NDSS SYMPOSIUM/2020

Hold The Door! Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft

Kyungho Joo*   Wonsuk Choi*   Dong Hoon Lee

Korea University

* Co-first Authors

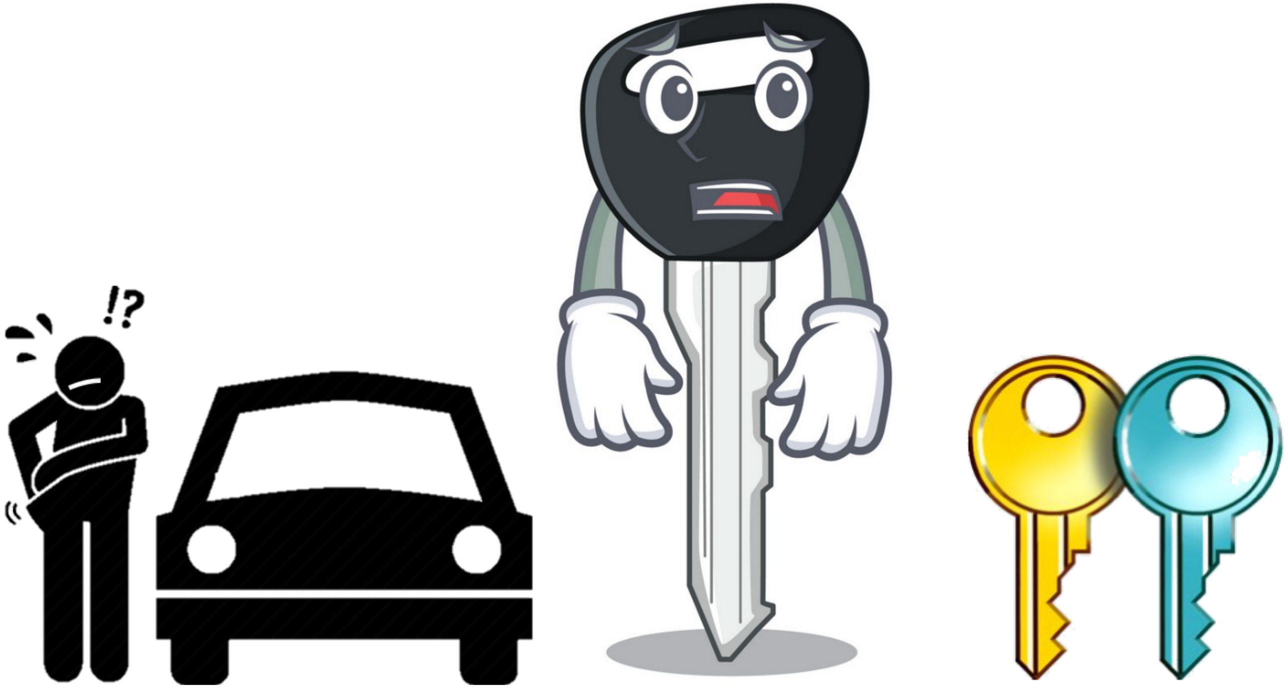
KOREA UNIVERSITY

Outline

- Introduction
- Attack Model
- Our Method
- Evaluation
- Discussion
- Conclusion

Introduction

- Traditional system
  - Physically insert a key into the keyhole
  - Inconvenient
  - Vulnerable to key copying

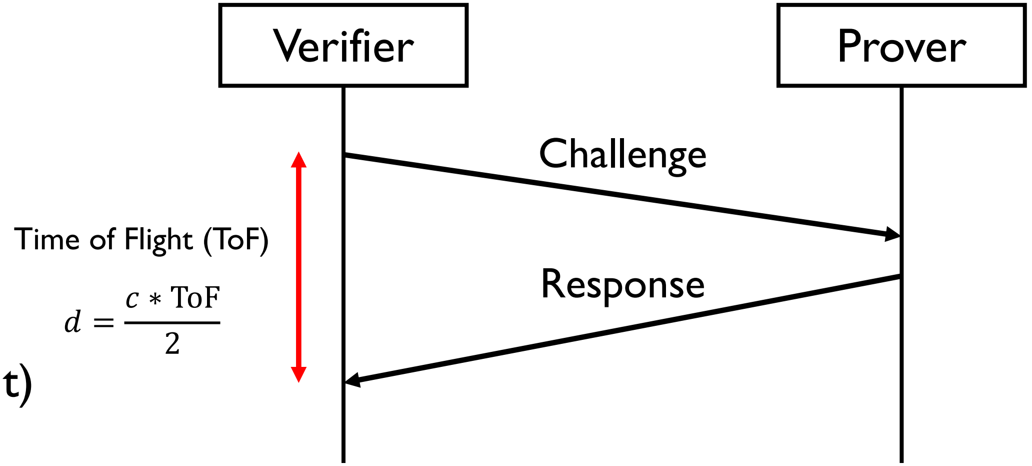


Introduction

- Keyless Entry System
  - Remote Keyless Entry (RKE) System
  - Passive Keyless Entry and Start (PKES) System
- Attacks on Keyless Entry System
  - Cryptanalysis
  - Relay Attack
  - etc. (e.g., Roll-jam)

Introduction

- Countermeasures
  - Distance bounding protocol
    - Sensitive to timing error (Propagates at the speed of light)
  - UWB-IR Ranging System
    - Efforts are underway (IEEE 802.15.4z Task Group) [1-3]
    - Requires an entirely new keyless entry system
- Motivation
  - Device Fingerprint: Exploits hardware imperfection
  - PHY-layer signal analysis



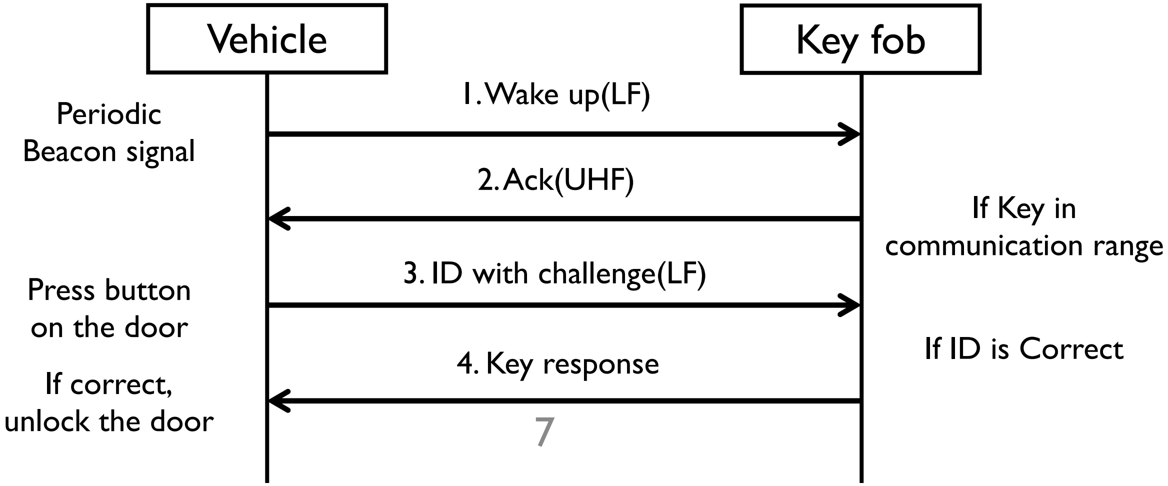
[1] UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks (M. Singh et al.)
[2] UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband (M. Singh et al.)
[3] Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Measurement (P. Leu et al.)

Introduction

- Contributions
  - New attack model
    - Combines all known attack methods; our attack model covers both PKES and RKE systems
    - Single/Dual-band relay attack, Cryptographic attack
  - No alterations to the current system
    - Easily employed by adding a new device that captures and analyzes the ultra-high frequency (UHF) band RF signals emitted from a key fob
  - Evaluations under varying environmental factors
    - Temperature variations, NLoS conditions (e.g., a key fob placed in a pocket) and battery aging

Introduction

- Passive Keyless Entry and Start (PKES) System
  - LF band (125~135 kHz, Vehicle)
    - 1 ~ 2 meter communication range
  - UHF band (433, 858 MHz, Key fob)
    - ~100 meter communication range)
  - Shared cryptographic key between the key and the vehicle



