

# **SADS**

Spoofing Attack Detection System  
At Indoor Positioning using BLE

# Index

SADS

**01**

Background

**02**

System Design

**03**

Performance Evaluation

**04**

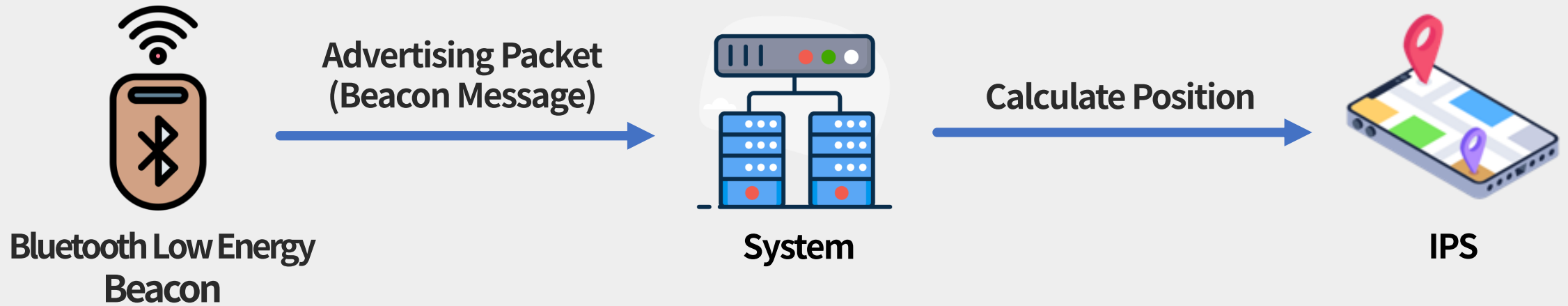
Result

## 01 Background – IPS

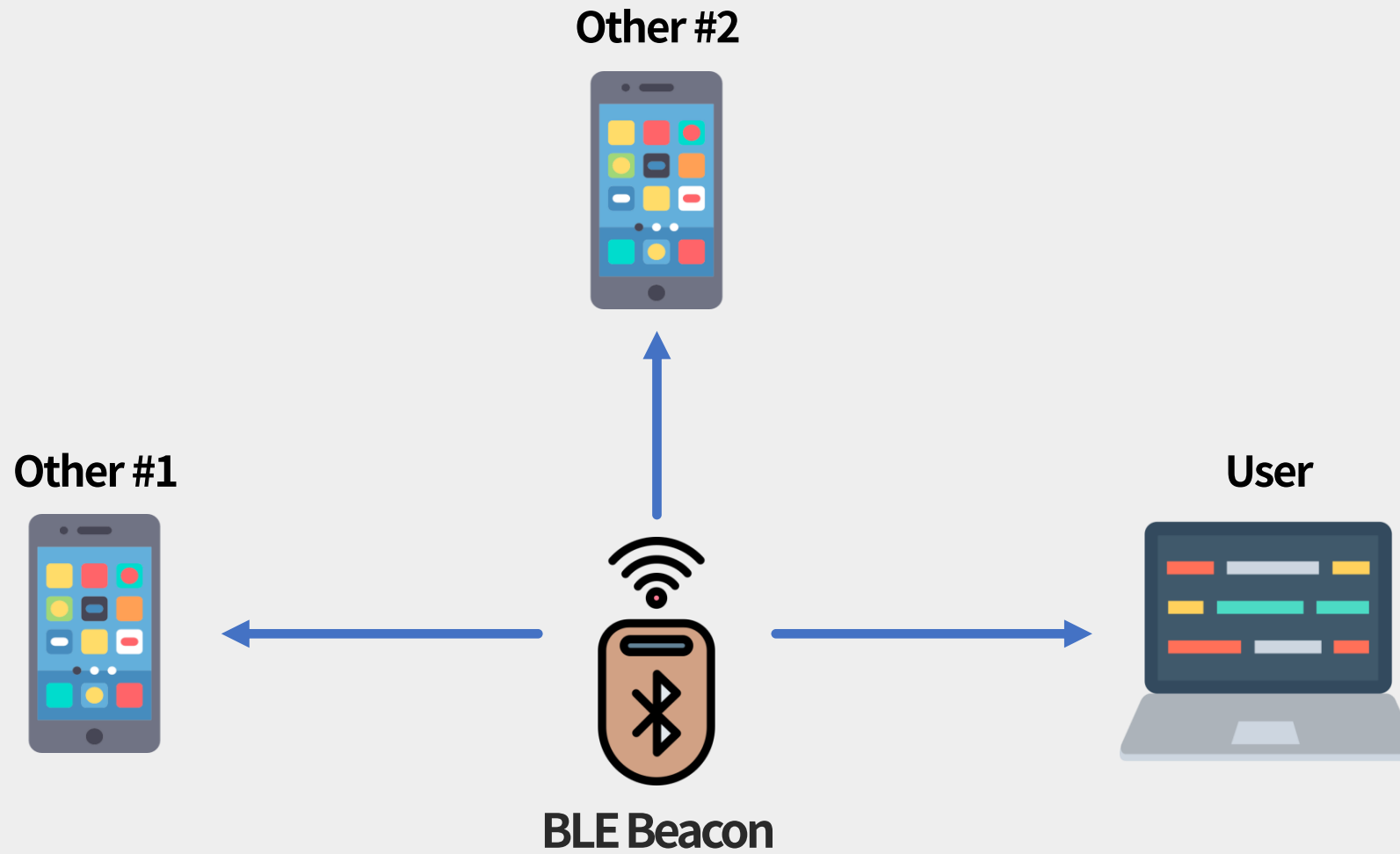
# Indoor Positioning System



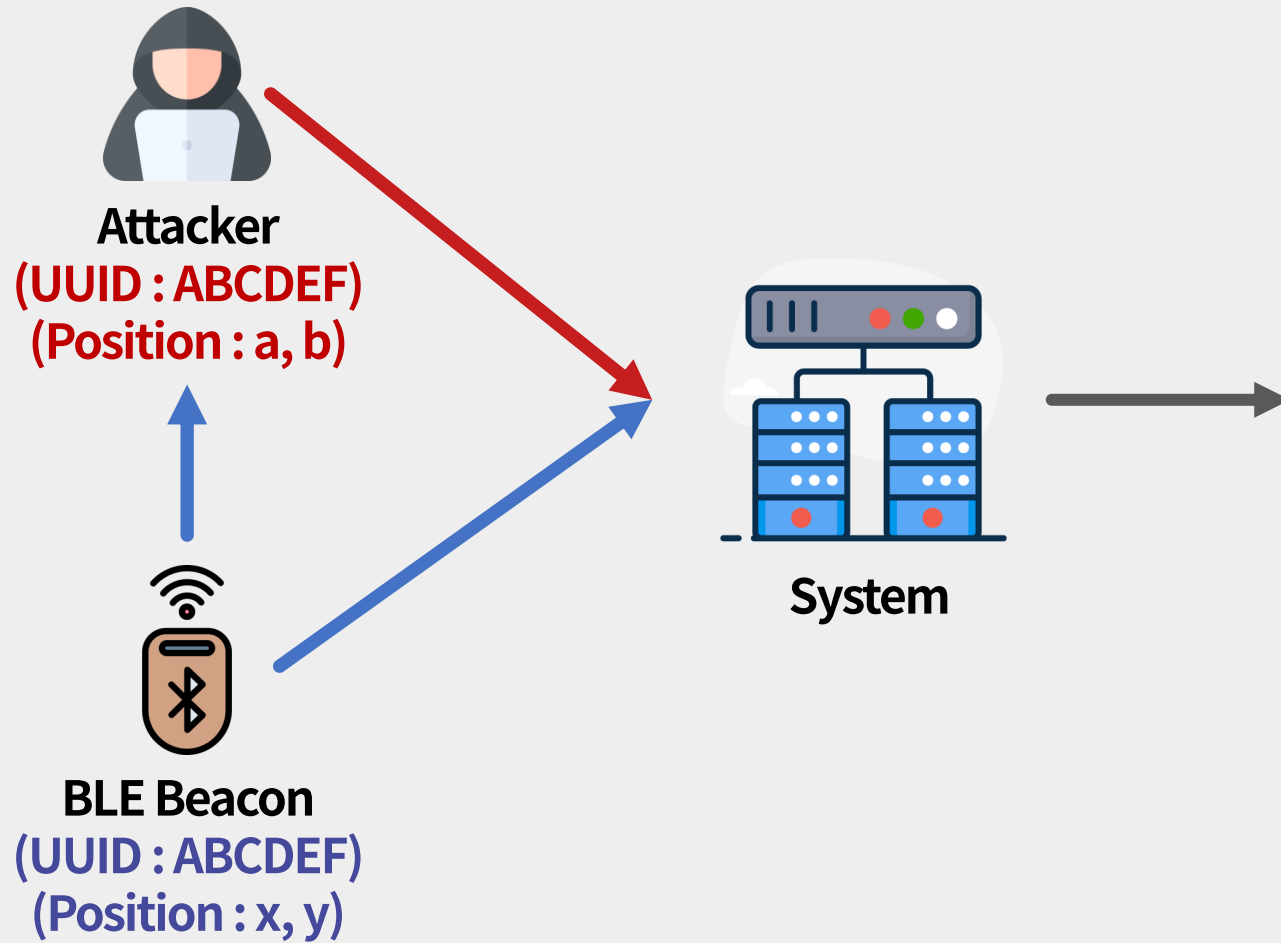
# 01 Background – BLE Beacon



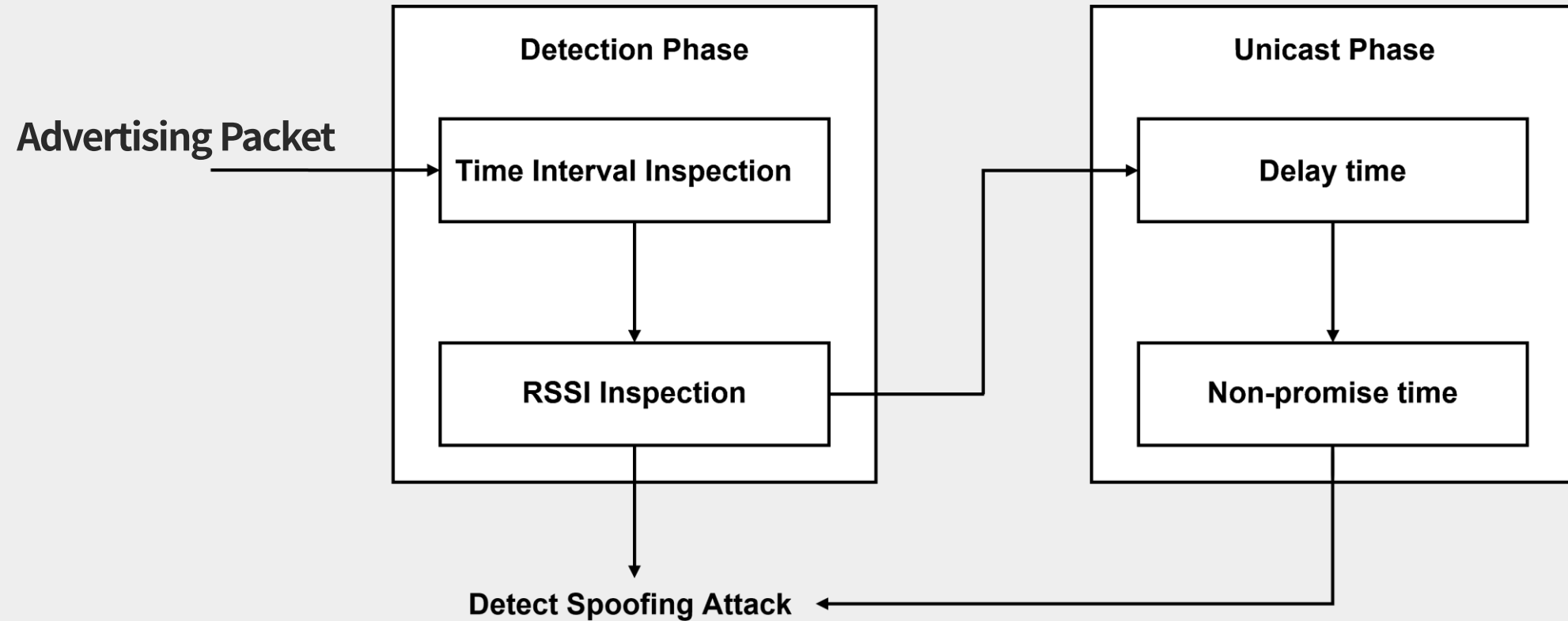
# 01 Background – Beacon Broadcast



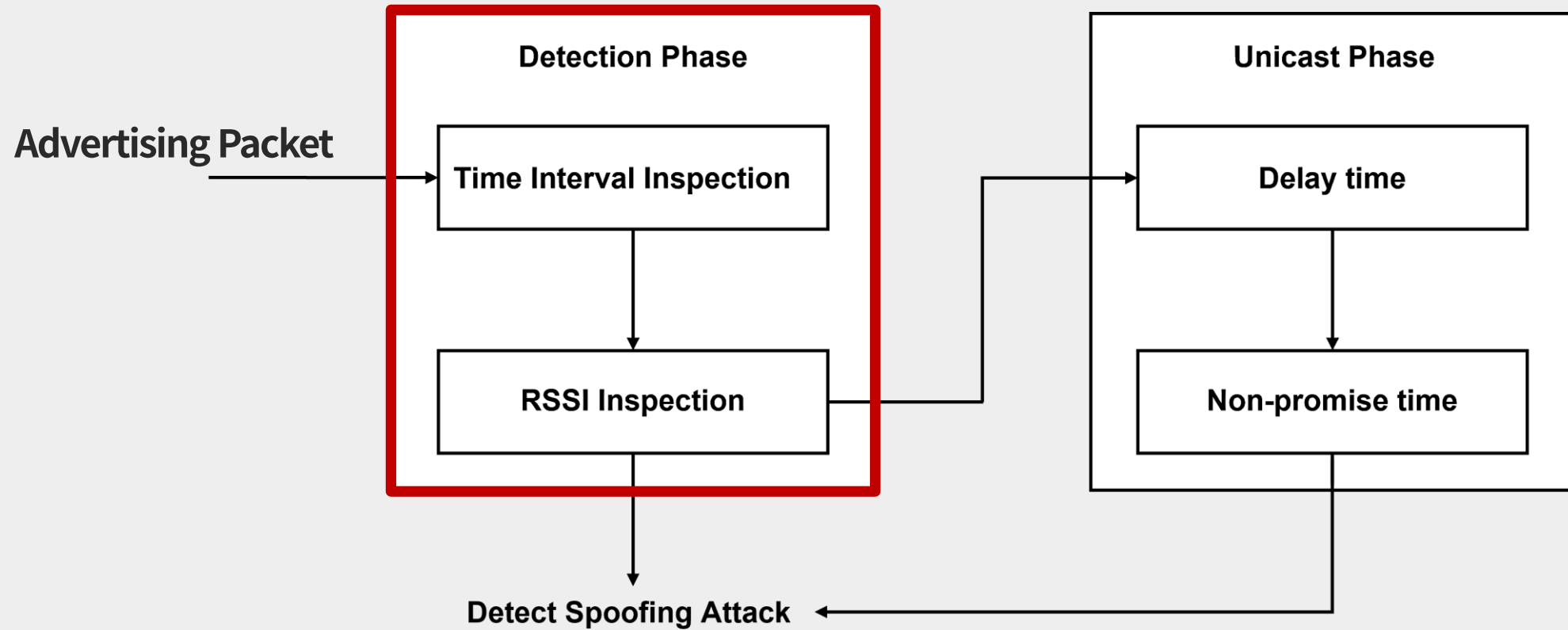
# 01 Background – Spoofing Attack on IPS



## 02 System Design – System Architecture



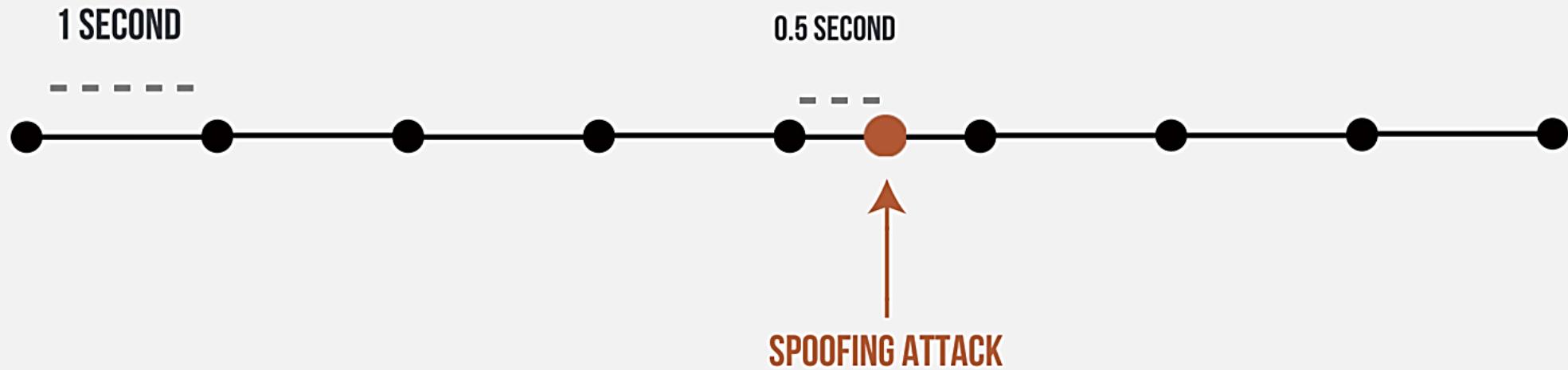
## 02 System Design – Detection Phase





## 02 System Design - Time Interval Inspection

● → RECEIVE ADVERTISING PACKET



