AAAI 2024: 利用基于学习的技术保护十亿蓝牙设备

—— 如何把本科毕设发表到权威会议？

蔡汉霖 832002117

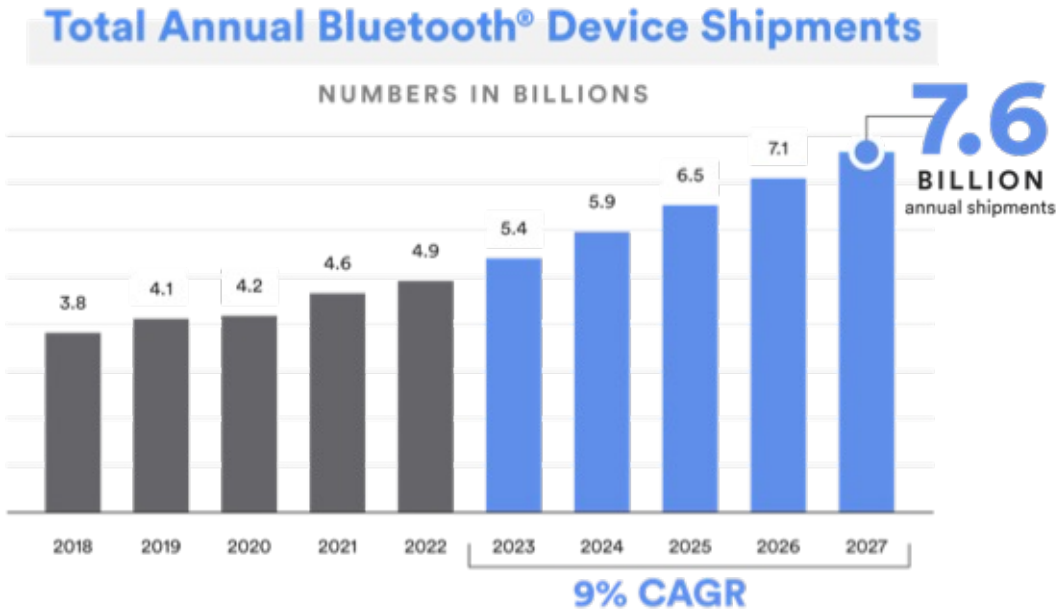
汇报目的

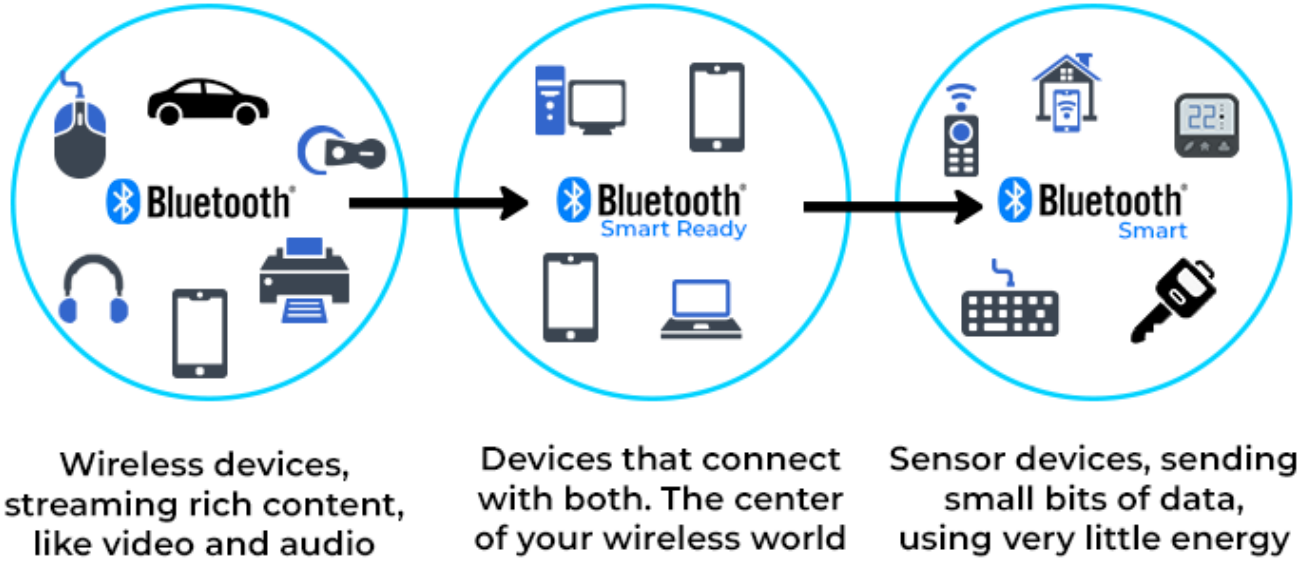
① 工作介绍：Securing Billion Bluetooth Devices Leveraging Learning-Based Techniques (AAAI 2024, review in KDD 2024)

② 知识点讲解：蓝牙网络，时间序列分析，时序卷积网络 TCN

③ 经验分享：如何把本科毕设发表到领域权威期刊 / 会议？

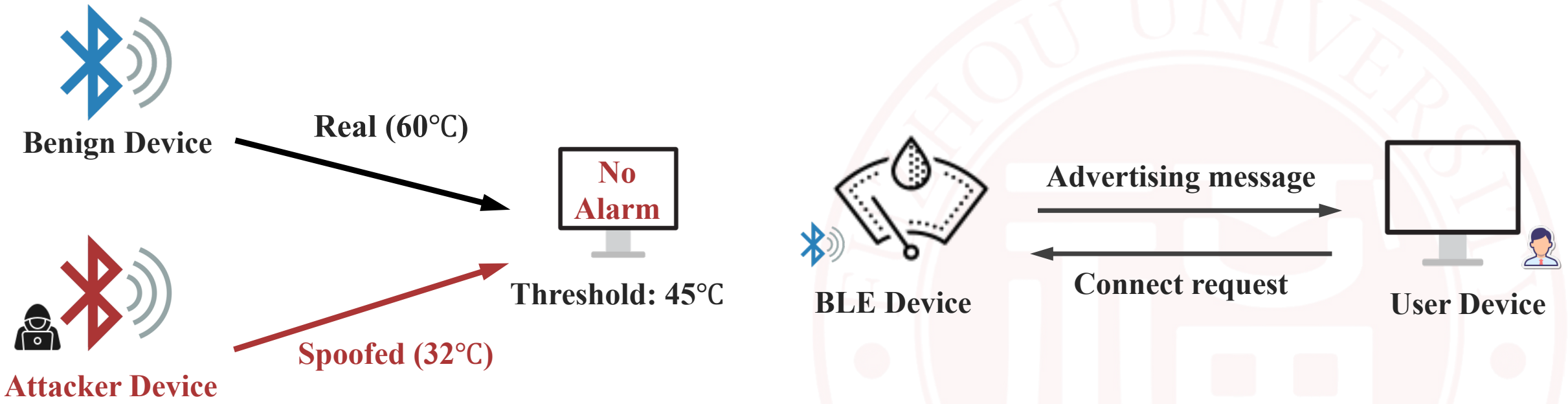
Research Background





- **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. BLE devices are ubiquitous!
- 低功耗蓝牙设备几乎无处不在：教育、医疗、工业、生活中的诸多场景

