GNSS-API: GNSS Anomaly Perception and Intelligence (AI/ML Driven)

Associate Professor Chee Kiat Seow ,Lawrence

University of Glasgow, Singapore

GNSS-API: GNSS Anomaly Perception and Intelligence (AI/ML Driven)

- GNSS (GPS, Beidou, QZSS, Galileo etc.) is the baseline technology to provide position, timing and velocity (PVT) to essential smart initiatives such as




Power Grids
GNSS Time
GNSS supporting Smart Grid

Digital Payment
Grab
Stock Exchange

Internet Banking

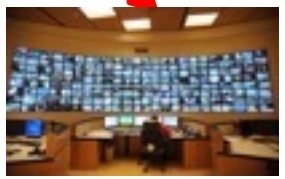
GNSS Time
GNSS supporting Smart Finance

Under Spoofing Attack

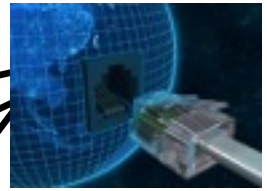
A $200 spoofer can mimic the set of fake GNSS satellites to change the PVT


Driverless Car
Ride and Delivery
Grab Uber
GNSS Time & Position
Air Traffic Control

Ship Routing
Drone


Command & Control Centre

GNSS supporting Smart Transportation

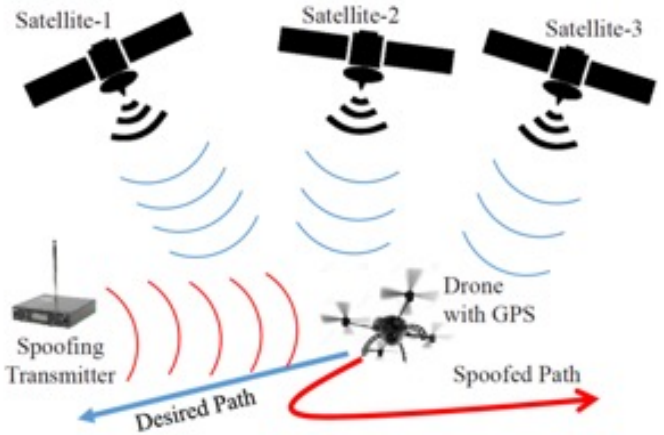
GNSS Time & Position
Comms Networks


5G/6G Cellular , Satellite and wireless internet

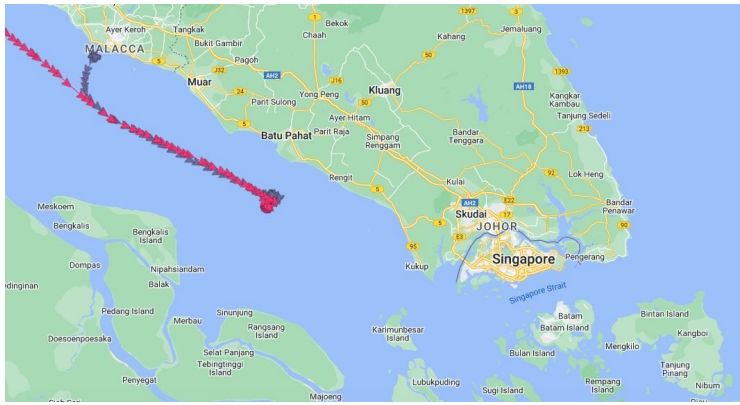
WeChat
Google Maps
Access GIS/Map
GNSS supporting Smart Network

GNSS-API: GNSS Anomaly Perception and Intelligence (AI/ML Driven)

- **Various ASEAN Countries suffers GNSS interference, jamming and spoofing threat. E.g**
  - Indonesia, Singapore and Malaysia [2-4]
    - Driver spoofed their location to GOJEK so that customer at their preferred location can be assigned to them
    - Collison of the crude oil tanker Zephyr I along Malacca Strait
  - Philippines [1]
    - Jamming Automatic identification signals (AIS) of Philippines ships for Filipino fisherman
    - Manila International Airport experiences chronic GPS disruptions
    - Illegal signal boosters and jammers that cause widespread disruption
- **Targets of the proposed solution: GNSS-API [5-7]**
  - Address real threats to solve documented GNSS jamming/spoofing
  - CORS based multimodal AI/ML detection using existing infrastructure without edge device dependency
  - Position ASEAN as global pioneer in infrastructure-based GNSS security



