UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

SecAuthUAV:
an authentication protocol for UAVs

Dott. Gabriele Voltan

OUTLINE

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- IoD: types of UAVs, their applications, security and safety
- The mysterious DJI case: the importance of open source
- Problems and limitations of UAVs
- System and Threat model
- Security goals
- SecAuthUAV: phases and operation
- Security analysis
- Attacks and Vulnerabilities
- Security and Performance comparison
- Conclusions

TYPES OF UAVs

- NATO classification divides them into three categories:

Class I

Class II

Class III

CIVIL APPLICATIONS OF UAVs

- Photography, videomaking, cinematography
- Precision agriculture
- Civil engineering
- Monitoring and coordination of environmental disasters
- Transporting material
- Providing connections in remote places
- Humanitarian rescue operation
- Drone-based light show

MILITARY APPLICATIONS OF UAVs

- Reconnaissance
- Command and Control
- Combat
- Target tracking
- Signal Intelligence (SIGINT)
- Logistic

NOT ONLY SECURITY... ALSO SAFETY

DJI

- DJI, a Chinese company that produces remotely piloted flight systems
- In 2018 DJI occupies more than 70% of the global civilian drone market

- NOT JUST DRONES: DJI sells Aeroscope, a device that allows law enforcement to locate DJI drones and the pilot operating them

- PROBLEM: DJI encodes its firmware in a proprietary file format encrypted with AES and signed with RSA

DJI PROPRIETARY PROTOCOLS

- OcuSync: DJI radio protocol, which encrypts all packets with AES, using a key generated when the UAV is turned on with a PNRG

- DUML: DJI Universal Markup Language format, used to set the internal parameters of the drone, such as maximum speed and maximum altitude that can be reached, and for commands between the RC and the drone

- DroneID: DJI proprietary tracking protocol, designed to transmit the position of both the drone and its operator to authorized entities

MYSTERIOUS CASE OF DJI's DroneID

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- PROMISE: DroneID packets are encrypted and only the authorities can decrypt them

- After reverse engineering the drone's firmware, it was discovered that the protocol did not encrypt packets
- Spoofing the pilot's location: no check is performed regarding the consistency of the coordinates → Aeroscope unreliable
- It has been found a DUML command that allows to disabling the different DroneID values

PROBLEMS AND LIMITATIONS OF UAVs

- Use of cryptographic keys:
  - Capture of drones and key theft
  - Limited computational capabilities → running common encryption algorithms is not trivial
  - Limited memories

- One possible solution is to use Physical Unclonable Functions (PUFs)

PHYSICAL UNCLONABLE FUNCTIONS (PUFs)

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- Mechanism usable for low-cost authentication and key generation
- They receive a challenge C as input and return a response R = PUF(C) as output
- GENERAL IDEA: uniqueness of their physical microstructure, due to random factors introduced during the manufacturing process

Impossible to clone both physically and mathematically

- Strong vs Weak PUFs: the main difference between the two is the size of the challenge-response space that the function has

PHYSICAL UNCLONABLE FUNCTIONS (PUFs)

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- PRO: they avoid the use of memories to memorize cryptographic keys
- PRO: PUF hardware uses simple digital circuits that are easy to fabricate and consume less power and area than a standard memory
- PRO: Invasive attacks are more difficult to execute without modifying the physical characteristics from which the secret is derived

