Vehicle-Key: A Secret Key Establishment Scheme for LoRa-enabled IoV Communications

Huanqi Yang[1,2], Hongbo Liu[3], Chengwen Luo[4], Yuezhong Wu[5], Wei Li[6], Albert Y. Zomaya[6], Linqi Song[1,2] and Weitao Xu[1,2]

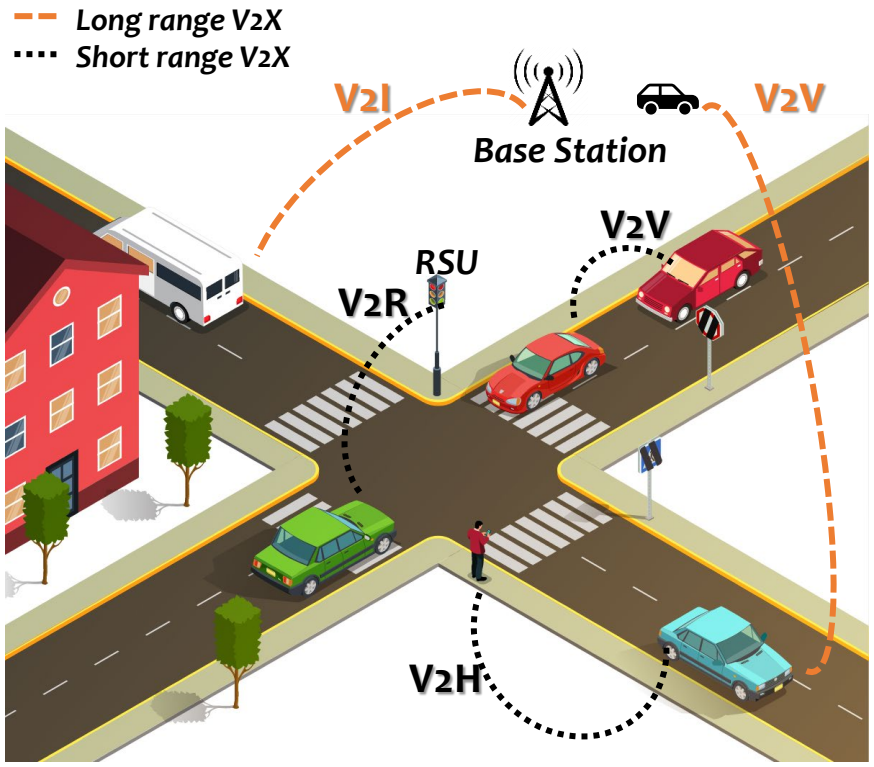
[1]City University of Hong Kong Shenzhen Research Institute, [2]City University of Hong Kong, [3]University of Electronic Science and Technology of China, [4]Shenzhen University, [5]University of New South Wales, [6]The University of Sydney

Contents

香港城市大學
City University of Hong Kong

- Background
- Current solutions
- System design
- Evaluation
- Conclusion

Background



V2V: vehicle-to-vehicle **V2I:** vehicle-to-infrastructure
V2R: vehicle-to-road **V2H:** vehicle-to-human

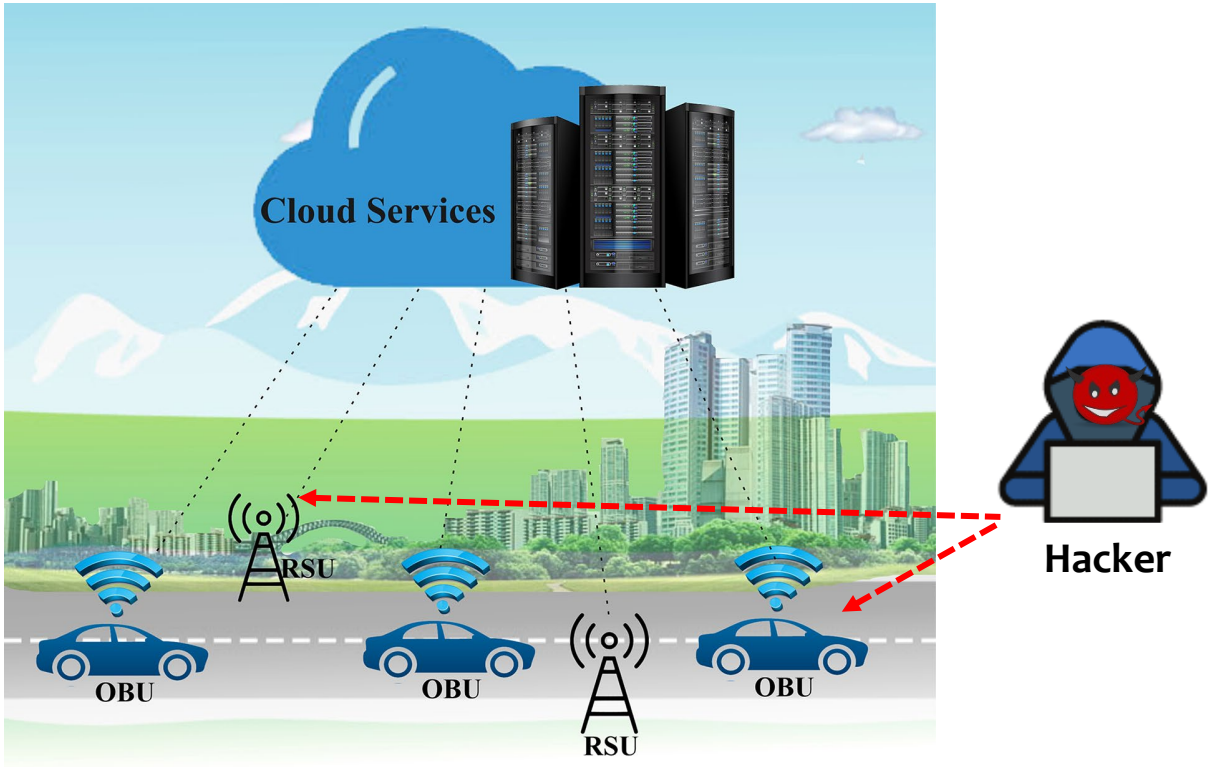
- **The rapid development of the Internet of Vehicles (IoV)**
- **Vehicle-to-everything (V2X) systems require sensitive instantaneous information**
- **Securing such information exchange is critical to ensure both the normal operation of vehicular systems and the safety of passengers**

Current solutions

香港城市大學
City University of Hong Kong

❖ Public key infrastructure

- Authenticated methods need extra infrastructure
- Vulnerable to MITM (man-in-the-middle) attack

