



37. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2025. április 22–24.
Nemzeti Közzolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

**The possibility of developing a new generation of protection against
swarms of drones**

JELIGE: qwertyz

2024.11.18.

Table of content

Introduction - topicality of the topic	4
Introduction.....	4
Goal of this Paper.....	4
Use of drones in the Russia-Ukraine war	4
1. Technological structure of Uavs	6
1.1. UAVs categorized by usage	6
1.2. Types of UAVs.....	7
1.3. Structure of electric UAVs.....	8
2. OSI model	9
3. Possibilities to interfere with drones – Electronic Countermeasures.....	10
3.1. Denial of service attacks comparison in cyber space	11
4. Presentation of developed methodology: Deauthentication attacks	12
4.1. Introduction to IEEE 802.11	12
4.1.1. General Characteristics and authentication.....	12
4.2. Deauthentication and disassociation frames in the IEEE 802.11	15
4.2.1. IEEE 802.11i Security Amendments – Robust Security Framework	16
4.2.2. IEEE 802.11w – Protected Management Frames	17
4.3. The frame structure according to standard.....	18
4.4. DEAUTHENTICATION BASED ATTACK IN OTHER RESEARCHES.....	18
4.5. Result of the previous research	19
4.5.1. Equipment used in the research.	19
4.6. Graphical representation of the used hardware and software	20
4.6.1. Process description – Vulnerability research	20
4.6.2. Preparation for the measurement	21
4.6.3. Results of the experiment.....	21
4.6.4. Limitations of the measurements	22
4.6.5. Evaluation of measurement.....	23
4.7. Graphical representation of the measurements	23
5. New oppurtunaties agains UAV swarms	24
5.1. IEEE 802.11 Multicast standard overview.....	24
5.1.1. Multicast Group Concept.....	24

5.1.2. IP Multicast Addresses	24
5.2. Layer 2 multicast address.....	25
5.3. Theory of IEEE 802.11 multicast deauthentication	25
5.4. proposed method	26
6. architectural design for a finished solution.....	27
6.1. Visions behind the new system and capability requirements.....	27
6.2. Design and architectural patterns used.....	27
6.2.1. Docker Containers	27
6.2.2. Microservice architecture.....	27
6.2.3. gRPC	28
6.3. Design figure and description	29
Summary, presentation of the results of the thesis	30
ACKNOWLEDGMENT.....	30
References.....	31

INTRODUCTION - TOPICALITY OF THE TOPIC

INTRODUCTION

The rapid advancement of drone technology over the past few decades has transformed modern warfare and conflict landscapes. The ISR (Intelligence, Surveillance, Reconnaissance) UAVs (Unmanned Aerial Vehicles) evolved in a variety of use cases. Some UAVs have Electronic Warfare (EW) capabilities, some UAVs are used as C3/C4 (Command, Control, Communication, Computers) points, some are equipped with variety of weapons systems like rockets for targeted strikes, or smaller UAVs are equipped with only just a hand grenade. But we can draw the conclusion, that with the rapid development of Electrical Engineering and Computer Science these UAVs are becoming more powerful than ever.

GOAL OF THIS PAPER

The goal of this paper is to develop a new method to counter UAV/UAS attacks and to create the ability to hijack UAVs that uses IEEE 802.11 based communication.

USE OF DRONES IN THE RUSSIA-UKRAINE WAR

In the Russia-Ukraine war we can clearly see that the UAVs are used heavily by both parties. CNN wrote that at November 10th, that there was a record number of UAVs exchanged by the parties. At that night Russia launched 145 “Fire and Forget” preprogrammed attack drone. According to the information provided by the Ukrainian Defense Forces only 62 drones were shot down.[1]

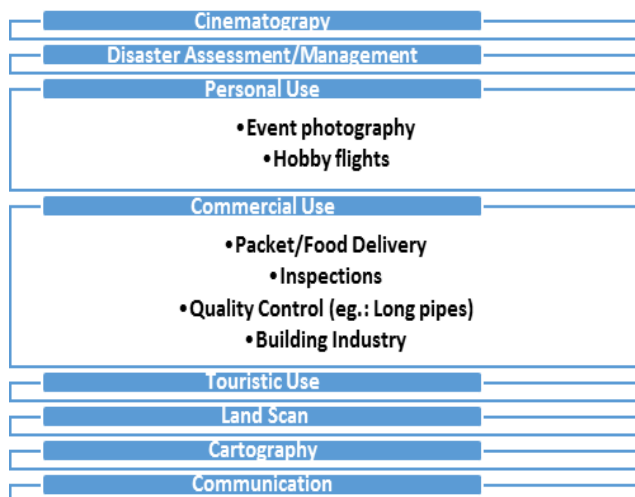
The article from Defense Express discusses the increasing use of FPV (First-Person View) drones by both Ukrainian and Russian forces in the ongoing conflict. Researchers from Tochnyi.info analyzed data on FPV drone usage from August 2023 to January 2024, revealing significant trends and statistics. FPV drones have become a crucial element on the battlefield, with their usage expected to grow. The analysis shows that Ukraine has a slight overall advantage in FPV drone strikes, with 3,886 recorded strikes compared to Russia's 2,889. However, Russia is rapidly increasing its drone usage, particularly in strikes against infantry, where they have started to outpace Ukraine. The data is categorized into three types of FPV strikes: infantry, defensive positions, and vehicles. Ukraine leads in strikes on vehicles, with 2,057 compared to Russia's 632. In terms of strikes on infantry, Ukraine has a slight edge with 1,779 strikes versus Russia's 1,752. However, Russia's numbers are growing faster, with a significant increase in strikes in recent months. The article highlights the strategic differences in drone usage. Ukraine focuses on targeting Russian vehicles to disrupt logistics, while Russia has a higher number of strikes on defensive positions. This shift in tactics has changed the dynamics of battlefield protection, making trenches less effective against drone attacks. The conclusion drawn by analysts is that while Ukraine currently holds an advantage, Russia's rapid increase in drone usage could soon close the gap. This underscores the need for Ukraine to boost its drone production and adopt more advanced systems to maintain its edge in this technological race. [2]

The article "Drones on the Frontline: Charting the Use of Drones in the Russia-Ukraine Conflict and How Their Use May Be Violating International Humanitarian Law" by Jeremy Julian Sarkin and Saba Sotoudehfar provides an in-depth analysis of drone usage in the ongoing conflict between Russia and Ukraine. It explores the implications of drone warfare on international humanitarian law (IHL) and the potential violations arising from their deployment. The study begins by detailing the types of drones used by both sides, highlighting their capabilities such as speed, endurance, and altitude. It emphasizes how drones have transformed modern warfare by providing efficient surveillance, targeted attacks, and reconnaissance with minimal risk to human soldiers. The widespread use of drones in this conflict marks a significant shift in military strategy and raises concerns about the ethical and legal ramifications. One of the key points discussed is the principle of distinction and proportionality in IHL. The authors argue that the use of drones often blurs the lines between combatants and civilians, leading to indiscriminate attacks and collateral damage. They provide evidence suggesting that both Russian and Ukrainian forces may have conducted drone strikes that do not comply with IHL standards, potentially resulting in civilian casualties and damage to civilian infrastructure. The article also examines the role of artificial intelligence (AI) in drone operations. The autonomy of AI-driven drones complicates accountability for IHL violations, as it is challenging to determine responsibility for decisions made by autonomous systems. This raises important questions about the future of warfare and the need for updated legal frameworks to address the unique challenges posed by AI and autonomous weapons. Furthermore, the authors discuss the geopolitical implications of drone warfare. The conflict between Russia and Ukraine is not only a regional issue but also has broader implications for international security and the balance of power. The use of drones by both sides reflects a new era of military technology that could influence future conflicts worldwide. In conclusion, the article calls for a thorough investigation into the use of drones in the Russia-Ukraine conflict to ensure compliance with IHL. It stresses the importance of developing new legal standards to regulate the use of AI and autonomous weapons in warfare, to prevent indiscriminate attacks and protect civilian lives. The authors advocate for greater accountability and transparency in drone operations to uphold international humanitarian principles and maintain global peace and security. [3]

1. TECHNOLOGICAL STRUCTURE OF UAVS

1.1. UAVs CATEGORIZED BY USAGE

I previously made categorization diagrams. The UAVs could be categorized based on the usage. In my research I concluded that the UAVs usage could be good: civilian and state/government usage. Or could be harmful: criminal or terrorist usage. [4]



1. Figure Civilian Usage of Drone [4, p.1]



2. Figure Government Usage of Drones [4, p.1]



3. Figure Criminal usage of Drone [4, p.1]



4. Figure Terrorist usage of Drones [4, p.1]

1.2. TYPES OF UAVs

According to there are 6 classes of UAVs based on wings and rotors [5]:



