

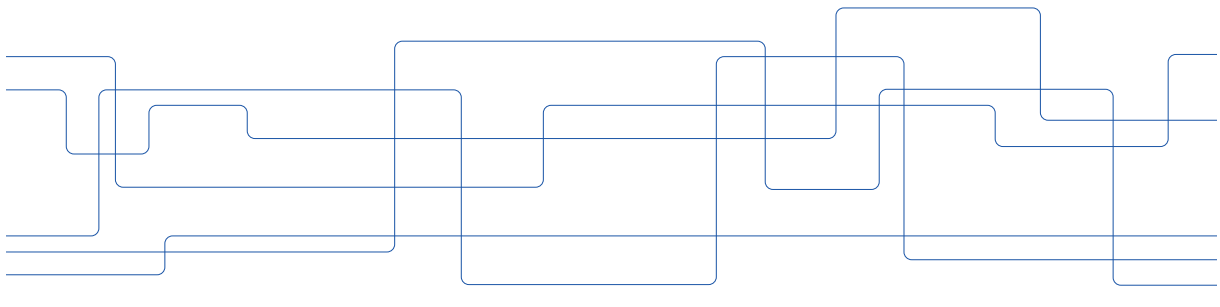


KTH ROYAL INSTITUTE
OF TECHNOLOGY

Securing location and reducing device exposure

Panos Papadimitratos

www.eecs.kth.se/nss



0

Acknowledgements

- Current NSS members

- **Marco Spanghero**
- **Wenjie Liu**
- **Hongyu Jin**

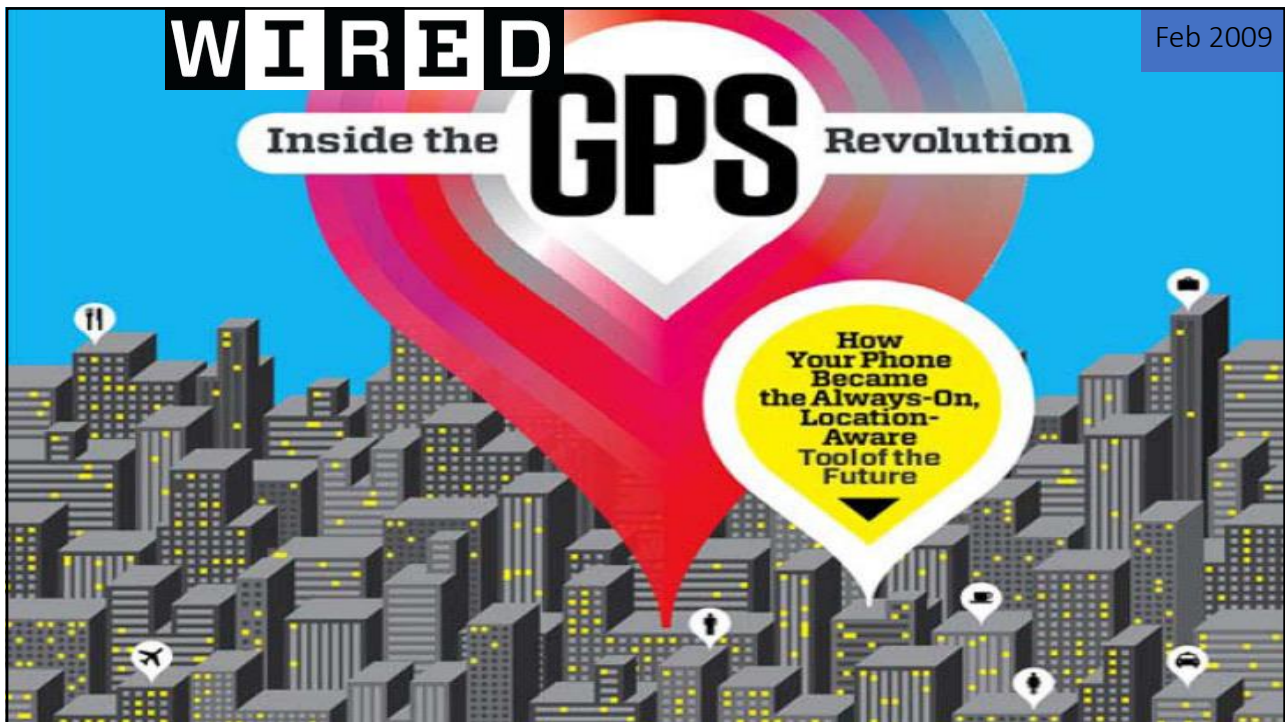
- Alumni

- **Kewei Zhang**
- **Malte Leinhart**
- **Mohammad Khodaei**

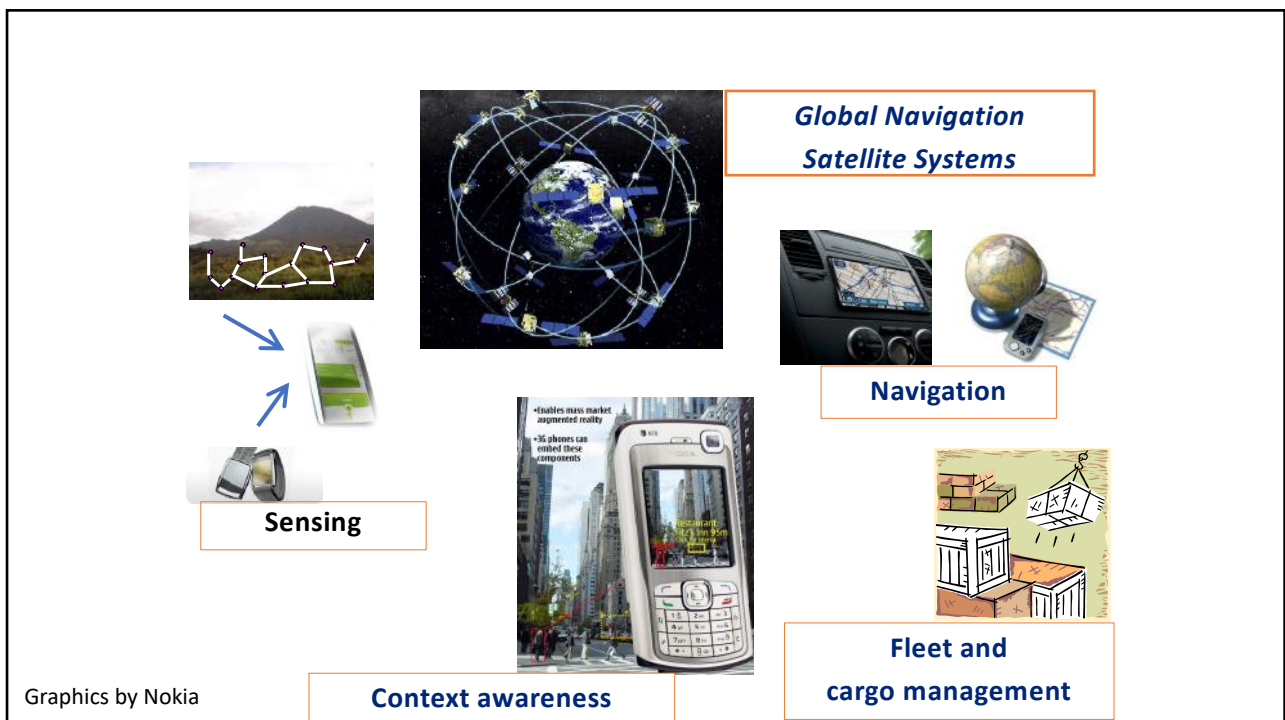
- Knut and Alice Wallenberg (KAW) Foundation, Academy Fellows Program
- Swedish Foundation for Strategic Research (SSF), SURPRISE project

1

1



2



3



4

Global Navigation Satellite Systems (GNSS)

GPS GLONASS Galileo BeiDou-2

GNSS receiver, V

1. Receive NAV_i from satellite S_i at position s_i
2. Estimate the NAV_i propagation delays, and thus V - S_i distances (pseudoranges), ρ_i
3. Minimize the system of equations given by the ρ_i
4. Obtain own position, loc_V , and clock correction, t_V

$\rho_i = |s_i - loc_V| + c \cdot t_V$

Networked Systems Security (NSS) group

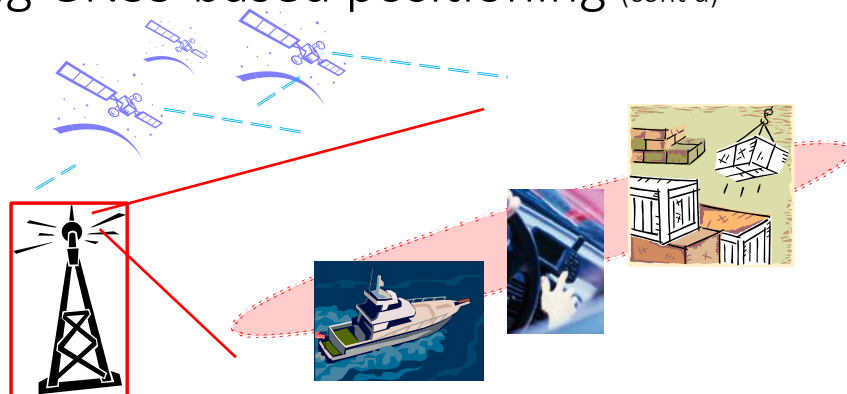
5

Attacking GNSS-based positioning

- Mislead devices (and their users) about their location
 - Compromise the device: hard
 - Compromise the infrastructure: much harder
 - Interfere with the infrastructure-to-device wireless communication
 - Easy
 - Jam → Outage
 - Not too hard
 - Overwrite legitimate transmissions with synthesized ones → Control loc_V and t_V

6

Attacking GNSS-based positioning (cont'd)



- *Attacker:* Record and replay, or forge, GNSS signals, overwriting the legitimate GNSS signals
- *System:* GNSS receiver locks on spoofed signals
- *Consequence:* User provided with a false, attacker-controlled location and time

7

Attacking GNSS-based positioning (cont'd)

Armored Vehicle Demonstration flop [2001]

Russian Truck Hijacking [2007]

California Cell Infrastructure Outage [2008]

Seoul airport jamming [2012]

US Unmanned Area Vehicle downed [2012]

8

8

The collage features several news articles and maps. Top left: 'Mass GPS Spoofing Attack in Black Sea?' with a map of the Black Sea showing blue dots. Top middle: 'Iran shows 'hacked US spy drone' video footage' with a video player. Top right: 'Disruption of GPS systems at Ben Gurion Airport resolved after 2 months' with a photo of an airport. Middle left: 'Chinese vessels off Galapagos 'cloaking' in New Zealand' with a photo of a ship. Middle right: 'Russia suspected of jamming GPS signal in Finland' with a photo of a soldier. Bottom left: 'Chinese GPS spoofing circles could hide Iran oil shipments' with a map of the Persian Gulf showing red circles. Bottom middle: A photo of a soldier in a vehicle. The collage also includes a 'NEWS' header with navigation links and social media sharing icons.

