

Improving Security of Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements *A Position Paper*

*Raja Naeem Akram¹, Pierre-François Bonnefoi², Serge Chaumette³,
Konstantinos Markantonakis⁴ and Damien Sauveron²*

¹ Department of Computer Science, University of Waikato, Hamilton, New Zealand

² XLIM (UMR CNRS 7252 / Université de Limoges) Département Mathématiques Informatique, Limoges, France

³ LaBRI, Bordeaux 1 University, Talence, France

⁴ Information Security Group Smart Card Centre, Royal Holloway, University of London, Egham, United Kingdom

Damien Sauveron
<http://damien.sauveron.fr/>

10/09/2014

Roadmap

- Introduction
- Contributions
- Adversary model
 - Capture of UAV by an Attacker
 - Attacks on a “Captured” UAV
 - Attacks on a UAV in a Network
 - Rationale for the Adversary Model
- Requirements
 - Functional Requirements
 - Security Requirements
- Candidate Secure Elements
- Future works: Our vision on how to secure UAVs fleet
- Questions/Discussions

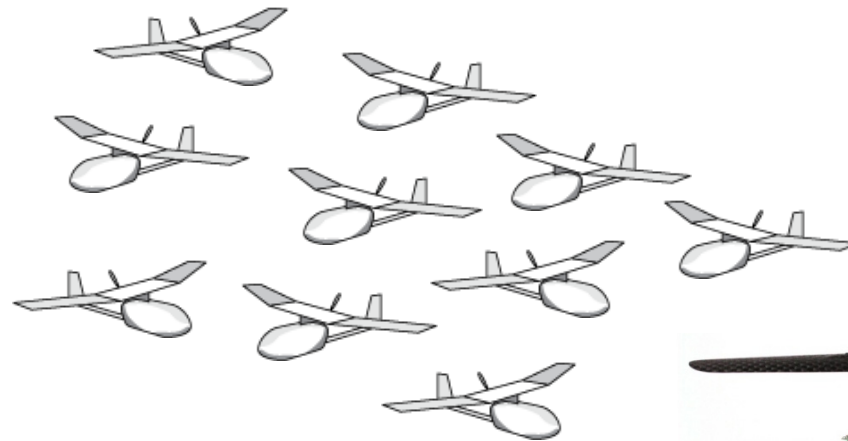
Introduction

- UAVs fleet are more effective and may be costless than a single big drone

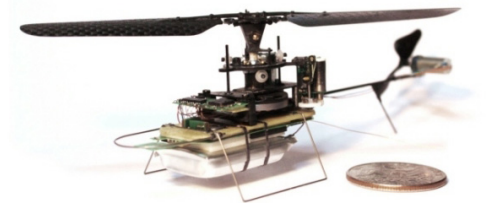


Drone predator

versus



UAVs fleet



Proxy Dynamics PD-100 PRS Black Hornet Prototype

- Each UAV can be equipped with different sensors
- They can collaborate altogether and fly in swarm
- They can cover a larger geographic area
- If one UAV is destroyed, others can continue the mission

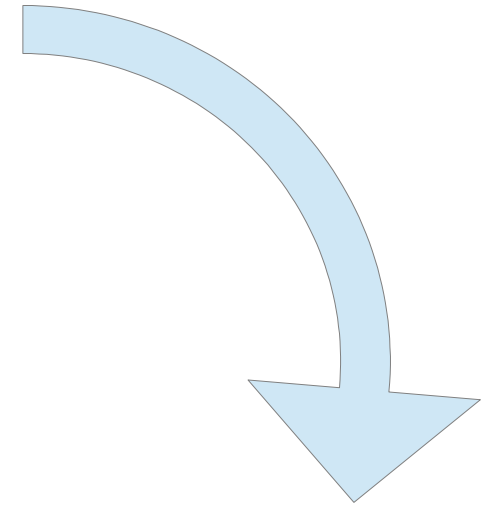
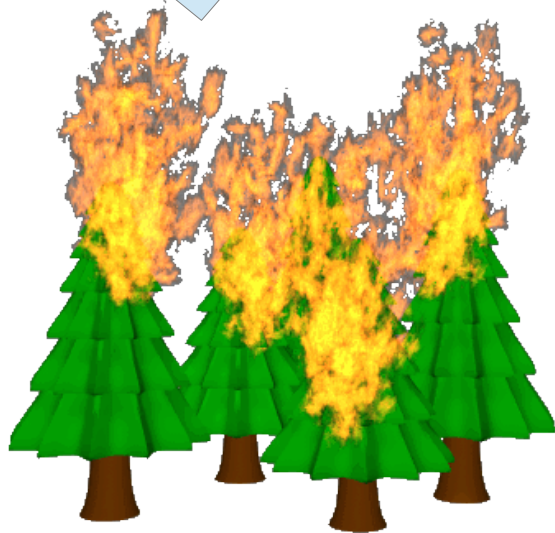
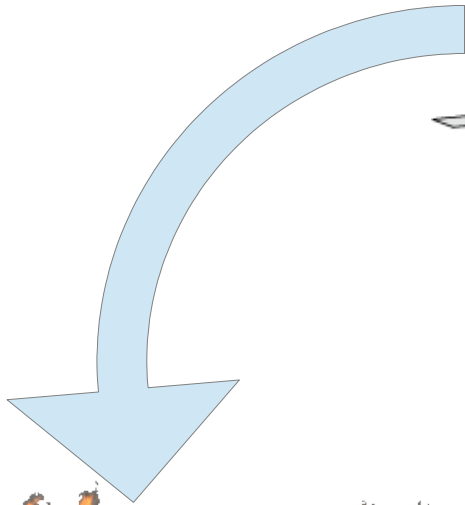
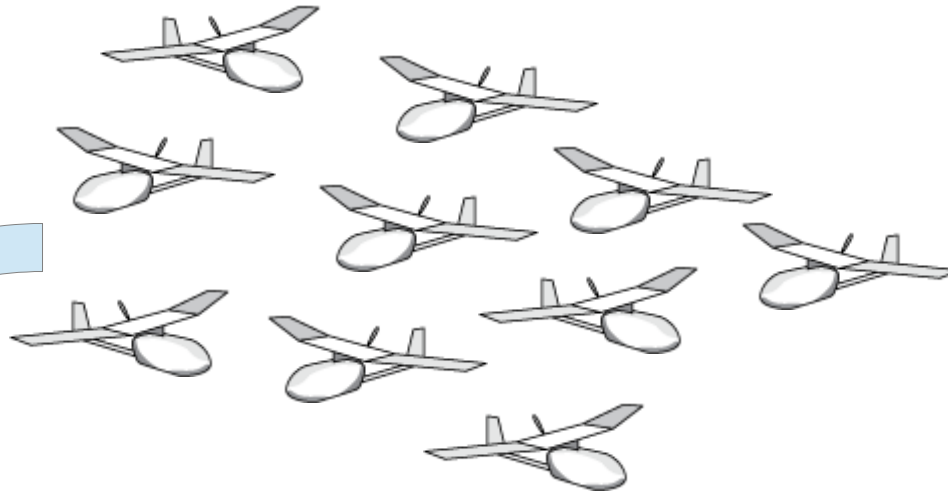


