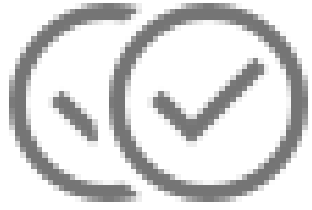


Signal Metadata: Episode II

The Receipts Strike Back

Justin Tracey

April 10, 2023

Hope of Delivery: Extracting User Locations From Mobile Instant Messengers

Theodor Schnitzler[1,2], Katharina Kohls[3], Evangelos Bitsikas[4,5], Christina Pöpper[5]

NDSS 2023

https://arxiv.org/abs/2210.10523

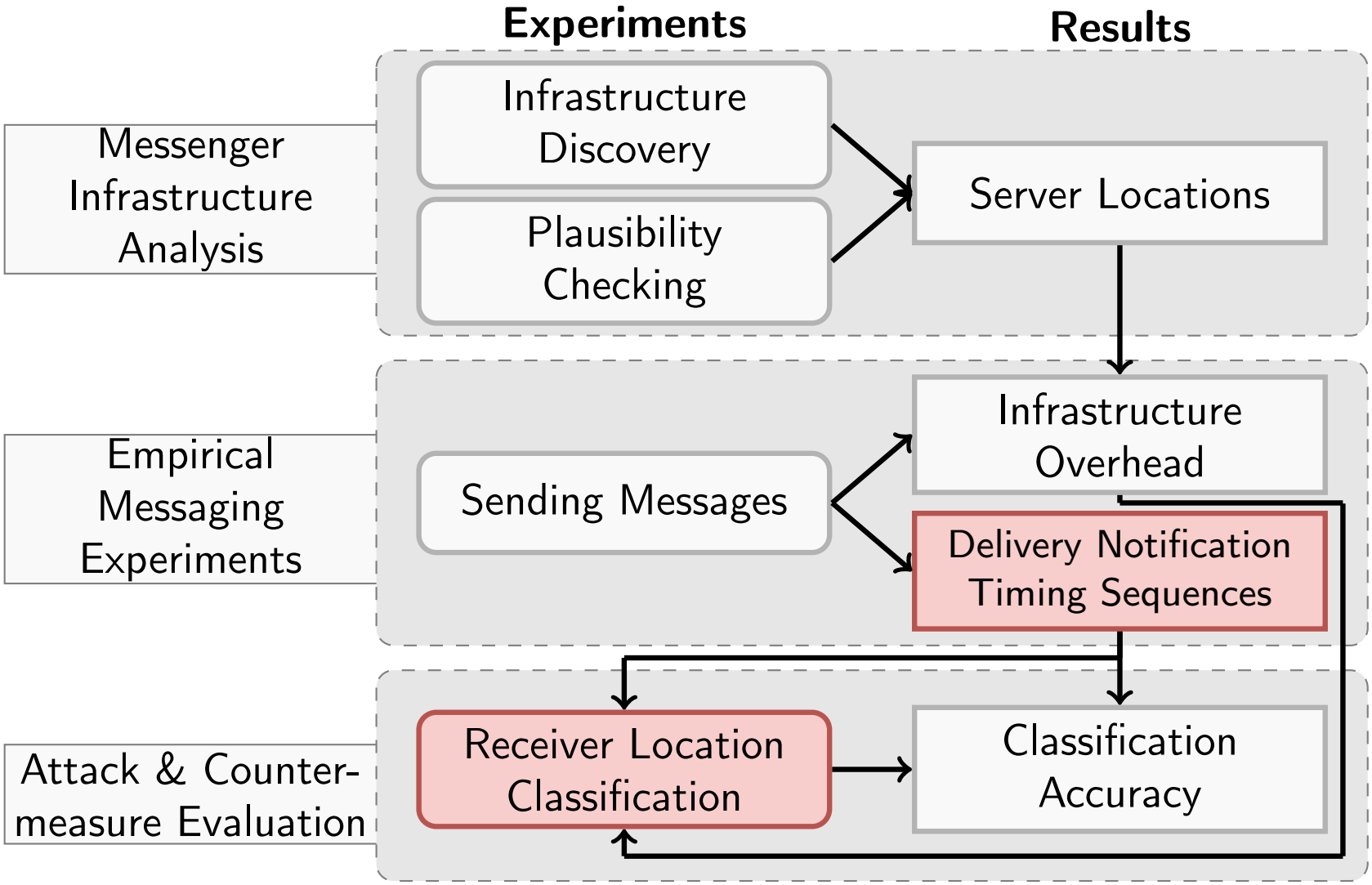
[1] Research Center Trustworthy Data Science and Security, TU Dortmund, Germany

