IEEE VTS

Connecting the Mobile World

WEBINAR SERIES ON ADVANCED MOBILITY

Acknowledgement

The presenter wishes to acknowledge the IEEE Vehicular Technology Society for their sponsorship of the Webinar Series on Advanced Air Mobility.

WEBINAR SERIES ON ADVANCED MOBILITY

Security in V2X Communications for UAS Networks

Dr. Gürkan Gür

Zürich University of Applied Sciences (ZHAW)

November 2024

About Me (Highlights)[1]

Current position: Senior Lecturer @ ZHAW, member of InIT ISE Group

Education:

Bogazici University, Istanbul, TURKEY. Ph.D. in Computer Eng., 2013

- In addition to academia, more than 10 years of experience in technology companies ("on-off" mode)
- Involved in various Horizon 2020, Horizon Europe, ITEA, CELTIC, Innosuisse, and TÜBiTAK (TR) research projects as senior researcher, project coordinator and academic consultant
- >100 scholarly papers, two patents (1 US, 1TR), IEEE senior member, ACM member
- Currently, a member of the IEEE 1920.2 Vehicle to Vehicle Communications for Unmanned Aircraft Systems and the IEEE 3349 Space System Cybersecurity Work Groups

Current key research interests: Information security, Future Internet, Critical Infrastructure Protection (space cybersecurity)

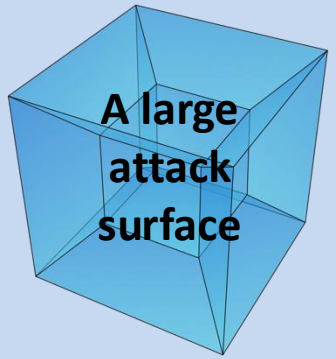
[1] More information: www.zhaw.ch/en/about-us/person/gueu/

Outline

Key message:

UAS networking security

$$\frac{\text{Vulnerabilities} \times (\{\text{Cyber} + \text{Physical}\}\ \text{sec\_issues})}{\text{Resource constraints} + \text{Heterogeneity}} =$$



- Outline:
  - Security in V2V UAS Networks
  - Challenges
  - What to consider for security solutions
  - IEEE 1920.1/2 WG outcomes

Security aspects in UAS networks

Physical security

As CPS, open to physical manipulations (compare that to a data center)

Use-case driven, close interaction with the physical world

Cybersecurity

Connected systems

Ad hoc mode («pure» U2U)

Infrastructure-based mode (tethering to 5G, 6G, NextG ...)

Hybrid mode

May become a security threat on its own.

Mission critical services emerging ...

Challenges against UAS network security

Some old ...

- Cyber threats on CIA
- Access control
- Software security
- IoT security
- Mobile ad hoc network security
- ...

Some new ...

- DoSt attacks
- Quantum computing
- AI security
- Scale
- Omnipresence
- Democratization

Some magnified ...

- Physical security
- Resource constraints
- Supply chain security
- Security management in a fragmented world
- **Standardization** ☺ (A tale of two cities: security vs aviation people)

Core elements of security solutions for UAS networks

Key guidelines

- Use existing knowledgebase as much as possible (e.g., Tactics, Techniques, and Procedures (TTPs))
- Keep CPS perspective
- Do not let things to be excuses:

  «Sorry, no resources ☹»

  «First, we need it running!»

  «Security is frankly not the top priority in this phase of our project ☹»

  …

Core elements of security solutions for UAS networks (cont.)

Solutions

- **Security by design**
- Additional security controls (layers)
- Deeper monitoring and threat awareness: *A Good Decision Relies on Good Data. $(GD)^2$*
- Dedicated security functions, e.g., SIEMs
- Resource-aware security controls
- More open systems based on standards

  → **CHECK OUT our work on IEEE P1920.2 standard ;-)**
- Security testing of UAS (e.g., vulnerabilities or baseline security testing)

  Can AI be used for large-scale testing of numerous network nodes autonomously?
- Pursue smarter systems regarding security -> «I see LLMs everywhere … » -> what about their security?

