Beek en Donk
Oirschot
Best
Helmond
Nuenen
Mierlo
Eindhoven
Geldrop
Waalre
Heeze
Hapert
Eersel
Valkenswaard
Leende
Bergeijk
Maarheeze
Budel
Hamont-Achel
Lommel
Pelt
Hamburg
Groningen
Bremen
Amsterdam
Hanover
Bielefeld
Netherlands
Rotterdam
Essen
Antwerp
Brussels
Cologne
Germany
Lille
Liège
Belgium
Frankfurt
Luxembourg
Mannheim
Paris
Karlsruhe
Stuttgart
Strasbourg
Recklinghausen
Waltrop
Lünen
Castrop-Rauxel
Herne
Gelsenkirchen
Dortmund
Bochum
Witten
Schwerte
Hattingen
Herdecke
Wetter
Sprockhövel
Hagen
Gevelsberg

Amplifying Threats: The Role of Multi-Sender Coordination in SMS-Timing-Based Location Inference Attacks

Evangelos Bitsikas, Theodor Schnitzler, Christina Pöpper, Aanjhan Ranganathan

USENIX WOOT Conference on Offensive Technologies
Philadelphia, PA, USA
August 12, 2024

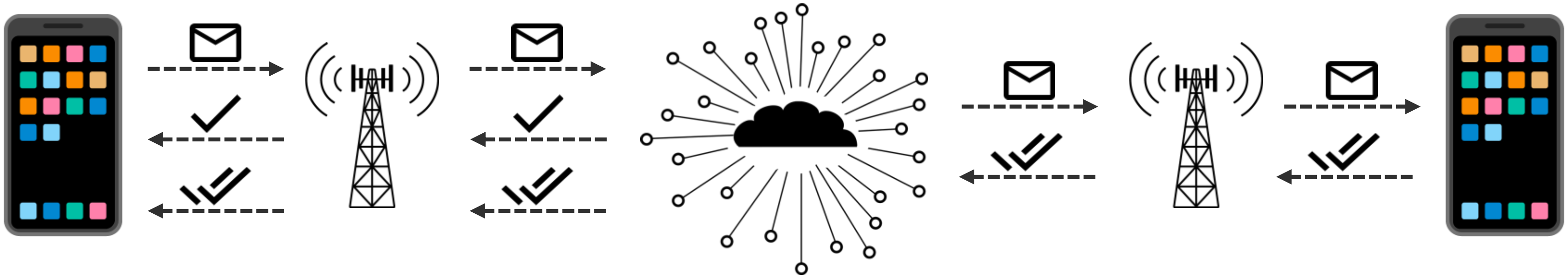
Maastricht University
Department of Advanced Computing Sciences

