Trustable Global Navigation Satellite System (GNSS) for Secure Community and Applications

Asst. Prof, Dr. Chee Kiat,Seow

University of Glasgow, Singapore

Trustable Global Navigation Satellite System (GNSS) for Secure Community and Applications -TGSCA

- 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

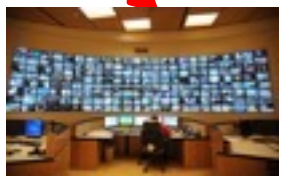
GNSS Time
GNSS supporting Smart Finance

Under Spoofing Attack

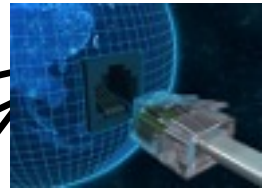
A $200 spoofer can mimic the set of fake GNSS satellites to change the PVT


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

Ship Routing
Drone


Command & Control Centre

GNSS supporting Smart Transportation

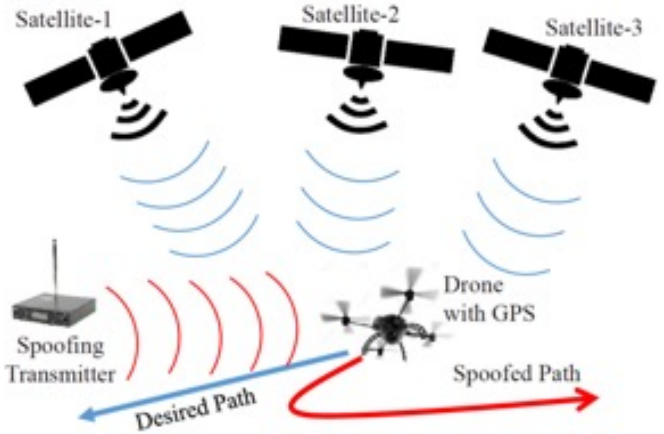
GNSS Time & Position
Comms Networks


5G/6G Cellular , Satellite and wireless internet

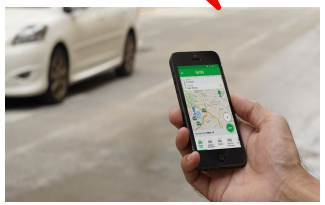
WeChat
Google Maps
Access GIS/Map
GNSS supporting Smart Network

Trustable Global Navigation Satellite System (GNSS) for Secure Community and Applications-TGSCA

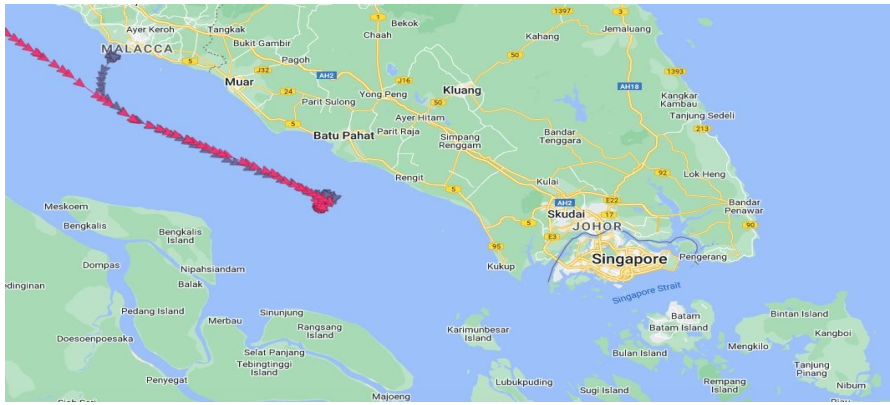
- **Various ASEAN Countries suffers GNSS spoofing threat. E.g**
  - Malaysia
    - GRAB drivers steal bookings from other drivers [1]
    - GRAB drivers give their fake location to GRAB company [1]
    - Collison of the crude oil tanker Zephyr I along Malacca Strait[2]
    - Masquerade as potential GRAB driver to customer [3]
  - Indonesia & Singapore
    - Driver spoofed their location to GOJEK so that customer at their preferred location can be assigned to them [4]



- **Targets of the proposed solution**
  - Provide authentic GNSS signal [5]
    - any company and applications that make use of GNSS such as transportation company e.g. GRAB
    - any GNSS users especially ladies and kids
    - National infrastructures such as 5G/6G system etc.



