Security Conference 2022

AI aided Security for Space Robotics in FAIR-SPACE project

Dr. Haitham Cruickshank

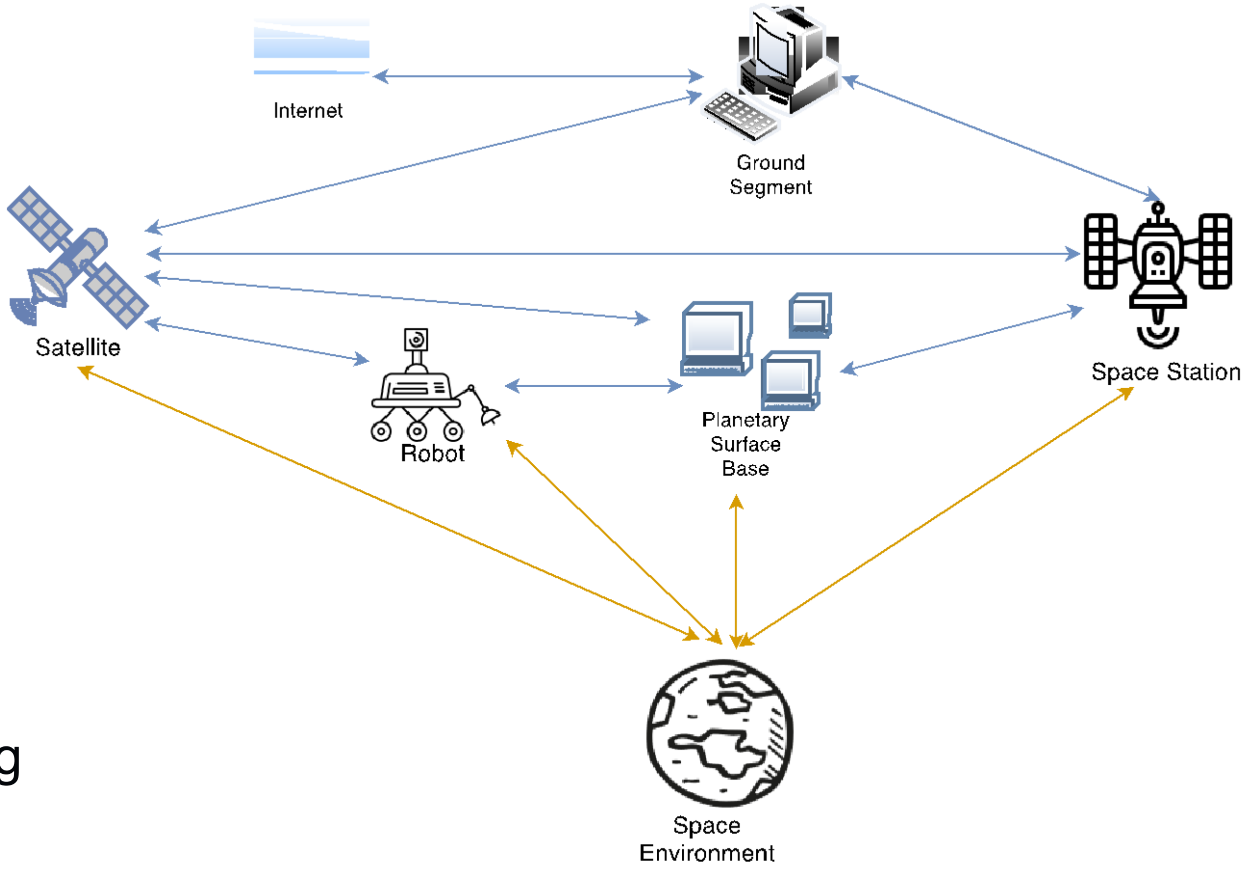
05/10/2022

Outline

- Introduction to FAIR-SPACE robotics operations
- Presentation of two security scenarios (robots in-orbit and remote)
- Analysis of secret, public and quantum safe crypto systems
- Future outlook for satellite and 6G security unification
- Conclusions

