

One of the well-known programs that attackers have demonstrated that can be used to access the video feeds of predator drones is Sky-Garber. Attackers using this software can take advantage of the unsecured data feeds that are transmitted to the ground station via communication satellites that employ an unauthenticated communication channel. Attackers can use it to spy on targets and gain access to images and other files transferred between the drone and the base station.

4.2.5. RTL-SDR

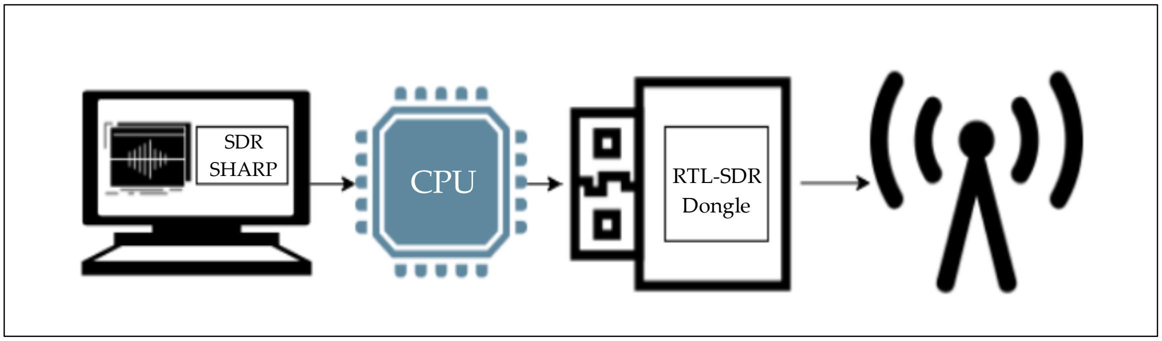


Fig. 5 RTL-SDR

RTL-SDR is vulnerable software that affects the aviation industry. This software allows for easy interception of all information exchanged between the ground station and the UAV. Through this software, it can be easy to listen to all information shared between the ground station and UAV. In this way, by using this software the attackers can easily tune the radiofrequency of the drone and can also access the data shared between the ground control system and the drone by using the same radio frequency (Johnson, 2019).

4.2.6. Death Attack

By this method, the attackers can flood messages by decrypting and intercepting network traffic. Through this method, the attackers can break the communication link between the Wi-Fi signal and can hijack the data coming from the drone to the sender.

4.2.7. Denial of Service Attack

This attack was found in the small drone where the attackers were able to access the flight controller system and interfere with the UAV software mechanism. Anyone with access to the UAV control systems can view and modify flight control commands. Including potentially triggering a shutdown command unintentionally while the drone is operational.

4.2.8. Sky Jack

The drone that hangs around searching for other drones in the area disconnects the wireless connection of the target drone's true owner after convincing it to act as its owner and feeding it commands, along with all other personal zombie drones.

4.2.9. Geofence

The drone was restricted in a no-fly zone, but in the meantime, the attackers downloaded the database, started changing it, uploaded the new database, and after that, were able to make its drone ignore the manufacturer set, no-fly zone. Example: DJI drones 11000 registered for geofences.

4.2.10. Fabrication

It is a method of changing data coming from the UAV to the receiver that will confuse the network, consume the network and disrupt the functioning of the network.

4.2.11. Open WIFI

There are some drones, like Bebop drones, that have the capacity of free Wi-Fi, which enables many users to access the network. The drone can be controlled by numerous non-authenticated users simultaneously because the device supports multiple user connections.

4.2.12. De-Authentication

The business must register with a global aviation organization to operate drones. However, it can be disrupted by the authorized owner by repeatedly sending authentication signals into the UAV, jamming the entire network, and making it impossible for anybody else to communicate with the UAV save the adversary who can take control of it.

4.2.13. Telnet

When a hacker establishes a Telnet connection to the drone system, he has immediate access to the system and can make changes to important system files and launch a shell code script utilizing parrot to wreak havoc. The drone's engines can be completely restarted by the invader under certain conditions, causing it to lose power and plummet into the ground.