Proxy Dynamics PD-100 PRS Stealthy Look

- For all these reasons UAVs fleets are becoming more apparent.

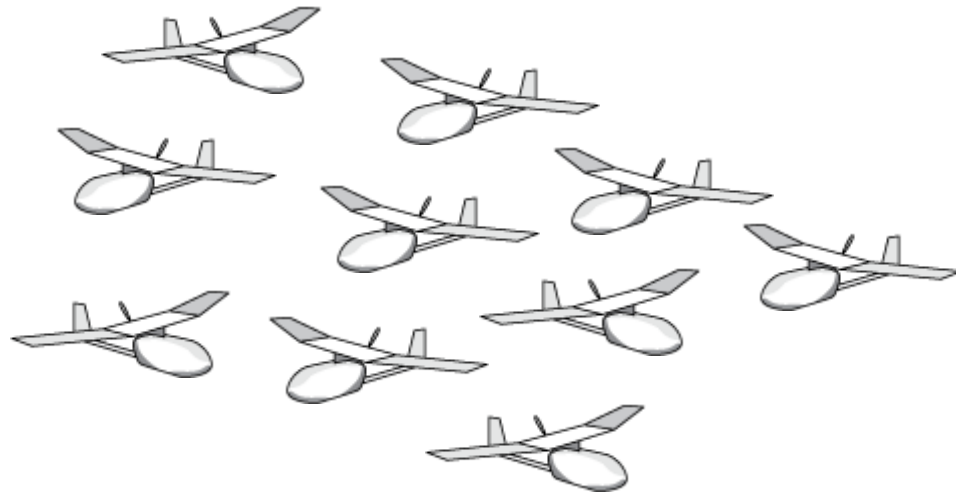
Introduction

- Civilian applications
- Military applications

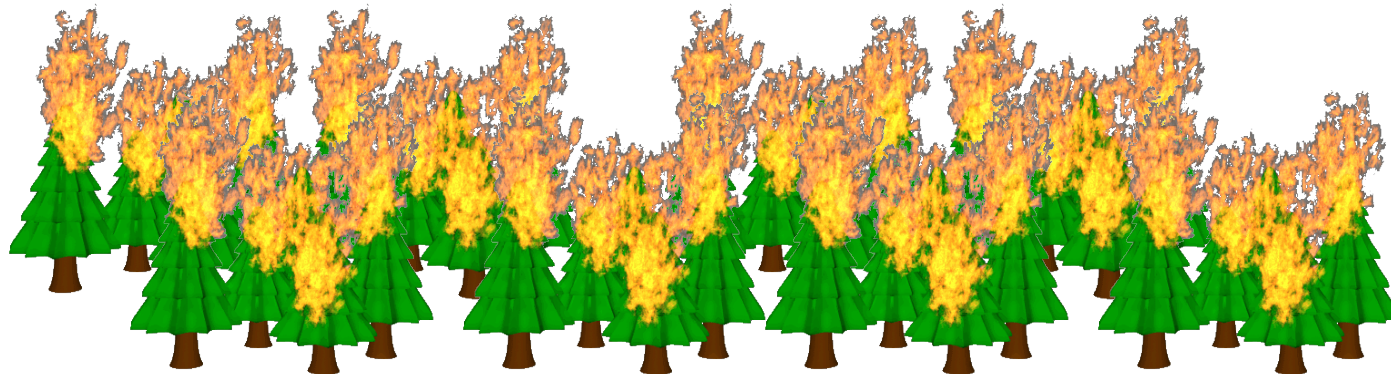


Introduction

- Civilian applications