5. Figure Single Rotor UAV [6]



6. Figure Tricopter UAV [7]



7. Figure Quadcopter UAV [8]



8. Figure Hexacopter UAV [9]



9. Figure Fixed Wing UAV [10]



10. Figure Fixed wing hybrid VTOL [11]

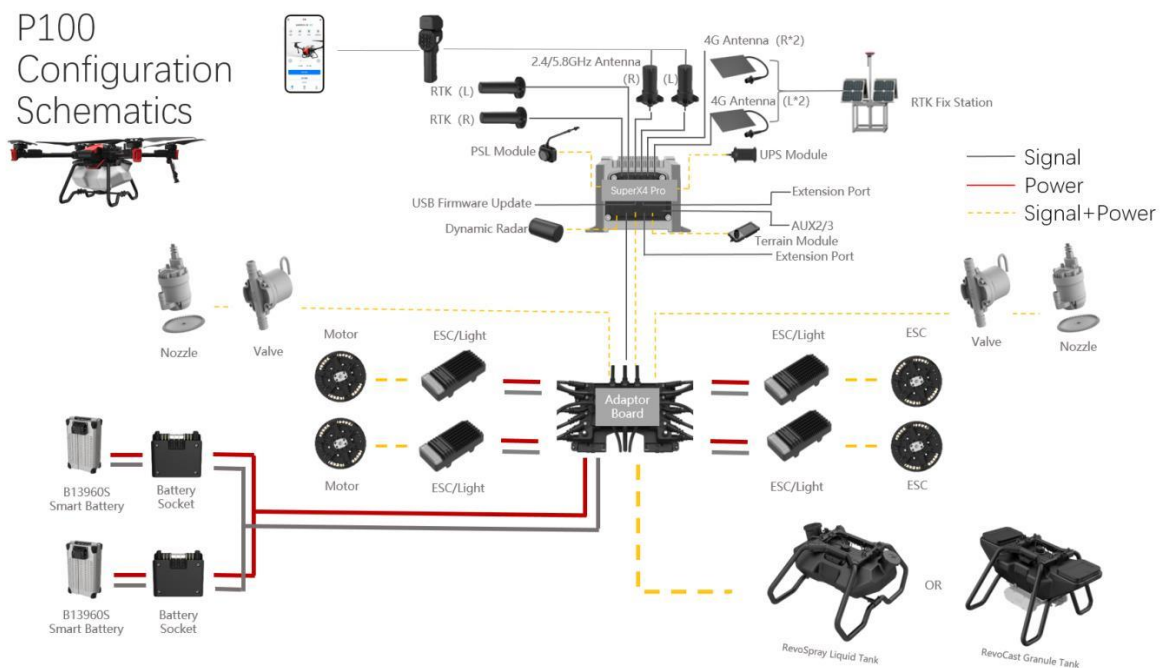
The main differences between a UAV and an aircraft are that the drones are always unmanned (could be operated remotely or fly by preprogrammed patterns or by autonomously). Furthermore, UAVs are usually smaller than aircraft and as a result they are more maneuverable and versatile, also it is highly cost effective.

1.3. STRUCTURE OF ELECTRIC UAVs

I'll only discuss the types of the UAVs mentioned in my subtitle 1.2, because that's the only relevant UAV cluster from my research point of view now.

The larger groups of the structures are the following according to Békési Bertold, Gajdács László, Knapiczus Attila [12]:

- Battery system
- Propulsion system, engines and propellers system
- Central Controller Unit
- Communication System
- Data storage system
- Payload and systems for payloads (eg.: Sensors and Camera)
- Frame of the UAV
- Flight Controller (outside of the UAV)



11. Figure Exploded view of a UAV [13]

2. OSI MODEL

OSI Model

Layer	Function	Data	Example
Application Layer	human-computer interaction layer, where applications can access the network services	Data	HTTP, FTP, SSH, DNS, Telnet, DHCP, Ping, etc
Presentation Layer	ensures that data is in usable format; layer where data encryption occurs	Data	SSL/TLS, SSH
Session Layer	maintains connections and responsible for controlling ports and sessions	Data	IPv4/IPv6, ICMP, IPSec, IGMP, ARP
Transport Layer	transmits data using transmission protocols	Segments	TCP, UDP
Network Layer	decides which physical path the data will take	Packets	Sockets, NFS, SMB, RPC, P2P
Transport Layer	defines the format of data on the network	Frames	Ethernet, PPP, Switch, Bridge
Physical Layer	transmits raw bit stream over the physical medium	Bits	Optical Fiber, UTP Cables, Routers, Hubs

12. Figure OSI Model graphical representation with data types and examples [15]

In the further chapters I'll use a lot of terminology based on the famous ISO (International Organization for Standardization) Open System Interconnection (OSI) Modell. The reference model contains the necessary datatypes like Frames (L2 data type) and Packets (L3) which will help forward our data to the destination. The OSI model use an embedding methodology. It will start with the data we want to send, and it will put the necessary layers around it. [14]

3. POSSIBILITIES TO INTERFERE WITH DRONES – ELECTRONIC COUNTERMEASURES

According to the NATO's new doctrine Electronic Warfare was renamed Electromagnetic Warfare. Due to the adaptation cycle most of the available sources use the older form Electronic Warfare (EW). [16]

According to the book Electronic warfare by (Haig Zsolt; Kovács László; Ványa László; Vass Sándor; Németh András) definition of EW is: “Electronic countermeasures is the area of electronic warfare that includes the emission of electromagnetic and other directed energies in order to prevent or reduce the electromagnetic spectrum enemy effective use by”. [17]

There are 3 main domains of the electronic countermeasures:

1. Electronic jamming
2. Electronic deception
3. Electronic destruction

This chapter focuses on the Electronic Jamming due the scope of the research.

The definition of the Electronic Jamming can be found in the mentioned book as well: “Electronic jamming is the intentional emission, reradiation or reflection of electromagnetic energy with the aim of limiting or preventing the intended operation of electronic devices, equipment and systems used by the enemy.” [17]

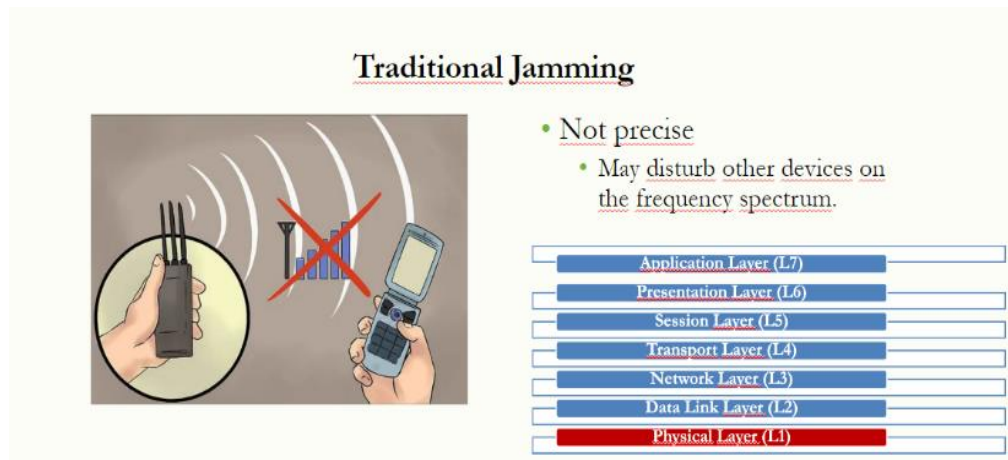
The Electronic jamming could be natural for example a cosmic natural jamming could be a radio radiation created by the sun, interstellar space, and the entire galaxy. [17]

The Electronic Jamming could also be artificial. This must be intentional or unintentional. Due to the nature of this paper, I'll discuss the first type.