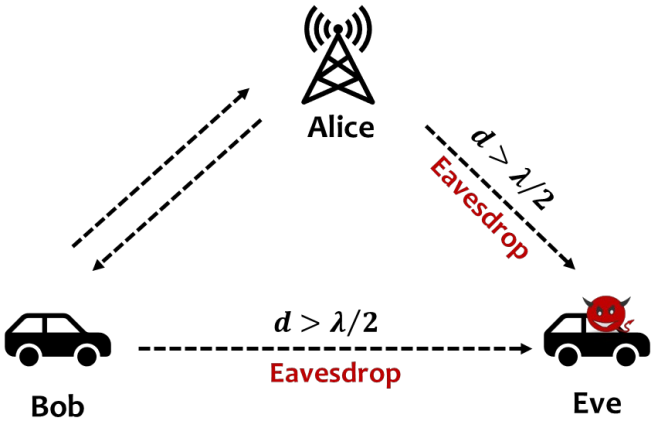


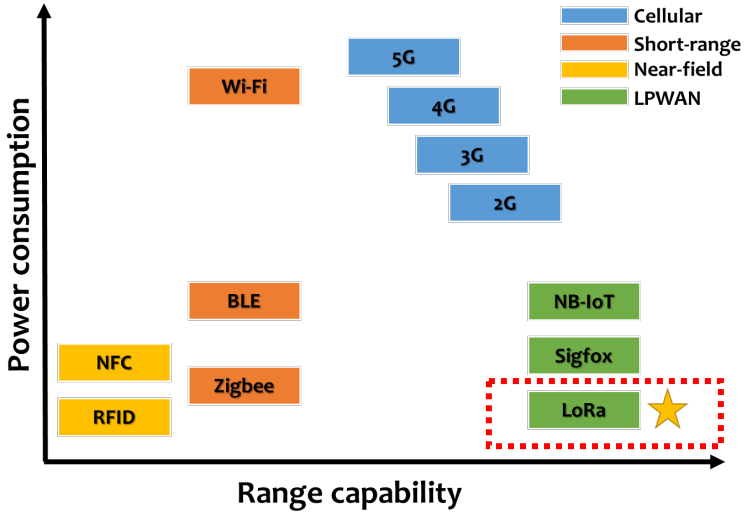
Current solutions

香港城市大學
City University of Hong Kong

❖ Physical layer key generation

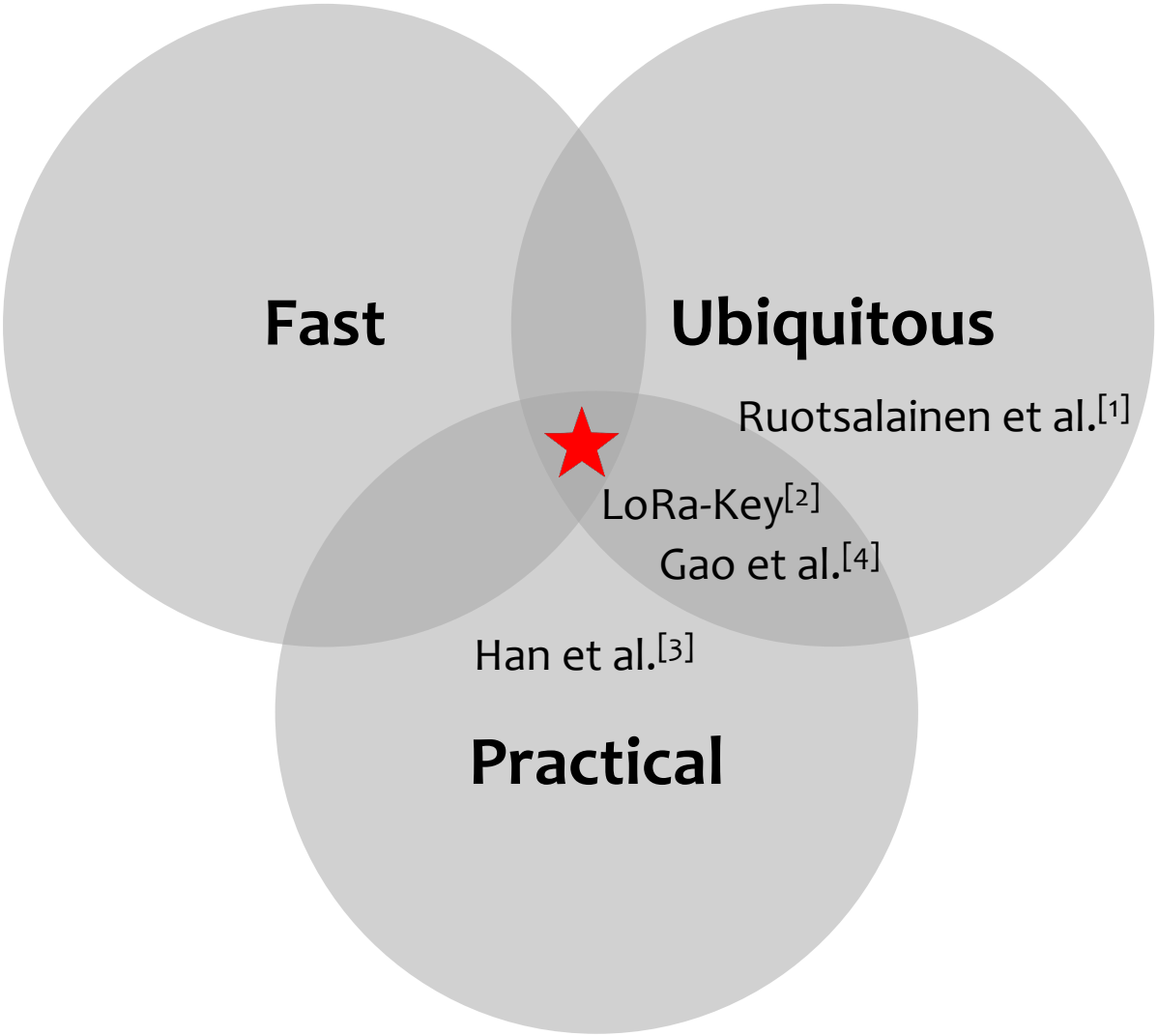
- Existing studies mainly focus on legacy communication technologies with **limited communication distance**
- **LoRa** provides a promising solution to long-range communication
- **Low data rate of LoRa** poses novel challenges for IoV key generation





Research gap

香港城市大學
City University of Hong Kong



[1] H. Ruotsalainen, J. Zhang, and S. Grebeniuk, "Experimental investigation on wireless key generation for low-power wide-area networks," IEEE Internet Things J., 2019.
[2] W. Xu, S. Jha, and W. Hu, "Lora-key: Secure key generation system for lora-based network," IEEE Internet Things J., 2018.
[3] H. Biao, P. Sirui, W. Celimuge, W. Xiaoyan, and W. Baosheng, "Lorabased physical layer key generation for secure v2v/v2i communications," Sensors, 2020.
[4] J. Gao, W. Xu, S. Kanhere, S. Jha, J. Y. Kim, W. Huang, and W. Hu, "A novel model-based security scheme for lora key generation," in IPSN, 2021.