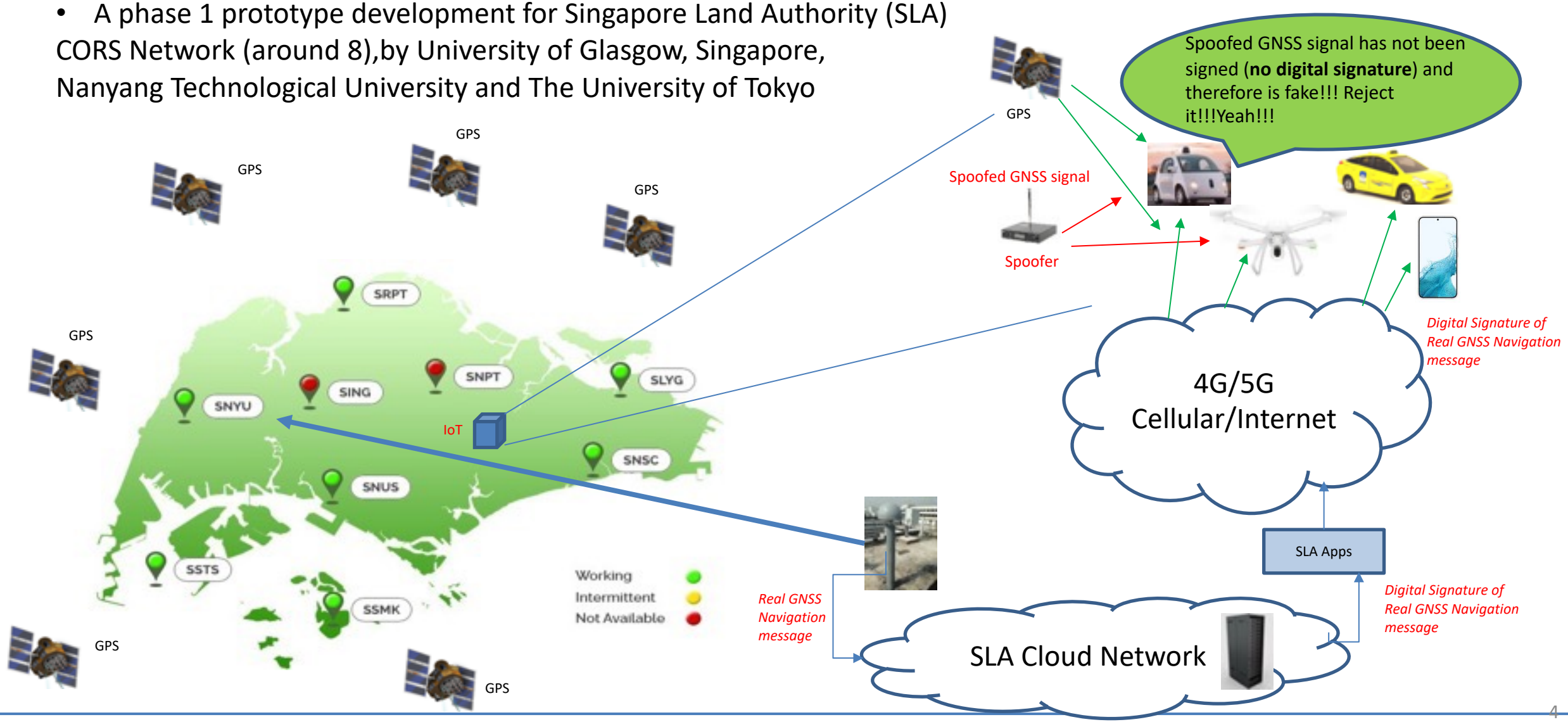
HackRF transceiver in the car to spoof own location or nearby vehicle



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.