4.3. Cyber Incidents on Drone

During testing, Schiebel's S-100 Camcopter was subjected to a suspected GPS jamming incident that caused it to crash into the ground control van. This incident resulted in the death of one schiebel enginner and injuries to two remote pilots. Lockheed Martin's RQ-170, a large fixed-wing UAV, was the target of an alleged GPS jamming and GPS spoofing attempt, which led to its capture with just minor left-wing damage (BinSaeedan et al., 2023). In September 2011, Creech Air Force Base in Nevada experienced one virus attack on GCS used for predator and reaper drone communication. In 2012, Iran attacked the scan eagle, a fixed-wing UAV by Boeing institute. On the hornet mini, a rotor-based UAV, a GPS Spoofing attack was carried out under controlled circumstances via adaptive flight, leading to a commanded drop (BinSaeedan et al., 2023). UT Austin's radio navigation lab is responsible for the attack in July 2012 at the white sands test facility in new mexico to show the hornet mini's weakness.

4.3.1. Cyber-Attack on Drone and Security Issues

In the ground control system, security threats take place due to various reasons like virus attacks, malware attacks, keylogger attacks, and Trojan attacks. Particularly in armed drone data hijacking, one of the major issues for the UAS. The most common cyber threat methods for communication links are identity counterfeiting, cross-layer attacks, hijackings, protocol-based assaults, and espionage. Similarly, attacks in the form of jamming, denial of service, and false are prominent among them. The use of drones is no longer restricted to laboratories or the military due to technological advancements. Hobbyists, pranksters, and troublemakers can also use them. As cyber-physical systems, drones depend primarily on the interaction between systems like aircraft/GCS and computing components like flight control computers, data links, and other computational systems for the accomplishment of their objectives (Siddappaji & Akhilesh, 2020).

In 2012, North Korea conducted a GPS jamming strike on the area it shares with South Korea, interfering with the navigation of aircraft, ships, and ground vehicles. The top 47 drone disasters between 2001 and 2013 were enumerated in a news report by the Washington Post. In December 2008, a significant incident occurred when members of a terrorist group based in Iraq were found to have intercepted a UAV feed. This marked the first prominent attack on a UAV system. Two years later, in December 2011, Iran announced that it had successfully brought down a US RQ-170 Stealth drone. An Israeli Heron Stealth, radar-evading drone that might have been modified and used against the US and its allies was shot down and captured, Iran claimed once more in 2014. Drones are now essential tools in many facets of contemporary life, such as disaster relief, trade, and defence. However, as the use of drones becomes more prevalent, the risk of cyber-attacks targeting these systems also increases (Johnson, 2019).

