DIGITAL TWIN TECHNOLOGY

Chapter 7:
Digital Twin and the Detection and Location of DoS Attacks to Secure Cyber-Physical UAS

***Gita Donkal**, Chandigarh University*
***Anjali Donkal**, National Institute of Technology*

Presented by: Oscar Llerena

Content

7.1. Introduction

- Digital twin technology (DTT) is also known as computational mega model, avatar, device shadow, synchronized virtual prototype or a mirrored system (Michael Grieves, 2002).
- DTT is the most immediate digital representation of an actual system and if a hacker procured the twin, then, it will serve as a prototype to the original system.
- DoS and spoofing are cyber-attacks that could be ignored for a while when launched on civil applications, but when they target military of a nation, indeed it is not possible to ignore them anymore.
- UAVs functionality can be compromised by DoS attacks: incapacitate network availability, GPS navigation system, video streaming operations display false negative data, etc.
- Moreover, autonomous aerial vehicles these days can be trained to be smart enough to detect and prevent adverse autonomous activities, caused by DoS attacks.

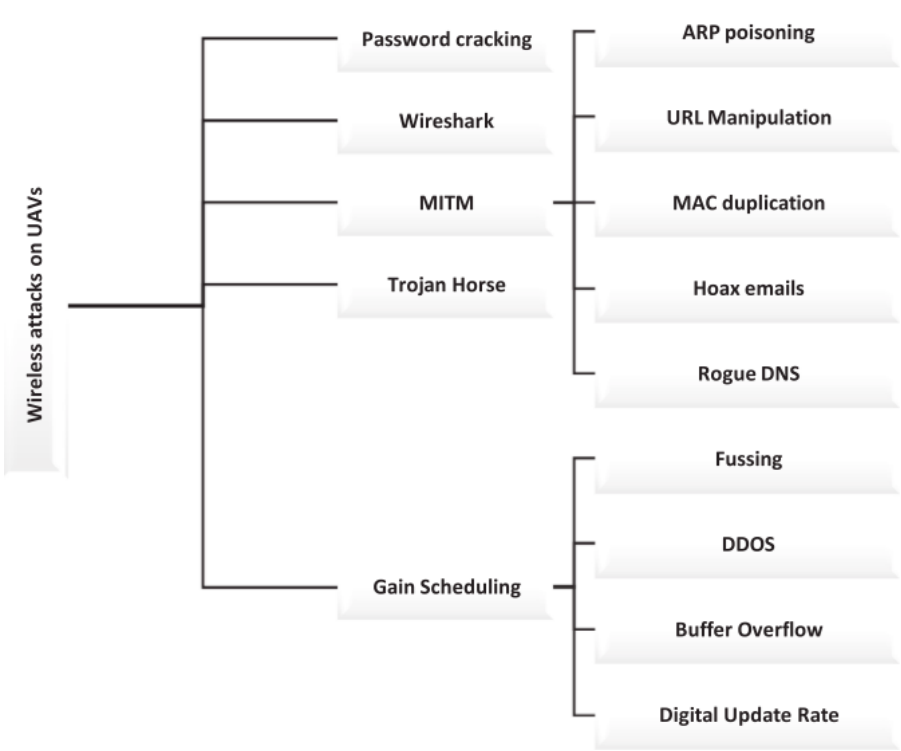

Figure 7.1. Multifarious wireless attacks on UAVS

7.1. Introduction

- The aim is also to study more about GPS and GNSS systems since they will be used to detect and mitigate spoofed attacks.
- Figure 7.2 shows a simplified diagram of GPS spoofing attack, where the attacker has overpowered an authentic GPS signal and represents three different scenarios.
- First scenario, the attacker is launching a form of DoS attack, which is a GPS spoofing attack.
- Second scenario, the adversary has succeeded in spoofing the trajectory of the UAV that was on its way to the original trajectory but instead of reaching to its legitimate and un-spoofed destination, it has reached to a spoofed destination, where this UAV can be hijacked and can be used for reconnaissance by the adversary.
- In third scenario, this attack needs to be dealt with a strong mitigation technique, so that the UAV can be put back on its original and non-malicious trajectory.
- However, the true potential of an attacker is always unknown as there are anonymous ways to launch DoS attacks.