Vehicle

Key fob

Periodic Beacon signal

1. Wake up(LF)

2. Ack(UHF)

If Key in communication range

Press button on the door

3. ID with challenge(LF)

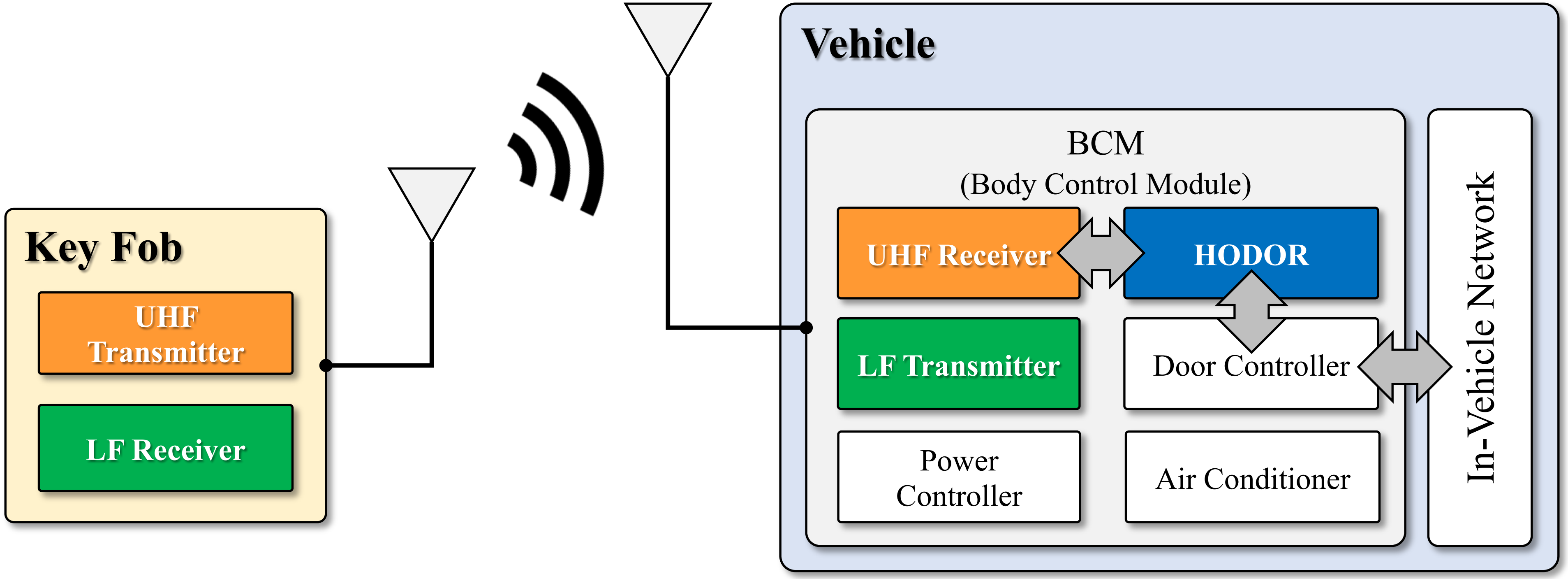
4. Key response

If ID is Correct

If correct, unlock the door

Introduction

- System Model

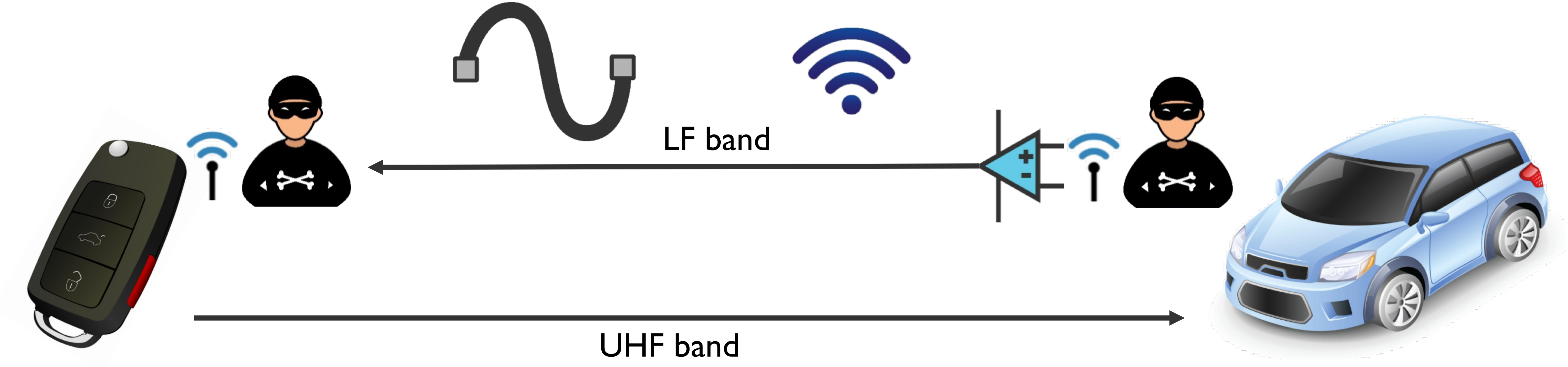


Outline

- Introduction / Background
- Attack Model
- Our Method
- Evaluation
- Discussion
- Conclusion

Attack Model

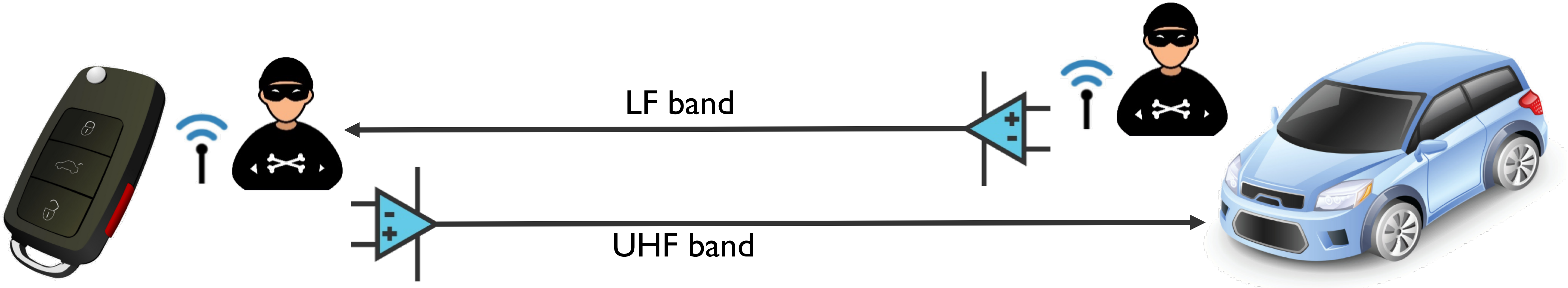
- Single-band Relay Attack [*]
  - Manipulate LF band signal only
  - Wired / Wireless Attack



[*] Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars (Aurelien Francillon et al.)

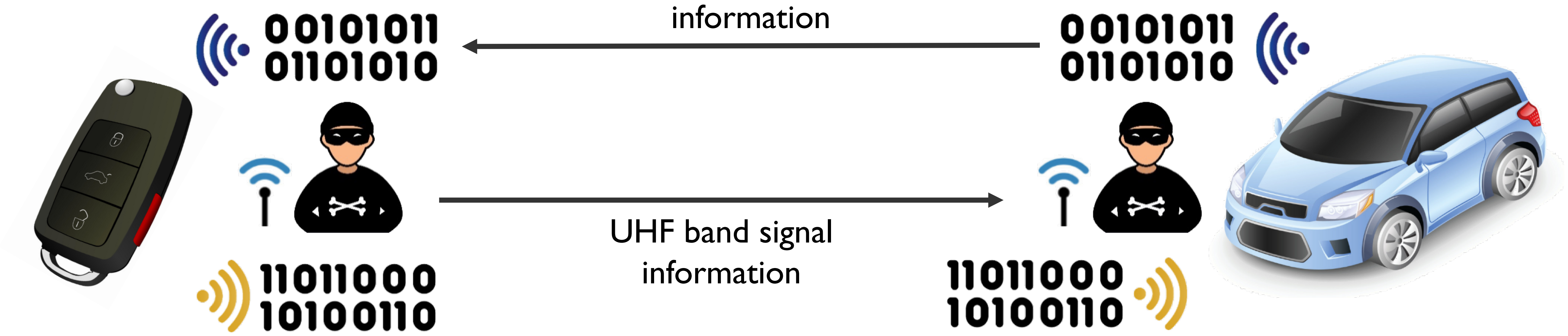
Attack Model

- Dual-band Relay Attack (Ⅰ .Amplification Attack)
  - Manipulate both LF and UHF band signals
  - Amplifies UHF band signal and injects to the vehicle



Attack Model

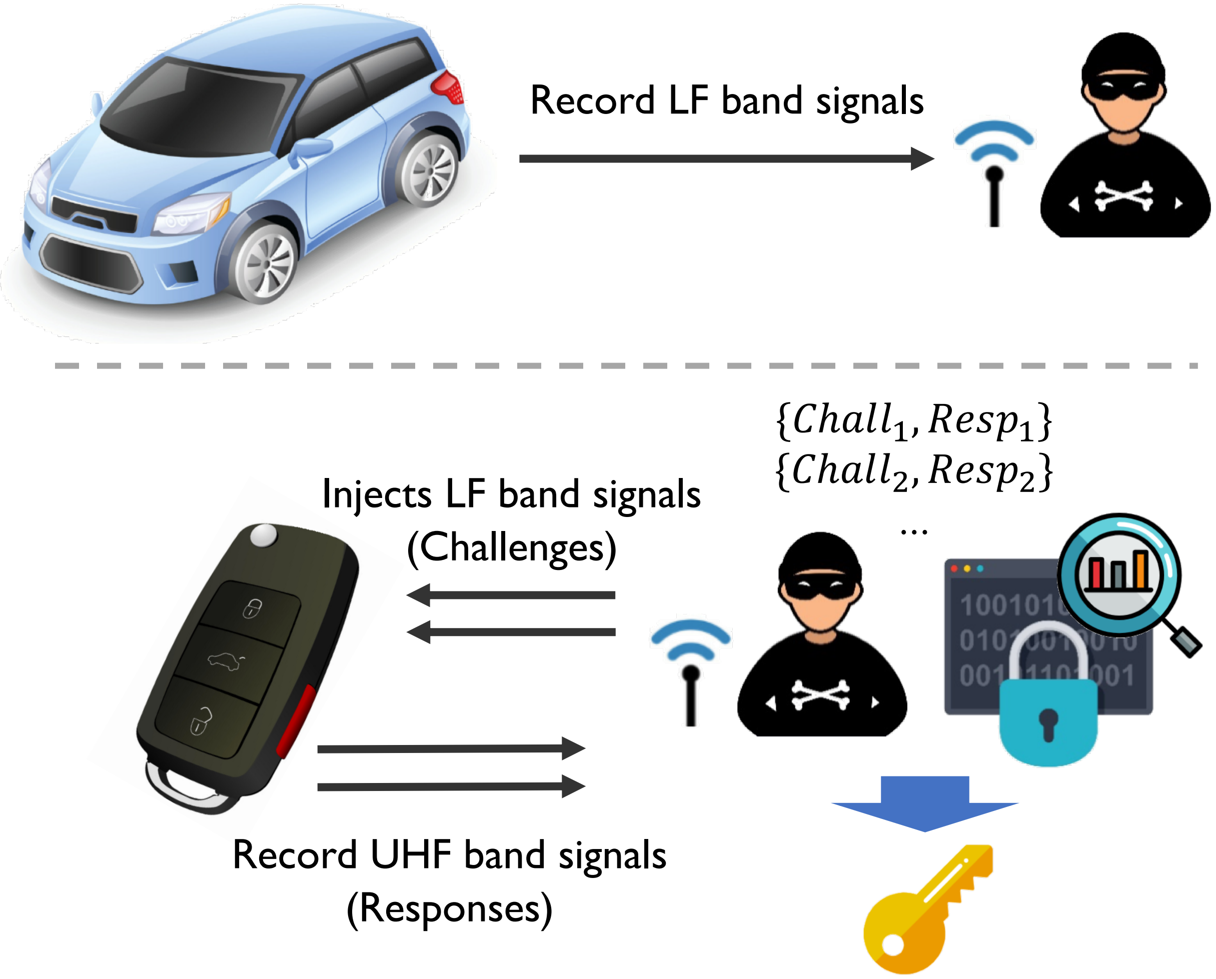
- Dual-band Relay Attack (Ⅱ. Digital Relay Attack) [*]
  - Performs the whole process of digital communication
  - Demodulate LF/UHF band signal
  - Relay binary information



[*] Car keyless entry system attack (Yingtao Zeng et al.)