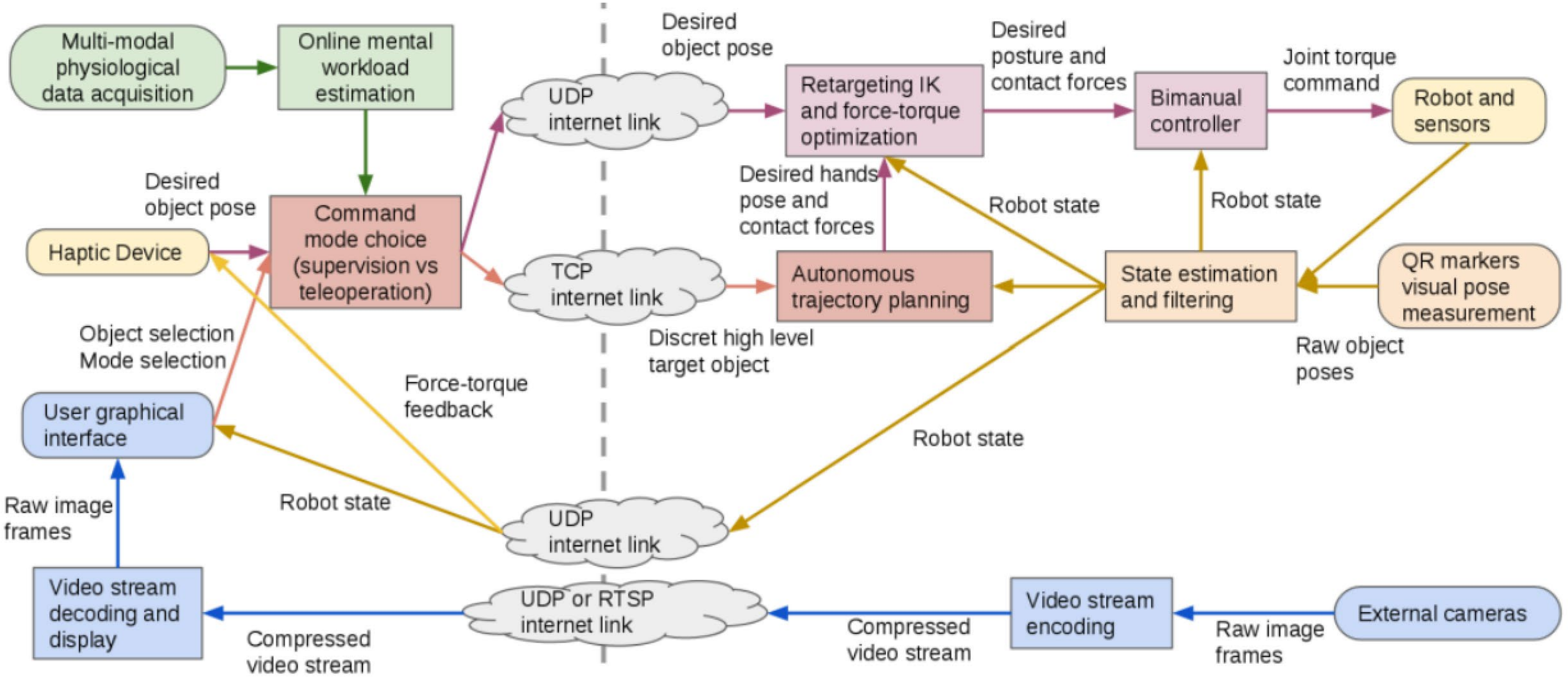
High level view of FAIR-SPACE vision

- FAIR-SPACE is the UK national centre of research excellence in space robotics and AI:
  - The security was joint effort between Surrey and Warwick universities.
- In-orbit construction and maintenance of large-scale structures such as the International Space Station (ISS) have led to increasing interest in developing effective and efficient <u>teleoperation systems</u>.
- However, teleoperation requires communication of data between the operator and the operation site which may be <u>subject to cyber-attacks</u>.
- Cyber security measures such as encryption and integrity checks can prevent these attacks from being successful however, these security measures create <u>additional overheads in communications</u> that can impact on the operators ability to effectively control the operations at a distance.



Robotic scenarios:
1. On space station for repairs
2. On planetary surface

Teleoperated robots system architecture



Multi-modal physiological data acquisition
Online mental workload estimation
Desired object pose
Haptic Device
Command mode choice (supervision vs teleoperation)
Object selection
Mode selection
User graphical interface
Raw image frames
Video stream decoding and display
Compressed video stream
Force-torque feedback
Robot state
UDP internet link
TCP internet link
UDP internet link
UDP or RTSP internet link
Desired object pose
Retargeting IK and force-torque optimization
Desired hands pose and contact forces
Discret high level target object
Autonomous trajectory planning
Desired posture and contact forces
Bimanual controller
Joint torque command
Robot and sensors
Robot state
Robot state
State estimation and filtering
QR markers visual pose measurement
Raw object poses
Robot state
Compressed video stream
Video stream encoding
Raw image frames
External cameras