Challenges

香港城市大學
City University of Hong Kong

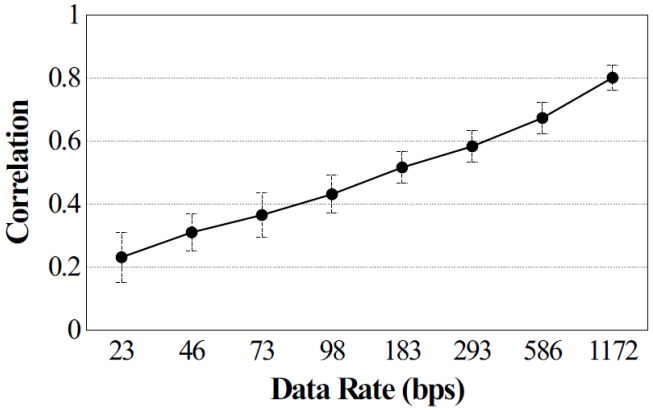
- **Long packet airtime of LoRa.**
  - the data rate of LoRa can be low as tens of bps.
  - the low data rate increases the packet airtime
  - thus decreases the channel reciprocity

- **High mobility of the vehicles.**
  - Vehicles are highly mobile
  - Environment is fast-changing
  - The fast fading effect will further exacerbate low channel reciprocity problem

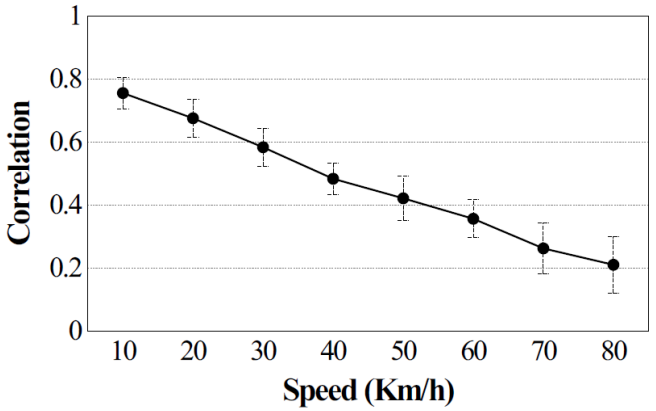
Preliminary

香港城市大學
City University of Hong Kong

- **Impact of packet airtime:**
  - fix the vehicle speed
  - calculate the correlation between Alice's RSSIs and Bob's RSSIs by changing the data rates
- **Impact of vehicle's speed:**
  - fix the data rate
  - Calculate the correlation between Alice's RSSIs and BoB'S RSSIs by changing the speed



(a) Impact of packet airtime



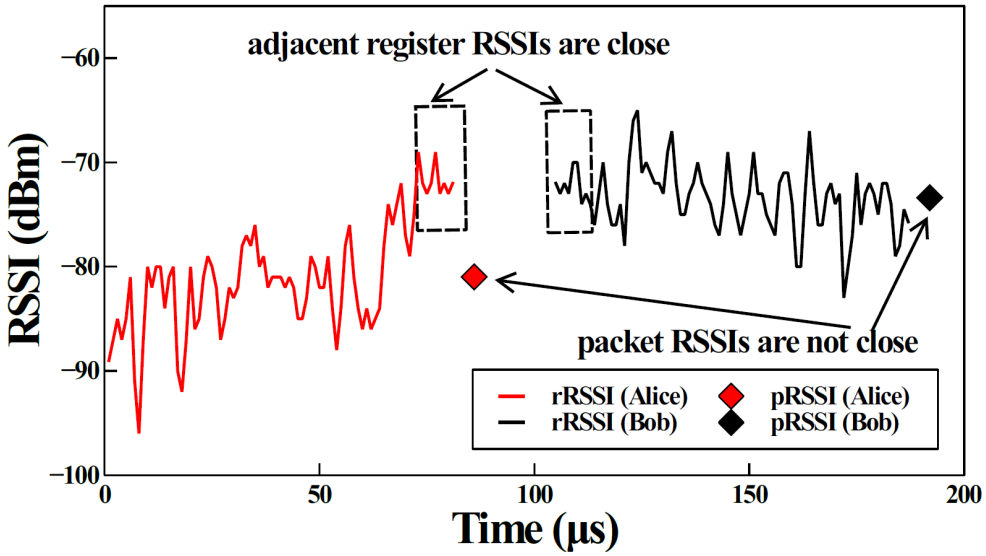
(b) Impact of vehicle speed

The two factors have significant impact on LoRa-enabled IoV key generation

Our findings

❖ Channel features

- Averaged packet RSSI (pRSSI)
  - *pRSSIs of Alice and Bob are not close*
- Instantaneous register RSSI (rRSSI)
  - *Adjacent part of register RSSIs of Alice and Bob are close*



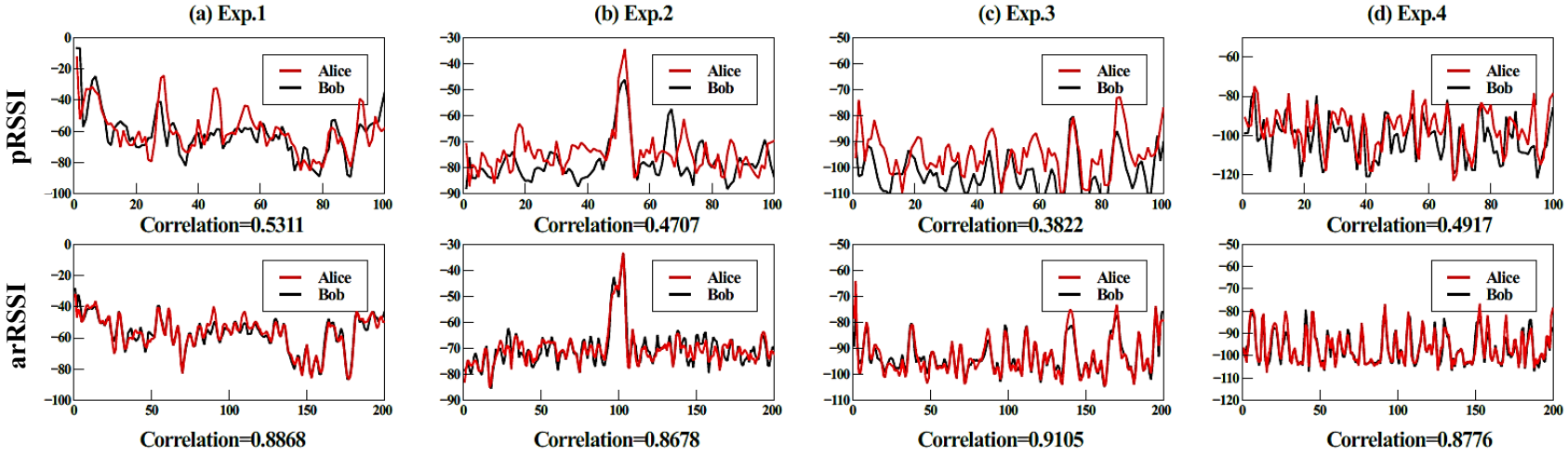
We propose to employ the mean value of adjacent rRSSI as a new feature for key generation, namely *adjacent register RSSI (arRSSI).*

Our findings

香港城市大學
City University of Hong Kong

❖ pRSSI v.s. arRSSI experiments:

- Experiment 1: Vehicle to Vehicle in rural.
- Experiment 2: Vehicle to Infrastructure in rural.
- Experiment 3: Vehicle to Vehicle in urban.
- Experiment 4: Vehicle to Infrastructure in urban.