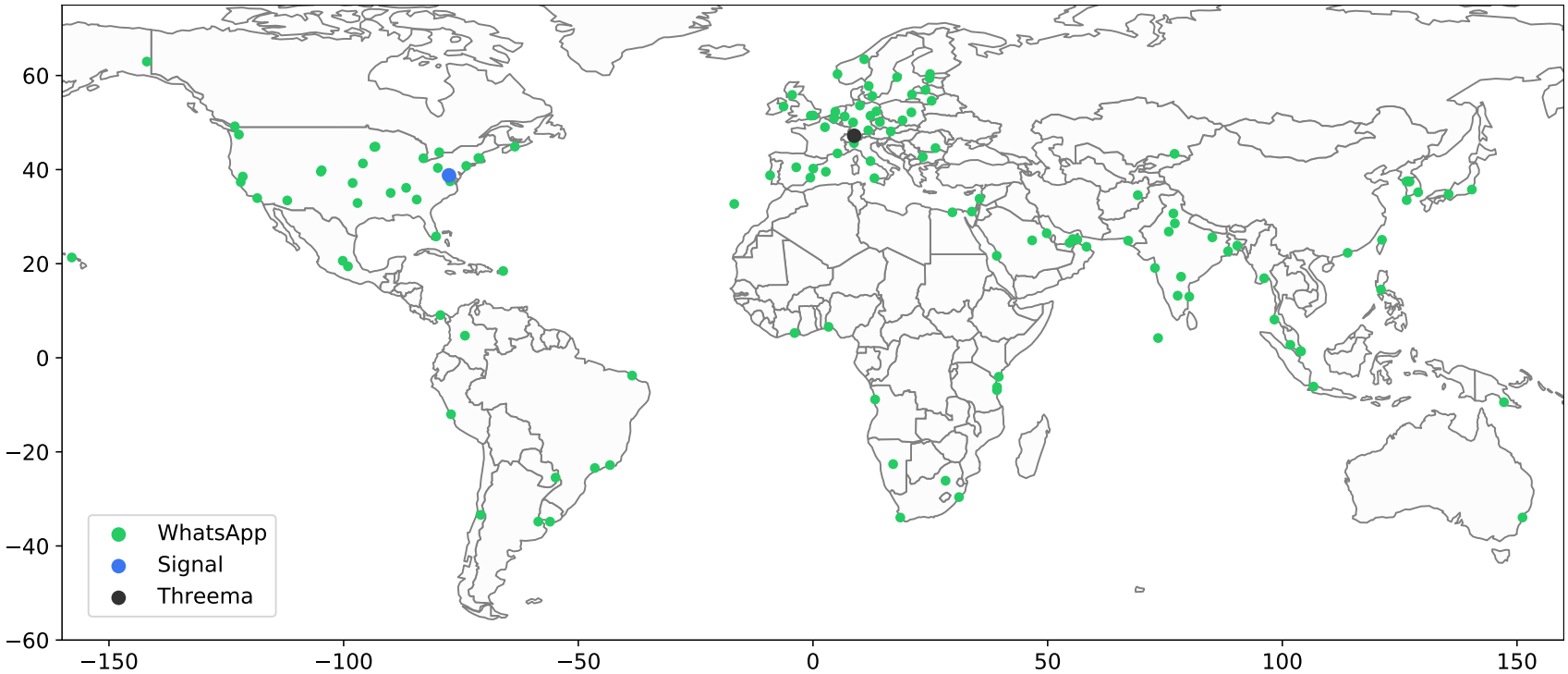
[2] Ruhr-Universität Bochum, Germany

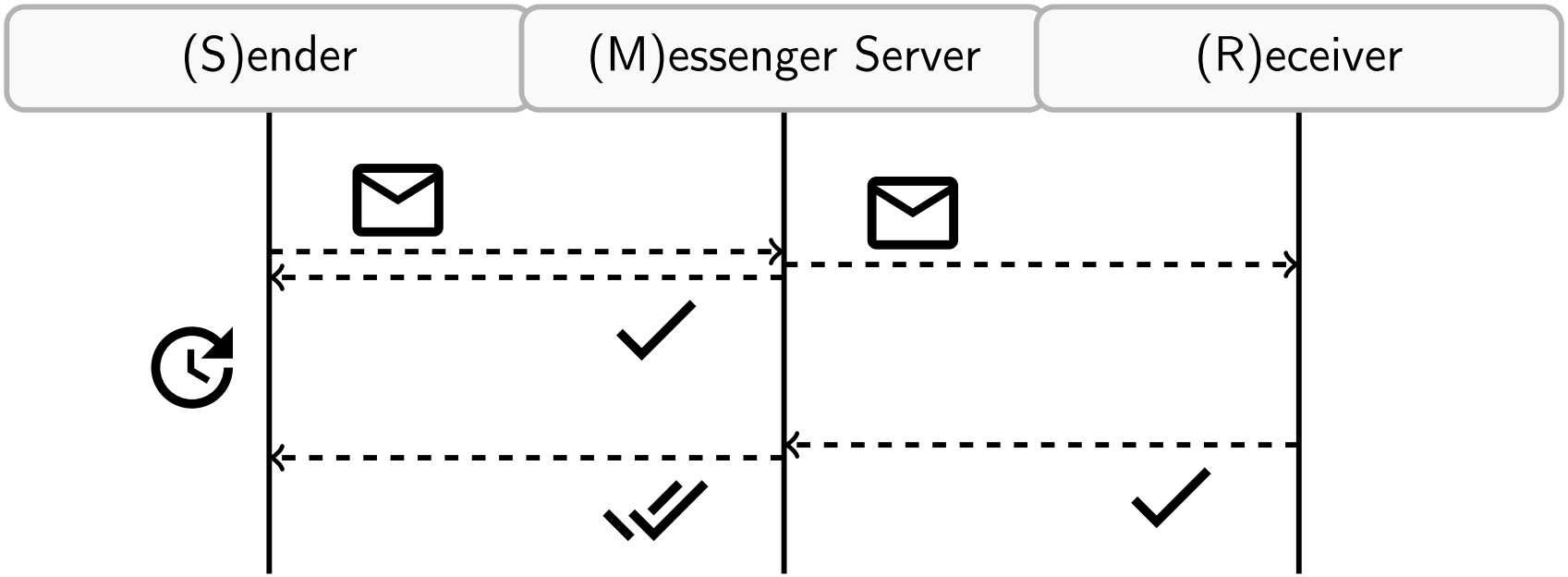
[3] Radboud University, Netherlands

[4] Northeastern University, USA

[5] New York University Abu Dhabi, UAE


Experiments
Results
Messenger Infrastructure Analysis
Infrastructure Discovery
Plausibility Checking
Server Locations
Empirical Messaging Experiments
Sending Messages
Infrastructure Overhead
Delivery Notification Timing Sequences
Attack & Counter-measure Evaluation
Receiver Location Classification
Classification Accuracy


60
40
20
0
−20
−40
−60
−150
−100
−50
0
50
100
150
WhatsApp
Signal
Threema


(S)ender
(M)essenger Server
(R)eceiver

idx=207, t=53.9259, dir=outbound, len=536	
idx=208, t=53.9261, dir=inbound, len=42	
idx=209, t=53.9263, dir=outbound, len=97	m
idx=210, t=53.9264, dir=inbound, len=42	
idx=211, t=54.0722, dir=inbound, **len=123**	n_1
idx=212, t=54.1225, dir=outbound, len=42	
idx=213, t=55.0154, dir=inbound, **len=776**	n_2
idx=214, t=55.0656, dir=outbound, len=56	

idx=207, t=53.9259, dir=outbound, len=536	
idx=208, t=53.9261, dir=inbound, len=42	
idx=209, t=53.9263, dir=outbound, len=97	m
idx=210, t=53.9264, dir=inbound, len=42	
idx=211, t=54.0722, dir=inbound, **len=123**	n_1
idx=212, t=54.1225, dir=outbound, len=42	
idx=213, t=55.0154, dir=inbound, **len=776**	n_2
idx=214, t=55.0656, dir=outbound, len=56	