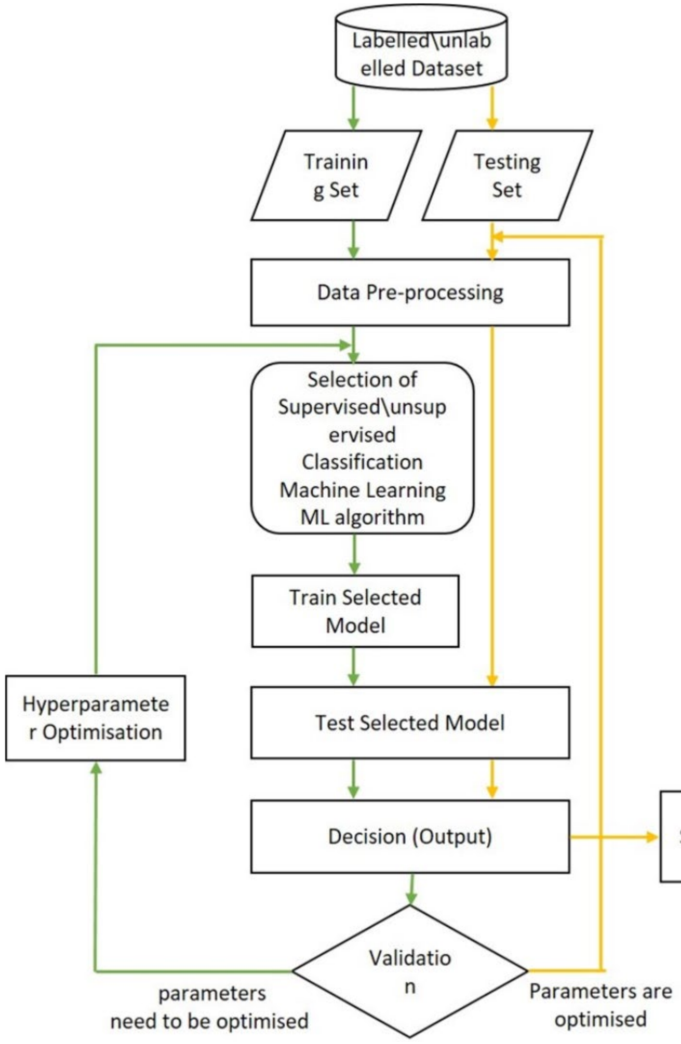
Security analysis of Robotics scenario 1: Repairing satellites (in-orbit)

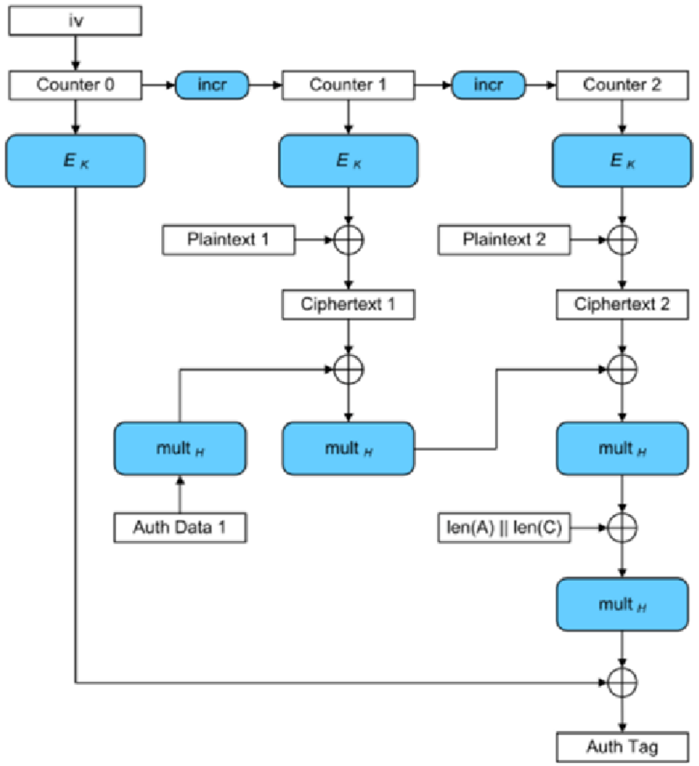
- The operator (inside the satellite) is located close to the robot (outside the satellite)
- The possibility of a message being intercepted or tampered with, are low
- Thus integrity check is sufficient and may be there is no need for encryption.
- Two example integrity check methods, Hashed Message Authentication Code (HMAC) and checksums are analysed:
  - Checksum is used when the traffic is high (e.g. video streaming by the robot)
  - HMAC (e.g. HMAC-256) can be used when the traffic between communicating parties is low (e.g. control messages)