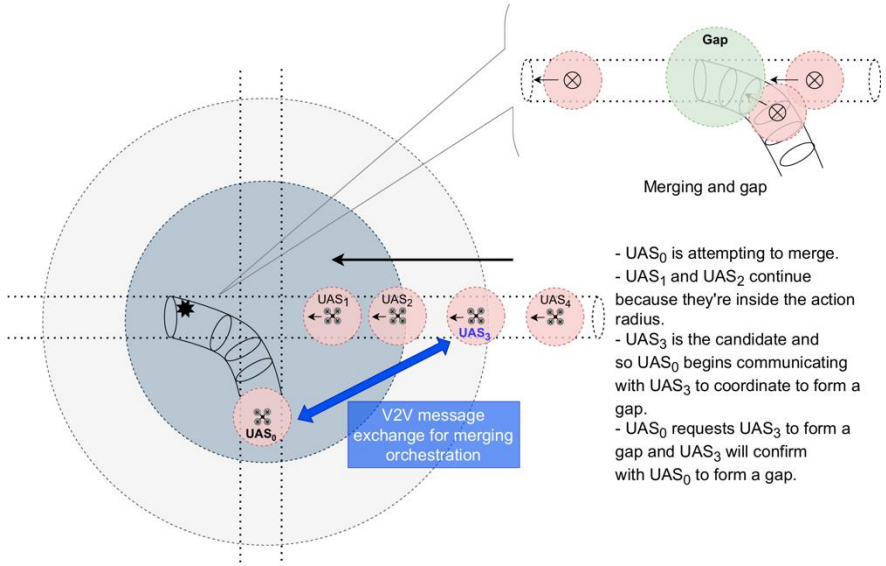
  Cognitive systems

  …

V2V missions/use cases lead to sec. requirements - (IEEE 1920.2 case)

Let’s switch to more specific uses:

- Collision Avoidance
- Merging and Spacing/Sequencing of Traffic
- Airborne Separation
- Airborne Rerouting
- Collaborative Sensing of Weather Conditions
- …



Security landscape and vulnerabilities in V2V UAS networks (@IEEE 1920.1/2)

- Data: C2, telemetry, navigation safety messages such as Detect-And-Avoid (DAA), and application-specific data information for applications in Visual Line of Sight (VLoS) and Beyond Visual Line of Sight (BVLoS), …
- No Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) system
- May be high risk
- Profile:
    - Small UAVs have limited resources in terms of energy consumption and computational processing
    - Conventional cyber-security solutions? Not always.
    - Patching and fixes? («IoT's world»)
    - UAVs have many types of hardware and software components

UAS vulnerabilities

Hence, UAS vulnerabilities stem from various factors:

- Inadequate policies and procedures to develop and maintain hardware and software UAS platforms.
- Insufficient defense and security protections and the curse of closed systems
- Remote access without appropriate access control policies and authentication
- Inadequate secured wireless communication protections
- Lack of tools to detect anomalous activity

Threat model

Passive and active attacks are possible. Adversaries come with different capabilities.