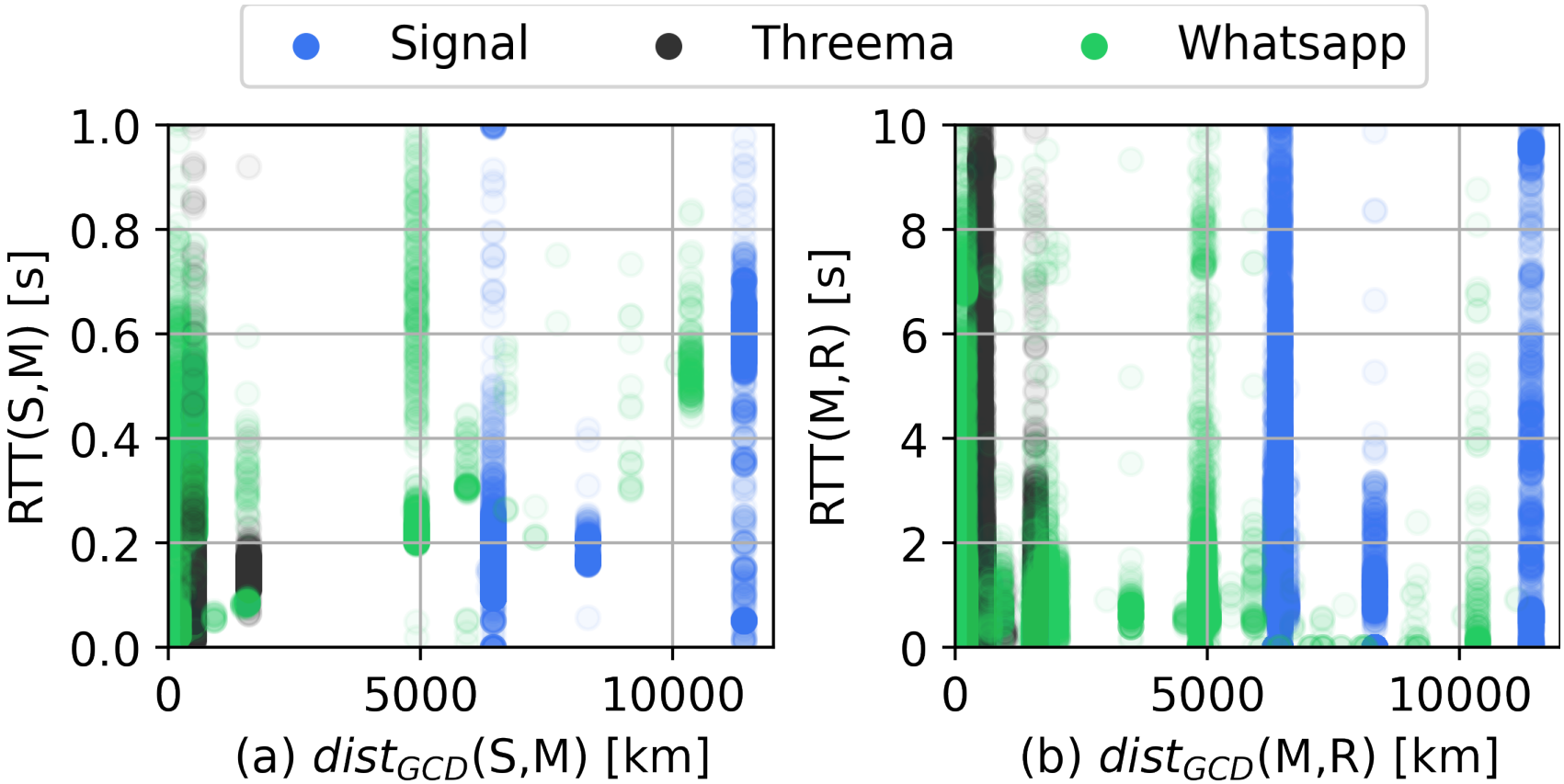
$$RTT_{S,M} = t(n_1) - t(m) \tag{1}$$

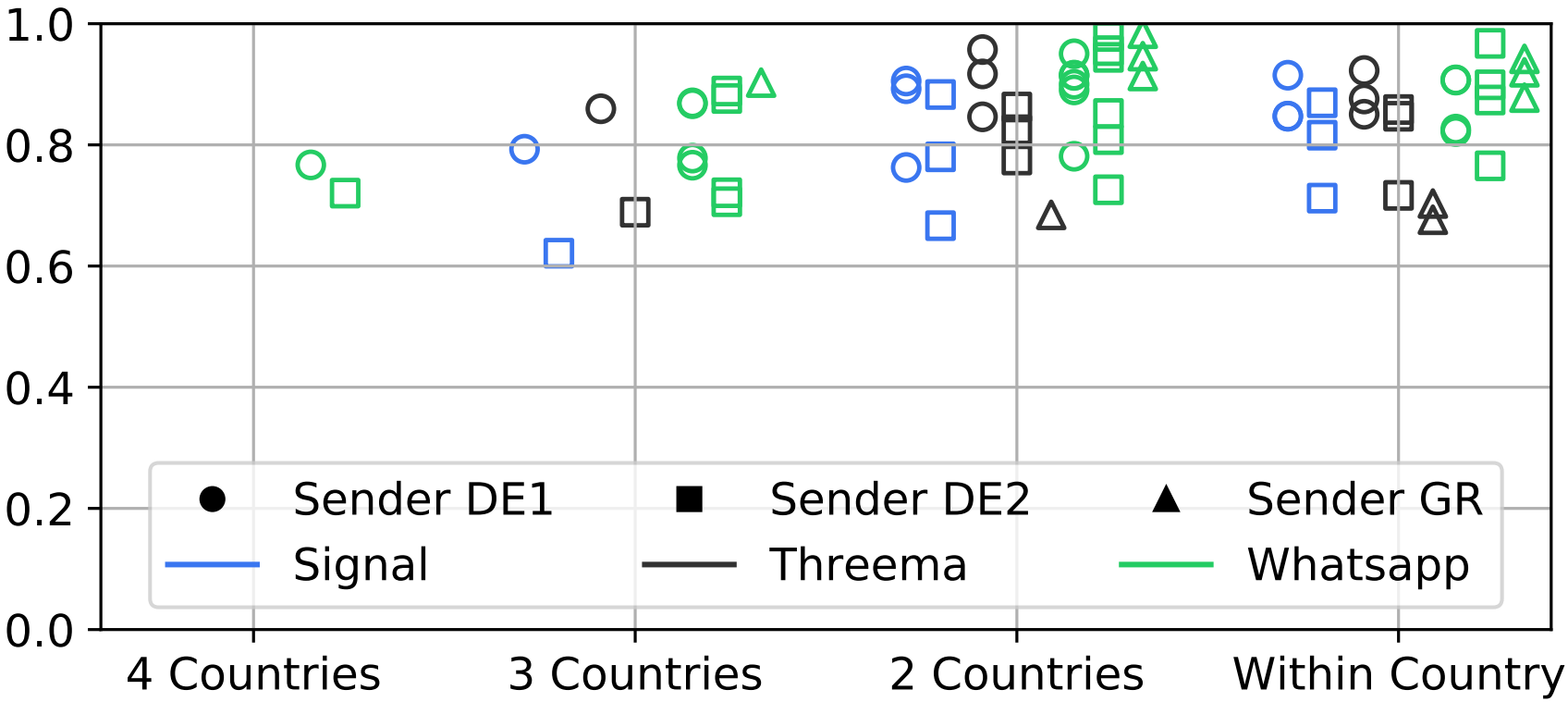
$$RTT_{S,R} = t(n_2) - t(m) \tag{2}$$