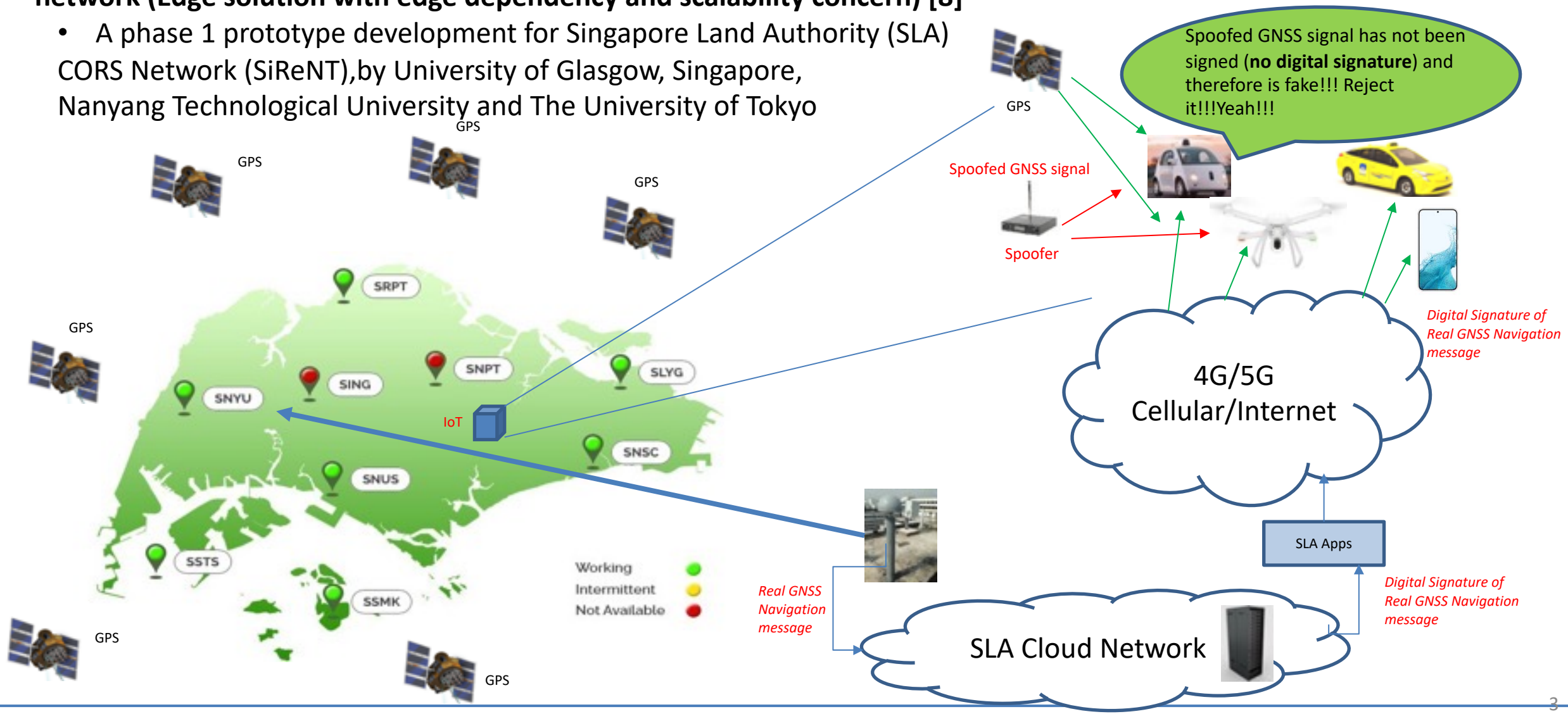
HackRF transceiver in the car to spoof own location or nearby vehicle



Crude oil tanker Zephyr I and the fully-cellular GSL Grania collided in the waters of Batu Pahat, Malaysia, at around 20:37 GTM on September 26, 2022.