Security may not be an issue

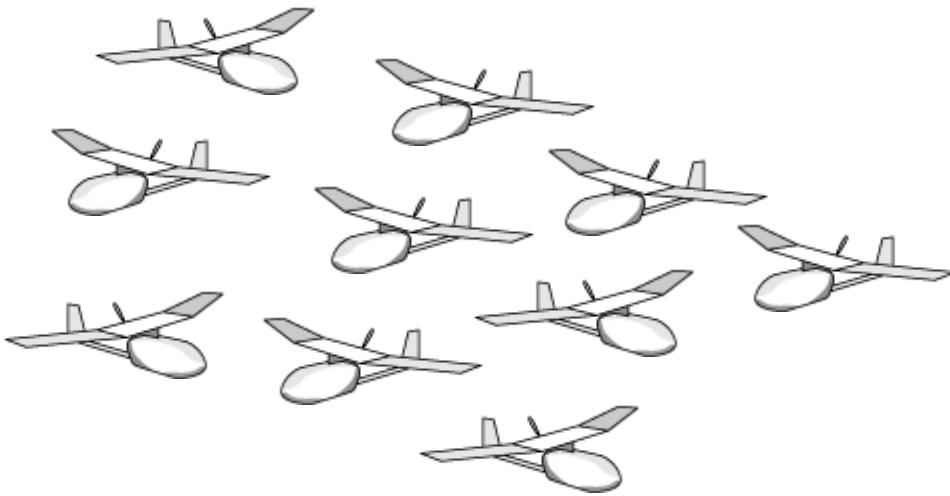


Introduction

- Military applications

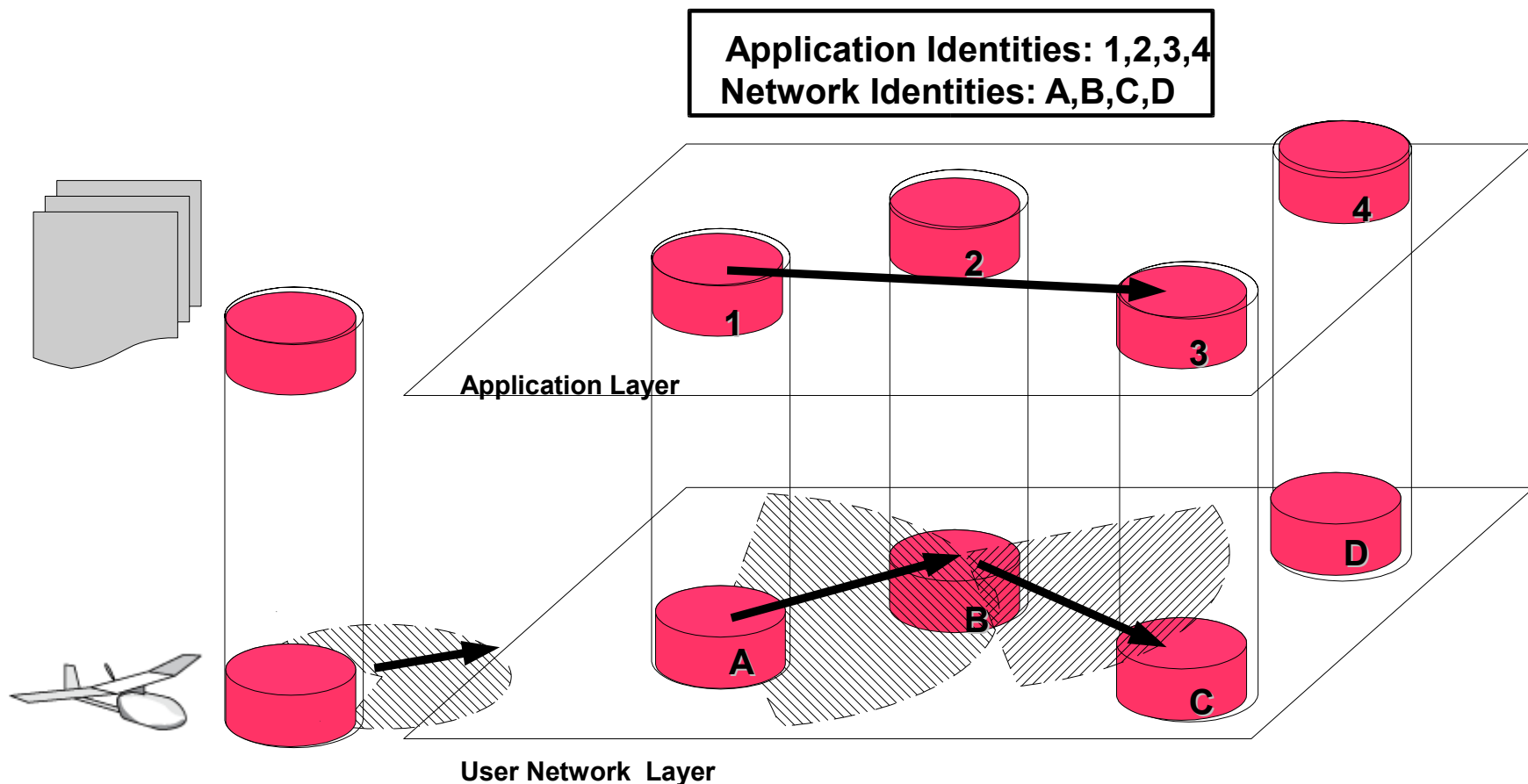
- UAVs may store and exchange lot of assets

- Flight-plan for the mission
- Photos
- Coordinates of points of interest (enemies or allies)



Security is an issue!