Research Background



- **BLE Spoofing attack:** Feed malicious data to the user devices (manager) 欺骗攻击频发
- Due to BLE‘s inherent security limitations and firmware vulnerabilities, spoofing attacks can easily compromise BLE networks and tamper with privacy data[1]. 蓝牙设备普遍缺乏验证机制
- 并且，超过60%的蓝牙设备不支持固件升级，无法防御新型攻击。亟需开箱即用的防御模式

Research Objective

➢ Our Goals

① A physical Bluetooth Low Energy network testbed will be built for attack simulations.

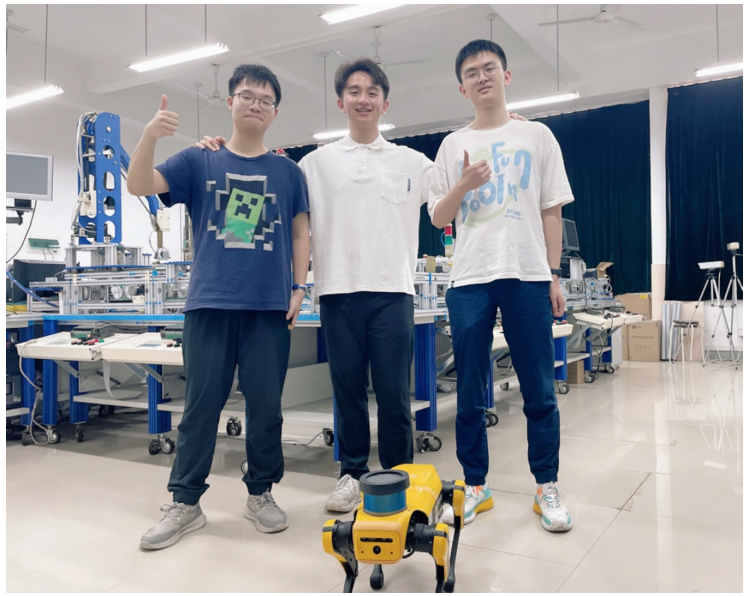
② Detection algorithm will be designed to recognize spoofing attacks.

③ Experiments will be conducted based on real-world advertising datasets.

④ Overall, this FYP aims to address a crucial challenge in Bluetooth security and provides a substantial dataset for wireless security research.