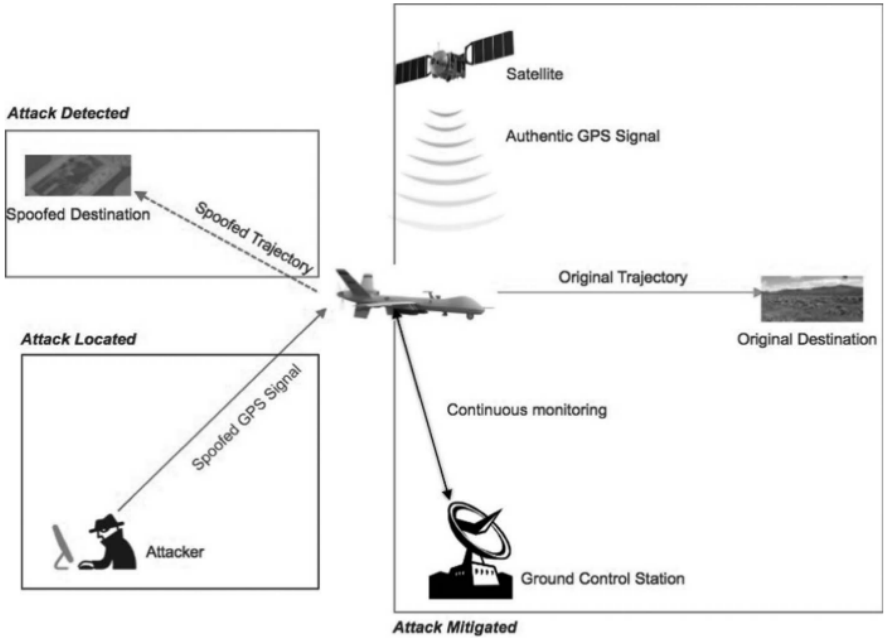

FIGURE 7.2 Attacker compromising a UAV using spoofed GPS signal.

7.2. Related Terminologies

7.2.1 Digital Twin and Unmanned Aerial Vehicles (UAV)

- A Digital Twin is considered as a multiscale, incorporated multi-physics, probabilistic simulation of an as-built system. It makes use of the best available sensor updates, physical models, fleet history, etc. for mirroring the life of its corresponding flying twin.
- Cyber-physical systems (CPS) are new-generation systems incorporated with physical and computational capabilities. UAVs are CPS as they are reliant on the interaction between physical and computational elements.
- Figure 7.3 depicts the modelling framework of a cyber-physical system. It helps in understanding the layout of interactions taking place between its two integral components, including physical space and cyber space.
- UAVs can be flown by a remote pilot.
- UAVs are embedded with cameras and sensors.

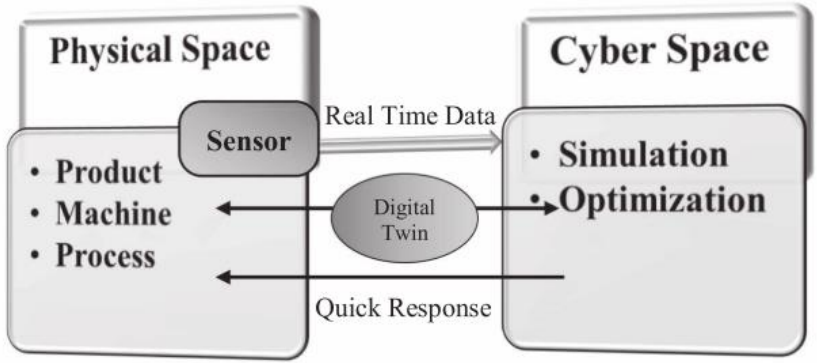

FIGURE 7.3 Modelling framework of the cyber-physical system [6].

7.2. Related Terminologies

7.2.2 Challenges with Current Technology/UAVs

- Record low false negatives and false positives.
- Adaptation of novel circumstances (to generalize), including degradation or failures of subsystems.
- Learning from past experiences and effective integration.
- Promptness and availability of system data with on-board processing resources for analyzing data trends.
- Anticipation of futuristic events such as predictive modelling of imminent faults.

7.2.3 Pros of Digital Twin

- DTT is a specimen that considers performance, structure, mission-specific characteristics including malfunctions confronted, miles covered, and restoration and maintenance history of the physical twin.
- It assists in preventive maintenance schedule based on knowledge of the behavior and history of systems' maintenance.
- DTT allows understanding how physical twin performs, and the expectancy of its performance in the future.
- Traceability is ensured amongst different phases of life cycle via connectivity, facilitated by digital thread.
- Refined conjectures can be provided along with predictive analytical data and they can be further assimilated in the DTT to analyze in parallel to other information sources, for making predictions about performance of system in the future.
- It is also capable of troubleshooting malfunctions confronted by remote equipment along with their maintenance.
- Physical systems' data and IoT data is combined using DTT that facilitates service optimization, manufacturing processes and identification needed for design enhancements.
- It assimilates the operational and maintenance data from the tangible systems into its models and simulations.