Northeastern University

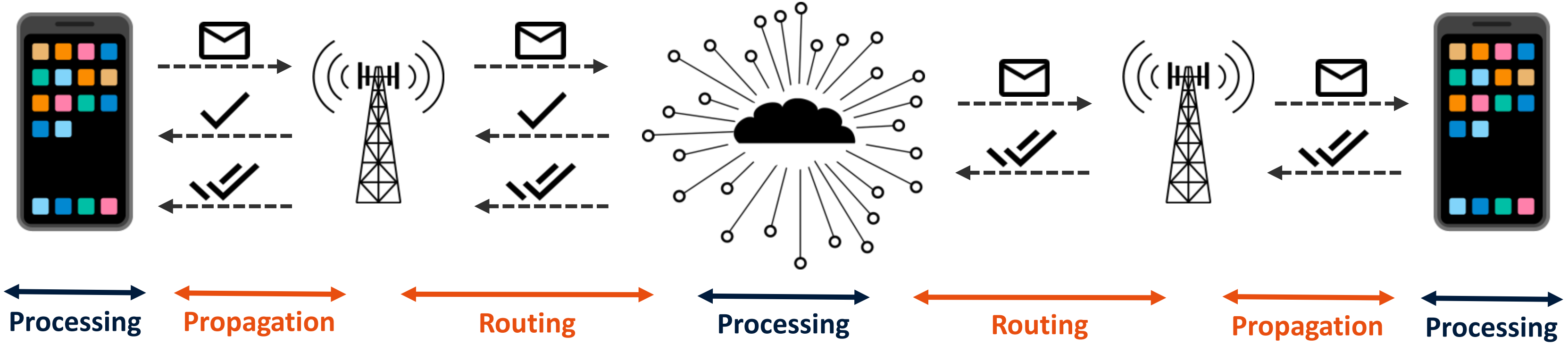
جامعة نيويورك أبوظبي
NYU ABU DHABI

CENTER FOR TRUSTWORTHY DATA SCIENCE AND SECURITY
UA RUHR RESEARCH ALLIANCE

Problem Statement



Problem Statement



Processing · Propagation · Routing · Processing · Routing · Propagation · Processing

Sender: *Philadelphia*

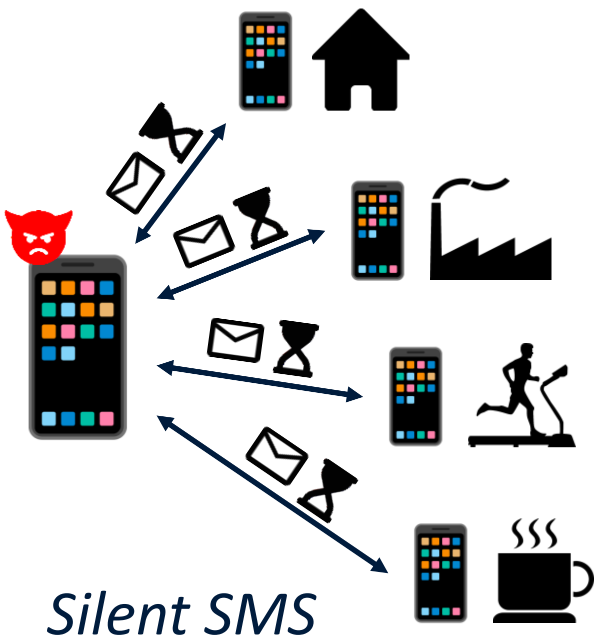
c = 299 792 458 m/s

Receiver:	$2 * \ dist_{e2e}$	$RTT \ \ (v_{Internet} = \frac{2}{3}c)$
Boston	≥ 870 km	≥ 4.35 ms
Maastricht	≥ 12 200 km	≥ 61.04 ms