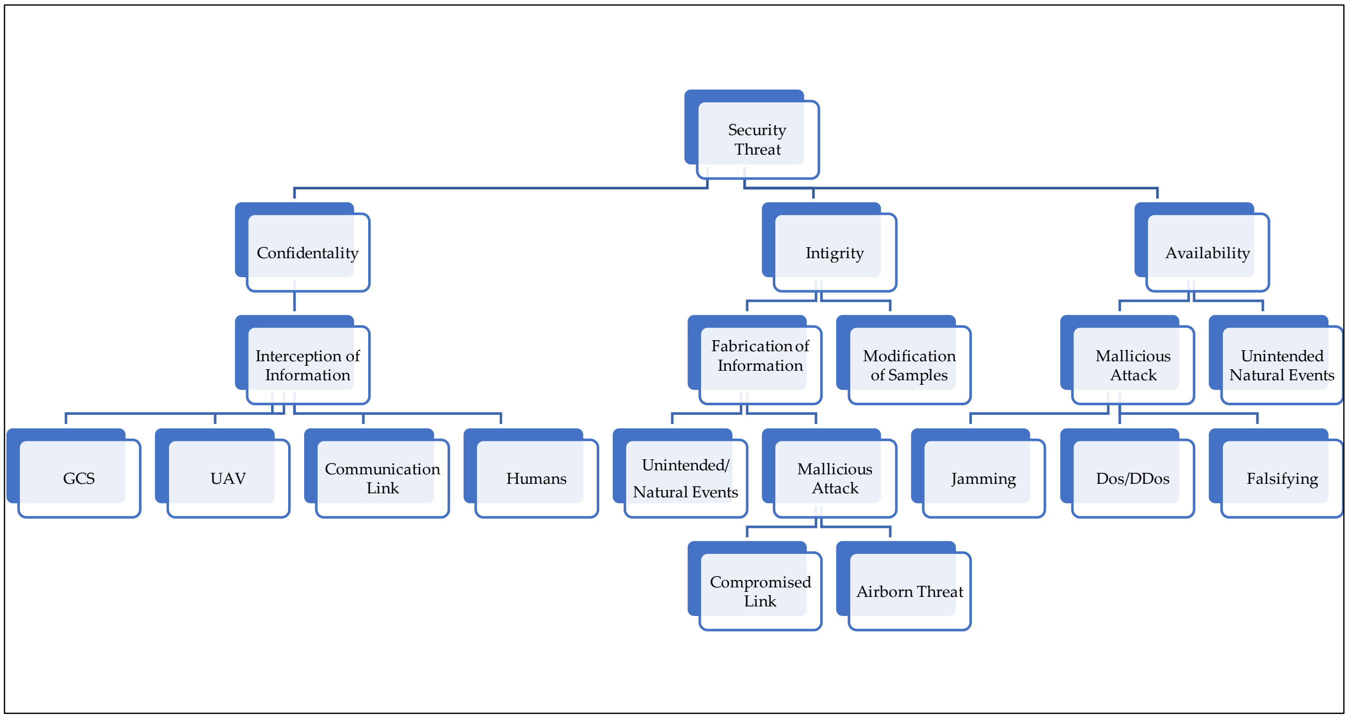


Fig. 6 Mechanism of cyber threat on drone

A successful cyber-attack on a drone can jeopardize national security, compromise sensitive data, and disrupt critical operations. Drones rely heavily on complex communication systems, data networks, and onboard computing capabilities. These interconnected components create vulnerabilities that cyber attackers can exploit. Unauthorized access is another problem that puts security threats to a country. Hackers might breach the drone's communication channels or ground control systems to gain unauthorized access and control over the UAV. This could lead to hijacking the drone's flight path, altering its mission, or shutting down its systems entirely. Data theft is one of the major problems that threaten the national security of a country (BinSaeedan et al., 2023). The drones often capture sensitive and classified information during their missions, including intelligence data and strategic reconnaissance.

Cyber attackers could intercept and steal this data, compromising national security and exposing critical assets. Armed drones carry weapons or deliver payloads, making them potential targets for cyber attackers seeking to tamper with the delivery mechanism or weapon systems, leading to disastrous consequences. A successful cyber-attack could disrupt drone operations, hindering their ability to carry out vital missions, such as disaster response, search and rescue, or border surveillance; with the manipulation of surveillance data, the operation may become unsuccessful. In a military context, drones play a crucial role in intelligence, surveillance, and reconnaissance missions. A cyber-attack that compromises these capabilities could result in a significant loss of strategic advantage on the battlefield. Drones are used in various critical infrastructure sectors, including energy, transportation, and telecommunications. An attack on drones operating in these areas could disrupt essential services and create chaos (Tu & Piramuthu, 2023). Unauthorized access to drones' surveillance capabilities can infringe upon citizens' privacy and raise concerns about mass surveillance and abuse of power. The commercial use of drones is growing rapidly, contributing significantly to various industries. A cyber-attack on drones used for commercial purposes could lead to financial losses and undermine economic stability.

4.3.2. Mitigative Measures

Data Encryption and Secure Communication

Employing strong encryption techniques for communication between control stations and drones is essential. This prevents unauthorized access to private information and directives, lowering intercept risk or manipulation by malicious actors.