7.2. Related Terminologies

7.2.4 Detection System for UAVs

7.2.4.1 Satellites

- Satellites are majorly used for navigational purposes to locate exact longitudes and latitudes.
- GNSS comprises a constellation of orbiting satellites in conjunction with a network of ground station. Radio Detection and Ranging (RADAR) technology in drone will signal that enough drone GNSS satellites have been detected.
- There are three types of return to home techniques that include pilot initiated returned to home (R2H) by pressing button on remote controller or in an application. Second, low battery level, where UAV will fly back automatically back to home and third, laws of transmission between UAV and remote controller ensure that the UAV flies back automatically to its home point.
- To avoid obstacles, UAV makes the use of vision sensor, ultrasonic, infrared, Light Detection and Ranging (LIDAR), time of flight and monocular vision, also including GPS, speed of movement, increased level of computational functionalities and much more. To be more cautious, one can always use multiple GPS satellites to provide better coverage, generation of rogue signal to mislead or block GPS device and military GPS systems can rely on encrypted signals.

7.2. Related Terminologies

7.2.4 Detection System for UAVs

7.2.4.2 Kalman Filter Algorithm and RADAR

- It is named after Rudolph E. Kalman and used for optimal estimation of location, speed and direction. It is used to estimate the trajectories of manned spacecraft to the moon and back.
- To constantly track and acquire trajectory information can be called as state estimation problem. For filtering stochastic measurement errors in linear radar systems, Kalman filter has been adopted. For practical applications, non-linear systems are more common.
- In order to filter random errors for motion models, Kalman filter and its variants can be assimilated. The same approach can also be used to track UAVs with mobile radars.
- Radar is one of the most integral detection systems of UAVs that are used for surveillance purposes. Radar is also capable of performing multimode operation including range detection, Doppler sensing, SAR mapping, etc.

7.3. Taxonomy for Cyber-attacks on UAVs/DTT

- Four major factors that these attacks can affect include confidentiality, integrity, availability, and authenticity.
- Confidentiality ensures reading the content of a secret message by only authorized entities.
- Integrity checks for the undetected alteration of the content of a message when it is being transmitted via network.
- Availability is accountable for ensuring the availability of resources whenever they are requested by a legitimate user.
- Authentication is the mandatory duty of a receiver to confirm that the data received is from the correct and u n-spoofed sender.
- Assume a scenario, where a hacker successfully exploits the susceptibilities in a DTT, then the hacker will leverage this potential and uncover the organization to the core system attacks. These DTT based systems are directly called by the twin and this threat will just unlatch the gates of backend/ core systems to an attacker.
- Code analysis, popularly known as reverse engineering is one of the most probable attacks on all platforms.
- Software designed for Linux OS or Windows can be conveniently reverse-engineered. The associated parties must acknowledge some foundational guidelines while designing and implementing digital twin.
- Attacks are categorized in two types that can threaten entire cyber-physical model. Attacks can threaten infrastructure from its infrastructure to its software.

7.3. Taxonomy for Cyber-attacks on UAVs/DTT

7.3.1 Active Attacks

- They target integrity, authenticity and availability of data that can be done using modification, fabrication and interruption respectively. Modification in data compromises integrity of data that can be done by fraudulently forging information. Fabrication affects authenticity aspect and can be executed, using counterfeited messages, UAV spoofing, GPS spoofing and much more.
- Active eavesdropping aims to attack the main channel by degrading the channel capacity. An active eavesdropper may also aim to improve the capacity of the eavesdropping channel.
- An active eavesdropper is transmitting the jamming signals to the legitimate receiver in order to degrade the main channel's capacity.

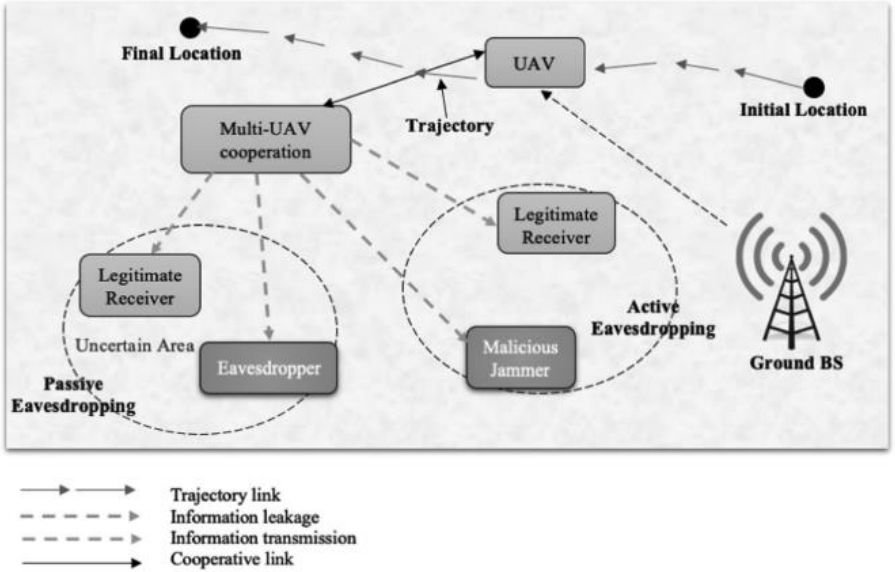

Figure 7.5 Illustration of Active and Passive eavesdropping leading to attacks like GPS spoofing.