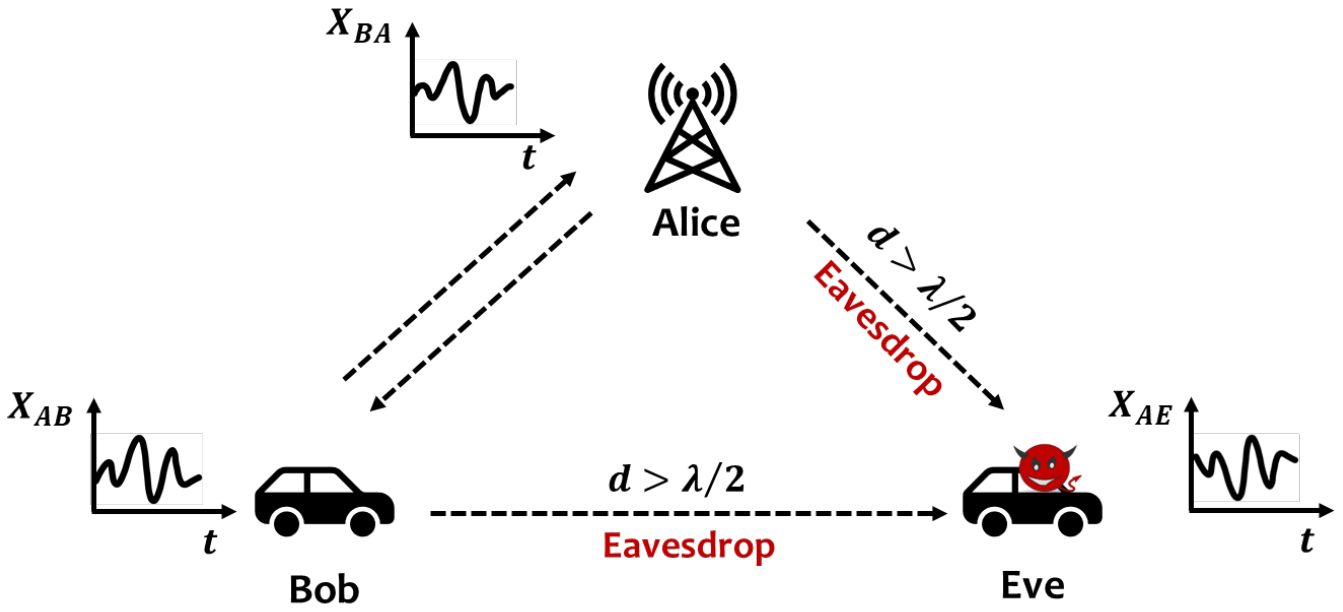


Using arRSSI as the channel feature can increase the correlation between legitimate nodes in IoV communications.

System model

香港城市大學
City University of Hong Kong

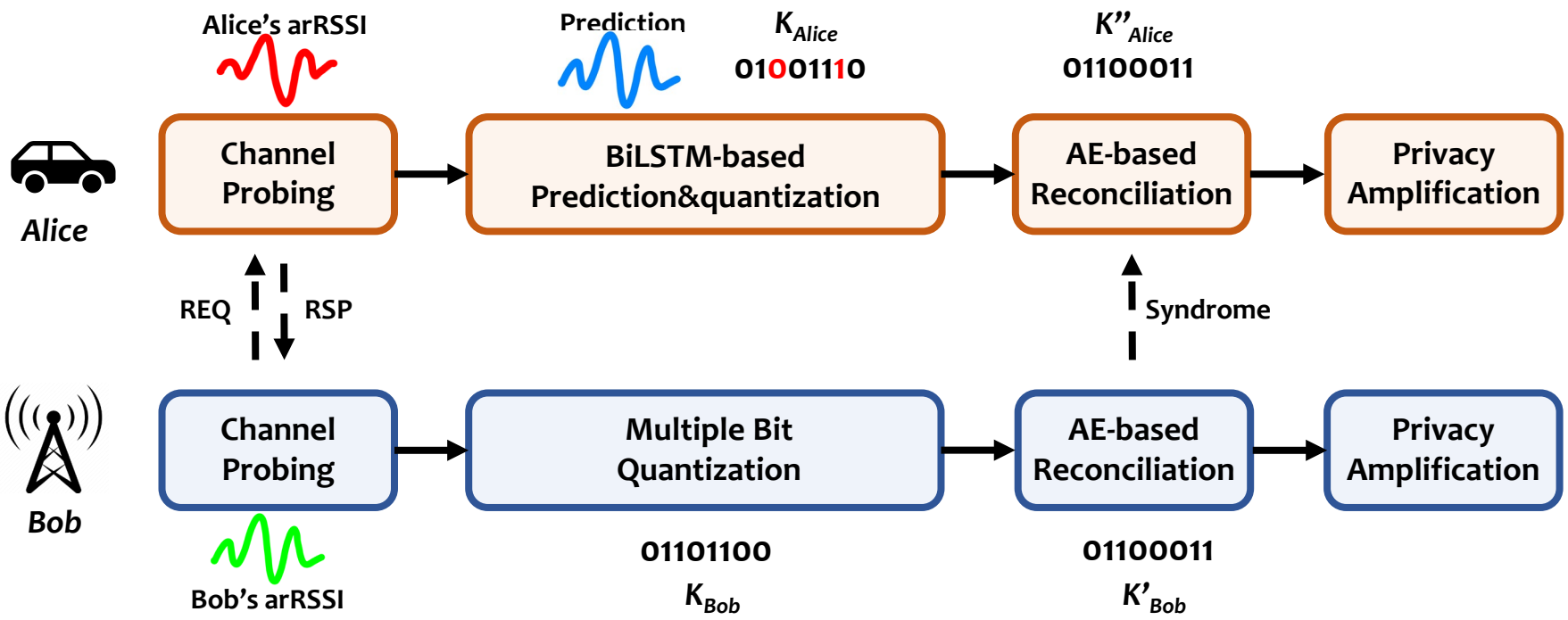
- **User model**
  - Based on channel reciprocity, the communication channel between Alice and Bob are unique
- **Adversarial model**
  - Eavesdropping attack
  - Imitating attack