Timing Side Channel for Location Inference

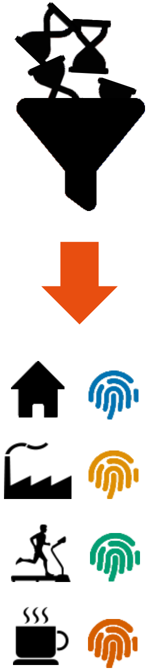
SMS-based Location Inference

(1) Data Collection

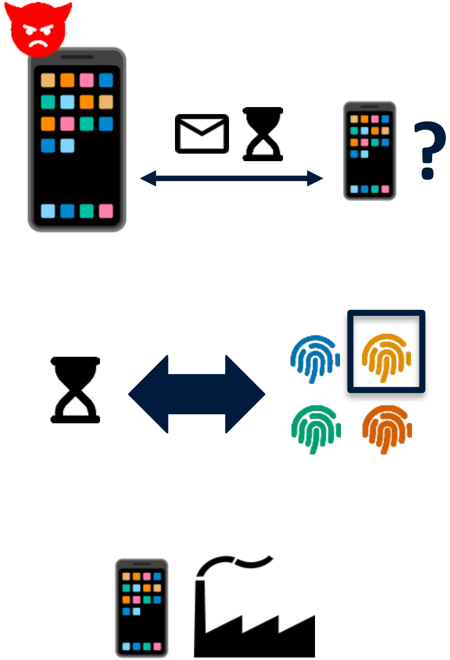


Silent SMS

(2) Evaluation

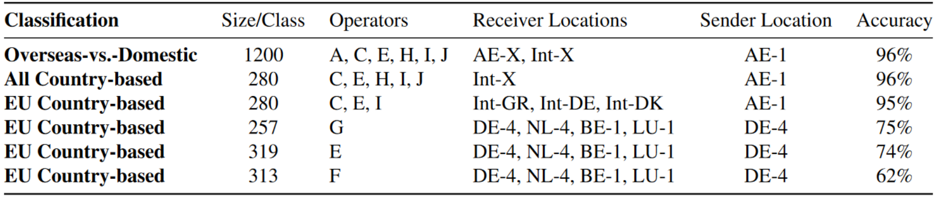


(3) Location Inference

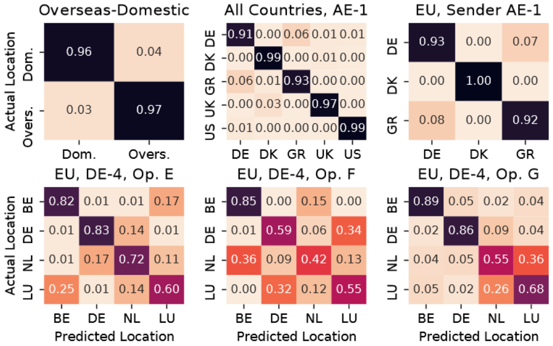


SMS-based Location Inference

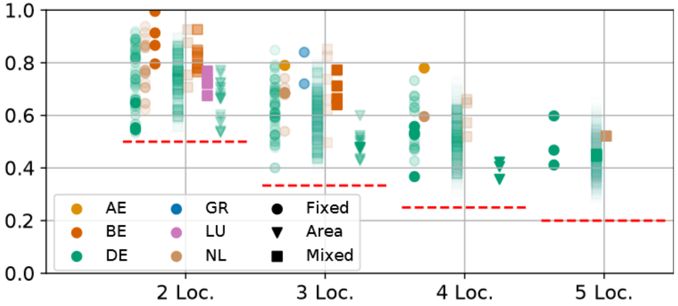
Locations in different countries



Classification	Size/Class	Operators	Receiver Locations	Sender Location	Accuracy
Overseas-vs.-Domestic	1200	A, C, E, H, I, J	AE-X, Int-X	AE-1	96%
All Country-based	280	C, E, H, I, J	Int-X	AE-1	96%
EU Country-based	280	C, E, I	Int-GR, Int-DE, Int-DK	AE-1	95%
EU Country-based	257	G	DE-4, NL-4, BE-1, LU-1	DE-4	75%
EU Country-based	319	E	DE-4, NL-4, BE-1, LU-1	DE-4	74%
EU Country-based	313	F	DE-4, NL-4, BE-1, LU-1	DE-4	62%