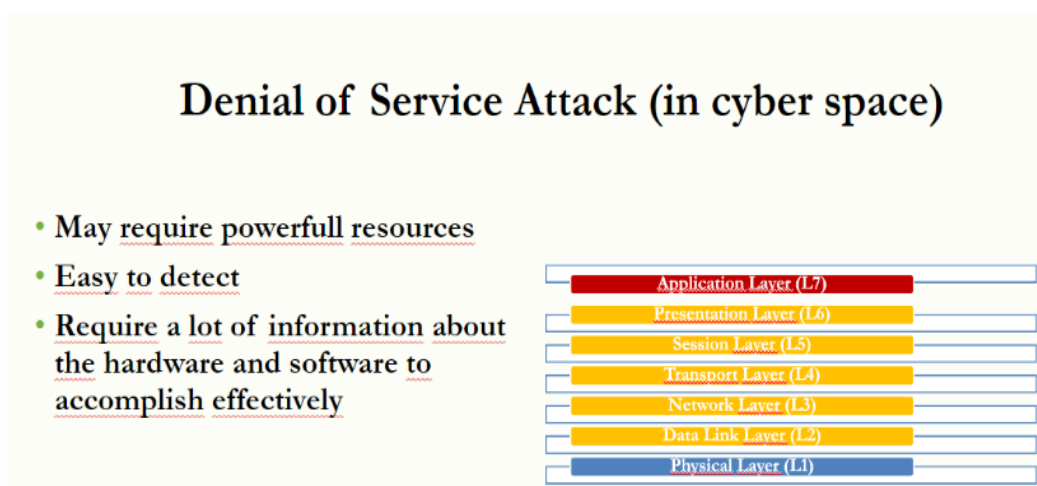
The intentional Electronic Jamming could also divide to 3 subcategories based on the intensity of the jamming. It could be weak when 15% or less information has been corrupted, moderate when it is 50% or less, and powerful when, it is 75% or more. The real damage is not in direct proportionality with the jamming %, because the information could contain redundant parts and the higher layer protocols in the OSI model could help to resist the jamming attacks. [17]

3.1. DENIAL OF SERVICE ATTACKS COMPARISON IN CYBER SPACE

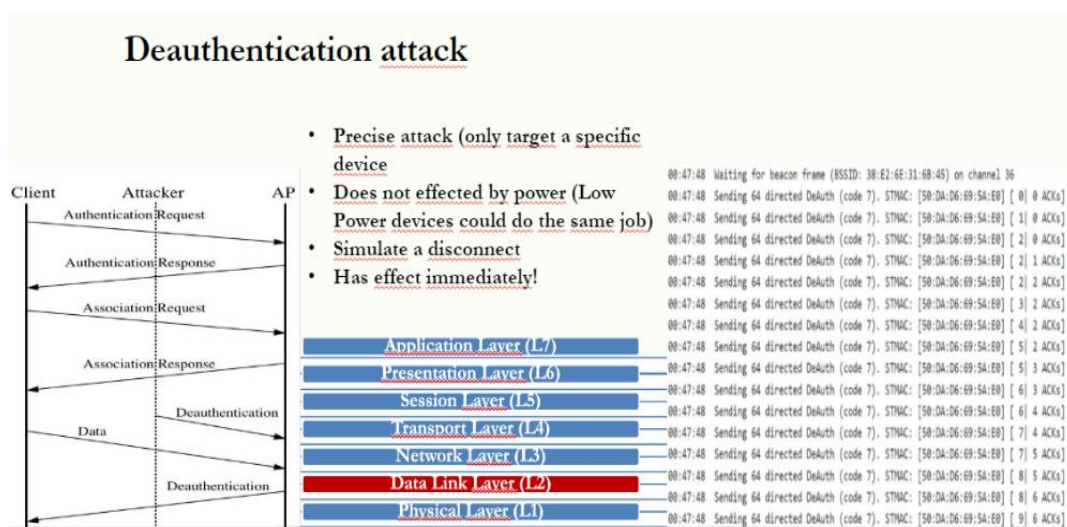
In this chapter I want to graphically compare the 3 most common ways to terminate a connection:



13. Figure Jamming representation based on [4] edited by the author



14. Figure Denial Of Service representation based on [4] edited by the author



15. Figure Deauthentication attack representation based on [4] edited by the author

4. PRESENTATION OF DEVELOPED METHODOLOGY: DEAUTHENTICATION ATTACKS

4.1. INTRODUCTION TO IEEE 802.11

4.1.1. General Characteristics and authentication

IEEE 802.11, commonly referred to as Wi-Fi, is a set of standards developed by the Institute of Electrical and Electronics Engineers (IEEE) for implementing wireless local area network (WLAN) communication in the 2.4 GHz, 5 GHz, and other frequency bands. Since its introduction in 1997, IEEE 802.11 has evolved significantly, providing high-speed wireless connectivity and supporting a wide range of devices, from laptops to Internet of Things (IoT) gadgets. This text aims to provide an overview of the general characteristics of IEEE 802.11 and its authentication mechanisms, which are crucial for ensuring secure and efficient communication. [18][19]

4.1.1.1. General Characteristics of IEEE 802.11

IEEE 802.11 standards are designed to facilitate wireless communication with a focus on reliability, scalability, and compatibility. These standards specify the physical layer (PHY) and media access control (MAC) protocols for WLANs, forming the basis for modern Wi-Fi technologies. Key characteristics of IEEE 802.11 include: [18][19]

- 1. Frequency Bands:**

IEEE 802.11 operates primarily in the 2.4 GHz and 5 GHz frequency bands, with newer standards such as 802.11ax (Wi-Fi 6) and 802.11be (Wi-Fi 7) also extending to the 6 GHz band. The choice of frequency band impacts range, interference, and throughput, with higher frequencies generally providing faster data rates but shorter ranges. [18][19]

- 2. Modulation Techniques:**

To maximize data transmission efficiency, IEEE 802.11 employs advanced modulation schemes. Early versions used direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS), while later iterations adopted orthogonal frequency-division multiplexing (OFDM). These techniques minimize interference and maximize spectral efficiency. [18][19]

- 3. Data Rates and Throughput:**

Each successive IEEE 802.11 standard has improved data rates and throughput. For example, 802.11b (introduced in 1999) supported data rates of up to 11 Mbps, while 802.11ax offers theoretical data rates exceeding 9.6 Gbps. These enhancements have been achieved through innovations such as multiple input multiple output (MIMO) technology and improved channel bonding. [18][19]

- 4. Network Topologies:**

IEEE 802.11 supports several network configurations, including:

- **Infrastructure Mode:** Devices communicate via an access point (AP), creating a centralized network.
 - **Ad Hoc Mode:** Devices communicate directly without an AP, forming a decentralized network.
 - **Mesh Networks:** Nodes relay data to one another, providing robust connectivity and fault tolerance. [18][19]
5. **Compatibility and Backward Compatibility:**
To ensure seamless user experiences, IEEE 802.11 standards emphasize compatibility. Devices adhering to newer standards are typically backward-compatible with older ones, enabling coexistence within mixed-device environments. [18][19]
6. **Quality of Service (QoS):**
Standards such as 802.11e introduce mechanisms to prioritize traffic, ensuring that time-sensitive applications like video streaming and voice calls receive adequate bandwidth. [18][19]
7. **Power Management:**
Power-saving mechanisms like 802.11v allow devices to operate efficiently, a feature particularly important for battery-powered devices such as smartphones and IoT gadgets. [18][19]

4.1.1.2. Authentication in IEEE 802.11

Authentication is a fundamental component of IEEE 802.11 security protocols, designed to verify the identity of devices attempting to join a network. Ensuring secure authentication protects against unauthorized access, eavesdropping, and various cyber threats. IEEE 802.11 employs multiple authentication mechanisms, ranging from basic methods to advanced encryption-based approaches. [18][19]

4.1.1.2.1. Open System Authentication

Open system authentication is the simplest form of authentication in IEEE 802.11 networks. It does not require credentials or encryption, making it easy to implement but inherently insecure. Any device can connect to the network without verification, leaving the network vulnerable to unauthorized access. This method is typically used in public Wi-Fi networks where accessibility is prioritized over security. [18][19]

4.1.1.2.2. Shared Key Authentication

Shared key authentication provides a higher level of security than open system authentication by requiring devices to demonstrate possession of a pre-shared key (PSK). [18][19] The process involves:

1. The AP sending a challenge text (a random string) to the client.
2. The client encrypting the challenge text using the PSK and sending it back to the AP.
3. The AP decrypting the response and verifying its correctness.