System Overview

香港城市大學
City University of Hong Kong

❖ Vehicle-key

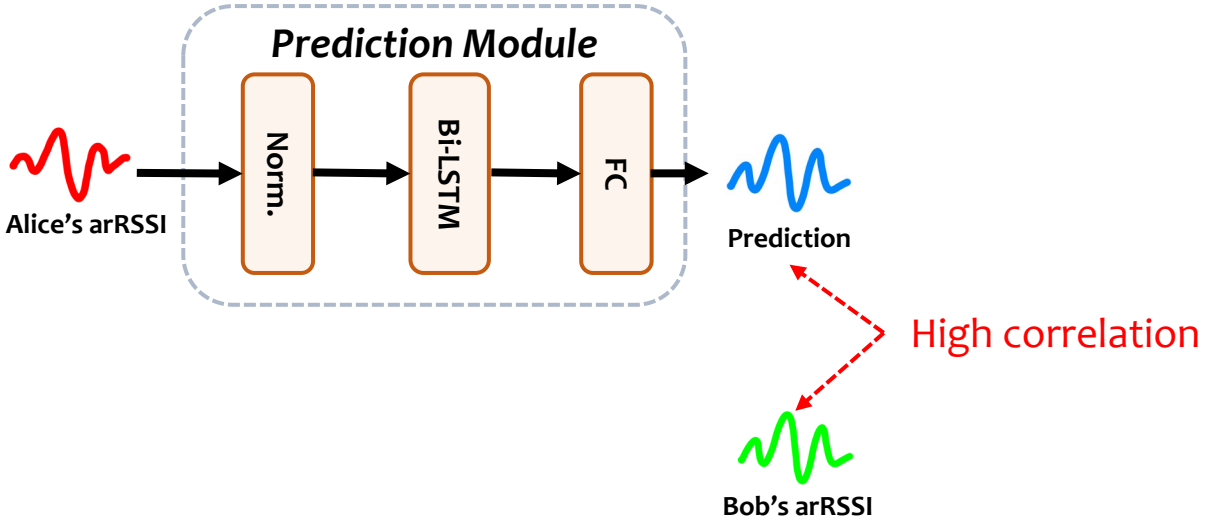


Prediction and quantization

香港城市大學
City University of Hong Kong

❖ Prediction module

- Problem: the channel measurements are not reciprocal
  - *Time delay on both directions*
  - *Hardware imperfection*
- Solution: Bi-directional LSTM (BiLSTM)-based model
  - *Alice makes prediction based on pre-trained model to improve correlation*
  - *Superior performance on learning features from correlated sequences*

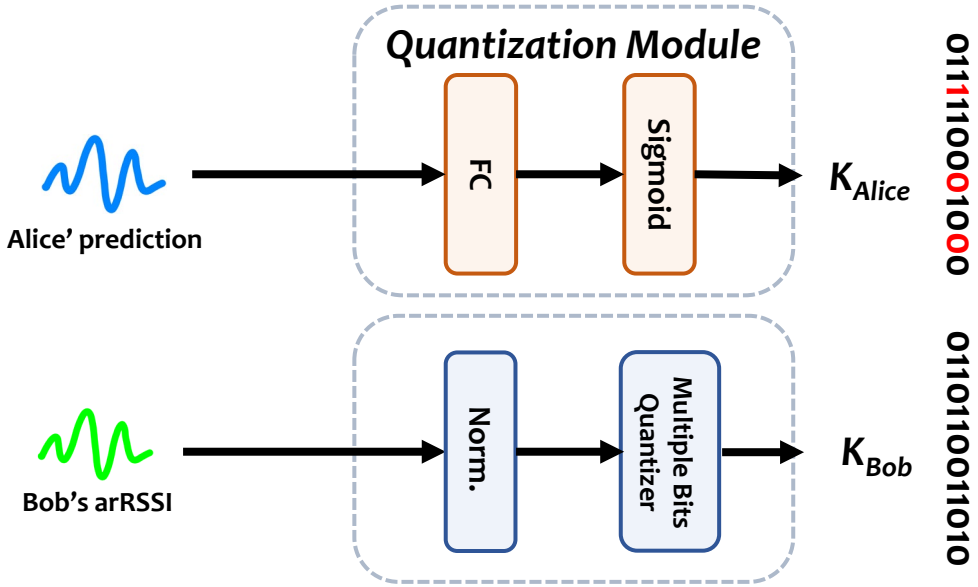


Prediction and quantization

香港城市大學
City University of Hong Kong

❖ Quantization module

- Convert the arRSSI values into binary bits
- Alice
  - *fully connected layer: fit a nonlinear transformation*
  - *sigmoid activation function: map real numbers to the interval (0,1)*
- Bob:
  - *multiple bit quantizer*[5]



[5] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in Mobicom, 2009.

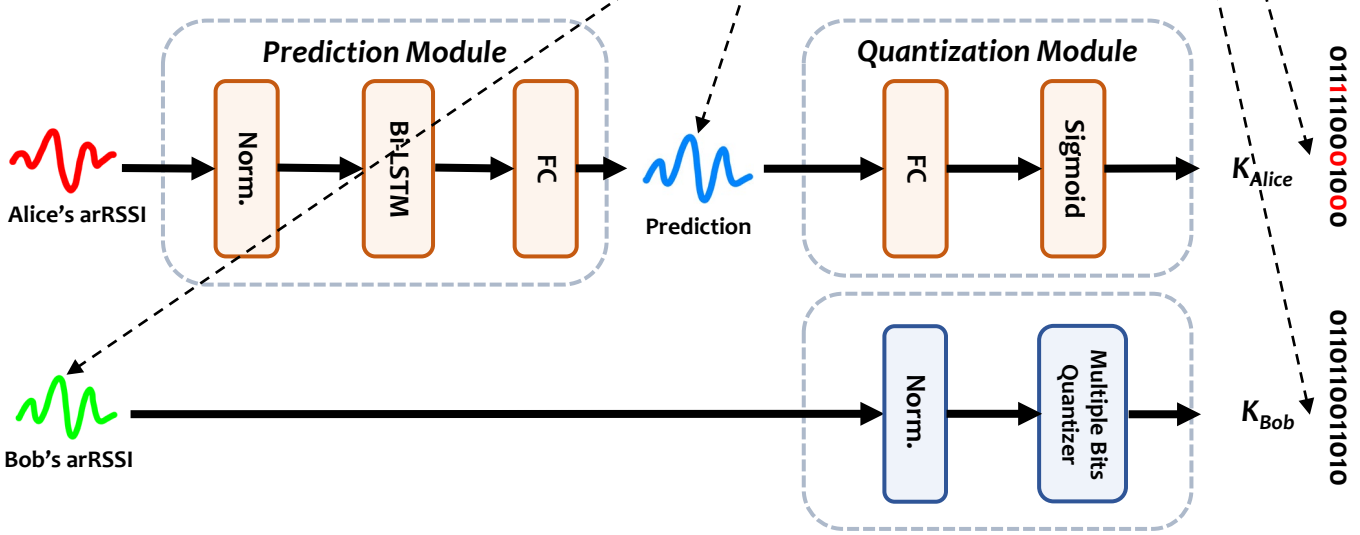
Prediction and quantization

香港城市大學
City University of Hong Kong

❖ Joint training

- Combining prediction module and quantization module into a neural network for convenience and efficiency
- Joint loss function
  - *Use Mean Squared Error (MSE) loss to train the prediction module*
  - *Use Binary Cross Entropy (BCE) loss to train the quantization module*
  - *Add a hyperparameter θ to balance the weights between BCE and MSE loss*

$$loss(y, \hat{y}, z, \hat{z}) = \theta \times MSE(y, \hat{y}) + (1-\theta) \times BCE(z, \hat{z})$$