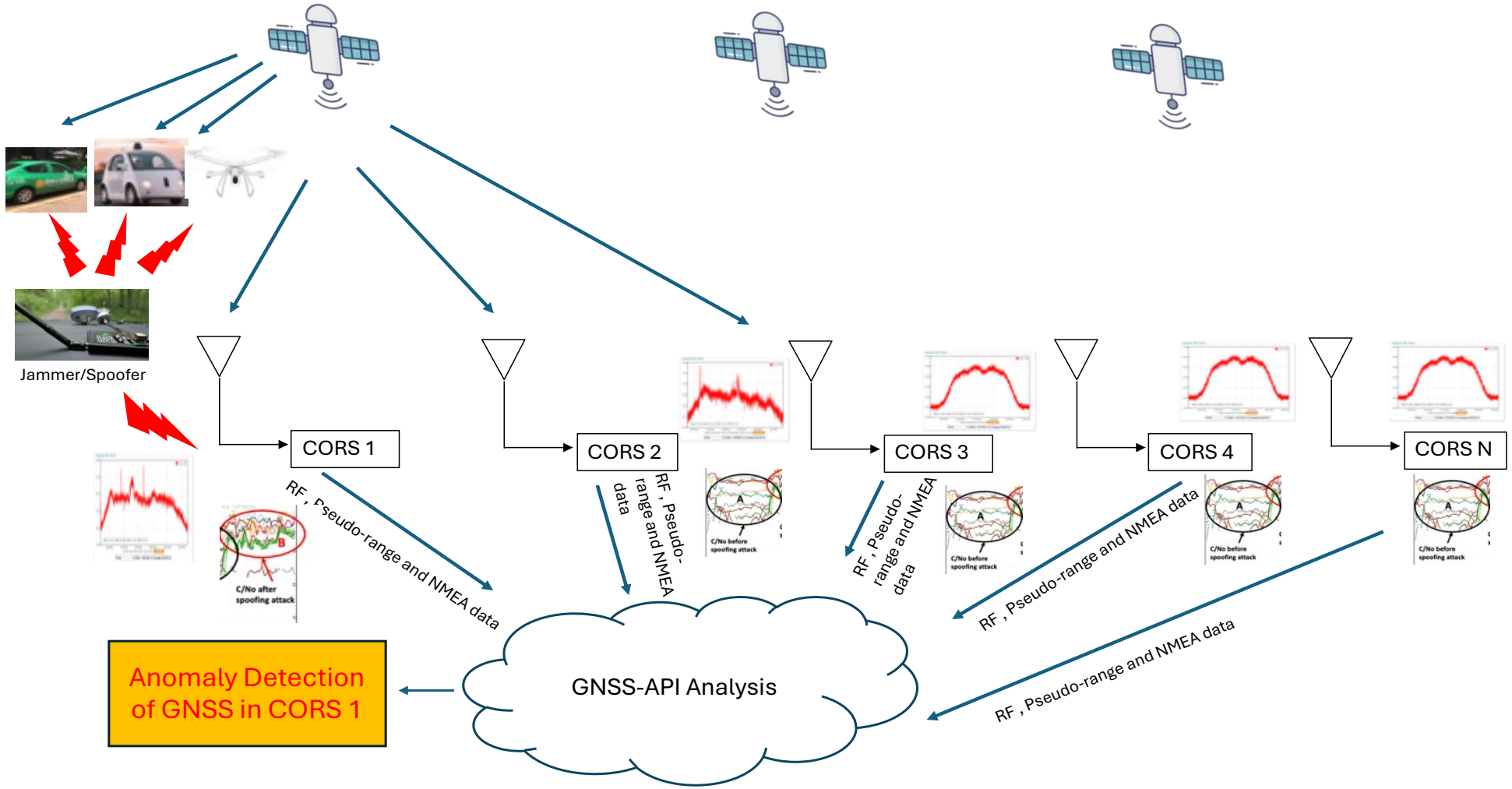
Proposed Method: GNSS-API: GNSS Anomaly Perception and Intelligence

- **Existing Solution : GNSS Navigation Message Authentication over Continuously Operating Reference Station (CORS) network (Edge solution with edge dependency and scalability concern) [8]**
  - A phase 1 prototype development for Singapore Land Authority (SLA) CORS Network (SiReNT),by University of Glasgow, Singapore, Nanyang Technological University and The University of Tokyo