Communication in UAVs fleet



- Classical security solutions from world of MANETs are **not sufficient** (reputation, virtual currency, etc.) for the **considered adversary model**

Contributions of this position paper

- We propose an original discussion on the **adversary model** for UAVs fleets
- We define the list of **security requirements** for UAVs fleets
- We propose some insights of how to implement these requirements with embedded **secure elements (SE)**
- We provide a **comparison with existing works** that proposed the deployment of “secure elements” on unmanned vehicles.

Adversary model

- We consider a strong adversary model with a high attack potential.
 - the adversary has capabilities and knowledge to capture a UAV in a functional state



Adversary model

- In a **functional state** means:
 - if there are self destruction mechanisms the attacker is able to bypass or deactivate them



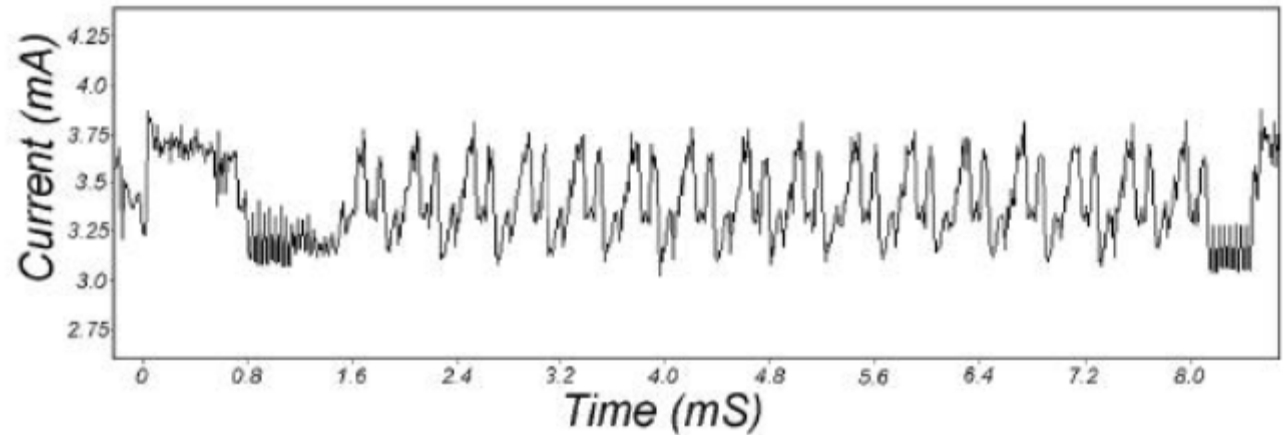
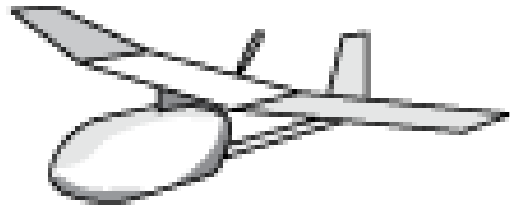
- Worst, the attacker might perform attacks during the flight



Adversary model: which kind of attacks?