环境搭建—— 算法研究 —— 实验测试 —— 性能验证 —— 实际应用

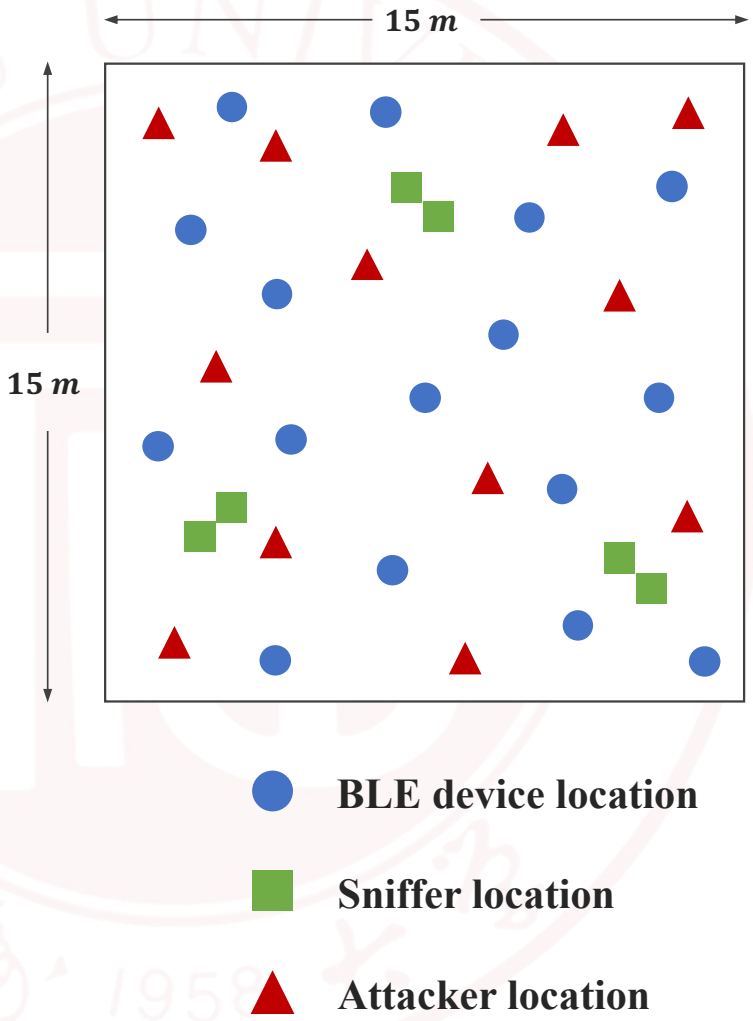
Testbed Implementation



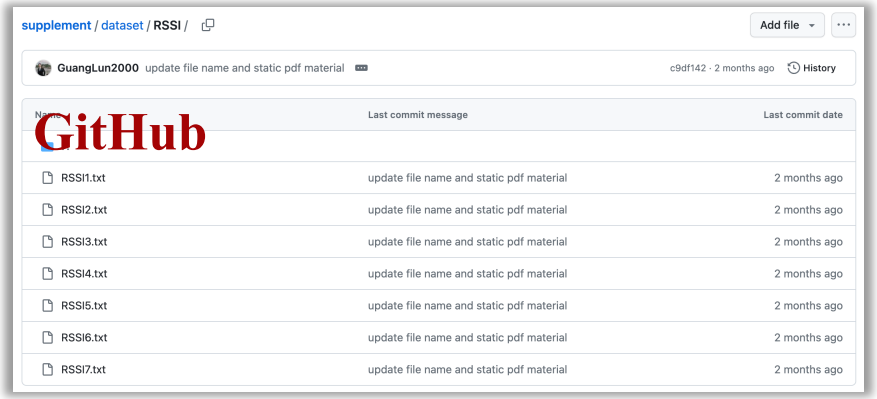
Experimental Lab

Selected BLE Devices

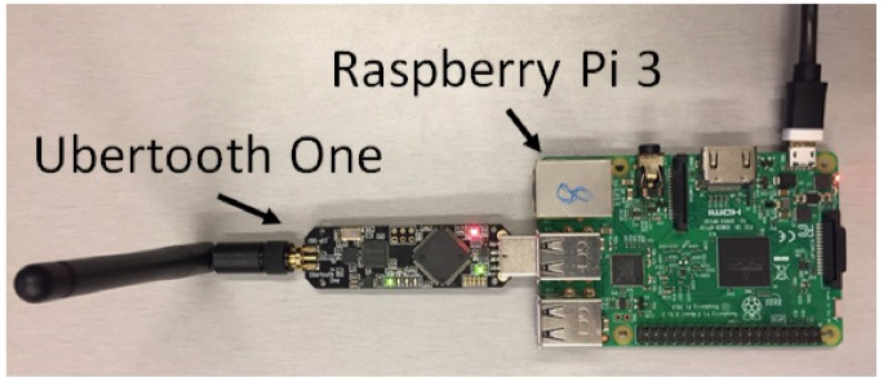
16 Types



Data Collections



BLE Datasets Collecting



Network Sniffers (3×2 copies)

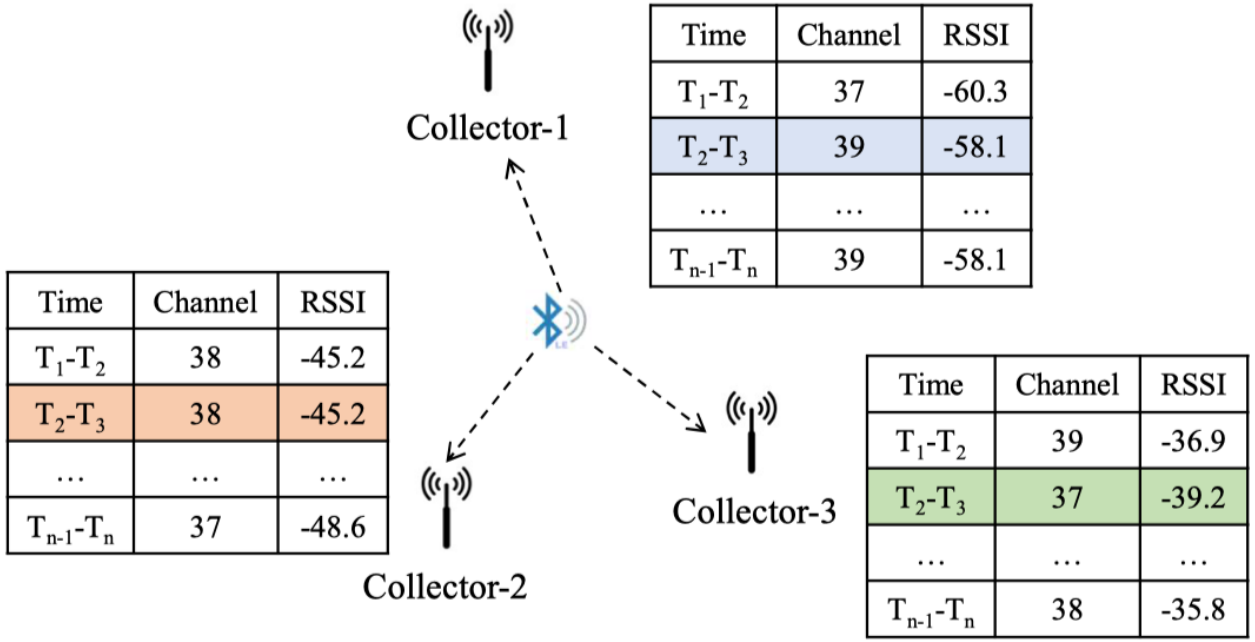
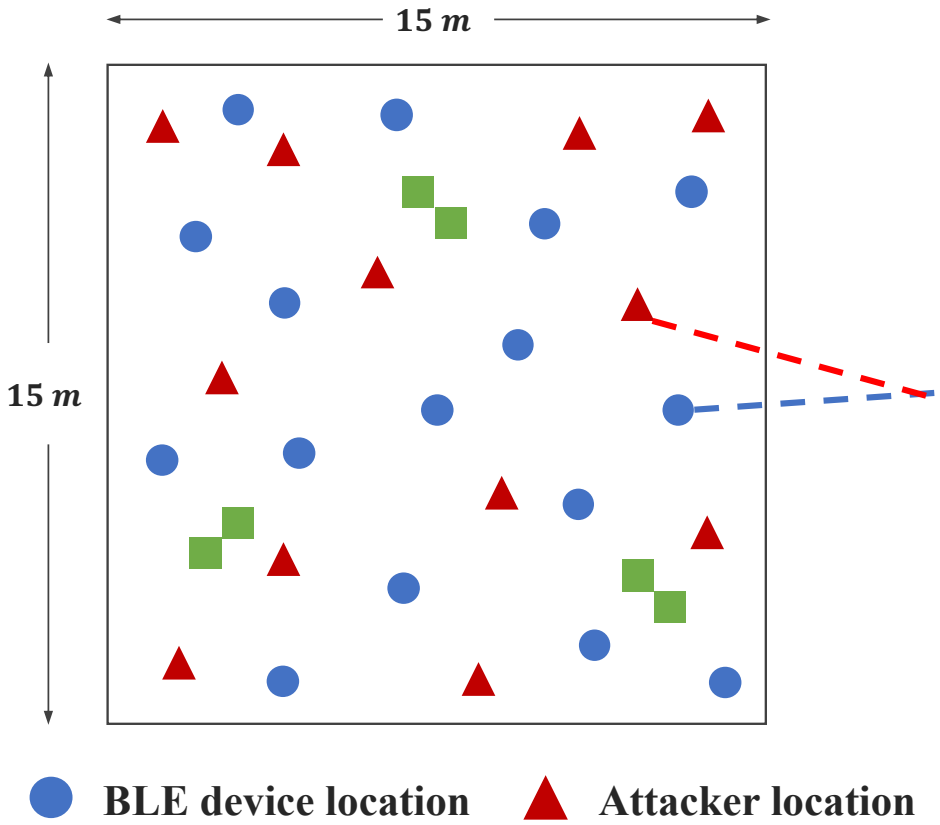
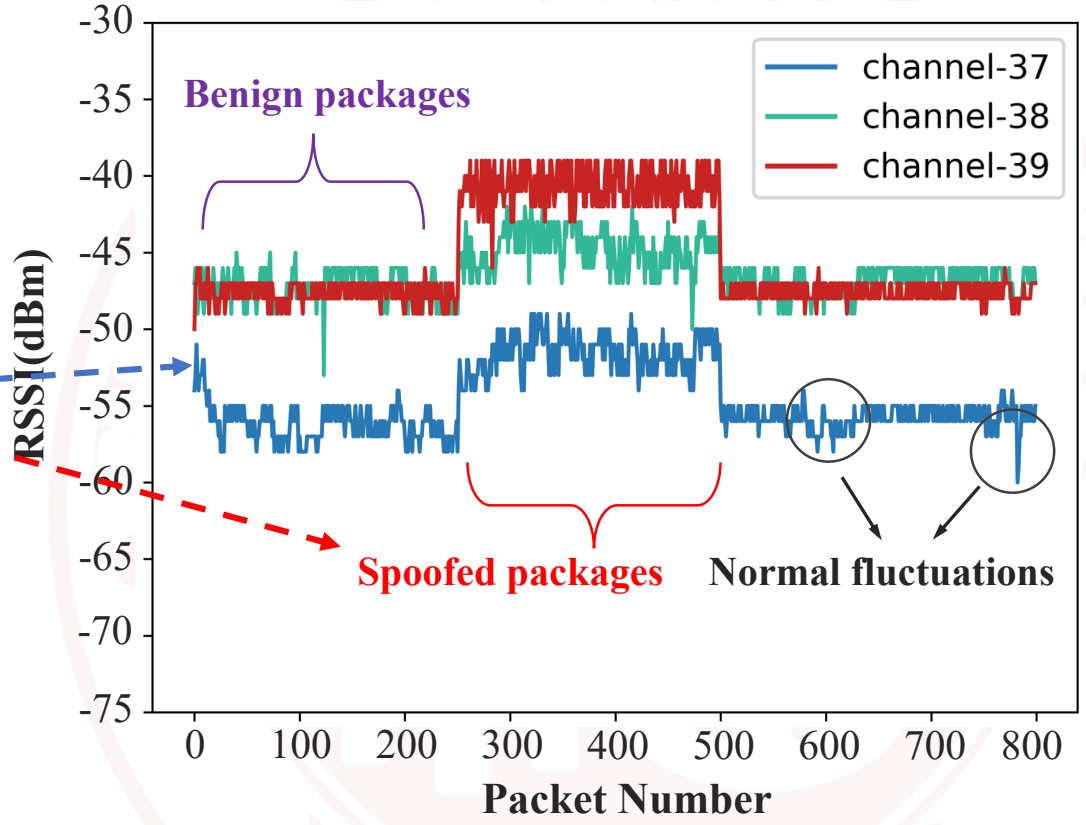