Security analysis of Robotics scenario 2: Planetary rovers (on the surface of planets)

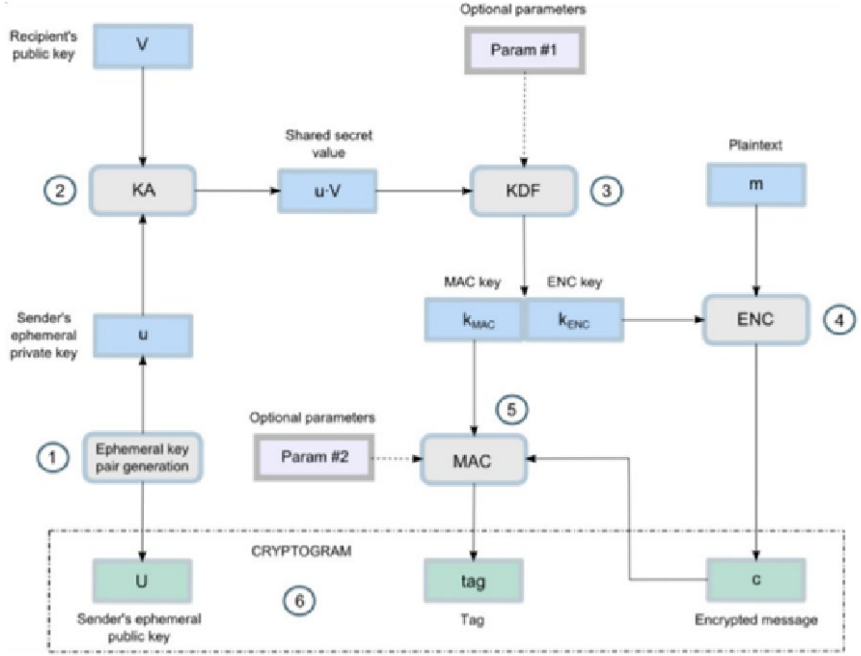
- The operator is located far away from the robot and controls it remotely.
- Therefore, the probability of a message interception or tampering are high. Therefore encryption and message integrity checks are required
- Two examples public-key and secret-key algorithms were analysed:
  - Secret-key system: The Advanced Encryption Standard-Galois Counter Mode(AES-GCM). When the data streaming is high, the AES-GCM is used, as it is lightweight and efficient encryption system
  - Public-key system: Elliptic Curve Integrated Encryption Scheme (ECIES). It provides key agreement, key derivation function, encryption/decryption and authentication. ECIES is used when the data flow is low.
- Also Quantum safe cryptography was examined and compared to the above two systems

AI/ML Framework for Selection of Different Cryptographic Algorithms


Labelled\unlabelled Dataset
Training Set
Testing Set
Data Pre-processing
Selection of Supervised\unsupervised Classification Machine Learning ML algorithm
Train Selected Model
Hyperparameter Optimisation
Test Selected Model
Decision (Output)
Selected Encryption Algorithm
Validation
parameters need to be optimised
Parameters are optimised