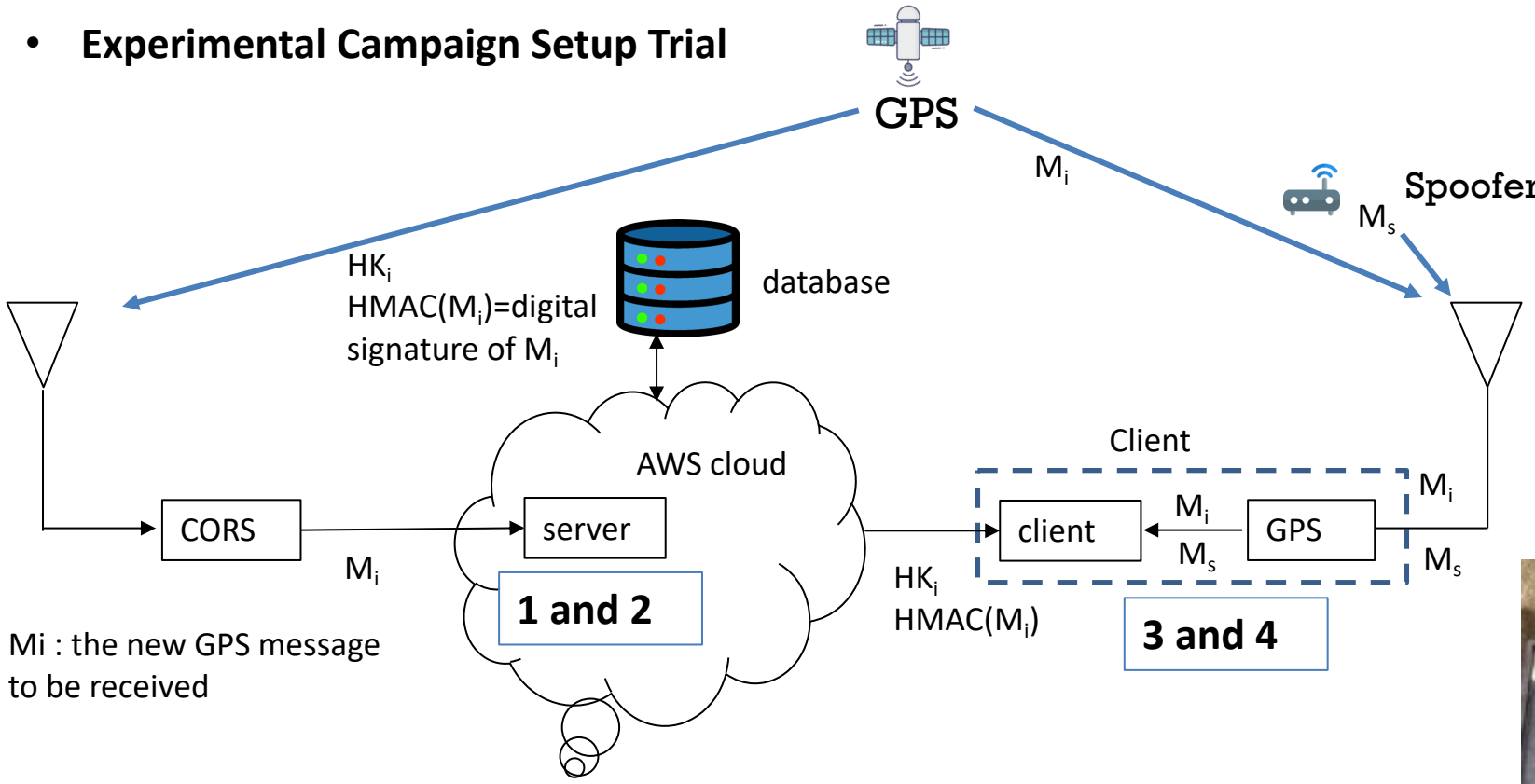
Proposed Method: Digital Signature for authentic, trusted GNSS signal

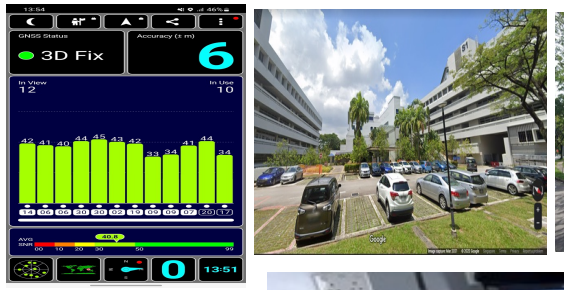
- **Provide GNSS Navigation Message Authentication over Continuously Operating Reference Station (CORS) network**
  - A phase 1 prototype development for Singapore Land Authority (SLA) CORS Network (around 8),by University of Glasgow, Singapore, Nanyang Technological University and The University of Tokyo