7.3. Taxonomy for Cyber-attacks on UAVs/DTT

7.3.2 Passive Attacks

- Interception can be carried out using traffic analysis, eavesdropping, launching viruses, malware, trojans, etc..
- Eavesdropping can be executed using man-in-the-middle attack where the interception of data being transmitted between the transmitter and receiver nodes is done by an illegitimate, unauthenticated person and the attacker is illegally permissible to gather critical information of control systems, software, data and much more.
- In traffic analysis scenario, an attacker can locate critical nodes of a wireless sensor network (WSN) in a UAV. Infecting valuable systems and software of a CPS with viruses like trojans and malwares can affect the overall functioning of CPS.
- A synthetic aperture radar equipped on the UAV can help detecting and tracking the positions of potential external eavesdroppers.
- Passive countermeasures are designed to safeguard the UAVs indirectly that includes physical protection, sensor jamming, cyber-spoof of signals for GPS.

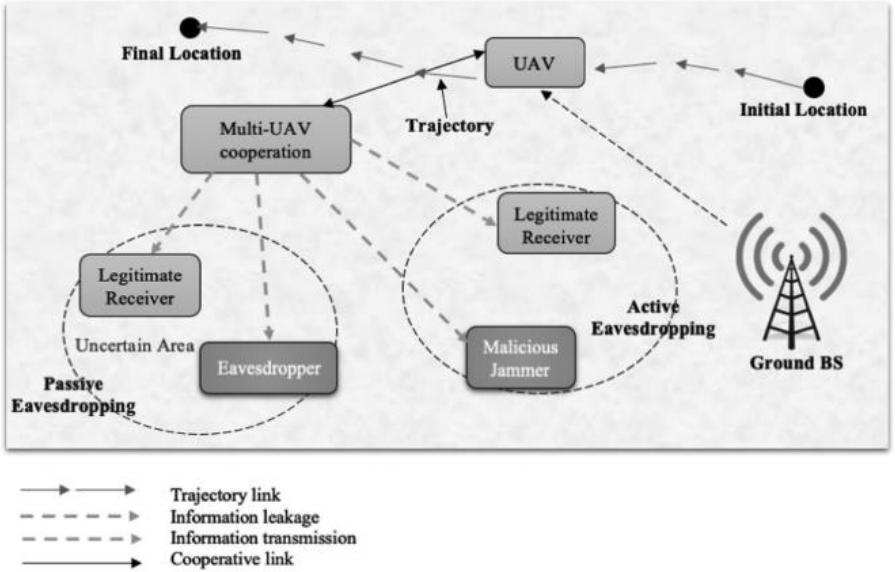

Figure 7.5 Illustration of Active and Passive eavesdropping leading to attacks like GPS spoofing.

7.3. Taxonomy for Cyber-attacks on UAVs/DTT

7.3.3 Man-in-the-Middle Attack

- Rodday (2016) launched a MITM attack on a UAV.
- This attack violates authentication protocols and standards that allows secure communication between the operator (user) and the UAV.
- As shown in Figure 2 from Paper: Exploring Security Vuln. of UAVs., in order to perform a MITM attack on the XBee 868LP chips, they used “Remote AT Commands”.
- This feature allows for the attacker to remotely change internal parameters of the XBee chips, such as destination high (DH) and destination low (DL), and therefore reroute any traffic.
- The write command persists changes within memory, allowing for two different attack modes: temporary or persistent.
- Authors were able to match commands transferred through the telemetry channel with specific functions within the UAV system. This enables an attacker to alter existing packets in a meaningful way, or inject new packets to communicate with the flight computer.