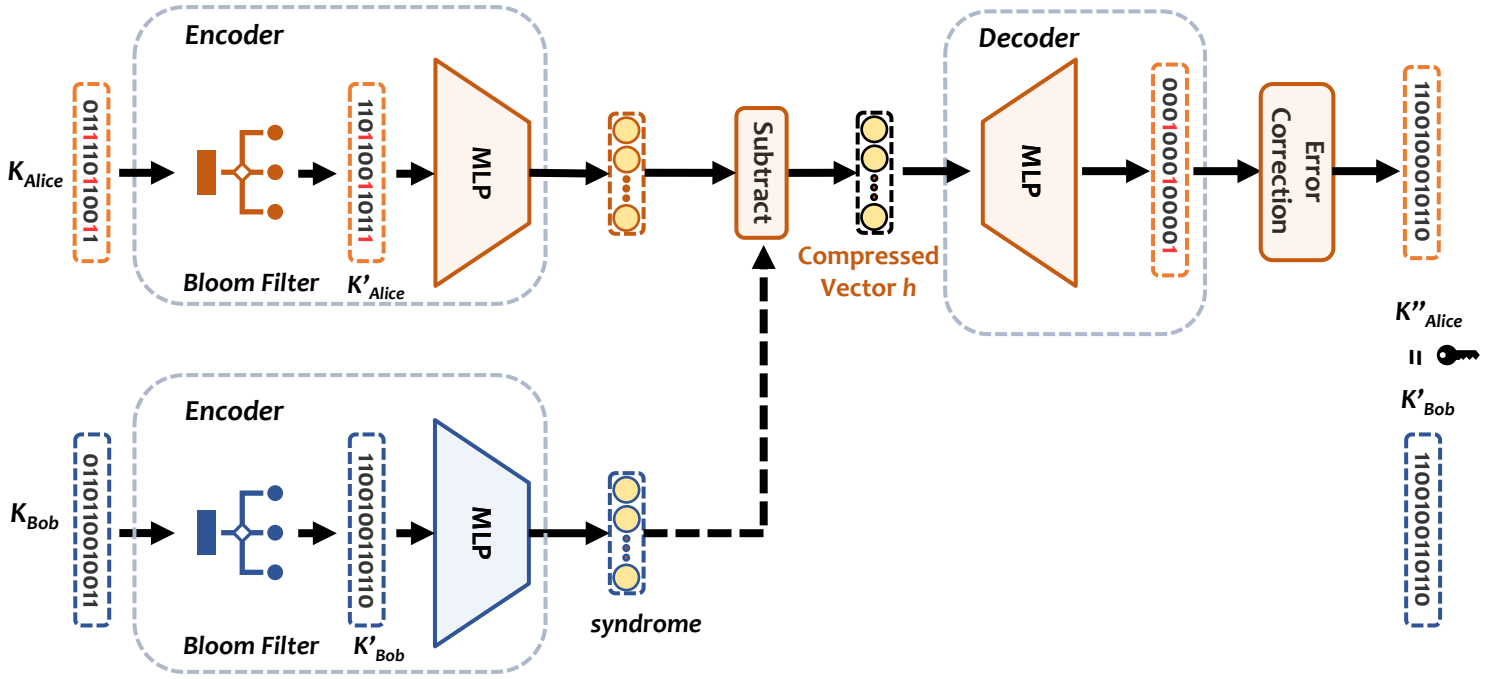


Reconciliation

香港城市大學
City University of Hong Kong

❖ Autoencoder-based reconciliation

- Reconciliation is used to correct mismatches: $K_{Alice} \approx K_{Bob}$
- We design a novel two-input structure autoencoder for error correction

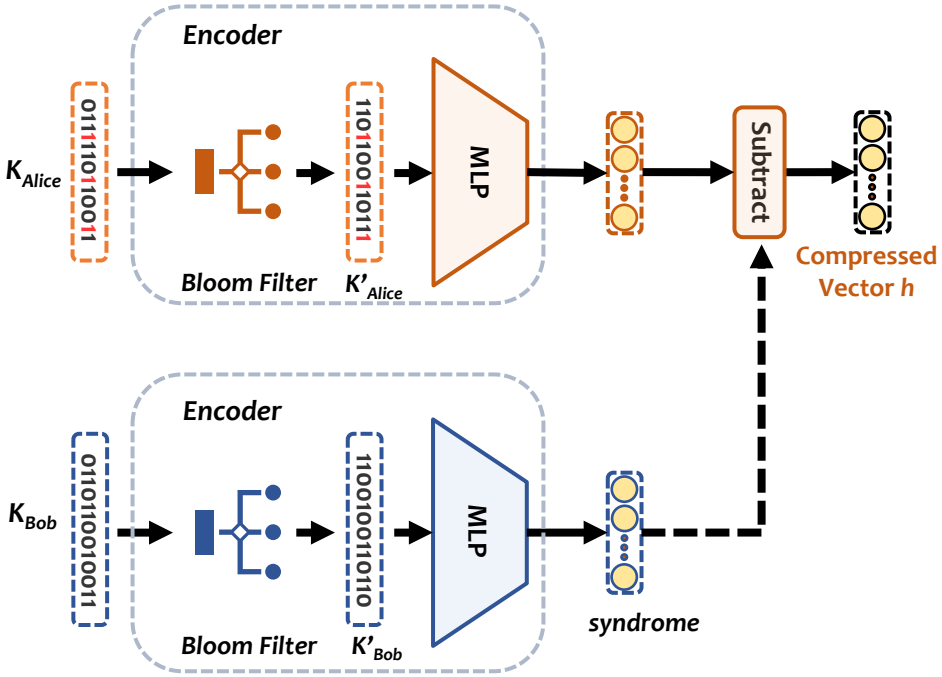


Reconciliation

香港城市大學
City University of Hong Kong

❖ Encoder design

- Bloom filter[6] protect the keys against reverse engineering attack
- Multilayer Perceptron (MLP) generate code vectors
- Bob transmits the code vector (syndrome) to Alice via public channel
- Subtraction layer get Compressed Vector for decoding



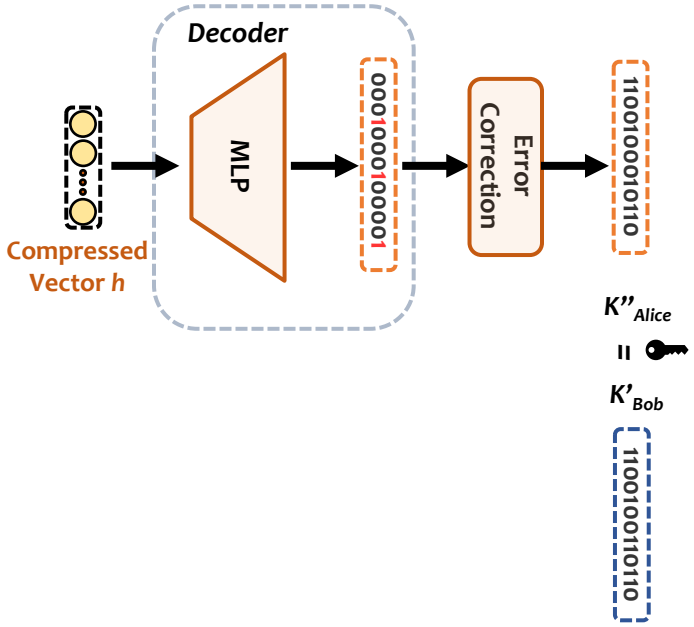
[6] W. Xu, Z. Li, W. Xue, X. Yu, B. Wei, J. Wang, C. Luo, W. Li, and A. Y. Zomaya, "Inaudiblekey: Generic inaudible acoustic signal based key agreement protocol for mobile devices," in IPSN, 2021.