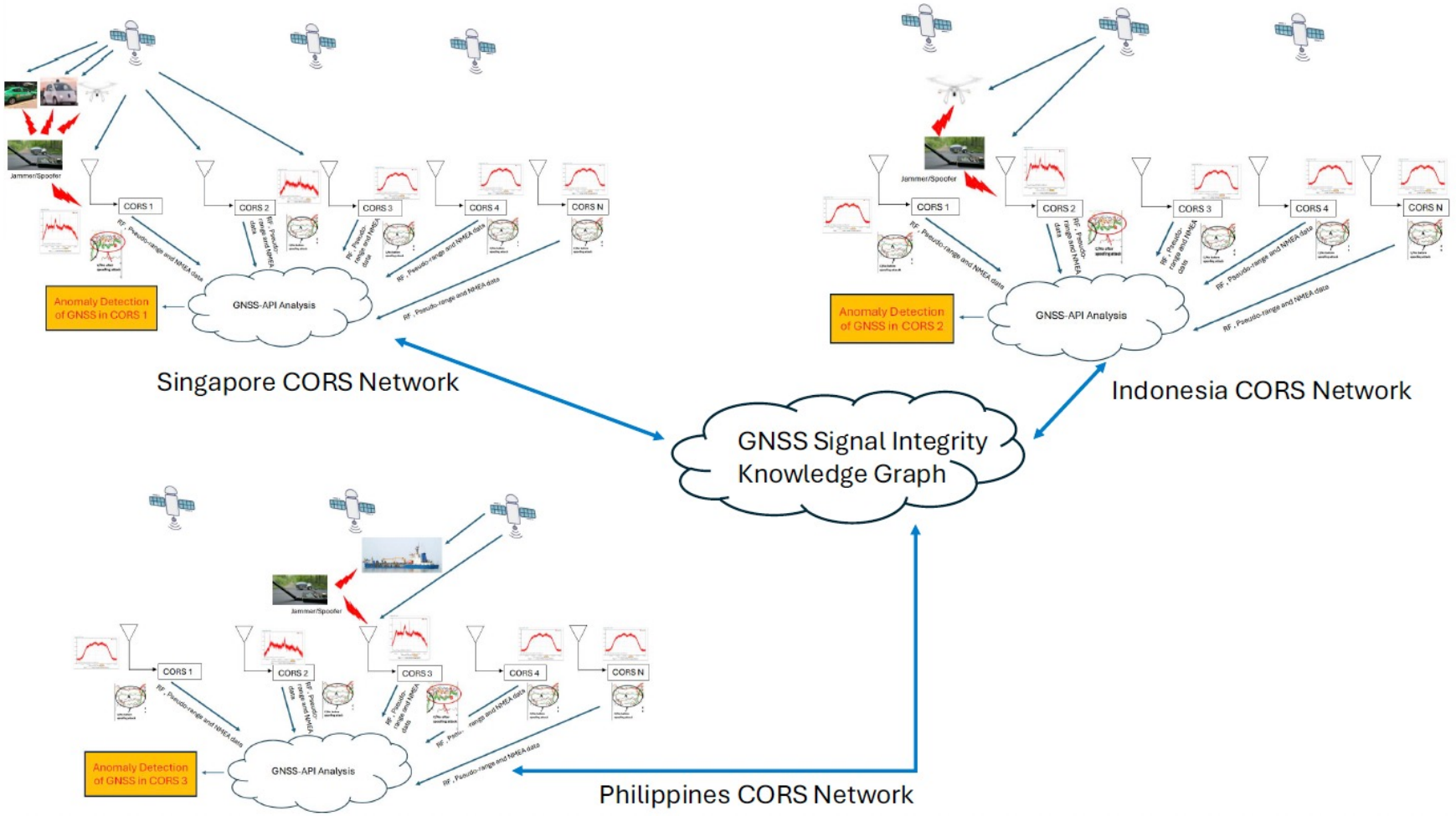
Proposed Method: GNSS-API: GNSS Anomaly Perception and Intelligence

- **Proposed Solution : Multimodal Anomaly Detection and Predictive spoofing/jamming analysis (CORS solution)**
  - **Integrate Multimodal information such as RF spectrum, pseudo range and data stream at each CORS**
  - **Leverage AI/ML engine to build GNSS anomaly signature database**



