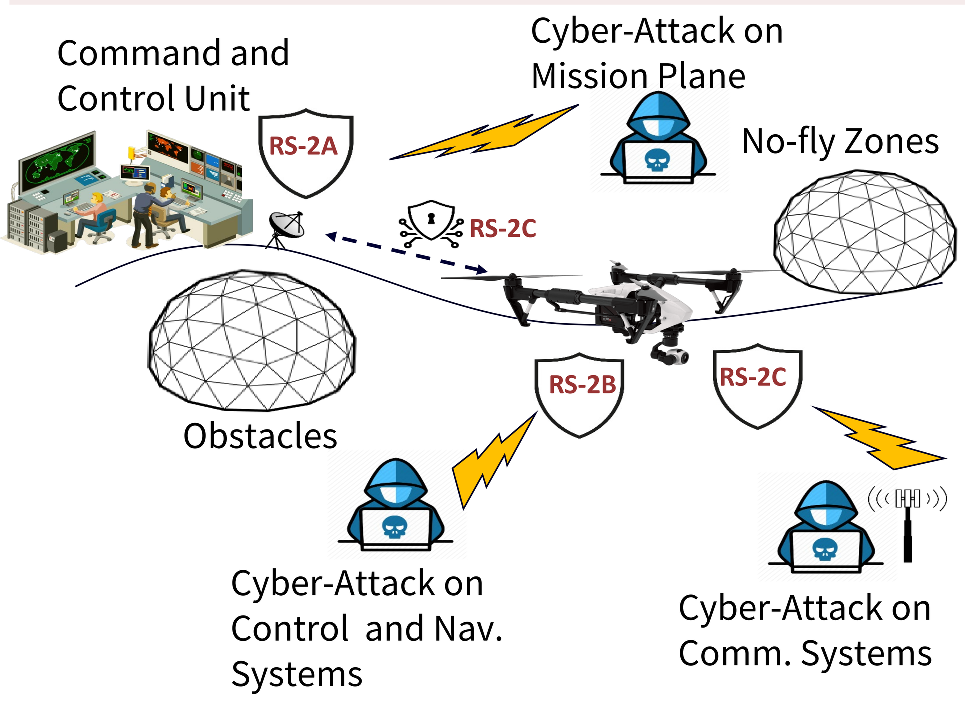
RS2: Secure Operations of Trustworthy Autonomous Systems

Cranfield University, Lancaster University

Researchers: Dr. Yi Li, Dr. Zhuangkun Wei, Dr. Burak Yuksek, Dr. Oscar Villarreal, Dr. Cynthia Yu, Pierre Ciholas, Alvaro Lopez . Investigators: Prof. Weisi Guo, Prof. Gokhan Inalhan, Prof. Plamen Angelov, Prof. Antonios Tsourdos, Prof. Dan Prince.

Secure Operation of Autonomous System



RS-2A: Exposure to cyber-physical attacks by characterizing the attack surfaces, i.e., entry points and likelihoods across mission surfaces in technology & mission-invariant manner.

RS-2B: Provide quantifiable safety and feedback to the mission surface when the limits of secure controllability are compromised

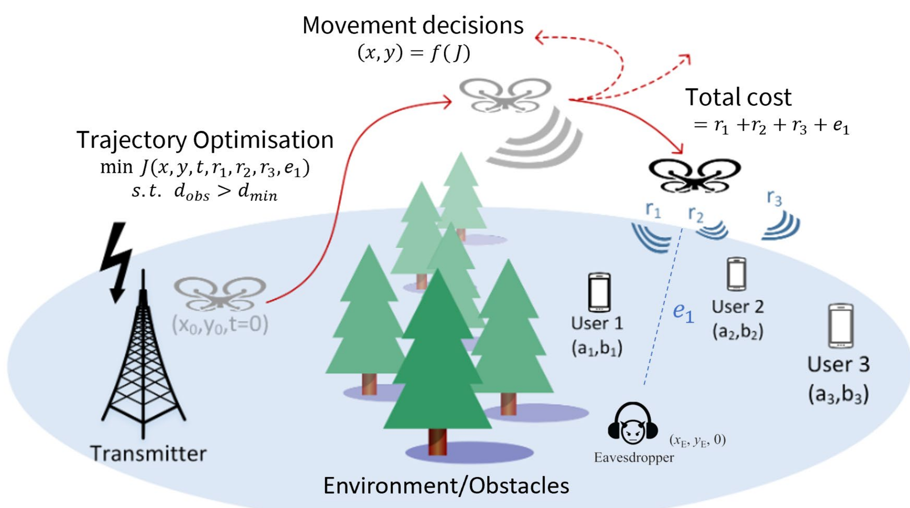
RS-2C: Provide secure communications across the different layers in the informatics plane from detection of signals to networking.