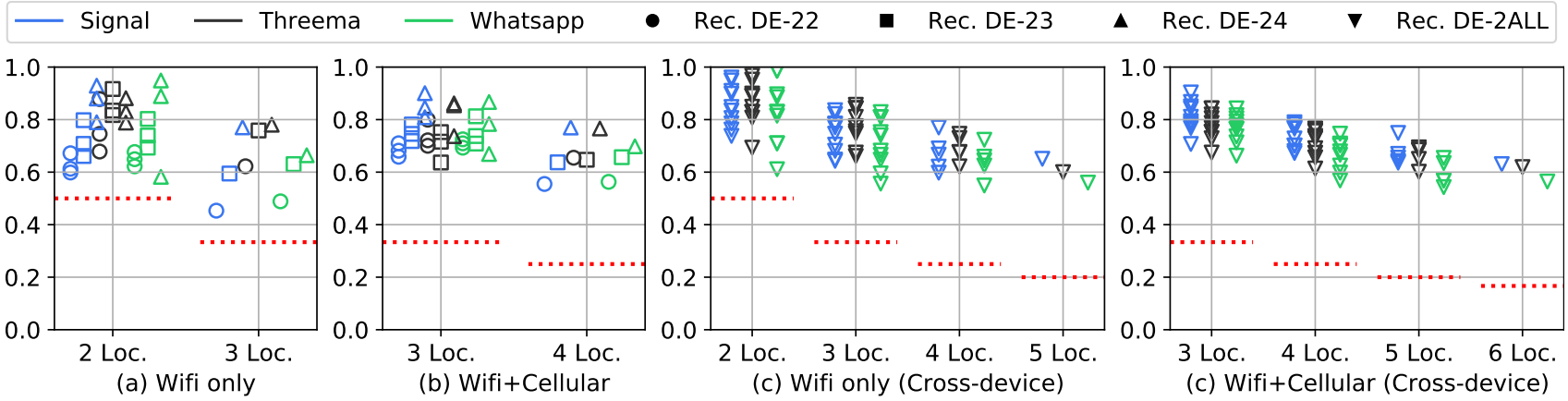
$$RTT_{M,R} = RTT_{S,R} - RTT_{S,M} \tag{3}$$

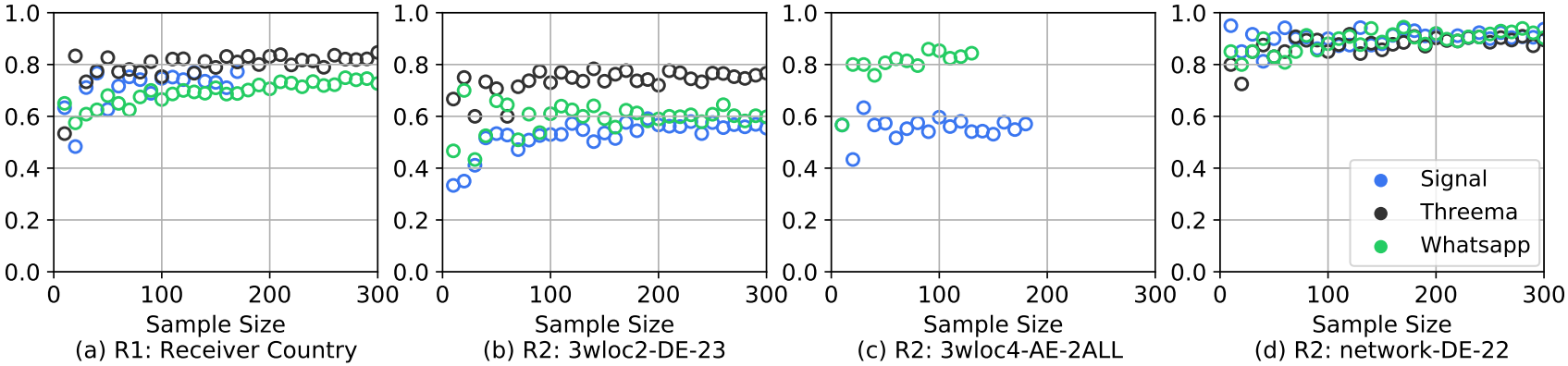
Table: Distances [km] between device locations.

Round 1					Round 2 (UAE)				Round 2 (Germany)				
	DE-B	*NL-A*	*GR-A*	*AE-A*		*AE-B*	*AE-C*	*AE-D*		*DE-B*	*DE-C*	*DE-D*	*DE-E*
DE-A	1.5	98.7	1972.9	4981.0	AE-A	7.8	0.4	19.3	DE-A	1.5	14.4	3.4	5.4
DE-B		97.5	1974.4	4982.2	AE-B		8.1	24.9	DE-B		13.5	2.3	4.0
NL-A			2065.8	5079.5	AE-C			18.9	DE-C			11.2	10.3
GR-A				3263.3					DE-D				2.3


Signal
Threema
Whatsapp
RTT(S,M) [s]
1.0
0.8
0.6
0.4
0.2
0.0
0
5000
10000
(a) $dist_{GCD}$(S,M) [km]
RTT(M,R) [s]
10
8
6
4
2
0
0
5000
10000
(b) $dist_{GCD}$(M,R) [km]


1.0
0.8
0.6
0.4
0.2
0.0
Sender DE1
Sender DE2
Sender GR
Signal
Threema
Whatsapp
4 Countries
3 Countries
2 Countries
Within Country

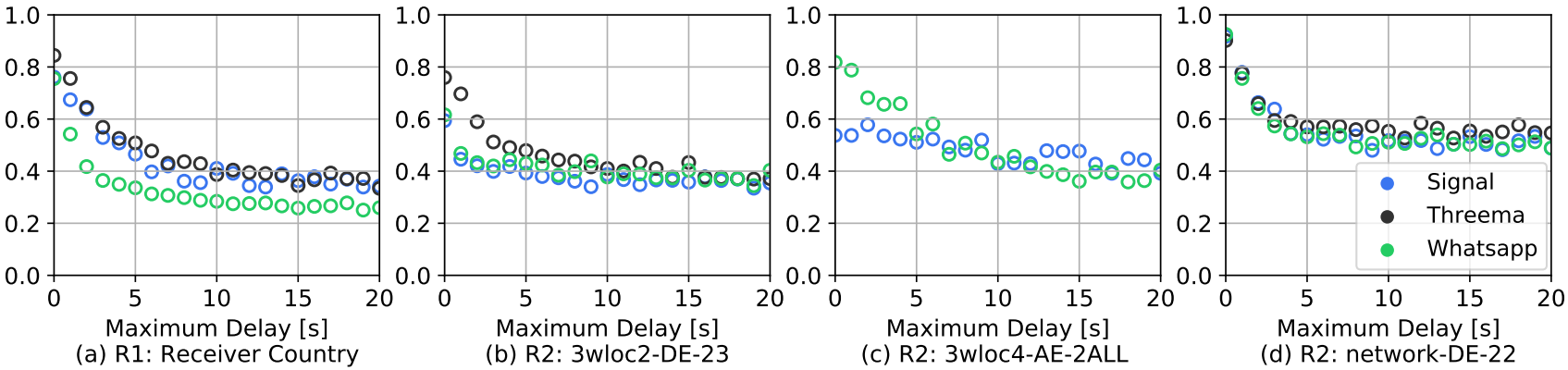

Signal
Threema
Whatsapp
Rec. DE-22
Rec. DE-23
Rec. DE-24
Rec. DE-2ALL
1.0
0.8
0.6
0.4
0.2
0.0
2 Loc.
3 Loc.
(a) Wifi only
3 Loc.
4 Loc.
(b) Wifi+Cellular
2 Loc.
3 Loc.
4 Loc.
5 Loc.
(c) Wifi only (Cross-device)
3 Loc.
4 Loc.
5 Loc.
6 Loc.
(c) Wifi+Cellular (Cross-device)