9

Defending GNSS-based positioning

- Many proposals/defense mechanisms
 - Monitor signal properties, e.g., received signal strength, Doppler frequency shift
 - Adversary could predict and adjust
- Cryptographic protection of civilian GNSS signals
 - Upcoming but adoption will take time
- Challenge: Attacks that do not change the navigation messages can still succeed
 - Relay/replay attacks
 - Distance-decreasing attacks

10

10

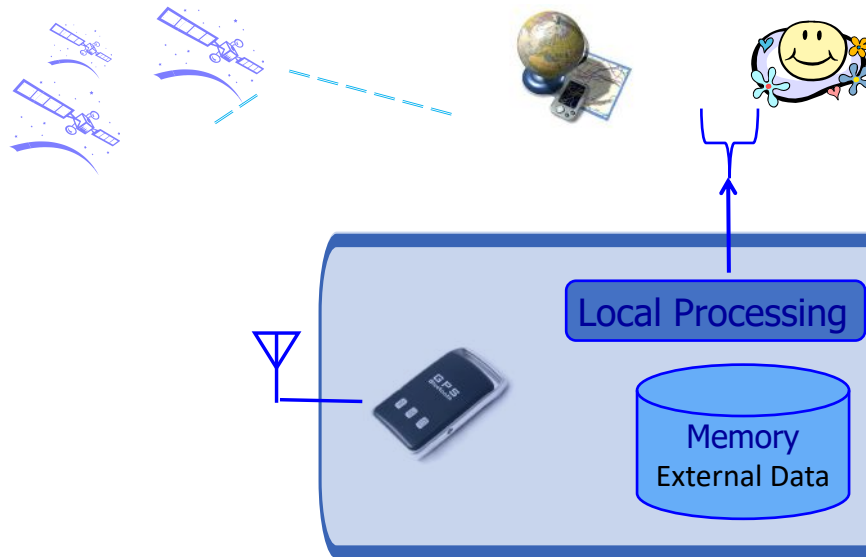
Defending GNSS-based positioning (cont'd)

- Approach 1
 - Detect attacks with tailored countermeasures
 - Develop defense mechanisms at the GNSS receiver
- Approach 2
 - Be attack-agnostic
 - Focus on the effect(s) of the attack: change of position or change of time
 - Use information beyond the GNSS receiver
 - In many cases, readily available
 - Develop defense mechanisms around the GNSS receiver

11

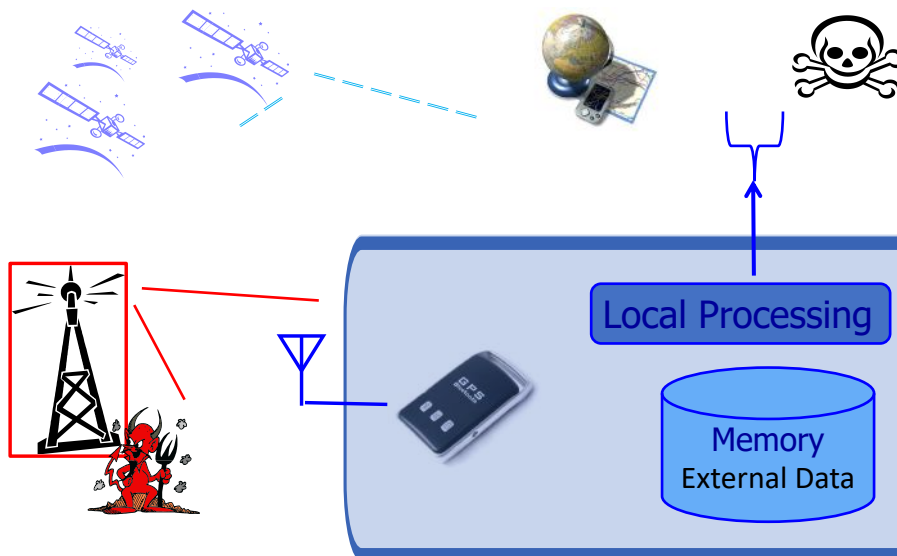
11

Defending GNSS-based positioning (cont'd)



12

Defending GNSS-based positioning (cont'd)



13

Defending GNSS-based positioning (cont'd)

Adversary

- Replay/relay attacks
- Distance decreasing attacks
- Spoofing attacks

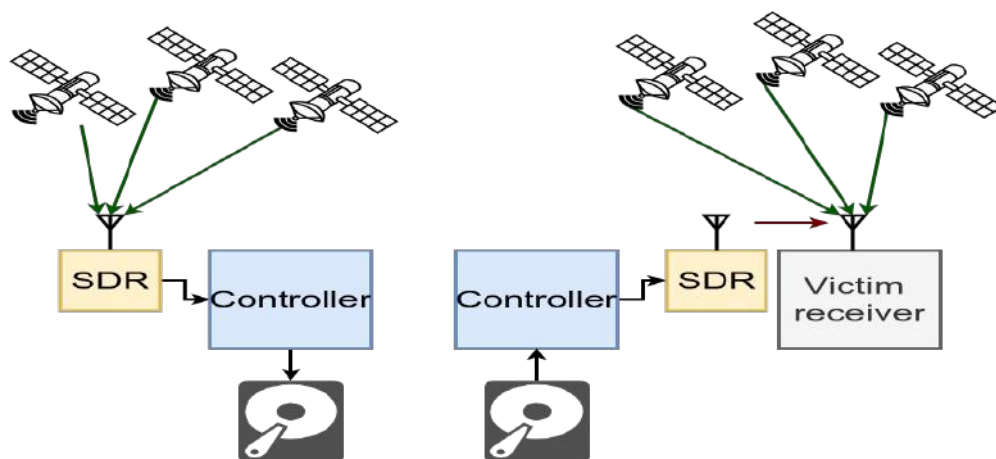
Defense mechanisms

- (approach 1) detect GNSS distance decreasing attacks
- (approach 2) use motion/position data to detect GNSS attacks
- (approach 2) use own/network time to detect GNSS attacks

14

14

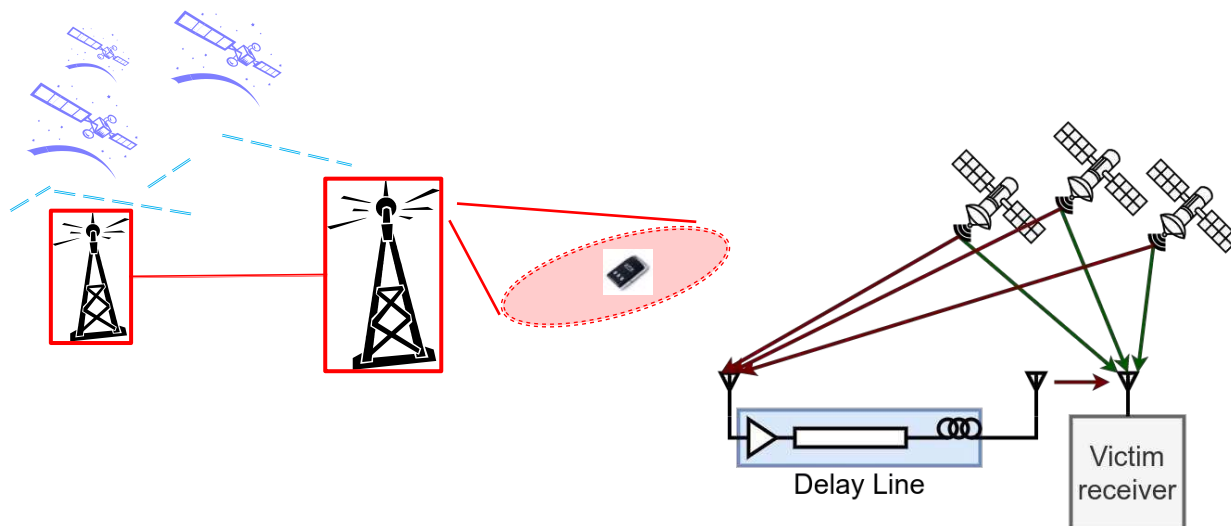
Attacking GNSS-based positioning (cont'd) Record and replay