Attack Model

- Cryptographic Attack [*]
  - Single attacker
  - Injects LF band signals to the key fob
  - Records valid responses and extract secret key
  - Exploits weaknesses of cryptographic algorithm



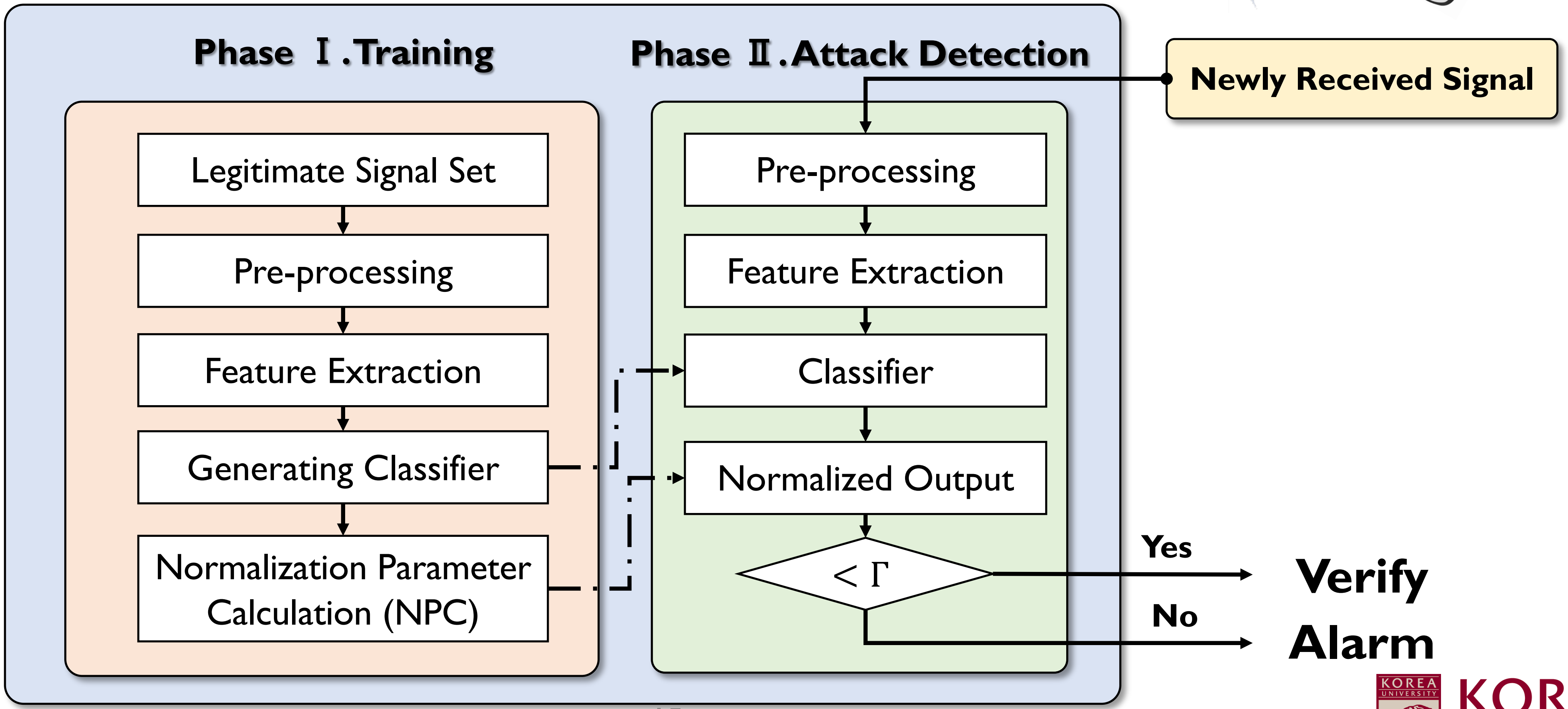
[*] Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars (Wouters et al.)

Outline

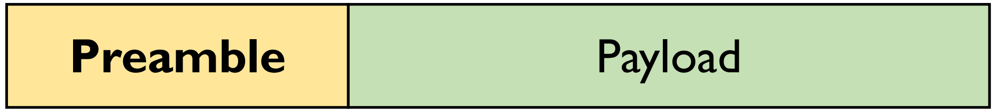
- Introduction / Background
- Attack Model
- Our Method
- Evaluation
- Discussion
- Conclusion

Our Method

- Overview (HODOR)

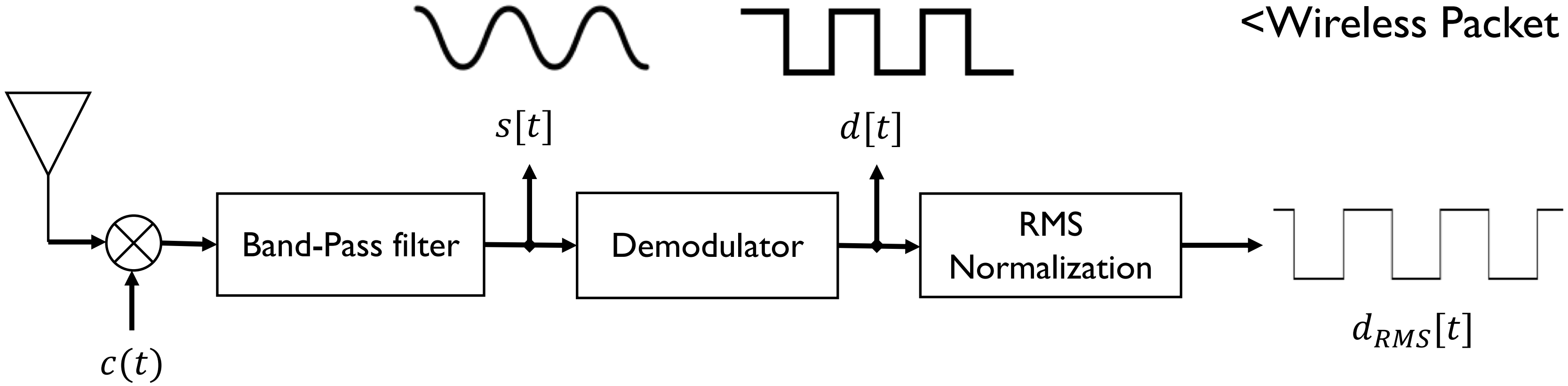


Our Method

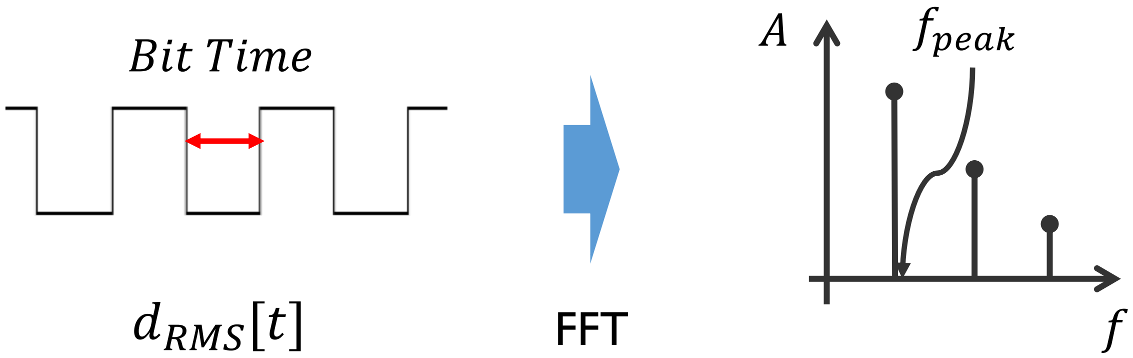


<Wireless Packet Structure>

- Preprocessing

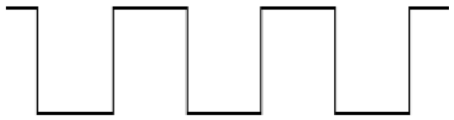


- Feature Extraction



Our Method

- Feature Extraction (Continue)



