Measuring Ambient Cellular Signals in High-mobility Conditions

Presenter: Yanjun Pan
Department of CSCE, University of Arkansas.

LASER Workshop 2022, San Diego

Talk Outline

Explore the experimental approach for our work that appears in NDSS 2022

Ziqi Xu, Jingcheng Li, Yanjun Pan, Loukas Lazos, Ming Li, and Nirnimesh Ghose. PoF: Proof-of-Following for Vehicle Platoons. In *Proc. of the NDSS Symposium,* 2022

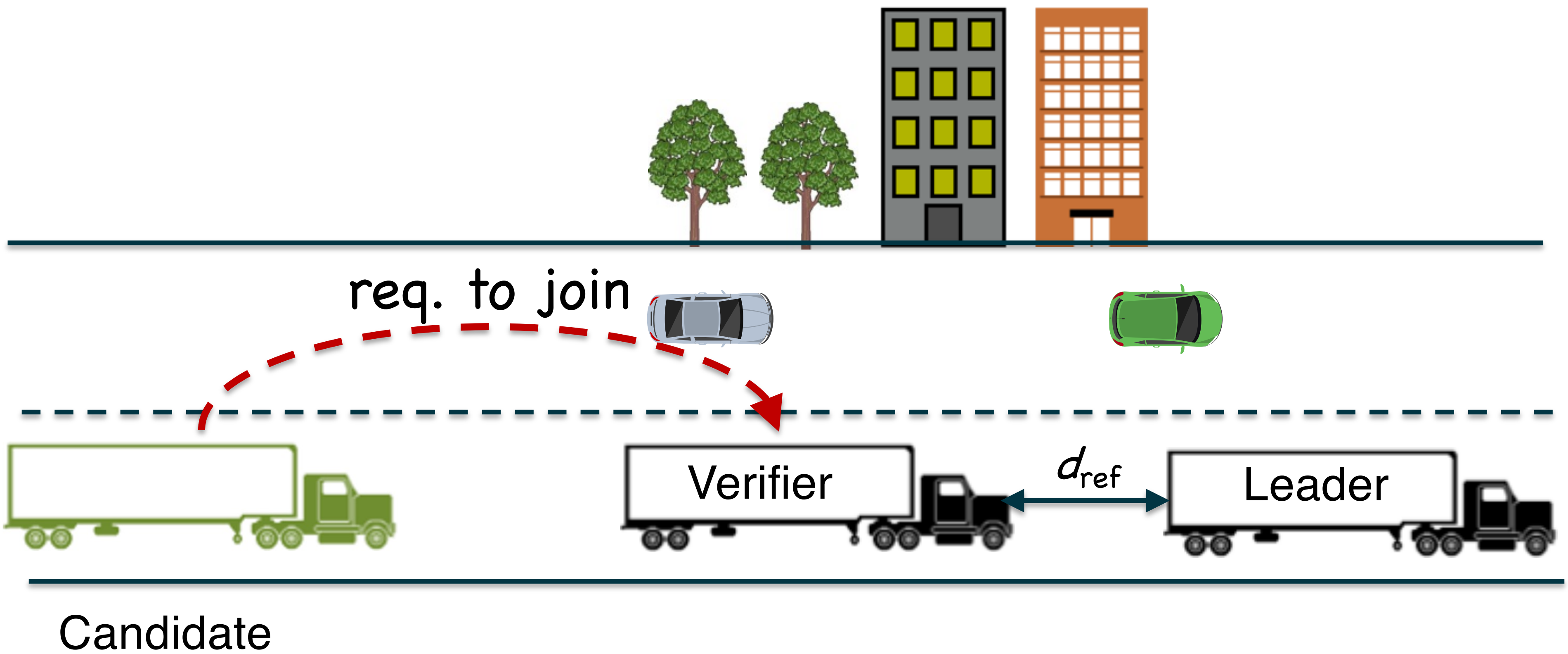
Present our initial research hypothesis

Describe the set of experiments designed to test our hypothesis in different settings

Describe the RF and platooning testbed

Share the challenges and useful experiences

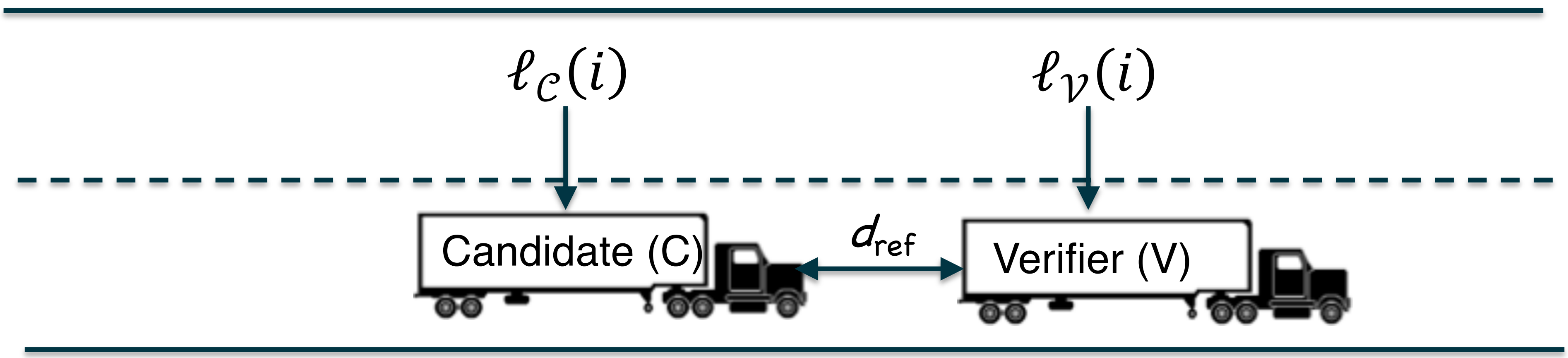
Dynamic Platoon Formation



Crypto machinery is not sufficient to verify physical properties

Location, Proximity, Time, Speed, Acceleration,
Physiological signals, temperature, state (open/close)

Proof-of-Following (PoF)



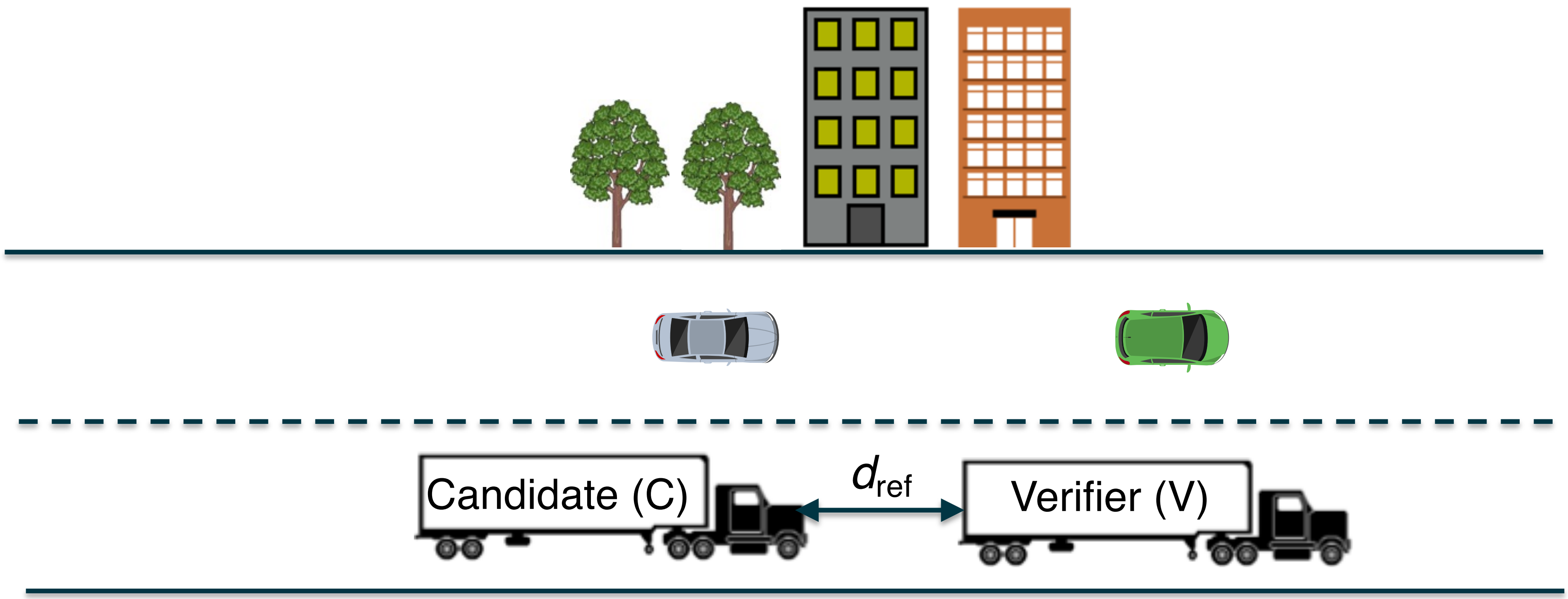
route of V: $L_{\mathcal{V}} = \ell_{\mathcal{V}}(1) \rightarrow \ell_{\mathcal{V}}(2) \rightarrow \cdots \rightarrow \ell_{\mathcal{V}}(n)$

route of C: $L_{\mathcal{C}} = \ell_{\mathcal{C}}(1) \rightarrow \ell_{\mathcal{C}}(2) \rightarrow \cdots \rightarrow \ell_{\mathcal{C}}(n)$

$$\text{PoF} : || \ell_{\mathcal{V}}(i) - \ell_{\mathcal{C}}(i)|| < d_{ref}, \forall i$$