15

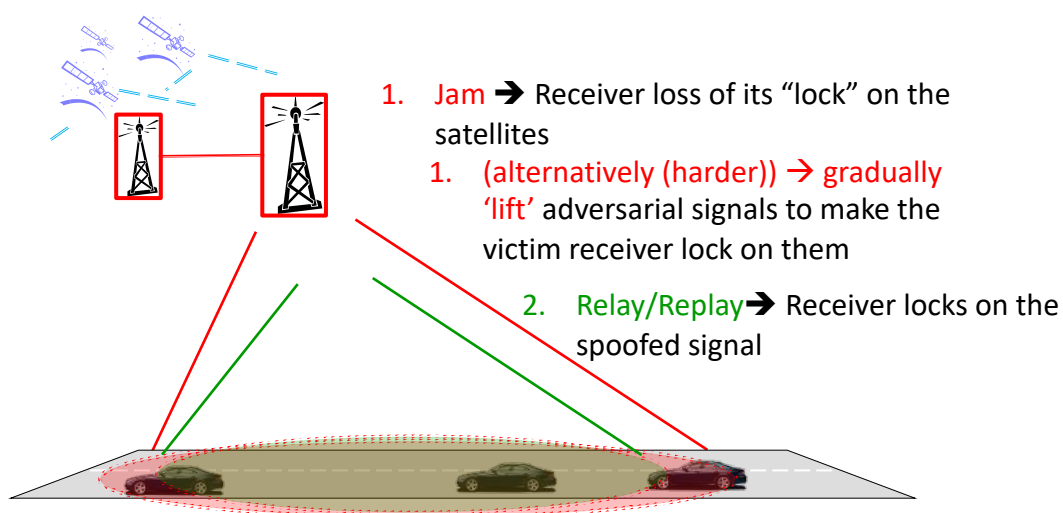
15

Attacking GNSS-based positioning (cont'd) Relay/Replay attacks (aka meaconing)



16

Attacking GNSS-based positioning (cont'd) 'Capturing' the victim receiver



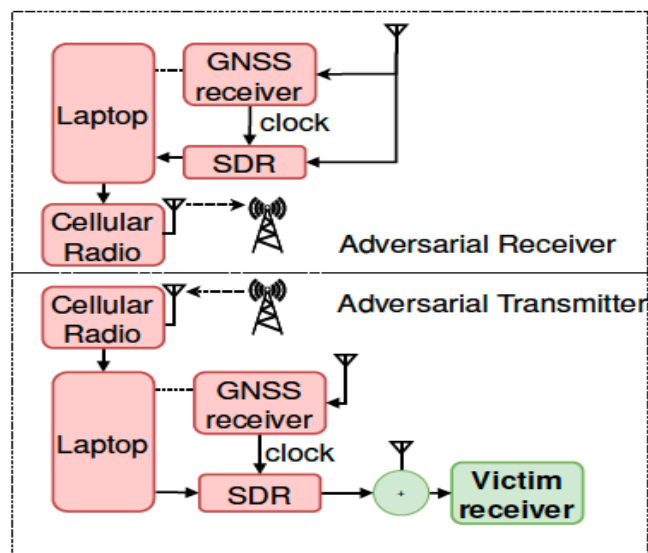
17

Attacking GNSS-based positioning (cont'd)

Practical relay/replay attackers

- Two colluding adversaries
- Off-the-shelf components
 - BladeRF 2.0 & LimeSDR
 - uBlox GNSS receivers
 - LTE cellular radio connection

[ACM WiSec 2021, ION ITM 2022]

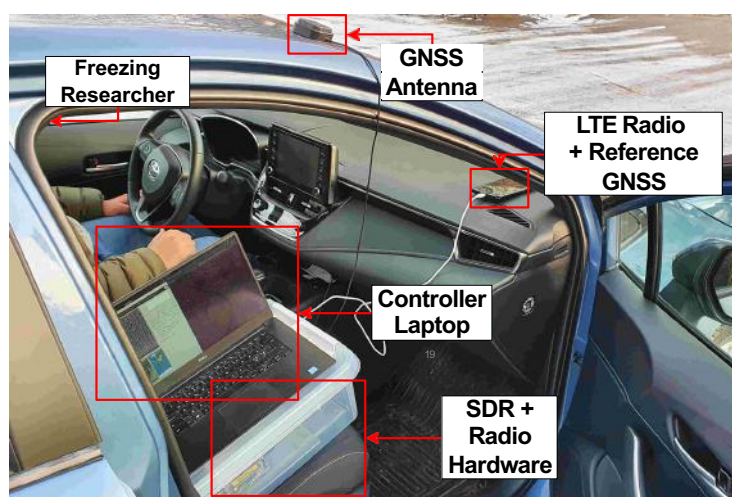


18

Attacking GNSS-based positioning (cont'd)

Practical relay/replay attackers

Receiver, mobile

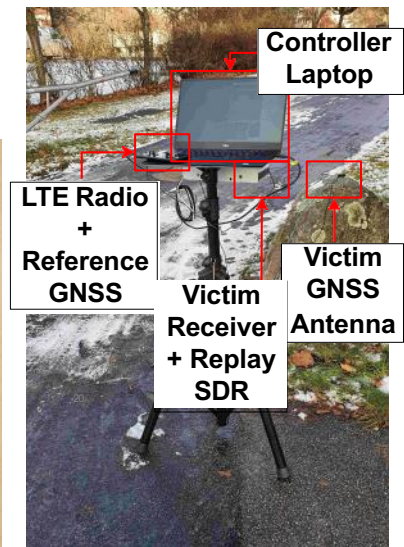


19

Attacking GNSS-based positioning (cont'd) Practical relay/replay attackers

Transmitter

- Connected to victim GNSS receiver
- Static

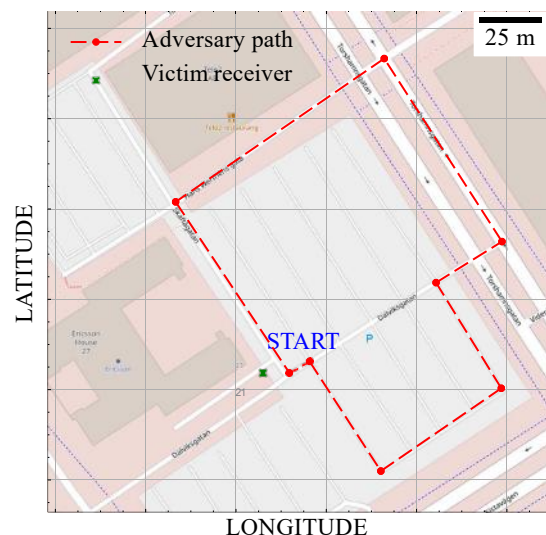


20

Attacking GNSS-based positioning (cont'd) Practical relay/replay attackers

Signal-level replay

- 1) Is LTE sufficient for signal-level replay?
- 2) Can we spoof with the attacker path and velocity?

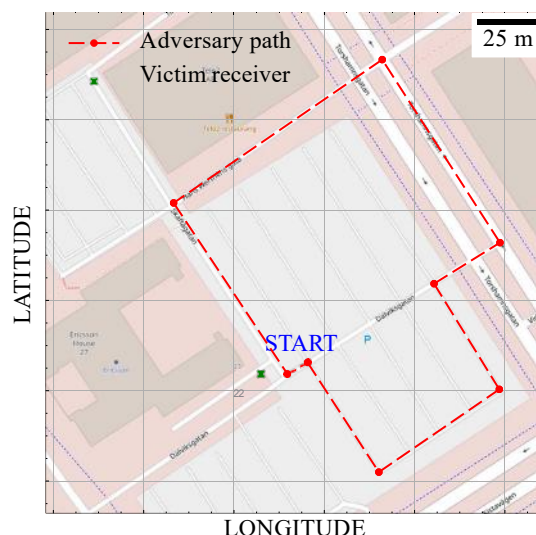


21

Attacking GNSS-based positioning (cont'd)

Practical relay/replay attackers

- 1) Cold start GNSS devices
- 2) Start satellite tracking, obtaining PVT fix
- 3) Attacker jams victim
- 4) Attacker starts replay & movement

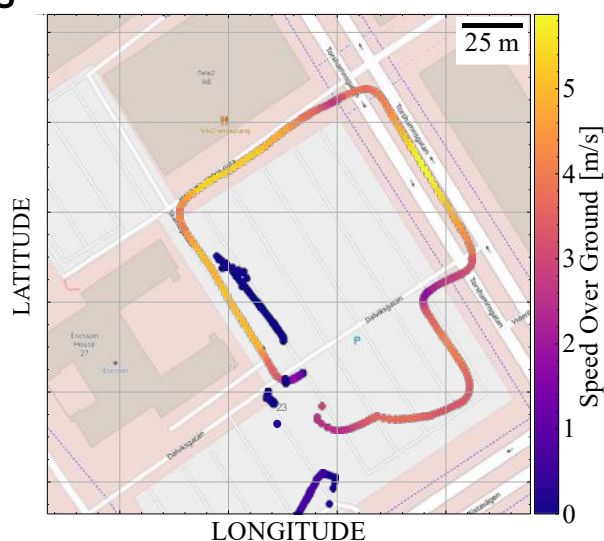


22

Attacking GNSS-based positioning (cont'd)

Practical relay/replay attackers

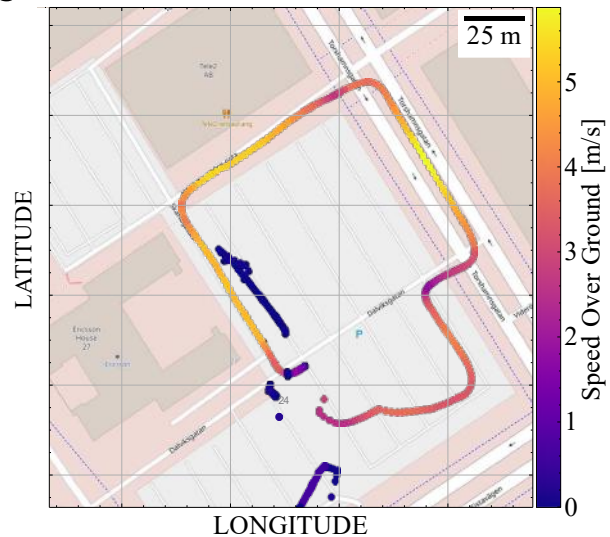
- ARX to ATX communication data rate approx. 3.8MB/s
- The victim follows the attacker path and velocity



