2020 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks

Kyuin Lee University of Wisconsin–Madison
Neil Klingensmith Loyola University Chicago
Dong He University of Wisconsin–Madison
Suman Banerjee University of Wisconsin–Madison
Younghyun Kim University of Wisconsin–Madison

ivPair: Context-Based Fast Intra-Vehicle Device Pairing for Secure Wireless Connectivity

July 8, 2020

Emerging IVI Systems

- **In-vehicle infotainment (IVI) systems utility maximized with user's mobile devices**
- **More sensitive data exchange than conventional car audio**
- **Traffic information, social networking, voice recognition**

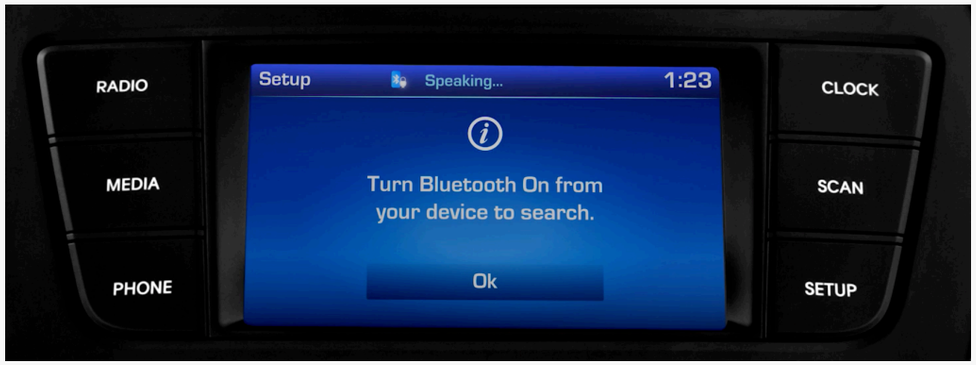
Importance of Secure IVI System

- **Privacy4Cars exploited infotainment systems of several makes via the Bluetooth protocol.**
- **Access stored contacts, call logs, text logs, and full text messages**

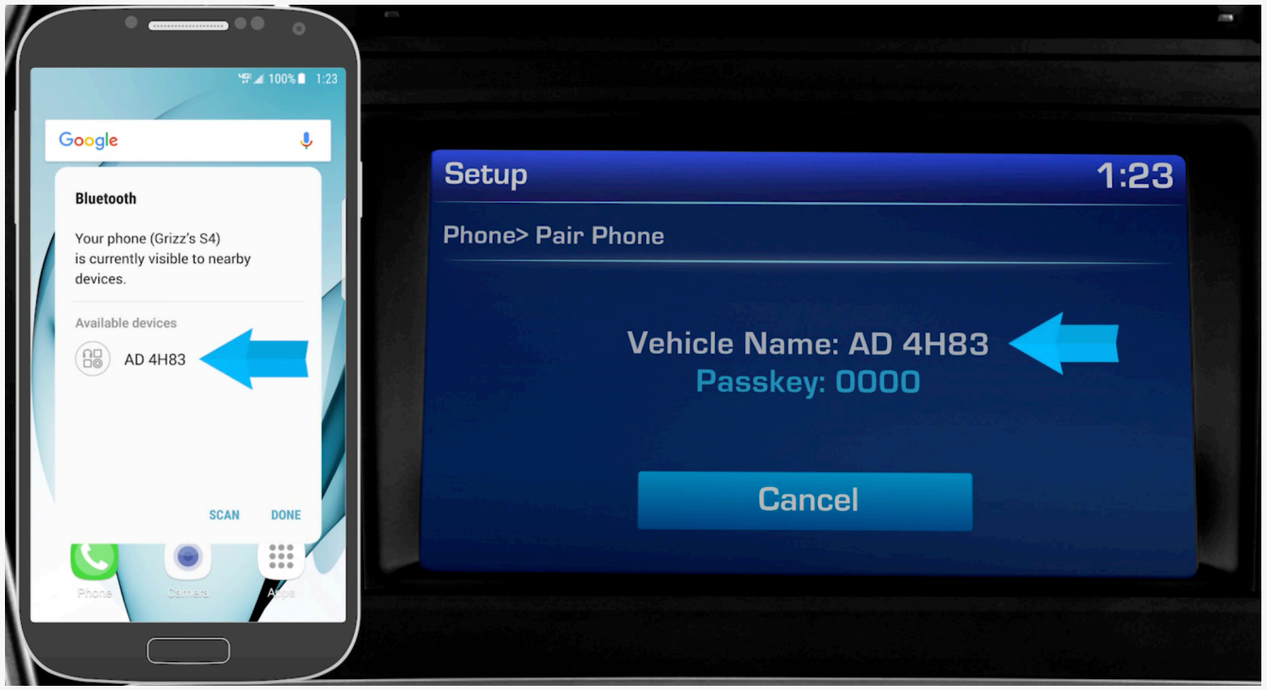
https://www.privacy4cars.com/can-my-car-be-hacked/default.aspx

CarsBlues©

Current IVI Pairing Procedure



1. Turn Bluetooth on and search



2. Passkey generated by the host

3. Confirm or enter the passkey

Goal and Requirement

Goal

Simple pairing process → **Periodic password update**

= **Low security vulnerability**

Requirements

Usability : Minimal or no user involvement

Low overhead : Small footprint and low-cost hardware

Security : Generated key or pin should be local and random

Context-based Pairing and Authentication

- Observing common **random** physical contextual information to generate authentication or pairing key:
  - Devices are in the **same place** at the **same time**
  - Devices belong to the **same user**

RSSI

Audio

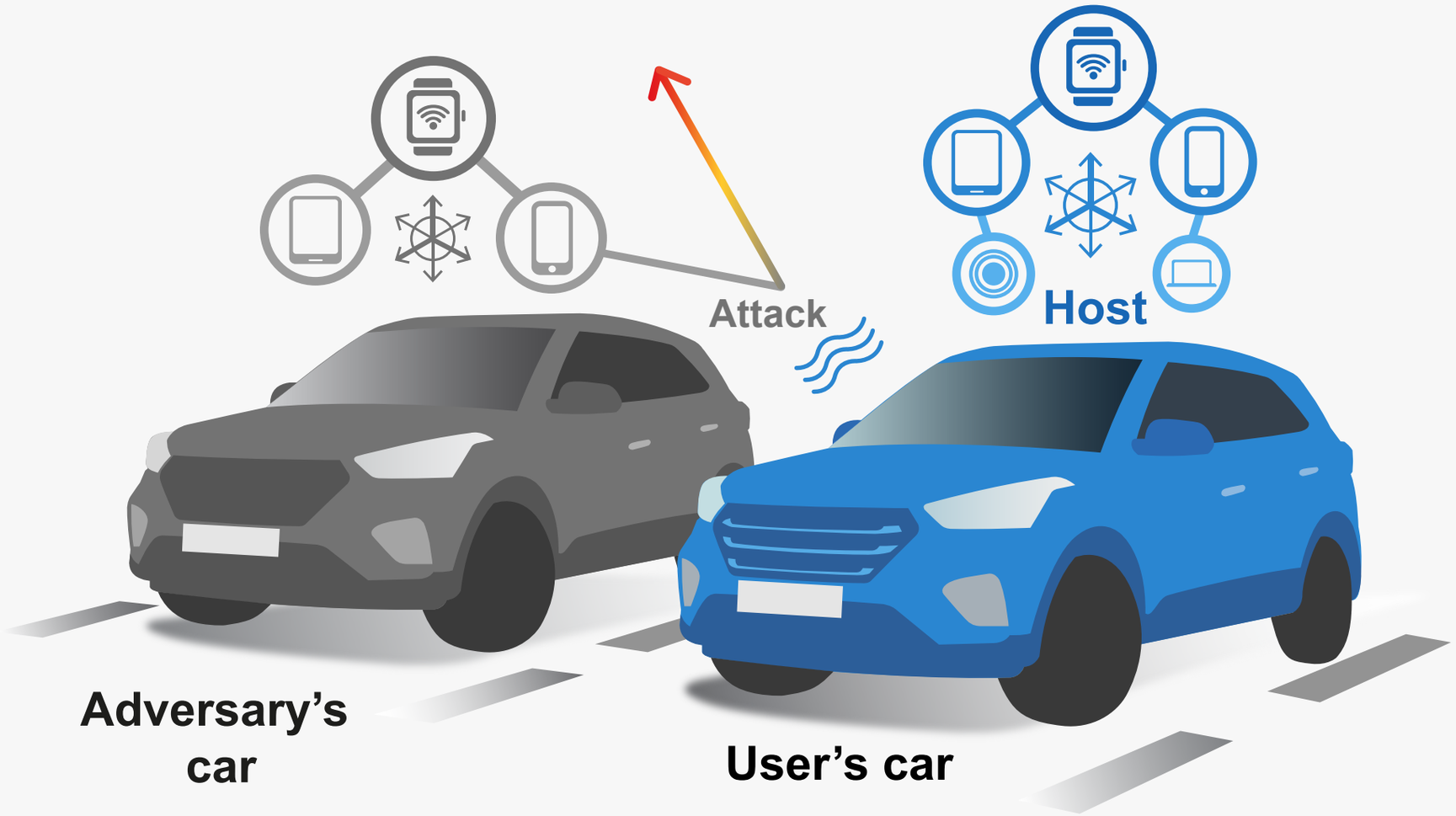
Luminosity

Image

. . .

Eliminates human-involvement during authentication

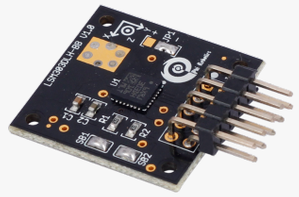
ivPair: Intra-vehicle device pairing

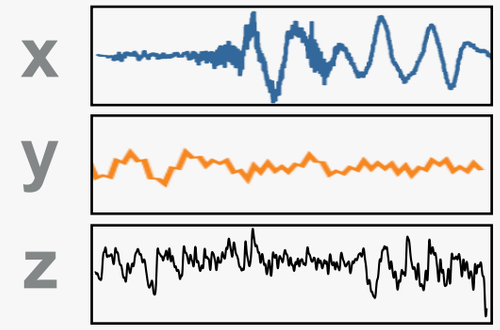


- Protocol to generate authentication pins for devices within the same car using vehicular vibration signal
- Adversary is trying to pair with the legitimate victim's (Host) vehicle or their mobile devices

IVPAIR: INTRA-VEHICLE DEVICE PAIRING

Mobile device



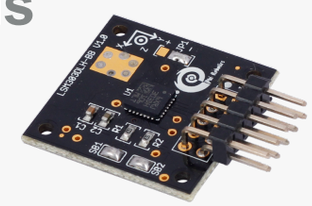


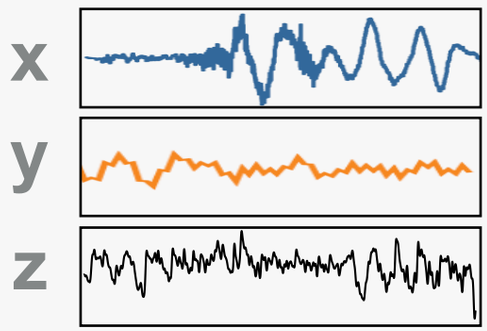
z-axis

acc.

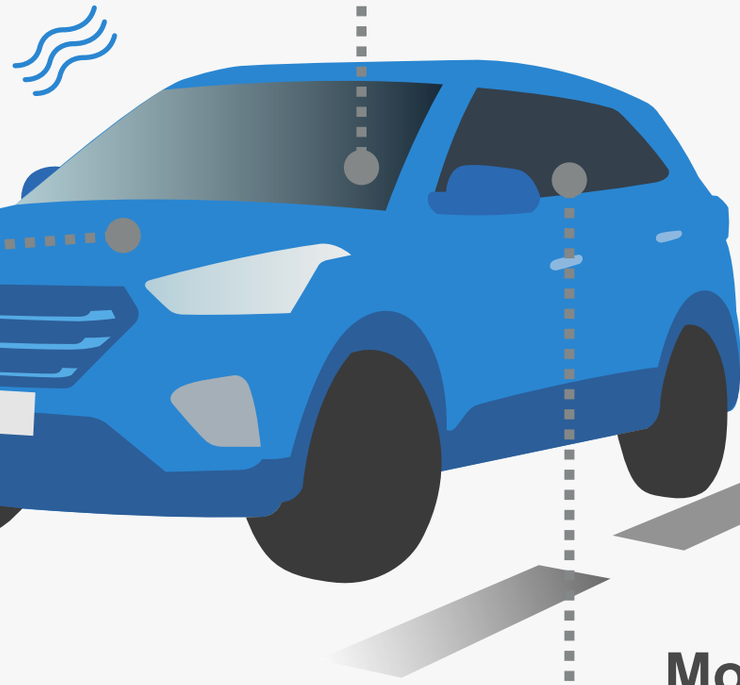
x-axis

y-axis

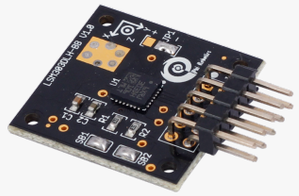


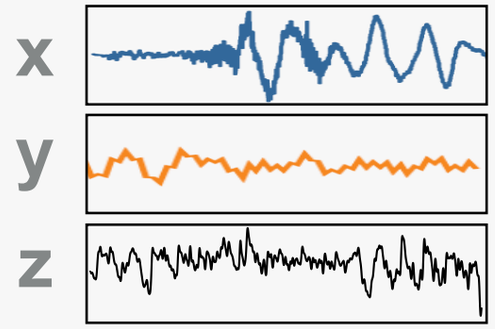


Host

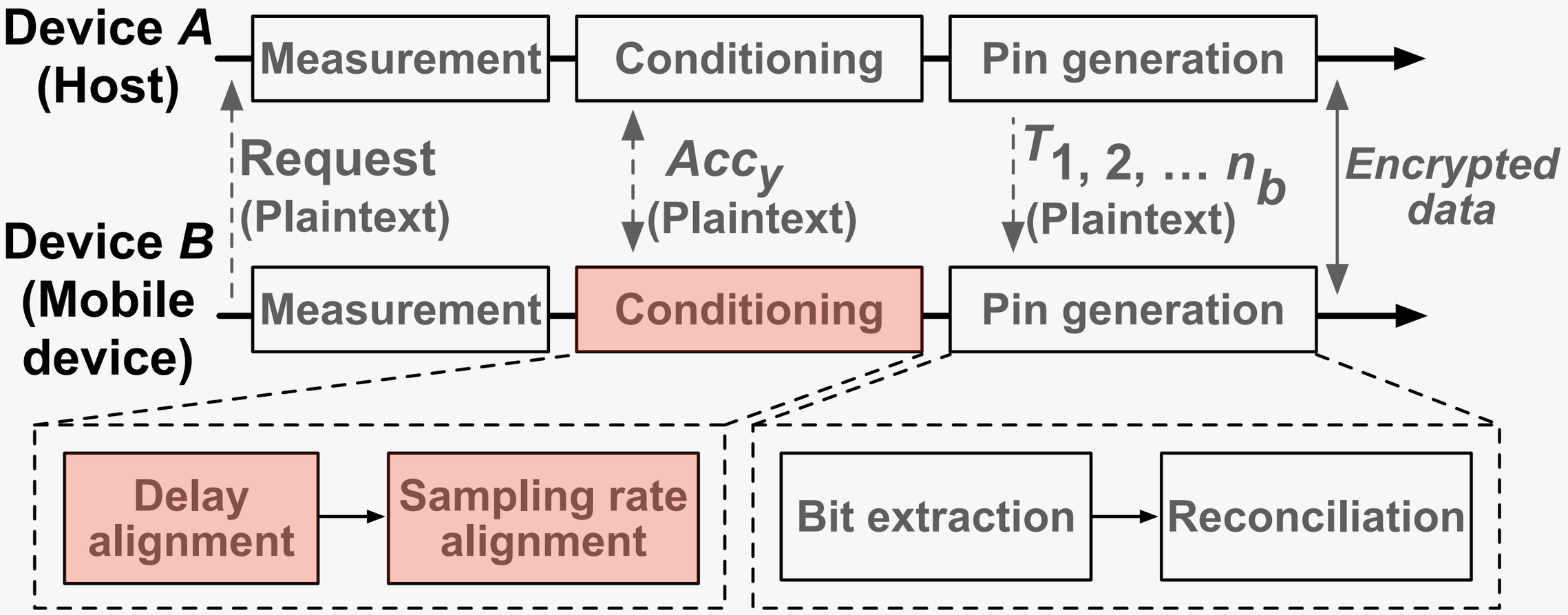


Mobile device

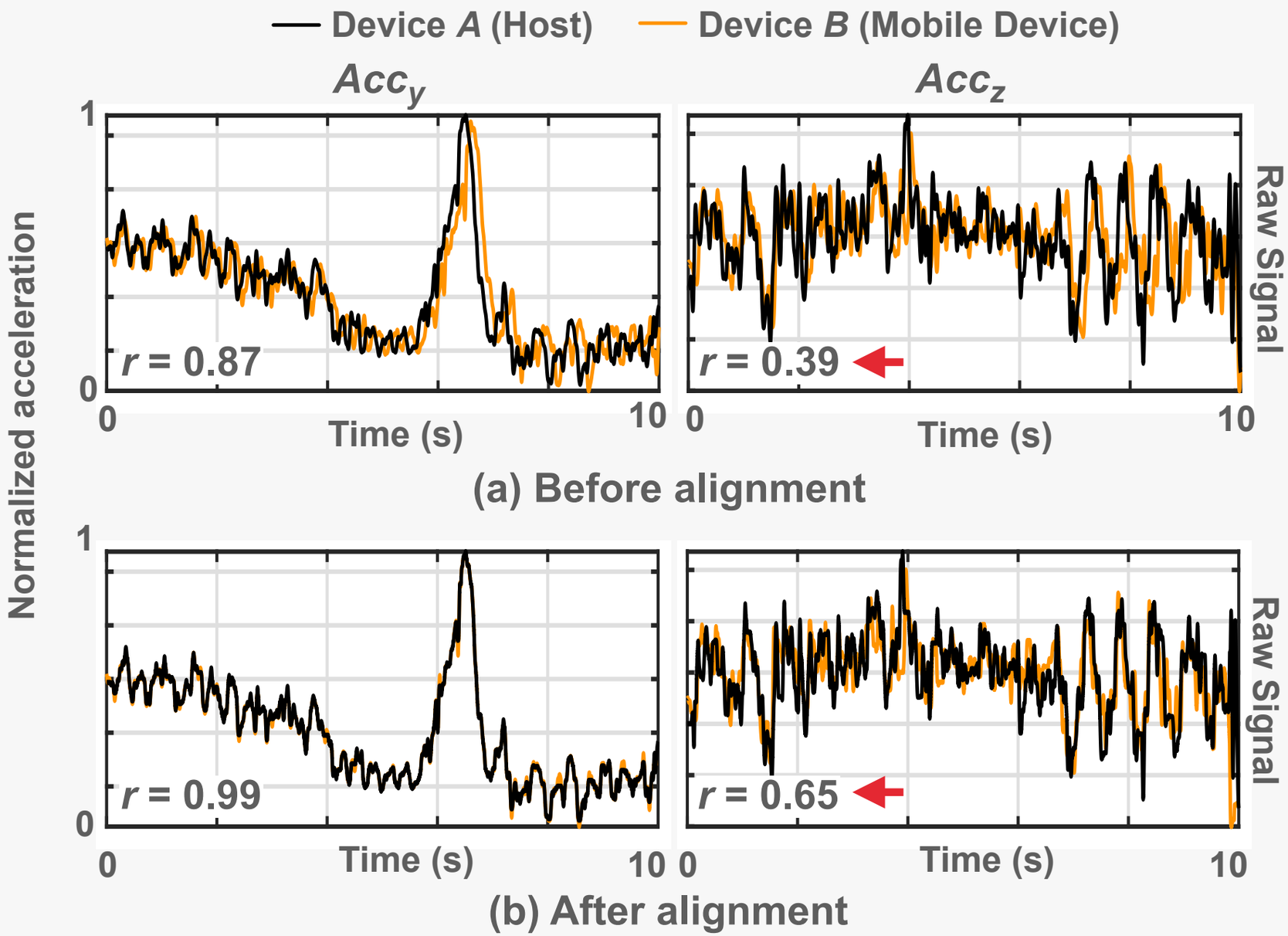




Proposed pairing protocol

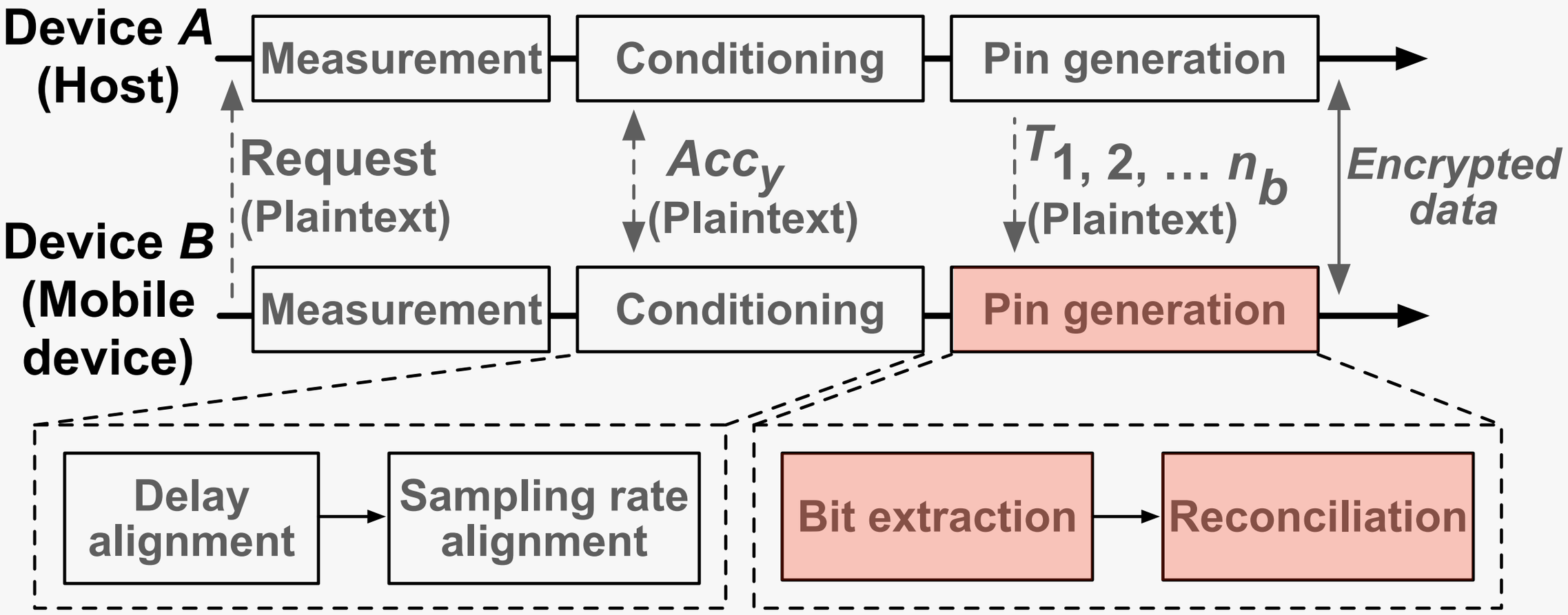


Conditioning Phase

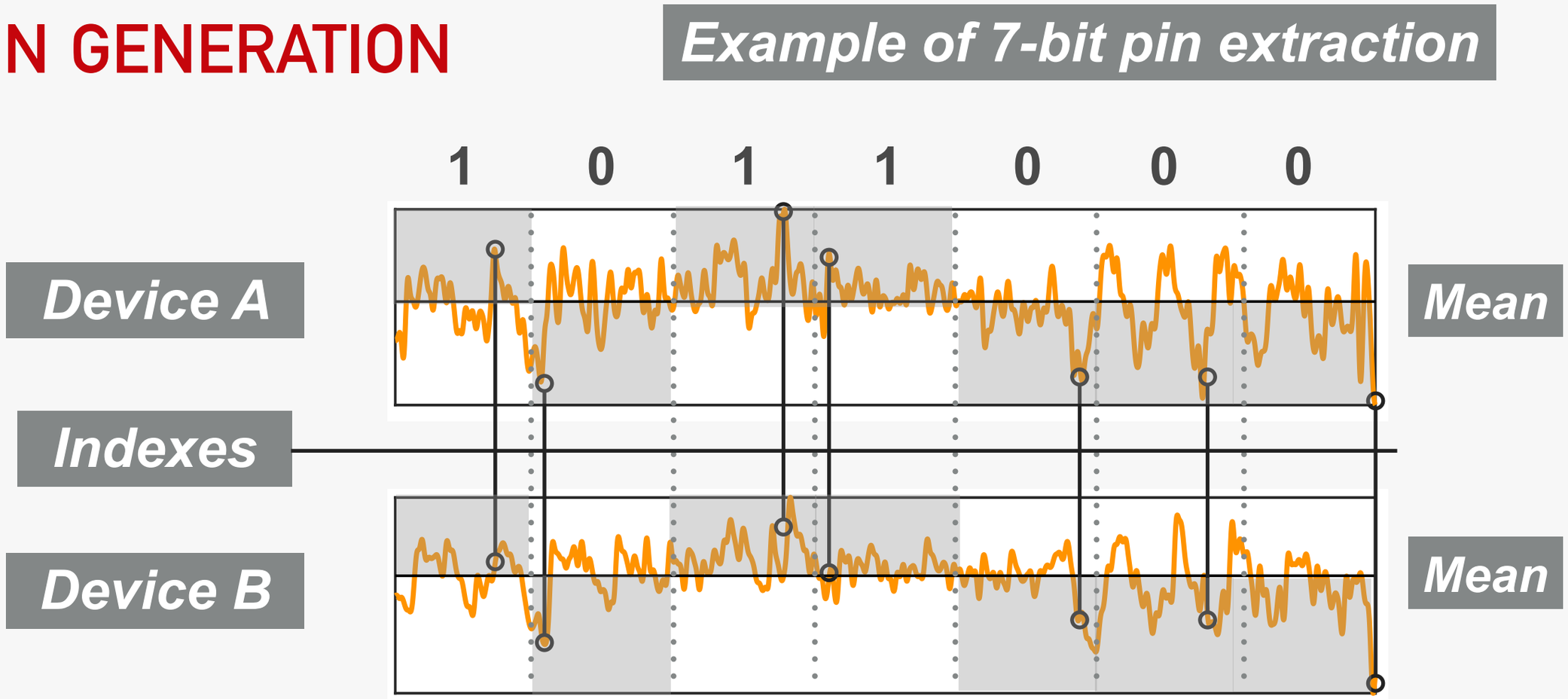


- y-axis acceleration is exchanged between devices to extract warping path using dynamic time warping (DTW)
- Warping path applied on z-axis
- z-axis used for pin extraction

Pin generation



PIN GENERATION



- Pin generation
    1. Device A divides its fingerprint into *7* bins
    2. If index of maximum absolute value within the bin is greater than mean of bin, bit **1**. Else, bit **0**.
    3. Indexes are transferred to Device B for same procedure
- Error correction is based on Hamming(*n,k)* correction scheme

Evaluation setup and metrics

- Hardware
    - Arduino UNO with ADXL345 MEMS accelerometer
    - Sampling frequency of **800 Hz**
- Pairing pin length: **14-bit**
- Signal measure time: **10 s**
- Hamming (7,4) error correction scheme
- Metric
    - *Bit agreement rate*: bit-wise comparison rate
    - *Success rate*: rate of 100% matching pins

Driving Environment

Vehicle type

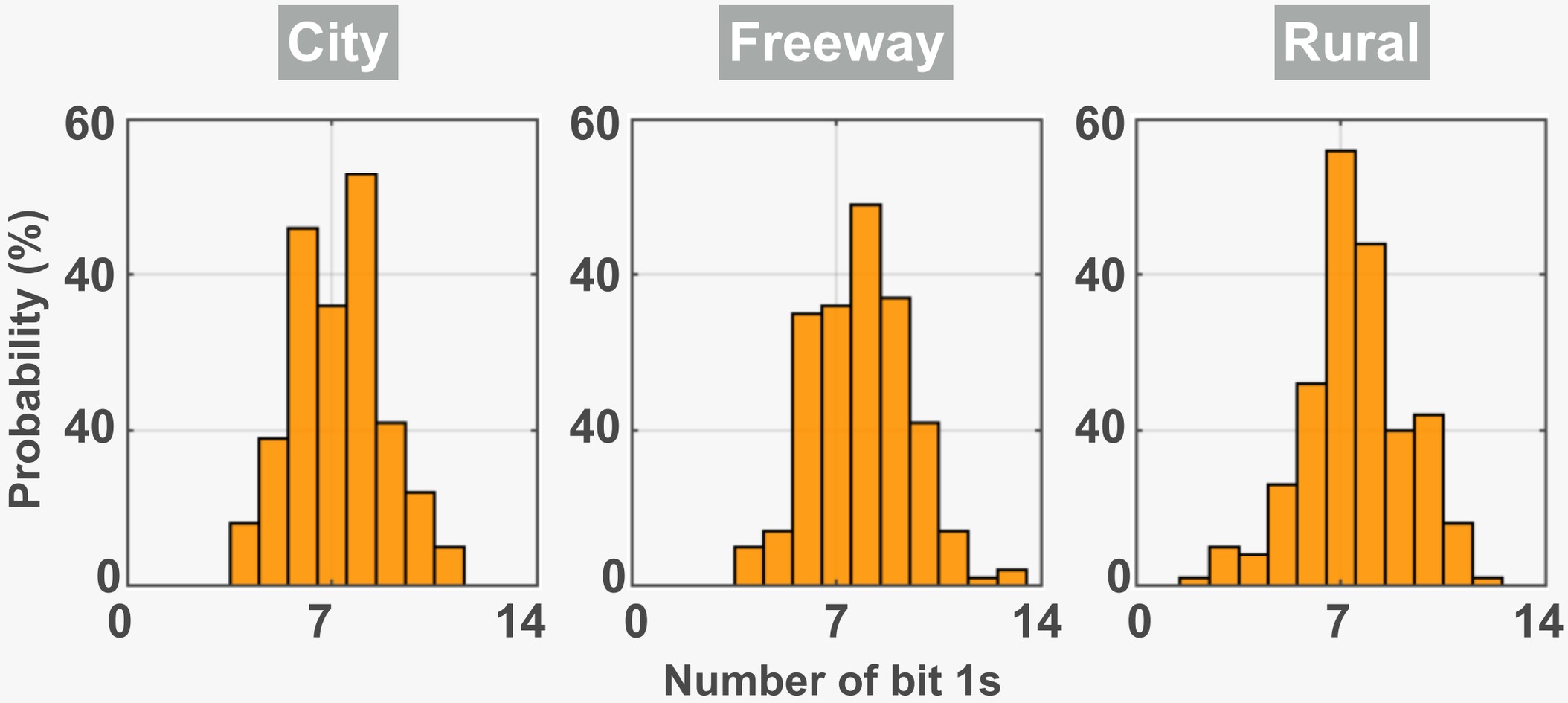
Sport utility vehicle (SUV)

Sedan

Road type

Madison, WI

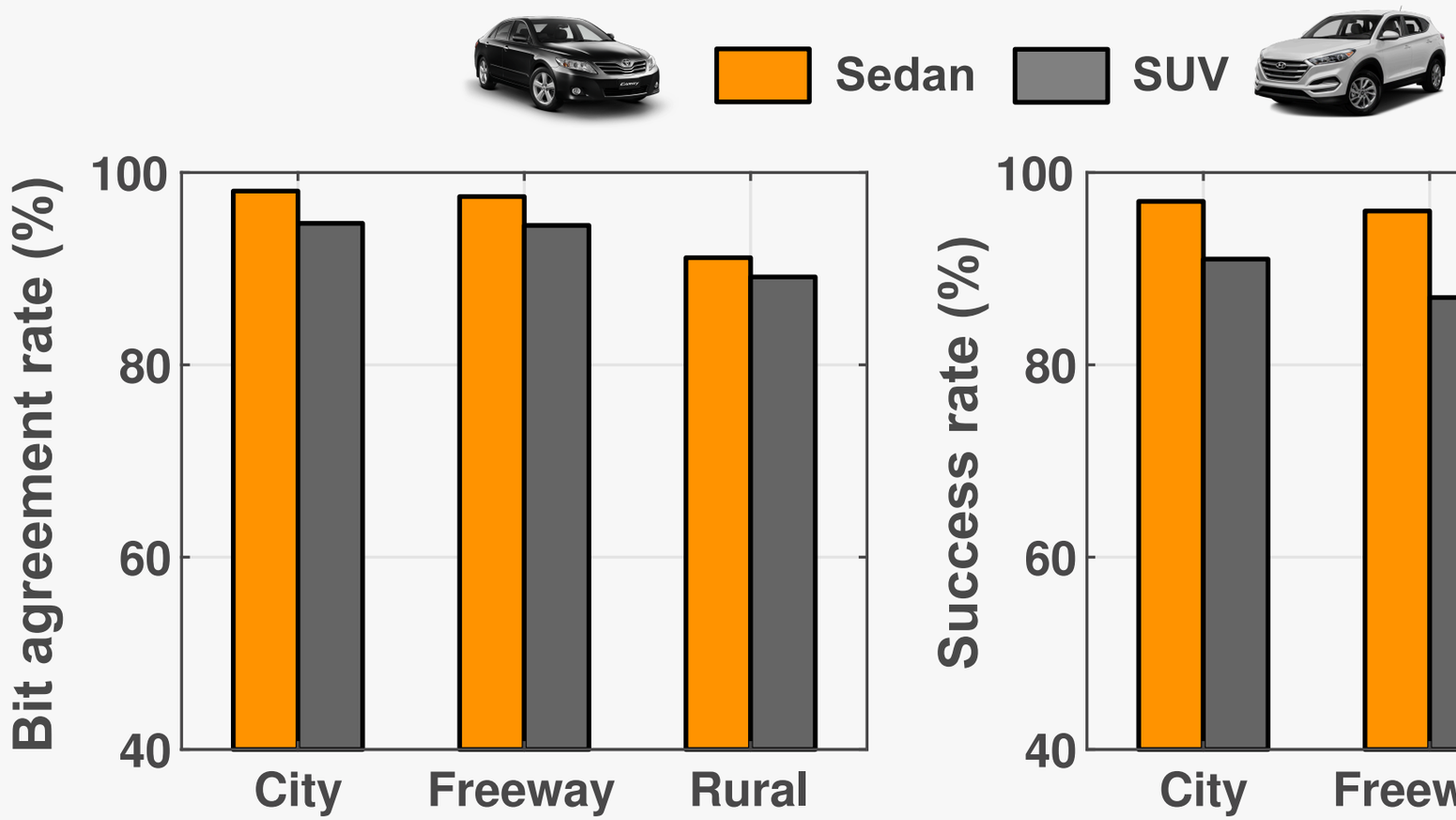
BIT RANDOMNESS



- Number of bit 1s in 14-bit pin
- Ideal number should be 7 (50%)

Exhibit binomial distribution under different road conditions

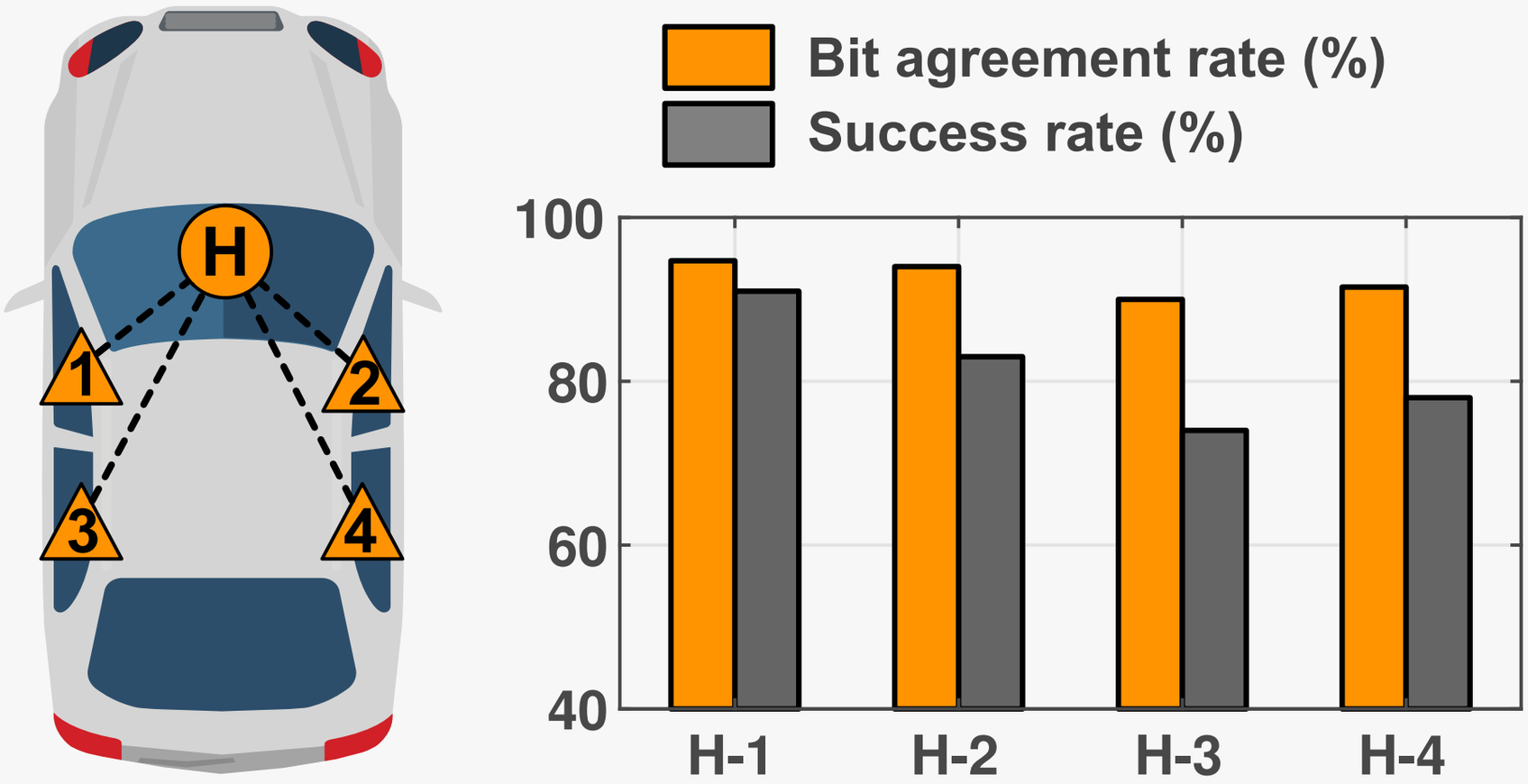
VEHICLE AND ROAD TYPES



- One device fixed to driver side door panel
- On each road type, 100 pairing requests are attempted

Above 85% success rate on city and freeway

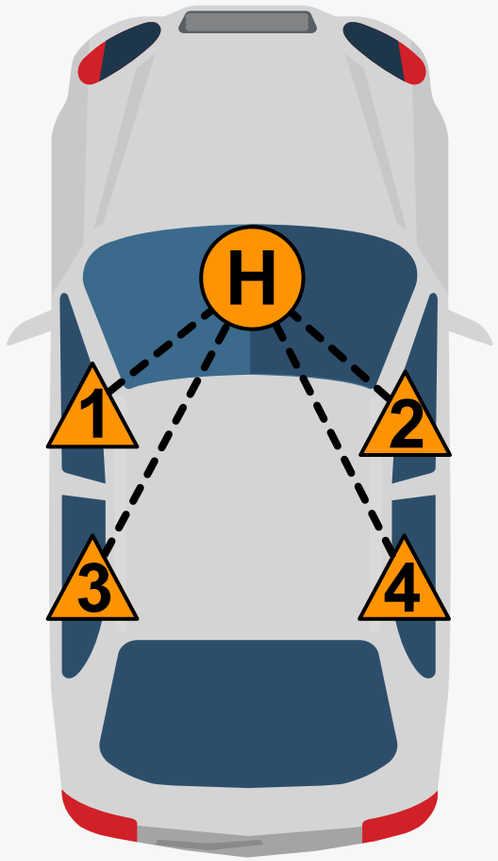
Device locations



- Each location pairs attempts 100 pairing requests

Above 85% success rate on average in all locations

Device locations

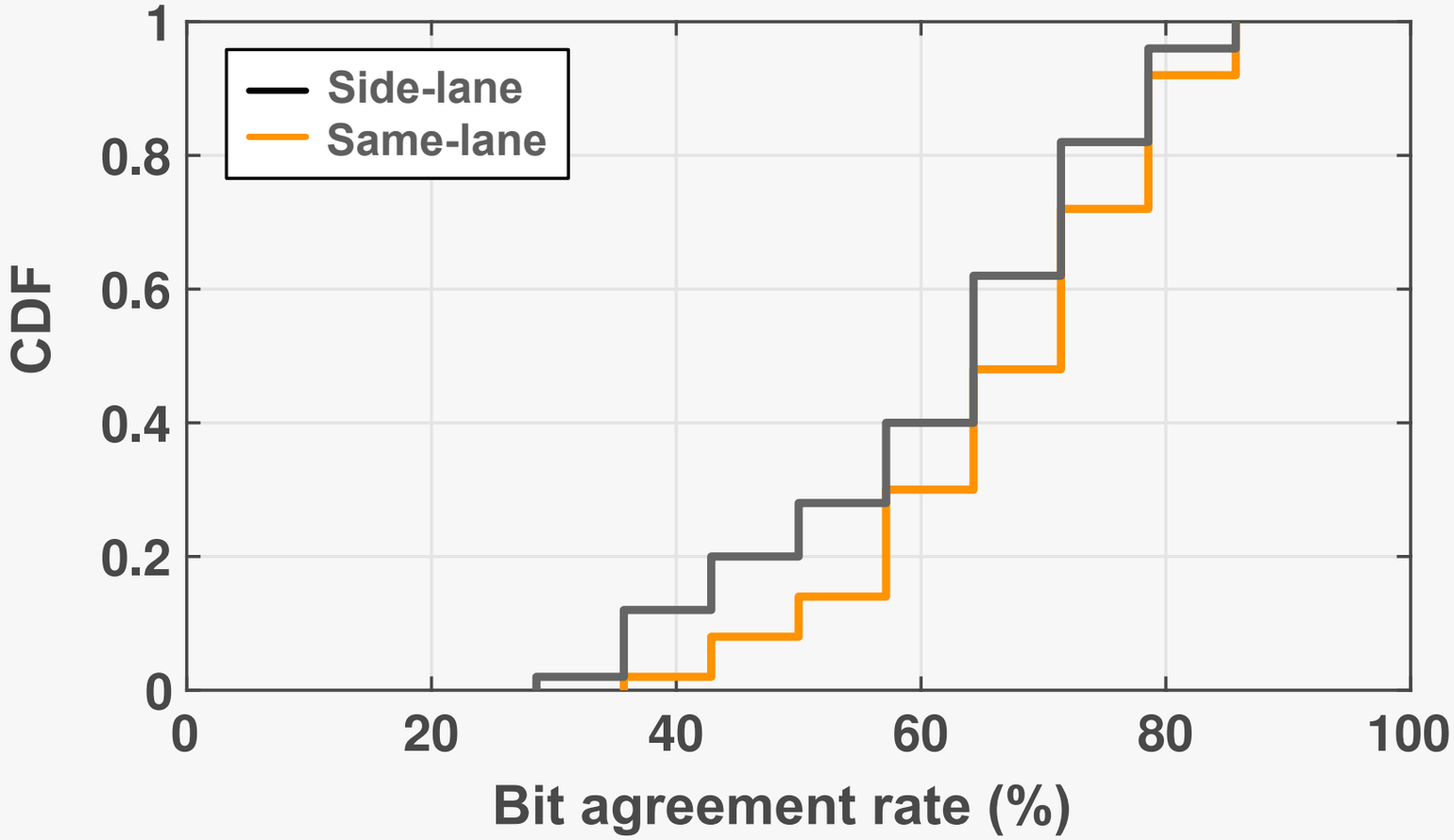


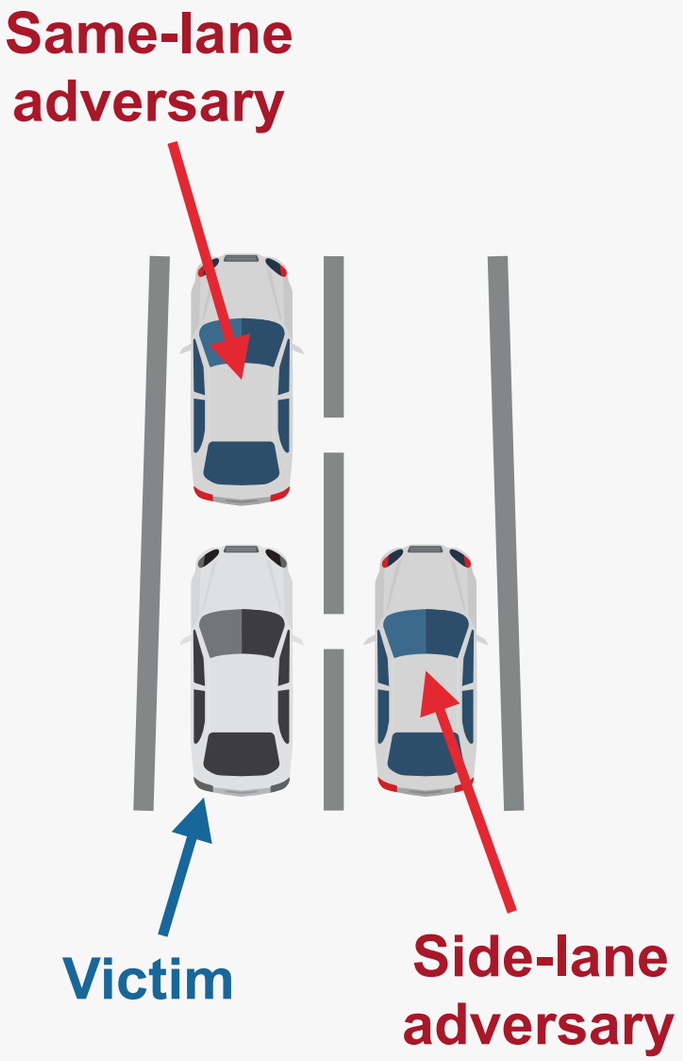
Device Pair	Correlation coe.	Expected Time
Host - 1	0.11 → 0.79	11.0 s
Host - 2	0.06 → 0.78	12.0 s
Host - 3	0.32 → 0.65	13.5 s
Host - 4	0.09 → 0.61	12.8 s

- **Expected pairing time: inversely proportional to the success rate times duration of measurement (10 s)**

Less than 14 s pairing time from any passenger location

Adversarial Scenarios

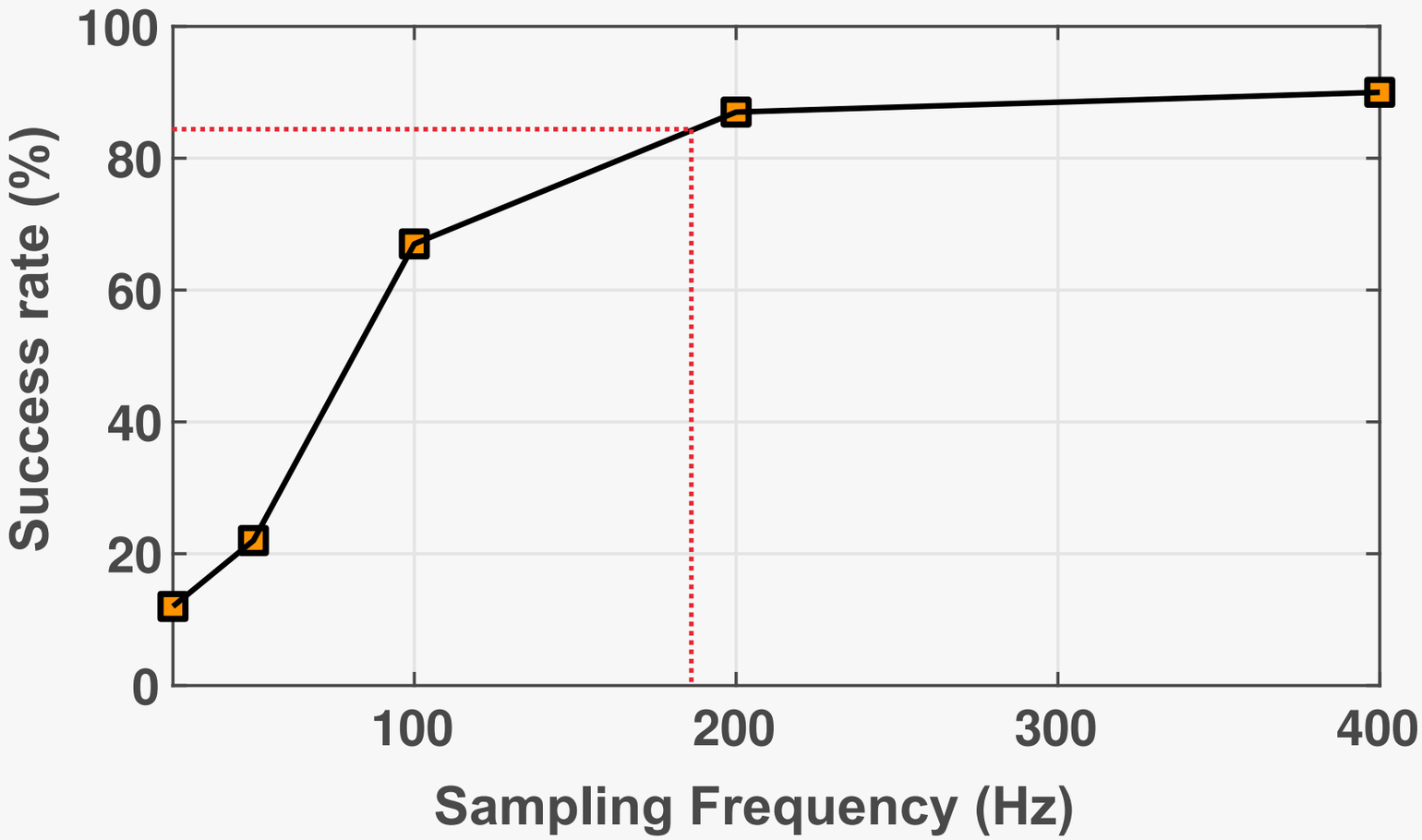




- Side-lane: adversary driving in next lane as victim vehicle
- Same-lane: adversary driving in front of victim vehicle

None of the attacks were successful

Minimum Sampling Rate



- Downsample fingerprints from 800 Hz to 25 Hz
- Sampling rate above 200 Hz maintains high success rate

Above 170 Hz sampling rate to maintain 85% success rate

Computational Overhead

- The main computation overhead of ivPair
    - Dynamic-time warping (DTW)
- Android application on LG Nexus 5X (Android 5.0)
    - Mid-range smartphone with 1.8 GHz processor
- Compute warping path of two time-series of 8,000 samples (10 s long fingerprint)

Computing alignment path takes only 546 ms

Conclusion

- Context based pairing method based on vehicular vibration context
- IVPair removes hassle of manual pairing procedure in vehicular scenario
  - Safe and usable for drivers and passengers
- Expected pairing time is around 11 s for 14-bit pairing pin

Key Features of IVPair

- **Usability** : Simple contact action from user
- **Low overhead** : Accelerometers are ubiquitously available
- **Security** : Context-based authentication pins