Physical Access Control: only platooning members can communicate

Main idea: Exploit common dynamic context

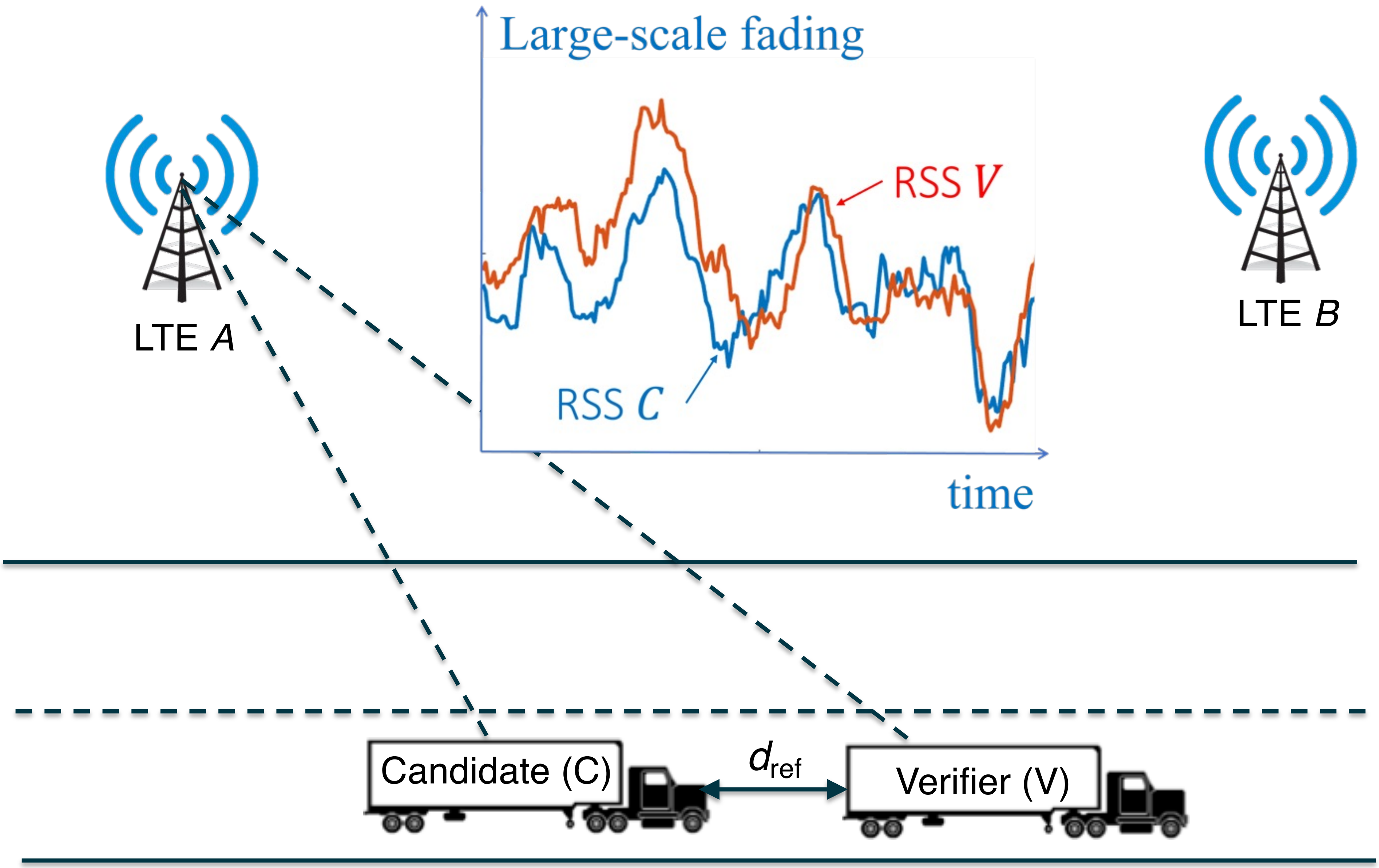


common dynamic context

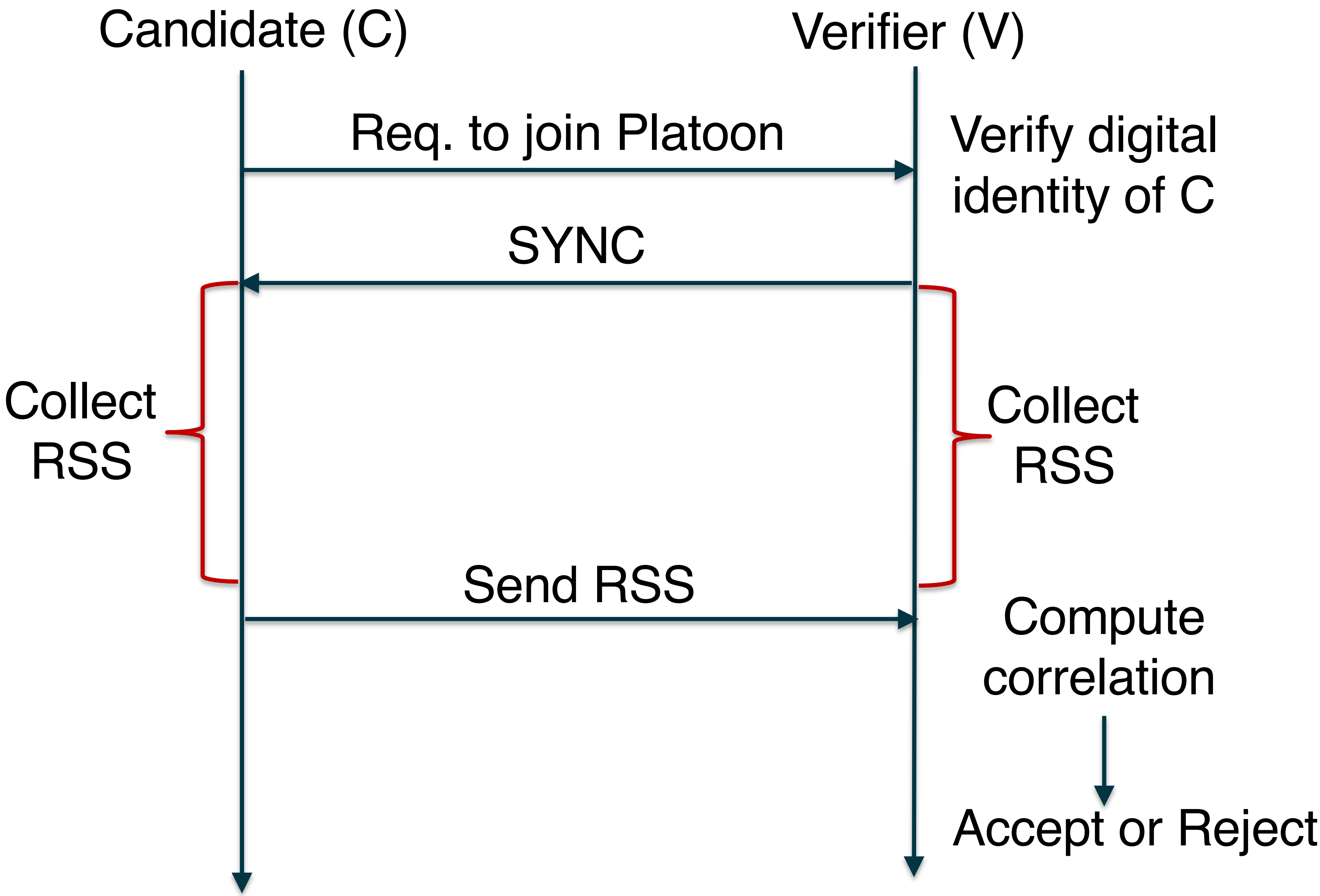
Spatial dynamics

Temporal dynamics

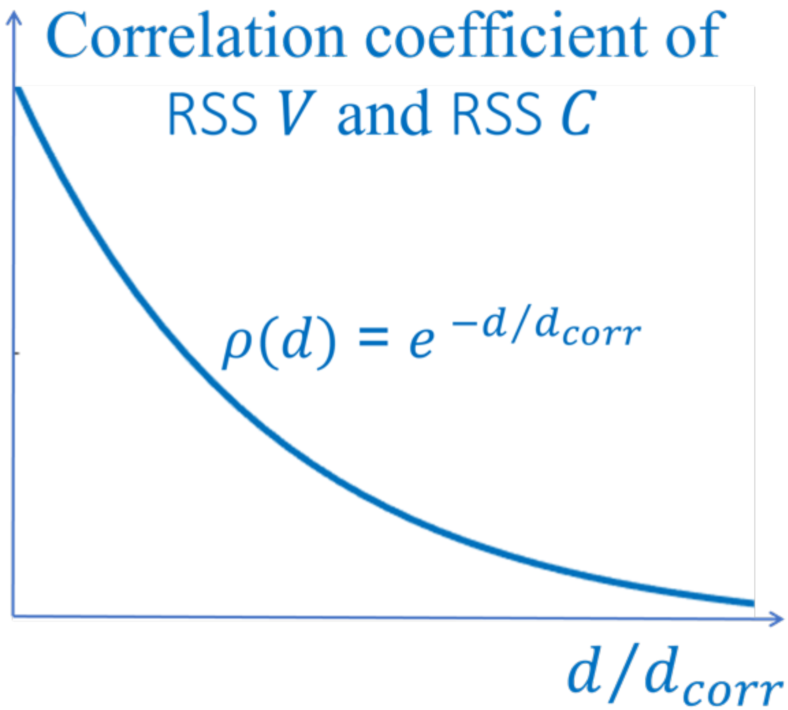
Dynamic context: Large-Scale RSS



PoF Protocol



Main Hypothesis



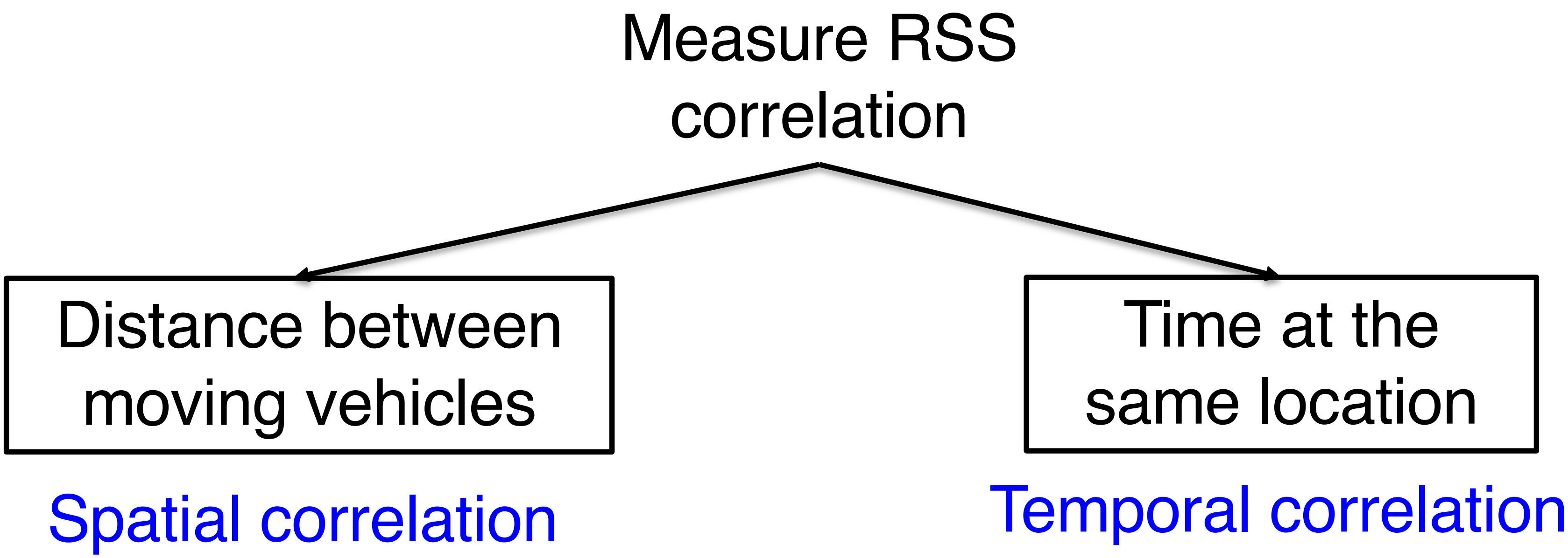
1) Spatial correlation decreases with distance