Reconciliation

香港城市大學
City University of Hong Kong

❖ Decoder design

- Alice feeds Compressed Vector into a MLP to decode the mismatches
- Alice can correct the mismatches by simply calculating XOR of Alice's bits and mismatches



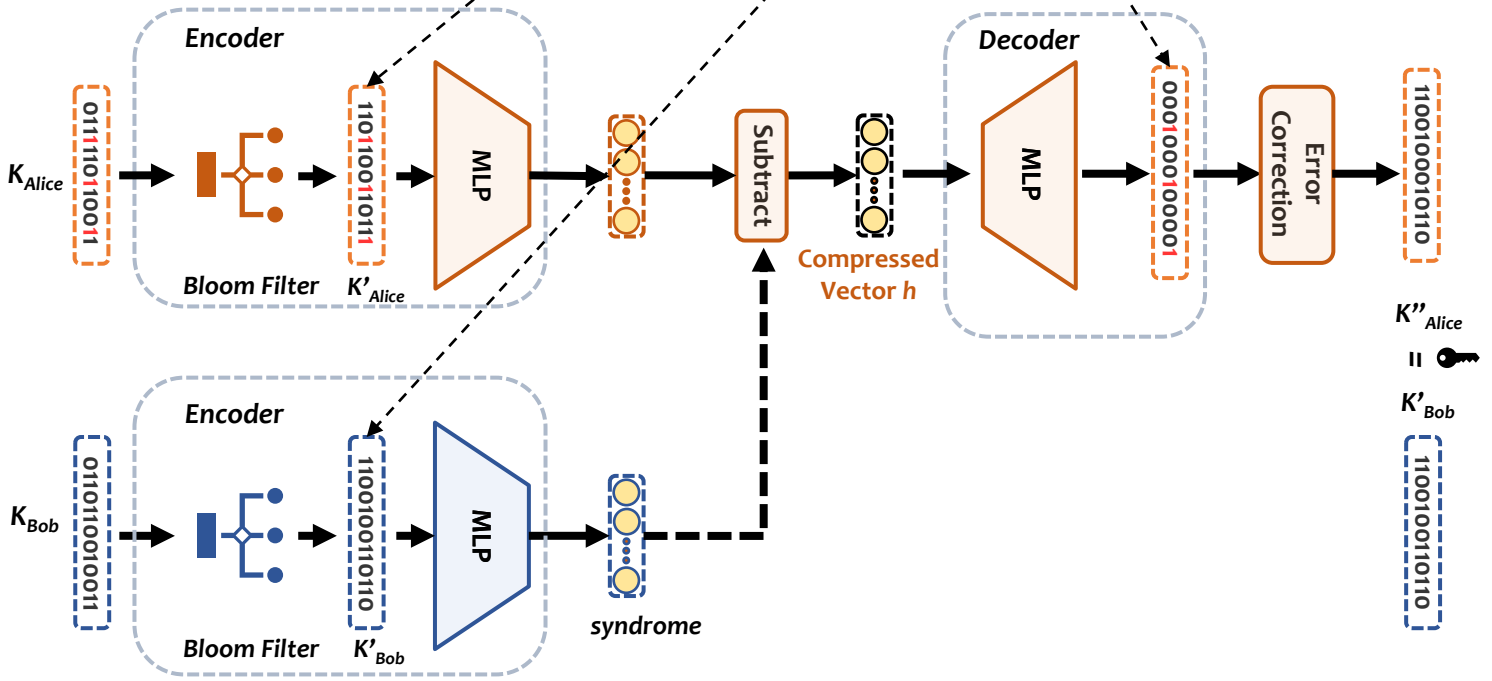
Reconciliation

香港城市大學 City University of Hong Kong

❖ Loss function

- the distance between the learned mismatches (Δx) and the real mismatches ($K'_{Bob} \oplus K'_{Alice}$) can be minimized

$$\arg\min_{f_1, f_2, g} \left\| \left(K'_{\text{Alice}} \oplus K'_{\text{Bob}} \right) - \Delta x \right\|^2$$



Evaluation

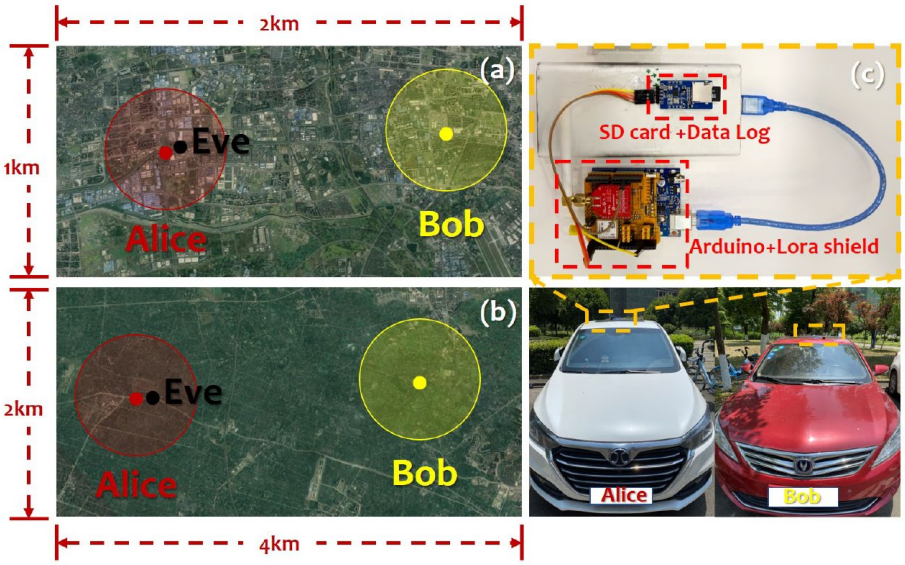
香港城市大學
City University of Hong Kong

❖ Set-up:

- Devices: Dragino LoRa Shield , MultiTech xDot, MultiTech xDot
- Different IoV scenarios: V2I-Urban, V2I-Rural, V2V-Urban, V2V-Rural

❖ Metrics:

- Key agreement rate:
  - *the percentage of bits matching between two keys generated by two devices*
- Key generation rate:
  - *the average number of agreed keys generated from the acceleration samples per second*