## 02 System Design - Time Interval Inspection

Data Collection  
Process



Attack Inspection  
Process

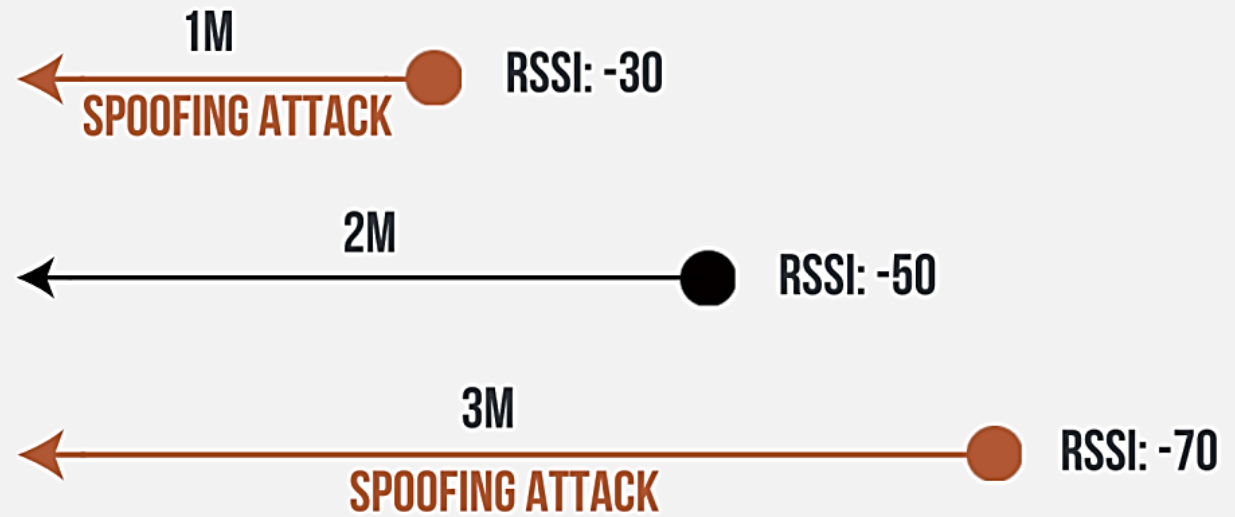
```
array([0.13903594, 0.27086401, 0.1410265, 0.12983084, 0.13377047,  
0.129565, 0.13679123, 0.13028932, 0.12855101, 0.13859153,  
0.13225484, 0.13605356, 0.13605714, 0.26212406, 0.13569713,  
0.40727139, 0.13730168, 0.12859988, 0.13983989, 0.13919306,  
0.4162488, 0.1372869, 0.13805246, 0.1303134, 0.12861204,  
0.13851595, 0.13357258, 0.13608646, 0.13928771, 0.27338481,  
0.1391573, 0.28028941, 0.13031459, 0.1286037, 0.13060451,  
0.13655567, 0.13444734, 0.13645554, 0.13431454, 0.13165903,  
0.13548613, 0.13032651, 0.12861896, 0.13730955, 0.27090859,  
0.13601017, 0.13614559, 0.13933253, 0.26389003, 0.13868809,  
0.13677359, 0.13035607, 0.13349867, 0.13069105, 0.13156629,  
0.13676906, 0.13917208, 0.13481236, 0.13810039, 0.13542295,  
0.12855744, 0.13306618, 0.13912535, 0.14115357, 0.13306975,  
0.13901281, 0.2709291, 0.13552809, 0.13915944, 0.14123201,  
0.12863588, 0.13047528, 0.13663793, 0.13060403, 0.13785195,  
0.13735318, 0.1322875, 0.14116859, 0.13108945, 0.13737416,  
0.13109231, 0.13862371, 0.13935828, 0.13908315, 0.13436842,  
0.27088761, 0.26602507, 0.26845694, 0.13161182, 0.13810444,  
0.13165212, 0.13104439, 0.13992715, 0.12858057, 0.13614225,  
0.13230777, 0.14119458, 0.13231206, 0.1373632, 0.1381681 ])
```