Figure 5: An illustration of the randomized channel switching.

Three Sniffer for each group

Cyber-physical Analysis





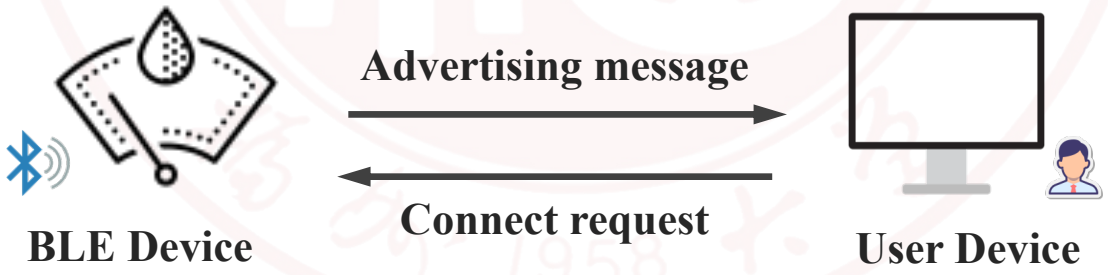
- In the spoofing attack scenario, the **cyber-physical features** of BLE network will undergo noticeable affected, resulting in significant deviations from the benign scenario. 可以采用信息物理特征分析

BLE Communication

BLE网络通信过程示例

```
[Advertising] Device A: "Advertising on Channel 37, Advertising Interval: 1024 ms, Payload Data: 'Hello Device B!'"
[Scanning] Device B: "Scans on Channel 37, Detects Device A, RSSI: -60 dBm"
[Connecting] Device B -> Device A: "Connection Request to Device A on Channel 37"
[Connection Established] Device A -> Device B: "Connection Acknowledged on Channel 38, Carrier Frequency Offset: +250 Hz"
[Data Exchange] Device A -> Device B: "Sending Payload Data: 'Sensor Data: 58°C', Channel: 38, RSSI: -55 dBm"
[Disconnecting] Device B -> Device A: "Disconnect Request, Channel: 38"
[Disconnected] Device A -> Device B: "Disconnection Acknowledged, Channel 39"
```

- BLE通信普遍缺乏Pairing验证环节
- 通过网络嗅探器(Sniffer)采集通信过程
- 相关文本用于深度学习的时序特征分析



Cyber-physical Features

➢ **How to distinguish malicious data from the benign data?**

BLE网络数据包示例

```
Packet No.: 3254
Timestamp: 2022-10-01 12:45:30.123456
Channel: 38 (Used Channel Number)
Source MAC: d4:36:39:ff:e5:12 (Device MAC Address)
Destination MAC: f4:4e:fd:2c:a9:3e (Central Device MAC Address)
Advertising Interval: 700ms (Time between consecutive advertising packets)
RSSI: -55 dBm (Signal strength indicator)
Carrier Frequency Offset: +2 kHz (Difference from the expected carrier frequency)
PDU Length: 27 bytes (Length of the protocol data unit)
Data:
  Opcode: 0x1b (ATT Handle Value Notification)
  Handle: 0x001C (Characteristic handle for Heart Rate Measurement)
  Value: 60 bpm (Heart rate measurement value)
CRC: 0x1234AB (Cyclic Redundancy Check for error-checking)
```

