ASEAN IVO FORUM 2026 · KUALA LUMPUR

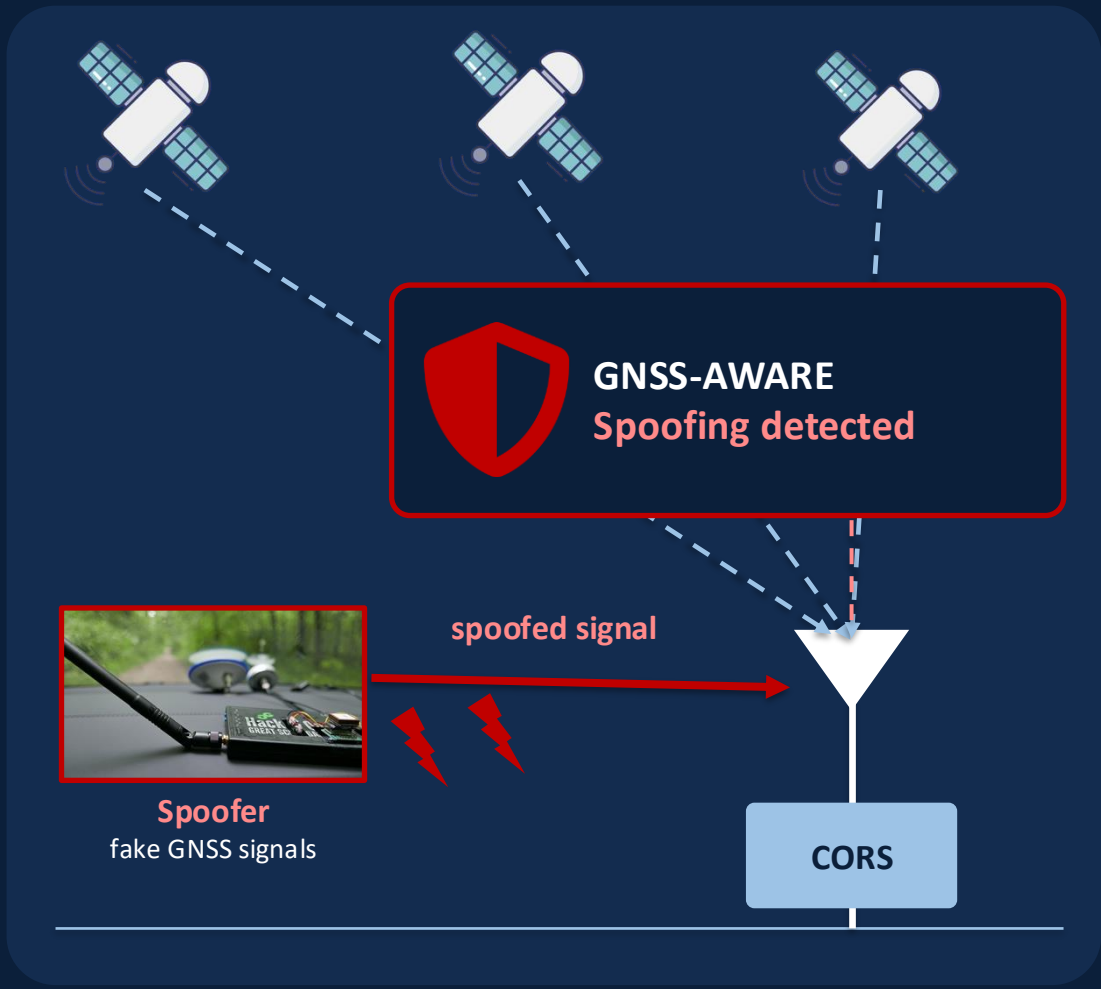
GNSS-AWARE ASEAN

GNSS Anomaly aWareness And Resilience Engine for ASEAN

Associate Professor Chee Kiat Seow (Lawrence)
University of Glasgow, Singapore

Presented on behalf of all project collaborators

with N. Tiglao, L. Yola, S.L. Keoh, H.S. Tan, D. Manandhar, Q. Cao



Project Title: GNSS-AWARE ASEAN — Why GNSS Integrity Matters

- 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

[1] LTA, ERP 2.0 (GNSS-based), 2024


Ride and Delivery
Grab Uber
Driverless Car
GNSS Time & Position
Drone


Command & Control Centre
Air Traffic Control

Ship Routing

GNSS supporting Smart Transportation

GNSS Time & Position
WeChat

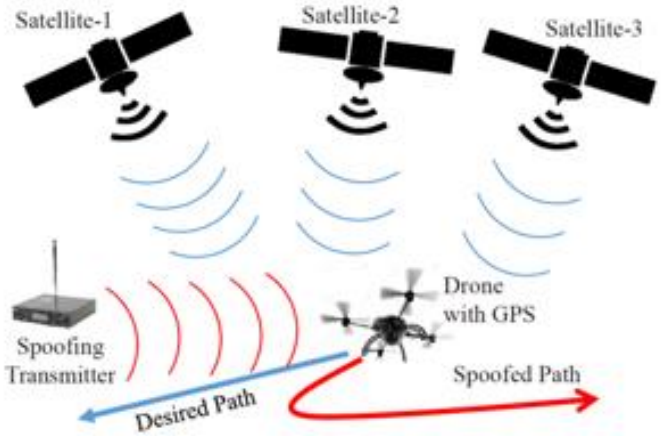
Comms Networks

5G/6G Cellular , Satellite and wireless internet

Google Maps
Access GIS/Map
GNSS supporting Smart Network

Project Title: Background and Targets

- **ASEAN is already under GNSS attack**