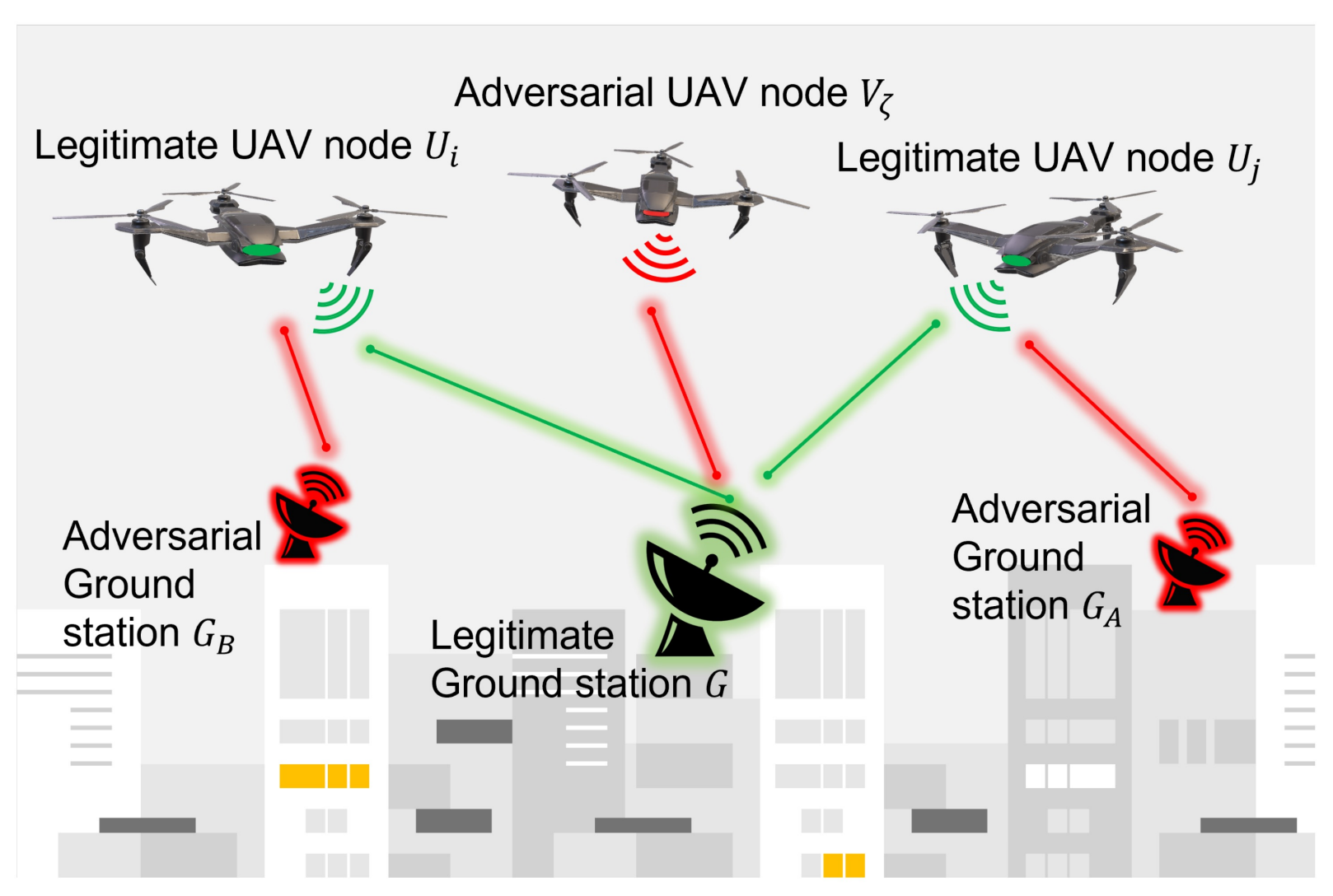
- Thanks to these characteristics they can be a valid substitute for cryptographic keys

SYSTEM MODEL

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- Consists of a series of UAVs and a GS ground station, whose common goal is to authenticate each other
- Once a mutual authentication between UAV and GS has been achieved, it will be possible to perform a mutual authentication between two UAVs, using the GS as trusted third party
- Each UAV has a PUF, which is used to generate a response to a challenge received as input

THREAT MODEL



THREAT MODEL

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- ASSETS:
  - The various legitimate UAVs and the legitimate ground station
  - Furthermore, we can also consider human beings and the flying environment as assets

THREAT MODEL

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- ATTACKERS:
  - Malicious ground station that wants to take control of legitimate UAVs
  - Malicious UAVs that want to send false information to legitimate ground stations
  - Human persons who want to capture the drone to extract secret information or to tamper with it

THREAT MODEL

- ATTACK VECTORS:
  - Masquerade attack
  - Man-in-the-middle attack
  - Eavesdropping
  - Replay attacks
  - Physical attacks