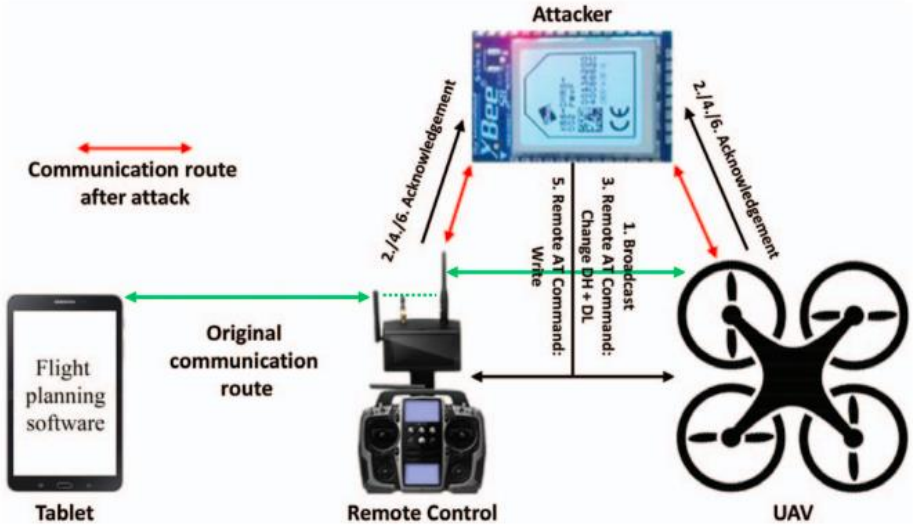

Fig. 2. Man-in-the-Middle attack

Exploring Security Vulnerabilities of Unmanned Aerial Vehicles

Nils Miro Rodday, Ricardo de O. Schmidt and Aiko Pras
Design and Analysis of Communication Systems
University of Twente, the Netherlands
rodday@arcor.de, {r.schmidt,a.pras}@utwente.nl

7.3. Taxonomy for Cyber-attacks on UAVs/DTT

7.3.4 Denial of Service (DOS)

- DoS attack is capable of causing widespread disruption. It can disrupt traffic flow, prevent important communications.
- Since DoS attack targets communication layers, it is very much possible to target any of the communication layers including physical link and network layer.
- Jamming attacks interfere with legitimate signals.
- IP Spoofing attack lead to discrepancy during navigation.
- Vampire attack can drain battery of UAVs.
- TCP/SYN flooding sends synch messages to the victim.
- Path-based DoS Attack injects fake and replayed packets.
- Wormhole attack. the two rogue nodes identify a distant location with a single jump that can misguide other nodes on original distances between two nodes.
- Black hole attack: An illegitimate node is inserted in the network that modifies the routing table, forcing adjacent nodes to route the information through it.
- Gray hole attack is an improved variant of black hole attack.

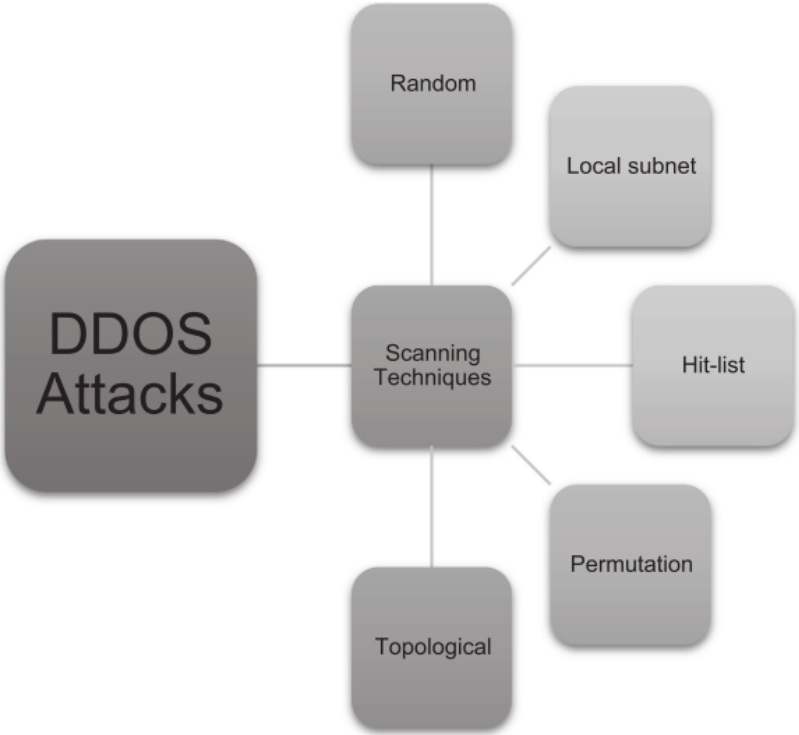

FIGURE 7.6 Different scanning techniques for DDoS attack.

7.3. Taxonomy for Cyber-attacks on UAVs/DTT

7.3.5 GPS Spoofing

- GPS spoofing mainly targets a cyber-physical system that relies excessively on GPS for positioning and navigation.
- Attackers are capable of spoofing GPS signals by transmitting fake or spoofed coordinates to the flight controller and taking over the full control of UAS.
- Rogue Updates: A network attack where an attacker deliberately introduces rogue device or rogue nodes to the interconnected network. Software updates for control system in UAVs are taken by attacks to introduce malicious updates.
- OBD port Exploitation: On-board Diagnostics (OBD) is physically located in a car that controls Engine Control Unit (ECU) and OBD. OBD can modify code-base responsible for engine, lighting and breaking functionality.
- Close proximity vulnerabilities: Signal jamming works by deliberately blocking, jamming or interfering with the authorized communication among connected devices. This kind of vulnerability can be exploited when exposed via short-range communication.
    - Possible solution of jamming attack can assimilate the detection of intended signal in environments where there is a large volume of noise. To prevent spoofing attacks and GPS jamming attack, integrated sensors can be used.
    - Hacking and infiltrating CPS affects the responsibility, liability, data ownership and privacy of systems. Sensors and actuators handling task including network embedded systems are connected with each other through internet.