2) Temporal correlation decreases with time

3) In-band modality using existing receivers

d_{corr}: decorrelation distance
E.g., d_{corr} = 50m for highway

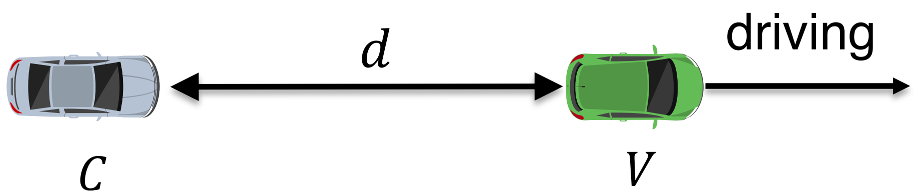
Hypothesis Validation



Main Challenges in Data Collection

Select the LTE band for ambient RSS sampling

Control the distance d between moving vehicles in realistic conditions

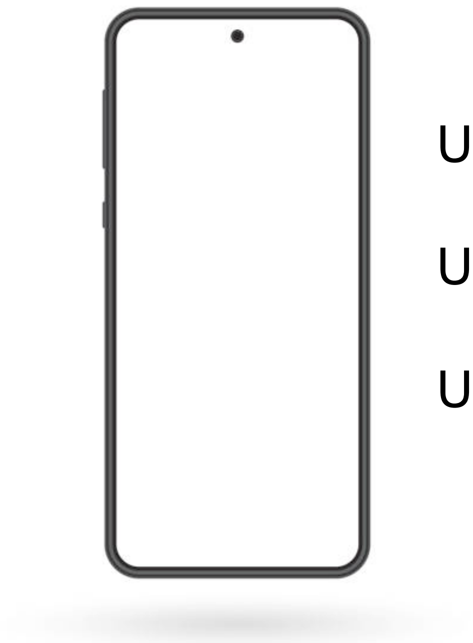


Geotag and timestamp RSS samples

Run experiments multiple times in various settings to collect sufficient data

Geotagging and Timestamping RSS Samples

Initial setup: Use onboard modules of an Android Phone



Use LTE receiver to record RSS

Use GPS to geotag

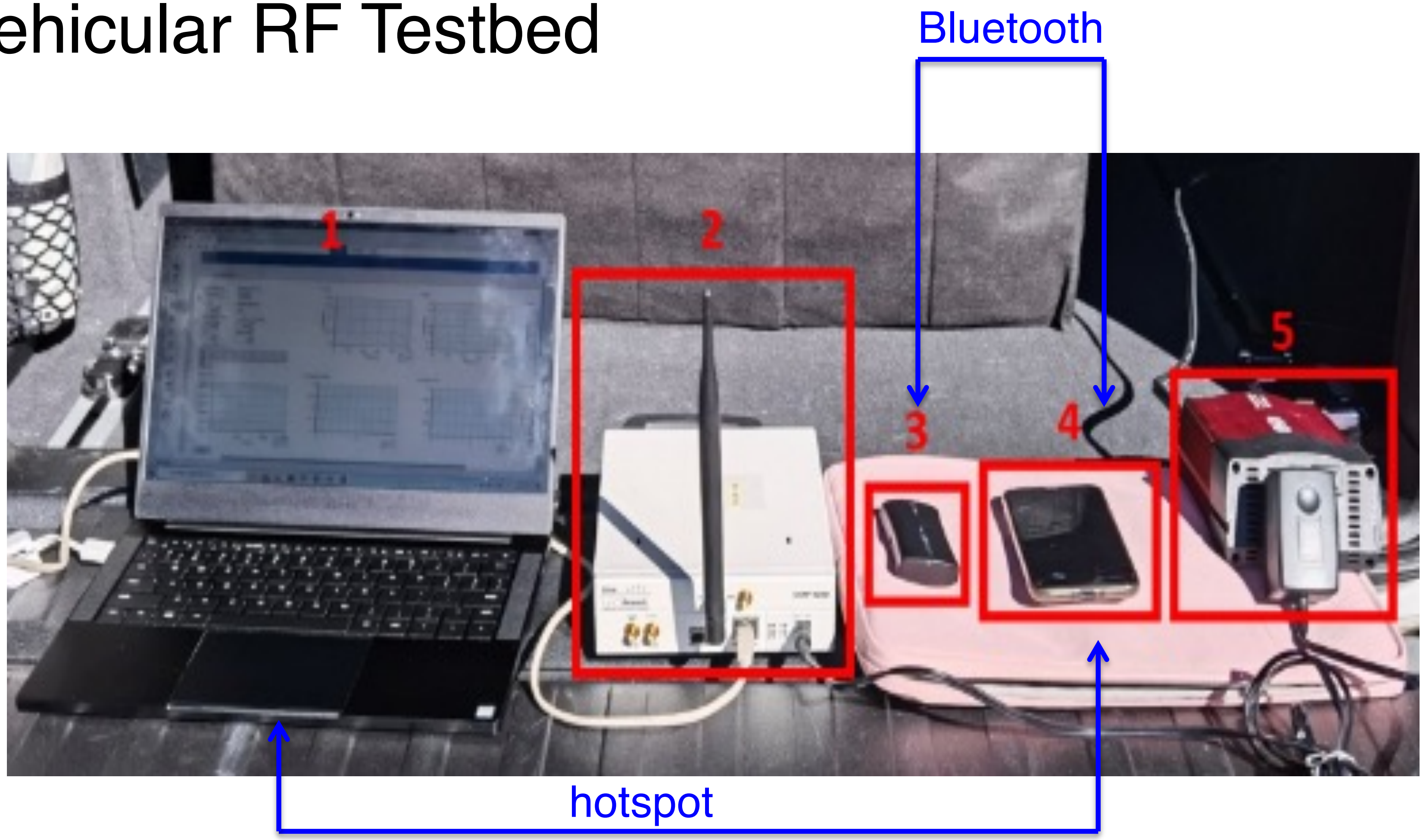
Use internal time to record timestamp

Insurmountable problems

- Could not control the LTE channel recorded by different phones
- Low GPS sampling rate relative to the RSS sampling rate
- Low resolution timestamping

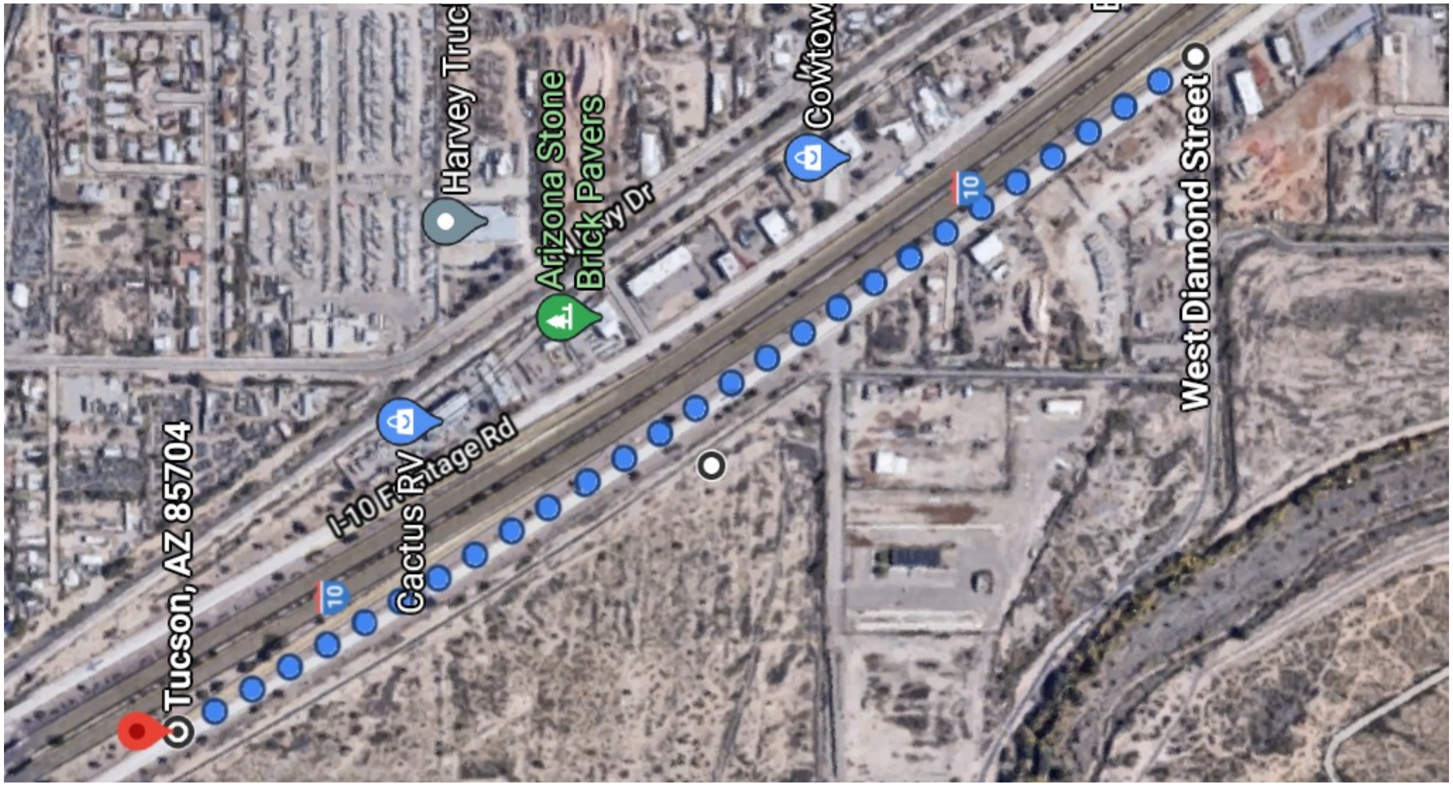
Switched to a proof-of-concept USRP testbed