$d_{RMS}[t]$

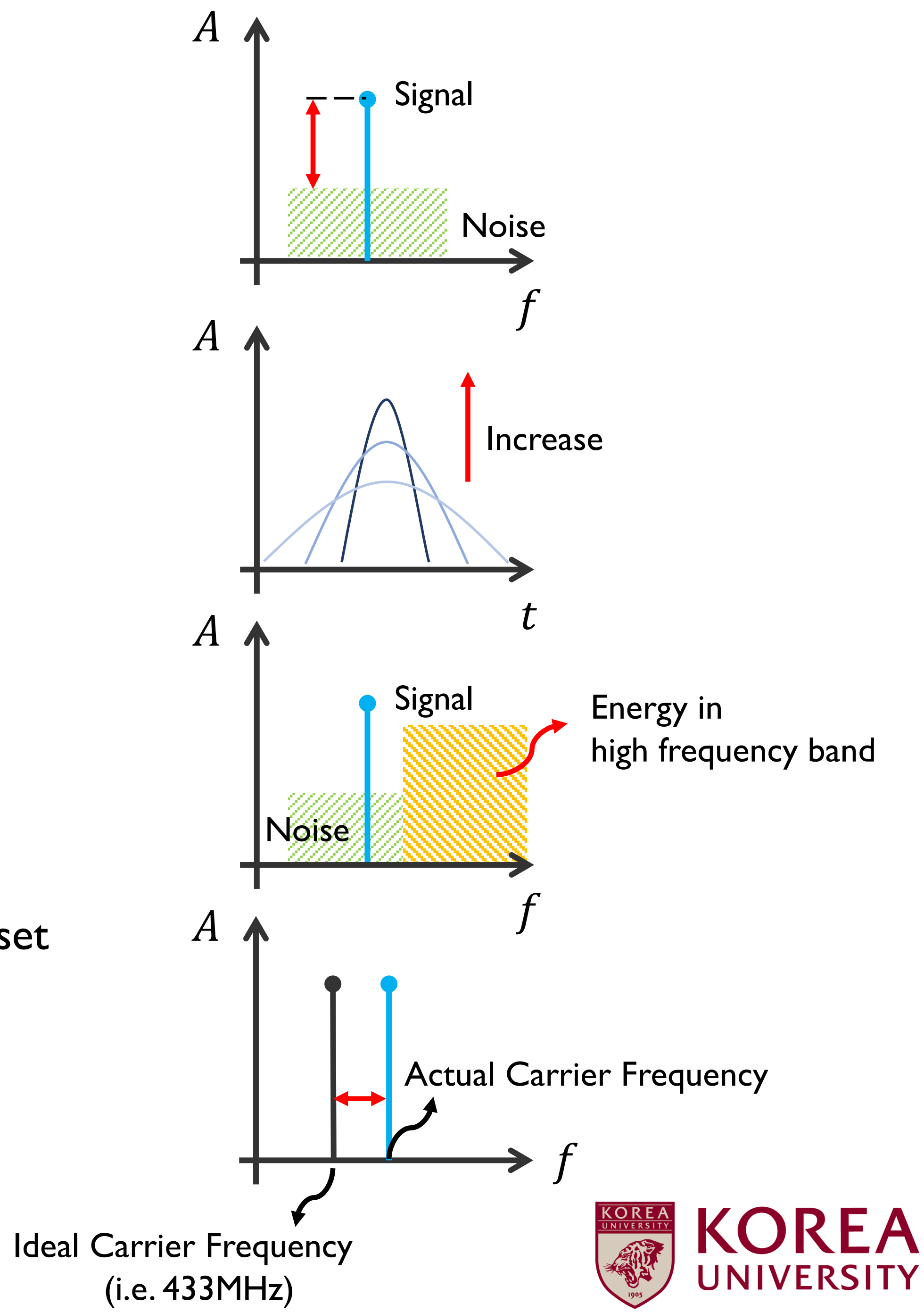
$s[t]$

SNR_{dB}

Kurtosis

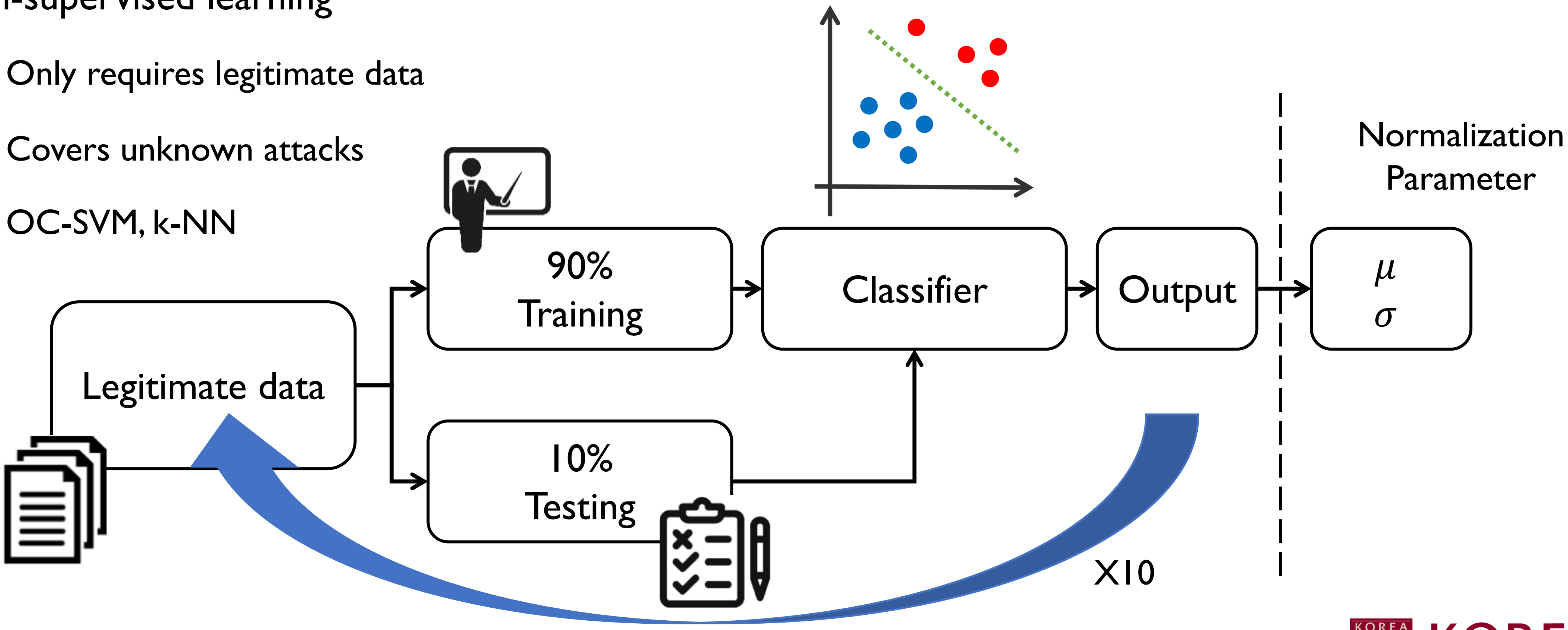
Spectral Brightness

Carrier Frequency offset



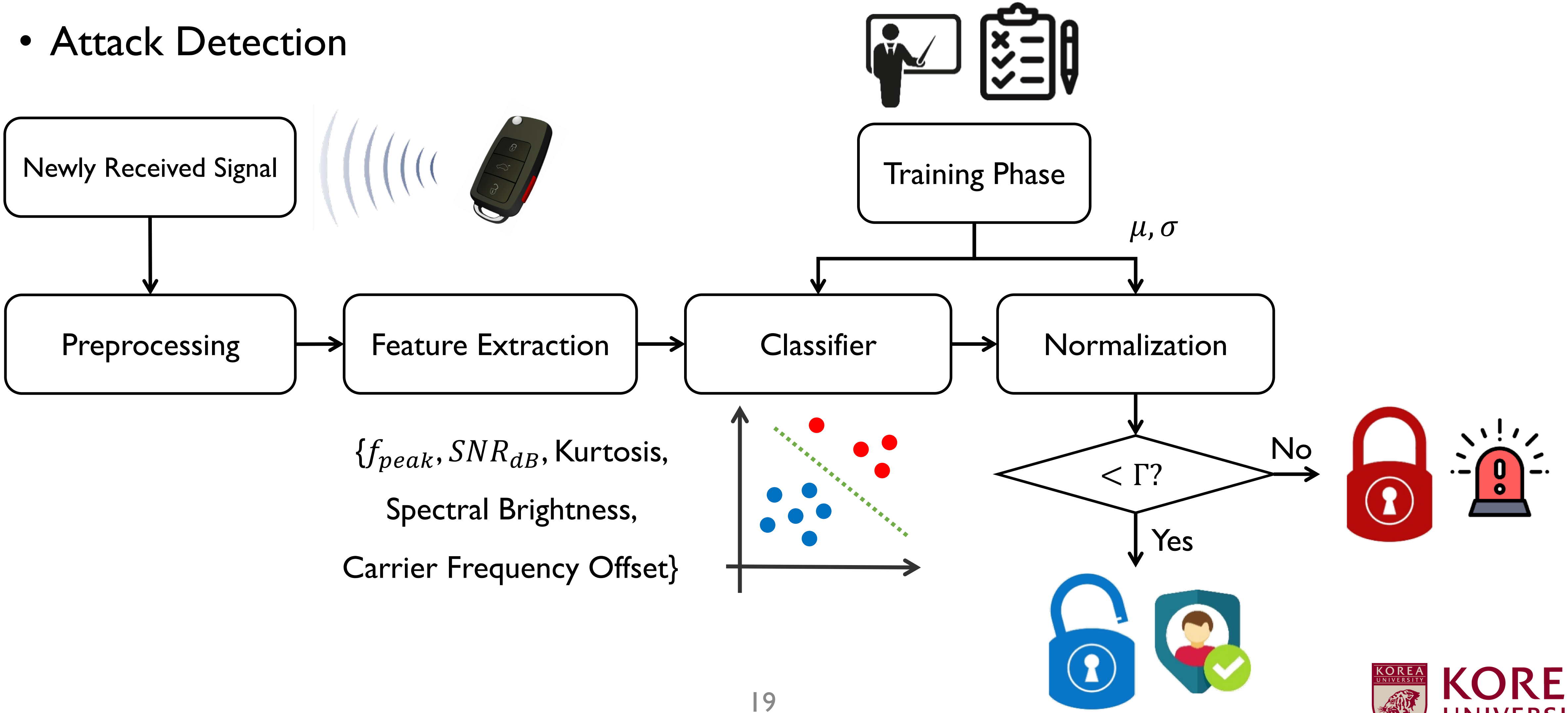
Our Method

- Training
  - Semi-supervised learning
    - Only requires legitimate data
    - Covers unknown attacks
    - OC-SVM, k-NN



Our Method

- Attack Detection



Newly Received Signal

Preprocessing

Feature Extraction

Classifier

Normalization

Training Phase

μ, σ

$\{f_{peak}, SNR_{dB},$ Kurtosis,

Spectral Brightness,

Carrier Frequency Offset$\}$

$< \Gamma?$

No

Yes

Outline

- Introduction / Background
- Attack Model
- Our Method
- Evaluation
- Discussion
- Conclusion

Evaluation

- Experimental Setup
  - Cars: KIA Soul, Volkswagen Tiguan
  - SDRs: HackRF One, USRP X310
  - SW: GNURadio
  - Loop Antenna, SMA Cable (Relay LF band signal)

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

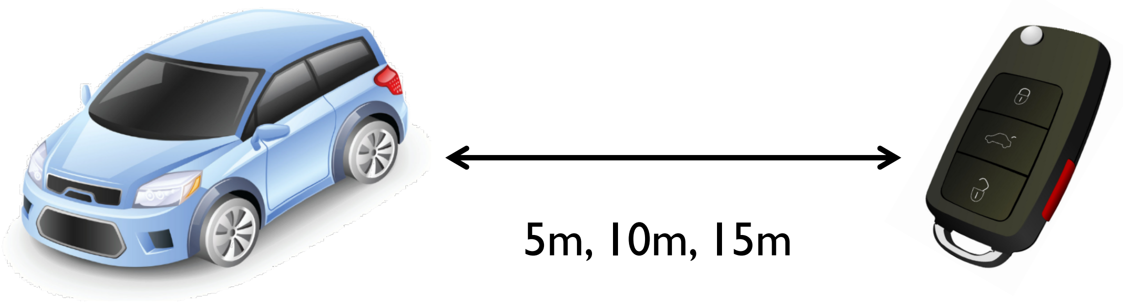
KOREA UNIVERSITY

Evaluation

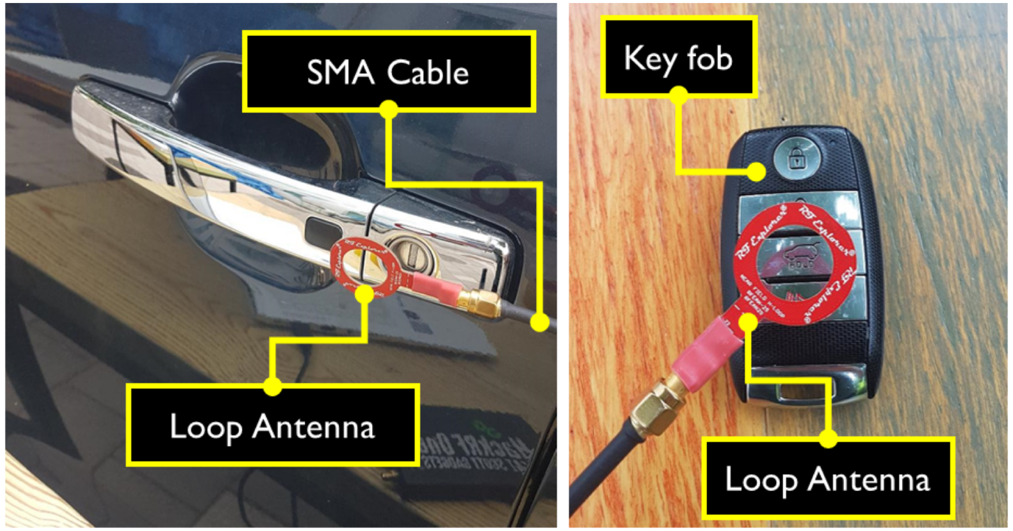
- Selected Classification Algorithms
  - One-Class SVM (OC-SVM) with Radial Basis Function (RBF) kernel
  - k-NN with Standardized Euclidean Distance
  - MatLab implementation
- Performance Metric
  - Assume False Negative Rate (FNR) as 0%
  - Calculate False Positive Rate (FPR)