23

Practical relay/replay attackers

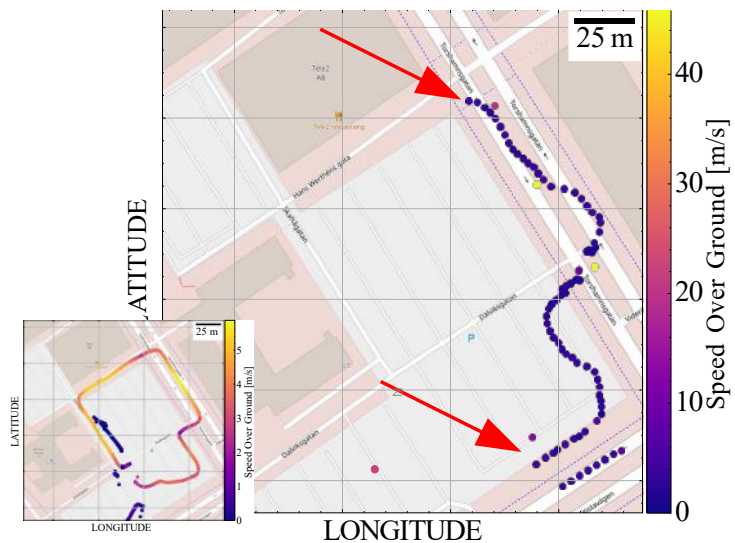
- What if ARX-ATX are connected with a low bandwidth link?
 - Data-rate reduction
 - Authentication-aware
 - Evaluate attack effectiveness & trade-offs



24




Practical relay/replay attackers

- What if ARX-ATX are connected with a low bandwidth link?
 - Extract signal parameters & authentication bits
 - Distribute to replaying node(s)
 - Re-generate GNSS signals
- Adversarial data rate: 15 KB/s



25

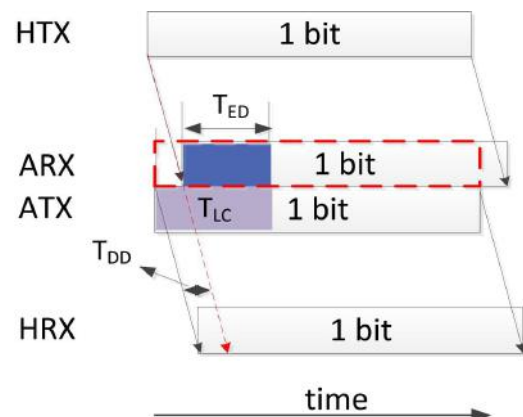
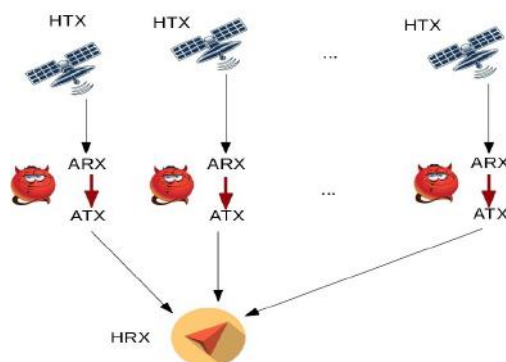
Attacking GNSS-based positioning (cont'd) Distance decreasing attacks

- Assume OOK:
 
- Early Detection* : an **adversarial receiver** does not wait for the end of the symbol
 
- Late Commit* : an **adversarial transmitter** can defer its signal transmission
 

26

26

Attacking GNSS-based positioning (cont'd) Distance decreasing attacks



- Each ARX-ATX pair represents one signal processing
- One transmitting antenna vs multiple transmitting antennas
- $T_{DD} = T_{LC} - T_{ED} - T_d$, where T_d is communication delay between ARX and ATX

27

27

Attacking GNSS-based positioning (cont'd)

Distance decreasing attacks

	Non-protection signals	NMA signals	Spreading-code encrypted signals					
Signals	GPS L1 C/A BeiDou B1I and B2I	Galileo E1 OS	GPS L1 P(Y) Code	GPS M-code	BeiDou B1Q	BeiDou B2Q	Galileo E1 PRS	Galileo E6
Target range	Integer multiple of spreading code length	Fraction of one spreading code length	Fraction of one spreading code chip length					
Level of T_{DD}	ms	ns to ms	Fraction of					
			$2\ \mu\text{s}$	195.5 ns	488.8 ns	97.8 ns	391 ns	195.5 ns
Shortened distance (pseudorange measurement)	$\geq 300\text{ km}$	meters to hundreds of km	meters to hundreds of km					

[IEEE ITM 2019]

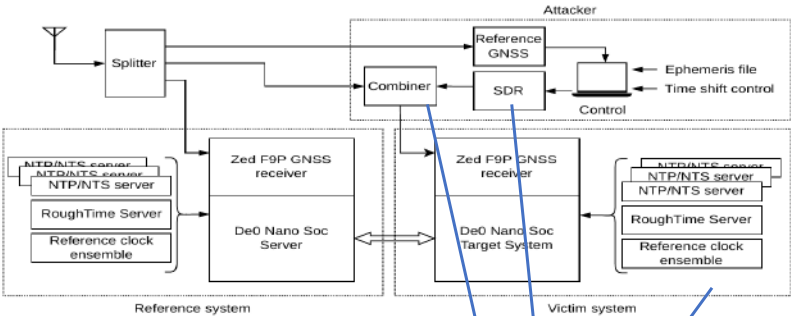
28

28

Attacking GNSS-based positioning (cont'd)

Spoofers

- Two DE0 Nano SOC computing nodes with ARM+FPGA
- Two uBlox ZED-F9P receivers
- USRP SDR (or any other SDR)
- Asynchronous simulation
- Synchronous simulation with reference receiver



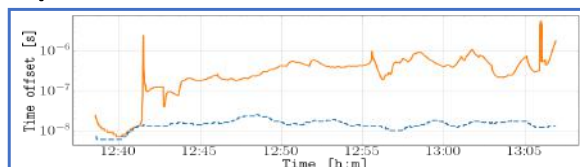
[IEEE/ION PLANS 2023]

9

29

Attacking GNSS-based positioning (cont'd)

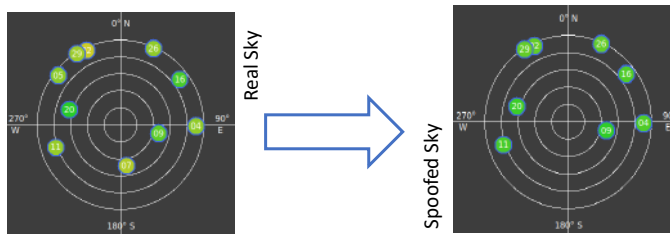
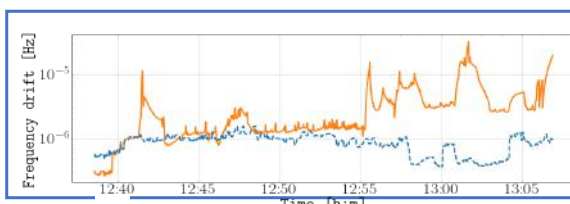
Spoofers



Synchronous lift-off attack: possible due to the precise frequency control during the attack. Effects still visible

We feed the legitimate sky-view to the spoofer to guarantee **coherent constellation maps**

Co-simulation step attack: discontinuity in the PVT solution, time skips forward or backwards



10

30

Defending GNSS-based positioning (cont'd)



A commercial off the shelf GNSS receiver



Embedded platform providing connectivity and computation



Set of local oscillators and a set of remote time providers



Inertial motion units (IMUs) (sensors)
Position estimation based on terrestrial networks

31

31

Defending GNSS-based positioning (cont'd) Position- and motion-based detection

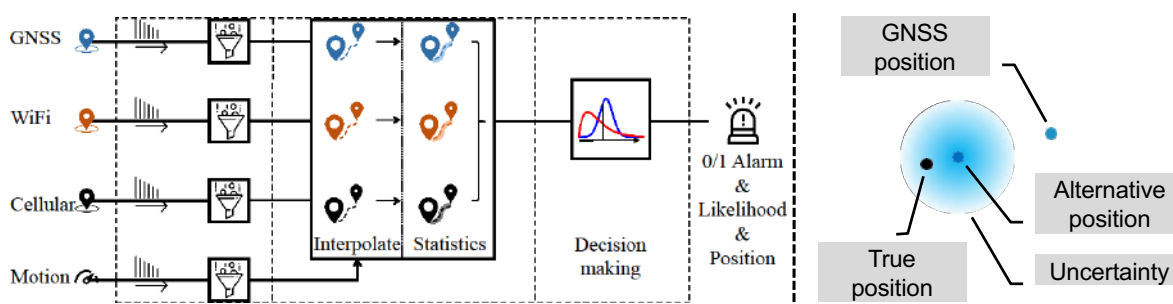
- IMUs accurate short-time; cumulative error
- Network localization is not accurate as GNSS
- Detection beyond a binary output
- Fuse heterogeneous data using model-based and -free methods
- Robust decision-making; a weighted integral form
- Opportunistic information: $\mathbf{p}_m(t)$, $\mathbf{v}(t)$, $\mathbf{a}(t)$, and $\boldsymbol{\omega}(t)$

