The Challenges of Securing and Defending Lighweight Unmanned Aerial Systems

Mike Burmester, Dan Schwartz and William Goble, Ryan Sloan, Sophia Villalonga, Jordan Gethers, Laura Battle

Computer Science Department, Florida State University

SUMMARY

We investigate the impact of cyberthreats on lighweight unmanned aerial systems (UASs) and in particular lighweight Flying ad hoc Network (FANET) systems. We propose secure and resilient architectures for autonomous UAS applications that address the CNSSP-28 [1] criteria for protecting & defending UASs against hostile cybersecurity threats.

SALIENT FEATURES

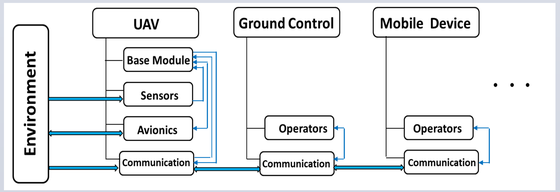
- Investigate the challenges of securing lightweight Flying Adhoc Network (FANET) systems.
- Design and evaluate protection mechanisms/architectures through SITL & HITL testing and simulations.
- Design secure operations architecture for FANET autonomous systems.

MAIN CONTRIBUTIONS

1. Develop an architecture for secure & resilient UAS. In particular, that protects & defends
   - Command and control (C2) transmitted data
   - Transmitted data that is not releasable
   - Continuous monitoring
   - Remotely controlled links for mission termination.
2. Develop methodologies, policies & mechanisms to protect and defend FANET architectures that offer real-time ongoing security awareness.
3. Design and test (SITL, HILT) real time lightweight protection mechanisms for UAS applications.
4. Design secure autonomous & intelligent FANET architectures to:
   - Monitor environmental events, or for tactical operations
   - Minimize search & rescue time when natural or man-made constraints endanger missions (dynamic randomized boundless search using behavior-based AI augmented algorithms)
   - Support 5G and beyond emergency communications and tactical operations (restore/establish connectivity)
   - Optimize real-time visual on board target tracking with deep convolutional neural network detectors, by distributing detection/ tracking tasks among drones.

UNMANNED AERIAL SYSTEMS (UAS)

A UAS consists of an unmanned aerial vehicle (UAV), a Ground Control Station (GCS), and one or more mobile devices (control interfaces). The basic components of the UAV are: the *Base Module (BM)*, the *Sensors Module*, the *Avionics* and the *Communication Module*.



The BM contains the flight control of the UAS: the OS (firmware, middle-ware and software) that links all the UAV components and controls the Sensor, Avionics and Communication modules. The Sensor Module consists of the sensory equipment with integrated functionalities. The Avionics Module converts received navigational and control commands to commands for engines, flaps, rudder, stabilizer and spoilers. Continuous availability of navigational data is assured by an inertial navigation system whose drift is compensated using global position system (GPS) measurements. The GCS is paired with the BM.

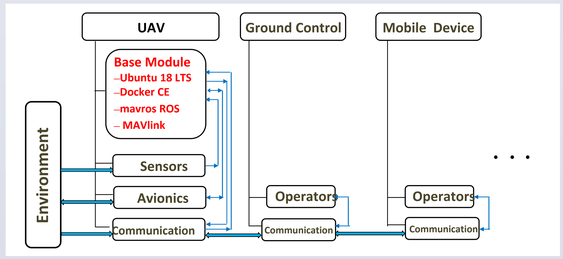
THREAT MODEL

The goal of the attacker is to exploit system vulnerabilities, while the goal of the system designer is to eliminate vulnerabilities. Despite the apparent symmetry, the threat model is highly asymmetric: the attacker just needs to find one exploit, whereas the designer must eliminate exploits before the attacker finds them, or mitigate their impact (for system resilience). For security analysis the adversary is modeled by a probabilistic polynomial time Turing machine that controls the communication channels, and may eavesdrop, block, modify and/or inject messages in any communication between parties (Dolev-Yao model). The adversary may also corrupt stored data, but not secret keys. Security is typically defined in terms of indistinguishability (*semantic security*). For complex systems such as UASs, security should be holistic, and an ongoing process that involves continuous monitoring, risk awareness/assessment and tolerance [2].

2. A SECURE & RESILIENT UAS ARCHITECTURE

We are only concerned with the protection of the Base Module that manages/controls the Sensors, Avionics and Communications. Protection should involve process isolation & encapsulation. Container virtualization technology allows for isolated user space instances to run on a single host. Although this may not be as secure as the full isolation of hypervisor virtualization (VMs), it is appropriate for lightweight applications. For the Base Module we propose to use the Docker CE container-based virtualization platform and the Ubuntu18.04 LTS OS.

For the Robotic Operating System (ROS) the mavros ROS package that enables MAVlink extendable communication is proposed.

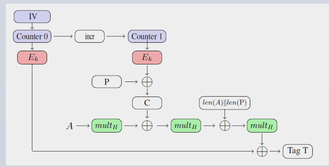


Mechanisms that Protect/Defend UAVs: Securing the Base Module
Protection should involve process isolation & encapsulation. Container virtualization technology allows for isolated user space instances to run on a single host. Although this may not be as secure as the full isolation of hypervisor virtualization (VMs), it is appropriate for lightweight applications. For the Base Module we propose to use the Docker CE container-based virtualization platform and the Ubuntu18.04 LTS OS.

For the Robotic Operating System (ROS) the mavros ROS package that enables MAVlink extendable communication is proposed.

Securing C2 and mission termination links

AES-GCM Authenticated encryption with associated data uses AES encryption and Galois field multiplication to ensure data authenticity and confidentiality. We adapted this algorithm for C2 protection.