Evaluation

- Single-Band Relay Attack Detection

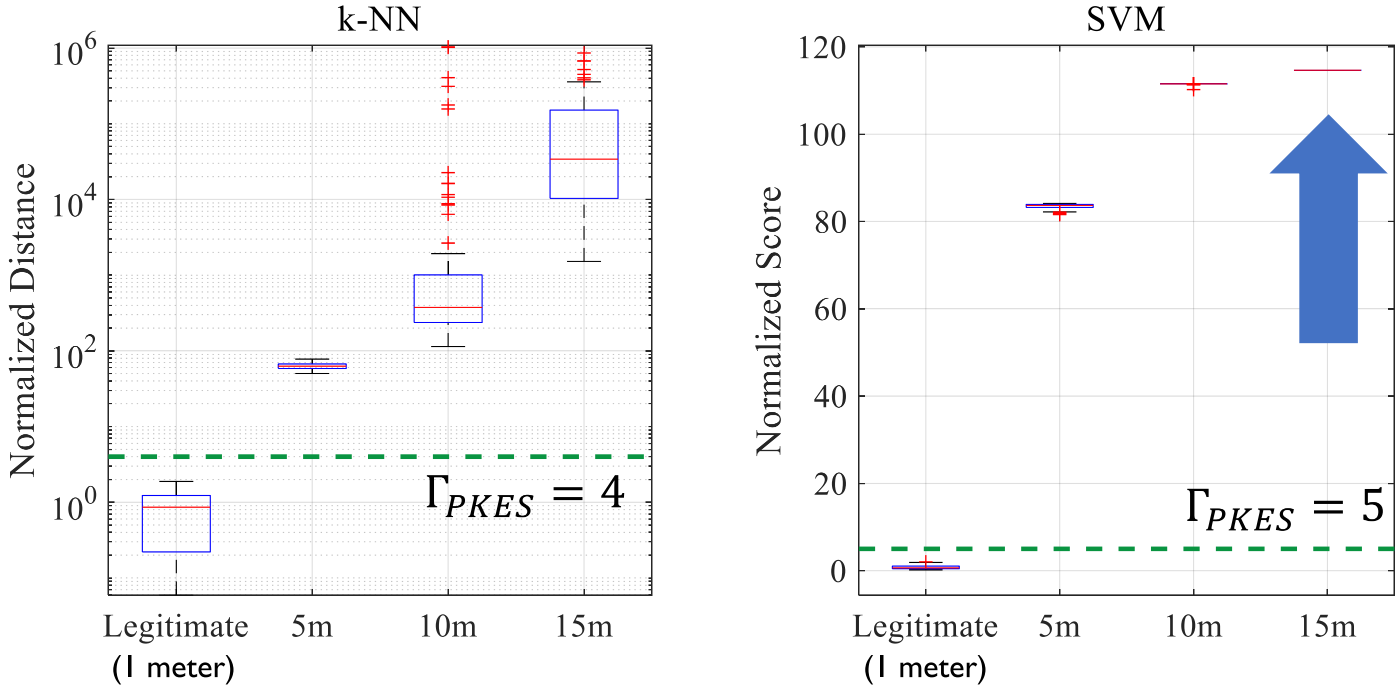


5m, 10m, 15m



Experimental Setup

(LF band signal relay)

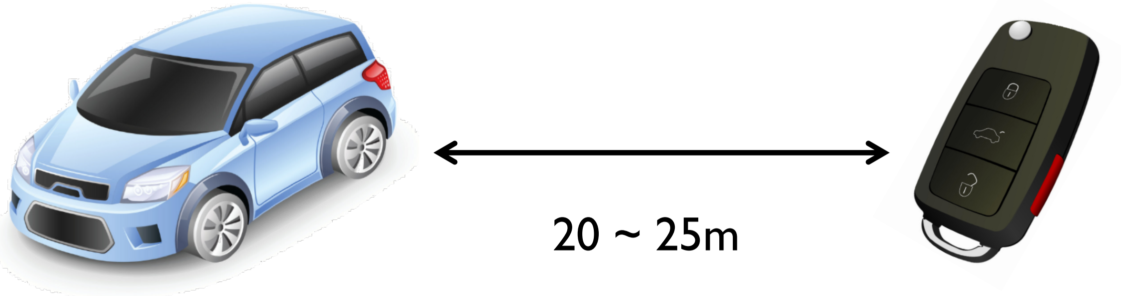


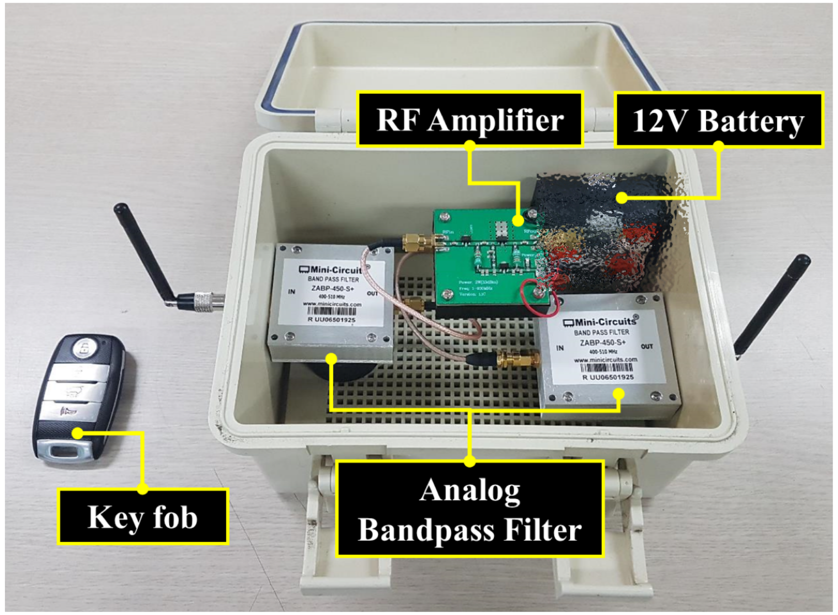
Results

(0% FPR in both algorithms)

Evaluation

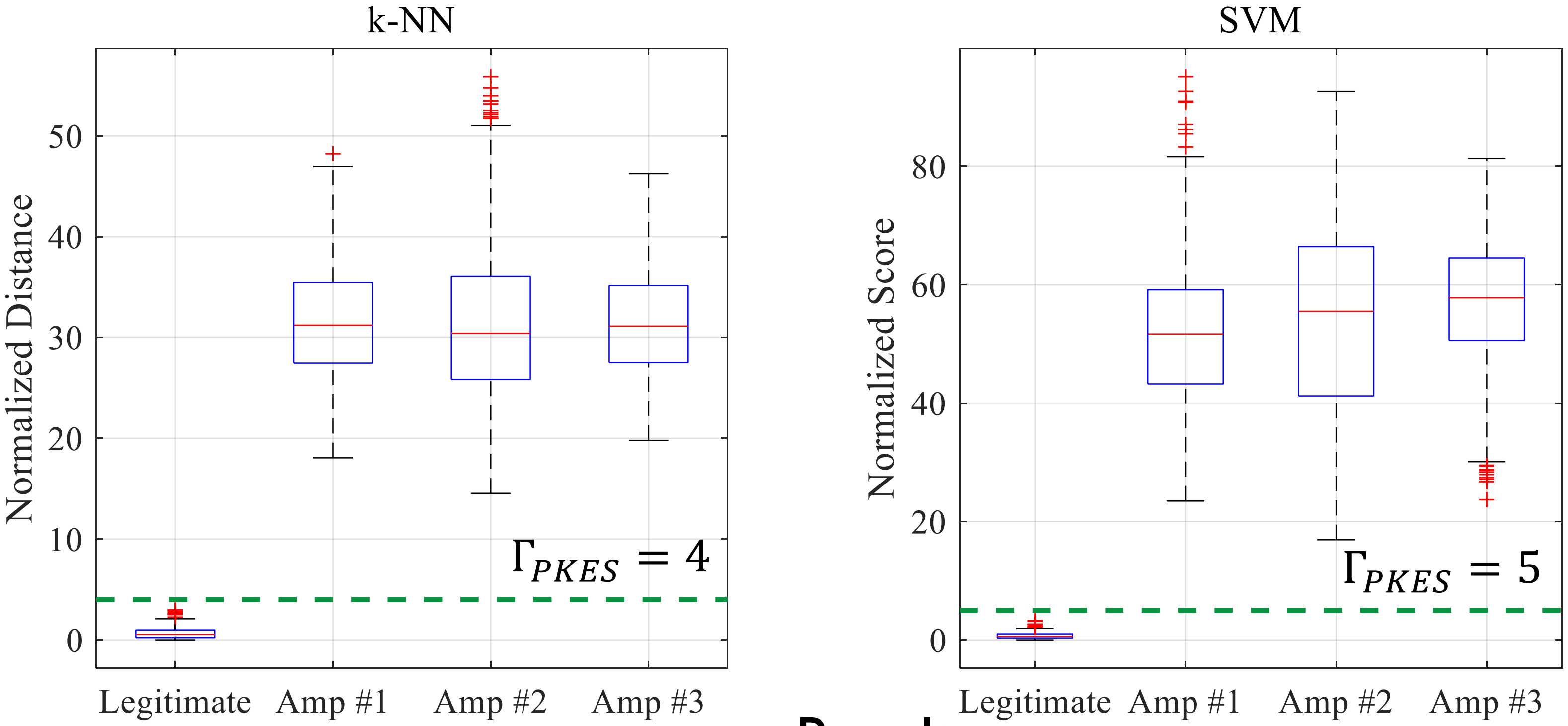
- Dual-Band Relay Attack Detection
  - Amplification Attack





Experimental Setup

(UHF band amplification)