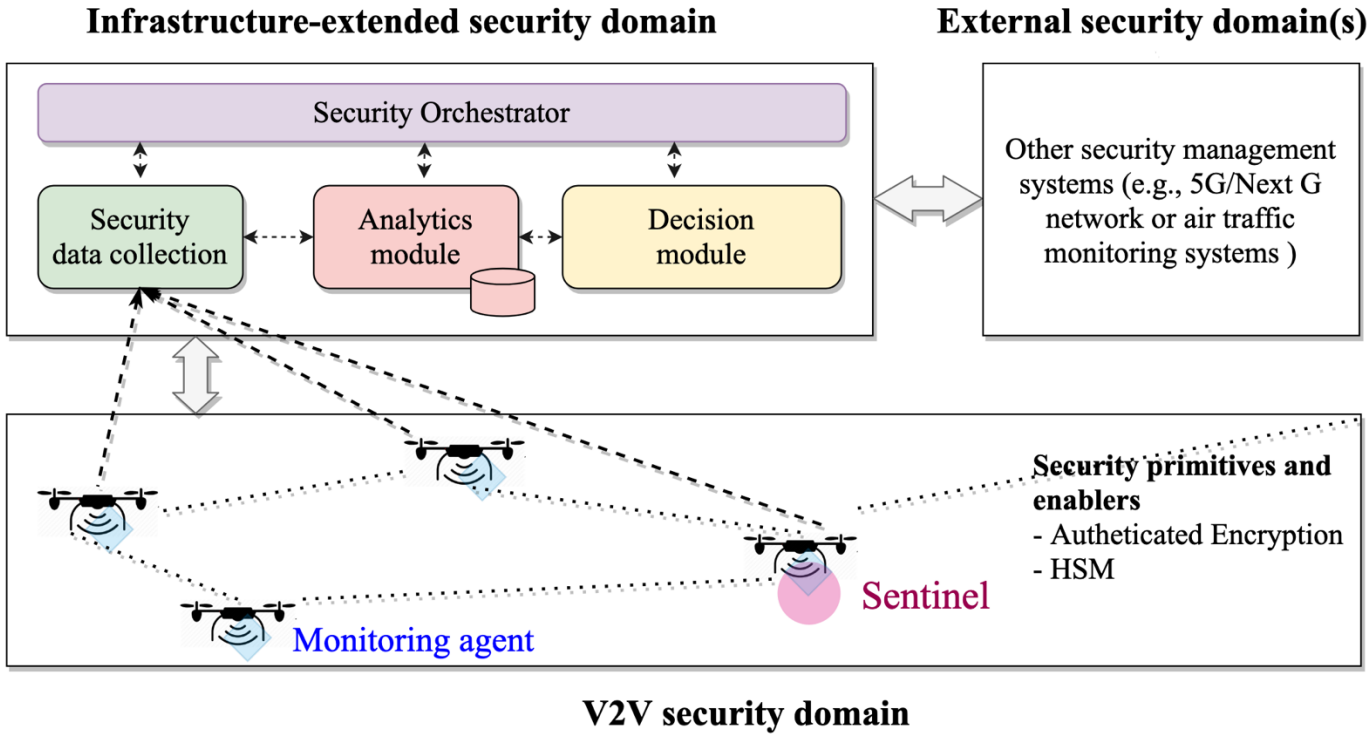
- Spoofing of (civil) GPS and Remote ID signals
- Jamming communication links (GPS, Remote ID, C2, DAA, data communications).
- DoS and DoSt attack
- Eavesdropping on command & control, data communications, or telemetry signals.
- Interception and altering command & control, data communications, GPS, or Remote ID signals.
- GPS denial
- Attacks on components and supply chain compromises (Remember the «Crypto AG»?)
- Lateral movements
- …

Security and trust model for UAS networks

How to prevent these threats -> Via a security protocol with the following capabilities?

- **Mutual entity authentication:** Data origin authentication for sender and receiver.
- **Mutual explicit key agreement authentication:** Mutual explicit key authentication is the property obtained when the sender and receiver have the assurance that only the other party knows the negotiated shared key.
- **Confidentiality:** Data information is protected with encryption.
- **Verification of data integrity:** The legitimacy of messages and protection against data tampering is implemented with authenticated encryption and Message Integrity Code (MIC).
- **Authorization policies are based on the ZTA:** Access to resources (control station, UAV interfaces, sensors, and actuators) is never granted until a subject, asset, or workload is verified by reliable authentication and authorization (access rules) while minimizing end-to-end latency.
- **Trusted computing techniques:** Use HW support such as TEEs

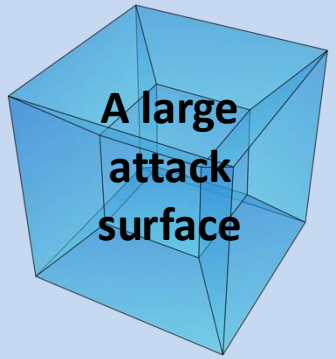
V2V UAS security management framework



Finally, so what could we have for security management in this scope?

Conclusion

$$\frac{\text{Vulnerabilities} \times (\{\text{Cyber} + \text{Physical}\}\ \text{sec\_issues})}{\text{Resource constraints} + \text{Heterogenity}} =$$



Zürcher Hochschule
für Angewandte Wissenschaften

zh
aw

Thank You!

Join IEEE VTS at
www.vtsociety.org

Follow IEEE VTS on social media

Website
www.vtsociety.org

Facebook
facebook.com/IEEEVTS

Twitter
@IEEE_VTS

LinkedIn
www.linkedin.com/company/ieee-vehicular-technology-society