While shared key authentication improves security, it has limitations. For instance, if the PSK is compromised, unauthorized devices can access the network. [18][19]

4.1.1.2.3. 802.1X and Extensible Authentication Protocol (EAP)

For enterprise environments requiring robust security, IEEE 802.11 supports 802.1X authentication. [18][19] This method integrates the EAP, which provides a framework for various authentication mechanisms, including:

1. **EAP-TLS (Transport Layer Security):** Relies on digital certificates for mutual authentication between the client and the authentication server. It is highly secure but requires a public key infrastructure (PKI).
2. **EAP-TTLS (Tunneled TLS) and PEAP (Protected EAP):** Create encrypted tunnels for transmitting authentication credentials, providing a balance between security and ease of implementation.
3. **EAP-SIM and EAP-AKA:** Designed for mobile networks, these methods authenticate devices using information stored on SIM cards. [18][19]

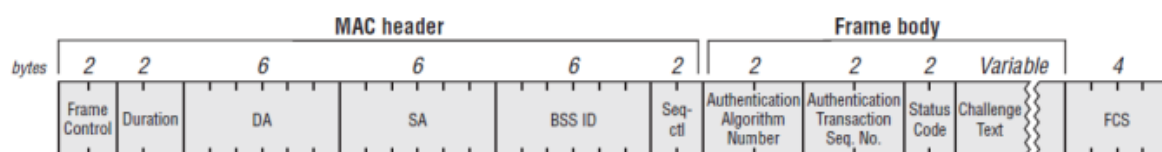
The 802.1X framework separates authentication, authorization, and accounting (AAA), providing centralized management and enabling features like dynamic VLAN assignment and session timeout. [18][19]

4.1.1.2.4. Wi-Fi Protected Access (WPA and WPA2/WPA3)

Wi-Fi Protected Access (WPA) protocols enhance authentication and encryption in IEEE 802.11 networks. Key features include:

1. **WPA2 and WPA3:** Successors to the original WPA, these protocols provide enhanced security through stronger encryption algorithms (AES for WPA2 and GCMP-256 for WPA3). WPA3 also introduces features like Simultaneous Authentication of Equals (SAE), which replaces the PSK mechanism with a more secure handshake. [18][19]
2. **Personal and Enterprise Modes:**
 - **Personal Mode:** Uses a PSK for authentication, suitable for home networks.
 - **Enterprise Mode:** Leverages 802.1X and EAP for advanced authentication, ideal for business environments. [18][19] crucial
3. **Forward Secrecy:** Implemented in WPA3, this feature ensures that the compromise of a single session's encryption key does not affect the security of other sessions.[18][19]

FIGURE 4.8 Authentication frame format

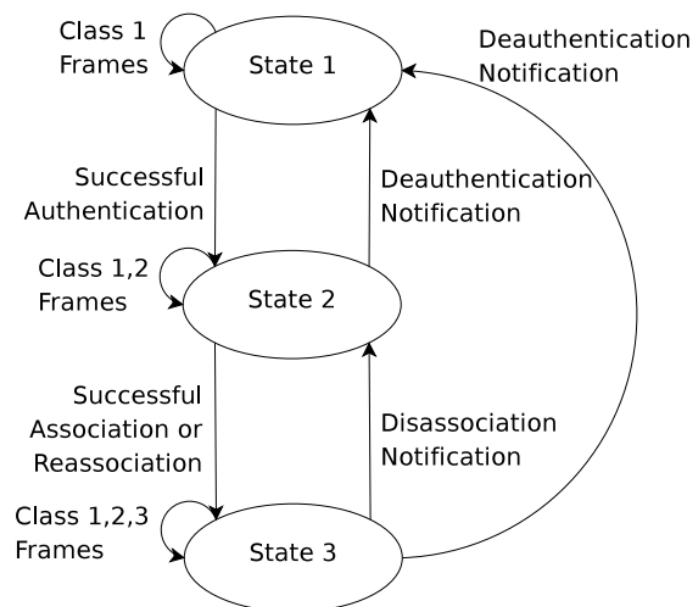


4.2. DEAUTHENTICATION AND DISASSOCIATION FRAMES IN THE IEEE 802.11

Deauthentication frames are used to terminate the connection. The station sends it to the access point (AP) when it does not want to be connected to the AP. The AP can also send deauthentication frames which might be sent to the broadcast address and deauthenticate all of the connected stations. In real life these are used for when for example we disconnect our smart phone from the 2,4 GHz Wi-Fi and connect it to the faster 5GHz then our smart phone will send a deauthentication frame to the 2,4GHz AP first and then it'll send an authentication frame to the 5GHz AP. The second situation could happen when we update our AP and it will shut down, but before that it will send a deauthentication frame to the broadcast address to let know the stations that the service will no longer be available. Deauthentication frames also generates a disassociation because when it is not authenticated to the network it could not be associated with the AP. [18] [19] [21]

Disassociation frames in the other hand only an indicator that it is not connected to the specific AP but it could be reconnect to an other AP in a mesh topology. This is also useful when we implemented a RADIUS¹ or TACACS+² service that use central authentication management and multiple AP-s exist in the building and our cell phone are just roaming to a different AP. [18] [19] [21]

It is really important to point out that these frames are not request and does no need a handshake or any kind of authentication. It is just a signal that the station is deauthenticated for example. In that case there is no need any kind of confirmation! [4][18] [19] [21]



17. Figure IEEE 802.11 State Transition [4] [22]

¹ RADIUS: Remote Authentication Dial In User Service

² TACACS+: Terminal Access Controller Access-Control System

4.2.1. IEEE 802.11i Security Amendments – Robust Security Framework

IEEE 802.11i is a significant amendment to the original 802.11 standard, designed to address the security vulnerabilities that plagued earlier versions. It introduced a robust security framework known as Robust Security Network (RSN), which significantly enhances the confidentiality, integrity, and availability of wireless networks. [4][18][19]

Key Features of the RSN Framework

Enhanced Authentication:

- **802.1X Authentication:** This mechanism provides strong authentication using a centralized authentication server (RADIUS).
- **PSK (Pre-Shared Key) Authentication:** A simpler method that uses a shared password between the client and the access point.

Robust Key Hierarchy:

- **Pairwise Keys (PKs):** Unique keys established between each pair of communicating devices (client and AP) for securing unicast traffic.
- **Group Keys (GKs):** Shared keys used to encrypt multicast and broadcast traffic.
- **Key Hierarchy:** A well-defined process for generating, distributing, and refreshing keys to ensure security.

Countermeasures Against Attacks:

- **Message Integrity Check (MIC):** A cryptographic checksum added to each frame to detect tampering or replay attacks.
- **Cipher Suite Selection:** Allows for the selection of strong encryption algorithms (e.g., AES-CCMP) to protect data confidentiality.
- **Key Temporal Keys (TKs):** Used to protect the integrity of key exchange messages and prevent replay attacks.

The 4-Way Handshake

The 4-way handshake is a crucial process in the RSN framework, used to establish secure communication between a client and an access point. It involves the following steps:

Authentication Request: The client sends an authentication request frame to the AP.

Authentication Response: The AP responds with an authentication response frame, including a nonce (a random number).

Key Exchange: The client and AP generate a Pairwise Master Key (PMK) using a key derivation function (KDF). They then exchange messages to establish Pairwise Transient Keys (PTKs) and Group Temporal Keys (GTKs).

Confirmation: The client and AP send confirmation frames to complete the handshake. [4][18][19]

4.2.2. IEEE 802.11w – Protected Management Frames

The IEEE 802.11w amendment, formally known as "Protected Management Frames," was introduced to bolster the security of wireless networks by safeguarding critical management frames. Before this amendment, management frames were often vulnerable to various attacks, such as deauthentication and disassociation attacks. [4][18][19][22]

Key Features of 802.11w:

Protected Management Frames (PMF):

- Encrypts management frames using the Pairwise Transient Key (PTK), which is derived from the 4-way handshake.
- Provides integrity protection for management frames using a Message Integrity Code (MIC).
- Implements replay protection to prevent attackers from reusing old frames.

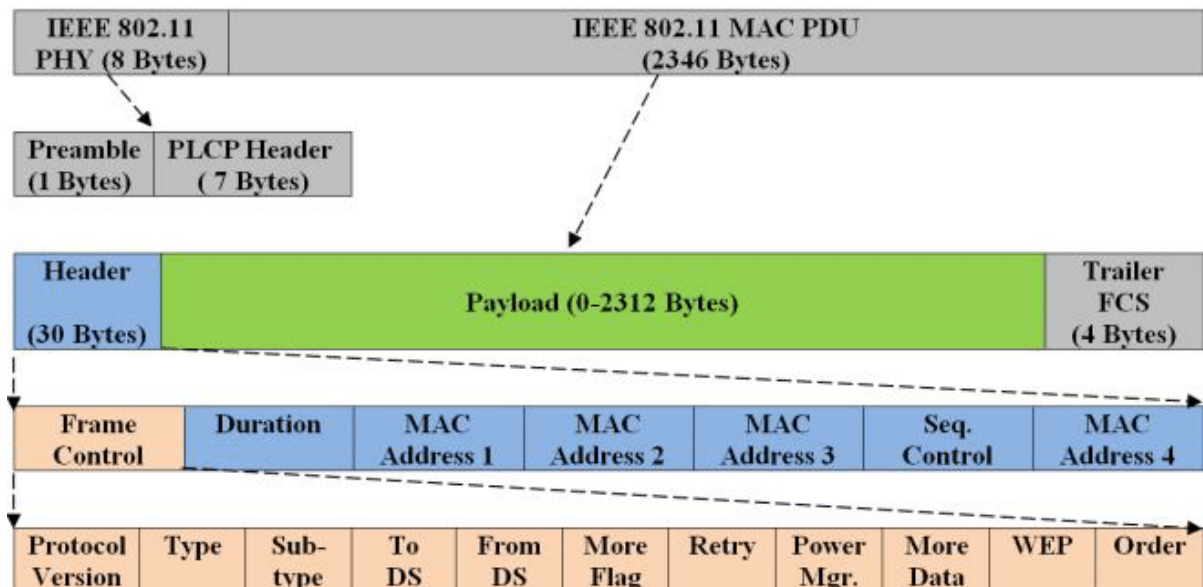
Robust Management Frame Protection (RMFP):

- A more advanced security mechanism that offers additional protection for management frames.
- Requires both the client and the access point to support RMFP.
- Provides stronger security guarantees by using advanced cryptographic techniques.