[IEEE/ION PLANS 2023]

32

32

Defending GNSS-based positioning (cont'd) Position- and motion-based detection



- Interpolate: local polynomial regression (motion of receiver)
- Statistics: Gaussian process regression (statistics of locations)
- Decision: generalized likelihood ratio, combining all information

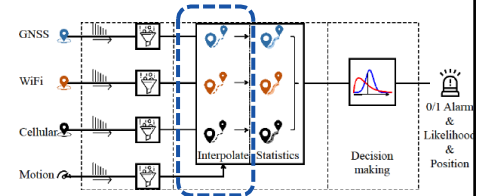
33

Defending GNSS-based positioning (cont'd)

Position- and motion-based detection

(1) Local polynomial regression

- Local polynomial, also known as moving regression
 - Fits data locally and uses a polynomial function
 - "Local" implemented by a kernel assigning weights



- Optimization problem:

minimize: the fitting error $\hat{\mathbf{p}}(t) - \mathbf{p}(t)$

such that: movement satisfies $\mathbf{v}(t), \mathbf{a}(t), \boldsymbol{\omega}(t)$



- Convex problem, it can be solved in polynomial time (real-time)

34

34

Defending GNSS-based positioning (cont'd)

Position- and motion-based detection

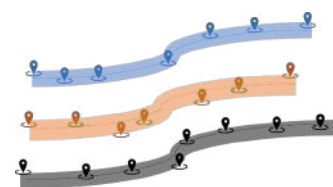
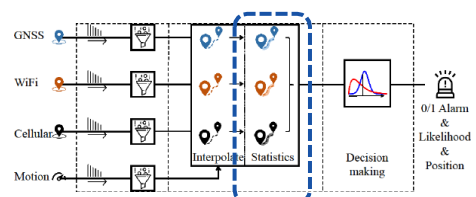
(2) Gaussian process regression

- Models the residual part $\mathbf{x}(t)$ of estimated positions
- $\mathbf{x}(t)$: difference between interpolated and measured positions

$$\mathbf{x}(t) = \hat{\mathbf{p}}(t) - \mathbf{p}(t)$$

characterized as Gaussian.

- Finally, by combining the $\mathbf{x}(t)$ and previous local polynomial results, we get confidence intervals



35

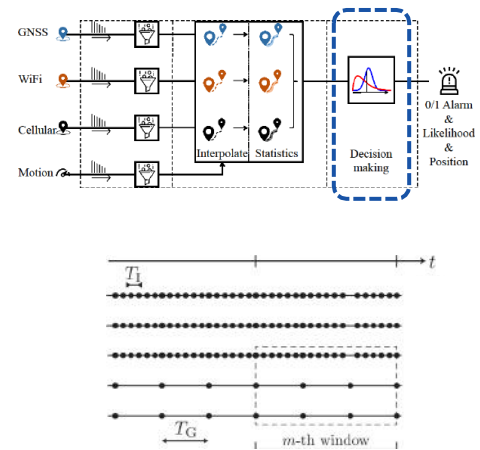
35

Defending GNSS-based positioning (cont'd)

Position- and motion-based detection

(3) Decision making based on confidence intervals

- Cross time perspective
 - Combine probability space of confidence intervals from time $t - w$ to t , where w is window size
- Cross information sources perspective
 - Multiply probability density functions of confidence intervals from different sources at time t
- Neyman-Pearson lemma
 - Fix false alert rate, optimize and compare true positive rate
 - False alert rate $\frac{\text{false positive detection}}{\text{number of real negative}}$



36

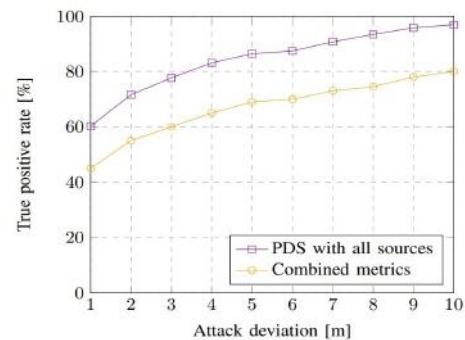
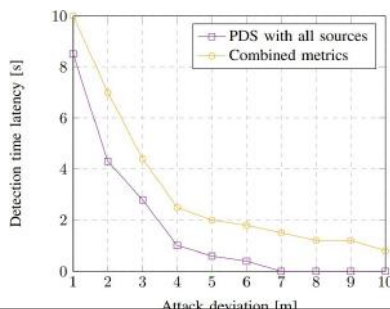
36

Defending GNSS-based positioning (cont'd)

Position- and motion-based detection

Some simulation results

- Network locations + on-board sensor data
- Up to 20% performance gain
- Up to 97% true positive rate (false alarm=0.05)

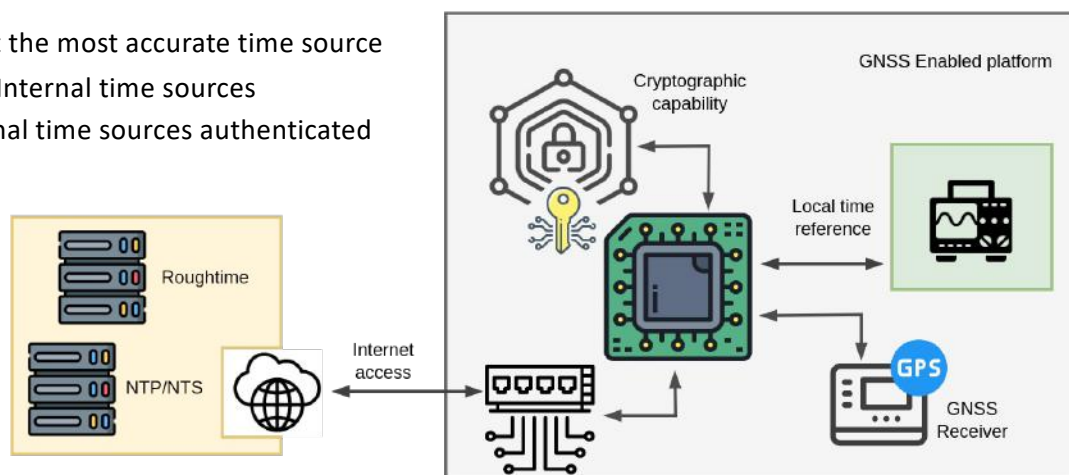


- 1-2 second lower detection latency
- Stable performance for large attack induced deviation

37

Defending GNSS-based positioning (cont'd) Time-based detection

- Select the most accurate time source
- Trust Internal time sources
- External time sources authenticated



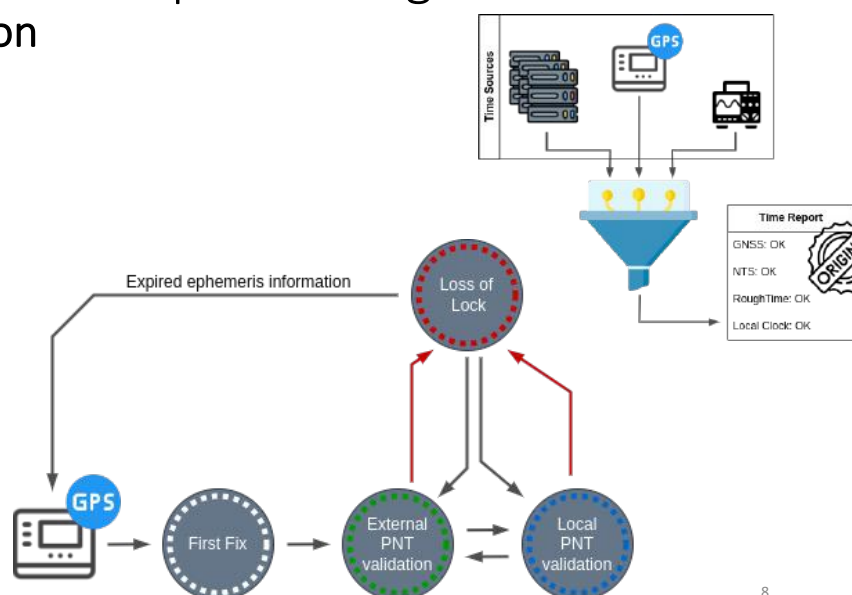
[IEEE/ION PLANS 2023, 2020; IEEE GNSS+ 2020, 2019]

6

38

Defending GNSS-based positioning (cont'd) Time-based detection

- Receiver state: cold/warm start
- Progressive refinement of time solution and its trustworthiness
- Best effort in terms of connectivity
- Continuous monitoring of the time solution
 - At each PNT update
 - Rate dependant on the application



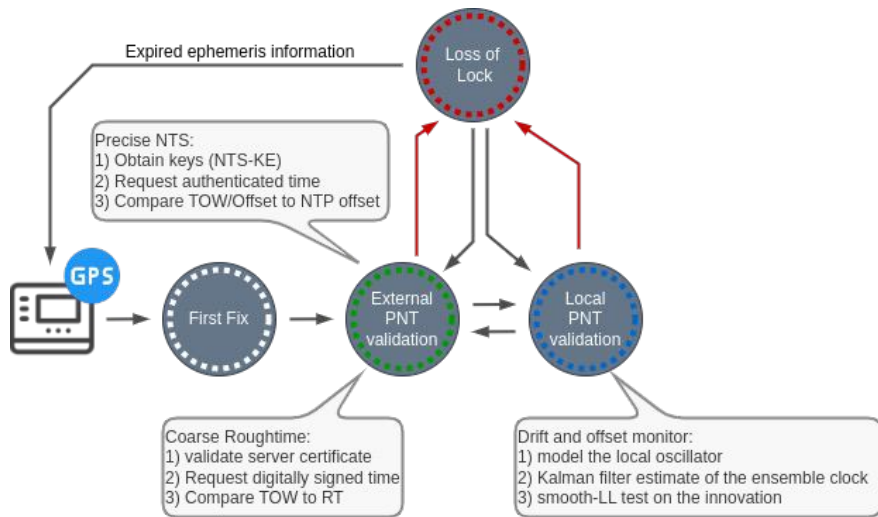
8

39

Defending GNSS-based positioning (cont'd)