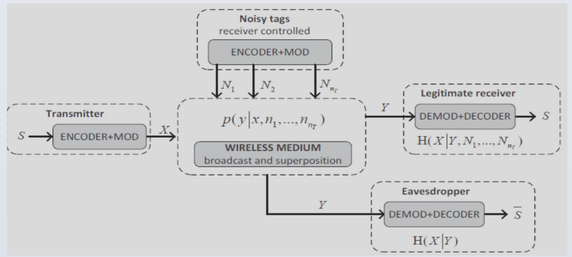


SITL testing with the Ardupilot simulator was used to estimate the additional time for AES-CM protection for C2 communication as $\sim 15\ \mu s$.

Stream authentication. The UAV and GCS share a pair of synchronized pseudorandom number generators (PRNGs) that are used for mutual and anonymous stream authentication. Only two flows (N_{i-1}, N_i) are needed to authenticate the drone, and two flows (N_i, N_{i+1}) to authenticate ground control, $i = 1,2, \ldots$, if the flows are not disrupted; if there is disruption, then the next two flows (N_{i+1}, N_{i+2}), resp. (N_{i+2}, N_{i+3}) are used for synchronization. The protocol is proven secure in the UC Framework (that supports semantic security [2].

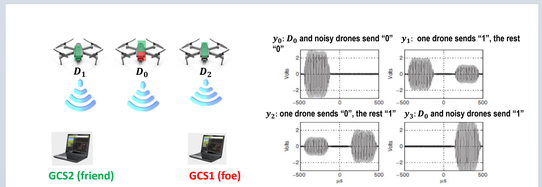
Steganographic protection: Wyner's wiretap channel with noisy drones

Wyner's communication model has two channels: a channel between the legitimate transmitter and the receiver, and a noisy version, called *Wiretap channel* that the eavesdropper can access .



Using Noisy drones to hide c2 and remotely controlled wireless mission termination links.

The approach we propose (based on [4]) uses pseudorandom bits generated by noisy drones to hide obfuscate transmitted signals. In this application the fundamental property of superposition of the wireless medium is used to mitigate eavesdropping with interference at the physical layer to degrade communication. For our application degrading will be controlled by noisy drones that act as interferers. In the Figure below we show how this is done.



a. Drone D_0 and trusted drones D_1, D_2 monitored by GCS1 (foe) and GCS2 (friend).

b. Superpositioned signals y_0, y_1, y_2, y_3 of D_0, D_1, D_2 (Pulse Position Modulation).

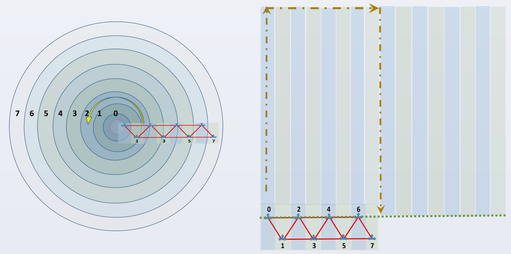
D_0 is a potentially compromised drone (foe), with noisy drones D_1, D_2 (friend) controlled by GCS2; the eavesdropper is GCS1. Figure a. shows two drones D_1, D_2 that transmit pseudorandom bits generated by the synchronized PRNGs G_1, G_2 shared with GCS2. Figure b. shows the superposition of a bit transmitted by G_0 and the bits transmitted by G_1, G_2 (Pulse Position Modulation). Signals y_0, y_3 leak the bit that drone G_0 transmitted to GCS1 (bit 0 and bit 1 respectively), while signals y_1, y_2 hide the bit.

UAS Mission planning

Assign tasks to UAVs → optimise [select routes → check constraints↲]

Optimal path finding for search of a moving target

Agent uses a constrained path defined by a hogoneous Markov chain. Reconnaissance in complex and dynamic environments with randomized sweeps (lawnmower or circular).



A regular UAV tessellation formation is used, with random sweeps of sectors so that an unknown area is uniformly covered.

Flying Ad hoc Network (FANET) systems

- Employing a FANET of drones has many operational advantages compared to flying single drones.
- With FANETs we have drone-to-drone communication & controller-to drone communication.
- The operating range of controller-to-drone communication is reduce
- *Routing protocols for drone-to-drone communication*: reactive (on-demand) and proactive (table driven, eg AODV (as for MANETs)
- *Mobility Models for FANET:*
  - Randomized: Random Walk, Random Way-Point, Random Direction
  - Time/space dependent models:, Gauss-Markov (GM) mobility
  - Path planned: use a predefined shape
  - Group mobility: Reference Point, Nomadic Community, Pursue

FANET systems to support 5G and beyond networks

- Wireless communication can leverage UAVs to provide ubiquitous connectivity for different device types.
- Design and investigate the security of network architectures that supplement/support 5G and beyond services
- Emergency communications
  - Users/devices that struggle with connectivity and data rates
- Tactical operations
  - Setting up adhoc networks where there is no network connectivity

Autonomous AI augmented FANET systems and applications

- Locate & track dispersed targets such as mobile missile launchers
  - for tactical operations
  - for search & rescue missions

REFERENCES

[1] CNSSP No. 28, Cybersecurity of Unmanned National Security Systems. https://www.cnss.gov/CNSS/

[2] NIST, SP 8000-137

[3] Challenges of Securing and Defending Unmanned Aerial Vehicles, *National Cyber Summit*, 119-138

[4] Jorge Munilla, Mike Burmester, Alberto Peinardo, Willy Susillo, RFID owenership transfer with positive secrecy capacity channels. *Sensors*, 17[1]:53, 2017.

ACKNOWLEDGEMENTS

This material is based on work supported by award BAA N00174-19-1-006.