7.3. Taxonomy for Cyber-attacks on UAVs/DTT

7.3.5 GPS Spoofing

TABLE 7.1
Different Mitigation Techniques to Prevent Cyberspace Spoofing Attacks

Authors	Methodology	Advantages	Drawbacks/Future Scope
Javaid et al. [55]	Receiver Autonomous Integrity Monitoring (RAIM) algorithm is used that determines integrity of GNSS solution. RAIM algorithm makes a comparison among pseudo-range measurements ensuring they all are consistent. RAIM exercises fault detection mechanism on computed set of navigational solutions isolating faulty satellites and providing mitigation level computation.	Integrity of position calculation using GNSS can be determined successfully. Once packets are received, RAIM is capable of detecting any attacking host.	For future scopes, further improvement of RAIM algorithm with quicker detection and correction can be considered.
Tanil et al. [44]	Use of aircraft autopilot response to deceptive trajectory to locate or detect GNSS spoofing attack. A tightly coupled INS-GNSS integration in Kalman filter is utilized to monitor spoofing attacks. It also investigates the impacts on spoofing attack detection due to aircrafts' dynamic response to control actions that are actuated by pilot/autopilot.	Even in worst case scenarios, spoofing attacks can be directly detected by the aircraft autopilot that provides a response to faulted GNSS signals.	
Mukherjee et al. [54]	It demonstrated three particular DoS attacks that uses J1939 data-link layer request and connection management protocols. Program ECU to drop incoming packets' request, lest already responded to the request from the same source address in a fixed interval of time.	This technique is useful to prevent overloading scenarios.	It can lead to exhaustion of resources as ECU will have to maintain state information.
He et al. [37]	A combination of visual sensor and IMU as a fusion of information in order to solve GPS spoofing issues.	Efficient use of UAV's own sensors with no auxiliary equipment requirement. Light weighted fusion algorithm. This approach can withstand sophisticated GPS spoofing attacks with acquisition of real-time flight speed.	Error accumulation during integration process. Gradual increase in cumulative error.

7.4. Penetration Testing with Kali Linux

- Three aspects have been considered in order to proceed with proposed methodology. These include detection, location and mitigation of DoS attack.

7.4.1 DETECTION OF DOS ATTACK

- Since a ground control station remains in a continuous contact with remotely controlled aircraft to monitor the position, velocity and the particular time at which the UAV is flying, therefore these three parameters can be used to detect the launched attack.
- Time: Whenever a UAV is in motion, it gets a request from the control station to change its altitude, direction or position in a specific time frame to monitor the navigation of UAV. However, when it comes to a DoS attack, this motion request can come in short intervals of time over and over that can perplex its navigational senses. Assessing the overall counts of requests coming to the navigational sensor of a UAV, a DoS attack can be detected with much ease.
- Velocity: Since the users monitoring a UAV from a ground control station know the exact speed at which the unmanned aircraft is flying such as 3 km/ s or 2,000 km/ h, it gets convenient for them to determine their exact arrival time at the destination. Now, if a UAV takes a detour or does not follow the original path, then its velocity can show fluctuations along with its arrival time. The velocity or angular velocity of a UAV is always synchronized with time and displacement, and if the unmanned drone is under a cyber-attack which is affecting the velocity of UAV showing frequent changes in the direction of drone on remote controller's screen, then it can be used to identify that a spoofed attack has been launched on a particular.
- Position: An unmanned airplane that is being monitored by a ground control station will definitely be affected by its sudden change in displacement that can affect the coordinates of the unmanned drone. The drone which is under a constant surveillance of control station will know immediately that an unplanned displacement with directional changes of the UAV is nothing but a spoofed cyber-space attack.

7.5. Location of DoS attack

- To detect a GPS spoofing attack, the incoming packet needs to be inspected so that useful details like source address, destination address, sequence number, hop counts and payload can be utilized to predict the provenance of attack so as to track down the attacker.
- LASER is used to provide elevation information with higher accuracy to improve GNSS navigational system. Besides, Navy uses laser gyroscopes, where there is no GPS signal availability
- The spoofed IP address can be tracked down, using a networked GPS and GNSS that can be used further to get the measurements of the position of the attacker's unmanned drone. These laser gyrocompasses can be upgraded and brought into use for detecting the location of other UAV that is launching the attack. Also, Laser Range Finders (LRF) can be used to determine accurate range and angle information.
- In order to use a laser in a combination with the networked GPS, we need to perform some mathematical formulations and development of executable algorithms is a must that can trace the IP address and location of the attacker’s UAV both in minimum time with no time delays at all since these armed UAVs have flight time constraints.