Proposed Method: GNSS-API: GNSS Anomaly Perception and Intelligence

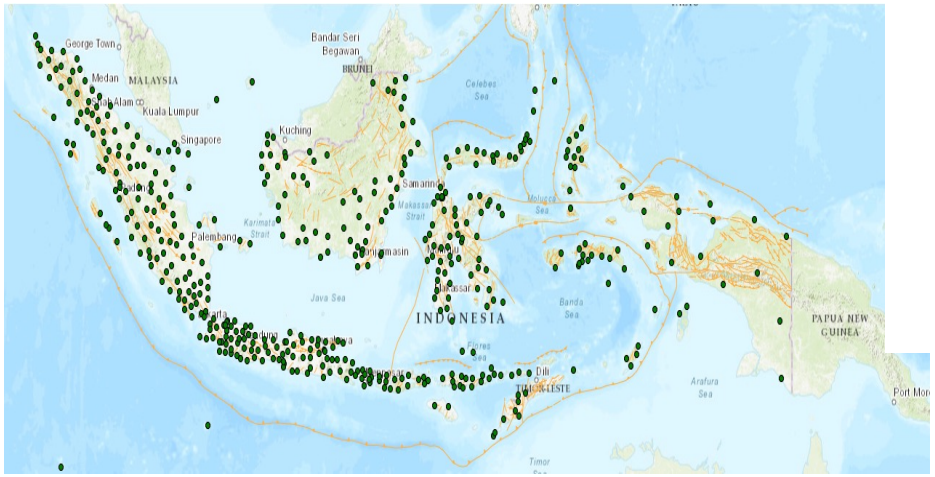
- **Proposed Solution : Multimodal Anomaly Detection and Predictive spoofing/jamming analysis (CORS solution)**
  - **Respective countries' anomaly signature database sharing to build GNSS signal integrity knowledge for ASEAN secure community**



Impact: GNSS-API: GNSS Anomaly Perception and Intelligence

- **The Proposed GNSS-API Multimodal AI approach for the CORS network in Philippines, Indonesia and Singapore**
  - enables cross validation of attack patterns and model training for robust GNSS anomaly detection systems to achieve **"the whole is greater than the sum of its parts"** since there are
    - 55 CORS stations for Philippine Active Geodetic Network (PAGeNet)
    - 484 CORS stations for Indonesian CORS (InaCORS)
    - 9 CORS stations for Singapore SiReNT

PAGeNet



InaCORS

SiReNT

Impact: GNSS-API: GNSS Anomaly Perception and Intelligence

- **Scientific and Technological Impact**
  - Shifts GNSS anomaly detection from vulnerable edge devices to secure CORS infrastructure (NAMRIA PAGeNet, InaCORS, SiReNT), using multimodal AI/ML integration of RF spectrum, pseudo-range, and data streams for pre-emptive threat detection before attacks propagate to end-users.
  - Pioneers machine learning approach across sovereign CORS networks, creating robust AI models trained on diverse attack vectors (Singapore, Philippine, Indonesian) while establishing ASEAN as global leader in AI-driven GNSS integrity solutions.

- **Societal Impact**
  - Protects critical infrastructure including aviation safety (Manila airport), maritime navigation (South China Sea), autonomous vehicles, emergency services, and financial systems by preventing GNSS spoofing/jamming attacks that threaten millions of daily users across ASEAN.
  - Secures ASEAN's digital economy by addressing ride-hailing fraud (GRAB/GOJEK "Tuyul" apps), protecting Singapore's satellite-based ERP toll collection, and enabling trustworthy deployment of smart city infrastructure essential for the region's rapid urbanization and digital transformation.

Impact: GNSS-API: GNSS Anomaly Perception and Intelligence

- **Collaborative Impact**
  - Establishes unprecedented tri-national research partnership (Philippines-Indonesia-Singapore) where each nation contributes unique threat intelligence through their CORS networks, creating collective AI models where "**the whole is greater than the sum of its parts**" while maintaining data sovereignty.
  - Creates scalable blueprint for regional GNSS security cooperation bridging academia-government-industry partnerships, with immediate deployability through existing infrastructure (PAGeNet, InaCORs and SIRENT stations) and potential expansion across ASEAN, positioning the region as pioneer in infrastructure-based satellite navigation security
  - The team comprises of
    - Associate Professor, Soon Yim Tan, Nanyang Technological University, Singapore,
    - Associate Professor, Chee Kiat Seow, Sye Loong Keoh, Qi Cao, University of Glasgow, Singapore,
    - Professor, Noriel Tiglao, University of the Philippines , Philippines
    - Associate Professor, Lin Yola, Universitas Indonesia, Indonesia
    - Principle Geomatics Manager, Hua Seng, Tan, Singapore Land Agency (SLA), Singapore
    - Dr. Dinesh Manandhar, Founder & CDO, LocationMind Inc, Japan
    - CORS network partners in Singapore, Indonesia and Philippines