< Real Time Interval Data >

```
/// Current INT: 0.13417553901672363  
Prediction Next INT: 0.13469626637804763  
Calculated Next Lower INT: 0.12187343180217869
```

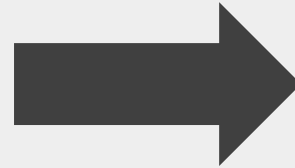
## 02 System Design - RSSI Inspection

● → THE BENIGN USER



## 02 System Design - Time Interval Inspection

Data Preprocessing  
Process



Attack Inspection  
Process

```
array([[ -39, -40, -37, -34, -40, -39, -42, -42, -40, -40, -44,
        -39, -40, -44, -36, -40, -40, -42, -39, -35, -39, -39,
        -40, -37, -42, -42, -39, -35, -41, -40, -37, -39, -40,
        -39, -44, -35, -40, -37, -37, -39, -36, -34, -39, -41,
        -34, -34, -41, -39, -44, -35, -40, -39, -41, -40, -39,
        -39, -34, -35, -36, -43, -43, -40, -35, -39, -42, -39,
        -35, -40, -44, -39, -34, -41, -39, -39, -35, -40, -42,
        -39, -39, -44, -40, -36, -34, -40, -42, -39, -40, -42,
        -40, -39, -39, -39, -35, -37, -42, -39, -39, -39, -34,
        -43, -44, -40, -39, -44, -35, -34, -42, -39, -34, -39,
        -39, -39, -41, -41, -39, -40, -42, -42, -39, -39, -35,
        -42, -39, -42, -44, -39, -35, -40, -37, -42, -40, -35,
        -40, -39, -35, -42, -39, -42, -42, -44, -40, -40, -39,
        -39, -39, -36, -39, -39, -35, -42, -39, -34, -40, -39,
        -35, -42, -40, -44, -35, -34, -40, -40, -39, -40, -34,
        -39, -40, -43, -39, -39, -40, -36, -42, -40, -35, -42,
        -39, -39, -42, -41, -39, -35, -39, -35, -41, -40, -42,
        -34, -35, -39, -39, -35, -39, -39, -44, -35, -42, -40,
```

< Real RSSI Data >

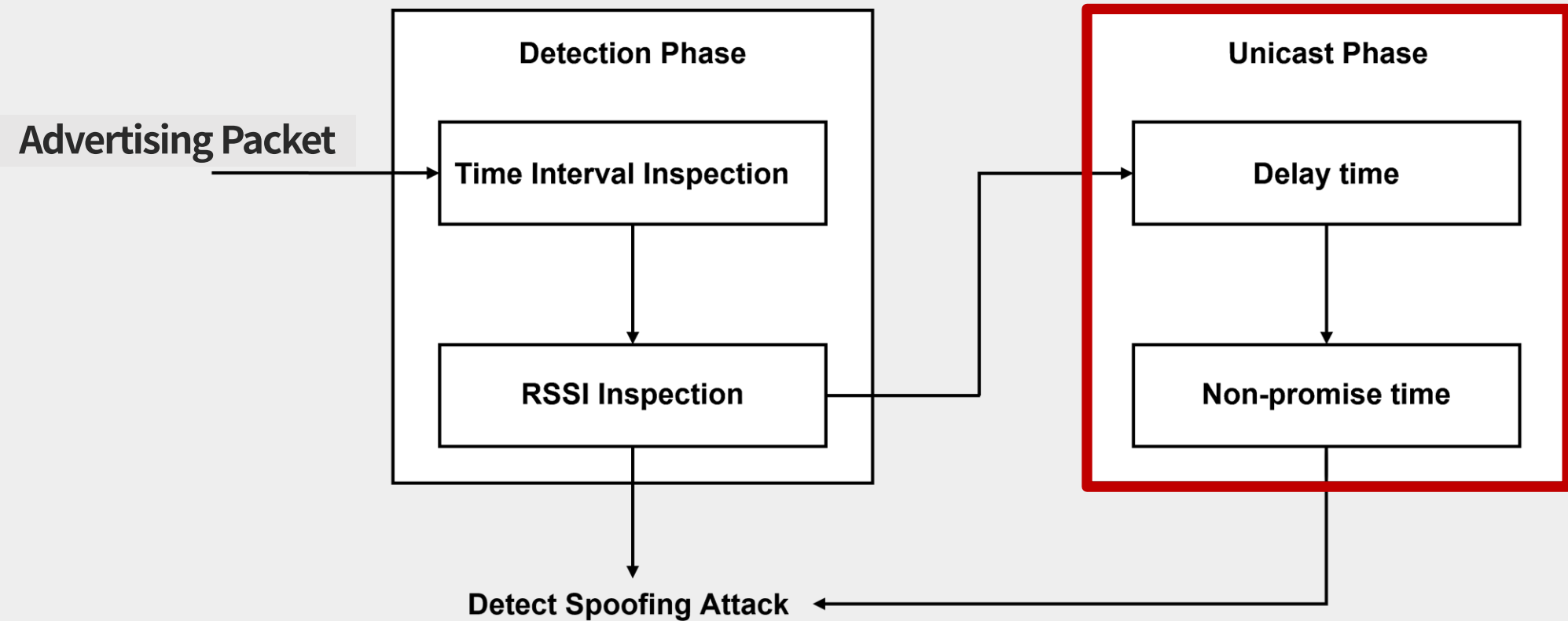
```
/// Current RSSI:  -45.84083483531045
Prediction Next RSSI:  -46.15979446087739
Calculated Next Lower RSSI:  -47.741109089177286
Calculated Next Upper RSSI:  -44.5784798325775
```