Authentication and Authorization

Implementing multi-factor authentication and stringent authorization protocols ensures that only authorized personnel can access and operate armed drones, preventing unauthorized parties from assuming control of the drone's functions.

Redundancy and Fail-Safe Mechanisms

Designing armed drones with redundant systems and fail-safe mechanisms can prevent catastrophic consequences in the event of a cyberattack. These mechanisms can include safe return-to-base procedures or the ability to operate independently in case of communication loss.

Securing Supply Chains

Ensuring the security of the entire supply chain, from manufacturing components to assembling and deploying drones, is essential. A compromised supply chain can lead to compromised drones and vulnerabilities.

Robust Cybersecurity Protocols

Drone manufacturers should make cybersecurity a top priority during the design and development phases of UAVs. This involves integrating encryption, authentication, and secure communication protocols to safeguard against unauthorized access.

Regular Software Updates

Regular updates and patches should be applied to the drone's software and firmware to address vulnerabilities and stay ahead of potential cyber threats.

Training and Awareness

Operators of drones and personnel involved in managing UAV operations should receive comprehensive training on cybersecurity best practices and be aware of potential threats.

Collaboration and Information Sharing

Governments and industries must collaborate to share information about cyber threats and vulnerabilities to foster a collective defence against cyber-attacks on drones.

5. Conclusion

In conclusion, it can be argued that implementing robust cybersecurity measures for armed drones is of paramount importance in today's technologically advanced and interconnected world. Cybersecurity for armed drones is an imperative safeguard in modern warfare. As these unmanned aerial systems become integral to military operations, their vulnerability to cyber threats grows. As armed drones become increasingly integrated into military operations, they present both strategic advantages and potential vulnerabilities. Cybersecurity for armed drones is an evolving challenge that requires a multi-faceted approach that integrates advanced cybersecurity measures, promotes awareness, and fosters international cooperation. It is possible to reduce the dangers of cyber threats and ensure the security and effective deployment of armed drones in military operations. In a nutshell, it can be admitted that safeguarding armed drones through comprehensive cybersecurity strategies is vital to maintaining military efficacy and preventing potential risks posed by cyber adversaries.

References

[1] Amina Khan, "*The Ambiguity in International Law and Its Effect on Drone Warfare and Cyber Security*," Thesis, Western University, pp. 1-61, 2023. [Google Scholar] [Publisher Link]

[2] Ankit Kumar, "Drone Proliferation and Security Threats," *Indian Journal of Asian Affairs*, vol. 33, no. 1/2, pp. 43-62, 2020. [Google Scholar] [Publisher Link]

[3] Apoorvaa Singh, Chandana Priya Nivarthi, and K.B. Akhilesh, "Implementing IoT in India-A Look at Macro Issues and a Framework for Recommendations," *Smart Technologies*, pp. 35-52, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[4] Bora Ly, and Romny Ly, "Cybersecurity in Unmanned Aerial Vehicles (UAVs)," *Journal of Cyber Security Technology*, vol. 5, no. 2, pp. 120-137, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] B. Siddappaji, Pinosh Kumar Hajoary, and K.B. Akhilesh, "UAVs/Drones-Based IoT Services," *Smart Technologies*, pp. 159-167, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Elham Kariri, "IoT Powered Agricultural Cyber-Physical System: Security Issue Assessment," *IETE Journal of Research*, pp. 1-11, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Edwin Vattapparamban et al., "Drones for Smart Cities: Issues in Cybersecurity, Privacy, and Public Safety," *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Paphos, Cyprus, pp. 216-221, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[8] Fallou Thiobane, "*Cybersecurity and Drones*," Ph.D. Thesis, Utica College, 2015. [Google Scholar] [Publisher Link]