➢ 时间序列数据分析

- Packet Number
- **Timestamp 时间戳**
- Used Channel
- Source MAC
- Advertising Interval
- **RSSI data 信号强度**
- CFO data 频率偏差
- Payload Data 负载数据

Temporal Convolutional Network (TCN)

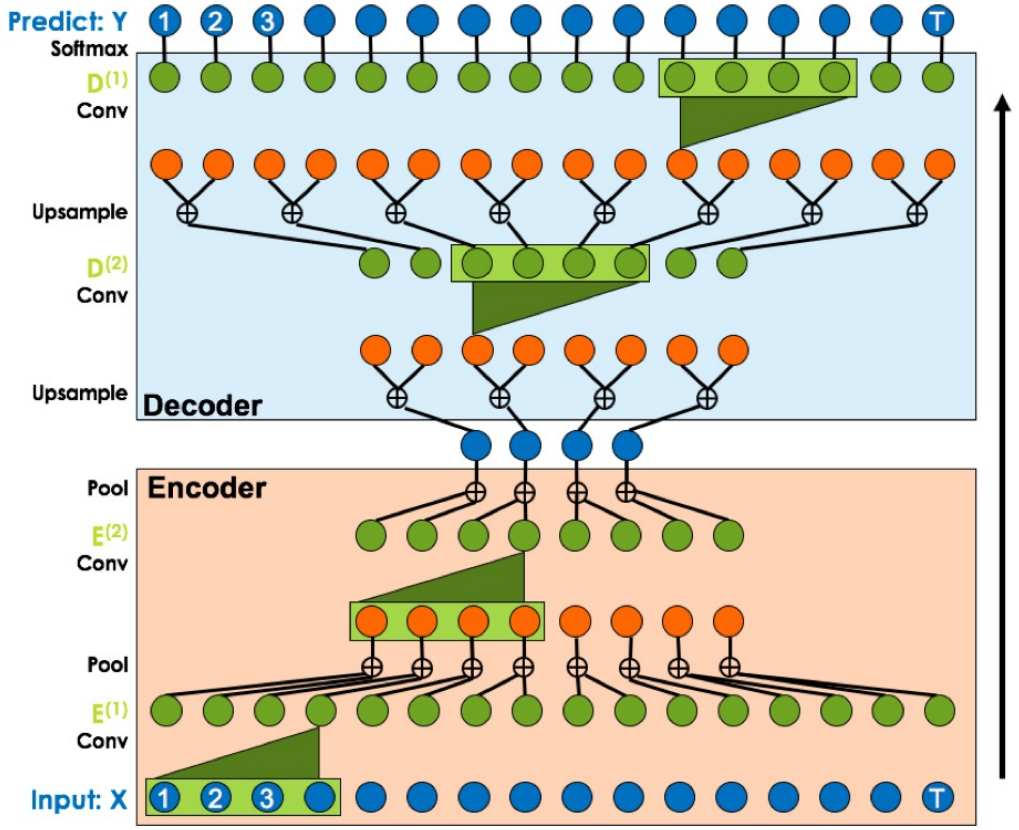


Figure 1. Our Encoder-Decoder Temporal Convolutional Network (ED-TCN) hierarchically models actions using temporal convolutions, pooling, and upsampling.

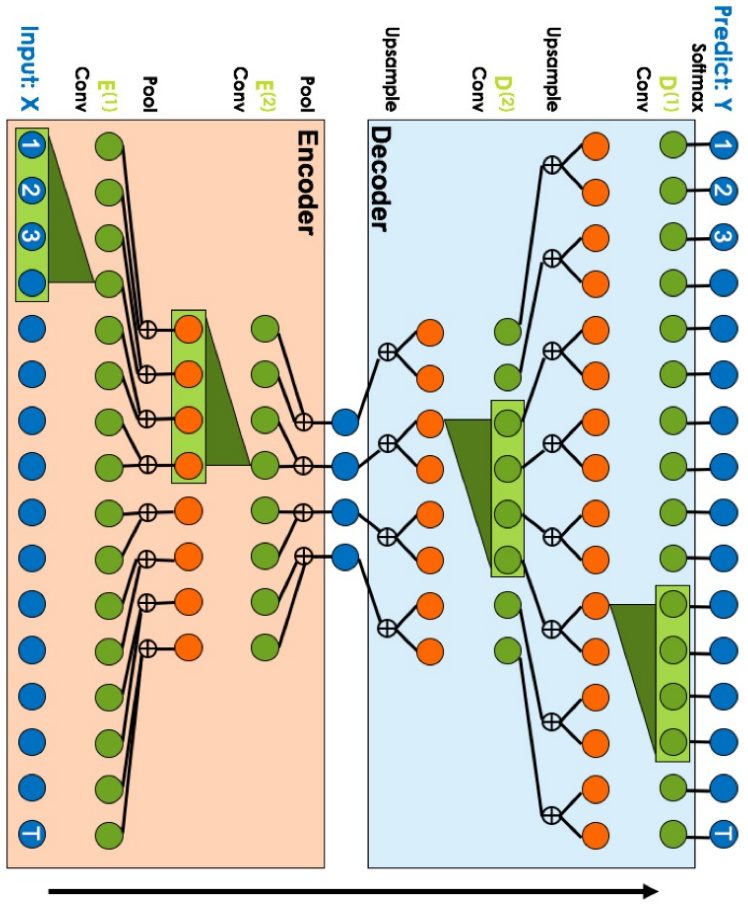
➢ 时序卷积网络（编码器+解码器结构）

- **输入（Input）：** 序列数据的输入，图中用蓝色圆圈表示。每个圆圈代表序列中的一个时间点上的数据。
- **编码器（Encoder）：** 分负责提取输入数据的特征。通过一系列的卷积层（Conv）和池化层（Pool），编码器抓取并压缩了时间序列的信息，每经过一层，时间序列就被进一步抽象。
- **解码器（Decoder）：** 解码器的工作是将编码器的输出重新构建为具有更详细信息的输出序列。它通常包含上采样（Upsample）层和卷积层，上采样层将数据扩展到更高的维度，卷积层则进一步精细化这些数据。
- **预测（Predict）：** 最顶部是输出层。它通常包含一个Softmax层，用于将解码器的输出转换成最终的预测结果，如分类或者下一个时间点的数据。