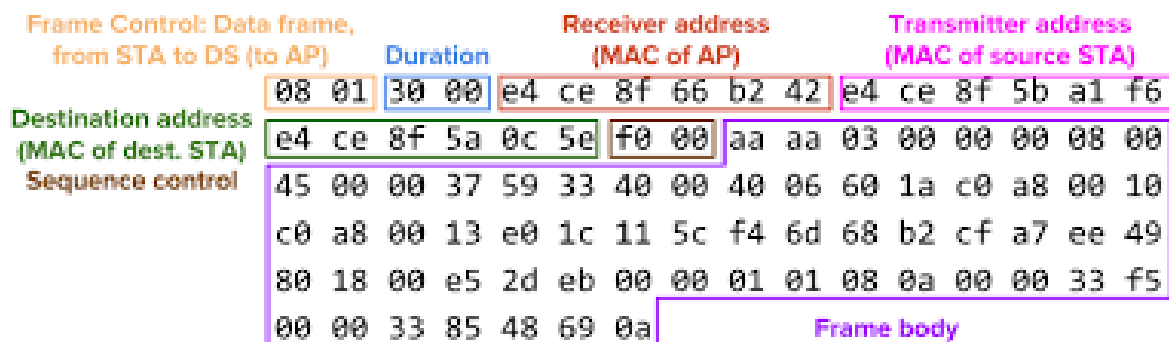
The IEEE 802.11w amendment could be useful to counter deauthentication attacks, although it will increase the efficiency of SA termination attack according to E. Martin. [4][18][19][22]

4.3. THE FRAME STRUCTURE ACCORDING TO STANDARD

IEEE 802.11 Frame Format



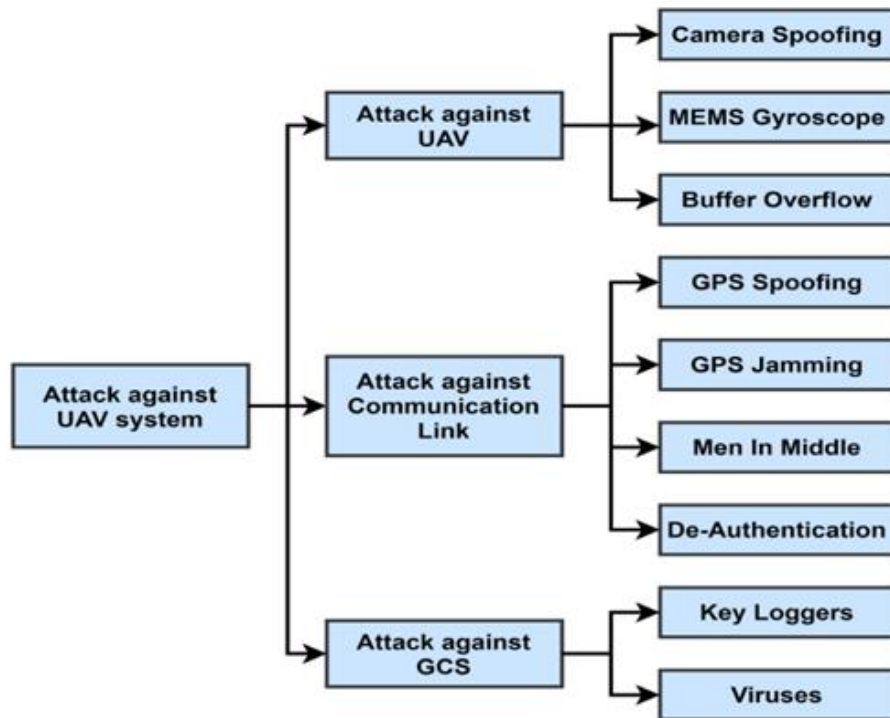
18. Figure IEEE 802.11 frame structure graphical representation [23]



19. Figure Frame structure in hex format[24]

4.4. DEAUTHENTICATION BASED ATTACK IN OTHER RESEARCHES

- In 2020 an Indian research group used a Raspberry Pi 3 device with Aircrack-ng framework to deauthenticate UAVs. [4] [41]
- In 2016 US researchers used deauthentication as prerequisite for a JSON fuzzing attack. [4] [42]
- In 2020 a deep research in attack vector was conducted in Pakistan [4] [43]



29. Figure Attack vectors against UAVs [4] [43]

- d) An Intrusion Detection System (IDS) was developed against deauthentication attacks in 2019 in India. [4] [44]
- e) Bahrainien researchers suggested Wi-Fi protocol improvements in 2022 after an extensive penetration test. [4] [45]
- f) SkyJacking was mentioned in a comprehensive survey [4] [46]
- g) In 2020 an Indonesian research group conducted penetration test on the IEEE 802.11 and came to the conclusion that management frames are not secure enough. [47]
- h) A Czech researchers measured the resilience of Wi-Fi based UAVs against traditional jamming. The jamming was not effective.[4][48]
- i) A Norwegian researcher made an extensive standard analysis and found a deadlock vulnerability in the standard. [22]

4.5. RESULT OF THE PREVIOUS RESEARCH

4.5.1. Equipment used in the research.

4.5.1.1. Hardware used for the research.

4.5.1.1.1. Wi-Fi card:

For the wireless capabilities, packet monitoring and injection we used Tenda AC650 usb Wi-Fi card.

4.5.1.1.2. UAVs used for the research:

UAV1st.	UAV2nd.	UAV3rd.
ZLRC SG906 Pro 2	TELLO-EF8E26	Yuneec H520E
		
20. Figure ZLRC SG906 Pro 2 [25]	21. Figure Tello-EF8E26 [26]	22. Figure Yuneec H520E [27]

4.5.1.2. Software used for the research.

The operating system was Kali Linux 2023.2 version on a VMWare Workstation Player 17. To scan the network and to create deauthentication frames the open source Aircrack-ng 1.7 framework was used. From the framework the Airmon-ng was used for killing the interfering processes and setting the Wi-Fi card to monitor mode, Airodump-ng for scanning the networks and Aireplay-ng for creating deauthentication frames.

4.6. GRAPHICAL REPRESENTATION OF THE USED HARDWARE AND SOFTWARE



23. Figure Visual Representation of equipment usage throughout the research based on [4] edited by the author

4.6.1. Process description – Vulnerability research

Due to the fact that mentioned earlier that the cheaper UAVs are using IEEE 802.11 poorly implemented versions the hypothesis born that the UAVs could be easily deauthenticated from the remote controller and with the proper software prepared it could be hijacked and gain full access towards controlling the UAV as we like.

In the research process a Bash script was developed which utilizes the tools from the Aircrack-ng framework. This script set the Wi-Fi card from access mode to monitor mode with killing the interfering processes. After that it scans for the spectrum for available networks and print out a list from that we can chose which UAV network it is possible to be attacked. Then it

performs a continuous deauthentication attack (because if the remote controller tries to reconnect, the reconnection cannot be successful). From the MAC address of the UAV/remote controller it is possible to determine the OEM brand. With enough preparation the brands remote control software could be installed on our device and used as a legacy looking remote controller. After the deauthentication attack happened with the new rogue controller the UAV can be connected and control the movement of it. For the research proof of concept, a smartphone was used. This could be particularly useful, because a soldier could easily carry a smart phone with the appropriate software and use it as the part of the Digital Soldier Program.

4.6.2. Preparation for the measurement

The equipment mentioned in 5.4.1.1 chapter was also prepared with the software mentioned above. Also, the attack bash script was developed before the measurements. For the measurements, the Yuneec H520E UAV, the ZLRC SG906 Pro 2 UAV and the TELLO-EF8E26 UAV turned on with the OEM remote controller software installed on a smart phone.

The measurements were conducted at a university laboratory. Faraday cage or any other interference preventive method were not implemented. Interference from other Wi-Fi access point is constantly present.

The virtual machine from VMWare Workstation Player was started with the Kali Linux operating system. The Network Interface Card (NIC) was checked for interfering processes with Airmmon-ng software and these processes were killed by their PID ID number. After that the NICs operation mode was changed from access to monitor mode to be able to capture packets.

4.6.3. Results of the experiment

The hijacking measurements were conducted on the 3 UAVs.