RS-2A: Securing the Mission Surface

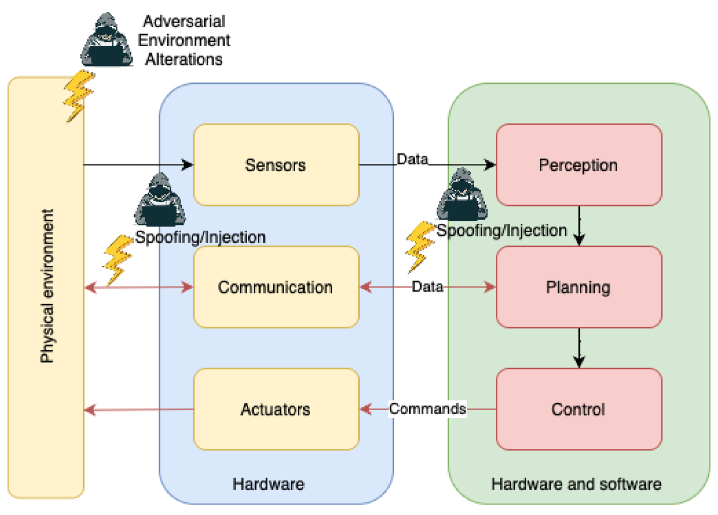
Mission Control for Secure Trustworthy Autonomous Systems requires flexible but reliable real-time optimal decision making and monitoring to handle a wide range of attacks

Methods and Focus:

- Real-Time Non-Convex Trajectory Optimization for Path Planning under constraints from control & communication
- Adaptive and Fault-Tolerant Learning-based Design for Mission Control to improve reliability of safety critical systems
- Reliable Self-Assessment under Learning-based Scenarios



Adversarial attacks



Critical Impacts

•**Perception layer**: Manipulate the sensory input of an AS, causing the system to perceive incorrect or misleading information.
•**Planning layer**: Adversarial attacks can also manipulate the AS's decision-making pro
•**Control layer**: Affect the control layer of an AS, leading to incorrect or harmful actions.

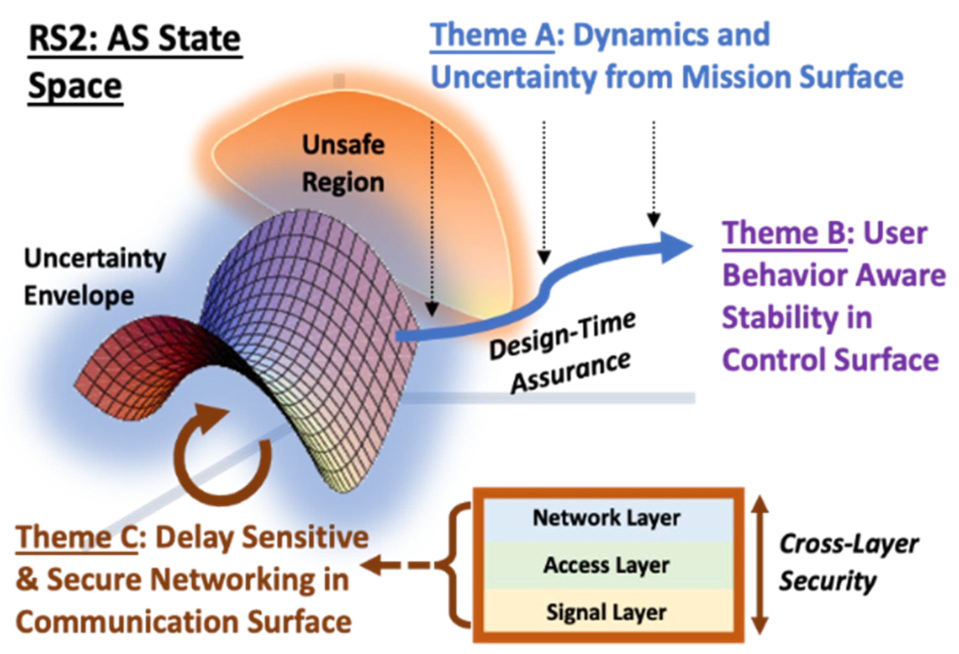
Requirements for robust to adversarial attacks systems in the context of AS:
•Able to detect attacks
•Able to react to detected attacks
•Evolve with new unknown types of attacks and situations