TCN model for BLE networks

Benign activities

Input



TCN Model

端到端模型

Output

Benign predictions

输入：来自BLE设备的一系列时间序列数据。一个特定时间点上的多维特征向量（序列）

可以包括RSSI值、所用的频道、当前时间步的数据包类型。这些数据是按照时间顺序收集的

输出：对应输入时间序列的每个时间步的预测结果

模型可能在每个时间步输出一个关于通信状态的分类（正常、可疑、异常），或者某个时间段内的信号强度

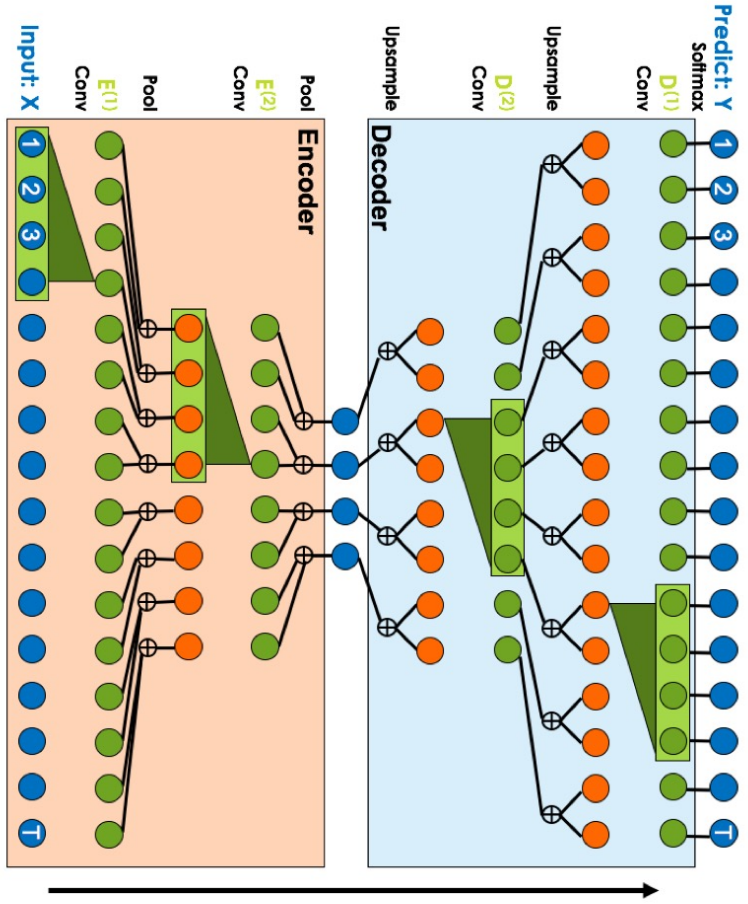
TCN Learning: Input to Output

Benign activities

Input

Malicious activities

Input



TCN Model

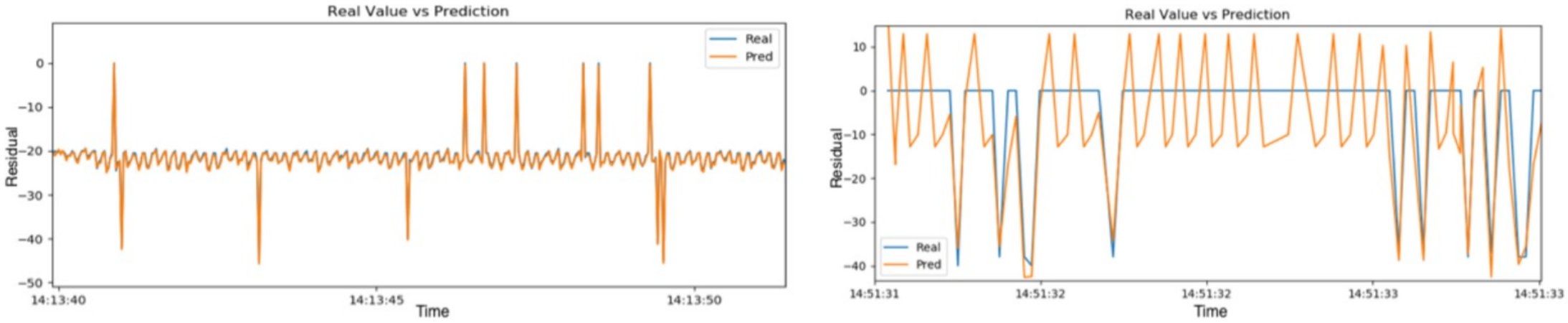
Output

Benign predictions

Output

Malicious predictions

Training and Testing of TCN model



(a) Training of the normal model

(b) Testing of the MitM attack model

Fig. 8. Training and testing of models reconstruction using TCN.

$$\alpha = \begin{cases} 0 & \text{if } |R(X_{test}, \widehat{X_{test}}) - \mu(R(X_{train}, \widehat{X_{train}}))| \leq 3 * \sigma(R(X_{train}, \widehat{X_{train}})) \\ 1 & \text{otherwise.} \end{cases}$$

Anomaly Detection (TCN)

➢ Key formula for anomaly detection (Anomaly Score: α)

$$\alpha = \begin{cases} 0 & \text{if } |R(X_{test}, \widehat{X_{test}}) - \mu(R(X_{train}, \widehat{X_{train}}))| \leq 3 * \sigma(R(X_{train}, \widehat{X_{train}})) \\ 1 & \text{otherwise.} \end{cases}$$

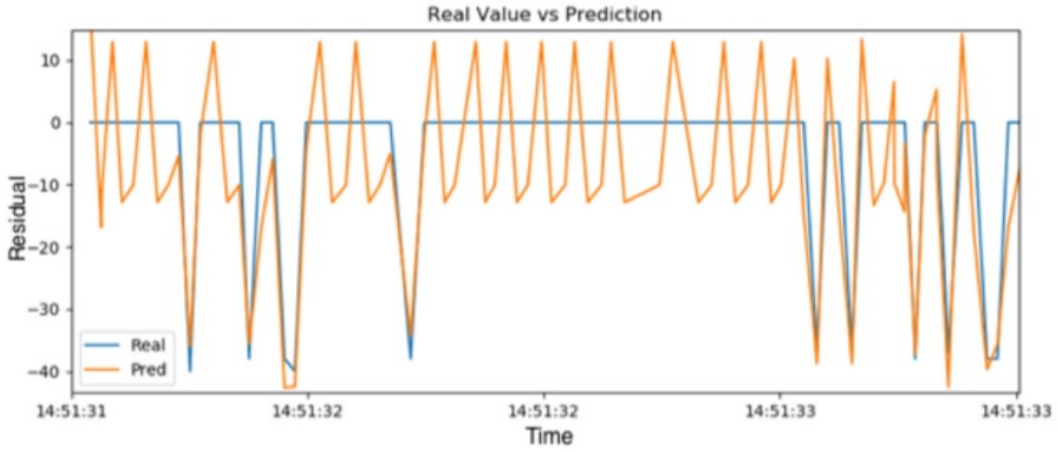
$R\left(X_{\text{train}}, \hat{X}_{train}\right)$：表示计算训练集的实际值 X_{train} 与模型预测值 $\hat{X}_{train}$ 之间的残差。