4.6.3.1. ZLRC SG906 Pro 2 UAV – Vulnerable to deauthentication based hijacking attack

The ZLRC SG906 Pro 2 UAV was vulnerable to the deauthentication based attack vector. After our attacking script attacked the UAV instantly lost the connection (the IEEE 802.11 Layer 2 connection is deauthenticated and disassociated) the remote controller tries to reconnect, but the reconnection never went through the process, it always fails due to the constant deauthentication attack provided by the attacking script. With the UAV lost in connection it will try to find the connection to one of the previous remote controller. Here the case is that it is a smartphone which tries to find a previous smartphone connection and at this moment with an other smartphone with the remote controller software installed it is possible to connect to the UAV. This attempt was successful. We gain full control over the UAV. In this case full control is defined as all function and capabilities are available that is provided with the OEM software. Practically the UAV sensor data, telemetry data and camera could be captured, the UAV can be controlled but it did not provide a root access to the UAVs internal operating system and software. Therefore, at this point no remote code execution is possible, but this is definitely a future direction to the research.

4.6.3.2. TELLO-EF8E26 – Vulnerable to deauthentication based hijacking attack

The case was the same for the Tello drone.

The TELLO-EF8E26 UAV was vulnerable to the deauthentication based attack vector. After our attacking script attacked the UAV instantly lost the connection (the IEEE 802.11 Layer 2 connection is deauthenticated and disassociated) the remote controller tries to reconnect, but the reconnection never went through the process, it always fails due to the constant deauthentication attack provided by the attacking script. With the UAV lost in connection it will try to find the connection to one of the previous remote controller. Here the case is that it is a smartphone it tries to find a previous smartphone connection and at this moment with an other smartphone with the remote controller software installed it is possible to connect to the UAV. This attempt was successful. We gain full control over the UAV. In this case full control is defined as all function and capabilities are available that is provided with the OEM software. Practically the UAV sensor data, telemetry data and camera could be captured, the UAV can be controlled but it did not provide a root access to the UAVs internal operating system and software. Therefore, at this point no remote code execution is possible, but this is definitely a future direction to the research.

```
00:47:48 Waiting for beacon frame (BSSID: 38:E2:6E:31:6B:45) on channel 36
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 0] 0 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 1] 0 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 2] 0 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 2] 1 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 2] 2 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 3] 2 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 4] 2 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 5] 2 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 5] 3 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 6] 3 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 6] 4 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 7] 4 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 7] 5 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 8] 5 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 8] 6 ACKs
00:47:48 Sending 64 directed DeAuth (code 7). STMAC: [50:DA:D6:69:5A:E0] [ 9] 6 ACKs
```

24. Figure Deauthentication attack – Edited by the author

4.6.3.3. Yuneec H520E – The attack was not successful

For the Yuneec H520E UAV there was some difficulties that I have faced. The Yuneec UAV hides the connection by implementing a feature in the IEEE 802.11 security amendment which is turning off the broadcasting of Beacon frames. Beacon frames are necessary to create deauthentication frames in Aireplay-ng, but I'll investigate further methods to get the necessary data out of other packets in the packet flow to create deauthentication frames.

4.6.4. Limitations of the measurements

- The proposed method can only be used if the UAVs/UASs are using 802.11 based protocol for communication. The scope for this research is only for analyzing WiFi based UAVs.

- The proposed method can only be used if the BSSIDs of the UAVs are not hidden, and the BSSIDs could be differentiated that should exist in the current network.
- The range of the proposed method is based on the WLAN card/device that has been used. Although deauthentication attack is not affected by the distance, the measurements taken in close distance (approximately 5-30 meters).
- The attack script cannot differentiate the friendly/rogue UAVs by itself. An external source or a human operator is needed for that.

4.6.5. Evaluation of measurement

The measurements were successful. Two drones out of three are vulnerable to the attack and for the Yuneec drone I have a direction where to improve the attacking script. Due to the deauthentication attack the UAV pilot/operator will lose connection and it would not be able to reconnect because the deauthentication being continued. The deauthentication attack disconnects the UAV from the remote controller in **15,625ms** according to our measurements which started when the user selected the desired UAV in the attack script and ended when the UAV lost the connection from the controller. The Aireplay-ng was used in the default configuration for deauthentication which means it is sending 64 deauthentication frames to the station and 64 frames to the AP, so overall 128 frames/iteration. The maximum achievable output with this configuration is **4992 deauthentication frames/second**. Consequently, I can draw the conclusion that the UAV has only **0,200321ms** before the next deauthentication arrive, so in practice this is not enough time to process an authentication reconnect. My experience is that 3-5 seconds (it is varied throughout the different manufactures) needed after I pair the drones with the remote controllers. Anytime the UAV tries to reconnect to the UAV the connection will be set to the default **disassociated – deauthenticated state** due to the incoming deauthentication packet.

4.7. GRAPHICAL REPRESENTATION OF THE MEASUREMENTS



25. Figure Hijacking Process based on [4] - Edited by the Author

5. NEW OPPURTUNATIES AGAINNS UAV SWARMS

5.1. IEEE 802.11 MULTICAST STANDARD OVERVIEW

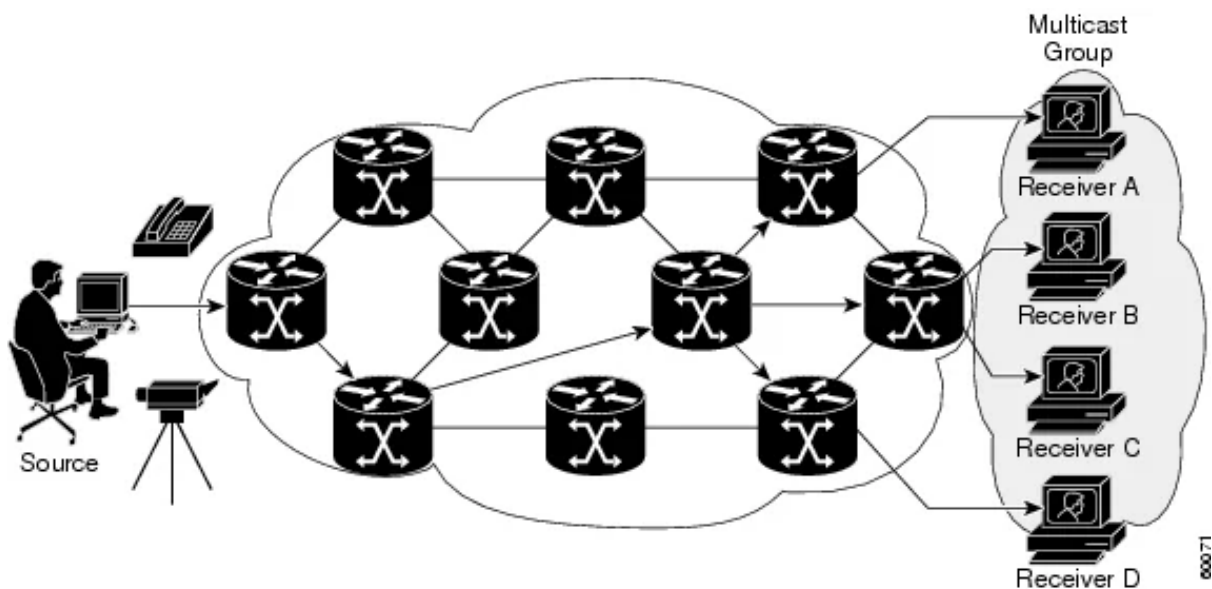
Multicast communication in IEEE 802.11 is designed to efficiently deliver data to multiple recipients simultaneously. Unlike unicast, multicast does not require individual acknowledgments from each receiver, which reduces overhead but also introduces reliability issues. The basic multicast mechanism in IEEE 802.11 involves sending data frames to a multicast address, which all intended recipients listen to. [28]

5.1.1. Multicast Group Concept

At the core of IP multicast is the concept of a multicast group. A multicast group is a set of receivers that express interest in receiving a particular data stream. These groups are identified by multicast IP addresses, which fall within the Class D address range (224.0.0.0 to 239.255.255.255) for IPv4. Hosts join multicast groups using the Internet Group Management Protocol (IGMP) for IPv4 or Multicast Listener Discovery (MLD) for IPv6. Once a host joins a multicast group, it can receive all data sent to that group address. [29]

5.1.2. IP Multicast Addresses

IP multicast addresses are used to specify the destination of multicast traffic. These addresses are reserved and managed by the Internet Assigned Numbers Authority (IANA). The Class D address range is specifically allocated for multicast traffic, with certain addresses reserved for specific protocols and applications. For example, 224.0.0.1 is reserved for all systems on a subnet, while 224.0.0.2 is reserved for all routers on a subnet. [29]