  - Jamming over South China Sea, Philippine Sea, E. Indian Ocean: affected flights rose from dozens/day (Feb 2024) to **1,100+ by Aug 2024** [2]
  - Multimodal attacks: RF overpowering, pseudo-range manipulation, NMEA injection [3]
  - GRAB/GOJEK fake-GPS fraud is widespread; detection accuracy as low as **74.7%** [4–6]
  - Spoofing threatens Singapore's ERP toll revenue, AVs, drone delivery and emergency services [1]



Targets of GNSS-AWARE

T1 Multimodal AI/ML GNSS anomaly awareness at secure CORS (RF, pseudo-range, Doppler, clock, NMEA)

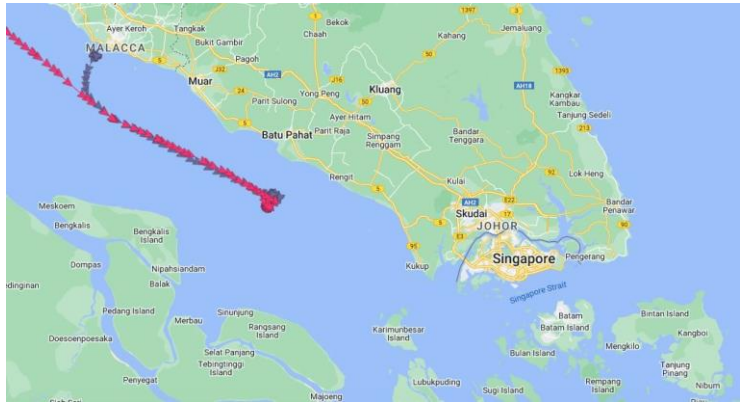
T2 A validated advanced AI detection engine (SIGNAL → federated, physics-informed AI)

T3 ASEAN-TEXBAT: an open regional spoofing benchmark for ASEAN IVO

[2] Dark Reading, Apr 2025 [3] Zhang, Seow et al., IEEE ICCC 2018 [4] Gojek blog, 2024 [5] Marii & Pangestu, ACM SIET 2021 [6] GPS World, Oct 2024



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 (1/3): From Edge Authentication to CORS-Level Multimodal AI

Phase 1 — edge authentication (completed)