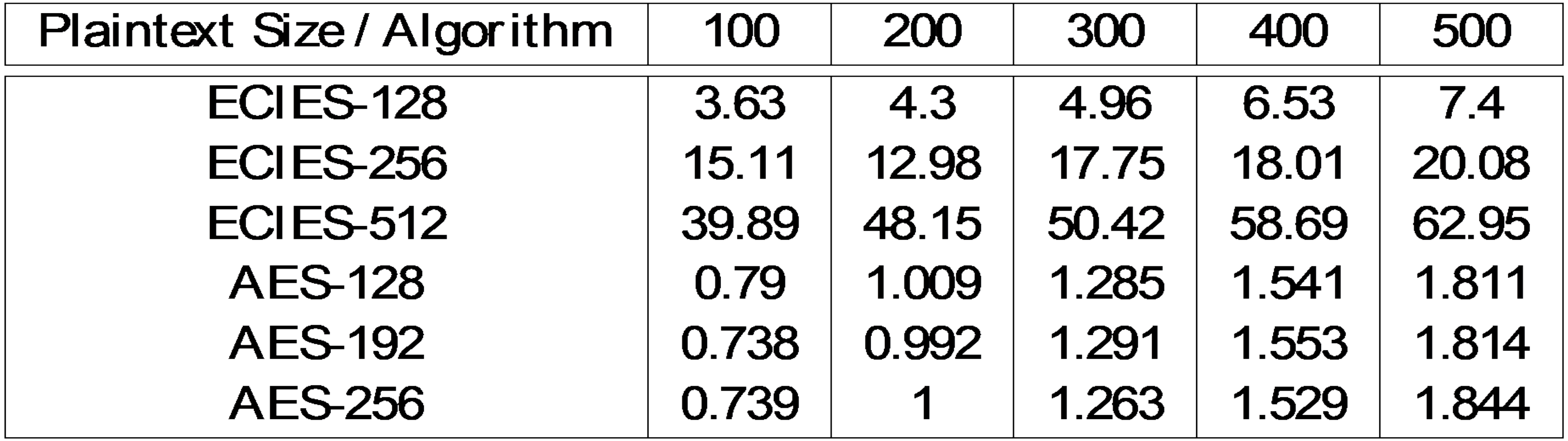


AES-GCM: Advanced Encryption Standard- Galois Counter Mode

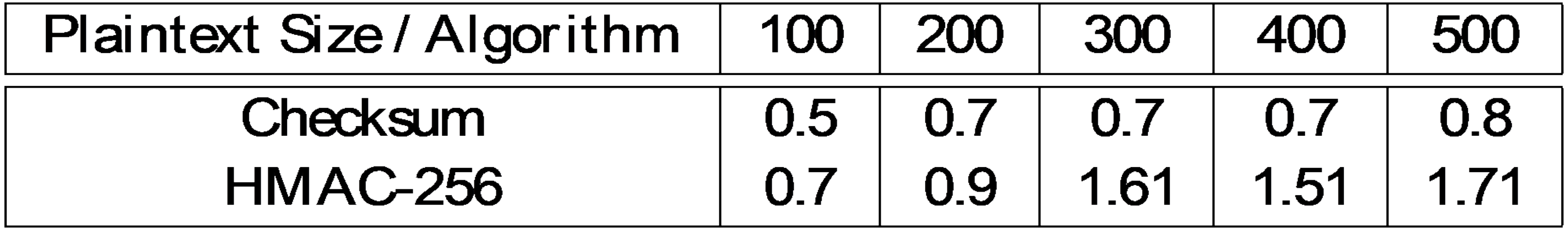


ECIES: Elliptic Curve Integrated Encryption Scheme

End-to-end encryption and integrity check delays (ms)



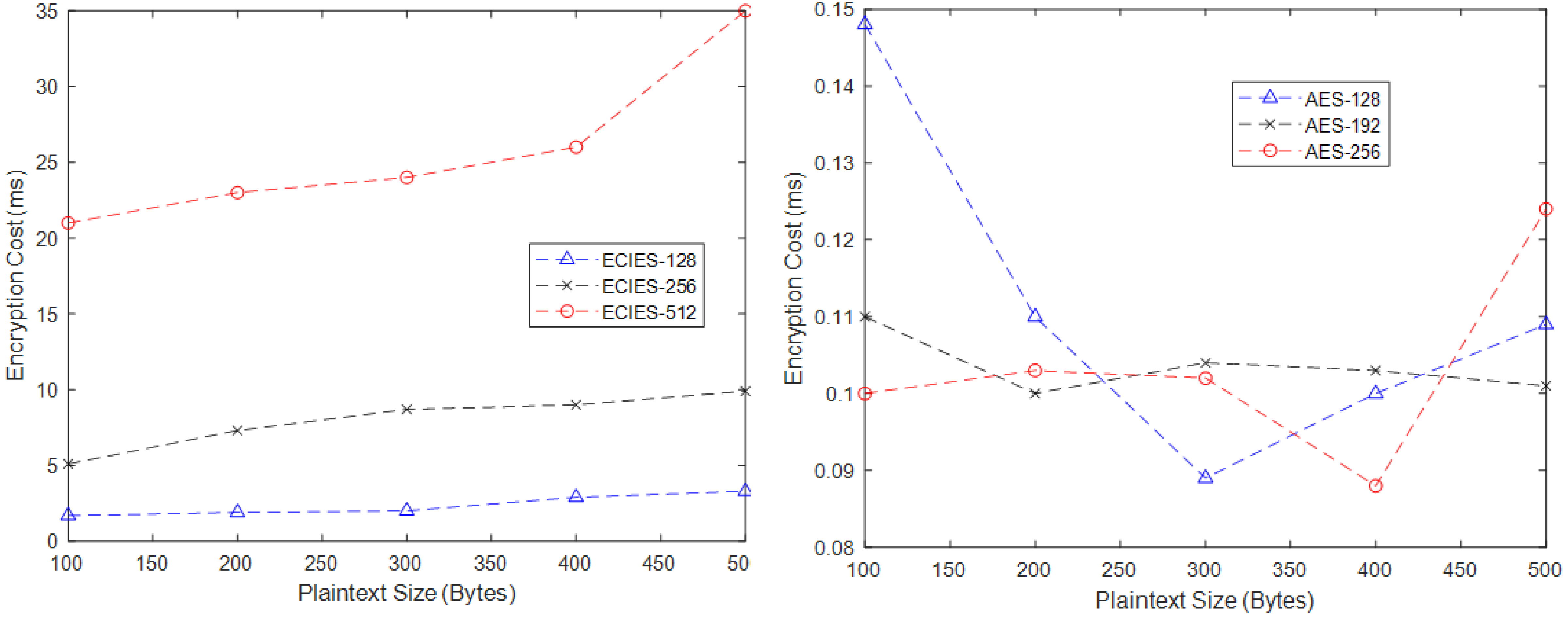
Plaintext Size / Algorithm	100	200	300	400	500
ECIES-128	3.63	4.3	4.96	6.53	7.4
ECIES-256	15.11	12.98	17.75	18.01	20.08
ECIES-512	39.89	48.15	50.42	58.69	62.95
AES-128	0.79	1.009	1.285	1.541	1.811
AES-192	0.738	0.992	1.291	1.553	1.814
AES-256	0.739	1	1.263	1.529	1.844