$\mu\left(R\left(X_{\text{train}}, \hat{X}_{\text{train}}\right)\right)$： 计算训练阶段残差的均值。

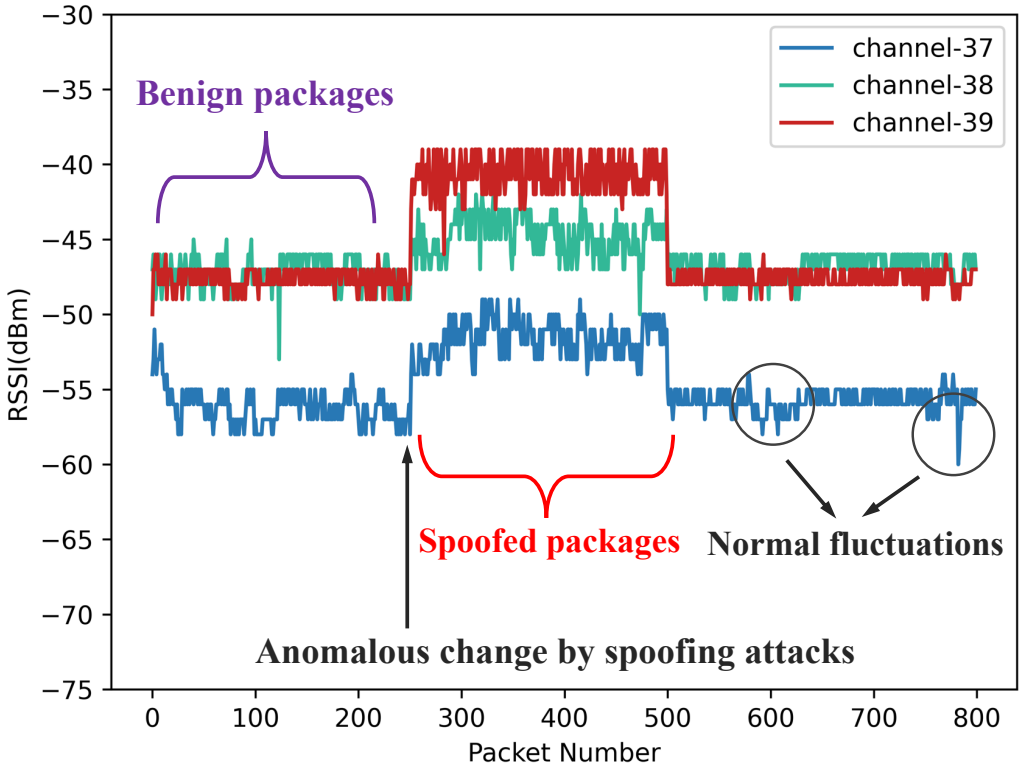
$\sigma\left(R\left(X_{\text{train}}, \hat{X}_{\text{train}}\right)\right)$：计算训练阶段残差的标准差。

- $\alpha = 0$ 表示测试集的残差在正常范围内，即 $|R(X_{test}, \hat{X}_{test}) - \mu(R(X_{train}, \hat{X}_{train}))| \leq 3 \cdot \sigma(R(X_{train}, \hat{X}_{train}))$。
- $\alpha = 1$ 表示测试集的残差异常，即 $|R(X_{test}, \hat{X}_{test}) - \mu(R(X_{train}, \hat{X}_{train}))| > 3 \cdot \sigma(R(X_{train}, \hat{X}_{train}))$。

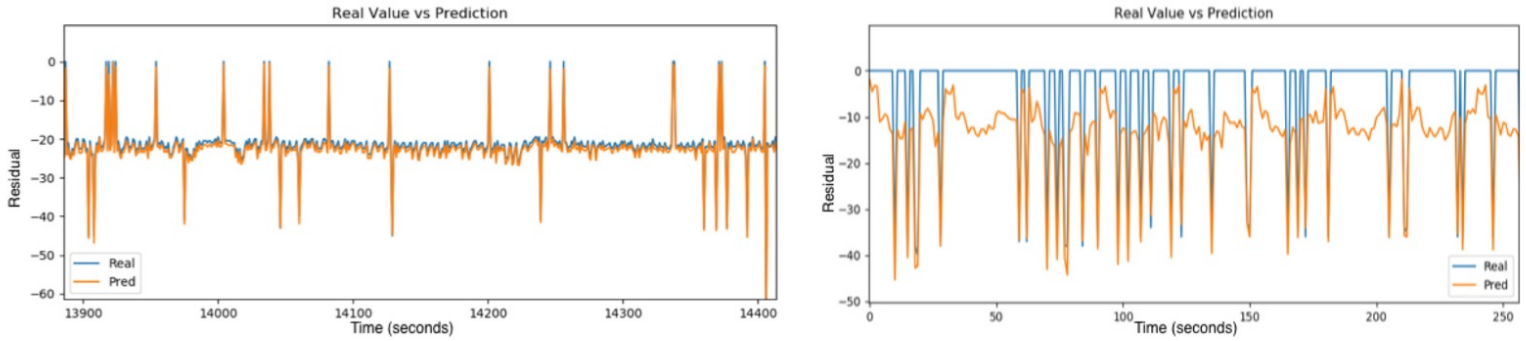
Testing Simulation & Real Attack Scenario