- 2023 PMO TRANS Grant for SLA: GNSS Navigation Message Authentication with Chameleon Hash Keychains on SiReNT [7]
- **Completed:** SiReNT Phase 1 work published in the Handbook of Wireless Positioning (2026) [8]
- **Limitation:** device-dependent, hard to scale to every receiver

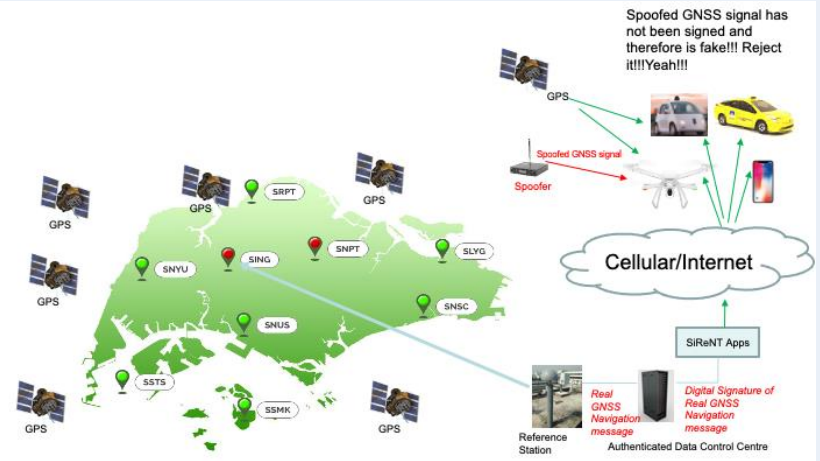


Fig. 1 NMA anti-spoofing on SLA SiReNT

GNSS-AWARE — integrity monitoring moves to secure CORS

- Fuse RF spectrum, pseudo-range, Doppler, clock drift and NMEA streams at every CORS — no edge-device dependency
- Stations co-train common models and cross-validate; GMM feasibility already shown [9,10]