Plaintext Size / Algorithm	100	200	300	400	500
Checksum	0.5	0.7	0.7	0.7	0.8
HMAC-256	0.7	0.9	1.61	1.51	1.71

Awareness of the performance cost of encryption and integrity check methods allows mission planners to consider the risk of security compromise and balance this against performance costs

Comparison of ECIES and AES-GCM Encryption Cost (ms) schemes



Brief analysis of Quantum Safe Algorithms

- Hash-based signatures were analysed: using the SPHINCS+ signature library Quantum safe algorithm and compare it with standard digital signature algorithms such as Elliptic Curve Digital Signature Algorithm (ECDSA) and Schnorr signature algorithm (light weight public key system used for generating Tokens).
- The SPHINCS+ cryptosystem has two different configurations:
    - SPHINCS+-128f that has a 64-byte private key, 32-byte public key, and ~16.9KB signature size.
    - SPHINCS+-128s has a 64-byte private key, 32- byte public key, and ~ 8KB signature.
    - Each of the above algorithms were tested in terms of time complexity of generating and verifying signatures, as well as the cost of communication overheads.

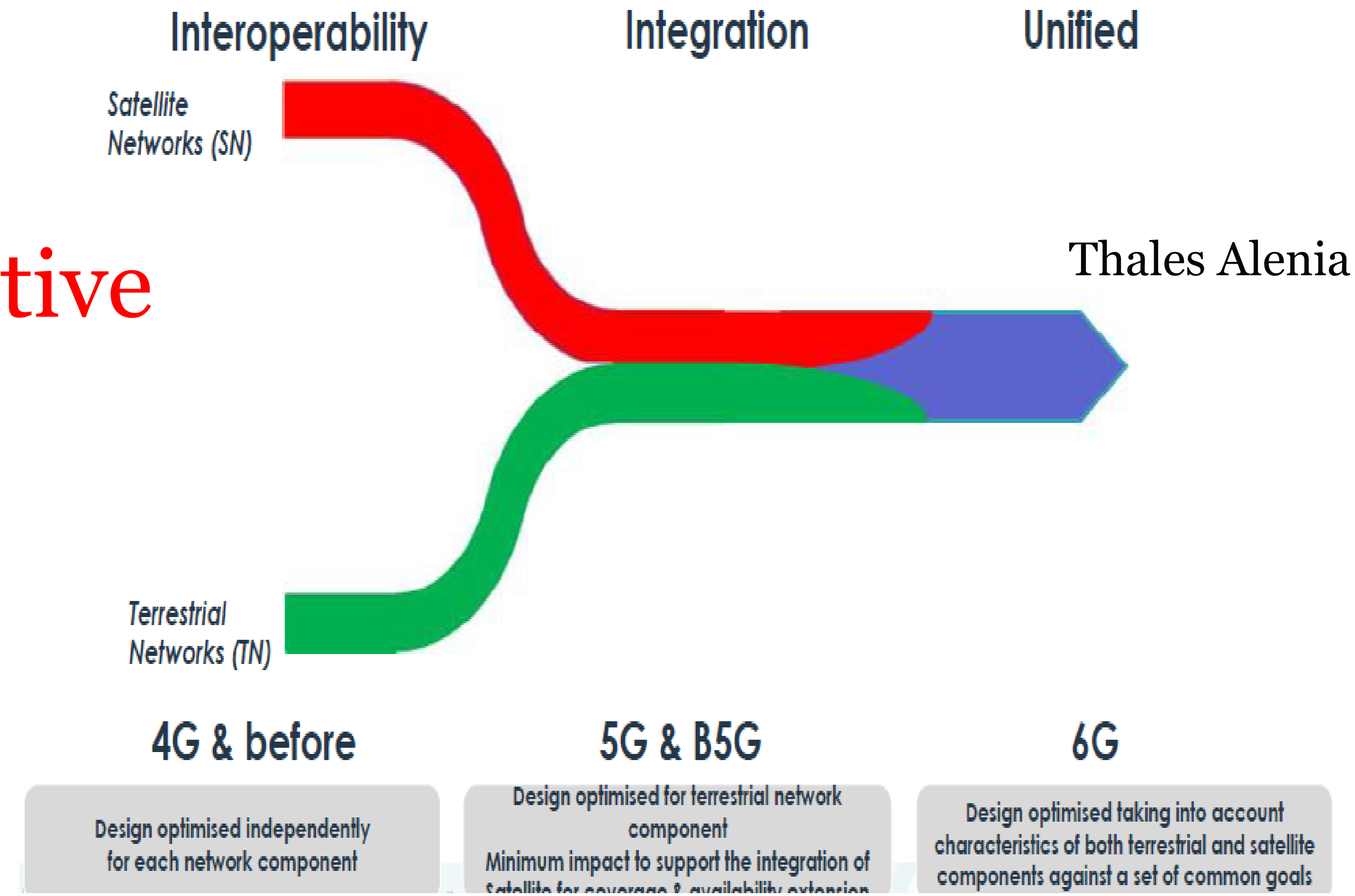
A comparison between the SPHINCS+ and the traditional (ECDSA and Schnorr signature) algorithms

- Both variants of the Quantum safe algorithms have larger overheads compared to the classical algorithms. Thus only useful for scenario 2 (remote operation)
- For 5G/6G connected satellites, there is extra communications cost for the extra message sizes that has to be carried. Thus Quantum safe algorithms can only be used if there is enough bandwidth (capacity) for such security message overheads:
  - Thus and high traffic situation (e.g. video streaming by the robot), traditional crypto algorithms are a better choice

Algorithm	Signing Cost	Verifying Cost	Communication Cost
ECDSA	4 milliseconds	7 milliseconds	56 Bytes
Schnorr	1.57 milliseconds	3.11 milliseconds	42 Bytes
SPHINCS+-128f	978.30 milliseconds	42.24 milliseconds	16976 Bytes
SPHINCS+-128s	15.90 second	19.74 milliseconds	8080 Bytes