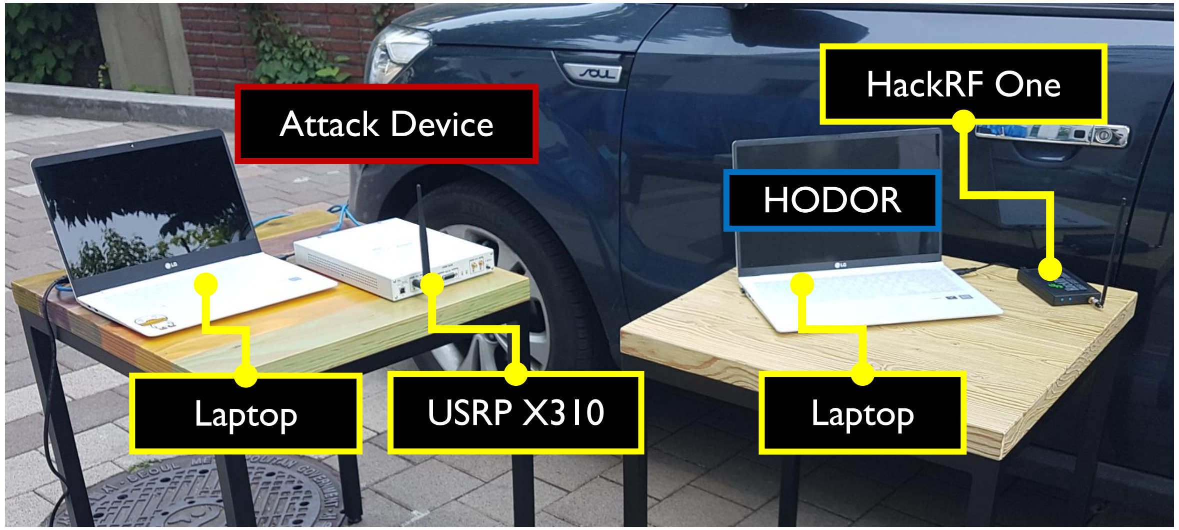


Results

(0% FPR in both algorithms)

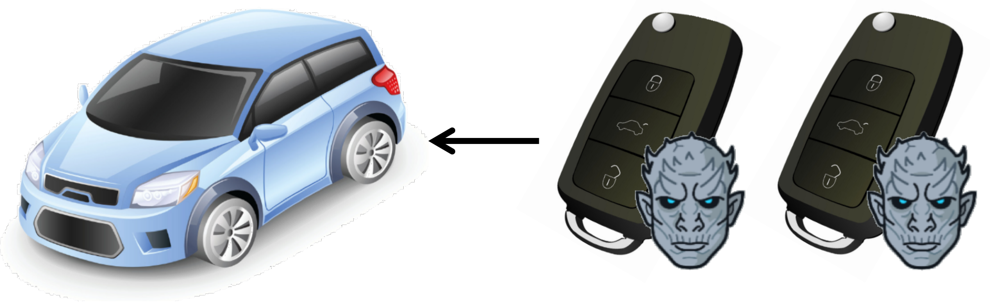
Evaluation

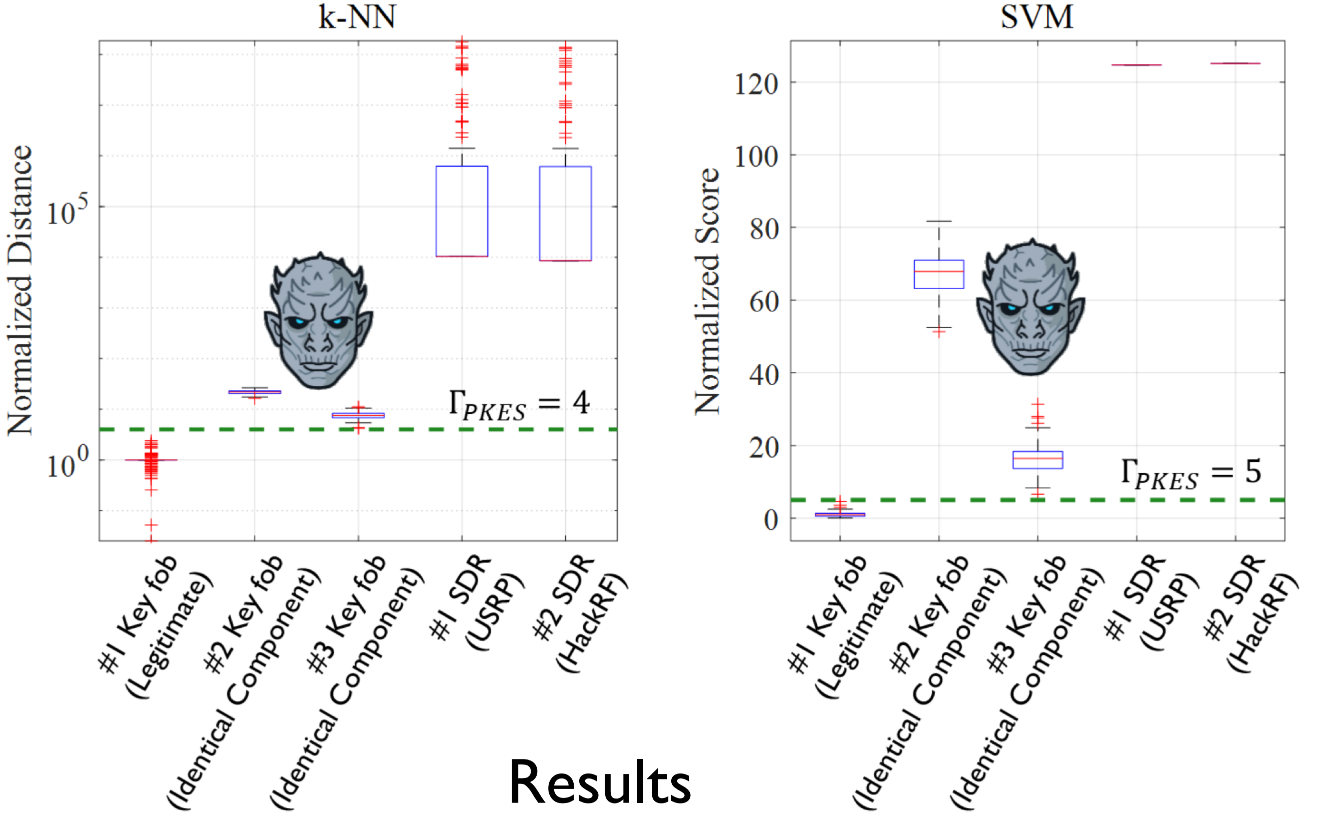
- Dual-Band Relay Attack Detection
  - Digital Relay/ Cryptographic Attack



Experimental Setup

(Cryptographic Attack)



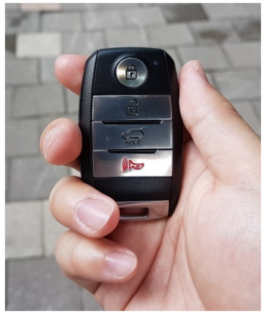


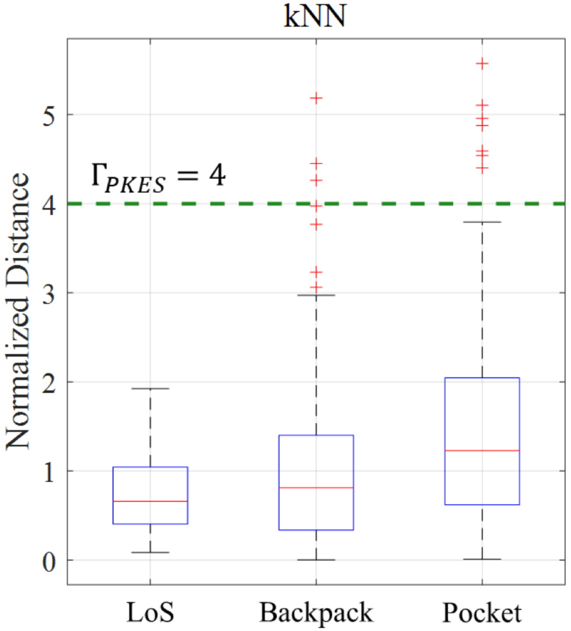
Results

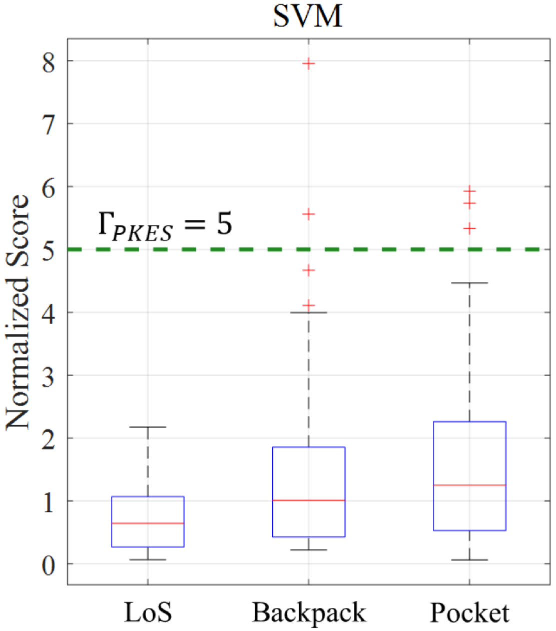
(Average FPR k-NN: 0.65%, SVM:0.27%)

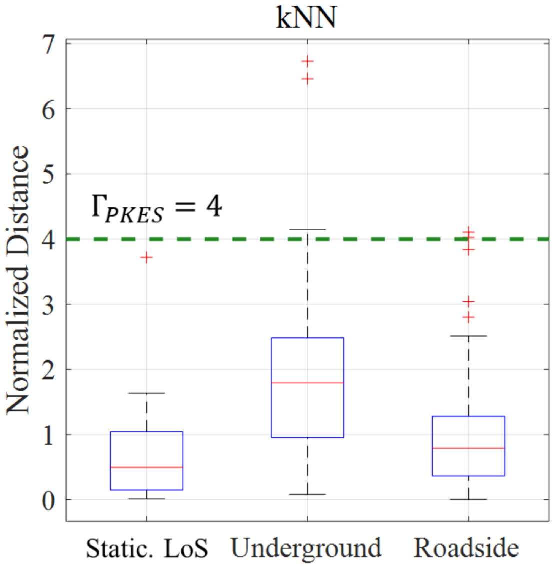
Evaluation

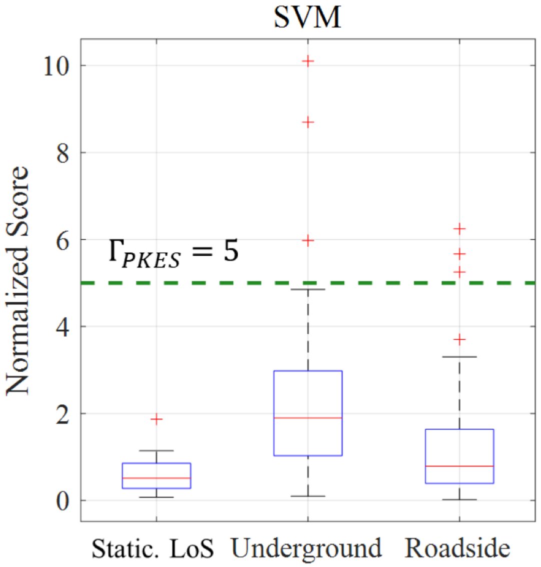
- Environmental Factors
  - Non-Line of Sight (NLoS) conditions, Dynamic Channel Conditions