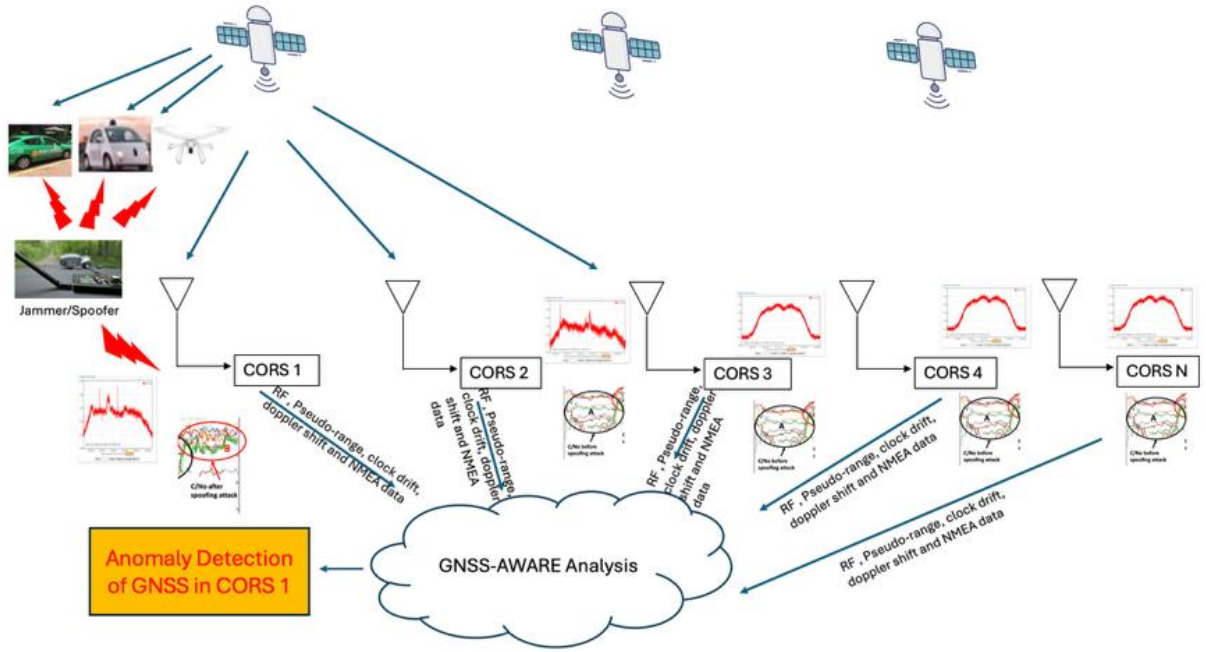


Fig. 2 GNSS-AWARE multimodal analysis across a CORS network

[7] Chu, Keoh, Seow et al., CIP XV, Springer 2022 [8] Zhang, Seow et al., "Cellular Positioning Vulnerability," Handbook of Wireless Positioning, Springer 2026 [9] Feng, Seow, Cao, ITSC 2022 [10] Babić et al., Electronics 2025

Proposed Method (2/3): SIGNAL — First Liquid Neural Network for GNSS Spoofing

Continuous-time state with adaptive time constant and gate [11]

$$\frac{dh}{dt} = \left[-\frac{h}{\tau(x_t)} + \tanh(W_x x_t + U_h h_t) \right] \cdot g$$

$$\tau(x_t) = \tau_0 \cdot \sigma(W_\tau x_t)$$

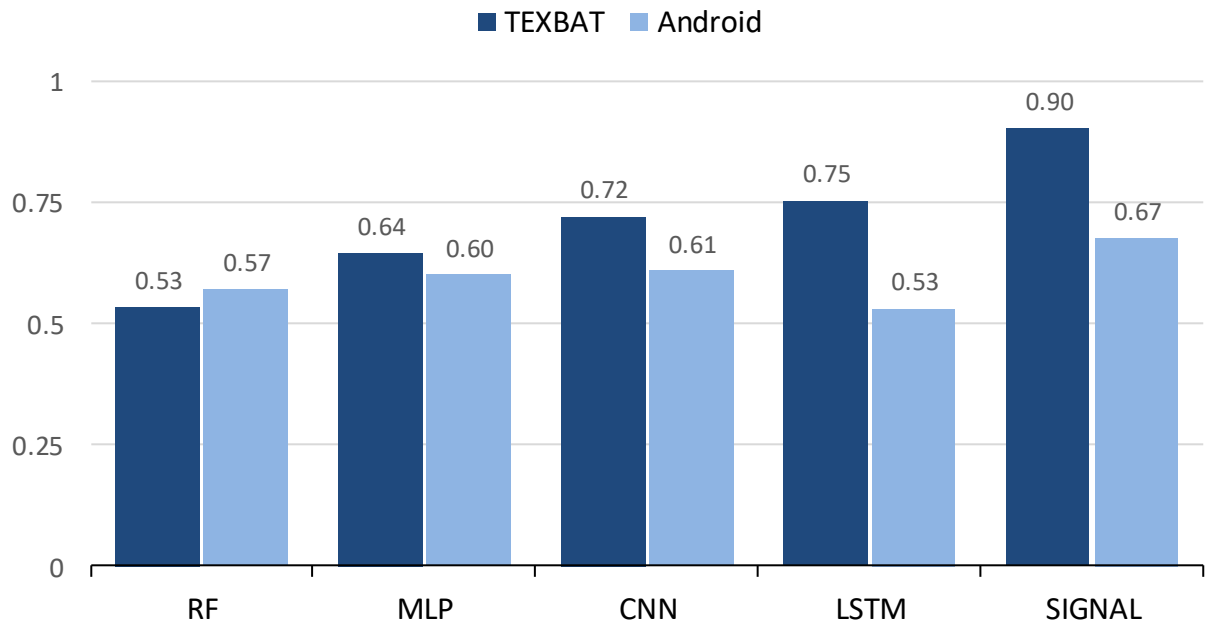
$$g = \sigma\left(W_g [x_t; h_t]\right)$$