Physical Attacks | Digital Attacks

RS-2B: Securing the Control and Navigation Surface

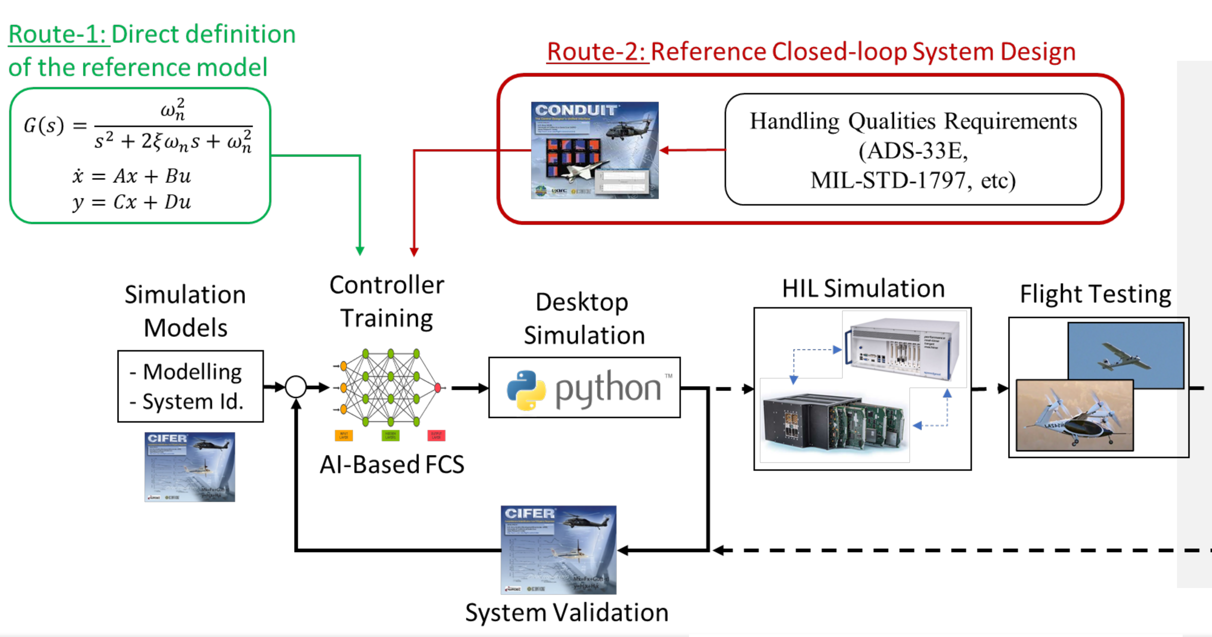
Autonomous Systems rely on the ability to conduct run time adaptations of control decisions over attacks or "perceived" attacks:

- Adversaries
- Environment uncertainties
- Degraded performance



Key Solutions for Operational Safety in Learning-Enabled Context

- AI-based Flight Control System Design and Validation of Dynamics
- AI-aided Visual Inertial Navigation for GPS-denied Environments and GPS Spoofing Detection