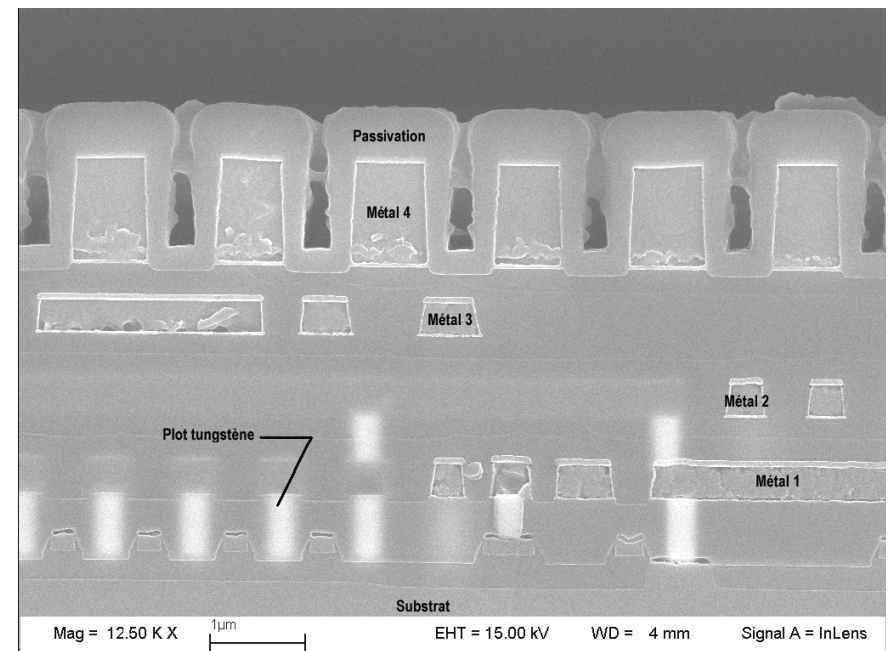
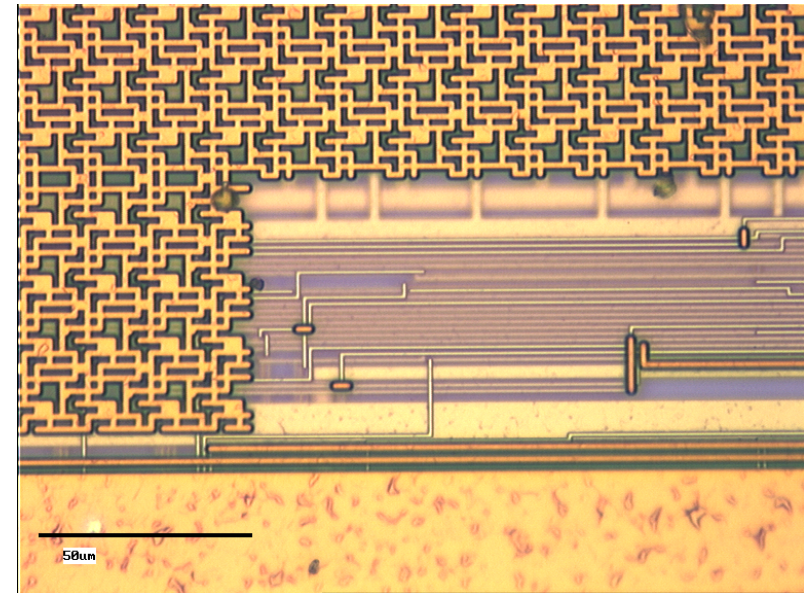
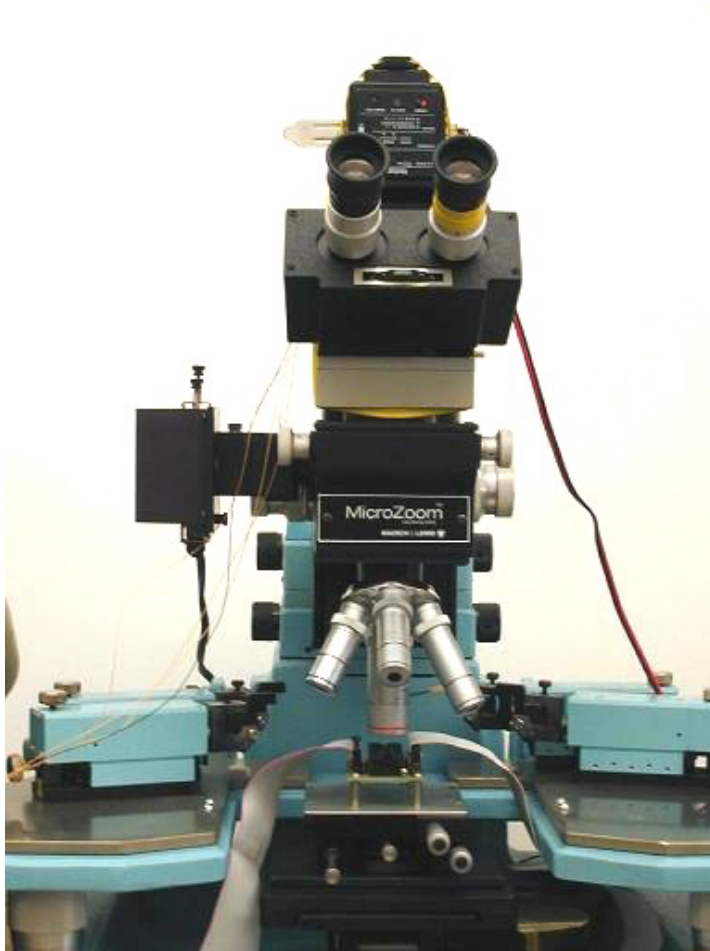
- Side channel attacks