- **Small τ** reacts fast to spoofing onset; **large τ** tracks slow drift
- **Gate g** keeps accumulated evidence through gradual, matched-power attacks
- **Data:** TEXBAT (8 attack scenarios) and a self-collected Android dataset (Suzhou): C/N_0, Doppler, I/Q, magnitude, pseudo-range
- **Test:** leave-one-scenario-out vs RF, MLP, CNN, LSTM

0.927
LOO mean F1, TEXBAT

0.904
LOO mean F1, Android

Hardest scenario ds6 (dynamic, matched-power position push): F1



SIGNAL vs LSTM on ds6: +19.7% (TEXBAT), +27.1% (Android)

Why ds6 matters

Dynamic, matched-power position push: easy for an attacker to implement, toughest to detect. Every model drops here.

WP1–WP2 target this hardest class of matched-power attacks — we are going to solve it.

[11] Lim, Seow, Abhishek, "SIGNAL", IEEE PIMRC 2026 [12] Humphreys et al., TEXBAT, ION GNSS 2012

Proposed Method (3/3): ASEAN-TEXBAT and Federated Physics-Informed AI

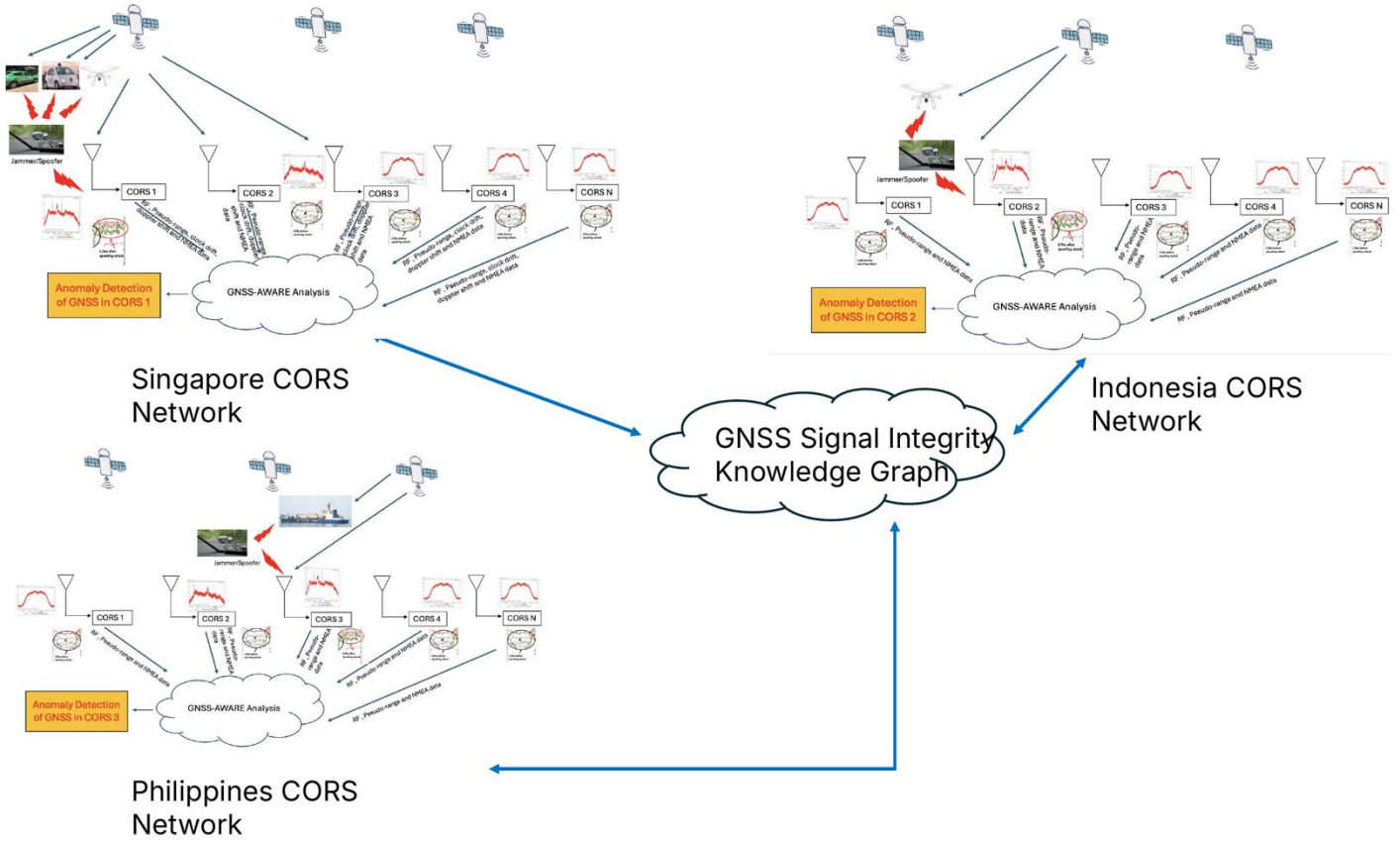
Gap: TEXBAT is static and temperate (USA) — no tropical or monsoon conditions relevant to ASEAN