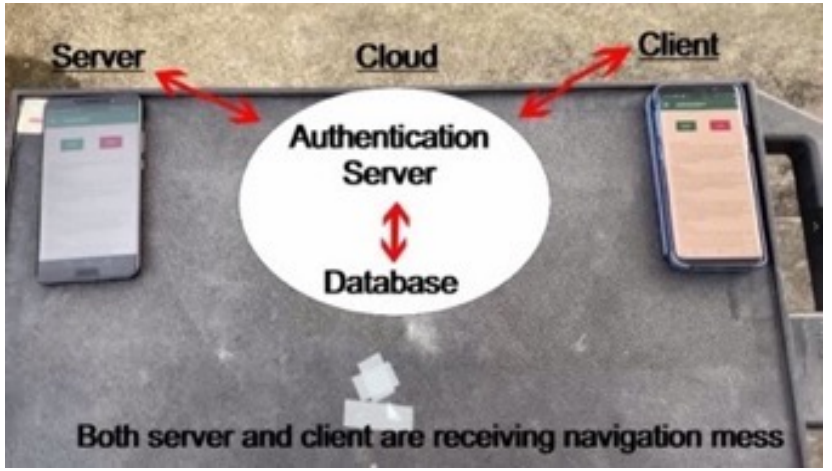
Proposed Method: Digital Signature for authentic, trusted GNSS signal

- **Experimental Campaign Setup Trial**





Spoofer using HackRF

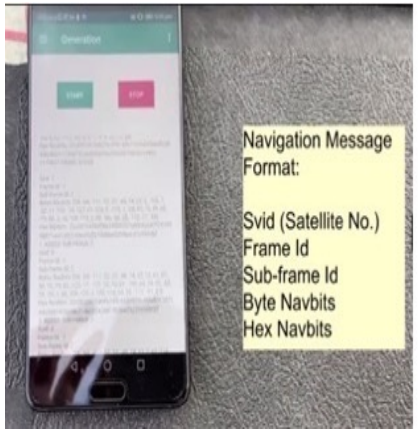


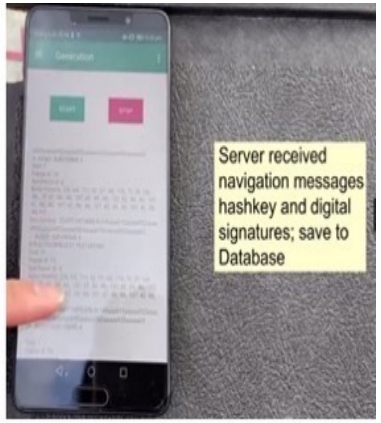
GNSS Digtal Signature using Chamelon Hashing for Server and Client Setup

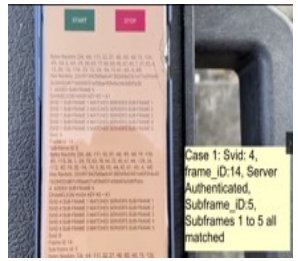
Step 1 : Server Compute hash key and HMAC digital signature for Message i, Hk_i, $HMAC(M_i)$
Step 2: Store Hk_i, $HMAC(M_i)$ in database
Step 3 : Client requests hash key and HMAC digital signature for Message i.
Step 4 : Client creates digital signature of incoming message Mi and spoofed message Ms with hash key. It compares the digital signature of spoof message and authentic message i. **Spoof message M_s digital signature cannot be matched with those stored->Ms is invalid/spoofed signal**

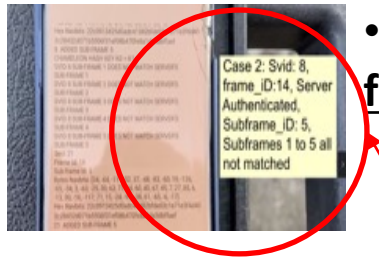
Proposed Method: Digital Signature for Authentic, trusted GNSS signal