Backpack: FPR k-NN: 1.32%, SVM:1.35%

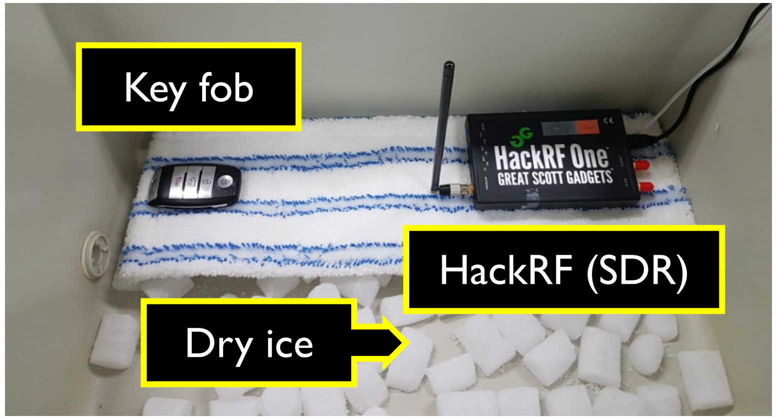
Pocket: FPR k-NN: 1.71%, SVM:1.67%

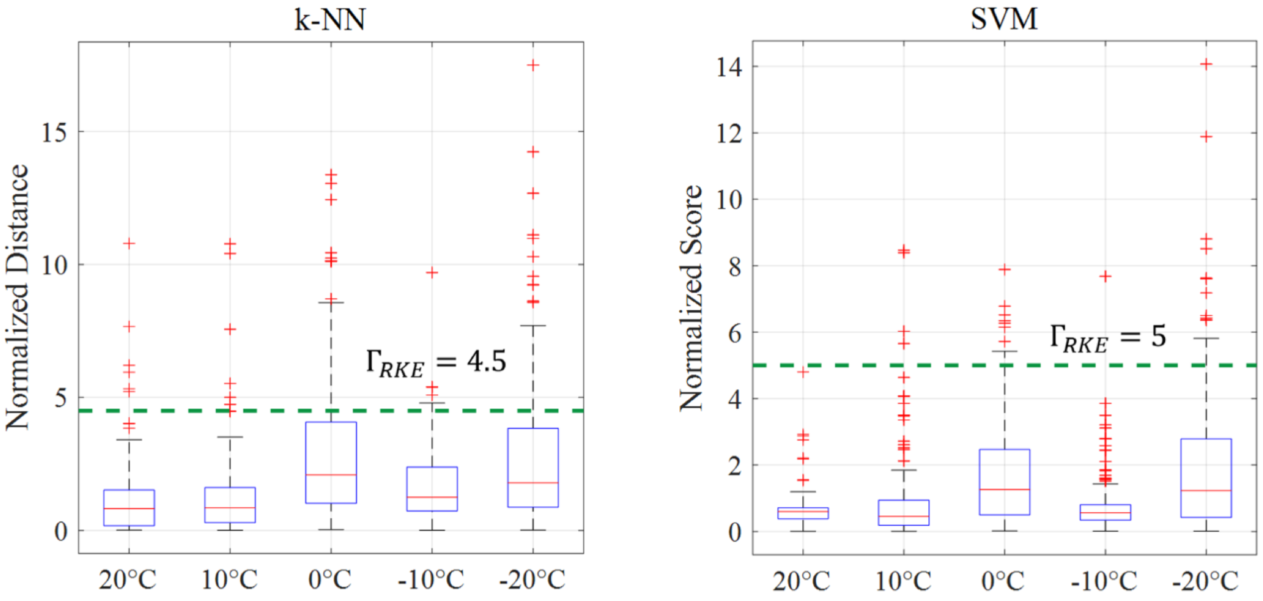
Underground: FPR k-NN: 5%, SVM:4%

Roadside: FPR k-NN: 2%, SVM:3%

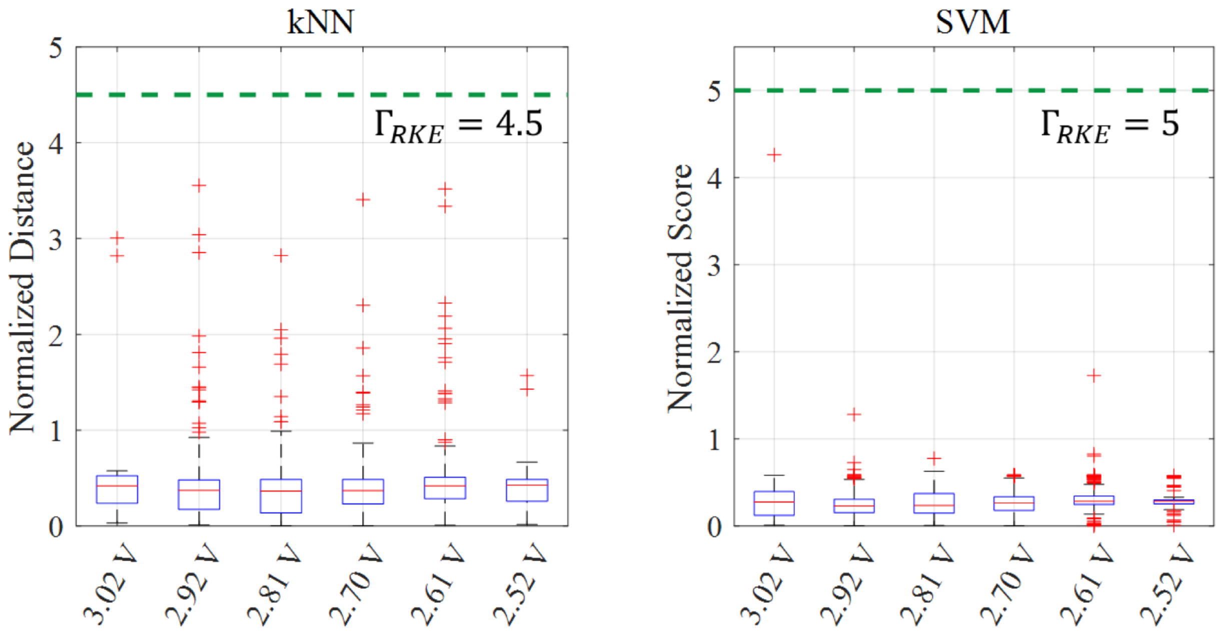
Appendix

- Environmental Factors
  - Signals from RKE system





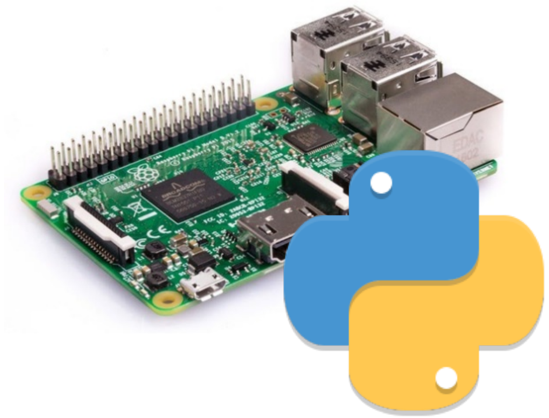
Average FPR k-NN: 6.36%, SVM:0.65%

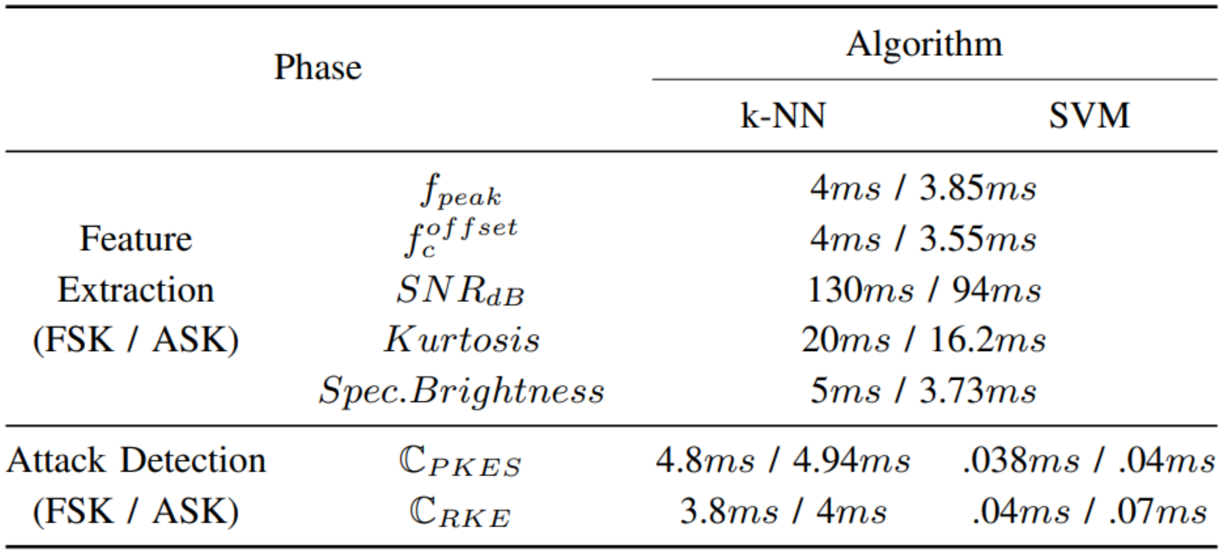


Average FPR k-NN: 0%, SVM:0%

Evaluation

- Execution time
  - Implementation on Raspberry Pi
    - 1.4Ghz Core, 1G RAM
  - Python Code





Phase		Algorithm	
		k-NN	SVM
Feature Extraction (FSK / ASK)	f_{peak}	4ms / 3.85ms	
	f_c^{offset}	4ms / 3.55ms	
	SNR_{dB}	130ms / 94ms	
	$Kurtosis$	20ms / 16.2ms	
	$Spec.Brightness$	5ms / 3.73ms	
Attack Detection (FSK / ASK)	$\mathbb{C}_{PKES}$	4.8ms / 4.94ms	.038ms / .04ms
	$\mathbb{C}_{RKE}$	3.8ms / 4ms	.04ms / .07ms