- These are the attacks that can be made on an authentication process, but obviously they are not all possible attacks on a UAV-GS system

ASSUMPTIONS

1) All UAVs have limited computational capacity and memory, while GSs have no limits

2) No UAV stores secret information. The secret used in the protocol is the response R generated by the PUF, after receiving the challenge C

3) Every legitimate UAV has a PUF, as described in the system model. In case of capture, any attempt to tamper with the PUF will make it unusable, and therefore the UAV will no longer be able to authenticate

SECURITY GOALS

1) Achieve mutual authentication between legitimate UAVs and GS ground station

2) The protocol must resist masquerade, man-in-the-middle, and replay attacks

3) The protocol must resist cloning and physical attacks, such as capture of the UAV and tampering with it

SECURITY GOALS

4) The protocol must generate a unique session key for each authentication session

5) If messages are tampered with, the receiving node must notice and abort the authentication process

6) No unauthorized authority should be able to trace the temporary ID of the UAV, in order to guarantee the anonymity of the UAV

SecAuthUAV PROTOCOL

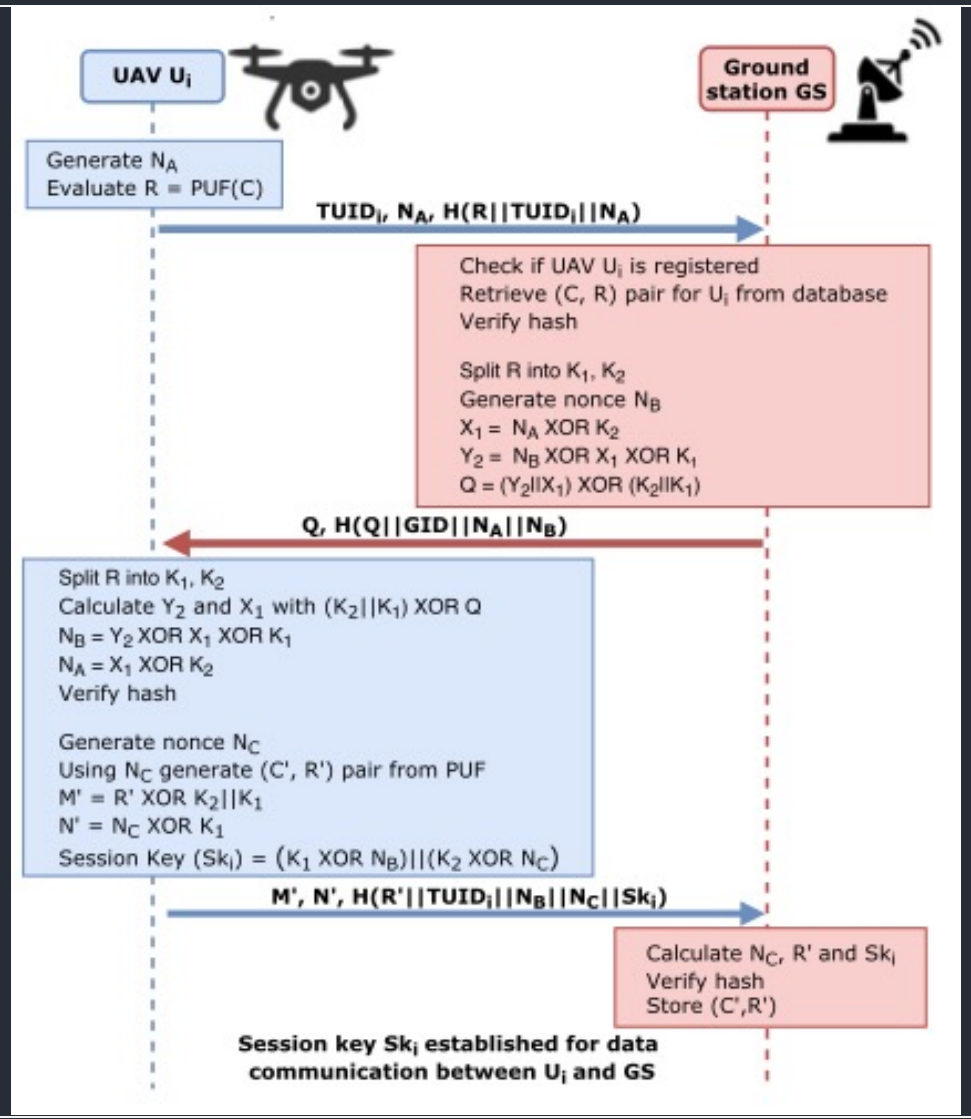
- The protocol is divided into three phases:
  1. UAV Registration Phase
  2. UAV-GS Authentication Phase
  3. UAV-UAV Authentication Phase