Our Vehicular RF Testbed



1. Laptop: records GPS and RSS data
2. USRP: receives ambient LTE signals
3. GPS: records location
4. Smartphone: act as a hotspot to laptop and connects via Bluetooth to GPS receiver
5. Power supply

LTE Band Selection

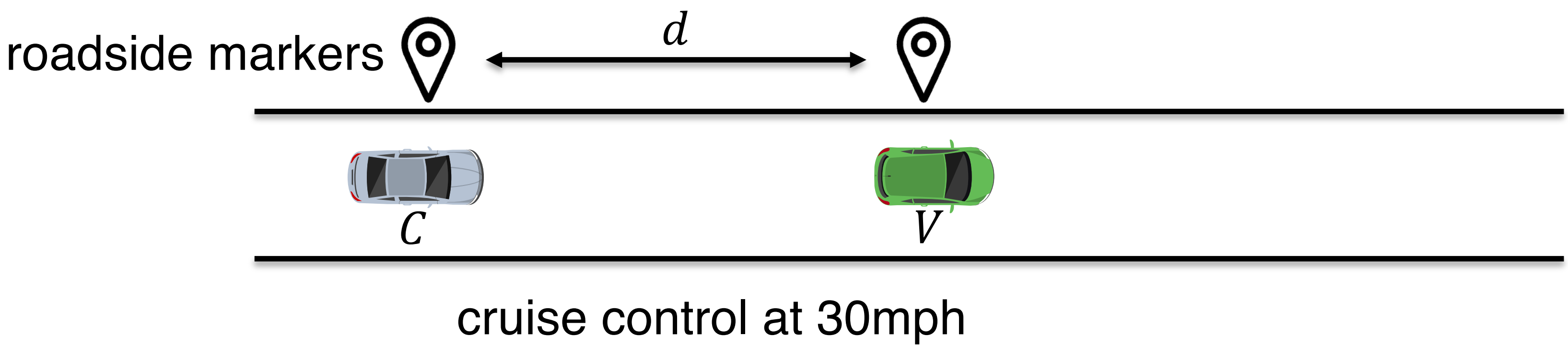


Multiple LTE band sampled: 2, 4, 5, 25, 26, 66

Selected bands with highest average RSS
Urban setting: 1.972GHz
Highway/Freeway: 875MHz

Bandwidth: 4MHz

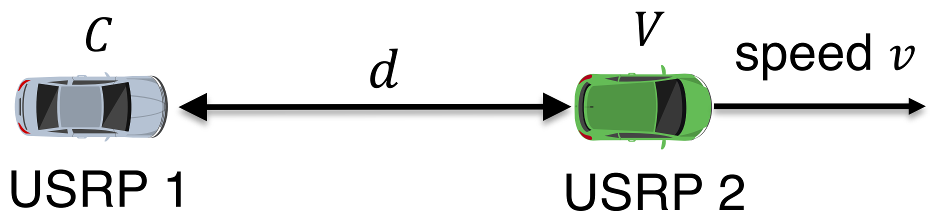
Following Distance Control



Verified average distance and distance variance via GPS data

Repeated experiments for different following distances

Geotagging and Timestamping RSS Samples



RSS timestamps generated by the Laptop connected to each USRP

USRP, Candidate

-10.080850	1614200773.162772
-11.737489	1614200773.214376
-12.806208	1614200773.266790
-15.456426	1614200773.319163
-14.515842	1614200773.368887
-13.001224	1614200773.420077
-12.150038	1614200773.472659
-15.612380	1614200773.522907

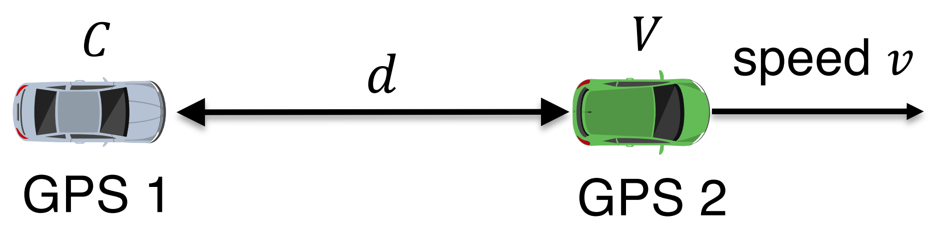
USRP, Verifier

-16.582575	1614200773.181551
-18.626912	1614200773.231747
-15.717246	1614200773.282426
-14.137355	1614200773.333816
-12.991919	1614200773.386459
-14.822561	1614200773.437256
-16.344071	1614200773.487171
-13.321490	1614200773.539378

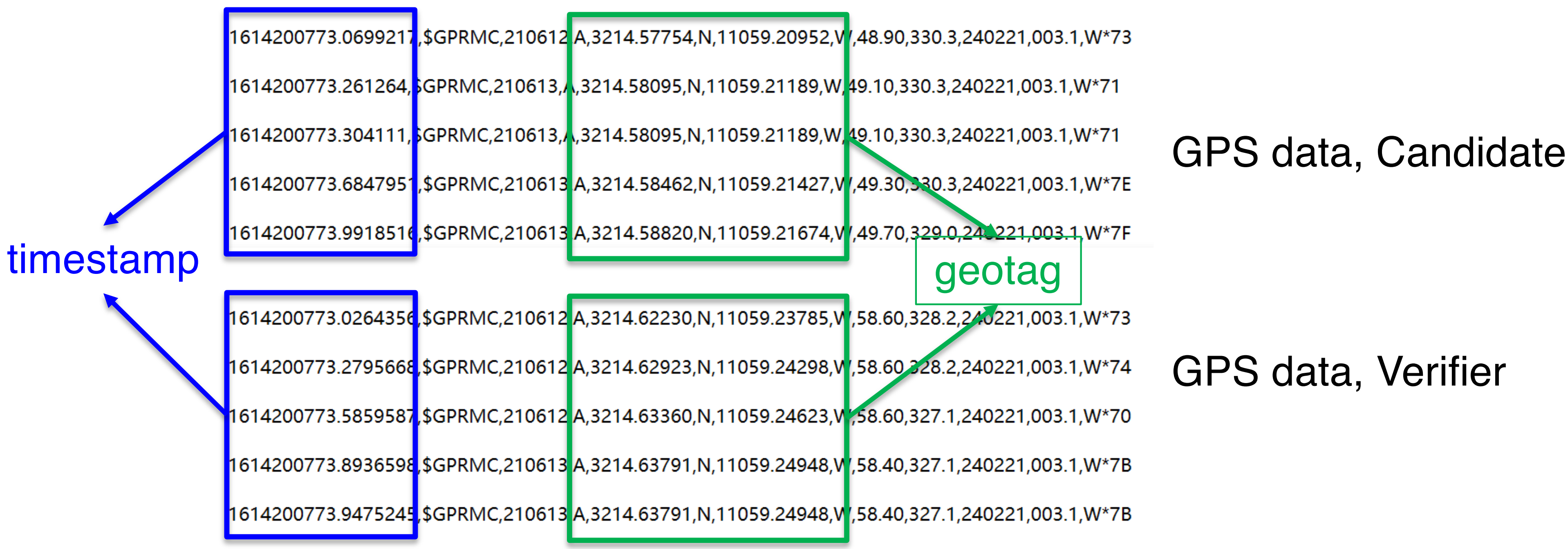
RSS timestamp

Geotagging and Timestamping RSS Samples

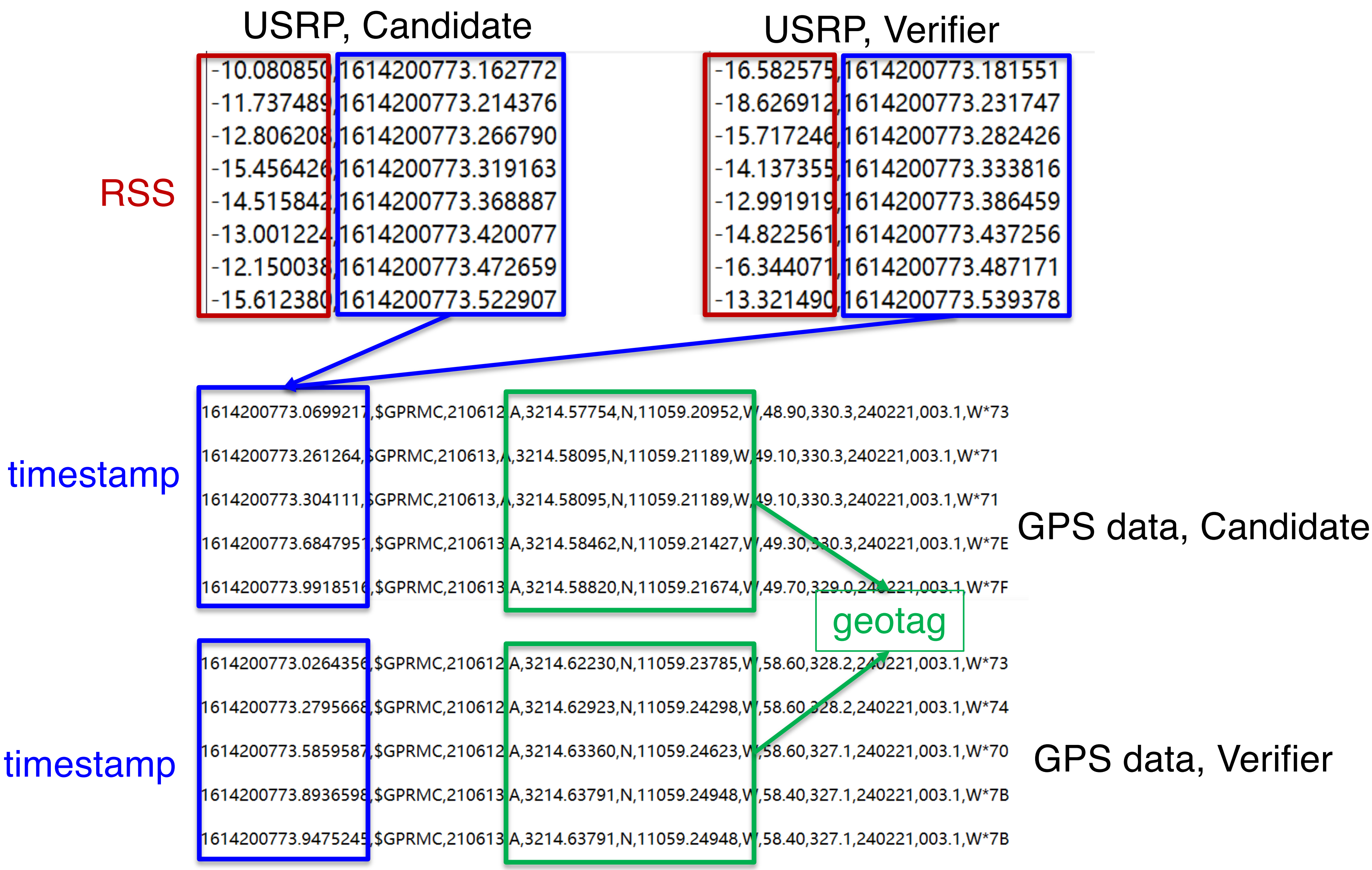
Geotag and timestamp RSS



Collect geotags and timestamp from the two GPS devices.

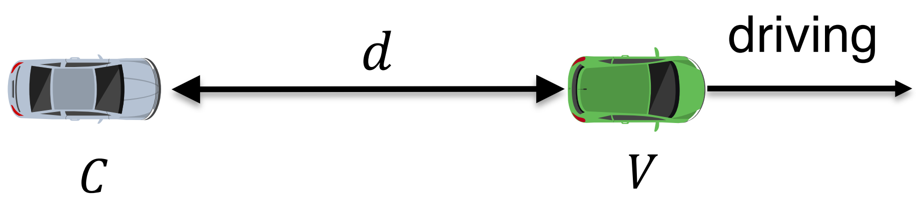


Geotagging and Timestamping RSS Samples



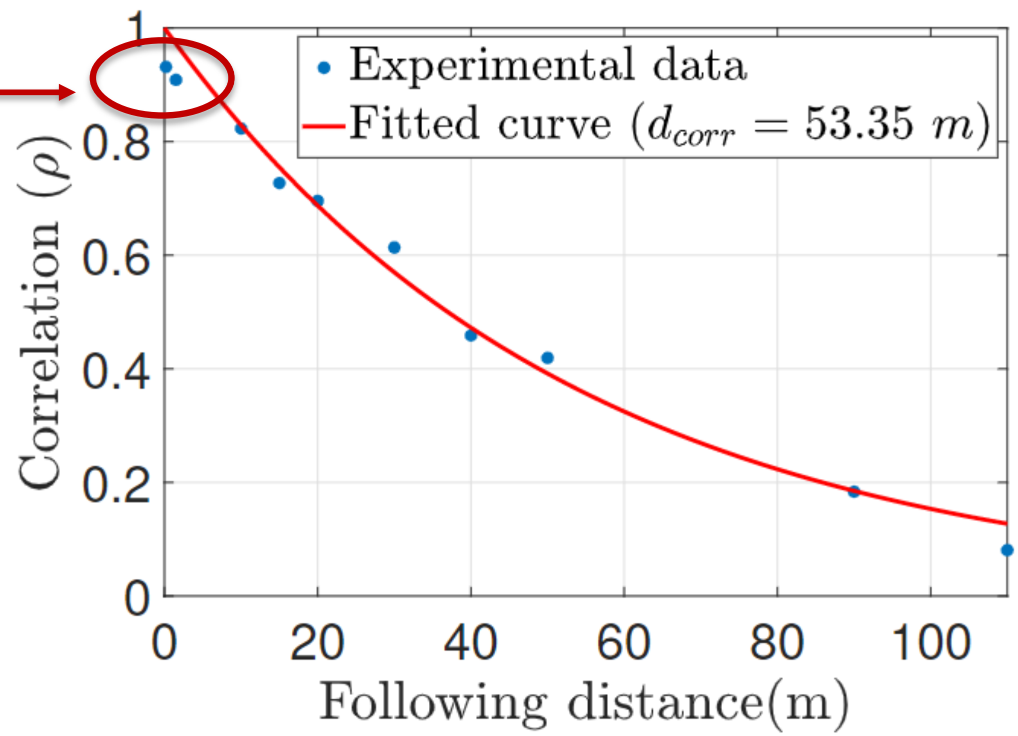
Hypothesis Validation (1)

Spatial correlation decreases with distance



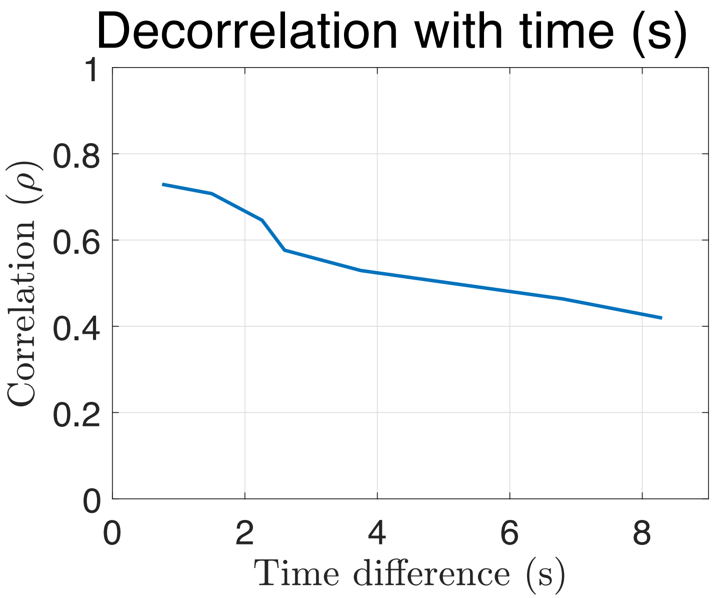
Decorrelation with distance

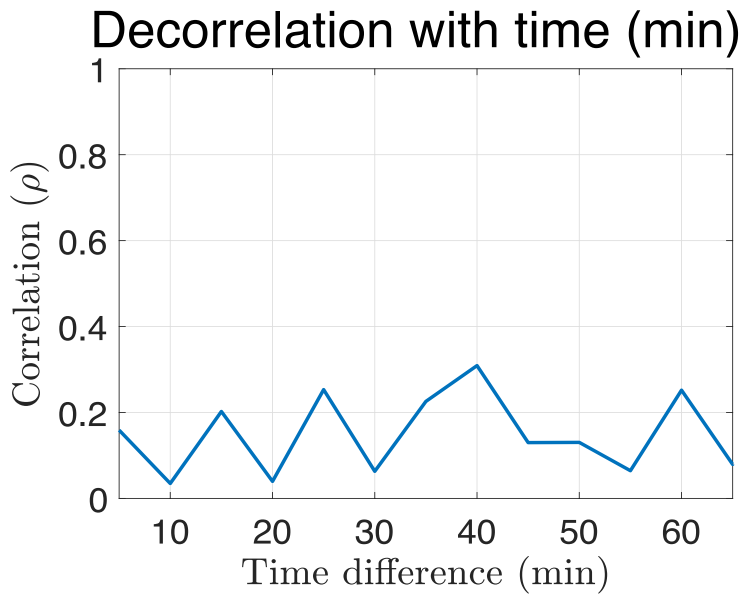
measured by placing two USRPs in the same vehicle



Hypothesis Validation (2)

Temporal correlation decreases with time





The RSS correlation took place at the same location but at different times

Platooning Testbed on Urban Environment

2.5-mile route inside Tucson

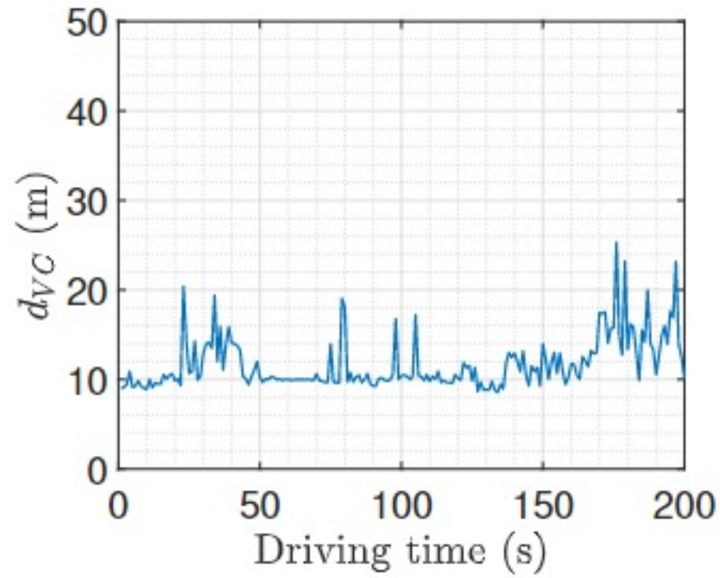
d_{VC}=11m on avg.

C

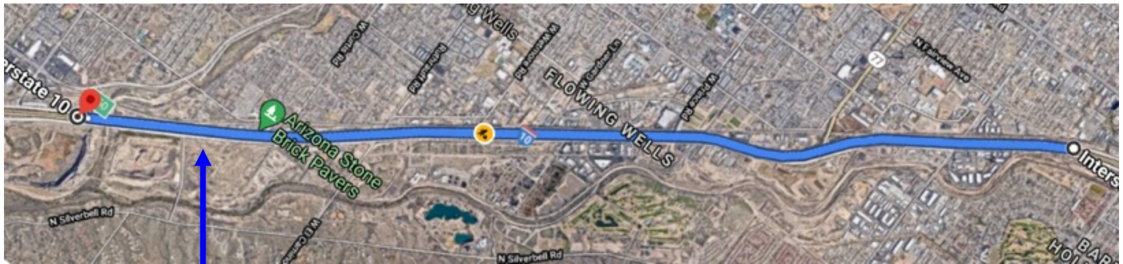
$v_V = v_C$=40 mph

V

the real-time d_{VC} in experiment.

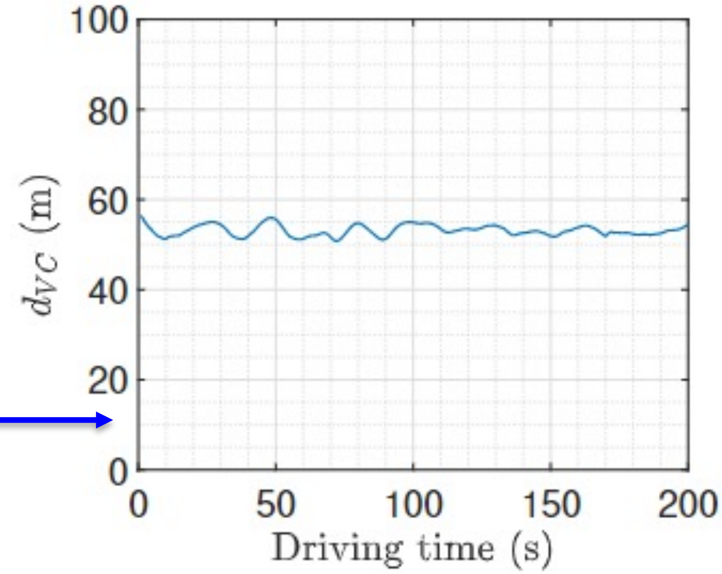


Platooning Testbed on Highway



6.5-mile route on the I-10 highway

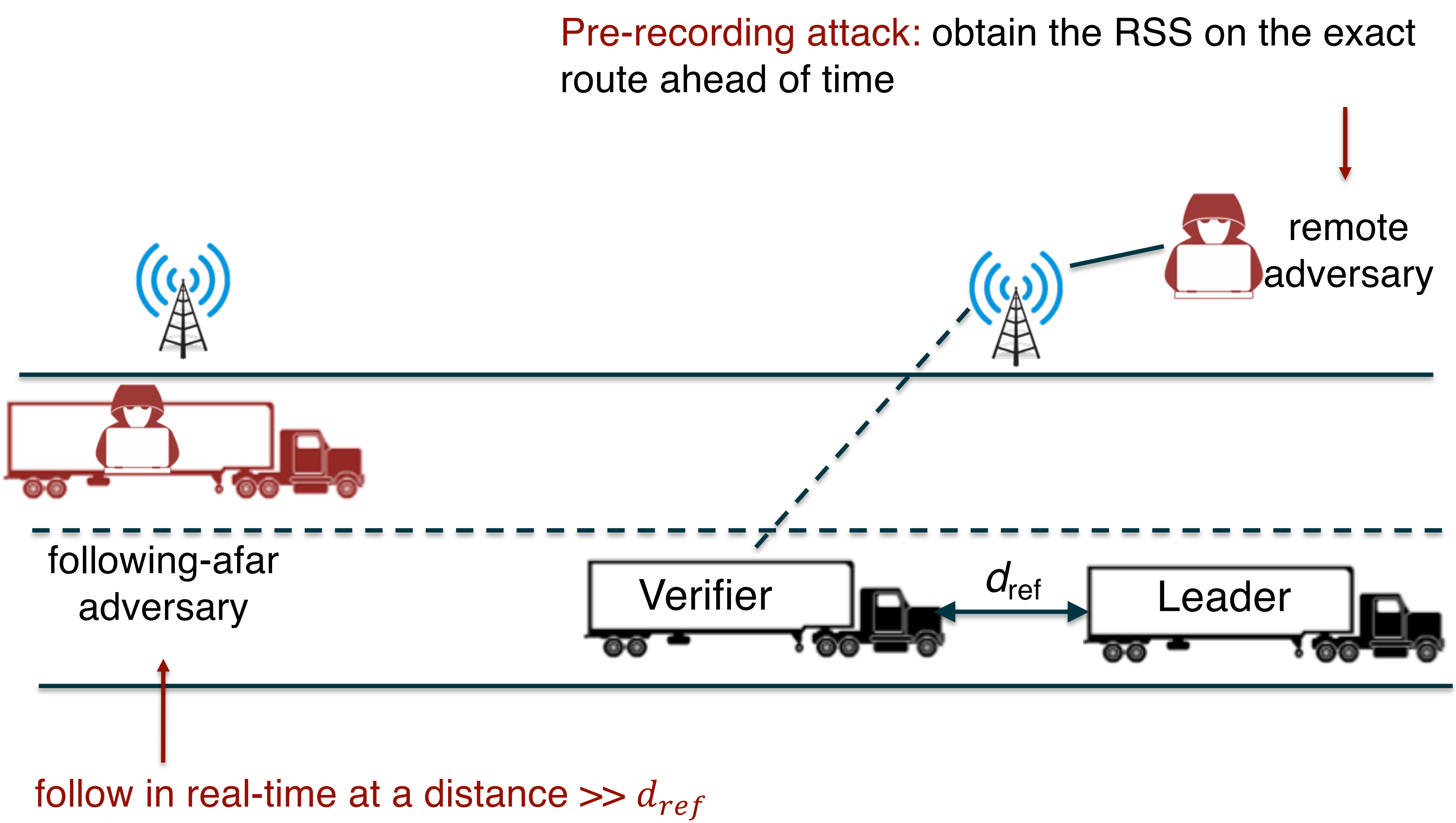
Two platooning vehicles driving at 55-60 mph with a stable distance of 53.4m.



The Verifier(V) on cruise control and Candidate(C) follows V on adaptive cruise control

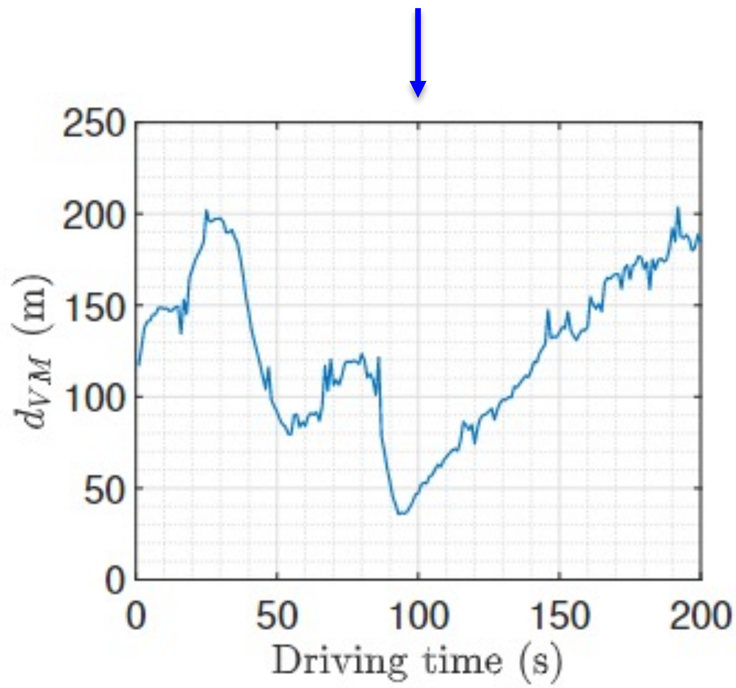
The Candidate (C) in experiment and its RF testbed.

Implementing the Threat Model



Adversary in Urban Experiments

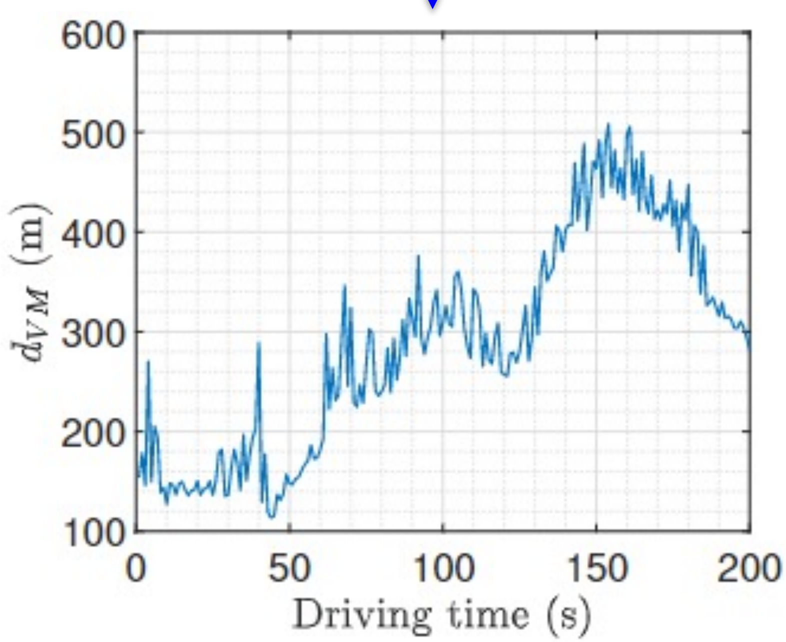
- remote adversary: one vehicle drove on the exact route and prerecorded the RSS 70 mins ahead of time
- following-afar adversary: one vehicle followed the verifier at an average distance of 125m



The distance between the following-afar adversary and verifier in real-time.

Adversary in Highway Experiments

- remote adversary: vehicle drove on the exact route and prerecorded the RSS 40 mins ahead of time
- following-afar adversary: one vehicle followed the verifier at a following distance of 250m on average.



The distance between the following-afar adversary and verifier in real-time.

Data Processing

Notation	Definition
N	Number of samples in subsets Γ_V^k and Γ_C^k
M	Moving average window size
K	Number of RSS subsets, correlation values, and correlation tests
τ	Passing threshold for a single correlation test
α	Fraction of correlation tests to pass *PoF* verification
f_C	Passing rate of a single correlation test achieved by $\mathcal{C}$
F_C	Passing rate of K correlation tests achieved by $\mathcal{C}$

$$\Gamma_V = \{(\gamma_V(1), t_V(1)), (\gamma_V(2), t_V(2)), \cdots, (\gamma_V(N), t_V(N)), \cdots, (\gamma_V(i), t_V(i)) \cdots\}$$

↓ K groups of N samples

K groups of $\Gamma_V^1 = \{\gamma_V(1), \gamma_V(2), \cdots, \gamma_V(N)\}$

↓ Applied an M-point moving average

smoothed Γ_V^k

↓

computed the correlation $\rho(k)$ between Γ_V^k and Γ_C^k

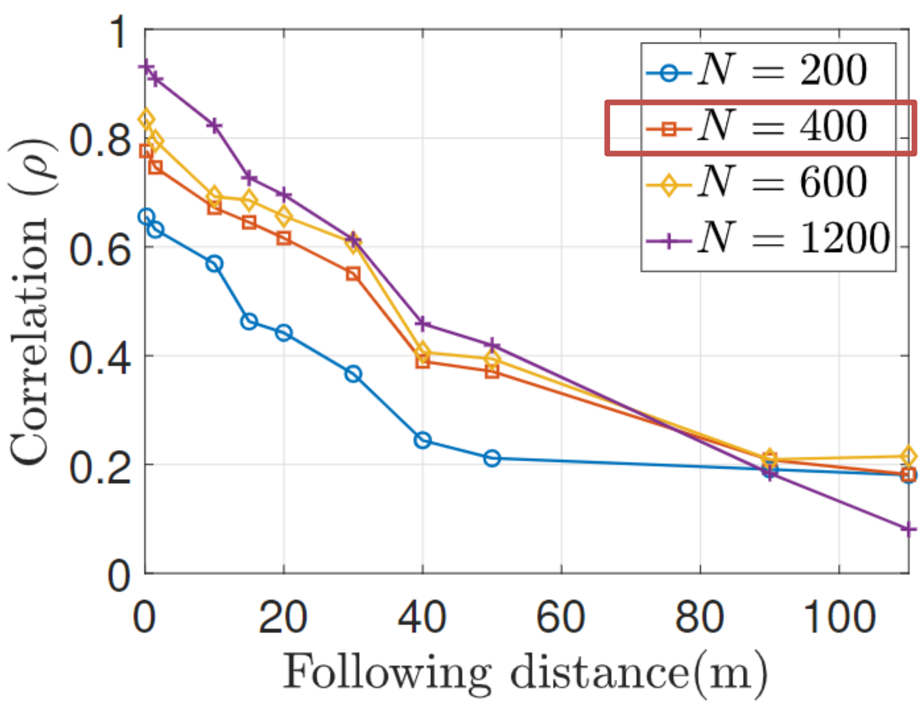
↓

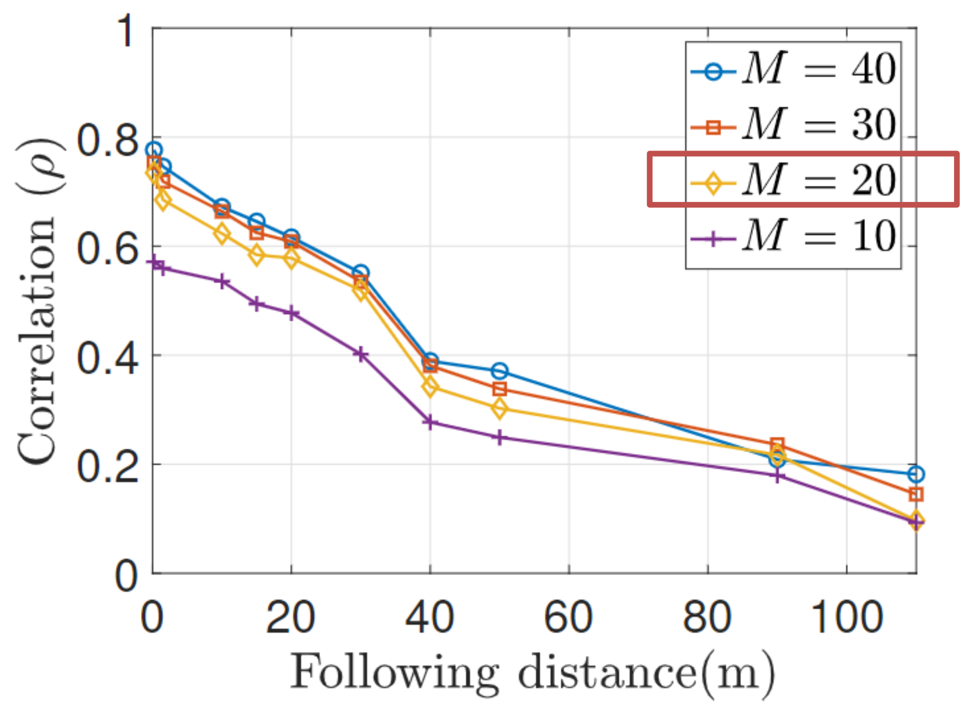
compared $\rho(k)$ with threshold τ

Selecting PoF Test Parameters (1)

Notation	Definition
N	Number of samples in subsets Γ_V^k and Γ_C^k
M	Moving average window size

Using the same data obtained from the hypothesis validation





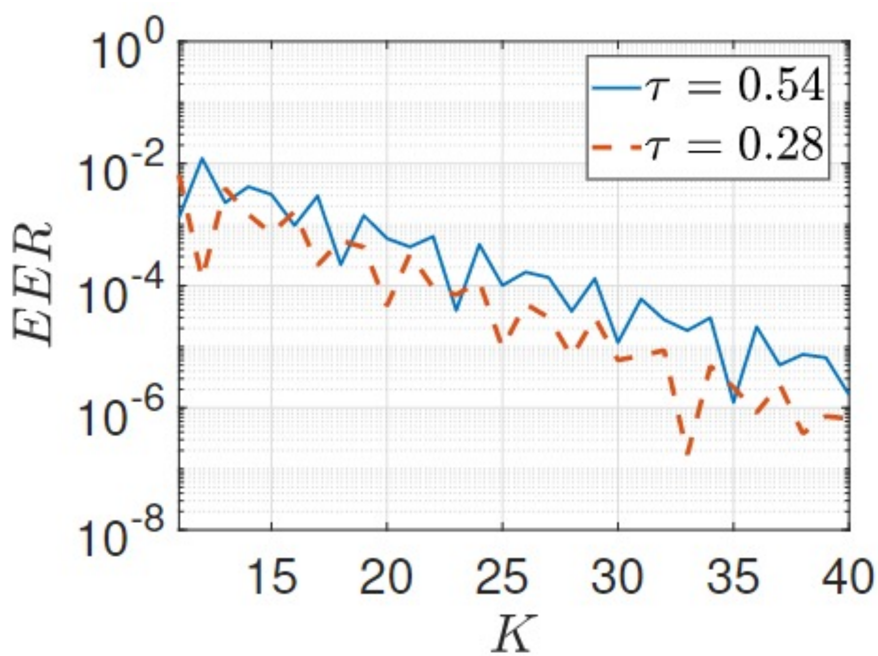
Selecting PoF Test Parameters (2): EER

Notation	Definition
N	Number of samples in subsets Γ_V^k and Γ_C^k
M	Moving average window size
K	Number of RSS subsets, correlation values, and correlation tests
τ	Passing threshold for a single correlation test
α	Fraction of correlation tests to pass *PoF* verification
f_C	Passing rate of a single correlation test achieved by $\mathcal{C}$
F_C	Passing rate of K correlation tests achieved by $\mathcal{C}$

$$F_C = \sum_{x=\lceil \alpha \cdot K \rceil}^{K} \binom{K}{x} {f_C}^x \cdot (1 - f_C)^{K-x}$$

$$F_M = \sum_{x=\lceil \alpha \cdot K \rceil}^{K} \binom{K}{x} {f_M}^x \cdot (1 - f_M)^{K-x}$$

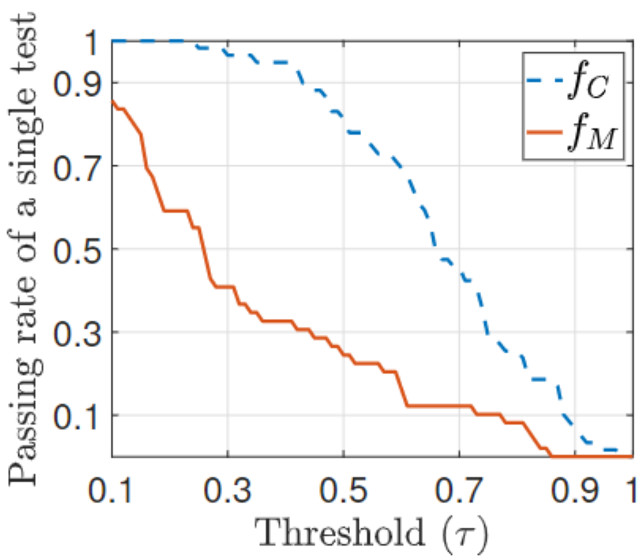
Equal error rate(EER): $1 - F_C = F_M$

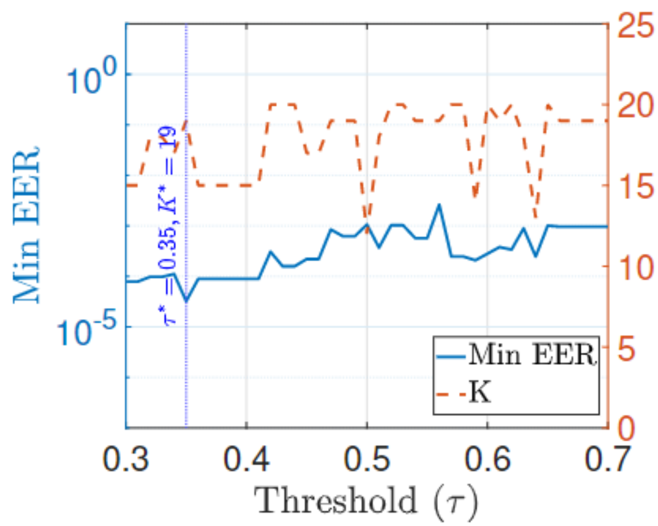


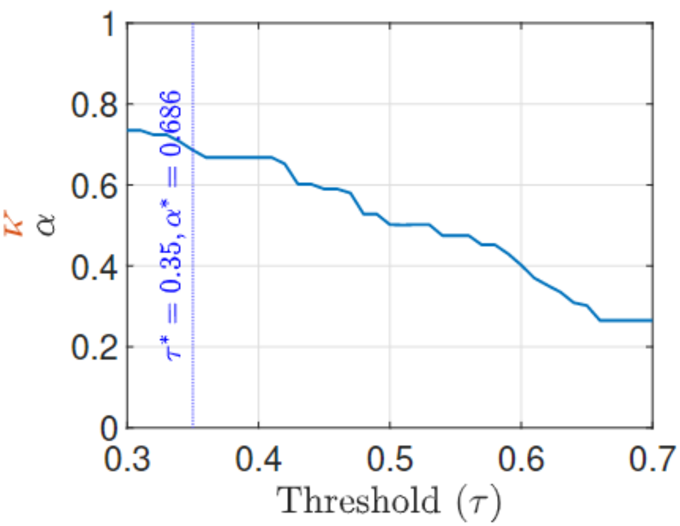
Selecting PoF Test Parameters(3): Exhaustive search

Notation	Definition
N	Number of samples in subsets Γ_V^k and Γ_C^k
M	Moving average window size
K	Number of RSS subsets, correlation values, and correlation tests
τ	Passing threshold for a single correlation test
α	Fraction of correlation tests to pass *PoF* verification

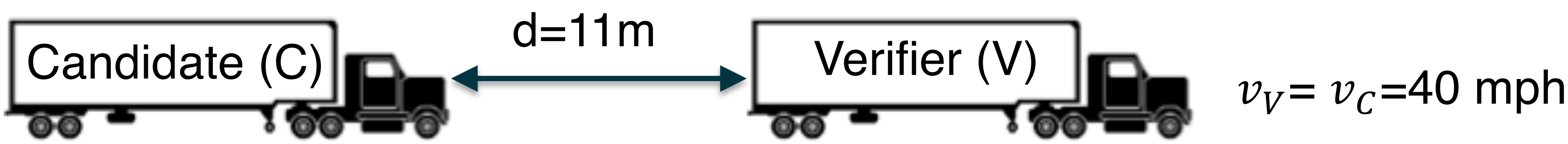
Parameters selected in the urban environment against remote adversary

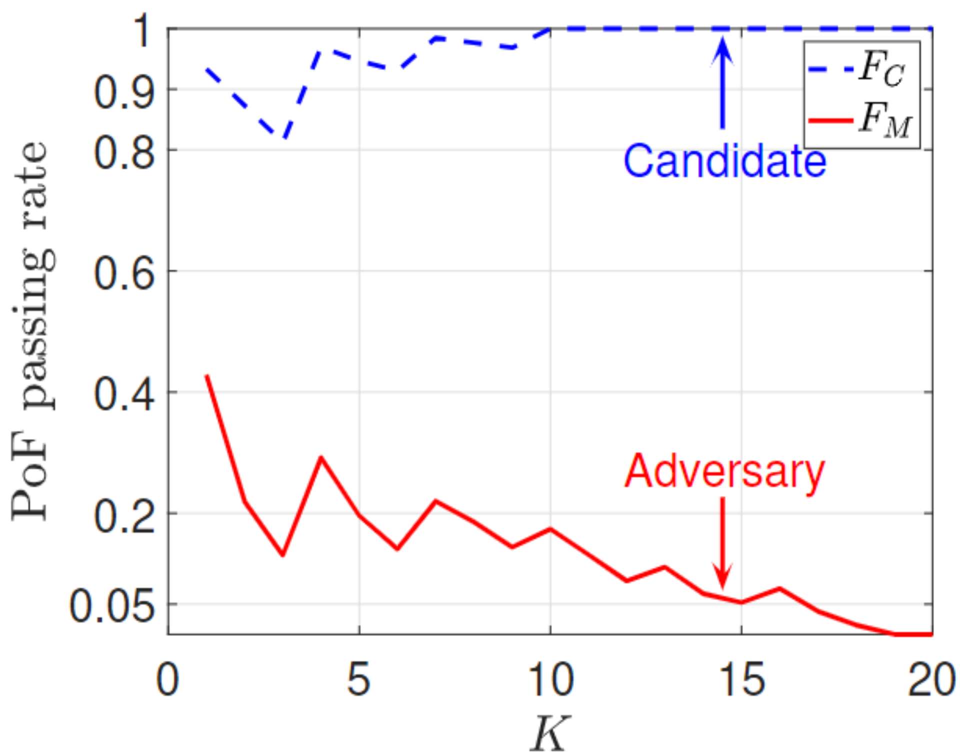




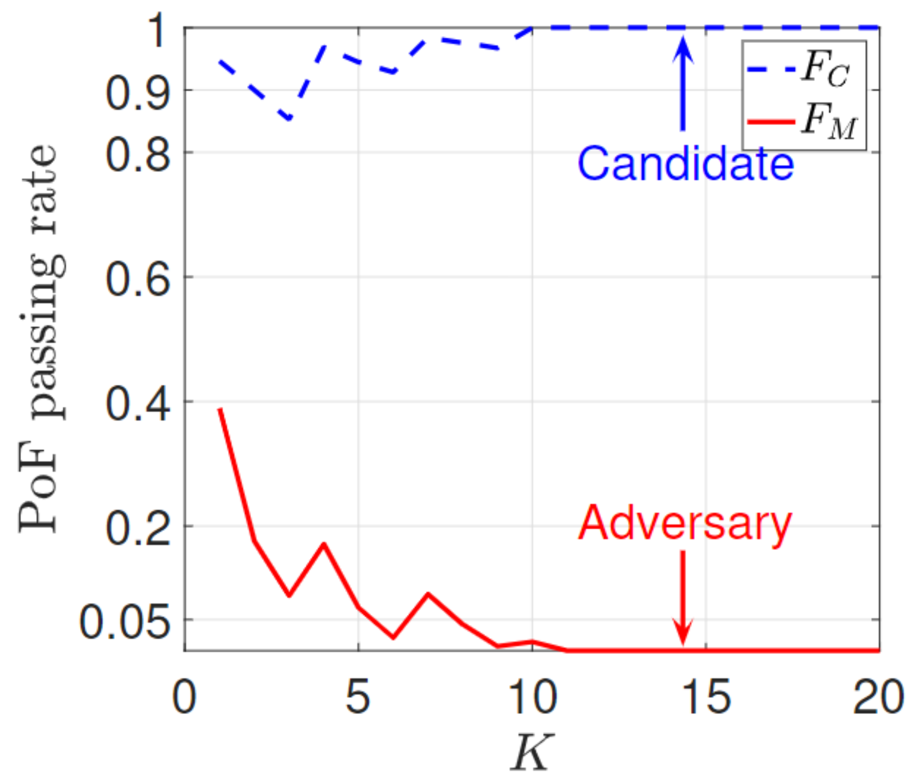


Urban Experiment Results



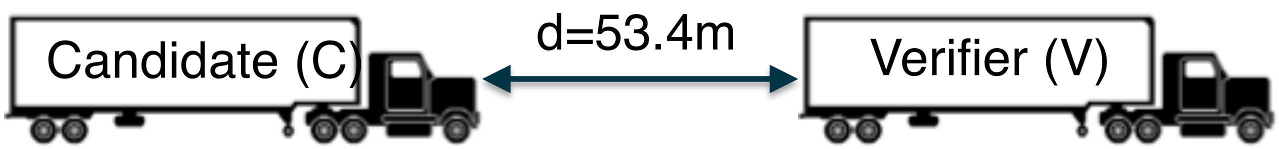


Pre-recording attack

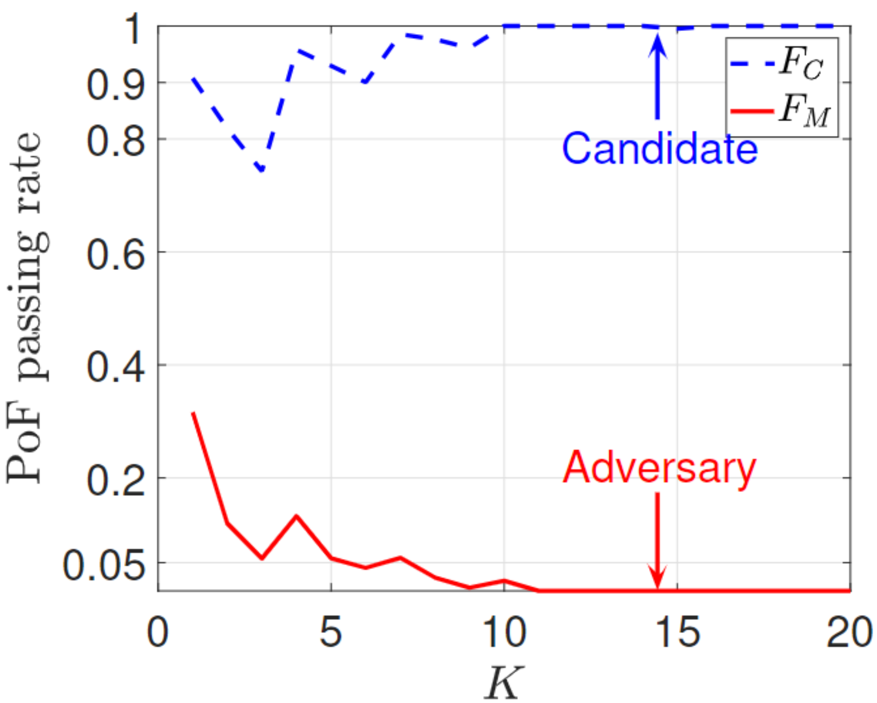


Following-afar adversary

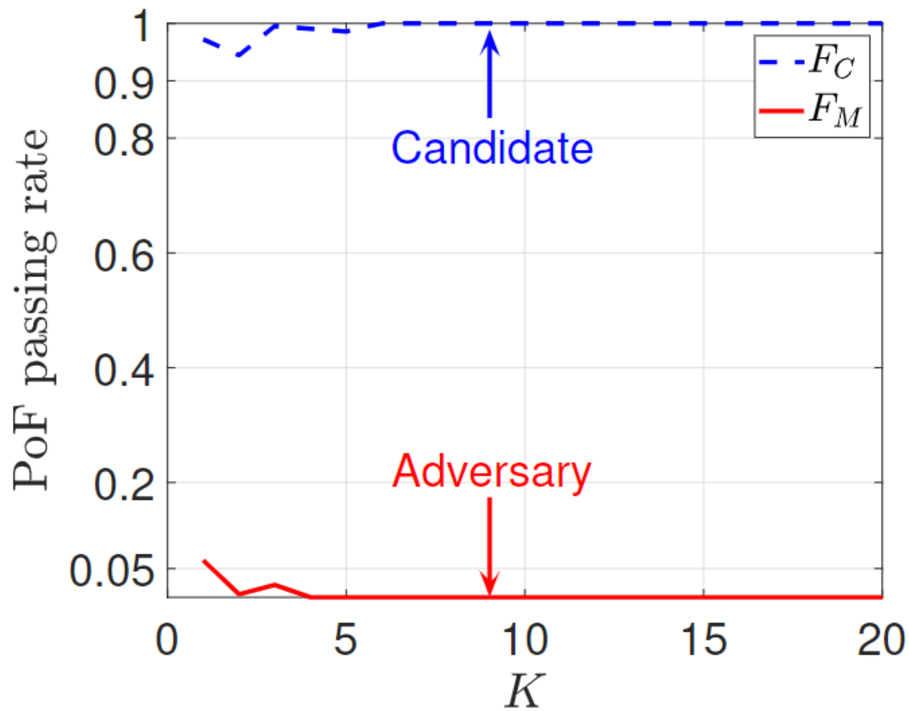
Highway Experiment Results



$v_V = v_C$=60 mph



Pre-recording attack



Following-afar adversary

Lessons Learned

Accurate geotagging and timestamping RF samples can be challenging with off-the-self equipment

Data collection in realistic driving conditions is a tedious process

- Equipment would not always record reliably
- Maintaining constant distance between vehicles without adaptive cruise control
- Surrounding traffic hardens controlling the experiment parameters (but adds realism

Testing the main hypothesis was crucial for further developing the method

Collection of large datasets allowed for fine-tuning test parameters – data was processed and analyzed in different ways