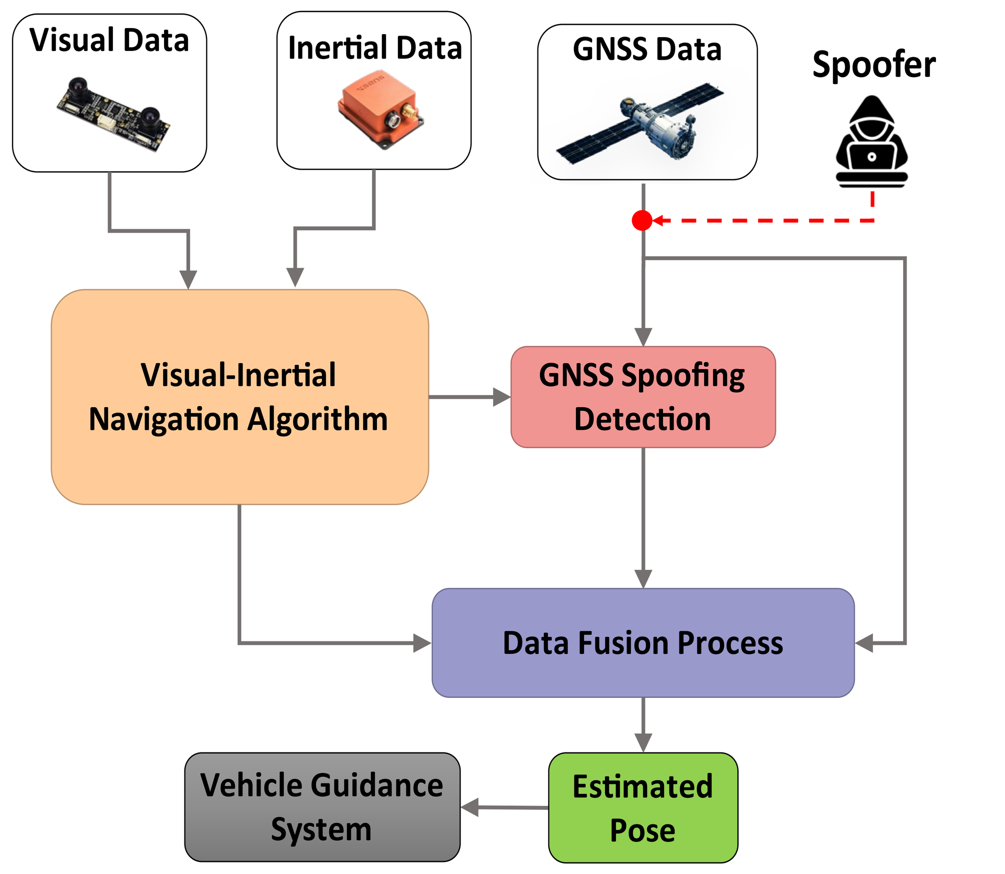
AI-based Flight Control System Design and Validation of Dynamics

- Designing an RL-based flight control system
- Covering the whole flight envelope
- Integrating handling qualities into the training process
- Validation of the closed-loop dynamics

Navigation in Extreme Adversarial Environment

AI-aided Visual Inertial Navigation for GPS-denied Environments and GPS Spoofing Detection

- Designing AI-aided Visual-Inertial navigation system to support the GNSS in the presence of spoofing attacks.
- Combining the AI-based solutions with classical filter-based approach
- Improving the pose estimation performance in austere environment
- **Case studies;**
  - Civil: Urban air mobility
  - Military: Perceptional intelligence in austere environments



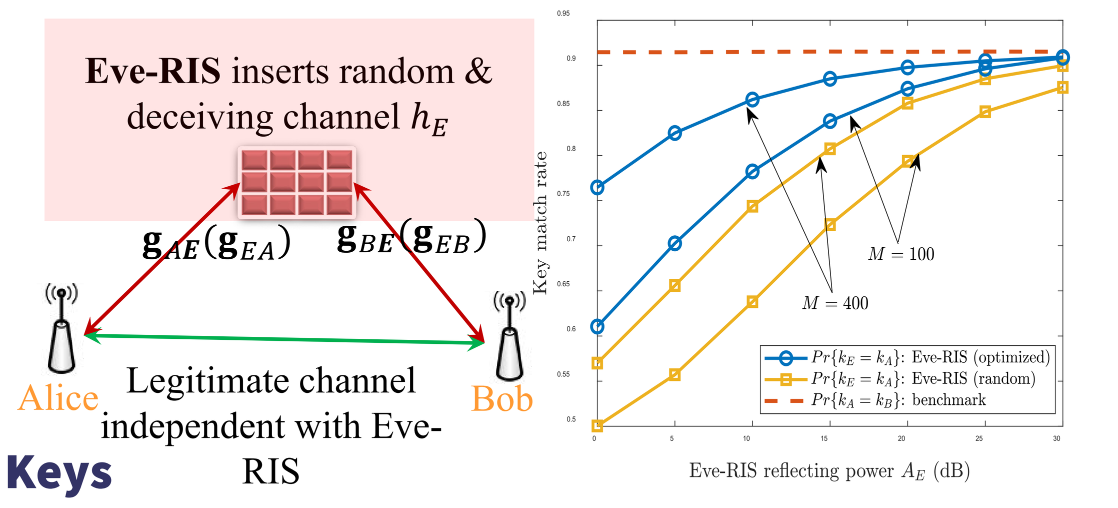
RS-2C: Securing the Communication Surface