UAV REGISTRATION PHASE

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

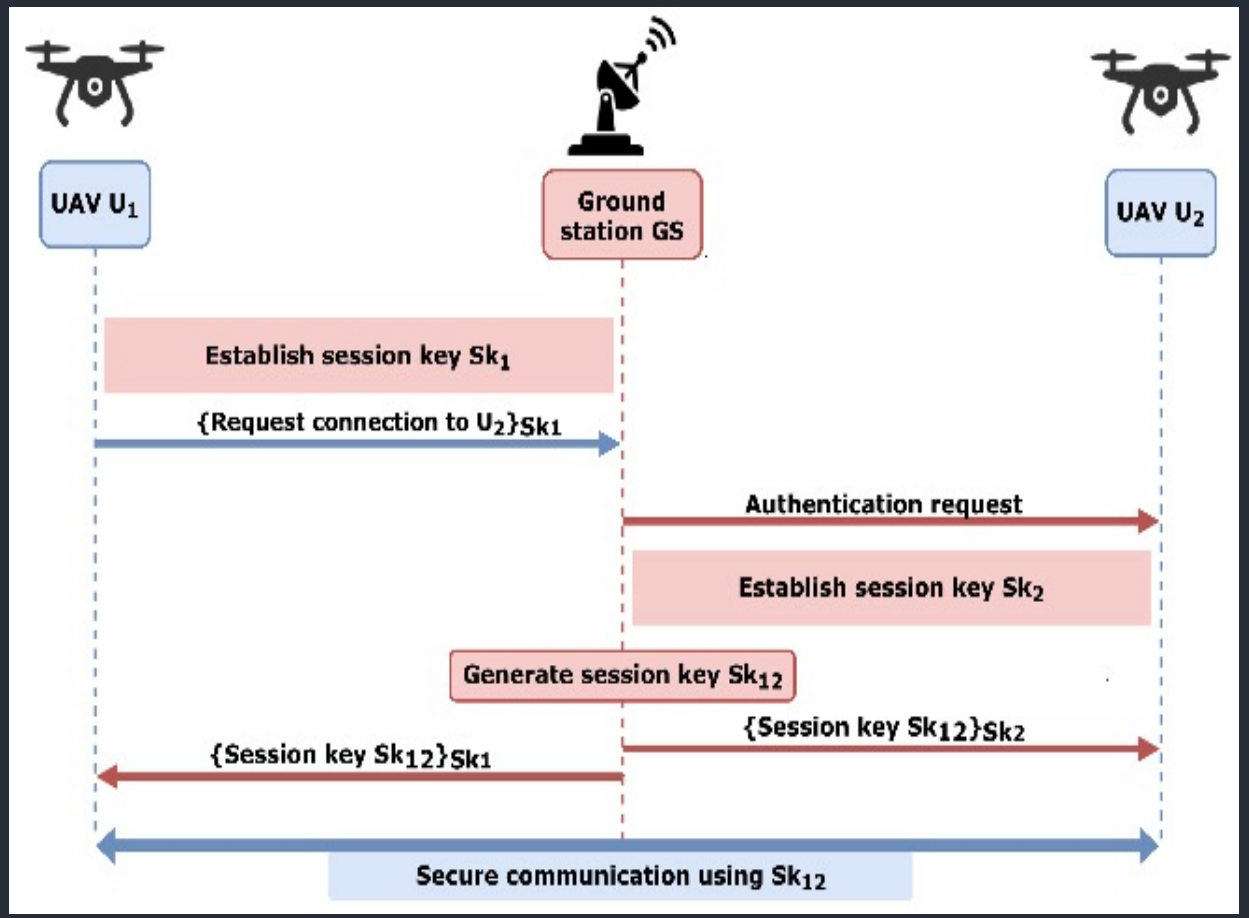
- This phase takes place before the take-off of the UAV, using a secure channel
- Three simple steps:
  1. The ground station generates a challenge C and a temporary ID for the UAV (TUID) and sends everything to the UAV
  2. The UAV calculates the answer R = PUF(C), sends it to the GS and stores in its memory the triple {TUID, C, GID}
  3. The GS, after receiving the response R, stores the triple {TUID, C, R} in its database