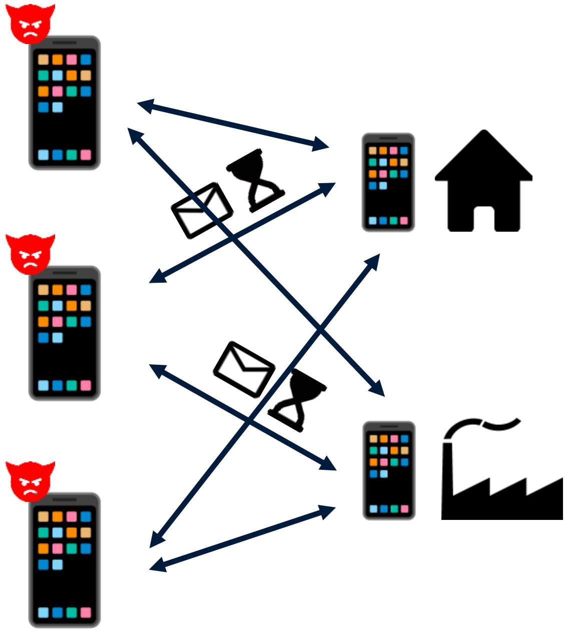


Locations within the same country



Bitsikas et al.:
Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings

Contributions of This Paper



The Role of Multi-Sender Coordination

How does controlling multiple senders

in different positions

affect the attacker‘s capabilities

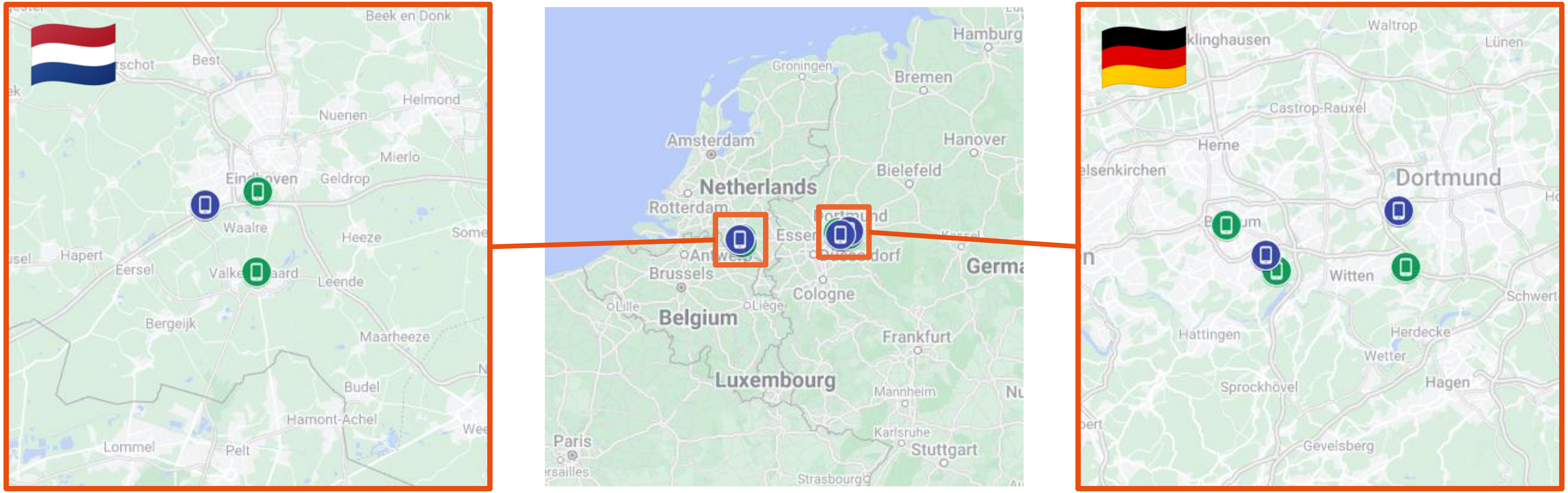
to infer the receiver‘s location?

Experimental Setup: Locations

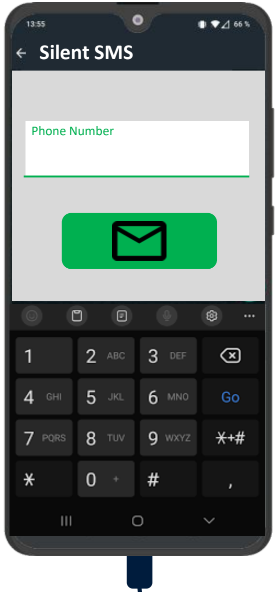
Sender: **V**eldhoven
3 Receiver Locations