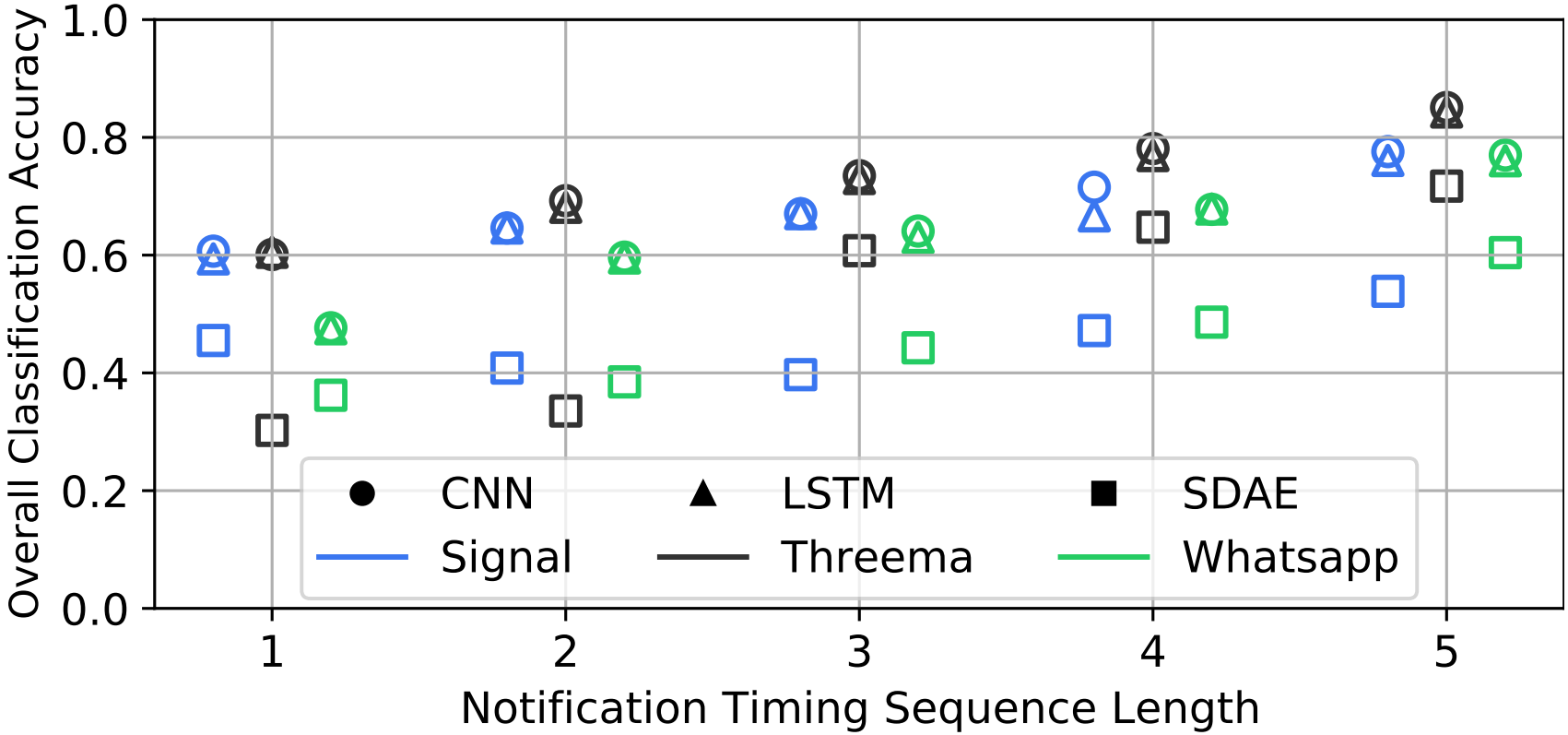


(a) R1: Receiver Country (b) R2: 3wloc2-DE-23 (c) R2: 3wloc4-AE-2ALL (d) R2: network-DE-22

Table: Classification accuracy for receiving devices' network connections (WiFi vs. mobile data)