SPA on DES ciphering



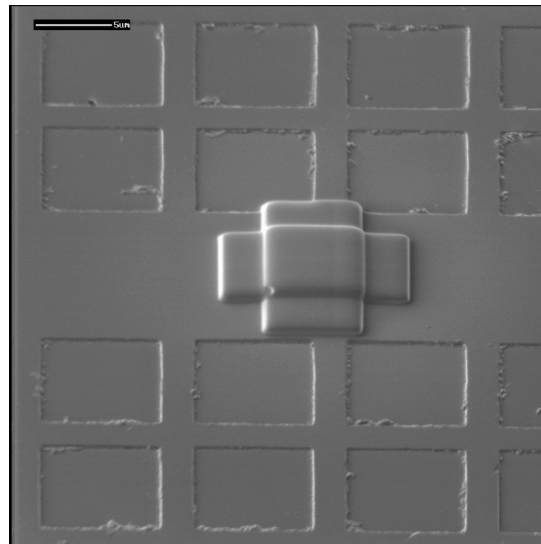
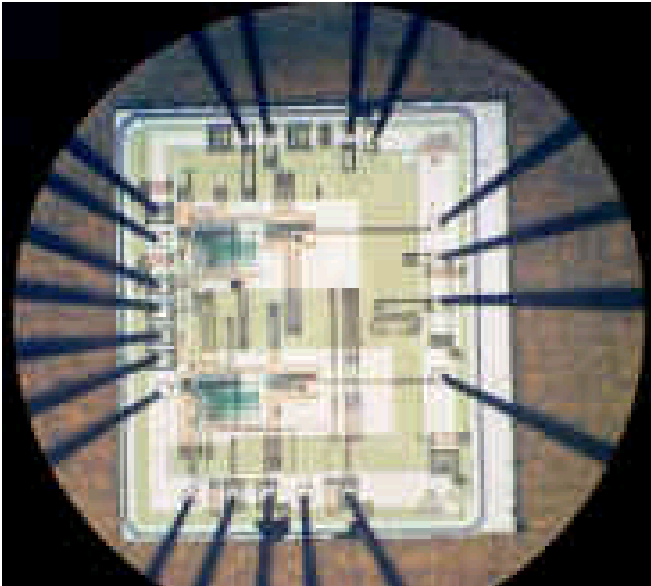
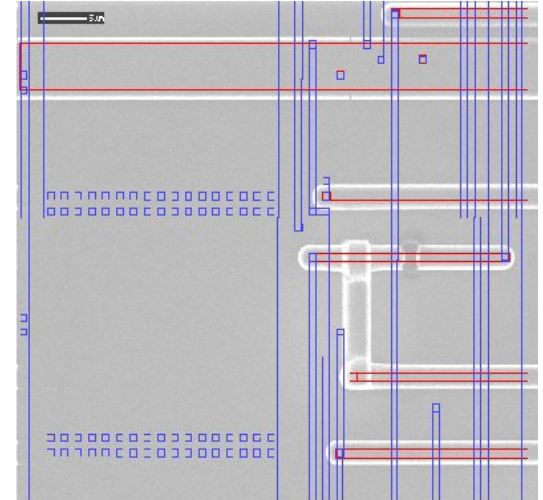
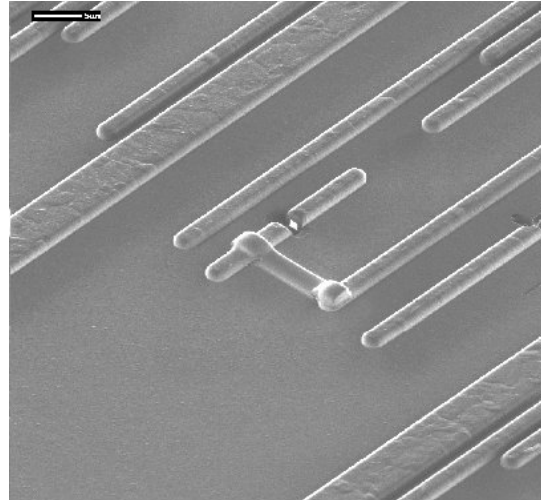
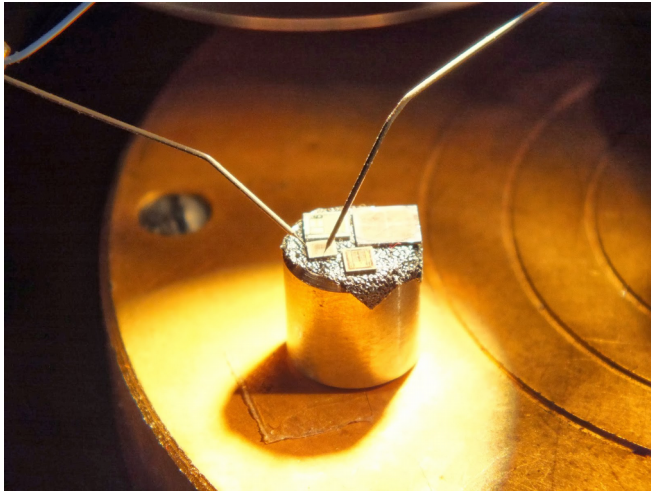
Adversary model: which kind of attacks?

- Fault attacks with a laser



Adversary model: which kind of attacks?

- Physical attacks (microprobing, modification with a Focused Ion Beam System, etc.)



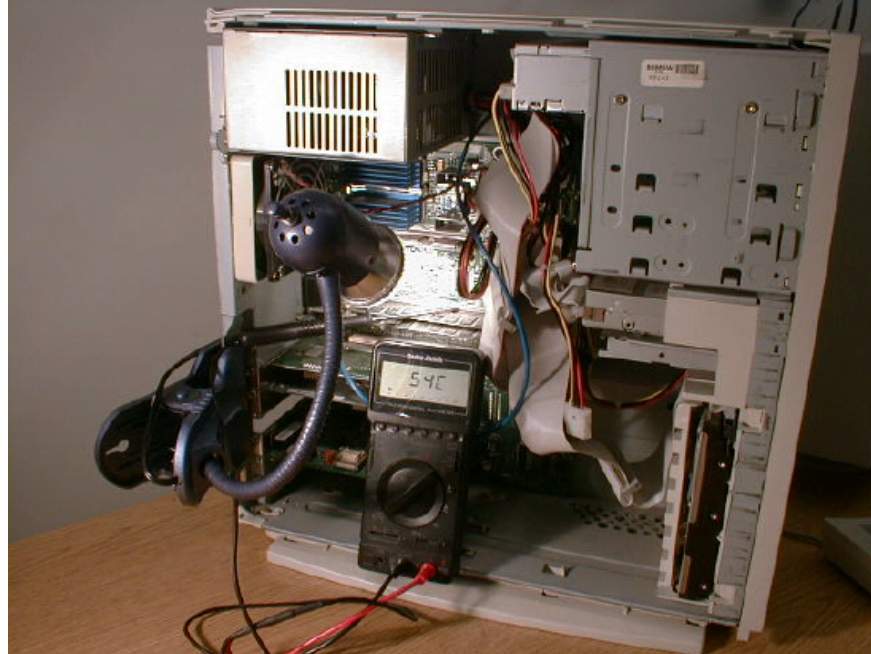
- There exist plenty other attacks referenced in the paper.