UAV-GS AUTHENTICATION PHASE



- R is the secret that only the two trusted parties can know → it is comparable to a symmetric key
- Nonces are used to ensure message freshness → anti-replay mechanism
- A fresh session key is calculated, which will be used for future communications
- TUID' = H(K_2 || TUID ||K_1)

UAV-UAV AUTHENTICATION PHASE



- Phase that can only take place after two UAV-GS auth phases
- GS is used as a trusted third party
- Using the symmetric keys between UAV and GS, the symmetric one between UAV and UAV is sent

SECURITY ANALYSIS

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- Formally verified using Mao Boyd logic
  - "U believes N_B is a good secret between U and G"
  - "G believes N_B is a good secret between U and G"
  - The same is proved also for N_C and R'
  - Without N_B, N_C and R' the adversary cannot understand the meaning of the communication

- In the future it will be analyzed using ProVerif

ATTACKS AND VULNERABILITIES

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- With the assumptions made by the authors on the PUF, the protocol does not report any vulnerabilities
- Physical attacks tamper with the PUF, altering it and rendering it unusable

- Vulnerabilities discovered on PUFs:
  - Cloning:
    - combination of machine learning and side-channels
    - response prediction with machine learning algorithms after observing a given number of (C,R)

BUT ARE THEY A PROBLEM FOR THE IoD?

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- The attacks presented require a physical capture of the drone
- Let's consider two scenarios:
  a. UAV is captured during a flight phase: both in the case of a civilian drone and a military drone, the pilot will consider the UAV as lost/captured/shot down
  b. UAV is captured on the ground:
     - Military scenario: capture practically impossible given surveillance
     - Civilian scenario: capture possible, but overall attack complexity increases
- We can conclude that for the IoD area these are not problematic attacks

SECURITY COMPARISON

- SecAuthUAV:
  - Is resistant to known attacks (MIMT, replay attack, masquerade, node tampering, cloning attack, de-synchronization attack)
  - Provide a fresh and secure session key after each successful auth process
  - Uses nonce instead of timestamp
  - Provide mutual authentication
  - Ensures the anonymity of the UAV
  - Ensures forward secrecy
- Other protocols:
  - They implement no defenses against tampering or cloning and use synchronized clocks
  - They do not guarantee the anonimity of the UAV

PERFORMANCE COMPARISON

- Run with NodeMCU v3.0 and Raspberry Pi 3B, using both C and Python

1. *Test in both env, using C*: SecAuthUAV is the most efficient
2. *Test with Rspb, using both C and Py*: SecAuthUAV is the most efficient
3. *Communication cost*: second place for only 64 bits (avg: 1670 bits)
4. *Minimum storage cost*: second place for only 32 bits (avg: 487 bits)

CONCLUSION

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- SecAuthUAV ensures mutual authentication and forward secrecy
- Uses PUFs avoiding tampering and cloning attacks
- It is resistant to known attacks
- Guarantees the anonymity of the UAV
- Does not use synchronized clocks
- It is safer than other protocols
- It is more efficient than other protocols

READING TIPS

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

- Civil Drones. Tactical Imagery Intelligence per la sicurezza e la difesa. Sabatino Coluccia
- Droni. Security, safety, privacy ed etica. Sistemi aeromobili a pilotaggio remoto: il future dell'aviazione militare e civile. Paolo G. Piccioli

THANKS FOR THE ATTENTION

DOTT. GABRIELE VOLTAN

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura