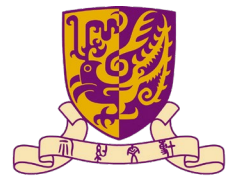
Wave-for-Safe: Multisensor-based Mutual Authentication for Unmanned Delivery Vehicle Services

Huanqi Yang[1], Mingda Han[1], Shuyao Shi[2], Zhenyu Yan[2], Guoliang Xing[2], Jianping Wang[1] , Weitao Xu[1]

[1]City University of Hong Kong

[2]The Chinese University of Hong Kong



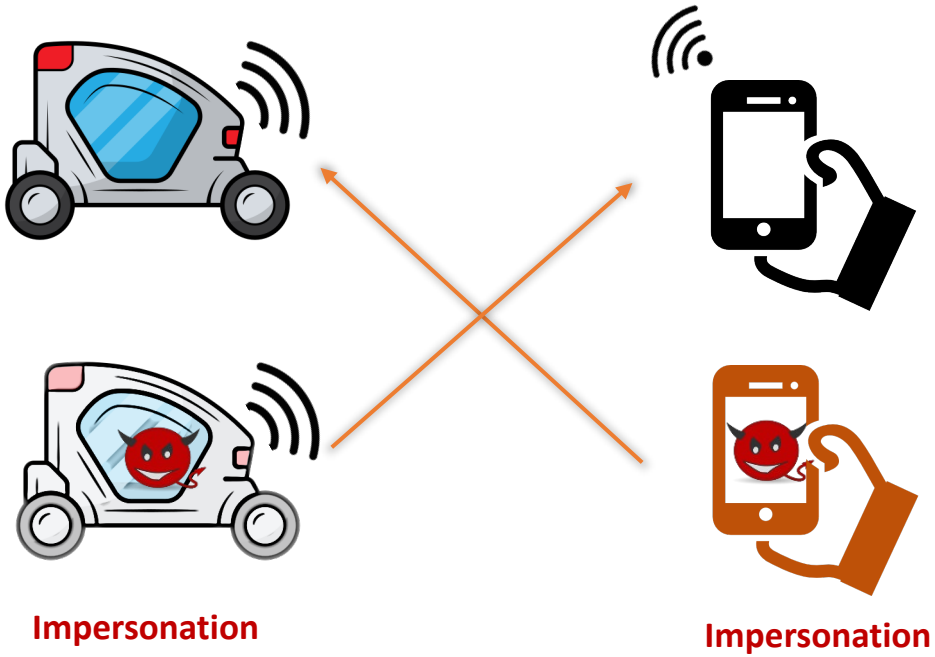
香港中文大學
The Chinese University of Hong Kong

Background

❑ Self-driving delivery car service

- ❖ Revolutionize last-mile delivery in a more sustainable and cost-effective way.
- ❖ The market is estimated to exceed $90.21 billion by 2030.
- ❖ It is critical to ensure package security.

Applications



Impersonation attack

Background

❑ Existing authentication solutions

- ❖ Biometric-based method
- ❖ QR code-based method
- ❖ Password-based access
- ❖ Distance-bounding authentication

❑ Design targets

- ❖ T1: no need for additional hardware
- ❖ T2: mutual authentication
- ❖ T3: being resistant to common attacks
- ❖ T4: no user privacy leakage risks

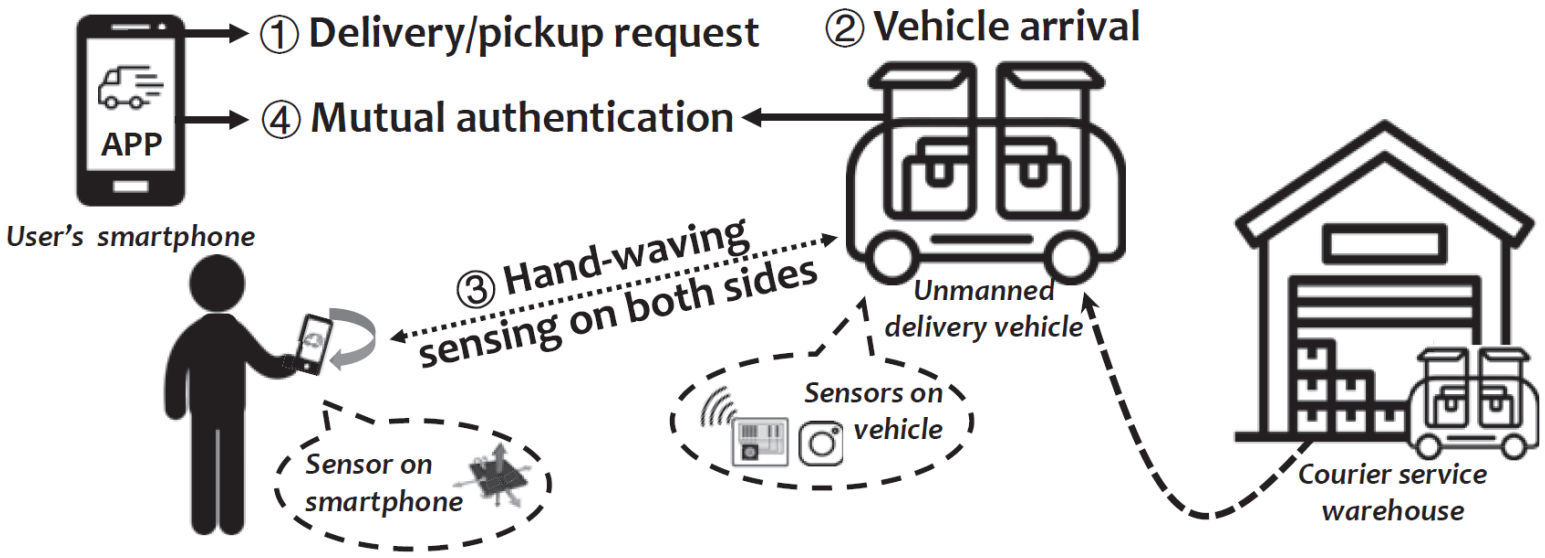
Table 1: Comparison with existing approaches.

Approaches	T1	T2	T3	T4
Biometric [26, 46]	✔	✖	✖	✖
QR code [18]	✔	✖	✖	✔
Password [8, 25]	✔	✖	✖	✔
Distance-bounding [28]	✖	✔	✖	✔
W4S	✔	✔	✔	✔

Our solution

❑ Wave-for-Safe: Multisensor-based Mutual Authentication

- ❖ W4S uses random hand-waving by the legitimate user to achieve robust authentication by obtaining highly correlated sensory data.
- ❖ W4S satisfies all four targets.



Our solution

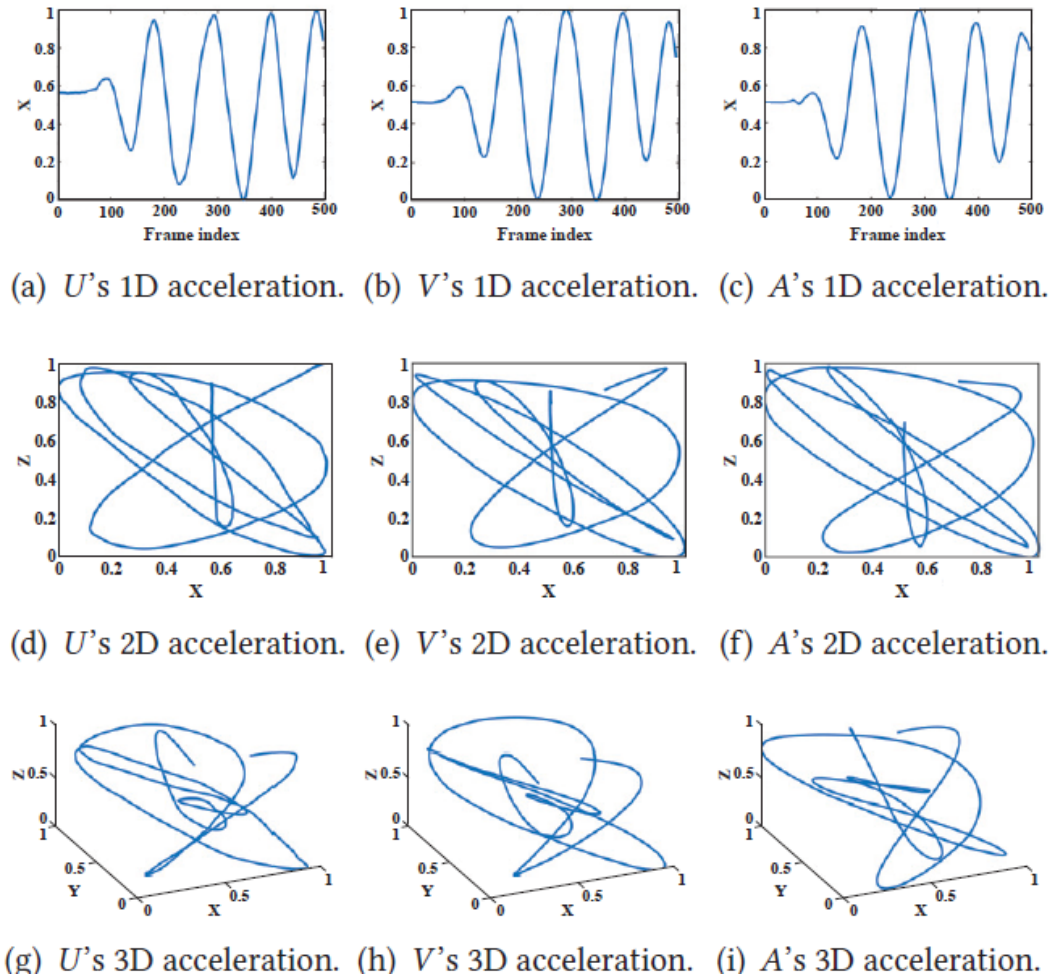
❑ Design choices

- ❖ Sensors: IMU, mmWave radar, and camera
- ❖ Metrics: 3D acceleration

❑ Feasibility

- ❖ The correlation of A-U or A-V is always lower than that of V-U irrespective of the dimension of acceleration used.
- ❖ Using 3D acceleration is more secure than using 1D or 2D acceleration.

(Note: A refers to Attacker, V refers to Vehicle, U refers to User)



(a) U's 1D acceleration. (b) V's 1D acceleration. (c) A's 1D acceleration.

(d) U's 2D acceleration. (e) V's 2D acceleration. (f) A's 2D acceleration.

(g) U's 3D acceleration. (h) V's 3D acceleration. (i) A's 3D acceleration.

1/2D acceleration vs. 3D acceleration.

Challenges

❑ Accurate sensing

- ❖ Designing algorithms for accurate 3D acceleration extraction from diverse sensors amid noise interference.

❑ Synchronization

- ❖ Synchronization: Establishing time and spatial synchronization between the unmanned vehicle and user's smartphone for accurate sensory data matching.

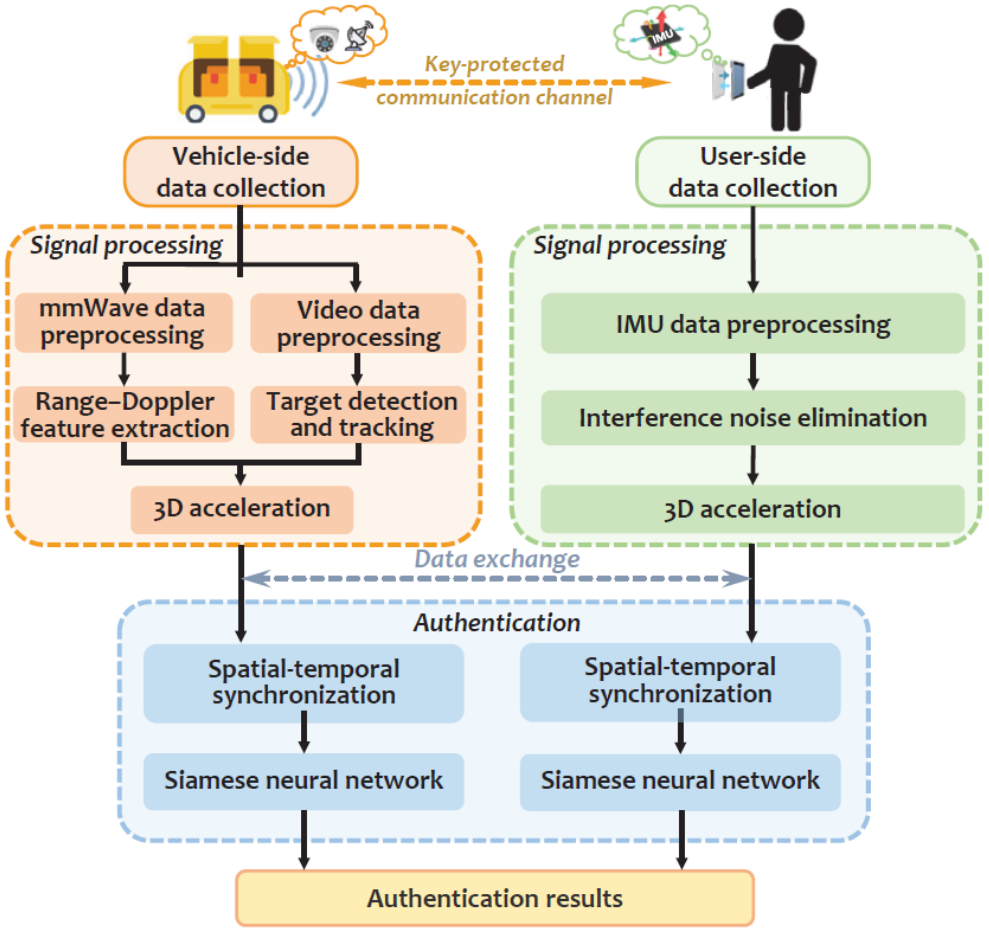
❑ Authentication

- ❖ Developing a fine-grained discrimination method for authentication, as the correlation coefficient alone is insufficient for distinguishing between a legitimate user and an attacker.

System overview

❑ **Step1: Order and communication:**

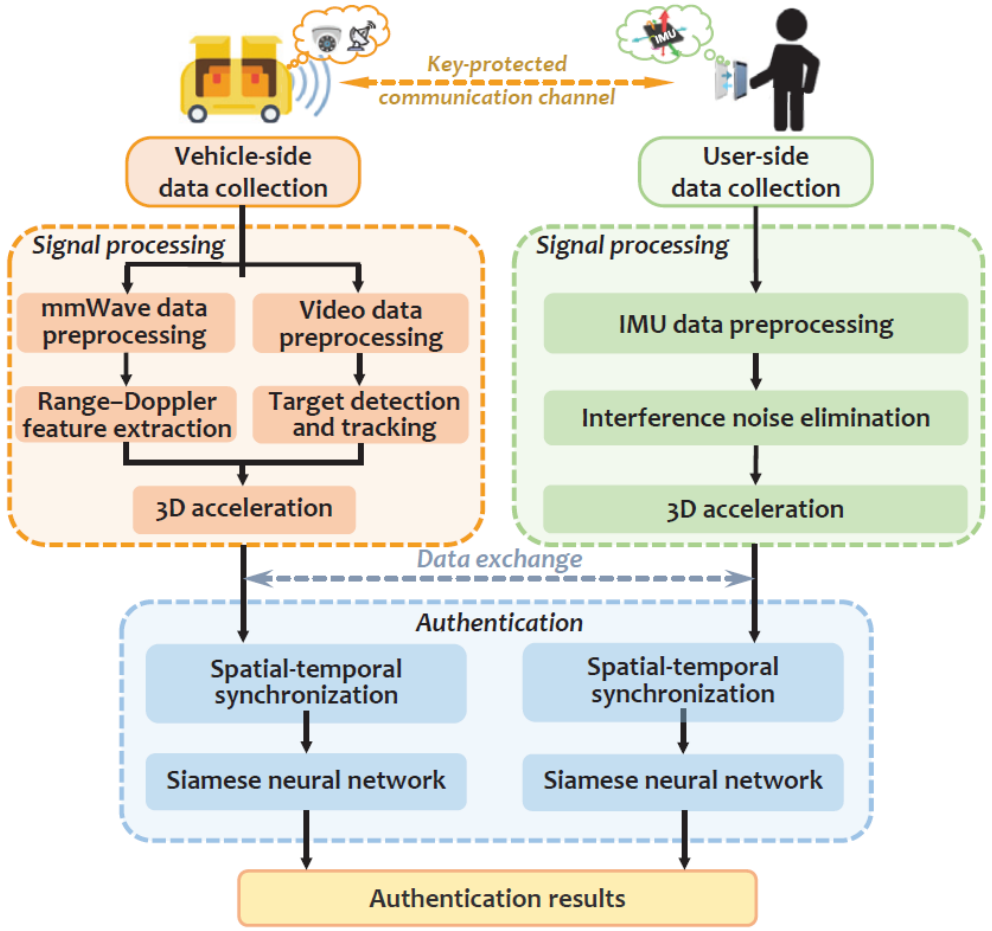
- ❖ User places a delivery/pickup order using the delivery app.
- ❖ The unmanned vehicle arrives at the designated location.
- ❖ A key-protected communication channel is established between the vehicle and the smartphone.
- ❖ The vehicle sends a start notification to the smartphone and activates its mmWave radar and camera.



Overview

System overview

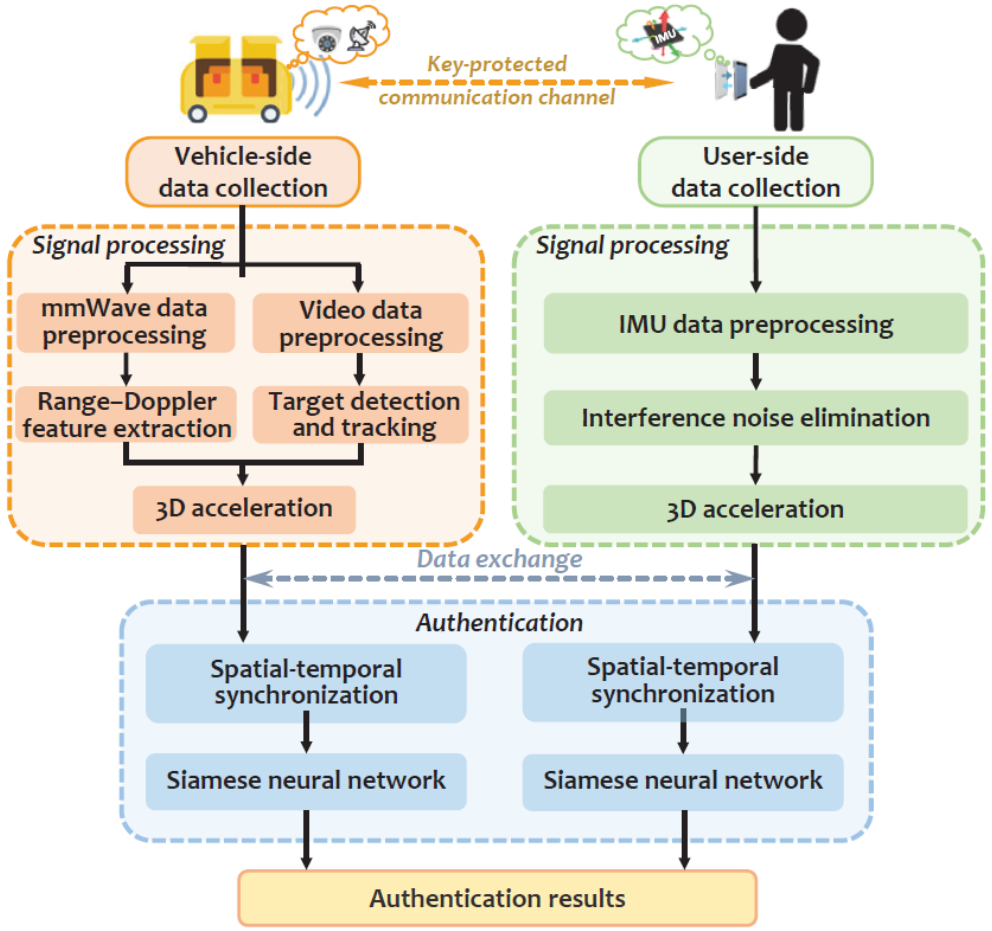
- **Step2: Hand-waving:**
  - On receiving the start notification, the smartphone generates a vibration to prompt the user to start hand-waving.
  - The smartphone collects data through the built-in IMU for a specified time duration (t).
  - After data collection, the smartphone generates another vibration to prompt the user to stop waving.
  - The smartphone then sends a stop notification to the vehicle.



Overview

System overview

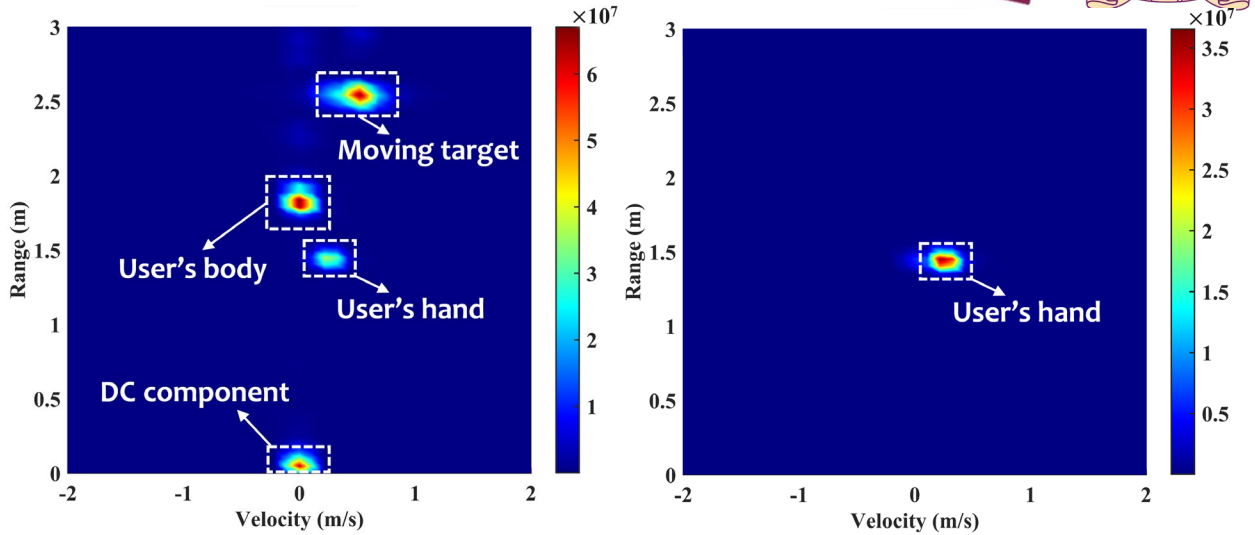
- **Step3: Authentication and delivery:**
  - The hand-waving data sensed by the smartphone and the vehicle is exchanged after local processing.
  - An authentication decision is made independently on both sides.
  - If the authentication is successful on both sides, the package delivery is executed.
  - If the authentication is not successful, the process returns to step 2 (hand-waving).
  - This retry loop continues until the maximum number of attempts is reached.



Overview

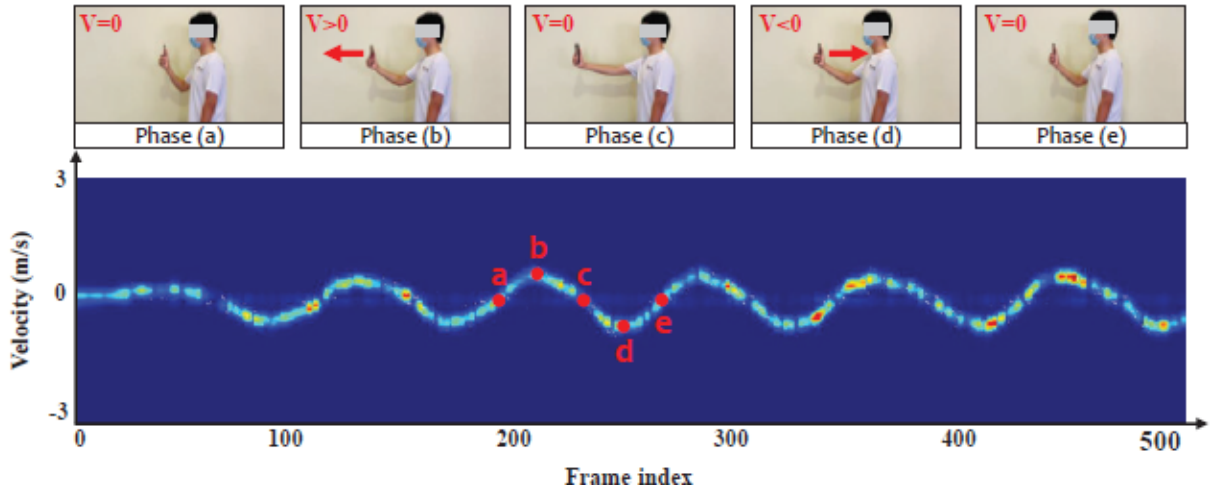
System design

- **Signal processing vehicle-side:**
  - **RDM Generation:** Generate Range-Doppler Maps from raw mmWave data.
  - **Noise Reduction:** Apply mean values of each RDM along the slow time dimension for static noise elimination.
  - **Acceleration Acquisition:** Convert all RDMs to one time-velocity map and derive acceleration by taking the velocity's derivative.



(a) Raw RDM. (b) Denoised RDM.

mmWave noise reduction.

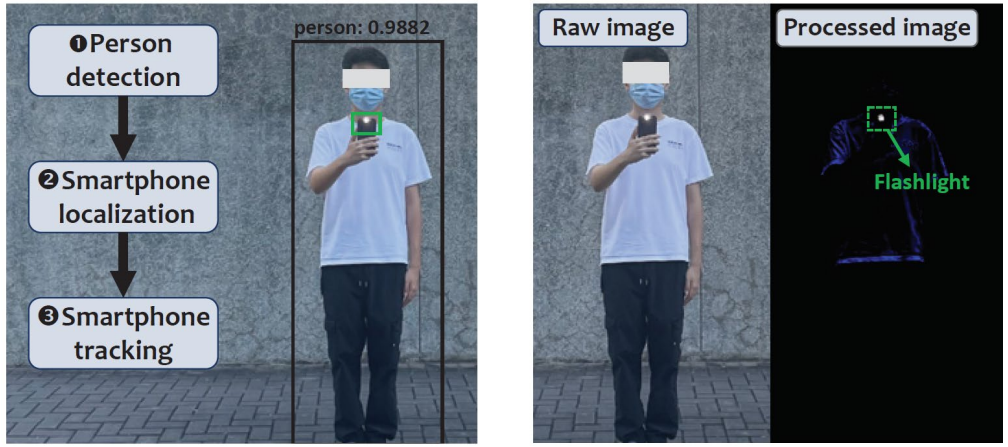


Correspondence between waving smartphone and velocity.

System design

❑ Signal processing vehicle-side:

- ❖ **Person Detection:** Use YOLO-FastestV2 to detect the user (dominant person in frame).
- ❖ **Smartphone Localization:** Identify smartphone's position using its flashlight, mitigating interference with contrast adjustments and frame difference methods.
- ❖ **Smartphone Tracking:** Track flashlight with SiameRPN++, smooth trajectory with Savitzky-Golay filter, and calculate 2D acceleration from the trajectory.



(a) Workflow. (b) Flashlight localization.

Video data processing.

System design

- **Signal processing user-side:**
  - **3D Acceleration Capture:** Obtain 3D acceleration from the smartphone's IMU, with preprocessing to remove gravity effects.
  - **Noise Reduction:** Use Independent Component Analysis (ICA) to separate the hand-waving acceleration component from interference, like hand tremors.

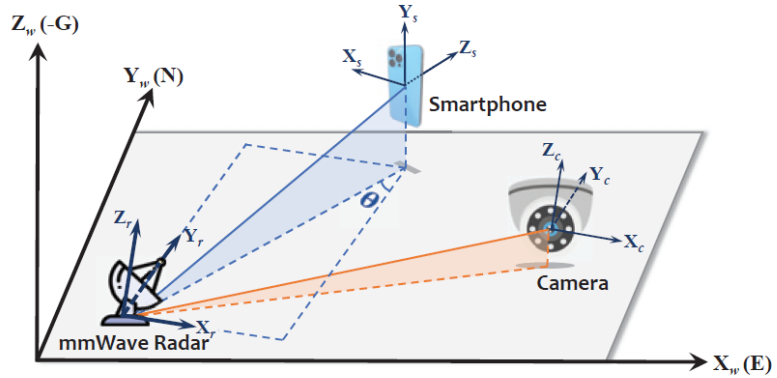
System design

❑ Spatial synchronization vehicle-side:

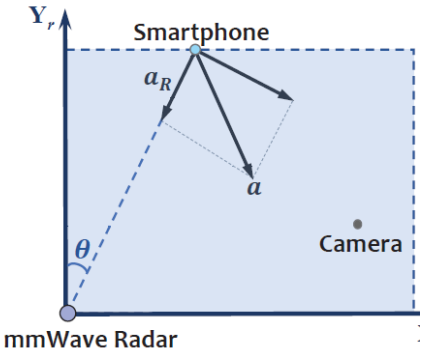
- ❖ Compute radial acceleration in the mmWave radar's coordinate system.
- ❖ Combine with 2D acceleration from the camera to get 3D acceleration in the camera's coordinate system.
- ❖ Lastly, transform this 3D acceleration to the world coordinate system using transformation matrix obtained from the vehicle's built-in GPS.

❑ Spatial synchronization smartphone-side:

- ❖ Transform the smartphone's IMU acceleration directly to the world coordinate system using a transformation matrix available from the smartphone API.



(a) Different coordinate systems in W4S.



(b) Top view in $\mathcal{R}$.

Spatial synchronization.

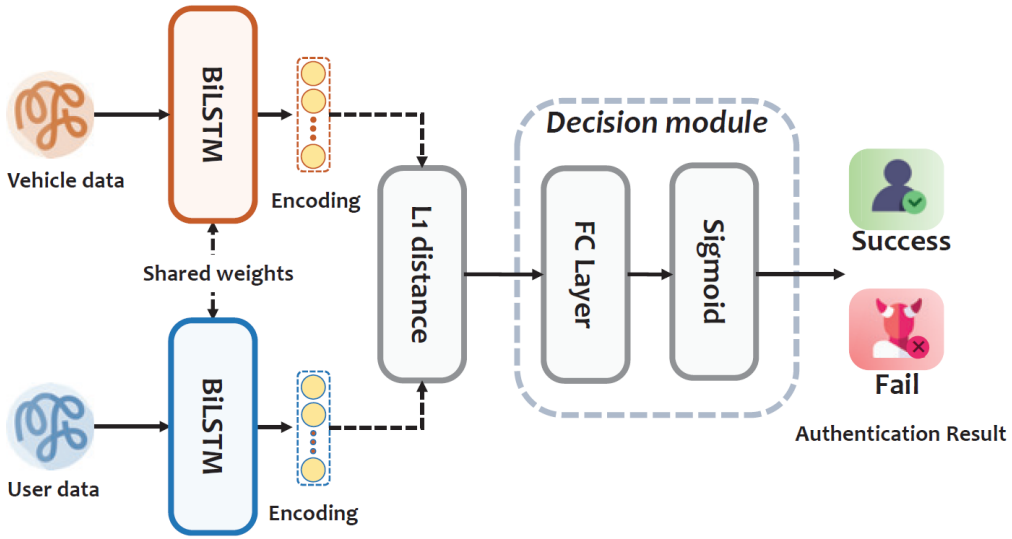
System design

- **Temporal synchronization:**
  - **Coarse-grained synchronization**: Use the start notification sent from the unmanned vehicle to the user‘s smartphone as the initial synchronization point.
  - **Fine-grained synchronization**: Leverage the average timestamps of the first three extreme points (peaks and valleys) on the acceleration axis with the highest variance for precise synchronization.

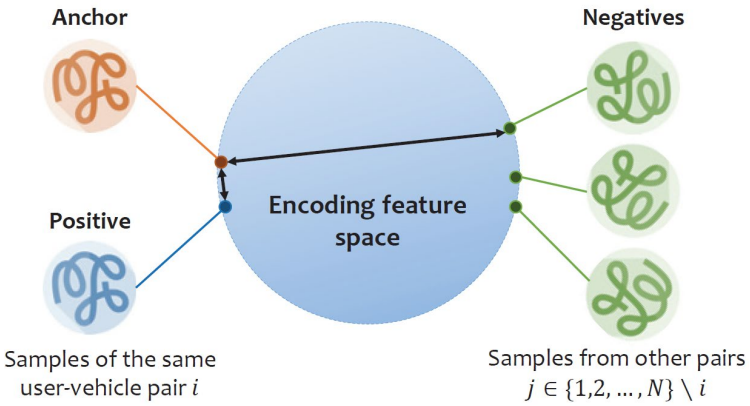
System design

❑ **Decision making module:**

- ❖ **Siamese Neural Network (SNN) Framework**
- ❖ **Sub-network Architecture:** two layers of Bidirectional Long Short-Term Memory (BiLSTM) as the encoder for input signals.
- ❖ **Two-stage training:** 1) shared layers training using a semi-hard triplet loss function, and 2) decision module training using binary cross-entropy as the loss function



Siamese neural network.



Triplet training.