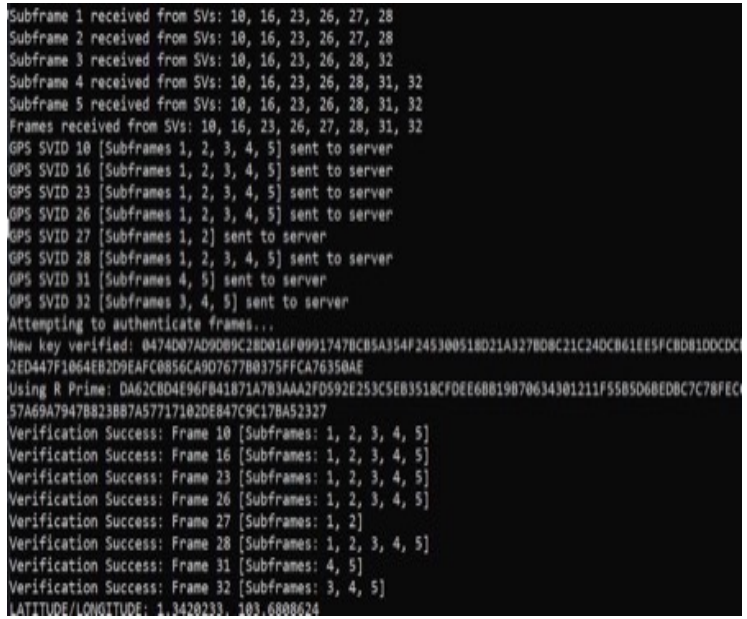
- **Experimental Campaign Setup Trial**
  - Evaluation and Experiment result at NTU@S2 Rooftop









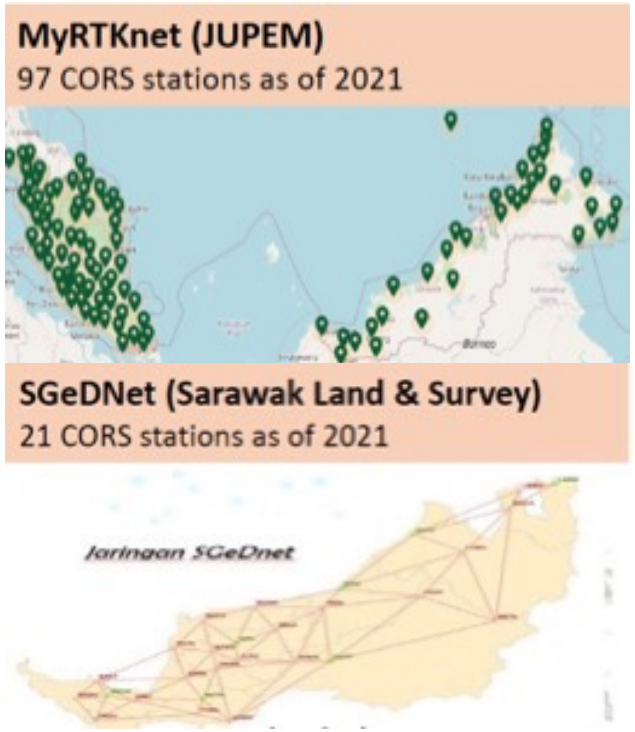


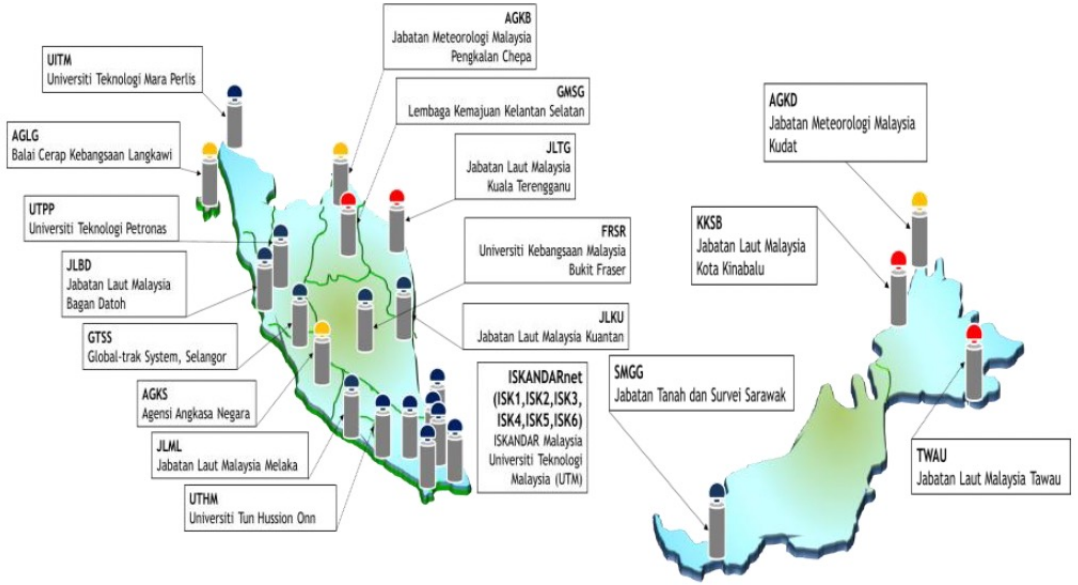
- Project required KPI authentication success rate is **95%**
- Authentication success rate is **99.4% for IoT device**
- Authentication success rate is **99.0% for Android phone**