Satellites and 6G vision of unification plans –1

What is the best approach from security prospective



Design optimised independently for each network component

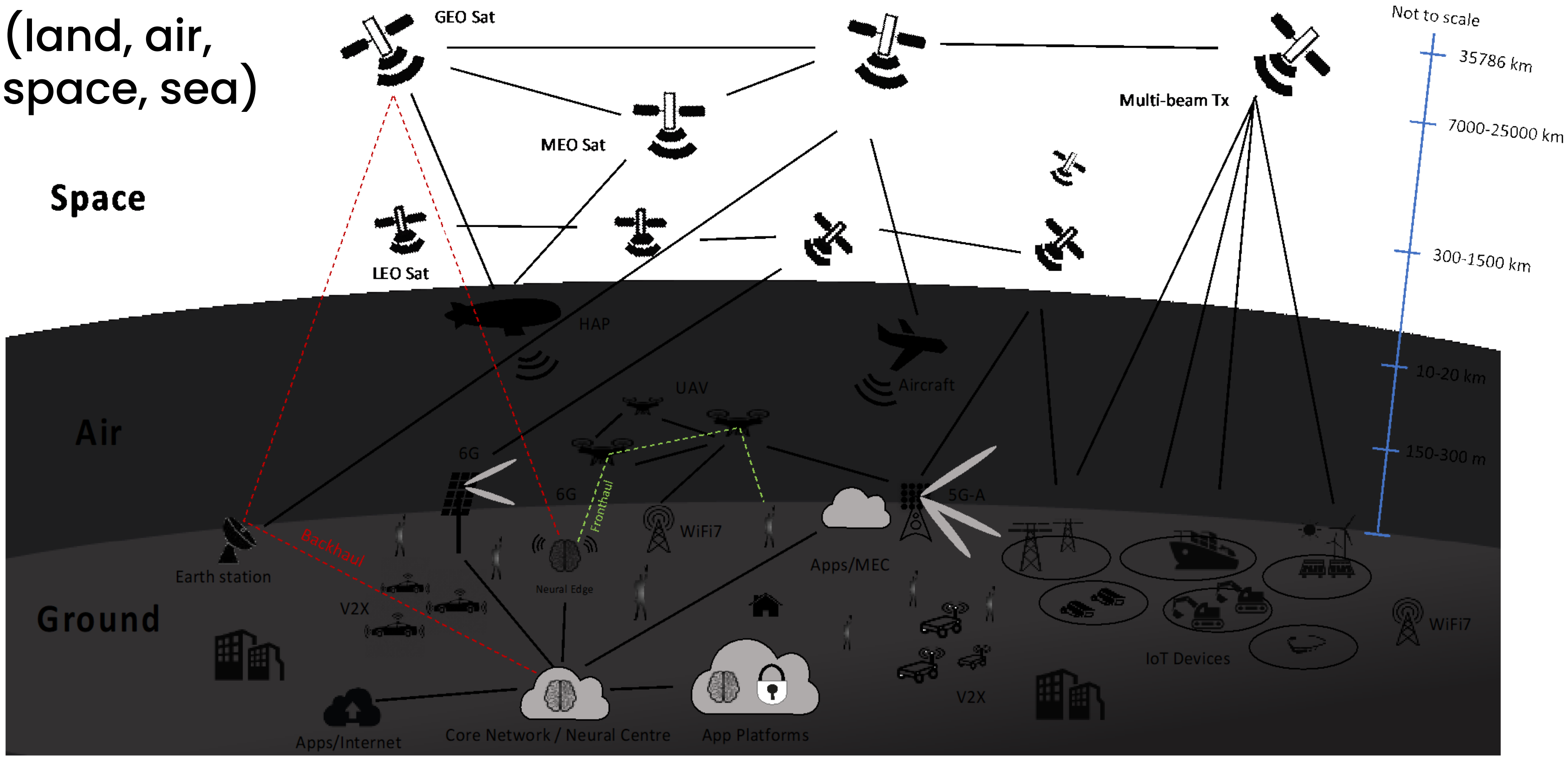
Design optimised for terrestrial network component
Minimum impact to support the integration of Satellite for coverage & availability extension

Design optimised taking into account characteristics of both terrestrial and satellite components against a set of common goals

Thales Alenia space vision

Future outlook - Non-Terrestrial Networks (NTN) as an integral part of the 6G wireless system - 1

Ubiquitous services (land, air, space, sea)



This is a challenging security problem

Future outlook – Non-Terrestrial Networks (NTN) as an integral part of the 6G wireless system – 2

- Security unification of satellites with 6G is best approach, but it is costly to satellite operators !!
- Distributed ML/AI approach for automated security: where satellite terminals, MECs (edge) and the cloud can all play part to build local and global view of threats and achieve effective response to attacks
- Distributed Ledger Technology (DTL) and blockchains to provide authenticated records and history of configurations:
    - A good approach to manage user privacy (identity hiding)
    - Smart contracts to protect DTL against blocks poisoning
- Post Quantum cryptography with two topics:
    - Quantum safe algorithms (needs deep understanding of cost and overheads)
    - Quantum key distribution (satellites are ideal for such secure distribution) - Not suitable for all 6G use cases. Thus traditional key agreements (such as 5G AKA) will be with us for a long time

Conclusions

- Space robotics is gaining momentum and security needs should be addressed
- A balanced approach to security is required to match network performance and the current threat levels
- Security requirements for in-orbit and remote robotics scenarios were presented.
- Secret and public key system were analyses for these scenarios.
- A brief analysis of quantum safe cryptography was also presented in terms of computational and communication overheads.
- AI aided crypto system selection was also presented.
- Future outlook: Federated AI/ML techniques can playing an important role in fast security synchronization of distributed satellite and terrestrial (5G/6G) security domains.

THANK YOU