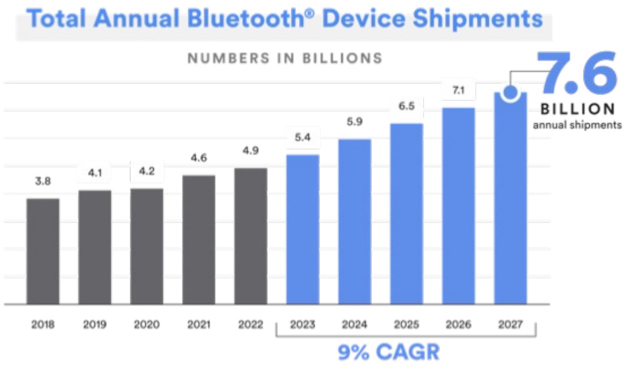
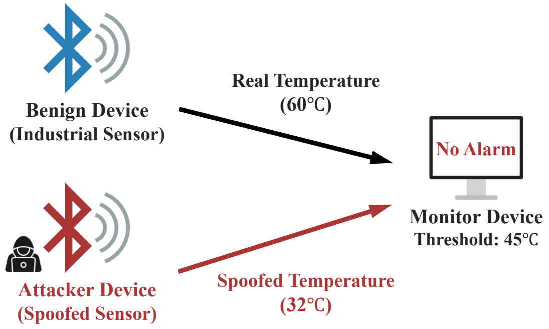
# Securing Billion Bluetooth Devices Leveraging Learning-Based Techniques

**Hanlin Cai**, Yuchen Fang, Meng Yuan, Tozammel Hossain, Zhezhuang Xu*

## What is Bluetooth Low Energy? Why Important?

Bluetooth Low Energy (BLE) is one of the most widely used wireless protocols. It is expected that the number of BLE devices will reach **7.6 billion** by 2027.

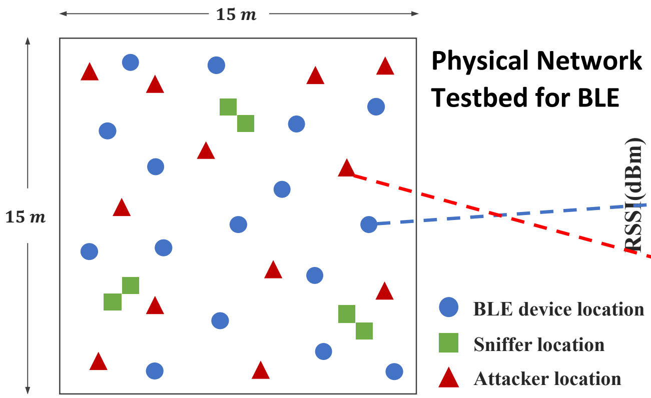


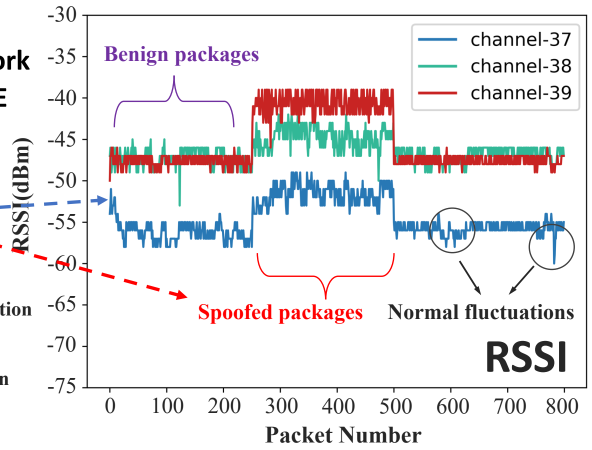


Benign Device (Industrial Sensor)
Real Temperature (60℃)
No Alarm
Monitor Device Threshold: 45℃
Attacker Device (Spoofed Sensor)
Spoofed Temperature (32℃)

Due to BLE's inherent security limitations & firmware vulnerabilities, **spoofing attacks** can easily compromise BLE networks and tamper with privacy data.