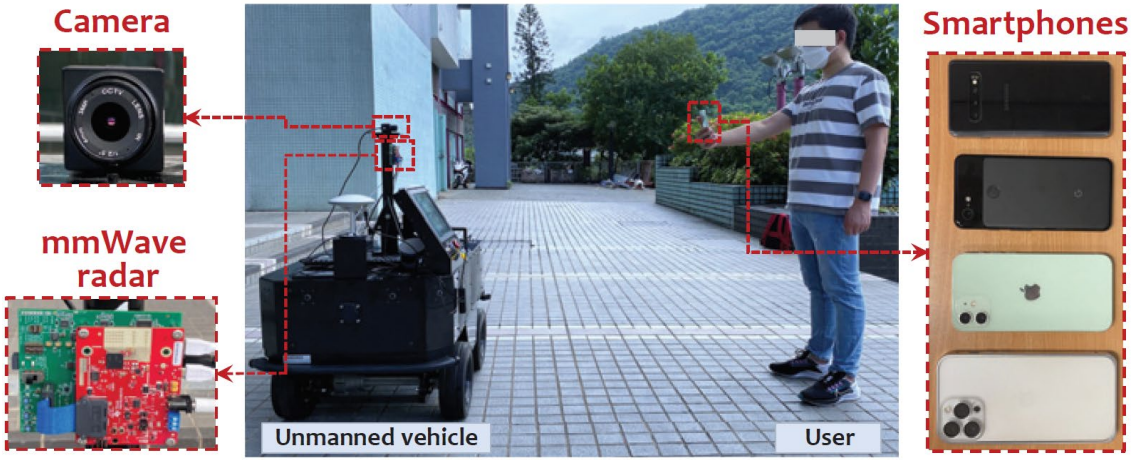
Experimental settings

❑ Data collection

- ❖ Apollo unmanned vehicle and four different smartphones.
- ❖ 40 subjects in various public locations.

❑ Metrics

- ❖ Equal Error Rate (EER): This is the point where the False Acceptance Rate equals the False Rejection Rate. A lower EER means superior system performance, as it indicates that the system has a lower overall error rate.

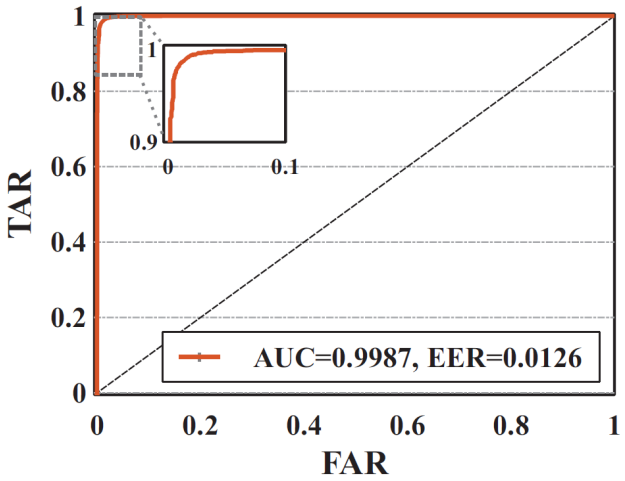


Data collection

Experiment results

❑ Overall performance

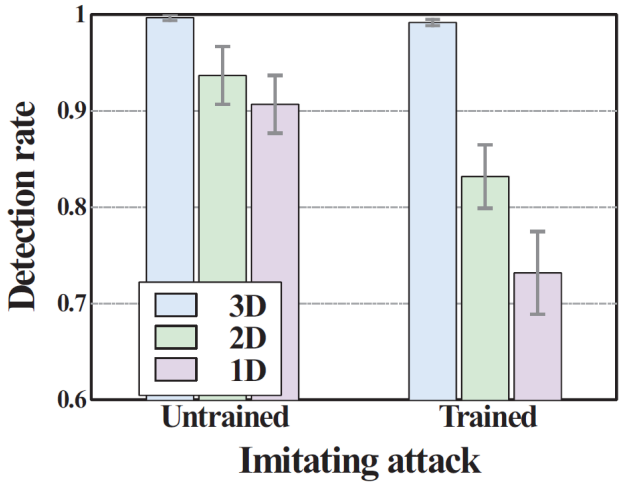
- ❖ W4S achieves an average EER of 0.0126.
- ❖ The low EER indicates that W4S can distinguish authorized accesses from unauthorized ones with high accuracy (i.e., 1-EER) of 0.9874.



Overall performance

❑ Security analysis

- ❖ W4S defended against untrained and trained imitating attackers with 99.67% and 99.17% detection rates, respectively.
- ❖ W4S is better than systems using 1D and 2D information.



Security analysis

Conclusion&future work

- We propose a mutual authentication system—Wave-for-save for unmanned delivery vehicle services, which addresses four key limitations in existing work.

- W4S achieves the goals of no need for additional hardware, mutual authentication, being resistant to attacks, and no user privacy leakage risks.

- Future work will be focused on authentication for UAVs.

Thank you!

Contact:
CityU S2MC Lab
huanqi.yang@my.cityu.edu.hk