Evaluation

香港城市大學
City University of Hong Kong

❖ System Robustness

- Impact of different devices
- Impact of different speeds

Device \ Speed (Km/h)	30	60	90	Mean
Dragino LoRa Shield	99.50%	99.10%	98.90%	99.17%
MultiTech xDot	99.20%	98.90%	98.10%	98.73%
MultiTech mDot	99.30%	98.90%	98.00%	98.73%
Mean	99.33%	98.97%	98.33%	98.87%

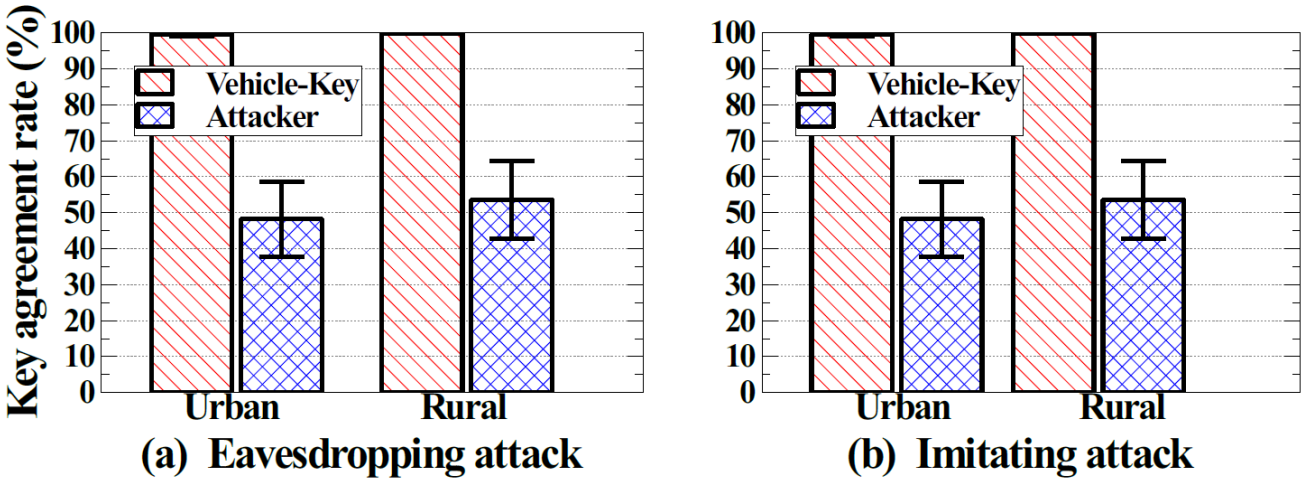
Vehicle-Key can achieve high agreement rate irrespective of the hardware used and the moving speed

Evaluation

香港城市大學
City University of Hong Kong

❖ Security analysis

- Eavesdropping attack
- Imitating attack



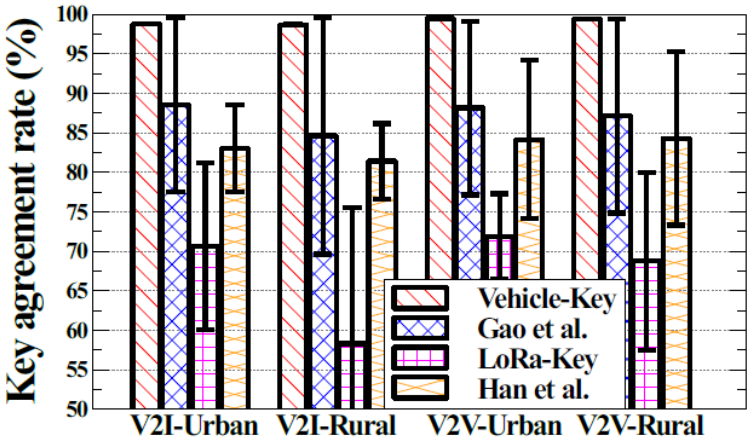
An attacker can only achieve approximately 50% bit agreement rate

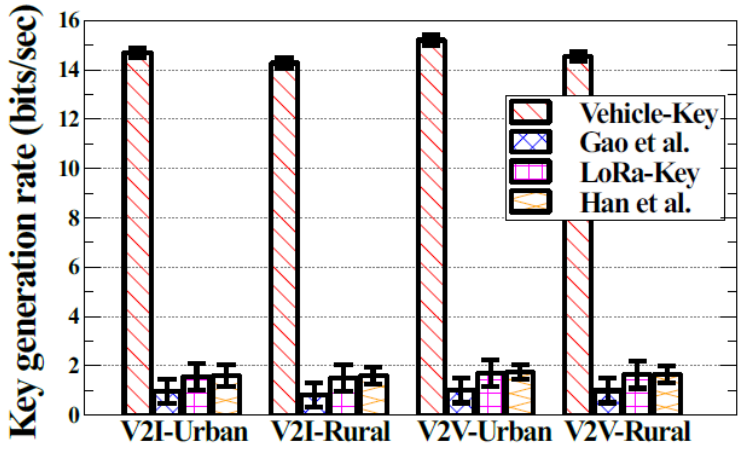
Evaluation

香港城市大學
City University of Hong Kong

❖ Comparison with state-of-the-arts

- Packet RSSI-based: LoRa-key (IoT-J 2018), Han et al. (Sensors 2020)
- Register RSSI-based : Gao et al. (IPSN 2021)



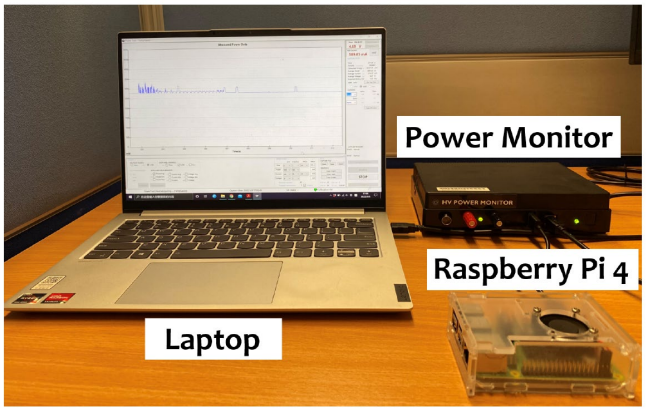


Vehicle-Key improves the key agreement rate by 15.10%–49.81% and key generation rate by 9–14 ×

Evaluation

香港城市大學
City University of Hong Kong

- **Energy consumption**
  - implement Vehicle-Key on a Raspberry Pi
  - use power monitor to evaluate the computation time and energy consumption



	Computation time (ms)		Energy consumption (mJ)	
	Alice	Bob	Alice	Bob
Prediction and quantization	3.38	0.42	12.8947	1.44
Reconciliation	0.0308	0.0077	0.1113	0.0278
Total	3.4108	0.4277	13.006	1.4678

Account to 0.0002 ‰ of the vehicle battery supply only

Conclusion

香港城市大學
City University of Hong Kong

- Vehicle-Key enables long-range IoV secret key generation with high robustness.
- Vehicle-Key can run real-time in current mobile devices and incur low system overhead.
- Future work will be focused on secret key generation for aircraft.

Thanks for your attention!

Questions and suggestions?