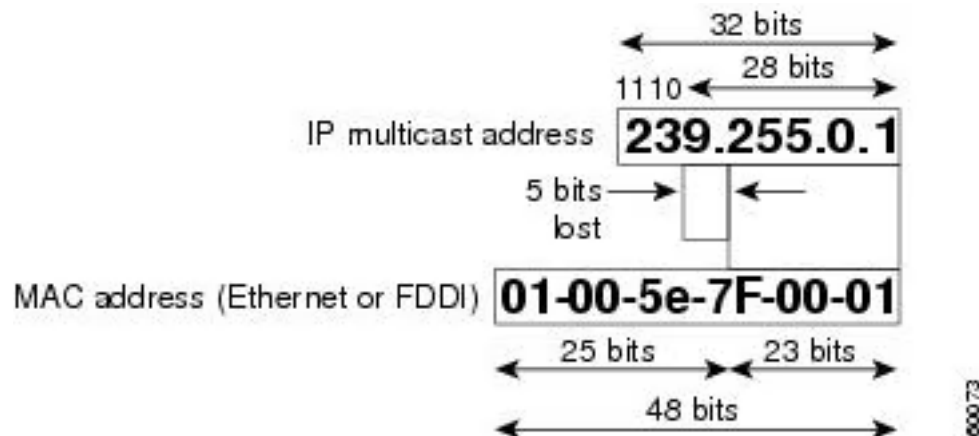


26. Figure Multicast Group [30]

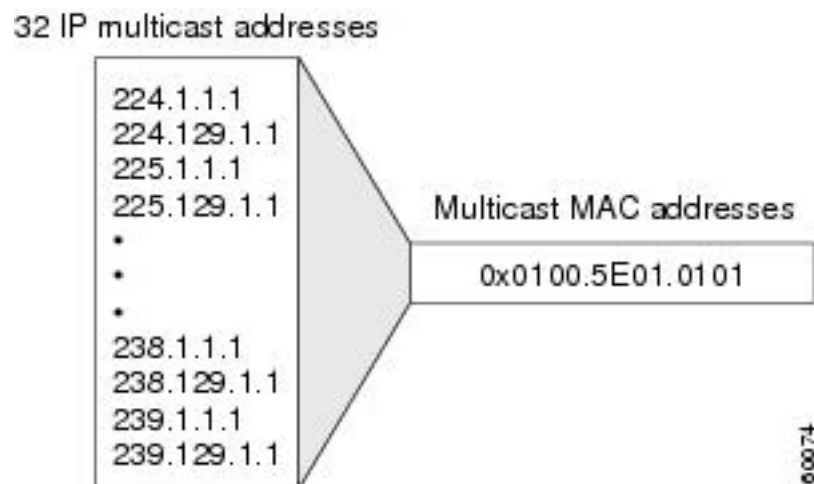
5.2. LAYER 2 MULTICAST ADDRESS

“The IANA owns a block of Ethernet MAC addresses that starts with 01:00:5E in hexadecimal format. Half of this block is allocated for multicast addresses. The range from 0100.5e00.0000 through 0100.5e7f.ffff is the available range of Ethernet MAC addresses for IP multicast.

This allocation allows for 23 bits in the Ethernet address to correspond to the IP multicast group address. The mapping places the lower 23 bits of the IP multicast group address into these available 23 bits in the Ethernet address” [31]



27. Figure Multicast IP to MAC address [32]



28. Figure Multicast IP addresses to Multicast MAC address [33]

5.3. THEORY OF IEEE 802.11 MULTICAST DEAUTHENTICATION

Removing a station from the network may happen two ways in 802.11 multicast. Either sending a deauthentication frame to the multicast address with the prepared information or with IGMP (Internet Group Management Protocol) or MLD (Multicast Listener Discovery) a leave request could be sent to leave the multicast group.

5.4. PROPOSED METHOD

The proposed method for deauthentication attack vector was executed using unicast addressing scheme. In nowadays weapons conflicts no single UAVs used, but rather swarms. UAV swarms use multicast communication, and my proposed method is to send deauthentication frames to the multicast mac address (L2) and send IGMP/MLD leave request (L3). This will be a multi-layer attack against the UAV Swarm.

The proposed method has not been measured till the submission of this paper, but it is planned to take place at the end of 2024 November in cooperation with CollMot Robotics Ltd. [34]

6. ARCHITECTURAL DESIGN FOR A FINISHED SOLUTION

6.1. VISIONS BEHIND THE NEW SYSTEM AND CAPABILITY REQUIREMENTS

The vision behind the design and development is to create a working framework where our UAS (Unmanned Aerial System) could deauthenticate enemy UAVs, crack the encryption if necessary and take control of it at a real-world scenario. I hope that the more sophisticated attack vectors will supplement the traditional Electronic Warfare capabilities. With the techniques that was developed I hope this will be able to contribute to the Cyber – Electronic Warfare capabilities of the Hungarian Defense Forces!

6.2. DESIGN AND ARCHITECTURAL PATTERNS USED

6.2.1. Docker Containers

Docker containers are a form of operating system-level virtualization that allows applications to run in isolated environments. Docker, an open-source platform, enables developers to package applications along with their dependencies into a standardized unit called a container. This containerization ensures that the application runs consistently across different computing environments, from development to production. [35][36]

Architecture and Components:

Docker Engine: The core component of Docker, responsible for creating and managing containers. It consists of a Docker daemon, a REST API, and a command-line interface (CLI).

Images: Immutable templates that define the contents of a container. Images are built from a series of layers, each representing a step in the build process, defined in a Dockerfile.

Containers: Runtime instances of Docker images. Containers are lightweight and share the host system's kernel, making them more efficient than traditional virtual machines.

Docker Hub: A cloud-based registry service that allows users to find and share container images. Docker Hub hosts public and private repositories of images.

Usage and Benefits: Docker containers streamline the development lifecycle by providing a consistent environment for development, testing, and deployment. They support continuous integration and continuous deployment (CI/CD) workflows, enabling rapid iteration and reliable delivery of applications. Containers are highly portable, running on various platforms, including local machines, data centers, and cloud environments [35][36]

6.2.2. Microservice architecture

Microservice architecture is an approach to software development where an application is composed of small, independent services that communicate over well-defined APIs. Each microservice is designed to handle a specific business function, allowing for independent development, deployment, and scaling. [37][38]

Key Characteristics:

Decentralization: Each microservice manages its own database and data model, promoting a decentralized approach to data management. This allows teams to choose the best technology stack for their specific needs.

Independence: Microservices are loosely coupled, meaning changes in one service do not directly impact others. This independence facilitates continuous delivery and deployment.

Scalability: Services can be scaled independently based on demand. For example, if a particular service experiences high load, it can be scaled out without affecting other parts of the application.

Resilience: The failure of one service does not necessarily bring down the entire system. Techniques like circuit breakers and bulkheads help isolate failures and maintain overall system stability.

Technology Diversity: Teams can use different technologies and programming languages for different services, allowing them to leverage the best tools for each specific task.

Implementation: Microservices communicate through APIs, often using REST or gRPC. They are typically deployed in containers, which provide the necessary isolation and resource management. Service discovery mechanisms, such as Consul or Eureka, are used to dynamically locate services. Monitoring and logging tools, like Prometheus and ELK Stack, provide visibility into the health and performance of the services. [37][38]

6.2.3. gRPC

gRPC is a high-performance, open-source framework developed by Google for remote procedure calls (RPC). It enables communication between client and server applications, allowing methods to be called on a remote server as if they were local. gRPC uses HTTP/2 for transport, Protocol Buffers (protobuf) as the interface definition language (IDL) and supports multiple programming languages. [39]

Core Concepts:

Service Definition: gRPC services are defined using Protocol Buffers. A service specifies the methods that can be called remotely, along with their parameters and return types.

RPC Types: gRPC supports various types of RPCs, including unary (single request-response), server streaming (single request, multiple responses), client streaming (multiple requests, single response), and bidirectional streaming (multiple requests and responses).

Channels and Stubs: A gRPC channel represents a connection to a server, while a stub (or client) provides the methods defined in the service. Clients use stubs to call remote methods.

Metadata and Deadlines: gRPC allows clients to send metadata with requests and specify deadlines for RPC completion. This ensures that calls do not hang indefinitely and can be terminated if they exceed the specified time limit.

SUMMARY, PRESENTATION OF THE RESULTS OF THE THESIS

In modern days conflicts during a war without UAVs are unimaginable and most countries use it at variable levels, but the existent is certain. UAVs are not just singular entities but rather used in swarms which makes more difficult to defend ourselves from the drones in a conflict. The traditional Electronic Countermeasure like jamming has their limitations and they might interrupt other devices communication. Although it is widely implemented in the defence forces there are a lot of cases (like in 5.4 chapters Czech researchers) where the traditional jamming is not effective against new generation drones. The drones also could be preprogrammed to do their suicide task and if only just the connection has been lost they are capable to complete their mission. Traditional jamming methods are also easy to detect because it has been present for a long time and might require high powered antennas with constant electricity supply. The higher layer Denial of Service attacks also require powerful hardware and could also be detected easily, because the businesses developed IDS for this case and a Dos attack require a lot of information gathered previously from the target. In this paper I proposed a new way to counter UAV attacks with deauthentication based attack vector and proposed a possibility to hijack UAVs and take full control over it. The deauthentication attack works very precisely! It does not affect other devices, only target the specific target. Does not affected by power! If the target is in range the attack will perform the same results regardless of the distance. It has immediate effect because it does not require any handshake processes.