2 Clusters
approx. 130km apart

Senders: **B**ochum, **D**ortmund
5 Receiver Locations



Data Collection



ADB-USB
Android Debug Bridge

Sending SMS

1 fixed sending device per location

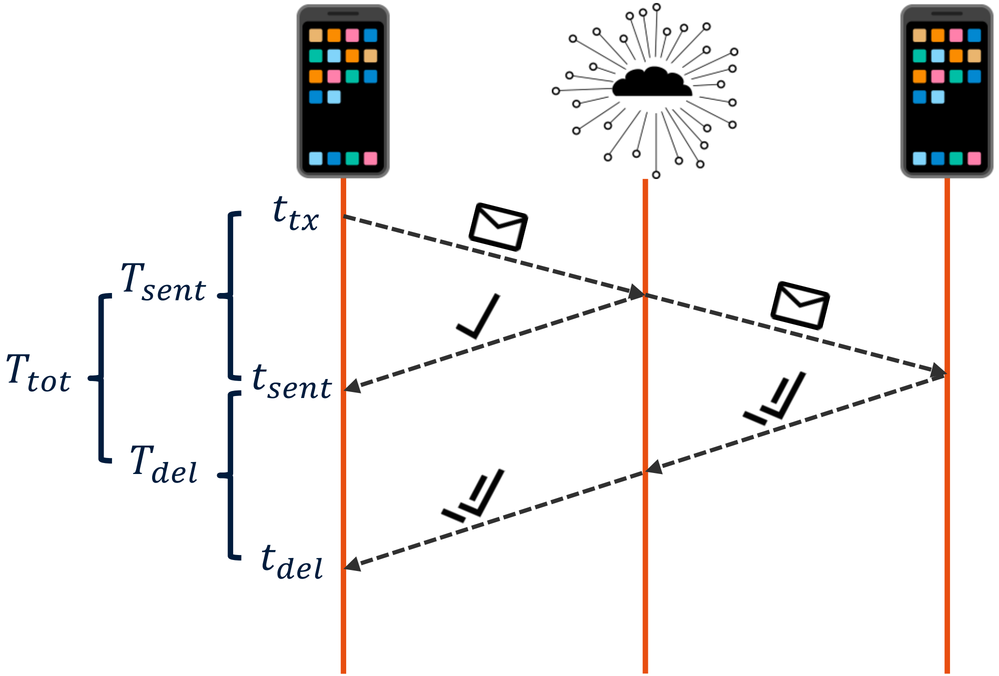
- Iterate through receivers
  - Send 20 SMS
  - Wait for sent + delivery reports
  - Store timings
- Hourly repeated
  - hh:00 to Rec. 1, hh:15 to Rec. 2, …
  - Best-effort syncing (local clocks)
- Σ 262.980 SMS

Receiving SMS

	PX6a	HuaP8	A53	OP7P
NL-1	✓	✓	✓	
NL-2	✓	✓	✓	✓
NL-3	✓	✓	✓	✓
DE-1	✓	✓		✓
DE-2	✓	✓		
DE-3	✓	✓	✓	✓
DE-4	✓	✓		
DE-5	✓	✓		

Maastricht University

Timing Features



Single-sender features

- Durations ($T_{sent}, T_{del}, T_{tot}$)
- Ratio T_{del} / T_{tot}
- Relative timing difference for two consecutive SMS