7.6. Demonstration of DoS Attack on UAVs

7.6.1. MITM Attack Using Ettercap on Kali Linux By ARP Poisoning

7.6.1.1 Locating Open Ports

- Nmap commands can be used on an identified host in a specified network that can assist in locating open ports.

7.6.1.2 NMAP

- Ettercap is a comprehensive suite to perform MITM attacks on local network. It sniffs live connections, content filtering and much more. It supports both active and passive dissection of various protocols.
- Figure 7.8 depicts port stealing on victims' network and targets that have been ARP poisoned.
- Since ARP poisoning allows you to spoof ARP of a device, hence all the incoming traffic on target's network will be redirected to adversary's network that will become a vantage point for the attacker.

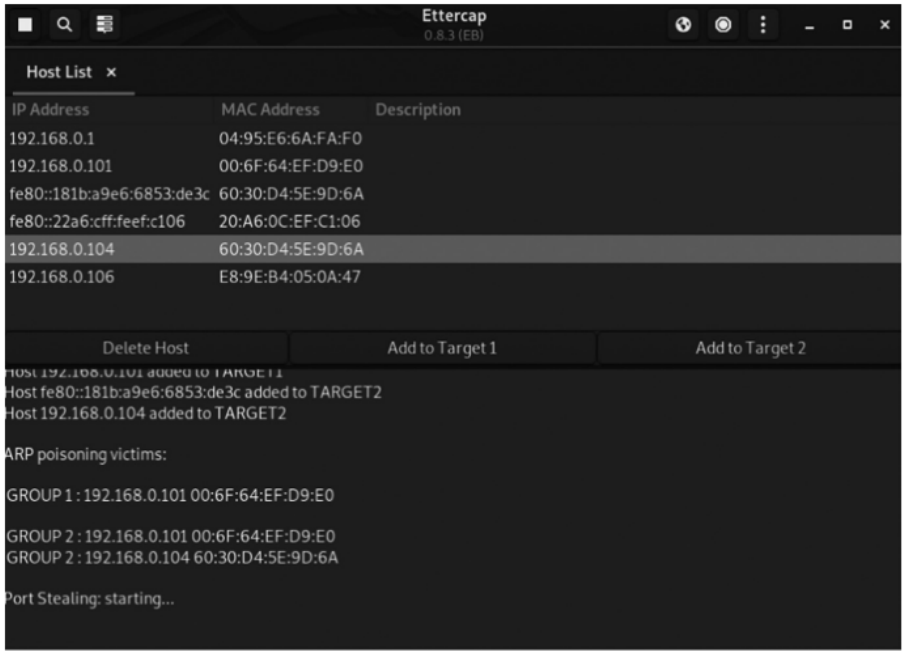

FIGURE 7.8 MITM attack using Ettercap.

7.6. Demonstration of DoS Attack on UAVs

7.6.1. MITM Attack Using Ettercap on Kali Linux By ARP Poisoning

7.6.1.2 NMAP

- Figure 7.9 shows unified sniffing on remote connections using MITM attack, using ARP spoofing technique.
- It also represents that currently during the attack, nearly 57 ports are being monitored.
- There are 24609 mac vendor fingerprints under surveillance.