## 02 System Design - RSSI Inspection

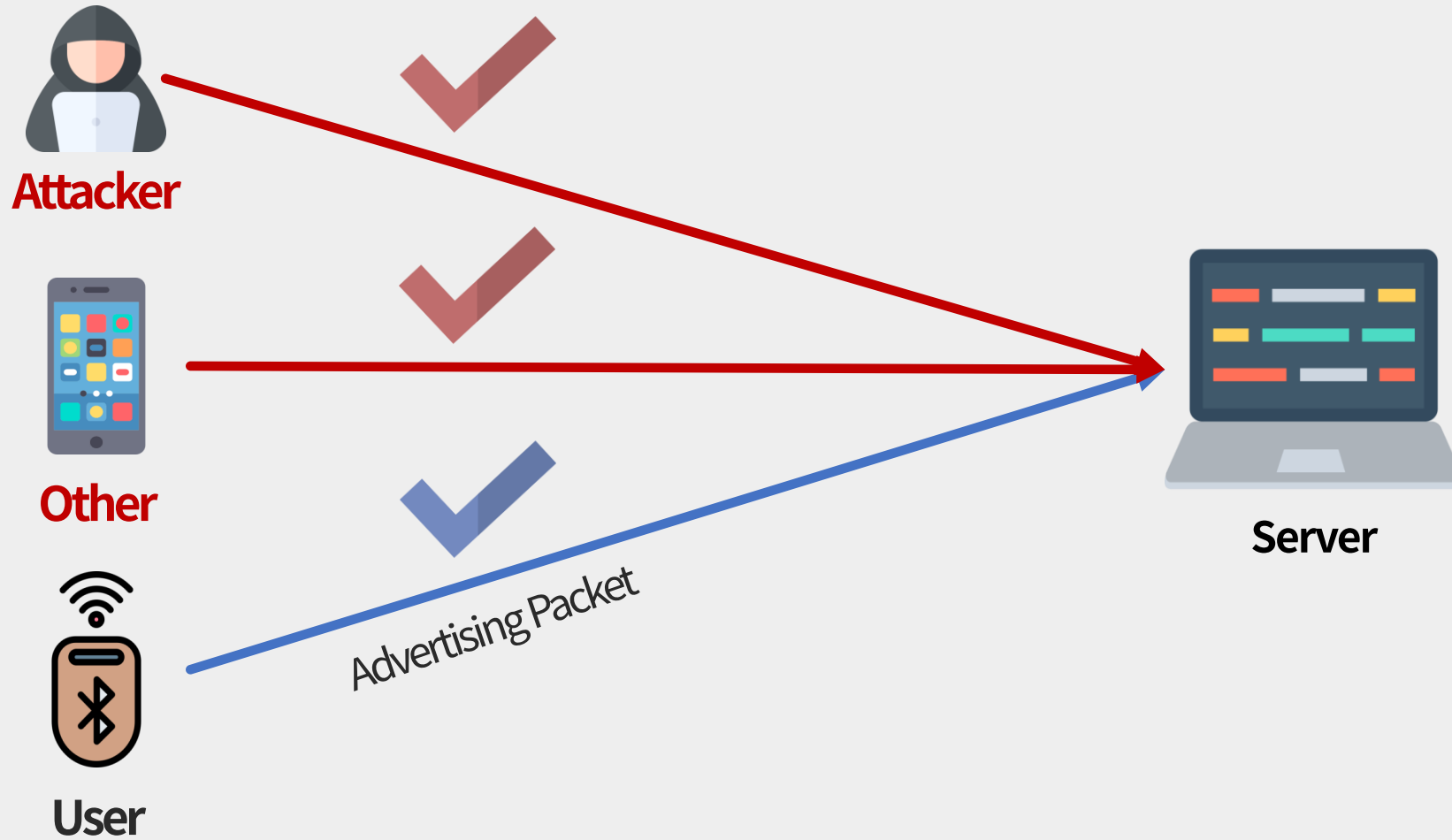
● → THE BENIGN USER



## 02 System Design - Unicast Phase



## 02 System Design - Unicast Phase



## 02 System Design - Unicast Phase (Non-Promise Time)

### Non-Promise Time





## 02 System Design - Unicast Phase

Data Exchange  
Process



Attack Inspection  
Process

```
array([4, 5, 2, 4, 2, 5, 6, 3, 5, 5, 3, 3, 2, 4, 4, 5, 6,  
       3, 4, 3, 4, 3, 4, 7, 5, 6, 4, 4, 4, 5, 3, 6, 4, 3,  
       7, 5, 7, 4, 7, 5, 3, 3, 4, 5, 2, 4, 2, 5, 7, 3, 5,  
       2, 3, 3, 3, 2, 3, 2, 5, 2, 5, 5, 5, 3, 5, 2, 4, 5,  
       3, 5, 5, 5, 4, 3, 6, 4, 5, 5, 4, 4, 4, 3, 4, 3, 2,  
       7, 3, 2, 4, 2, 4, 3, 3, 2, 4, 2, 5, 5, 4, 3, 4, 7,  
       3, 5, 2, 4, 5, 5, 3, 3, 6, 4, 5, 5, 2, 4, 3, 5, 6,  
       4, 4, 2, 3, 2, 5, 7, 3, 3, 4, 6, 4, 6, 3, 4, 3, 7,  
       5, 3, 7, 5, 3, 4, 5, 3, 5, 3, 7, 4, 7, 4, 4, 4, 3,  
       3, 3, 2, 4, 6, 3, 3, 4, 5, 4, 3, 3, 6, 4, 7, 5, 3,  
       6, 5, 6, 5, 6, 3, 6, 3, 3, 3, 7, 4, 7, 3, 6, 3, 6,  
       6, 5, 4, 3, 4, 5, 4, 4, 7, 3, 3, 3, 7, 3, 6, 5, 2,  
       6, 5, 4, 5, 2, 4, 2, 5, 7, 5, 5, 5, 3, 4, 7, 5, 4,  
       2, 5, 2, 3, 3, 3, 3, 4, 7, 5, 7, 4, 6, 4, 5, 3, 5,  
       7, 4, 6, 5, 4, 3, 7, 4, 2, 3, 5, 4, 7, 3, 4, 3, 5])
```