➔ *baseline from previous paper*

Multi-sender features

- Mean, median, stddev of **pairs** of senders of **5** consecutive SMS

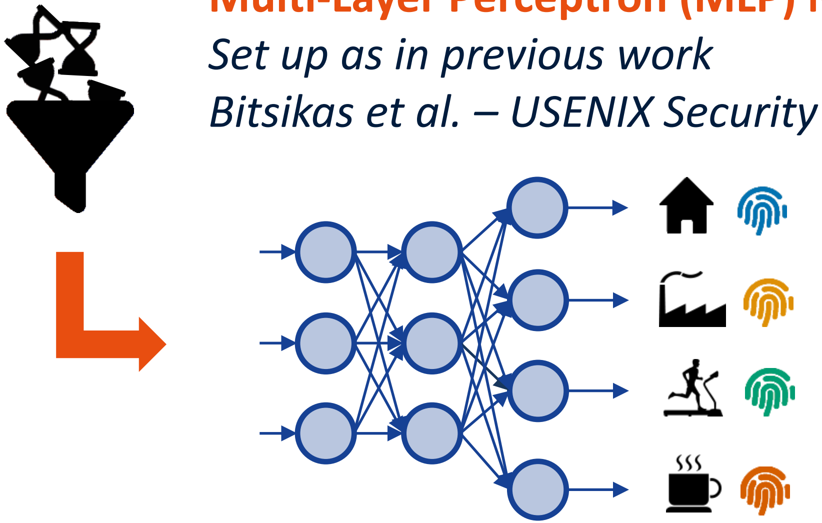
➔ *9 additional features*

Maastricht University

Location Inference Evaluation

Multi-Layer Perceptron (MLP) NN

Set up as in previous work
Bitsikas et al. – USENIX Security 2023



Classifications

- All possible combinations of *n* receiving locations
- *n = {2,3,4}*

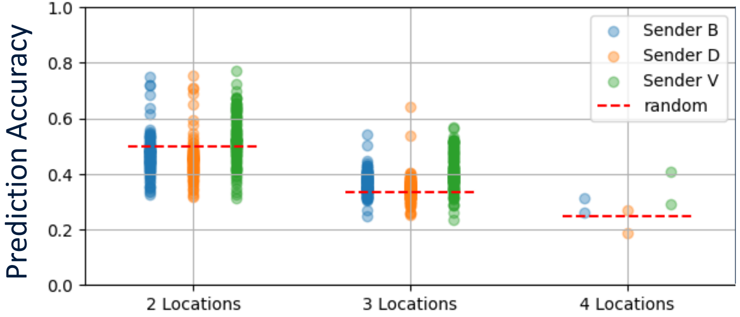