Adversary model: which kind of attacks?

- Attacks on a UAV in a Network
 - They are similar to those existing in MANets, DTN and Wireless Sensors Networks
 - The easiest attack is Denial-of-Service (DoS).
 - It can be achieved at physical, link, network or transport level
 - If communications are not ciphered, the opponent can perform eavesdropping, packet injection or corruption and Man-in-the-Middle or relay attacks
 - The attacker can also build a rogue UAV to attempt some attacks on routing protocols (blackhole attack, selective forwarding attack, sinkhole attack, rushing attack, sybil attack, wormhole attack, etc.)
 - Application-specific attacks can also exist (like source authentication).

Adversary model: rationale

- Fault and side channel attacks are already present on other computing systems



- For instance, in 2012, *A. Moradi, M. Kasper, and C. Paar.* have done a Correlation Power Analysis on Virtex-4 and Virtex-5 family, i.e. Xilinx FPGAs that are widely used in UAVs (including the Predator).
 - They have shown that the encryption mechanism can be completely broken **with moderate effort**.

Requirements

- **Functional requirements:**
 - **Autonomy:** The fleet should be autonomous and should not rely on communication with its base/user
 - to be more stealthy in the adversary conditions of the mission
 - **Management:** The fleet should be easy and transparent to manage both in terms of functionality and security
 - management should be possible prior or during the fleet operations
 - **Reliability:** The fleet should be reliable
 - each UAV with a dedicated mission may, for some reasons, decide to entrust its mission to another UAV according to the capabilities in term of equipments (e.g. sensors) and software stack of this UAV.
 - **Efficiency:** A UAVs fleet has to perform optimally in the adversely territories/environments.
 - It thus must be able to analyze the situation and make decisions in real-time.
- ▶ The fleet should be **self-organized** and should be equipped with some sort of **swarm intelligence**.

Requirements

- **Security requirements:**
 - (SR1): The UAV should be SE-driven to ensure security and privacy of its missions.
 - (SR2): The whole UAV should be tamper resistant, or at least a part of it (the SE)
 - (SR3): The UAV should provide assurance in implemented security mechanisms to its user
 - (SR4): The UAV at a very basic level should provide a secure unique ID on which the whole fleet can rely for its management and networking operations
 - (SR5): The UAV should provide secure key management and cryptographic features to protect communication integrity and confidentiality among the members of the fleet

Requirements

- **Security requirements:**
 - (SR6) UAV should provide a secure storage for data collected (e.g. measurements, photos) and/or those used for the purpose of the mission (e.g. flight-plan for the mission, coordinates of points of interest)
 - (SR7) The UAV should provide a secure multi application platform
 - this requirement is justified since in the context of SE-driven UAV there will be installation of new applications, transfer or update of applications
- **An additional functional requirement may be optionally added if the context of SE-driven UAV is accepted:**
 - (FR5) the SE may have its own communication capabilities to communicate with other SEs which can form an overlay network (for specific control operations)

Candidate Secure Elements

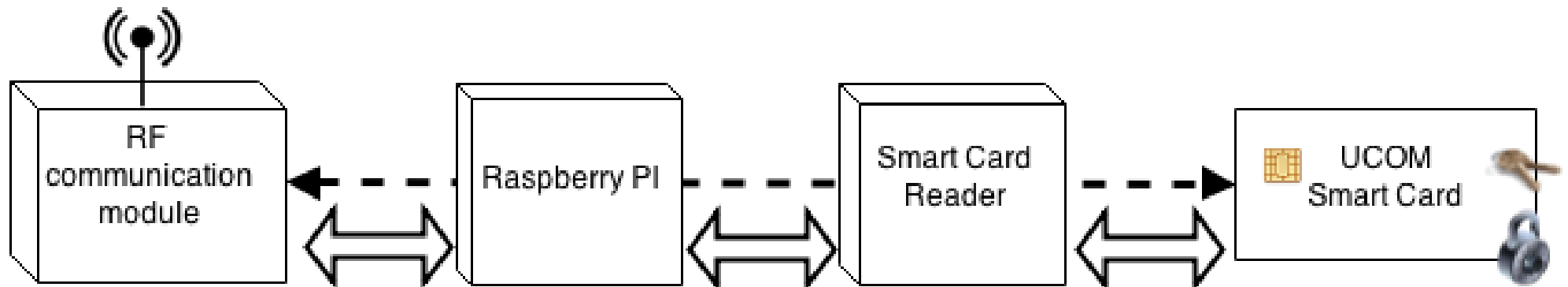
- **Wireless Sensor Node**
 - It has communicating capabilities that would satisfy FR5
 - However a WSN cannot be the SE because in case of capture it fails to satisfy most of the security requirements
- **Trusted Platform Module**
 - Fails to satisfy several security requirements:
 - SR3 for which the device has to provide an assurance of its own security
 - SR6 as it does have small (secure) storage but mostly for cryptographic material
 - It cannot execute code, thus it fails to satisfy SR1, and SR7

Candidate Secure Elements

- **Smart Card** intrinsically supports SR2 to SR6
 - User Centric Smart Card Ownership Model (UCOM):
 - It provides a dynamic, scalable and flexible architecture for multi-application platforms
 - the UCOM proposal of Trusted Execution and Environment Manager (TEM) has the potential to provide a strong trusted device and (application) execution architecture
 - do not possess the long range RF communication capabilities required by FR5
- **Active RFID**
 - At best, current Active RFIDs are only supporting SR4, SR5 and FR5.