WP1 — ASEAN-TEXBAT corpus

- Controlled spoofing/jamming data collected jointly at NAMRIA, InaCORS and SiReNT
- Regional threat and tropical conditions; released openly to ASEAN IVO members

WP2 — Federated physics-informed AI

- **Shared parameters:** each CORS trains locally and contributes only to a common set of physics-informed parameters. Raw data stays in-country
- Same attack physics everywhere, so each party's data strengthens all
- Tests cross-national, non-IID attacks — including hard matched-power attacks



Experiments: field collection at the three CORS networks, then cross-national, non-IID generalisation tests — harder and more realistic than single-client, single-dataset studies [11,12]

Diagram: national CORS networks share learned anomaly signatures into a common GNSS signal-integrity knowledge graph

Impact (1/3): A Tri-National CORS Backbone for Collective Threat Intelligence

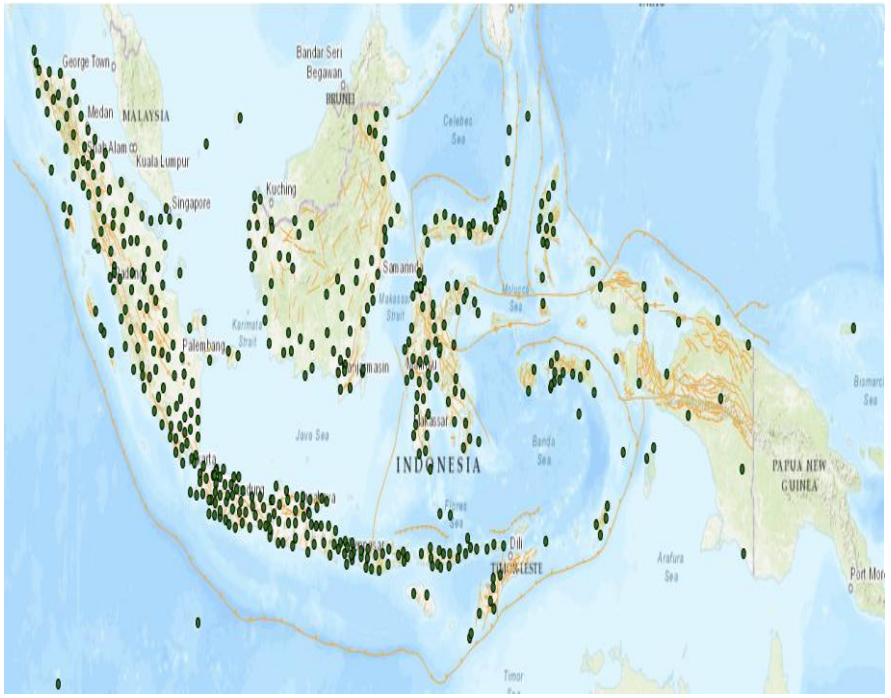
- **Physics-informed AI:** every country contributes through the same shared physical phenomena — so **"the whole is greater than the sum of its parts"**
- Deployable on existing CORS receivers (e.g. Trimble Alloy at SiReNT) — no new hardware at end-users