Rejected

Impact: Trustable GNSS for CORS implementation in Malaysia

- **The Technological Success of Phase 1 Prototype with at least 95% Authentication Success**
  - Exploring the outreach of the proposed GNSS authentication methodology to adapt to CORS network in Malaysia [6] since there are
    - 97 CORS stations for MyRTKnet (JUPEM) , 21 CORS stations for SGeDNet (Sarawak Land & Survey)
    - 6 CORS stations for SISPELSAT(MarineDepartment), 1 CORS station for GBAS (Civil Aviation Authority Malaysia)
  - Through leverage on some of the 23 R&D CORS network for phase prototyping and implementation



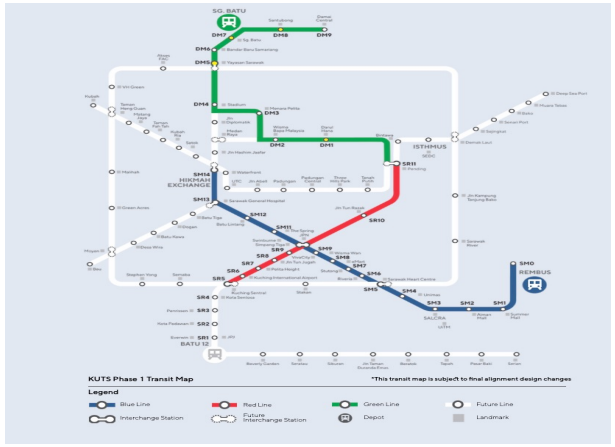


<u>23 R&D CORS Network station as a platform to develop space based applications for the country among Government, agencies, universities and industry</u>

Impact: Trustable GNSS for CORS implementation in Malaysia

- **Technological/ Societal Impact for Phase 1.0 (Singapore) and Phase 2.0 (Malaysia)**
  - Singapore
    - The acceleration of various smart nation initiatives that rely heavily on GNSS provides the momentum in the expected increase of spoofers.
      - Proposed phase 1 prototype give assurance to SLA end users on the integrity of the GNSS especially on smart construction sector where precise GNSS centimeters accuracy is required for piling and drones building façade inspection.
      - SLA and Govtech end users will be able to develop secure mobile apps for the community
  - Malaysia
    - resolve the above mentioned GNSS threat on
      - Business sustainability for companies and applications such as transportation& delivery company e.g., GRAB.
      - Drivers will be assured of guaranteed livelihood and safety
      - Commuters will be assured of personal safety especially ladies and kids.
      - National Infrastructure reliability and integrity especially growth of GNSS applications and addressing vulnerability is one of the key objectives of Malaysian Space Agency (MYSA)
    - Government Smart initiatives that affect commuters' behaviors and confidence such as Kuching Urban Transportation System (KUTS)-fully autonomous transport system