Time-based detection

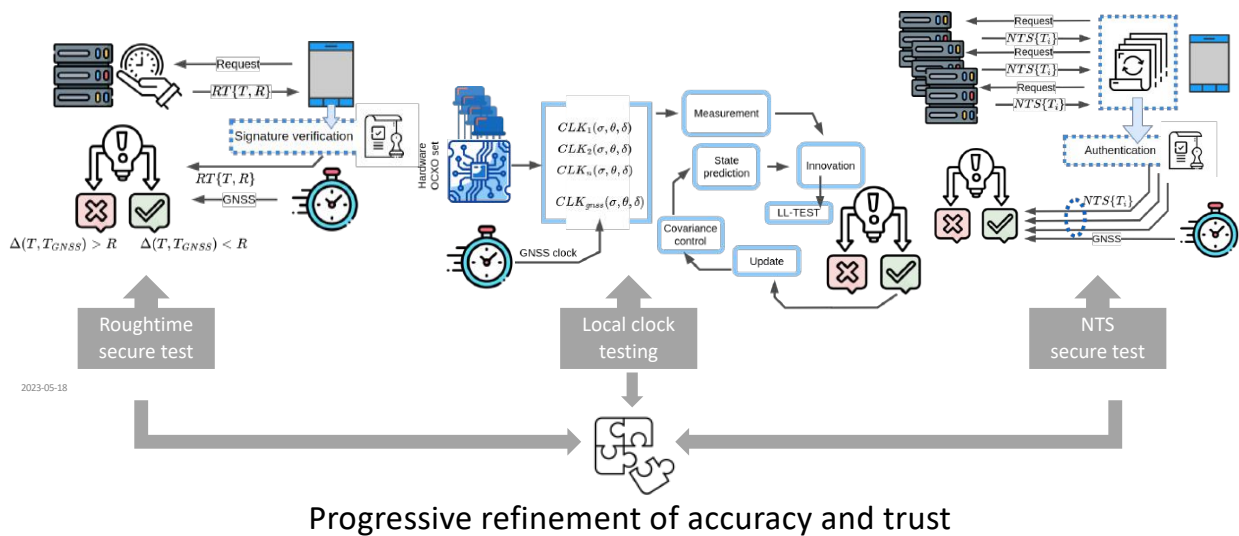
- Receiver state: cold/warm start
- Progressive refinement of time solution and its trustworthiness
- Best effort in terms of connectivity
- Continuous monitoring of time solution
 - At each PNT update
 - Rate dependant on the application



40

Defending GNSS-based positioning (cont'd)

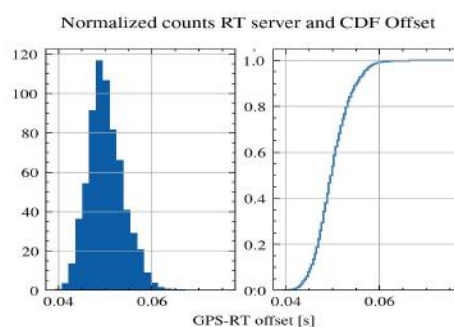
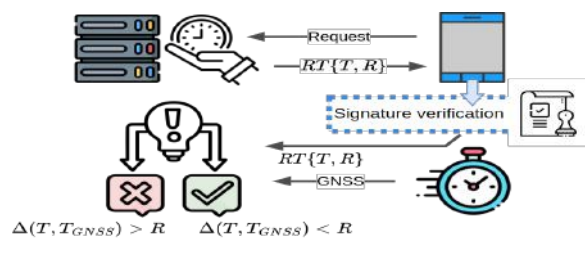
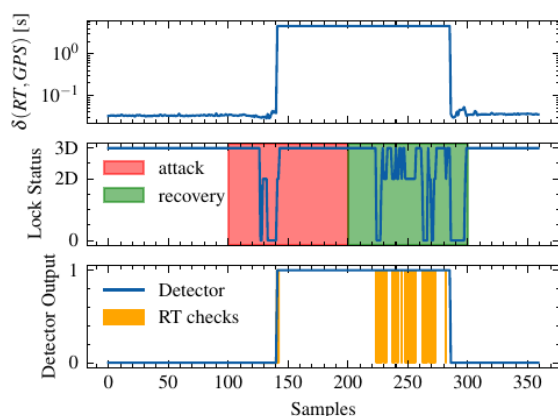
Time-based detection



41

Defending GNSS-based positioning (cont'd) Time-based detection

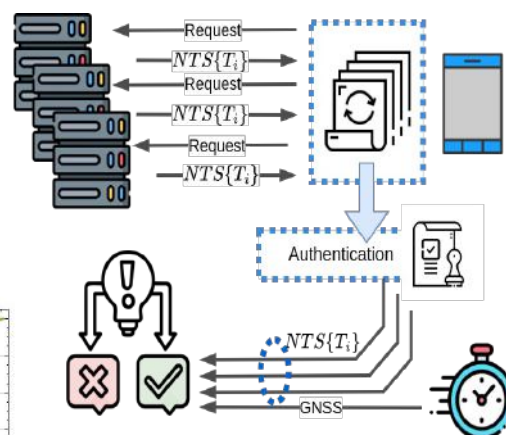
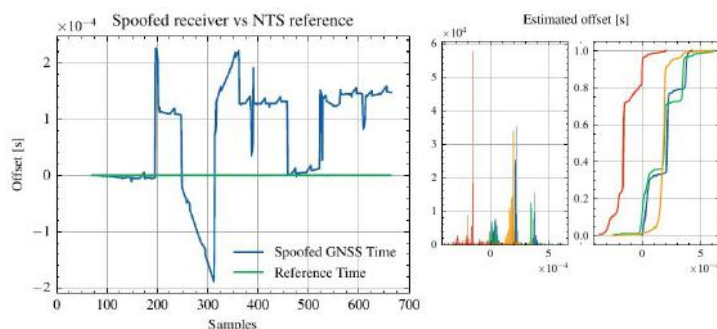
- Using Roughtime
 - Non repudiable time (multi-peer)
 - Disadvantage: (Very) Coarse



42

Defending GNSS-based positioning (cont'd) Time-based detection

- Using Network Time Security (NTS)
 - Multiple options
 - Requires connectivity
 - Latency sensitive



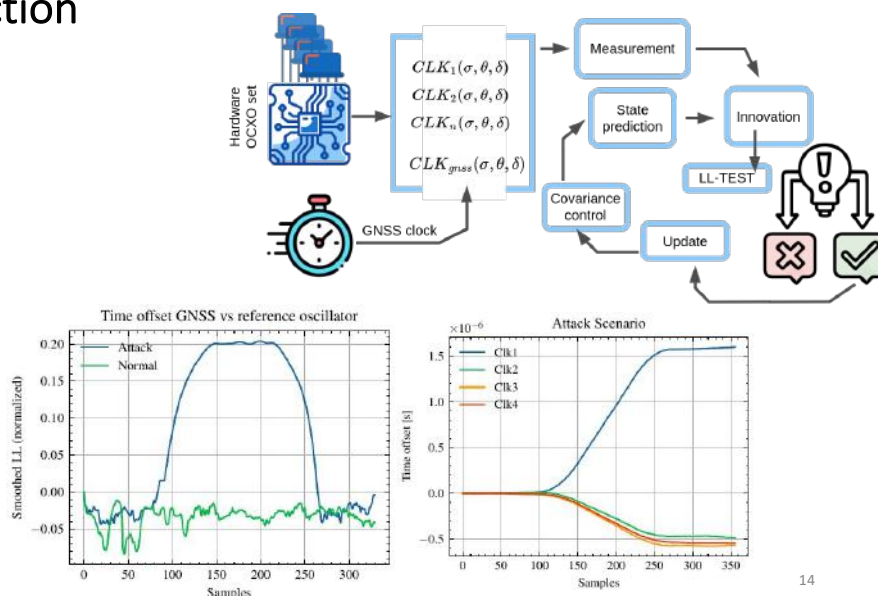
13

43

Defending GNSS-based positioning (cont'd)

Time-based detection

- Local clock (OCXOs) ensemble tracking
- Continuous monitoring
- Independent of connectivity
- Disadvantage
 - Additional hardware
 - No absolute time check
 - Periodic re-sync

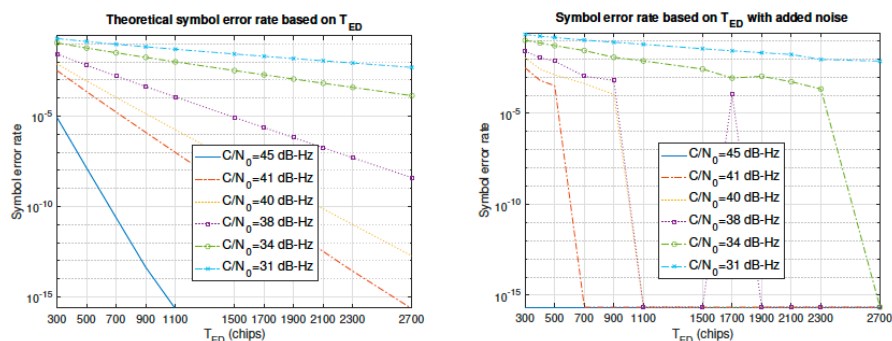


44

Defending GNSS-based positioning (cont'd)

Detecting distance decreasing attacks

- $T_b = 4092$ chips (4 ms)
- Recorded Galileo E1 OS signals: $C/N_0 = 45$ dB-Hz



[IEEE TAES 2022]

45

45

Defending GNSS-based positioning (cont'd) Detecting distance decreasing attacks

The transmitted signals from the ATX:

$$S_{ATX}(t) = \begin{cases} A_1 f_1(t, f_{Doppler}, b_{pre}) & 0 \leq t \leq T_{LC} \\ A_2 f_2(t, f_{Doppler}, \tilde{b}) & T_{LC} < t \leq T_b \end{cases}$$

- \tilde{b} is estimation value from ARX, and b_{pre} is adversary-chosen value that may use:
 - ✓ a fixed value
 - ✓ same as last bit value
 - ✓ prediction based on convolutional coding and interleaving
- $A_1 T_{LC} < A_2 (T_b - T_{LC})$

[IEEE TAES 2022]

46

46

Defending GNSS-based positioning (cont'd) Detecting distance decreasing attacks

- Legitimate signals → accumulator output at I arm:

$$I_P^0[n] = \sum_{i=0}^{T_{int} f_s} x_{I_P, i}^0 = \sqrt{\frac{P}{2}} f_s T_{int} b[n] + N_0[n] = Eb[n] + N_0[n]$$

where T_{int} is integration period, $E = \sqrt{\frac{P}{2}} f_s T_{int}$.