55 CORS stations



Philippines — PAGeNet

484 CORS stations



Indonesia — InaCORS

9 CORS stations



Singapore — SiReNT

Impact (2/3): Scientific, Technological and Societal

Scientific and technological

- Pre-emptive detection at secure CORS across RF, pseudo-range, Doppler, clock and NMEA — before disruption reaches users
- Continuous-time modelling shown to improve cross-scenario generalisation: an empirical, not just architectural, advantage
- To our knowledge, the first federated physics-informed detector across national CORS networks
- Scalable blueprint for global GNSS integrity, led from ASEAN

Societal

- Aviation and maritime safety: South China Sea jamming, Manila airport disruption, Malacca Strait shipping
- Digital economy: ride-hailing GPS fraud (GRAB/GOJEK) and Singapore's GNSS-based ERP tolling
- Autonomous vehicles, drone delivery and emergency services
- Serves **680M+** people (ASEAN)

1,100+ flights/day hit by GPS jamming in the region (Aug 2024) [2]

74.7% fake-GPS detection accuracy reported in ride-hailing [5]

0.927 SIGNAL F1 on unseen spoofing attacks (TEXBAT) [11]

Impact (3/3): Collaborative — Academia, Government and Industry

- Tri-national partnership: Philippines, Indonesia, Singapore, with Japan
- Each nation keeps its data; models learn from all
- Bridges universities, national mapping agencies (SLA, NAMRIA, InaCORS) and industry (LocationMind)
- ASEAN-TEXBAT becomes a shared asset for future ASEAN IVO cohorts

Team

- **A/P Chee Kiat Seow** University of Glasgow, Singapore
- **Prof. Noriel Tiglao** University of the Philippines
- **A/P Lin Yola** Universitas Indonesia
- **Prof. Sye Loong Keoh** University of Glasgow, Singapore
- **Hua Seng Tan** Principal Geomatics Manager, SLA
- **A/P Dinesh Manandhar** The University of Tokyo; CDO, LocationMind
- **A/P Qi Cao** National University of Singapore

Output/Outcome (1/2): New Technology and Public Assets

Scientific

- Published: SIGNAL, first LNN for GNSS spoofing detection (IEEE PIMRC 2026) [11]
- IVO extension: federated physics-informed AI engine with trained multimodal models, deployable on CORS networks
- New applications: protected drone delivery, authenticated timing for finance, secure emergency response

Societal

- ASEAN-TEXBAT: open dataset for ASEAN IVO members and end-users — SLA, NAMRIA, InaCORS, ride-hailing and drone operators
- Technical documentation on CORS-based multimodal integrity monitoring, as input to standards bodies
- Technology transfer to SLA, NAMRIA and InaCORS operations, and to industry via LocationMind; joint workshops

Delivered: SiReNT Phase 1 NMA, completed [7,8] · GMM detector [9] · SIGNAL at IEEE PIMRC 2026 [11]