[9] Hanna Martyniuk et al., "Analysis of Threat Models for Unmanned Aerial Vehicles from Different Spheres of Life," *Advances in Computer Science for Engineering and Education VI*, pp. 595-604, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Jay Gundlach, *Designing Unmanned Aircraft Systems*, Aerospace Research Central, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[11] James Johnson, "The AI-Cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability," *Journal of Cyber Policy*, vol. 4, no. 3, pp. 442-460, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Jeppe Teglskov Jacobsen, and Jens Ringsmose, "Cyber-Bombing ISIS: Why Disclose what is Better Kept Secret?," *Global Affairs*, vol. 3, no. 2, pp. 125-137, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[13] Jonathan Walatkiewicz, and Omar Darwish, "A Survey on Drone Cybersecurity and the Application of Machine Learning on Threat Emergence," *Proceedings of the 2023 International Conference on Advances in Computing Research (ACR'23)*, pp. 523-532, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Jean-Paul A. Yaacoub et al., "Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations," *International Journal of Information Security*, vol. 21, pp. 115-158, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Jean-Paul Yaacoub et al., "Security Analysis of Drones Systems: Attacks, Limitations, and Recommendations," *Internet of Things*, vol. 11, pp. 1-39, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Kim Hartmann, and Christoph Steup, "The Vulnerability of UAVs to Cyber Attacks Approach to the Risk Assessment," *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, Tallinn, Estonia, pp. 1-23, 2013. [Google Scholar] [Publisher Link]

[17] Mary Ellen O'Connell, "21st-Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and WMDs," *13th Global Studies Law Review*, vol. 515, pp. 1-21, 2014. [Google Scholar] [Publisher Link]

[18] Martti Lehto, "Drones in the Cyber Security Environment," *Cyberwatch Magazine*, vol. 2019, no. 4, pp. 8-17, 2019. [Google Scholar] [Publisher Link]

[19] Manimaran Mohan, "*Cybersecurity in Drones*," Ph.D. Thesis, Utica College, 2016. [Google Scholar] [Publisher Link]

[20] Mariusz Pyzynski, and Tomasz Balcerzak, "Cybersecurity of the Unmanned Aircraft System (UAS)," *Journal of Intelligent & Robotic Systems*, vol. 102, pp. 1-13, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Moritz Weiss, "The Rise of Cybersecurity Warriors?," *Small Wars & Insurgencies*, vol. 33, no. 1–2, pp. 272–293, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Nader S. Labib et al., "The Rise of Drones in the Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles," *IEEE Access*, vol. 9, pp. 115466-115487, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] Paolo Crippa, "Cyber Security and Drones," *Handbook of Security Science*, pp. 619-633, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Rizwan Majeed et al., "Intelligent Cyber-Security System for IoT-Aided Drones Using a Voting Classifier," *Electronics*, vol. 10, no. 23, pp. 1-19, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] Ryan Shaffer, "Drone Activity and Cyber Terrorism," *Terrorism and Political Violence*, pp. 1-6, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] Arnolnt Spyros, "*A Study of Cybersecurity Threats in UAVs and Threat Model Approaches*," Master Thesis, School of Science & Technology, International Hellenic University, 2023. [Google Scholar] [Publisher Link]

[27] Susheela Dahiya, and Manik Garg, "Unmanned Aerial Vehicles: Vulnerability to Cyber Attacks," *Proceedings of UASG 2019*, pp. 201-211, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[28] Vikas Sihag et al., "Cyber4Drone: A Systematic Review of Cyber Security and Forensics in Next-Generation Drones," *Drones*, vol. 7, no. 7, pp. 1-29, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[29] Wojdan BinSaeedan et al., "Security Challenges for UAV Systems Communications: Potential Attacks and Countermeasures," *Unmanned Aerial Vehicles Applications: Challenges and Trends*, pp. 269-288, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[30] Wasswa Shafik, S. Mojtaba Matinkhah, and Fawad Shokoor, "Cybersecurity in Unmanned Aerial Vehicles: A Review," *International Journal on Smart Sensing and Intelligent Systems*, vol. 16, no. 1, 2023. [CrossRef] [Google Scholar] [Publisher Link]