## What happened in the Bluetooth Low Energy networks?



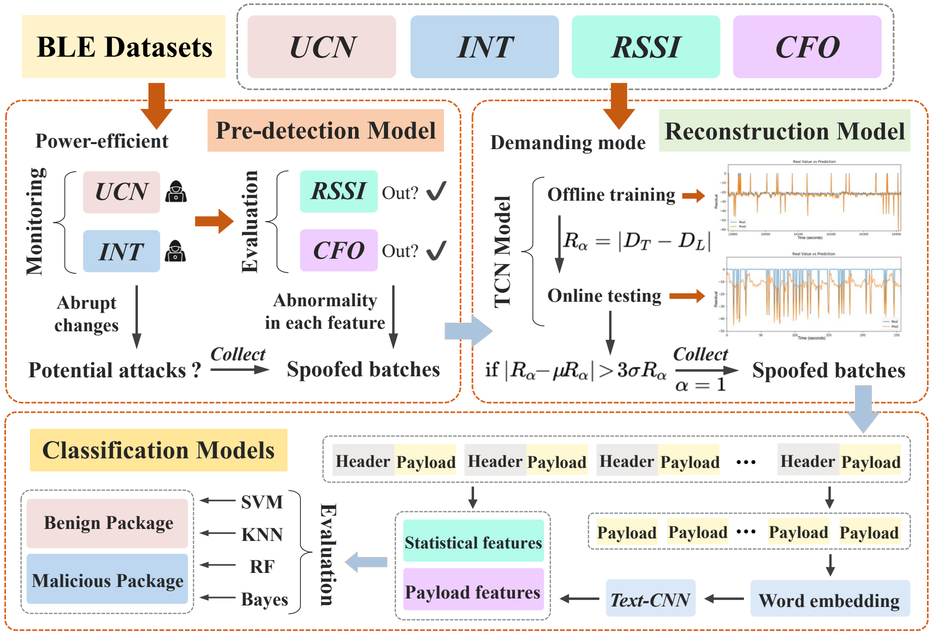


## Cyber-Physical Feature is What We Need!

- **Used Channel Numbers (UCN):** data channels number used during communication.
- **Advertising Interval (INT):** the time gap between two continuous BLE packets.
- **Received Signal Strength Indicator (RSSI):** the signal-to-noise ratio value in exchange.
- **Carrier Frequency Offset (CFO):** offset between designated & actual carrier frequencies.

## Hybrid Detection Mechanism (BLEGuard)

**We combined cyber-physical analysis with learning techniques.**



**Anomaly Score** $R(D_T, D_L) = |D_T - D_L|$

$$\alpha = \begin{cases} 0,\ when\ |R_\alpha - \mu R_\alpha| \le 3 * \sigma R_\alpha \longrightarrow Normal\ Batch \\ 1,\ when\ |R_\alpha - \mu R_\alpha| > 3 * \sigma R_\alpha \longrightarrow Suspicious\ Batch \end{cases}$$

Classify

$$\begin{cases} Benign\ Packet \\ Malicious\ Packet \end{cases}$$

## Preliminary Experiment Results

| Method | Accuracy | FAR | UND |
|---|---|---|---|
| BLEGuard (us) | 99.20 | 0.04 | **0.58** |
| BlueShield [1] | **99.54** | 2.37 | 0.72 |
| Lahmadi [2] | 99.00 | **0.03** | - |

### Our main contributions:

- Large-scale dataset
- Low online consumption
- Reliable offline analysis
- Fine-tune feedback design

**Dataset and code are publicly available:**

https://github.com/BLEGuard/supplement

**Seeking PhD Position!**

[1] Wu, et al, BlueShield, RAID'20 [2] Lahmadi, et al, PKDD'20