- DD signals → accumulator output at I arm:

$$I_P^{DD}[n] = \sum_{i=0}^{T_{int} f_s} x_{I_P, i}^{DD} = b_{pre}[n] E \frac{T_{LC}}{T_{int}} + b[n] A E \frac{T_{int} - T_{LC}}{T_{int}} + N_0[n]$$

where b_{pre} is adversary-chosen value during T_{LC} period.

[IEEE TAES 2022]

47

47

Defending GNSS-based positioning (cont'd) Detecting distance decreasing attacks

- Without knowledge, i.e., within-symbol transition, of DD signals

$$\begin{cases} \text{Null hypothesis:} & I_P \sim N(\mu_0, \sigma^2) \\ \text{Alternative hypothesis:} & I_P \sim N(\mu_0, \sigma^2) \end{cases}$$

- ✓ GoF test: Shapiro-Wilk test

- With the knowledge of DD signals

$$\begin{cases} \text{Null hypothesis:} & I_P \sim N(\mu_0, \sigma_0^2) \\ \text{Alternative hypothesis:} & I_P \sim \sum_{i=1}^K \phi_i N(\mu_i, \sigma_i^2) \end{cases}$$

- ✓ Generalized Likelihood Ratio Test (GLRT) —
Expectation-Maximization (EM) algorithm for Gaussian Mixture I (GMM)

[IEEE TAES 2022]

48

48

Defending GNSS-based positioning (cont'd) Detecting distance decreasing attacks

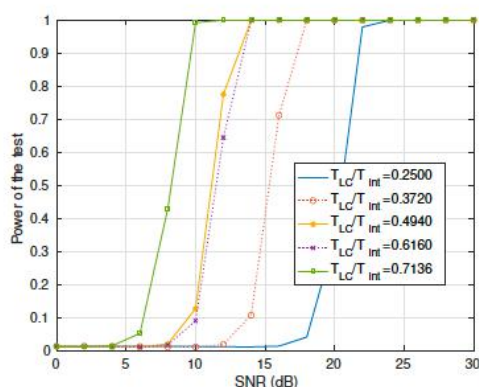


Figure: Shapiro-Wilk test.

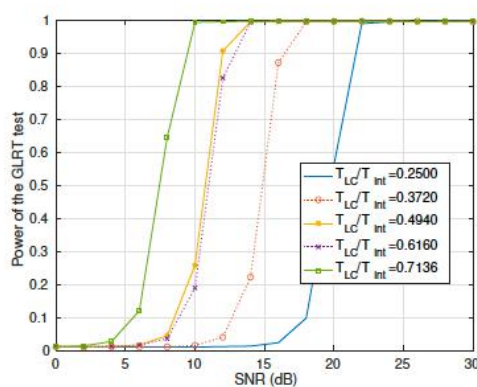


Figure: GLRT test.

49

49

References

- Wenjie Liu and Panos Papadimitratos, "[Probabilistic Detection of GNSS Spoofing using Opportunistic Information](#)," IEEE/ION Position Location and Navigation Symposium (IEEE/ION PLANS), April 2023
- Marco Spanghero and Panos Papadimitratos, "[Detecting GNSS misbehavior leveraging secure heterogeneous time sources](#)," IEEE/ION Position Location and Navigation Symposium (IEEE/ION PLANS), April 2023
- K. Zhang, E. Larsson, and P. Papadimitratos, "[Protecting GNSS Open Service Navigation Message Authentication Against Distance-Decreasing Attacks](#)," IEEE Transactions on Aerospace and Electronic Systems (IEEE TAES), vol. 58, no. 2, pp. 1224-1240, 2022
- M. Spanghero, and P. Papadimitratos, "[High-precision Hardware Oscillators Ensemble for GNSS Attack Detection](#)," IEEE Aerospace Conference, Big Sky, MT, USA, March 2022

50

50

References

- M. Lenhart, M. Spanghero, and P. Papadimitratos, "Distributed and Mobile Message Level Relaying/Replaying of GNSS Signals," *International Technical Meeting of The Institute of Navigation (ITM)*, Long Beach, CA, USA, pp. 56-57, January 2022
- Z. Gülgün, E. Larsson, and P. Papadimitratos, "Multiple Spoofers Detection for Mobile GNSS Receivers Using Statistical Tests," *IEEE Access*, vol. 9, pp. 166382-166394, 2021
- M. Spanghero, K. Zhang, and P. Papadimitratos, "Authenticated time for detecting GNSS attacks," *33rd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+)*, Virtual, pp. 3826-3834, September 2020
- K. Zhang, M. Spanghero, and P. Papadimitratos, "Protecting GNSS-based Services using Time Offset Validation," *IEEE/ION Position, Location and Navigation Symposium (PLANS)*, Portland, Oregon, pp. 575-583, April 2020
- K. Zhang, and P. Papadimitratos, "Safeguarding NMA Enhanced Galileo OS Signals from Distance-Decreasing Attacks," *International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019)*, Miami, FL, USA, pp. 4041-4052, September 2019

51

51

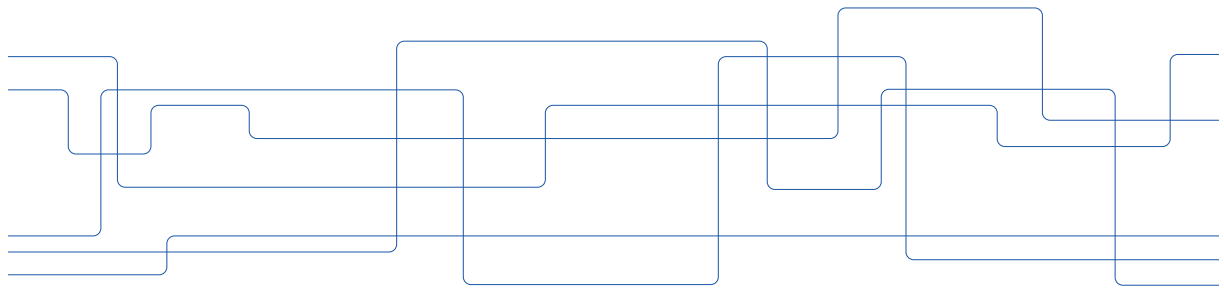


KTH ROYAL INSTITUTE
OF TECHNOLOGY

Securing location and **reducing device exposure**

Panos Papadimitratos

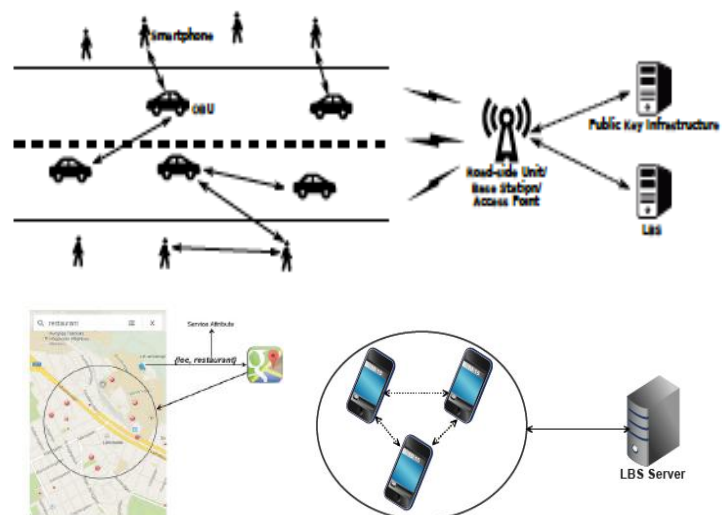
www.eecs.kth.se/nss



52

Location Privacy

- Secure and Privacy-Preserving Location Based Services (LBS)
 - Challenges
 - Honest-but-curious service providers
 - Malicious users/peers
 - Solution
 - Peer-to-peer operation
 - Privacy; reduced exposure to LBS servers and peers
 - Security
 - Efficiency

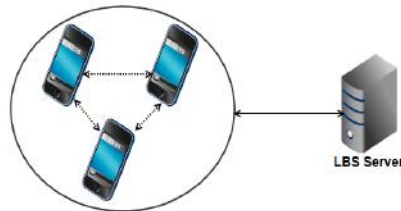


[ACM WiSec 2017, NordSec 2015, [IEEE TDSC 2014](#), [ACM TOPS 2019](#)]