Focus on Accuracy

Share of samples that are classified correctly

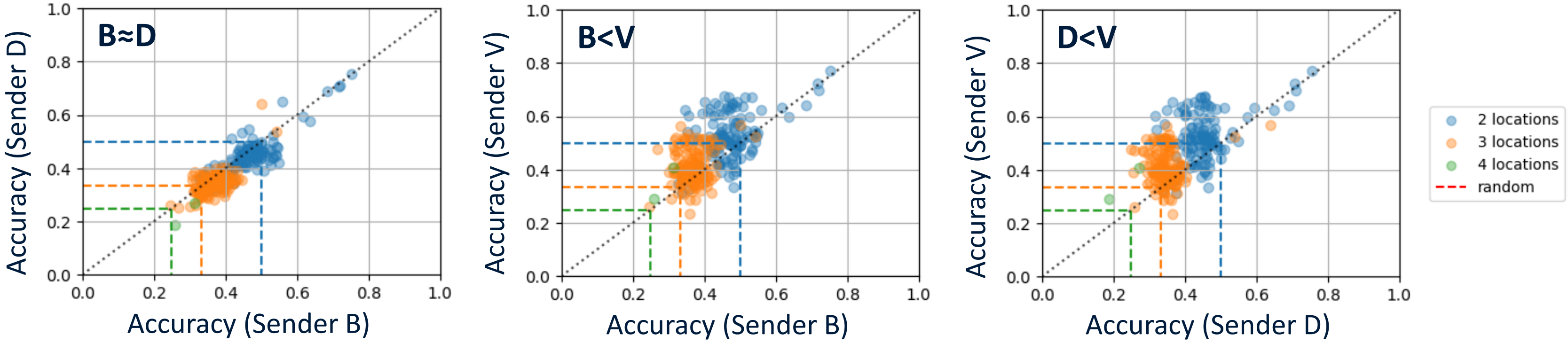
Consistency Across Senders

Compare prediction accuracy
between senders
by number of receiver locations

Overall



Pair-wise



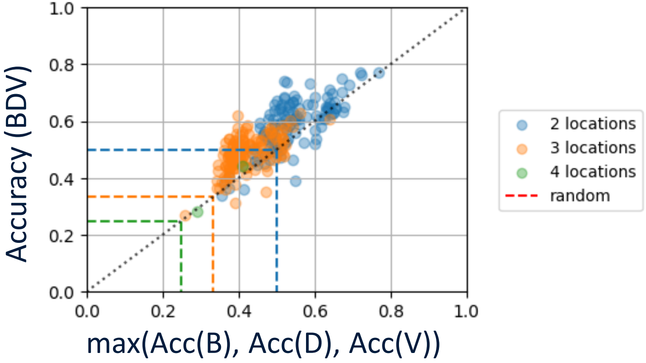
Maastricht University

Combining Senders

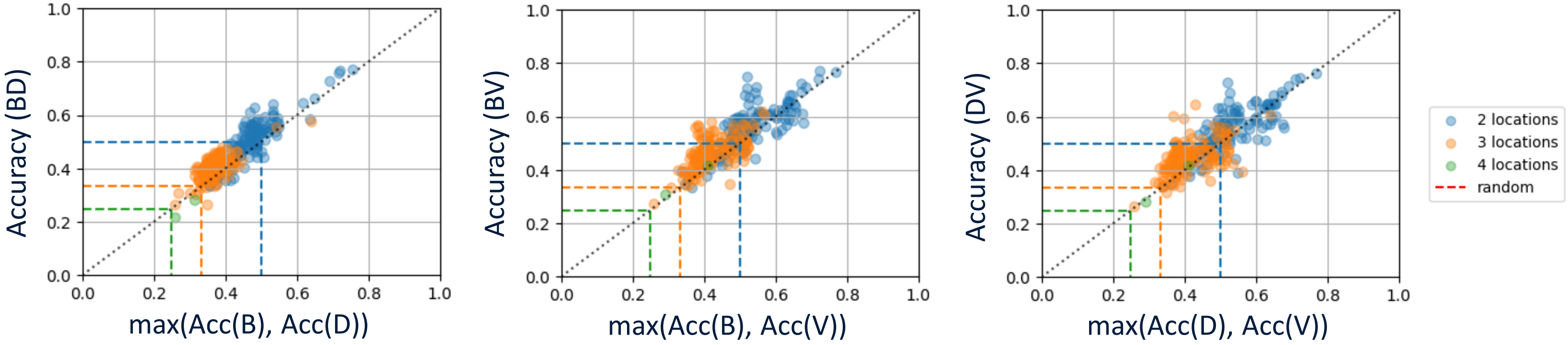
Combine timings from multiple senders and compare with maximum accuracy achieved by single sender

(single-sender features only)