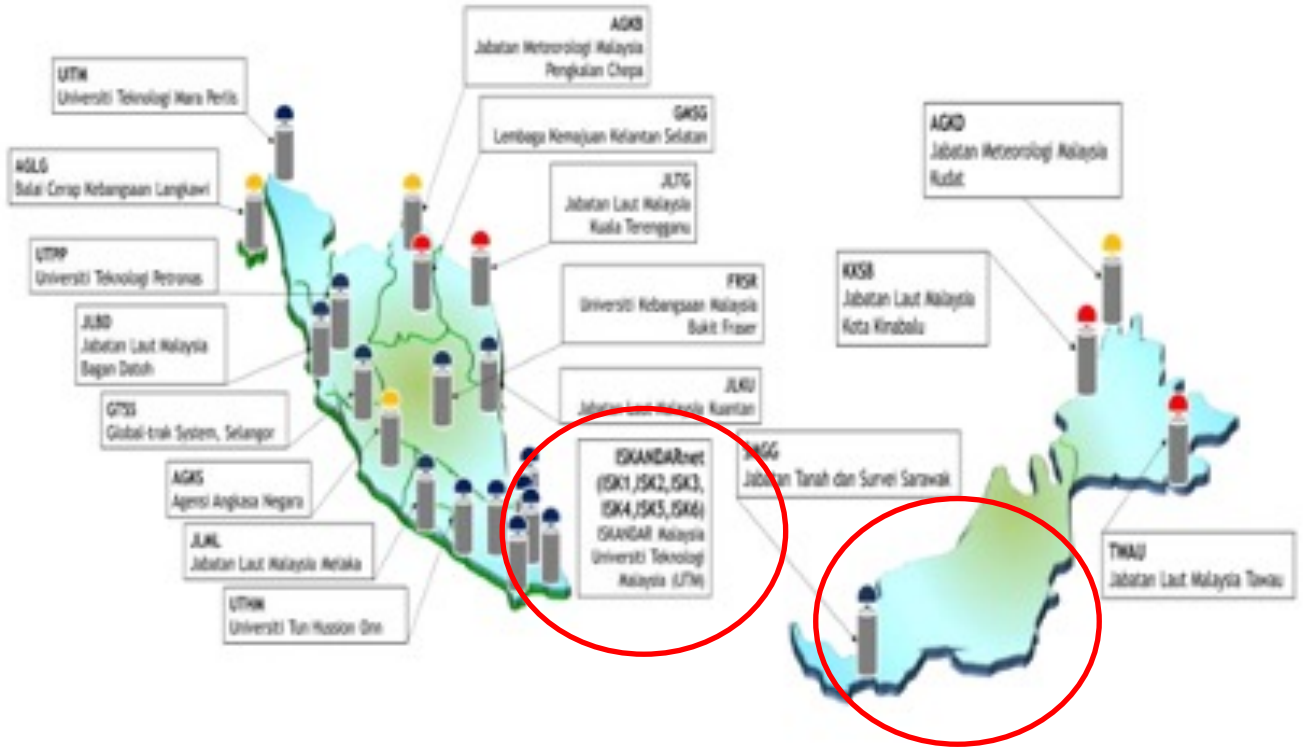
Impact: Trustable GNSS for CORS implementation in Malaysia