Physical & Control Layer Security

To secure the communication surfaces of AS, current cryptography and physical layer security (PLS) both have some severe security threats, which motivates the design of control layer security (CLS) that is specific for AS.

Cryptography
uses common key pool for cipher key generation, but has following issues:
➢Complex key generation & management & distribution
➢No secrecy guaranteed against post-quantum computing
➢High computational complexity & latency

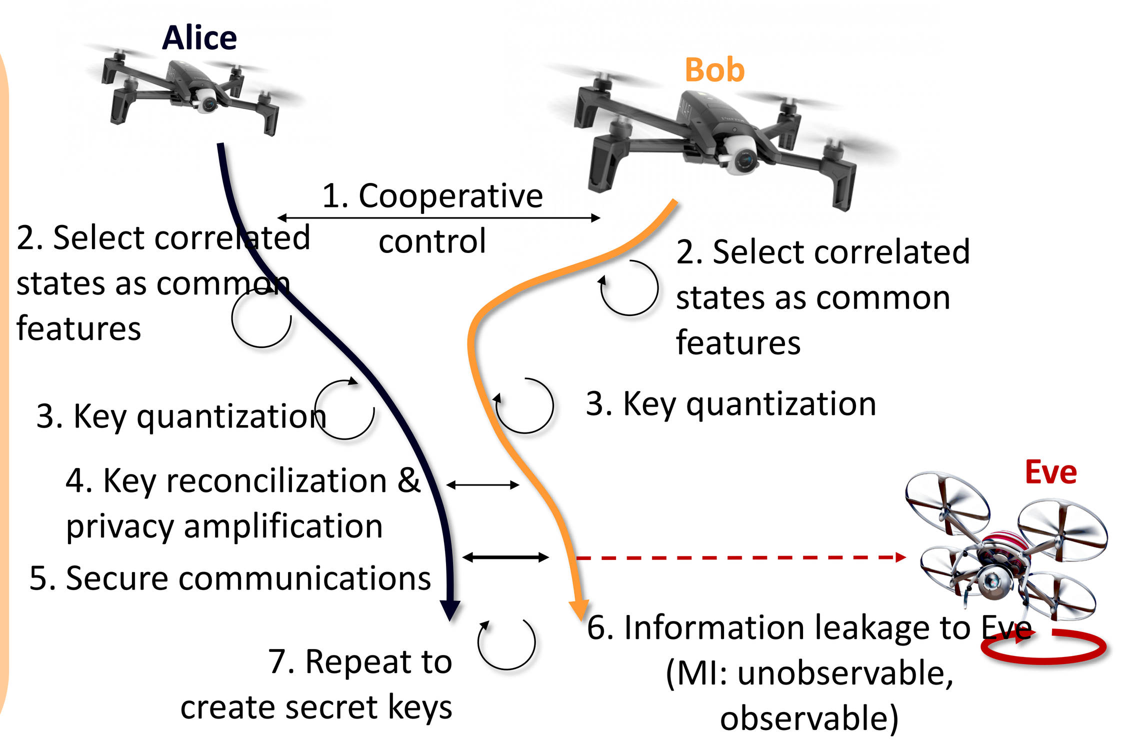
PLS
generates cipher keys via the reciprocal channel information, but has man-in-the-middle attack threats:

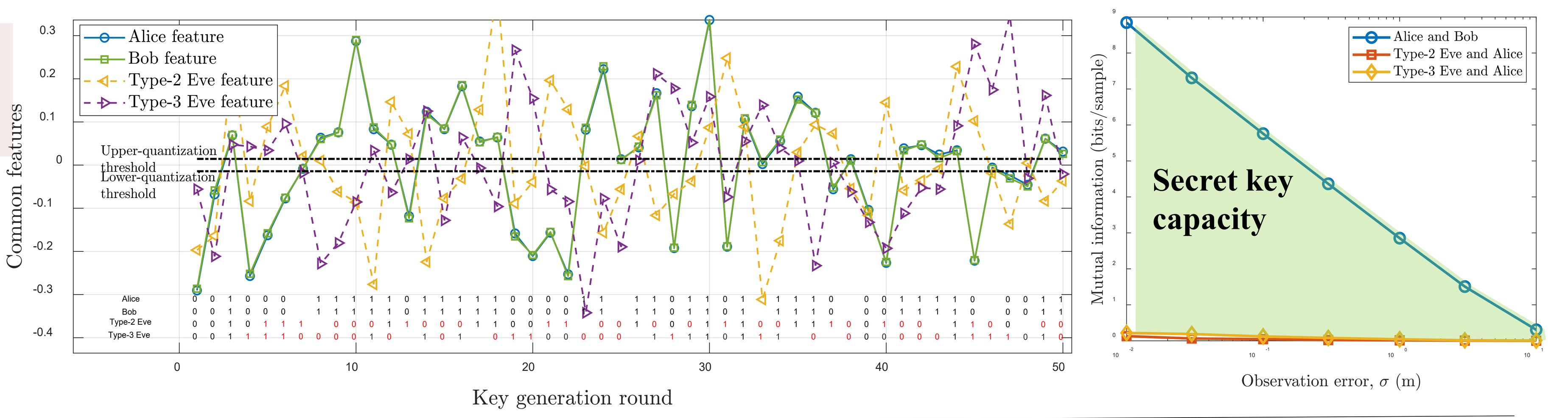


Designed Control Layer Cipher Keys

Legitimate Alice and Bob (two UAVs) create correlated but unobservable states (e.g., yaw angles), via cooperative control, and use these correlated states for cipher key generation.

Results show that by properly designing the cooperative control algorithm, UAV Alice and UAV Bob can have random but highly correlated states for cipher key generation, which prevent attackers from eavesdropping.



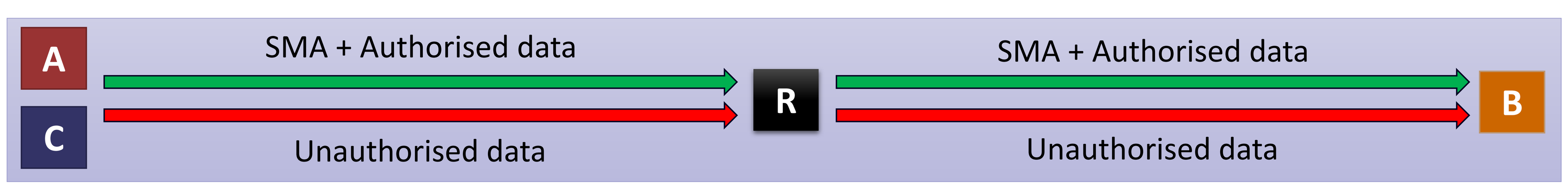


Data Link, Network, and Transport Layer Security

To secure communication on higher layers (Data Link, Transport, and Session), and potentially create a secure and trusted network within an untrusted network, we use cryptography assuming a pre-shared secret and a Single Message Authentication protocol of our creation.

Timestamp	User ID	Entropy	Access	MAC
Clear		Encrypted (KD/OTP)		Clear

The packet of the AS is intercepted before being sent, and we perform the authentication first before forwarding the AS packets. If the authentication succeeds, a single communication is allowed to get through (for stateful protocols such as TCP), whereas for stateless protocols (e.g. UDP) other solutions are available (e.g. merge authentication and data, of provide a hash of the expected payload). This solved the infamous "NAT problem" as it is known in the literature.



This work is supported by the Engineering and Physical Sciences Research Council [grant number: EP/V026763/1]