Our proposal

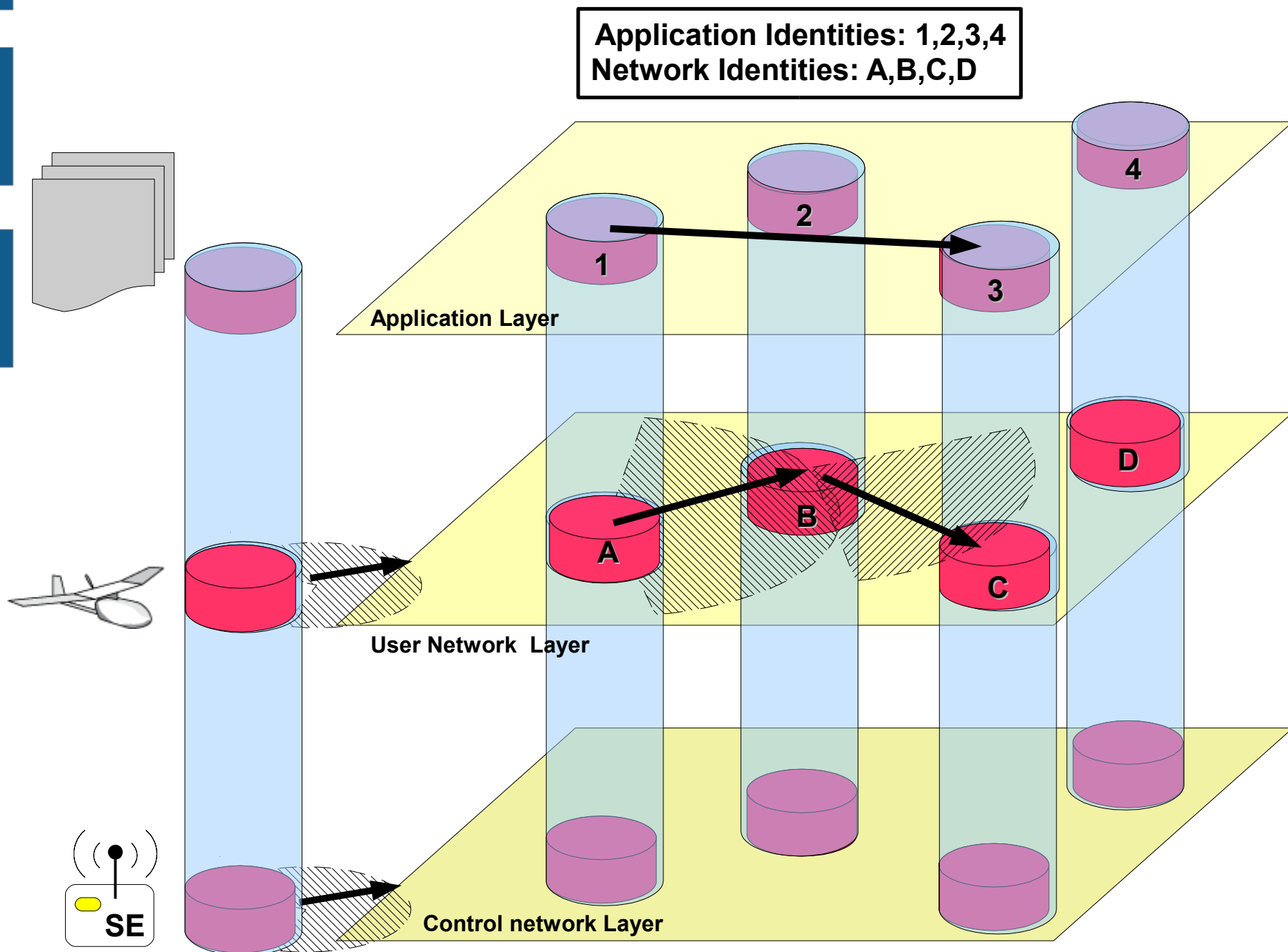
- Active Radio Frequency Smart Secure Device (ARFSSD)
 - our first prototype will be based:
 - on an ARM-based platform as the ubiquitous Raspberry Pi embedding Linux and the PC/SC middleware
 - on a smart card reader
 - on the UCOM smart card
 - on the RF communication module



Summary

	SR1	SR2	SR3	SR4	SR5	SR6	SR7	FR5
WSN								X
TPM		X	X	X	X	X		
Smart Card	X	X	X	X	X	X	X	
Active RFID				X	X			X
Our proposal	X	X	X	X	X	X	X	X

Future works: Our vision on how to secure UAVs fleet





**Questions?
Discussions!**