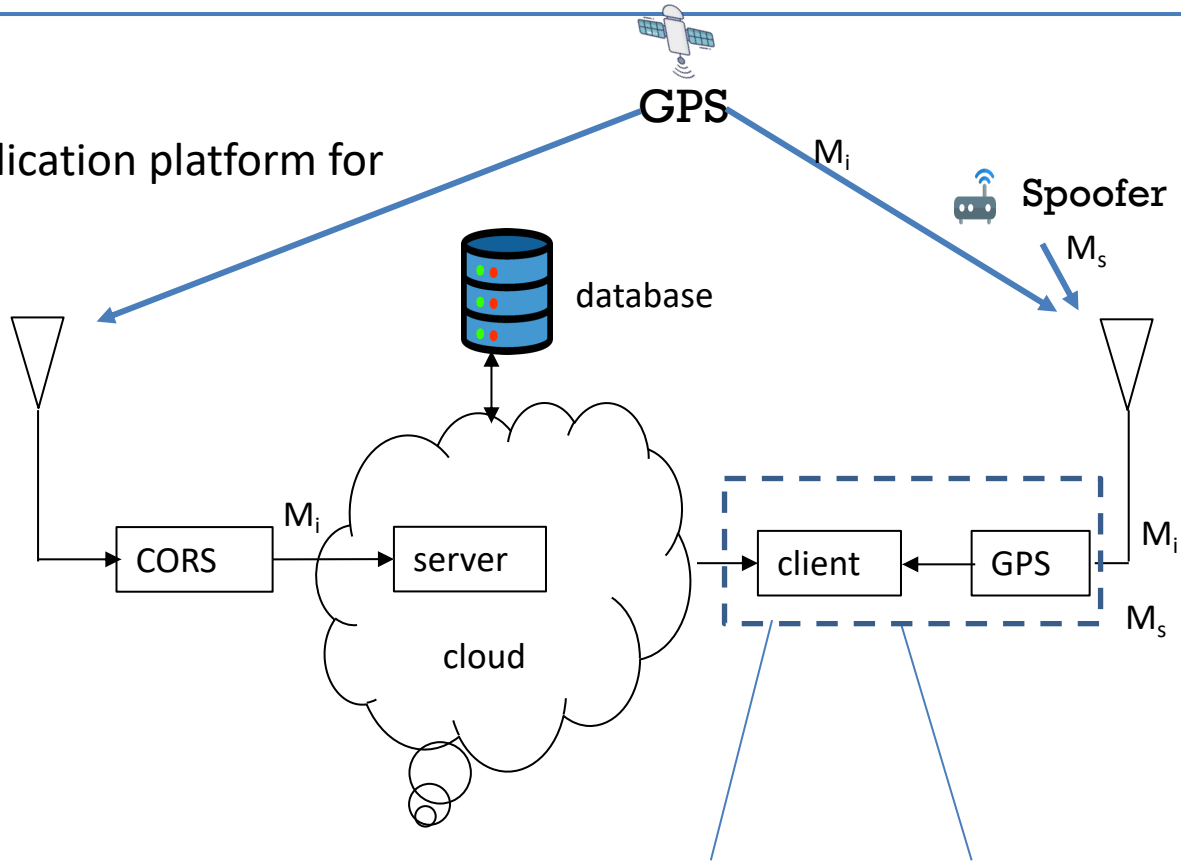


- **Collaborative Impact for Phase 2.0 (Malaysia)**
  - Expand strong collaboration from phase 1 that comprises of University of Glasgow, Singapore, Nanyang Technological University, Singapore and The University of Tokyo, Japan with
    - Universiti Teknologi Malaysia (UTM)
    - Universiti Malaysia Sarawak (UNIMAS)
    - Swinburne University of Technology Sarawak Campus (SUTS)
    - CORS network partners in Johor and Sarawak

Output/Outcome: Trustable Global Navigation Satellite System (GNSS) for Secure Community and Applications-TGSCA

- **Technological Outcome for TGSCA**
  - A new trustable GNSS for secure community and application platform for
    - Johor
      - Leverage on ISKANDARNET CORS
    - Sarawak
      - Leverage on SWGG CORS





1. Android phone
2. IoT devices such as raspberry

- To achieve 95% success in spoofing authentication

Output/Outcome: Trustable Global Navigation Satellite System (GNSS) for Secure Community and Applications-TGSCA

- **Societal Outcome for TGSCA**
  - A potential technological incubation platform to develop new customized TGSCA and transfer technology know-how under local context such as for KUTS companies or GNSS cybersecurity startup companies
  - Path the way for future Nation-wide GNSS Big Data Analytics capability where pockets of secure and insecure GNSS signals in different regions can be segregated- Smart Secure Nation

- **Collaborative Outcome for TGSCA**
  - Grow the technology collaboration and partnership among
    - Nanyang Technological University, Singapore
    - University of Glasgow, Singapore
    - The University of Tokyo, Japan
    - Universiti Teknologi Malaysia (UTM)
    - Universiti Malaysia Sarawak (UNIMAS)
    - Swinburne University of Technology Sarawak Campus (SUTS)
    - CORS network partners in Johor and Sarawak

Conclusion: Trustable Global Navigation Satellite System (GNSS) for Secure Community and Applications-TGSCA

Targets

- To prevent malicious spoofing by providing authentic GNSS signal to
  - any company and applications that make use of GNSS such as transportation company e.g. GRAB
  - any GNSS users especially ladies and kids
  - National infrastructures such as 5G/6G system etc.

Method (idea)

- Provide GNSS Navigation Message Authentication over Continuously Operating Reference Station (CORS) network

Scientific and societal impact

- The novel centralized GNSS digital signature provide integrity and reliability of GNSS
  - To ensure business sustainability and trustworthy of companies and industry
  - To safeguard the livelihood of transportation workers
  - To ensure personal safety for ladies and kids for private ride.
  - National Infrastructure reliability and integrity

References

[1] https://www.malaymail.com/news/money---international/2019/05/17/drivers-use-gps-spoofing-fake-apps-to-defraud-grab-says-ride-sharing-firm/1754081
[2] https://lloydslist.maritimeintelligence.informa.com/LL1142375/Subterfuge-tanker-in-collision-with-boxship-in-Malacca-Strait
[3] https://goodyfeed.com/therere-fake-grab-drivers-msia-grab-issue-warnings/
[4] https://dl.acm.org/doi/10.1145/3479645.3479657
[5] Y.H. Chu, S.L. Keoh, C.K.Seow, Q.Cao, K. Wen and S.Y. Tan "GPS Signal Authentication using a Chamelon Hash KeyChain", International Conference on Critical Infrastructure Proection XV, pp. 209-226, 2022
[6] A. Napiah, "Malaysia's GNSS Initiatives", Fifteenth Meeting of the International Committee on GNSS, 27 Sep – 1 Oct 2021.