Total Execution Time

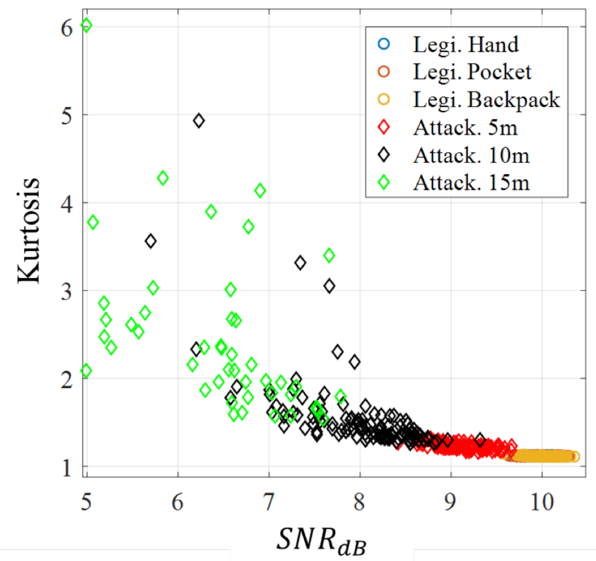
K-NN: 163.8ms and SVM: 159.038ms

Evaluation

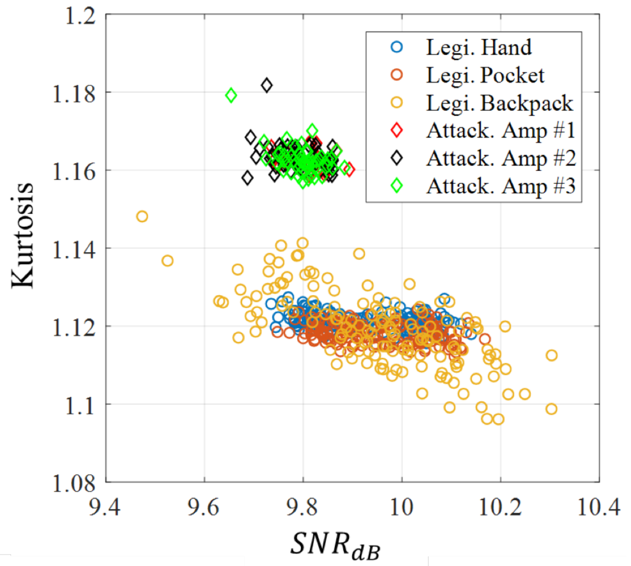
- Feature Importance
  - Utilizing Relief algorithm

Attack Scenario		Single-band Relay Attack	Amplification Attack	Digital Relay Attack	Playback Attack
Rank	1	**SNR**	**Kurtosis**	f_{peak}	**Spec. Brightness**
	2	Kurtosis	SNR	Kurtosis	Kurtosis
	3	Spec. Brightness	Spec. Brightness	Spec. Brightness	f_{peak}
	4	f_{peak}	f_{peak}	SNR	SNR

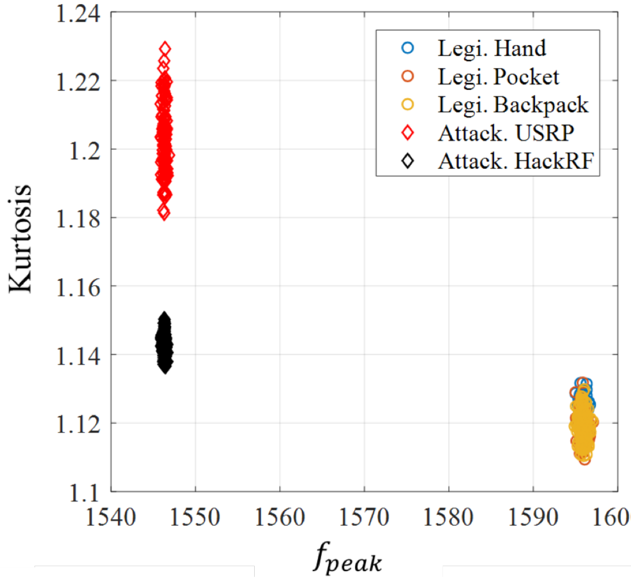
Single-band relay attack



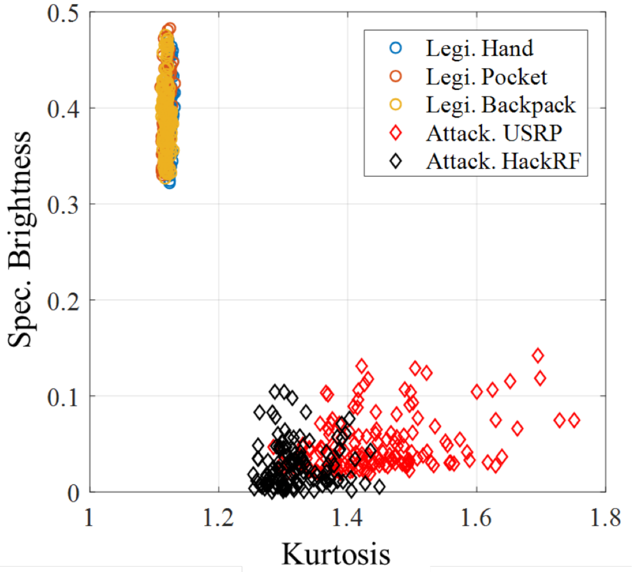
Amplification attack



Digital relay attack



Playback attack



Outline

- Introduction / Background
- Attack Model
- Our Method
- Evaluation
- Discussion
- Conclusion

Discussions

- HODOR and Security
  - Threshold is a trade-off parameter in HODOR
  - Small threshold leads to the false alarm; a large threshold leads to the false-negative (attack success)
- Feature Impersonation
  - Attacker must impersonate the whole feature at the same time
  - Impersonating a specific feature leads to a distortion in other features
- Practicality
  - Shortened execution time

Conclusion

- Proposed a sub-authentication system
  - Supports current systems to prevent keyless entry system car theft
- Effectively detect simulated attacks that are defined in our attack model
  - Reducing the number of erroneous detection occurrences (i.e., false alarms)
- Found a set of suitable features in a number of environmental conditions
  - Temperature variation, battery aging, and NLoS conditions

HODOR!

(Thank you!)

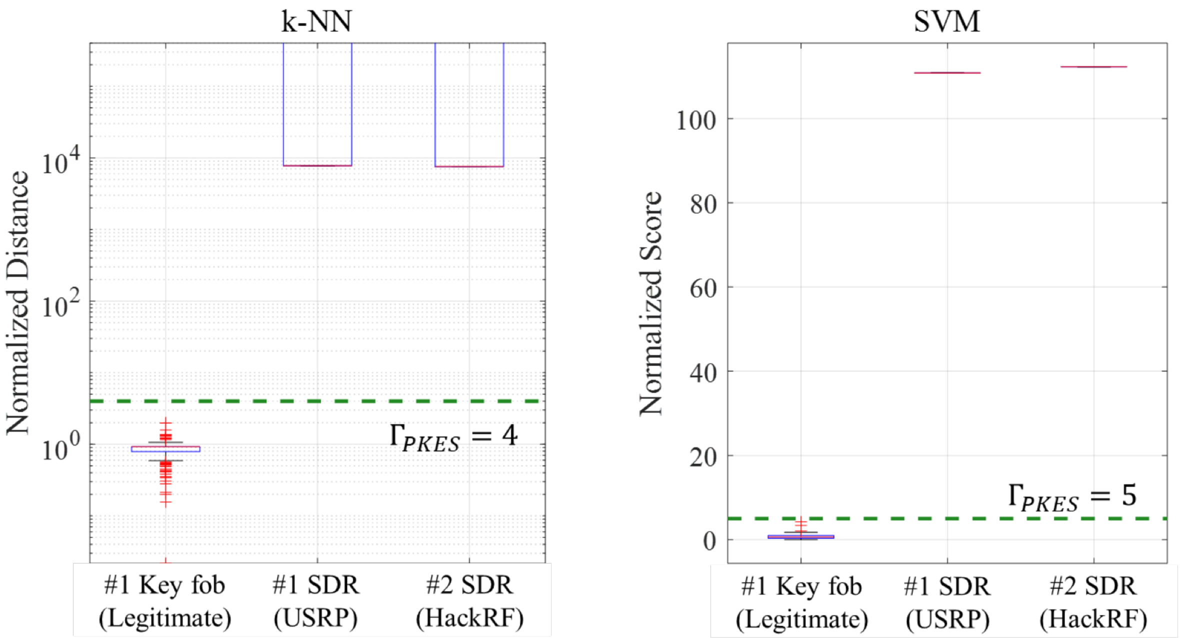
Q&A

This work was supported by Samsung Electronics

Appendix

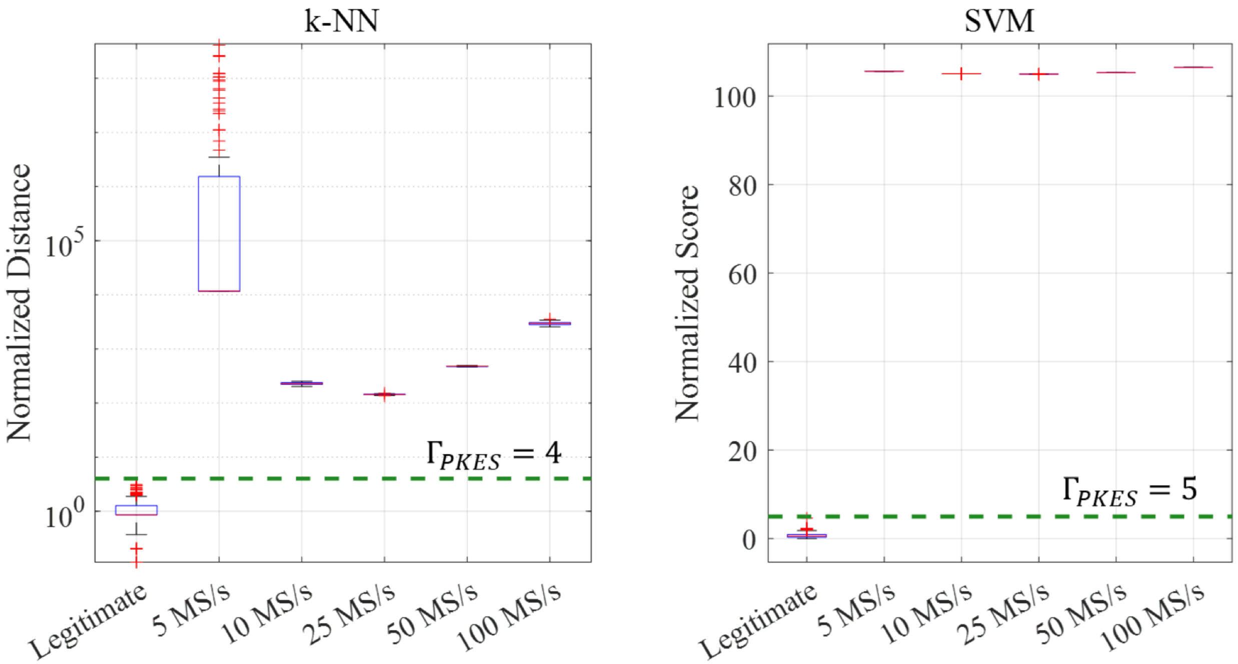
- Playback Attack Detection

Record & Playback
HackRF One
GREAT SCOTT GADGETS



Experimental Results

(SDR with 5MS/s)



Experimental Results

(USRP with various sample rate)