The deauthentication could also be the base for more sophisticated attacks like the hijacking mentioned previously. With these capabilities the goal is not just to stop or interrupt the enemy UAVs but to reverse the enemy UAVs and use them against their owner. The paper also has a vision with a High Level Design that solid framework against UAVs with Cyber – Electronic Warfare capabilities which could be a complete system against UAV swarms.

ACKNOWLEDGMENT

Project no. TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

REFERENCES

- [1] <https://edition.cnn.com/2024/11/10/europe/ukraine-largest-drone-attack-moscow-intl/index.html> Download date: 2024.11.12 20:32:10
- [2] https://en.defence-ua.com/analysis/detailed_fpv_drone_usage_statistics_show_russias_starting_to_ouptace_ukraine-9361.html Download date: 2024.11.11 19:02:41
- [3] https://research.unl.pt/ws/portalfiles/portal/85371059/Sarkin_Drones-on-the-Frontline.pdf Download date: 2024.11.9 16:22:08
- [4] B. Krasnyánszki, S. T. Brassai and A. Németh, "UAV weaknesses against deauthentication based hijacking attacks," *2024 IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Stará Lesná, Slovakia, 2024, pp. 000493-000498, doi: 10.1109/SAMI60510.2024.10432859.
- [5] [\(https://pigeonis.in/blog/detail-guide-about-uav-technology-supporting-aerial-task-operations/\)](https://pigeonis.in/blog/detail-guide-about-uav-technology-supporting-aerial-task-operations/) Download date: 2024.11.08 10:12:05
- [6] <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcS2V8E7QTr-3sc2Tjl8ib7Sg2y041AyG0rJQg&s> Download date: 2024.11.06 10:21:06
- [7] <https://i.ytimg.com/vi/TIec3gEcHXU/maxresdefault.jpg> Download date: 2024.11.08 13:03:12
- [8] https://upload.wikimedia.org/wikipedia/commons/thumb/6/6a/Quadcopter_camera_drone_in_flight.jpg/1200px-Quadcopter_camera_drone_in_flight.jpg Download date: 2024.11.01 05:04:23
- [9] https://www.tienda24hs.com/WebRoot/StoreES/Shops/62148069/5F5B/BA2D/775C/B855/18F3/0A0C/6D12/D3E4/H520E_tienda24hs_Yuneec_YUNH520EEU_seguridad_mejor_dron_mundo.jpg Download date: 2024.11.01 11:14:08
- [10] <https://gaotek.com/wp-content/uploads/2024/08/fixedwingdrone.jpg> Download date: 2024.11.02 15:23:14
- [11] https://img001.video2b.com/1195/file_01700726248435.png Download date: 2024.11.08 13:03:12
- [12] https://real.mtak.hu/181268/1/18_bekesi-gajdacs-knapiczus_257-274_RTK_2023_1.pdf Download date: 2024.10.31 12:13:22
- [13] <https://support.pegasusrobotics.com/hubfs/image-png-Jul-26-2023-03-39-33-5860-PM.png> Download date: 2024.10.21 14:35:02
- [14] ISO Open System Interconnection <https://www.iso.org/ics/35.100/x/> Download date: 2024.10.21 19:42:39
- [15] https://library.mosse-institute.com/_images/osi_model.png Download date: 2024.10.10 14:05:34
- [16] https://www.nato.int/cps/en/natohq/topics_80906.htm Download date: 2024.10.19 15:15:35
- [17] <https://opac.uninke.hu/webview?infile=&sobj=9276&source=webvd&cgimime=application%2Fpdf%0D%0A> Download date: 2024.10.11 10:23:10
- [18] IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications A

- [19] "IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN," in *IEEE Std 802.11ax-2021 (Amendment to IEEE Std 802.11-2020)*, vol., no., pp.1-767, 19 May 2021, doi: 10.1109/IEEESTD.2021.9442429.
- [20] <https://mrnciew.com/wp-content/uploads/2014/10/cwap-mgmt-auth-01.png?w=768&h=153> Download date: 2024.10.08 08:06:24
- [21] CWAP Certified Wireless Analysis Professional Official Study Guide (Exam PW0-205) First Edition ISBN 0-07-225585-4 https://www.cwnp.com/wp-content/uploads/pdf/CWAP_WLAN_ANALYSIS.pdf Download date: 2024.10.08 08:02:13
- [22] E. Martin, "Fragility of the Robust Security Network: 802.11 Denial of Service," 7th International Conference on Applied Cryptography and Network Security, 2009.
- [23] <https://www.researchgate.net/profile/Ayaskanta-Mishra/publication/321341034/figure/fig7/AS:668811866939395@1536468583145/shows-a-comparison-between-the-frame-structure-of-IEEE-80211-and-IEEE-802154-1-It.ppm> Download date: 2024.10.06 02:12:34
- [24] https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcS4-45XJuXk4b2fFQQm2TqgwLcgWn_KYrCAeg&s Download date: 2024.10.08 06:12:36
- [25] https://www.firstquadcopter.com/wp-content/uploads/2020/09/SG906_PRO_2_review.jpg Download date: 2024.10.07 09:08:22
- [26] https://m.media-amazon.com/images/I/51lgXiiHwL.AC_UF1000,1000_QL80.jpg Download date: 2024.10.08 08:06:24
- [27] https://mezohir.hu/wp-content/uploads/2021/10/abz_blogcikk_genetikai_potencialfelmeres2.jpg Download date: 2024.10.08 11:04:34
- [28] Choi, N., Seok, Y., Kwon, T. *et al.* Multicasting multimedia streams in IEEE 802.11 networks: a focus on reliability and rate adaptation. *Wireless Netw* **17**, 119–131 (2011). <https://doi.org/10.1007/s11276-010-0268-9>
- [29] https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html Download date: 2024.10.06 04:16:26
- [30] https://www.cisco.com/c/dam/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.fm/jcr_content/renditions/mcst_ovr-01.jpg Download date: 2024.10.04 06:34:22
- [31] https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html#wp1008769 Download date: 2024.10.04 09:26:44
- [32] https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html#wp1008769 Download date: 2024.10.01 12:45:45
- [33] https://www.cisco.com/c/dam/en/us/td/i/000001-100000/60001-65000/60001-61000/60074.ps/jcr_content/renditions/60074.jpg Download date: 2024.10.08 06:56:21

- [34] <https://collmot.com/company-info> Download date: 2024.10.01 08:16:04
- [35] <https://www.docker.com/resources/what-container/> Download date: 2024.10.06 10:34:12
- [36] <https://docs.docker.com/get-started/docker-overview/> Download date: 2024.10.07 08:23:21
- [37] <https://www.ibm.com/topics/microservices> Download date: 2024.10.06 09:05:21
- [38] <https://aws.amazon.com/microservices/> Download date: 2024.10.04 23:12:34
- [39] <https://grpc.io/docs/what-is-grpc/core-concepts/> Download date: 2024.10.05 22:23:20
- [40] E. Martin, "Fragility of the Robust Security Network: 802.11 Denial of Service," 7th International Conference on Applied Cryptography and Network Security, 2009.
- [41] K. N. Kadripathi, L. Y. Ragav, K. N. Shubha and P. H. Chowdary, "De-Authentication Attacks on Rogue UAVs," in 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020.
- [42] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson and W. Alexis, "Securing commercial WiFi-based UAVs from common security attacks," in MILCOM 2016 - 2016 IEEE Military Communications Conference, 2016.
- [43] A. D. Seth, S. Biswas and A. K. Dhar, "De-Authentication Attack Detection using Discrete Event Systems in 802.11 Wi-Fi Networks," in 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2019.
- [44] M. Alhamry and A. Alomary, "Exploring Wi-Fi WPA2-PSK protocol weaknesses," in 2022 International Conference on Data Analytics for Business and Industry (ICDABI), 2022.
- [45] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N. C. Luong, D. Niyato, F. R. Yu and M. Guizani, "Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, vol. 23, pp. 2802-2832, 2021.
- [46] Y. Kristiyanto and Ernastuti, "Analysis of Deauthentication Attack on IEEE 802.11 Connectivity Based on IoT Technology Using External Penetration Test," CommIT (Communication & Information Technology) Journal 14(1), 2020.
- [47] J. Farlik, M. Kratky and J. Casar, "Detectability and jamming of small UAVs by commercially available low-cost means," in 2016 International Conference on Communications (COMM), 2016.