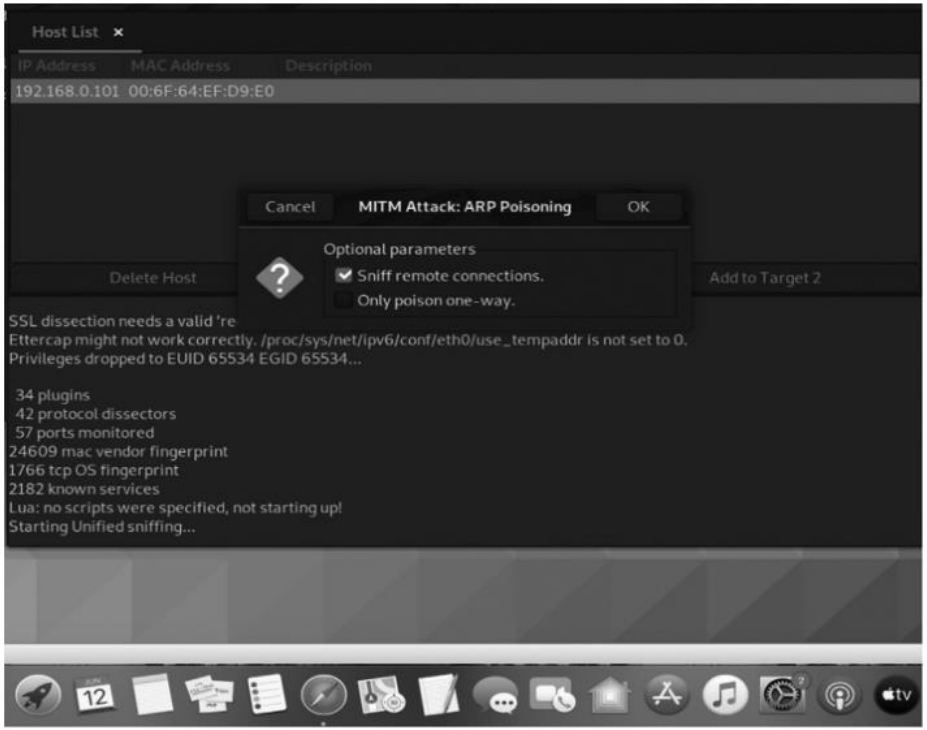

FIGURE 7.9 Unified sniffing on remote connections using MITM attack, using ARP spoofing technique.

7.6. Demonstration of DoS Attack on UAVs

7.6.1. MITM Attack Using Ettercap on Kali Linux By ARP Poisoning

7.6.1.2 NMAP

- Figure 7.10 demonstrates how packets can be captured using Wireshark and Ettercap. Wireshark is used to capture packets of any kind on any port and Ettercap can be used to spoof the ARP or IP address of that specific packet. Below, you can find some scanning techniques including cookie-echo scan, TCP scan, idle scan and many more can be explored using Kali.
- This empirical analysis demands us to concentrate more on reinforcement of cyber security tactics that includes using strong underlying infrastructure, foolproof protocols, updated software, VPNs, DMZs, strong firewalls, multi-level authentication and much more.

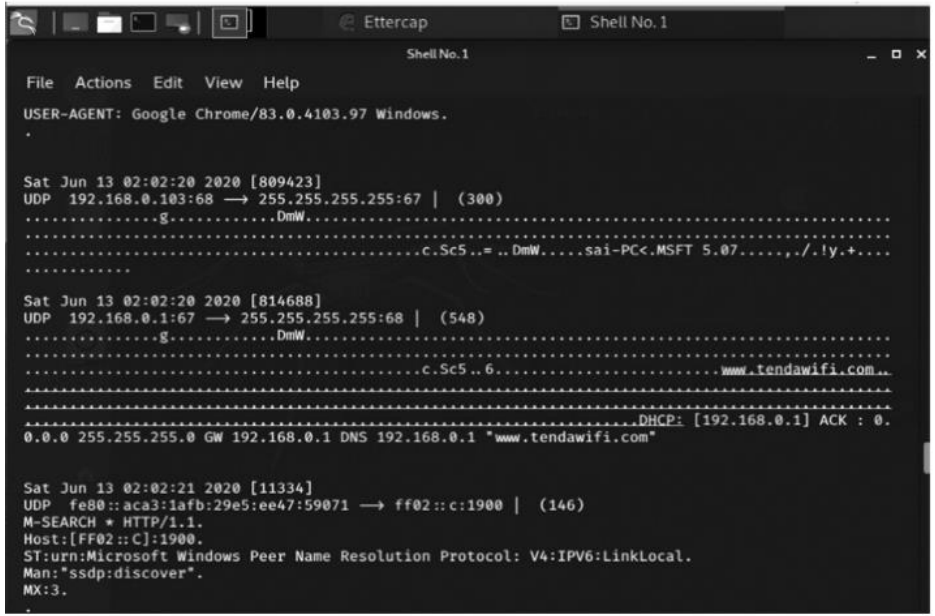

FIGURE 7.10 Packets captured using Wireshark and Ettercap

7.7. Conclusion and Future Scope

- To recapitulate, after going through various research papers, including different methodologies, we were able to come up with some of the techniques to cope up with the most disrupting attacks i.e., DoS attack, where the legitimate user has no control over the unmanned drone leading to disastrous and dire consequences.
- With the existence of multifarious techniques and methodologies to cope up with DoS attack, it gets more befuddling that which technique should be adopted and how to proceed with a particular methodology that may or may not be compatible with the aspects of dealing with detection and location of a DoS attack.
- For detection and location of an attacker in order to identify the spoofed IP-based DoS attack, the development of a much efficient and effective algorithm designed in collaboration with laser and networked GPS is much needed.
- For future directions, aspirants can work on mitigation of DoS attacks with the concept of advanced whitelisting and blacklisting concepts, and hashing function based advanced hash tables.
- Moreover, the propounded research is also flexible enough to explore several methods, for instance, the model can be enhanced to be employed for prevention against Distributed Denial of Service (DDoS) attacks by considering a greater number of sources of attacks generated that include ample number of spoofed IP packets.
- Keeping the baseline parameters, several techniques can be explored, including fuzzy logics, packet filtering techniques, kernel inspection methods, IDS with entropy-based systems and much more to cope with DDoS attacks on a UAV.