< Random Time Array >

Odd Index  
( Delay Time )

**Delay Time :**

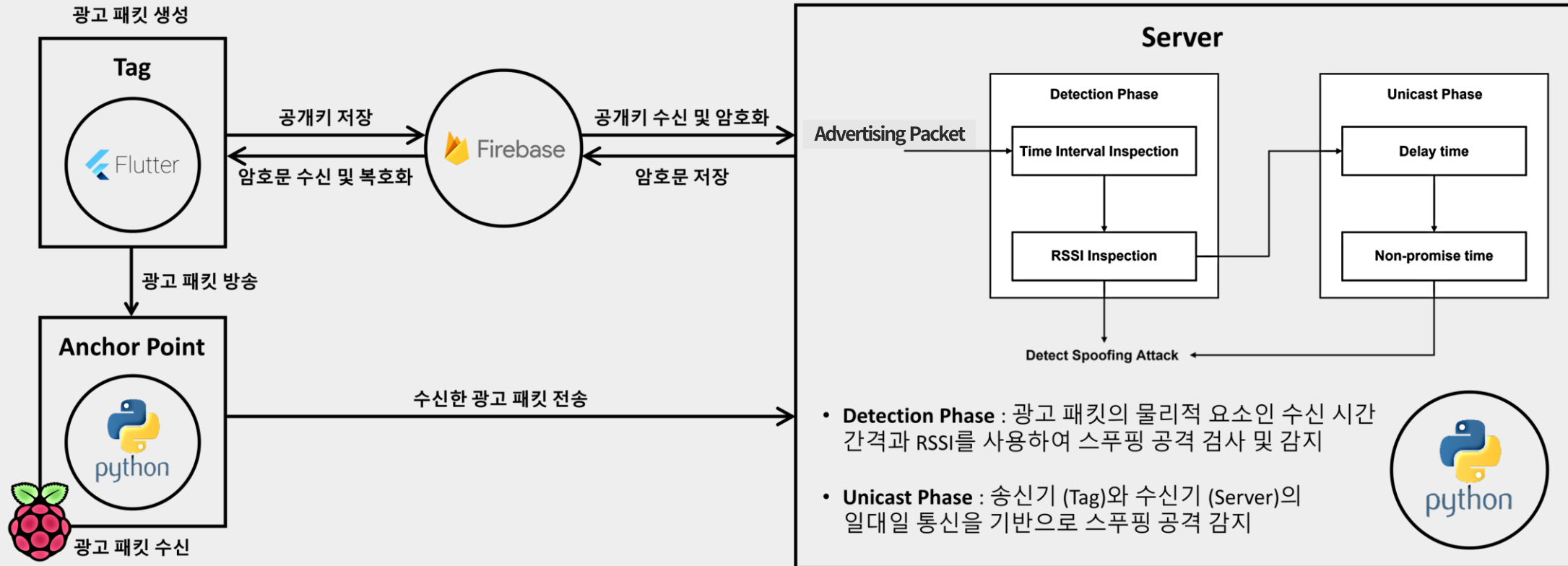
- 공격자가 시스템이 언제 Non-promise Time으로 바뀌는지 모르게 하기 위해 의도적으로 추가한 지연 시간
- Tag는 광고 패킷을 송신하고 Server는 광고 패킷을 수신 받지 않는 시간

Even Index  
( Non-promise Time )

**Non-promise Time :**

- 해당 시간에 들어오는 광고 패킷을 스푸핑 공격으로 간주
- Tag는 광고 패킷을 송신하지 않고 Server 또한 광고 패킷을 수신 받지 않는 시간

### 03 Performance Evaluation – Experiment Environment



### 03 Performance Evaluation – Use Data

광고 패킷의 수신 속도	빠름 (평균 0.03s)	보통 (평균 0.13s)	느림 (평균 0.35s)
공격자와 사용자의 거리	0m	1m	2m
검사에 사용된 데이터 개수	50개	100개	500개