53

53

Decentralized location privacy and security



- *Misbehaving peers?*
 - *Active*: Masquerading, tampering, DoS...
 - *Passive*: Eavesdrop queries and responses
 - Accountability
 - Privacy protection
-
- No need for an anonymizer: reliance on peers
 - Cache responses, contact the LBS server only when absolutely necessary

* *Hiding in the Mobile Crowd: Location Privacy through Collaboration*,
IEEE TDSC, 2014

◀ ▶ ⏪ ⏩ 🔍 ↺

54

54

Decentralized location privacy and security (cont'd)

- The PCA randomly assigns a small fraction of system nodes as serving nodes
- The serving period can be coincide with pseudonym request interval
- Serving nodes proactive request Point of Interest (PoI) data for the whole region and announce their presence and available data
- Any interested node listens to beacons and requests PoI data
- Can request responses from $N > 1$ serving nodes for cross-checking

* *Resilient Privacy Protection for Location-Based Services through Decentralization*,
ACM TOPS, 2019

◀ ▶

55

55

Quantitative analysis

$$ExpoDeg(Id_{LTC}, C) = \sum_{Id_i \in ID(Id_{LTC}, C)} \frac{T(Id_i)}{T(Id_{LTC})} * \frac{R_H(Id_i)}{R(Id_{LTC})} \quad (1)$$

- $ID(Id_{LTC}, C)$: set of identities corresponding to Id_{LTC} exposed to honest-but-curious (possibly colluding) entities
- $T(Id)$: trip duration of a node under identity Id
- $R(Id)$: number of regions the node visits as Id
- $R_H(Id)$: number of visited regions exposed
- $ExpoDeg$: accuracy of reconstructed node trajectories based on recorded node queries, taking into account pseudonymous authentication

56

56

Quantitative analysis (cont'd)

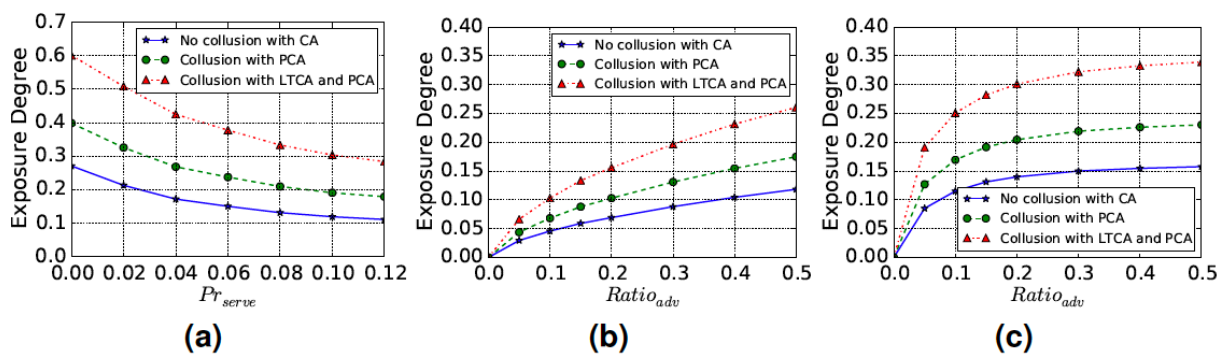


Figure: (a) Exposure degree to the LBS server as a function of Pr_{serve} . Exposure degree to colluding passive adversaries as a function of $Ratio_{adv}$ (b) with and (c) without encryption for P2P communication.

57

57

Quantitative analysis (cont'd)

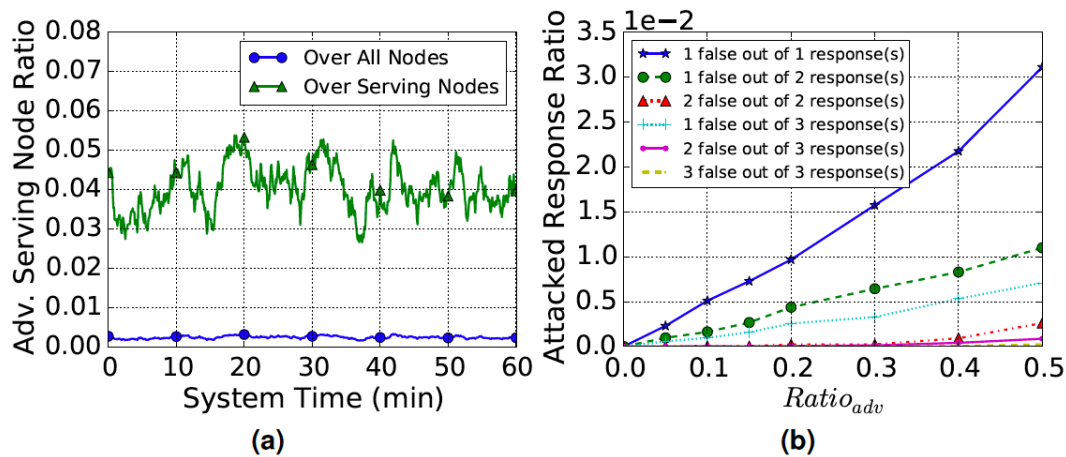


Figure: (a) Malicious serving node ratio during simulation (1 p.m. - 2 p.m.) with default settings. (b) Attacked LBS query ratio as a function of $Ratio_{adv}$.

58

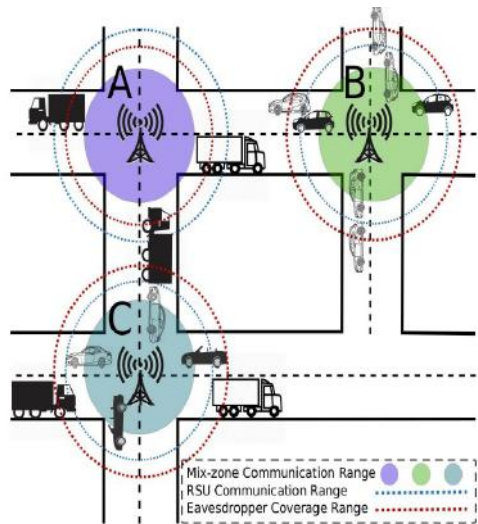


Fig. 2. Mix-zone construction with decoy traffic.

Cooperative Location Privacy in Vehicular Networks: Why Simple Mix Zones Are Not Enough

Mohammad Khodaei¹, Member, IEEE, and Panos Papadimitratos², Fellow, IEEE

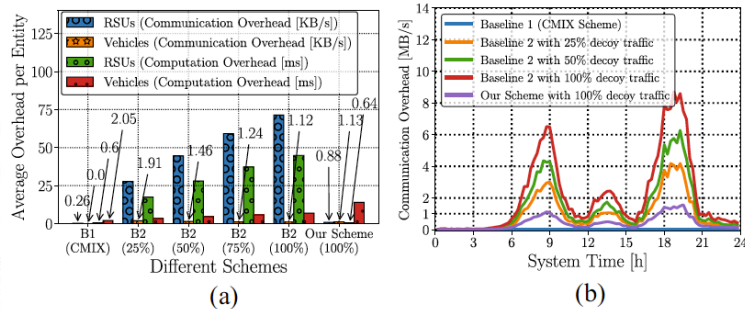


Fig. 8. Comparison among CMIX (B1) [37], chaff-based CMIX (B2) [42], and our scheme: 1K chaff pseudonyms in a CF with $\rho = 10^{-25}$; beacon frequency: $\gamma_{mz} = 0.5$, $\gamma_v = 0.2$. (a) Computation and communication overheads. (b) Communication overhead, averaged every 300 s.

59

References

- H. Jin, and P. Papadimitratos, "[Resilient Privacy Protection for Location-Based Services Through Decentralization](#)," *ACM Transactions on Privacy and Security (ACM TOPS)*, vol. 22, no. 4, pp. 21:1-36, September 2019
- M. Khodaei, and P. Papadimitratos, "[Cooperative Location Privacy in Vehicular Networks: Why Simple Mix-zones are not Enough](#)," *IEEE Internet Of Things Journal*, vol. 8, no. 10, pp. 7985-8004, May 2021
- R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J. Hubaux, "Hiding in the Mobile Crowd: Location Privacy through Collaboration," *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, vol. 11, no. 3, pp. 266-279, May 2014

60

60

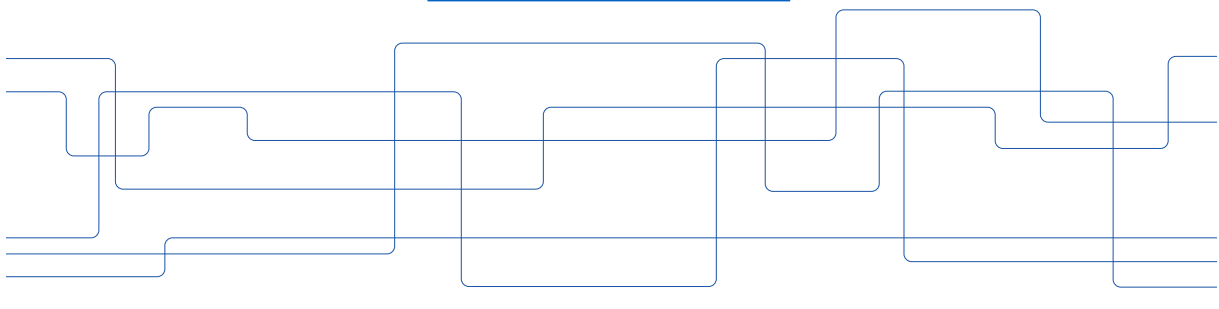


KTH ROYAL INSTITUTE
OF TECHNOLOGY

Securing location and reducing device exposure

Panos Papadimitratos

www.eecs.kth.se/nss



61