All 3 Senders



Pair-wise



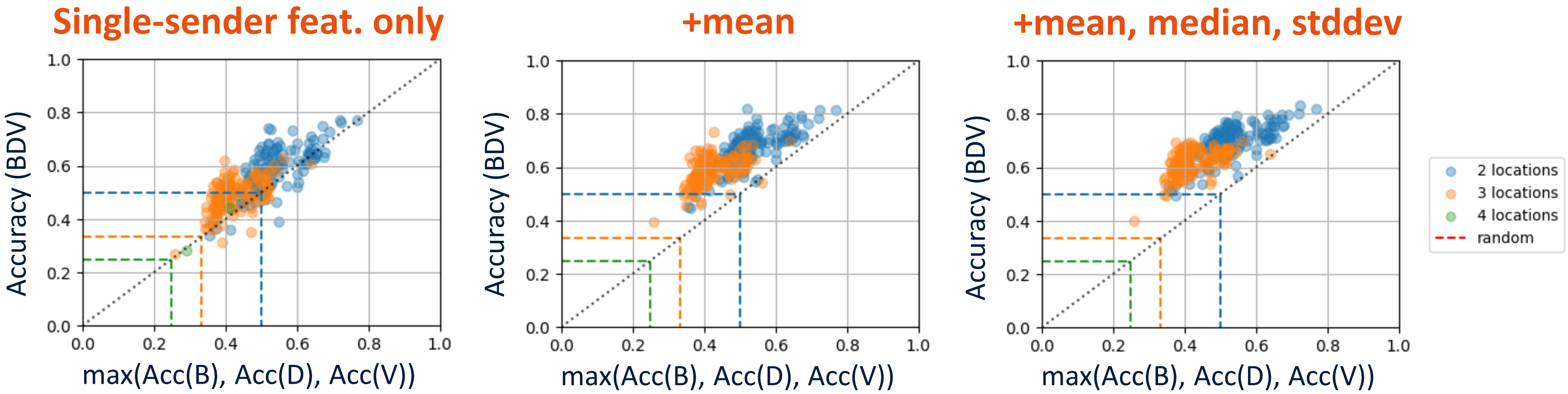
Adding Multi-sender Features

Combine timings from multiple senders and compare with maximum accuracy achieved by single sender

*(**with multi-sender features**)*

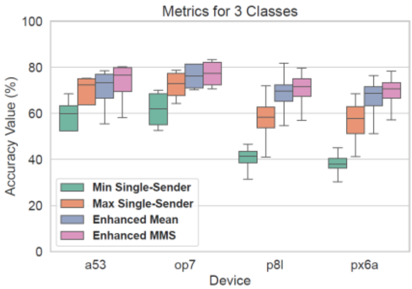
Multi-sender features

Mean, median, stddev
of **pairs** of senders
of **5** consecutive SMS

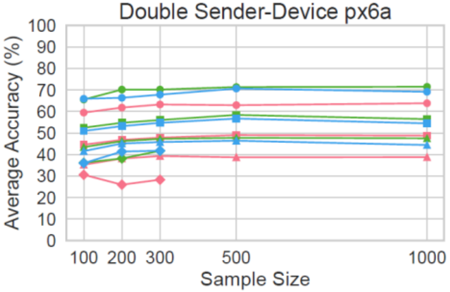


In the Paper

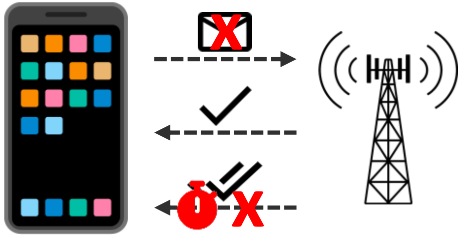
Per-device Analyses



Sample Sizes



Countermeasures



Network operator level only

Maastricht University
Department of Advanced Computing Sciences

Northeastern University

جامعة نيويورك أبوظبي
NYU ABU DHABI

CENTER FOR TRUSTWORTHY DATA SCIENCE AND SECURITY
UA RUHR | RESEARCH ALLIANCE

Amplifying Threats: The Role of Multi-Sender Coordination in SMS-Timing-Based Location Inference Attacks

USENIX WOOT Wonference on Offensive Technologies
Philadelphia, PA, USA
August 12, 2024

Key Takeaways

- Stealthy and targeted attack
- Technically easy (send SMS) but operationally difficult (send **many** SMS)
- Operating multiple senders can improve SMS-based location inference

Paper

Code & Data (Github)

USENIX Security 2023
Freaky Leaky SMS: Extracting User Locations by Analyzing SMS Timings

NDSS 2023
Hope of Delivery: Extracting User Locations From Mobile Instant Messengers

Theodor Schnitzler
theodor.schnitzler@maastrichtuniversity.nl
@the0retisch