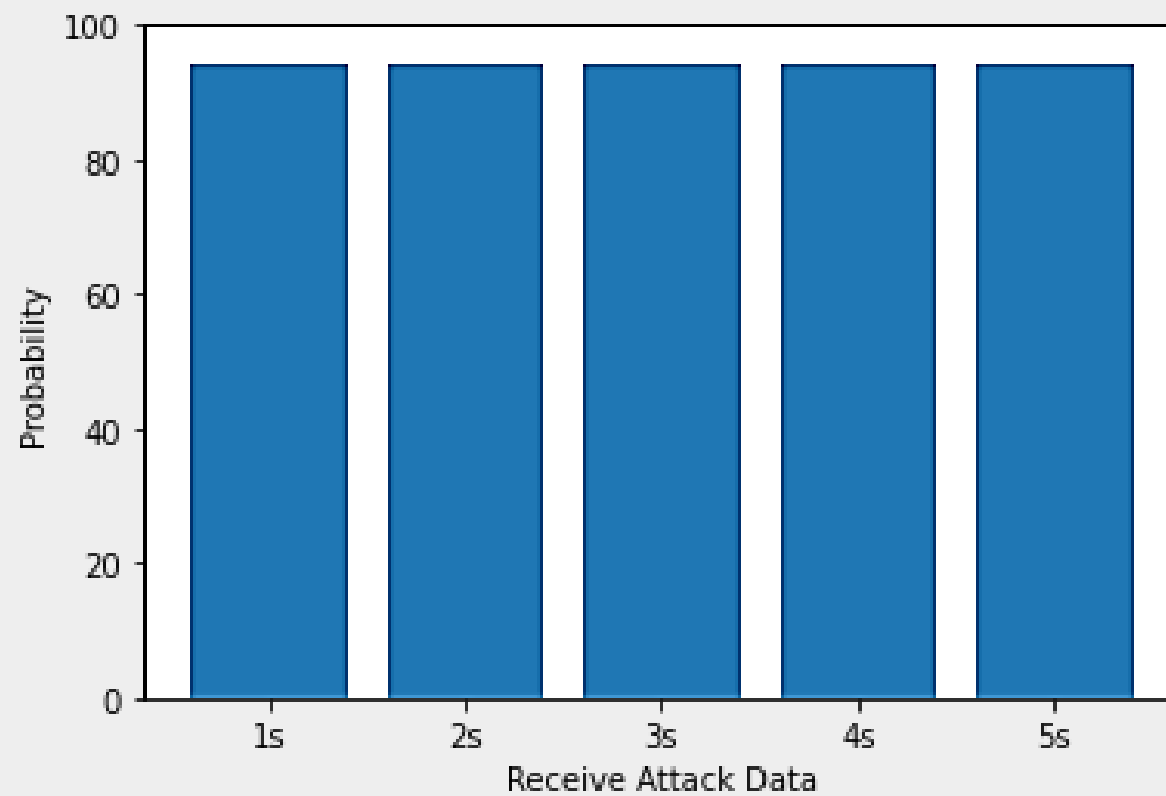
**X**

스푸핑 공격 진행 시간	1초	2초	3초	4초	5초
-----------------	----	----	----	----	----

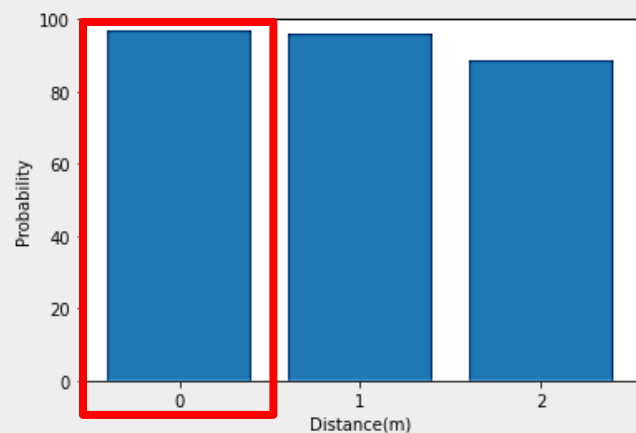
**||**

**13,500 csv (3,000,000 Advertising Packet)**

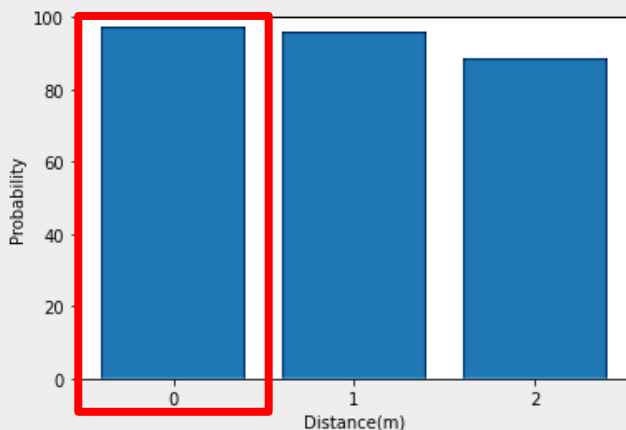
### 03 Performance Evaluation - SADS



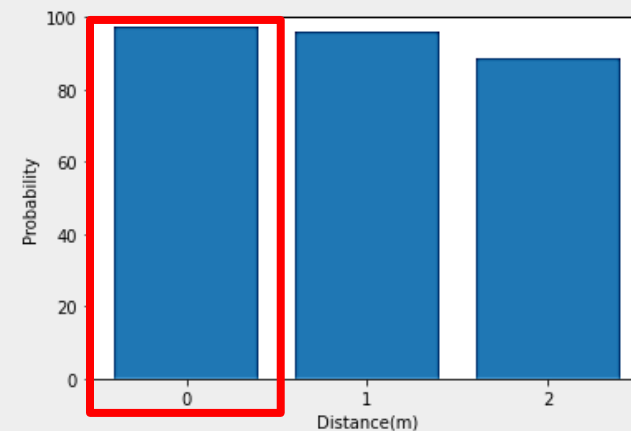
### 03 Performance Evaluation - SADS



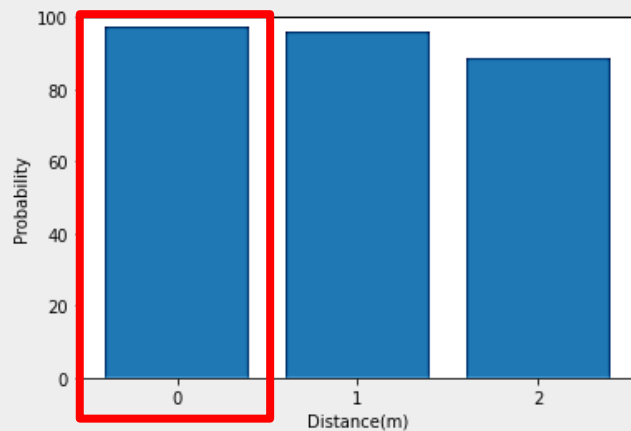
공격 데이터 1초 수신



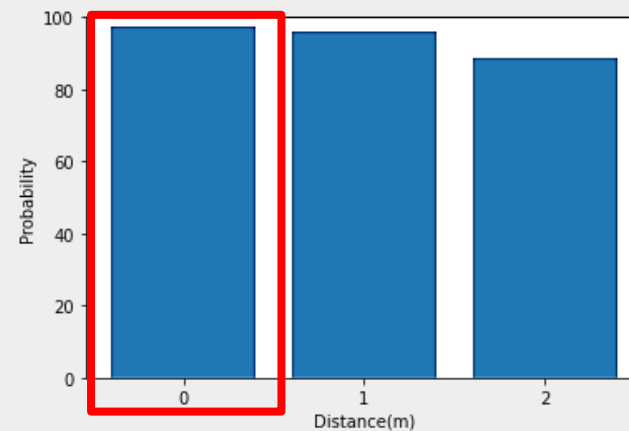
공격 데이터 2초 수신



공격 데이터 3초 수신



공격 데이터 4초 수신



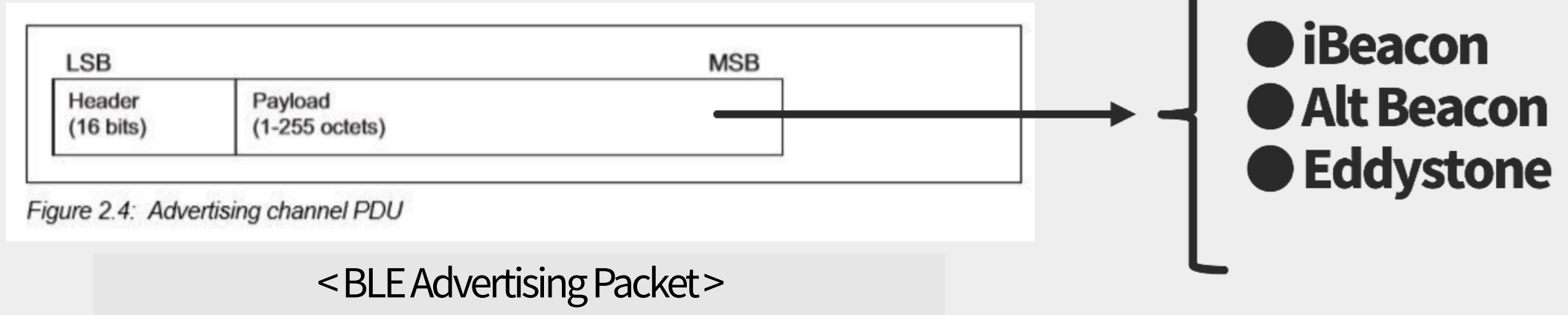
공격 데이터 5초 수신

## 04 Result – Compare to other system



	BlueShield	SADS
Tag	Stationary	Stationary + Moveable
Detection Range	Attacker is far from Tag	All ranges
Secondary damage	Unpreventable	Preventable
Number of APs required	3 or more	1 or more
Available Devices	Beacon + BLE Devices	Beacon