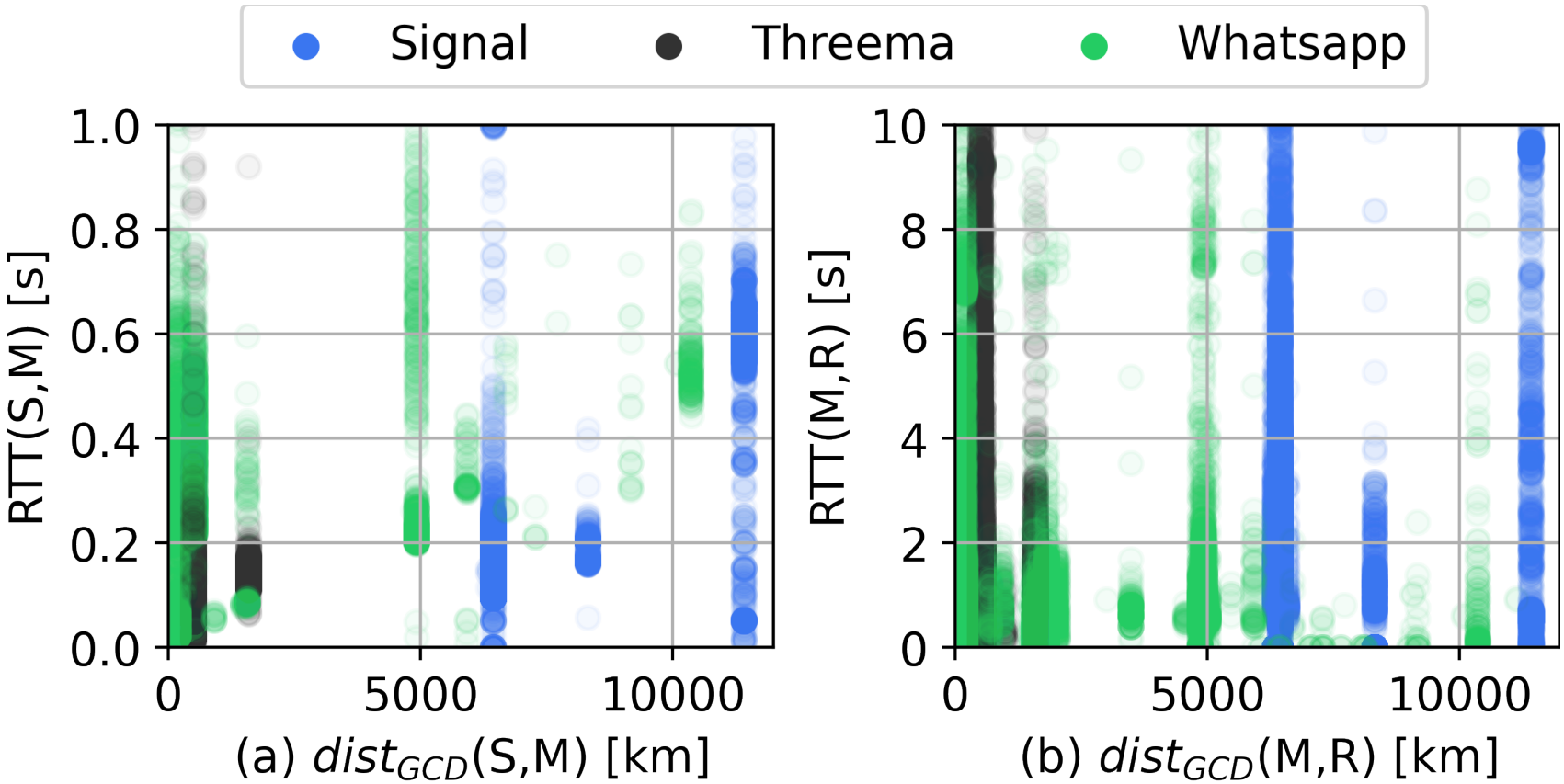
Germany				UAE		
Receiver	SIG	THR	WA	Receiver	SIG	WA
DE-22	92 %	90 %	94 %	AE-22	54 %	91 %
DE-23	90 %	75 %	90 %	AE-23	61 %	89 %
DE-24	95 %	94 %	92 %	AE-24	77 %	90 %
DE-2ALL	91 %	85 %	88 %	AE-2ALL	62 %	87 %


1.0
0.8
0.6
0.4
0.2
0.0
0
5
10
15
20
Maximum Delay [s]
(a) R1: Receiver Country
(b) R2: 3wloc2-DE-23
(c) R2: 3wloc4-AE-2ALL
(d) R2: network-DE-22
Signal
Threema
Whatsapp


Overall Classification Accuracy
1.0
0.8
0.6
0.4
0.2
0.0
1
2
3
4
5
Notification Timing Sequence Length
CNN
LSTM
SDAE
Signal
Threema
Whatsapp

"Since the messengers we consider use multiple layers of encryption (i.e., end-to-end encryption between the communication partners and TLS-encryption for connections between clients and servers on the transport layer), we are not able to access the contents of the communication."

idx=207, t=53.9259, dir=outbound, len=536	
idx=208, t=53.9261, dir=inbound, len=42	
idx=209, t=53.9263, dir=outbound, len=97	m
idx=210, t=53.9264, dir=inbound, len=42	
idx=211, t=54.0722, dir=inbound, **len=123**	n_1
idx=212, t=54.1225, dir=outbound, len=42	
idx=213, t=55.0154, dir=inbound, **len=776**	n_2
idx=214, t=55.0656, dir=outbound, len=56	


Signal
Threema
Whatsapp
RTT(S,M) [s]
1.0
0.8
0.6
0.4
0.2
0.0
0
5000
10000
(a) $dist_{GCD}$(S,M) [km]
RTT(M,R) [s]
10
8
6
4
2
0
0
5000
10000
(b) $dist_{GCD}$(M,R) [km]

Takeaways

- You can get decent closed-world location classification accuracy in just 5 messages.*
- There seems to be a lot of low-hanging fruit here.
- Delivery receipts continue to be a privacy headache.

*After 100 training samples per location