Output/Outcome: GNSS-API: GNSS Anomaly Perception and Intelligence

- **Scientific Outcome for GNSS-API**
  - Operational GNSS-API software platform with trained AI/ML models deployable across CORS networks, including open-source codebase, detection algorithms, data fusion pipelines, and real-time alerting system tested and validated across three national infrastructures.
  - New application domains enabled such as protected drone delivery systems, secure emergency response coordination, authenticated precision timing for financial networks, and GNSS-verified carbon credit systems for sustainable agriculture monitoring across ASEAN region.

- **Societal Outcome for GNSS-API**
  - Technical documentation on multimodal GNSS anomaly detection methodology that perhaps could become ISO standard for CORS-based positioning integrity.
  - Trained workforce of GNSS security specialists across three nations through workshops and certification programmes

- **Collaborative Outcome for GNSS-API**
  - Joint intellectual property portfolio with patent applications filed for multimodal anomaly detection methods, shared research infrastructure including cloud-based AI training platform, and co-authored peer-reviewed publications establishing team as leading experts in GNSS security.

Output/Outcome: GNSS-API: GNSS Anomaly Perception and Intelligence

- **Collaborative Outcome for GNSS-API**
  - Established quarterly Technical Exchange Program rotating researchers between NAMRIA Taguig facility, InaCORS operations center, and SLA Singapore headquarters, creating lasting professional networks and mentorship pipelines for next-generation GNSS researchers across ASEAN institutions.

Conclusion: GNSS-API: GNSS Anomaly Perception and Intelligence

Targets

- **Critical Threats** :GNSS jamming/spoofing in South China Sea, Manilla airport complete signal loss , GRAB/GOJEK fake GNSS fraud and Singapore ERP toll evasion
- **Protected Infrastructure**: Aviation safety, Maritime navigation, Autonomous vehicles, Smart City IoT, Emergency services and financial timing systems.

Method

- **Innovation** : Shift detection from vulnerable edge devices to secure CORS infrastructure (PAGeNET, InaCORS and SiReNT)
- **Multimodal AI/ML :** RF spectrum + Pseudo-range+ data fusion, machine learning across the respective CORS networks, preemptive detection before attack propagation

Scientific impact

- Infrastructure-based GNSS security paradigm
- Open-source algorithms and threat intelligence database
- Standards submitted for ISO

Societal impact

- Protect 680 million+ ASEAN population
- Prevents aviation/maritime accidents
- Secures economic systems (ERP, ride hailing)

Conclusion: GNSS-API: GNSS Anomaly Perception and Intelligence

Societal impact

- Train GNSS security specialists

Collaborative impact

- Permanent tri national CORS partnership
- Expandable to ASEAN-wide framework
- Global leadership in satellite navigation security

References

[1] Dark Reading, "GPS Spoofing Attacks Spike in Middle East, Southeast Asia," April 2025

[2] Gojek, "Hapus Download Aplikasi APK Tuyul Gacor Mod Fake GPS," Official Blog, 2024

[3]F. Marii and G. Pangestu, "Classification of Fake GPS in GOJEK Application using Logistic Regression," ACM, SIET, 2021

[4] GPS World, "GNSS spoofing threatens airline safety, alarming pilots and aviation officials," October 2024

[5] R. Zhang, C.K. Seow, K. Wen et.al, "Spoofing Attack of Drone," IEEE ICCC, pp. 1239-1246, 2018

[6] R. Zhang, C.K. Seow, et al, “Cellular Positioning Vulnerability”, Springer Nature, 2025 Accepted for publication

[7] Z. Feng, C.K. Seow, and Q. Cao, "GNSS Anti-spoofing Detection based on Gaussian Mixture Model Machine Learning," IEEE ITSC, pp. 3334-3339, 2022

[8] Y.H. Chu, S.L. Keoh, C.K. Seow, et al., "GPS Signal Authentication Using a Chameleon Hash Keychain," Critical Infrastructure Protection XV, pp. 209-226, Springer, 2022