## 04 Result – Project Extensions



**SADS: Spoofing Attack Detection System At Indoor Positioning using BLE**



**SADS: Spoofing Attack Detection System using BLE Beacon**

## 04 Result –SADS Use Case

### 박성호 "안전한 골목, 등교 위한 '비콘프로젝트' 추진"

범취약지역 중심 셉테드(CPTED)사업 확대, 골목길?통학로 전면 정비

### 손흥민 홈구장 '토틸럼 핫스퍼 스타디움'에 숨은 최신 기술들

구장 내 와이파이기는 6만명 이상의 관람객 수요를 수용한다. 블루투스 비콘은 관람객들이 스타디움 공식 앱을 통해 다양한 편의시설을 찾기 쉽도록 도와준다. 핫스퍼 스타디움 내부에 자체 소형 양조장과 미술랭 스타를 받은 식당을 포함한 65개의 식당, 스낵코너 등 다양한 상점이 있다.

### 스마트한 서비스 신설...교통약자 대중교통 편의성 ↑

지하철 역사에 설치된 9000여개의 블루투스 기기 '비콘(Beacon)'을 활용해 정보를 제공한다.

도착역 알림 서비스는 지하철 탑승 후 내릴 역을 앱에 등록하면 '비콘'이 열차위치를 실시간으로 자동 파악해 해당 역에 도착 시 휴대폰 문자·음성을 통해 알려준다.

서울교통공사가 운영하는 1~8호선 구간 뿐 아니라 코레일 구간도 이용할 수 있다.

아이비콘은 미국 프로야구 메이저리그(MLB) 구장에도 구축됐다. 지난 2013년 뉴욕 메츠의 '시티 필즈' 구장은 미국 야구장 최초로 서비스를 도입했다. MLB의 '볼파크' 앱과 연동돼 구장 내 판매상품 등 다양한 정보를 제공한다. 이어 LA 다저스와 샌디에고 파드리스의 구장에도 65개의 아이비콘이 설치됐다. MLB는 향후 미국 내 모든 구장에 서비스를 구축할 계획이다.

미국 백화점 체인 메이시스사는 벤처기업 샵키의 '샵비콘(Shopbeacon)'을 도입했다. 2013년 뉴욕과 샌프란시스코 지점에 시범 서비스를 시작한 이후 적용 매장을 확대 중이다. 회사는 고객이 매장에 들어서는 순간 비콘으로 소비자를 인식한다. 과거 구매이력을 분석해 이에 맞는 할인 쿠폰 등을 발행하는 맞춤형 정보를 제공한다.

### 국민건강보험 일산병원, 미래 의료를 디자인하다

의료진을 포함한 일산병원 직원들의 목걸이형 사원증에는 본인 동의하에 비콘(Beacon)이 달려있다. 비콘은 위치 정보를 전달하기 위해 신호를 주기적으로 전송하는 기기를 말한다. 의료진뿐만 아니라 환자와 보호자에도 붙어있다. 이 비콘은 병원 전체(지하2층~지상13층)에 설치된 900여개 감지기에 동선과 위치를 알려준다. 이로 인해 감염병 환자가 발생할 경우 병원 내 동선과 밀접접촉자, 격리대상자를 짧은 시간에 정확히 찾아낼 수 있다.

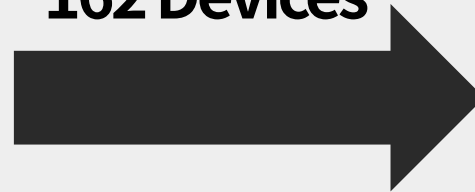


## 04 Result –SADS Use Case



**An hour**

**162 Devices**



**40%**  
Uniquely identifier



**10 hour**

**647 Devices**



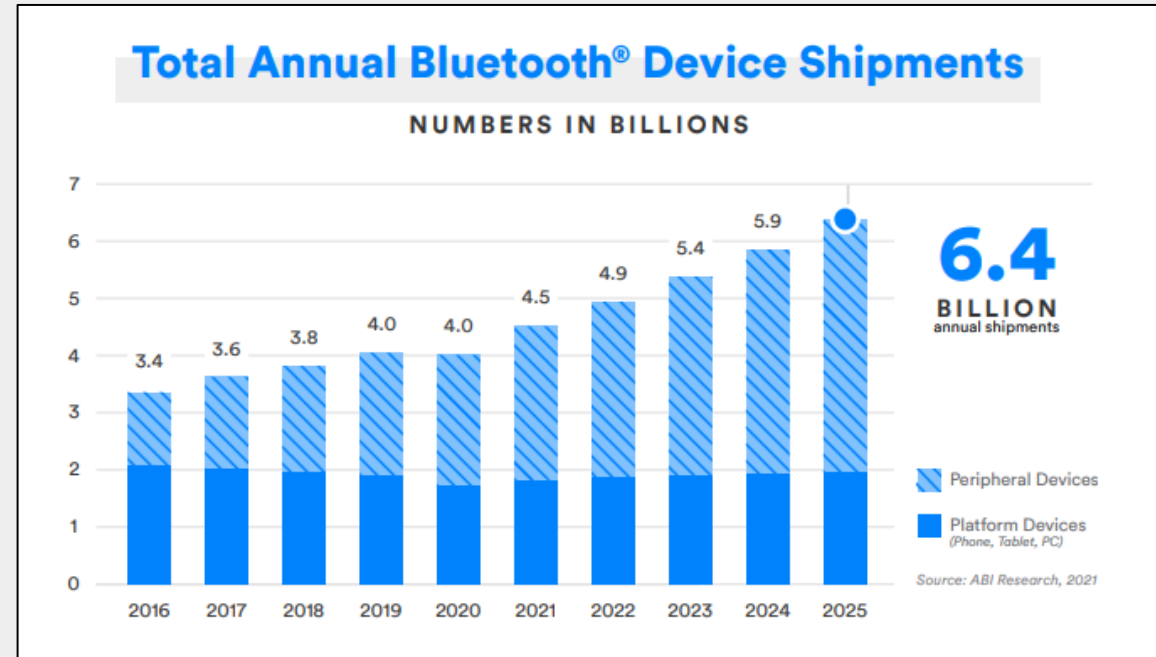
**47.1%**  
Uniquely identifier

## 04 Result –SADS Use Case

# Only Use Plaintext



80%+



**Q&A**