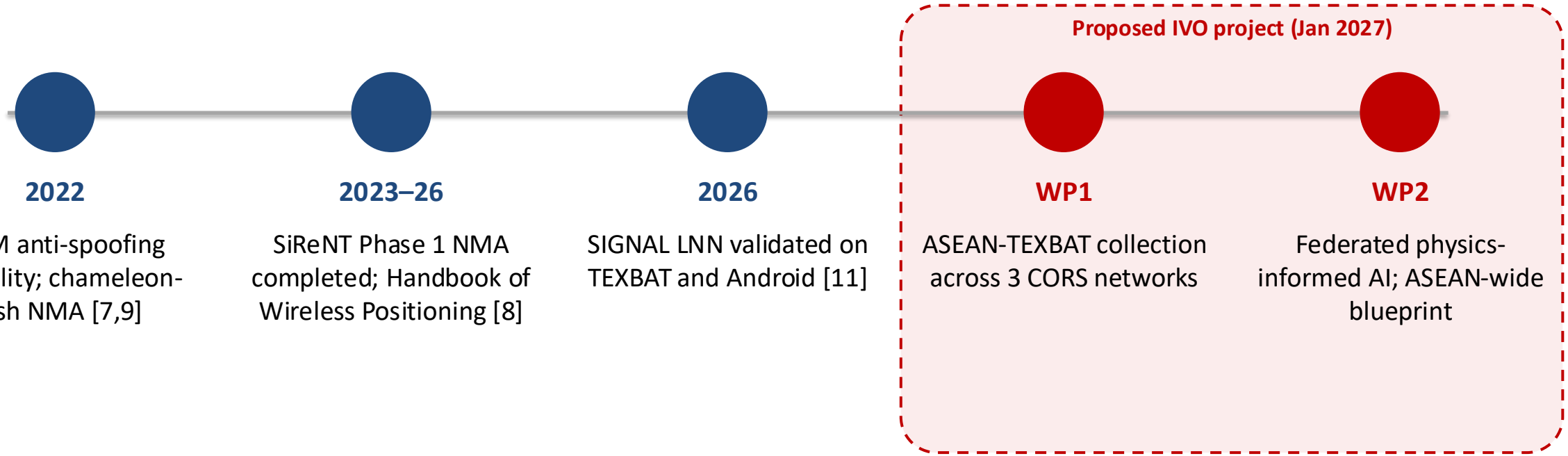
Proposed WP1–WP2: ASEAN-TEXBAT open release · federated GNSS-AWARE engine across PAGeNet, InaCORS, SiReNT

[7] Chu, Keoh, Seow et al., CIP XV 2022 [8] Zhang, Seow et al., Handbook of Wireless Positioning, Springer 2026 [9] Feng, Seow, Cao, ITSC 2022 [11] Lim, Seow, Abhishek, PIMRC 2026

Output/Outcome (2/2): Collaborative Outcomes and Roadmap

Collaborative

- Lasting tri-national CORS partnership, open to new national CORS partners across ASEAN
- Shared federated training platform, joint publications and IP, and researcher exchange across NAMRIA, InaCORS and SLA
- New colleagues for ASEAN IVO: national mapping agencies, universities and industry working on one benchmark



[7] Chu, Keoh, Seow et al., CIP XV 2022 [8] Zhang, Seow et al., Handbook of Wireless Positioning, Springer 2026 [9] Feng, Seow, Cao, ITSC 2022 [11] Lim, Seow, Abhishek, PIMRC 2026

Conclusion: GNSS-AWARE ASEAN

Targets	Method	Impact
• Documented ASEAN jamming/spoofing: aviation, maritime, ride-hailing fraud, ERP tolling • Three targets: multimodal anomaly awareness at CORS, a validated AI engine, and the ASEAN-TEXBAT benchmark	• Shift detection from edge devices to secure CORS (PAGeNet, InaCORS, SiReNT) • SIGNAL LNN: LOO F1 0.927 / 0.904; +19.7–27.1% over LSTM on hardest attack • Proposed WP1–WP2: ASEAN-TEXBAT + federated, cross-country physics-informed AI	• Scientific: continuous-time AI generalises to unseen attacks; open regional benchmark • Societal: safer skies, seas, roads and payments for 680M+ people (ASEAN) • Collaborative: tri-national partnership, expandable ASEAN-wide

Secure GNSS at the infrastructure, share the physics across borders — "the whole is greater than the sum of its parts."