(b) Testing of the MitM attack model

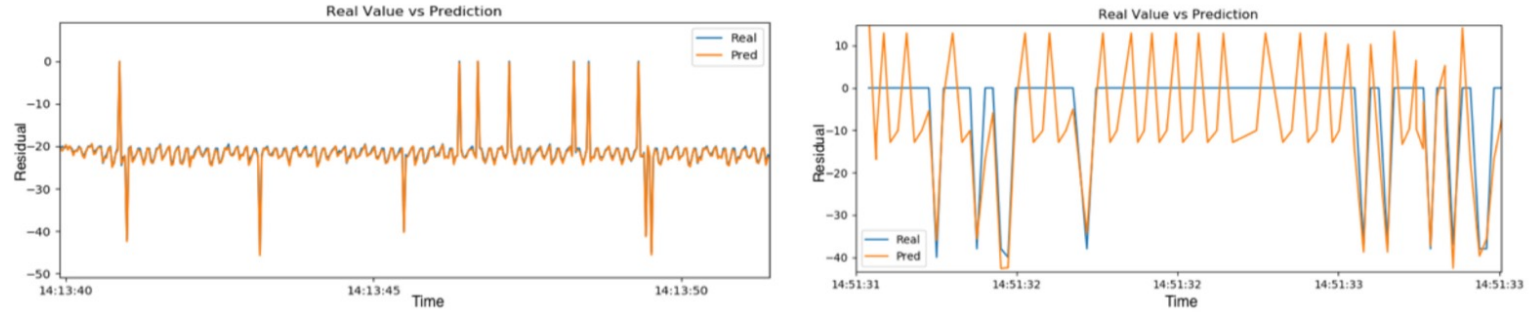


TCN model & LSTM model



(a) Training of the normal model (b) Testing of the MitM attack model

Fig. 6. Training and testing of models reconstruction using LSTM.



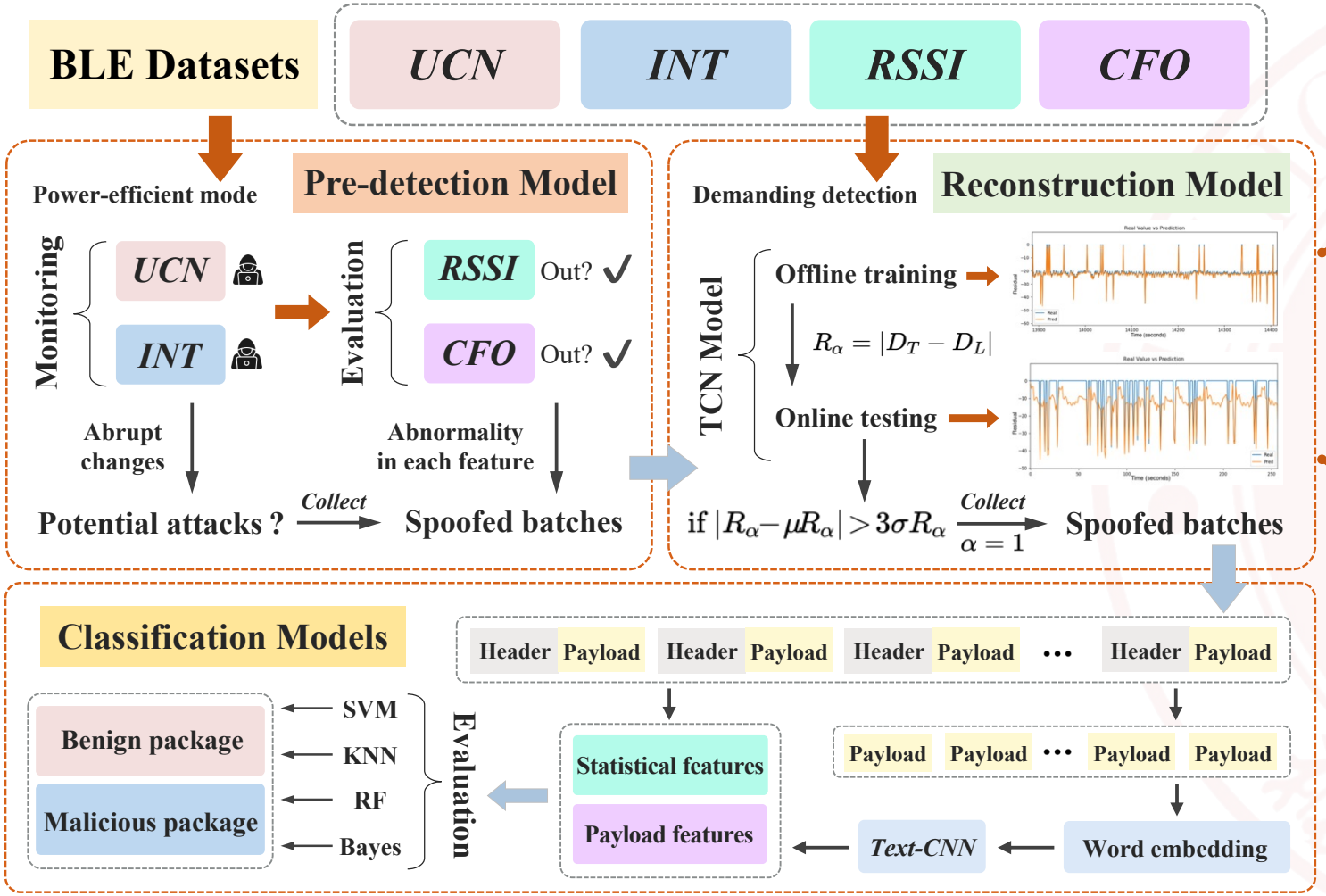
(a) Training of the normal model (b) Testing of the MitM attack model

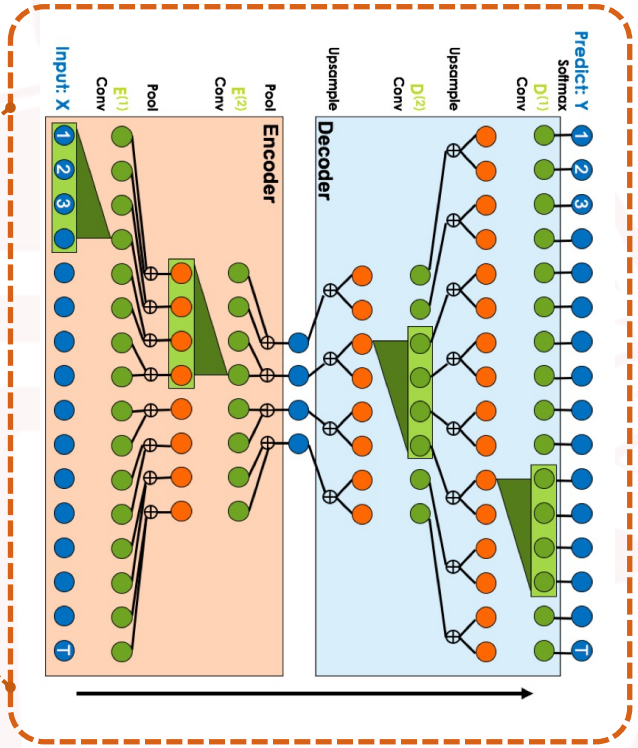
Fig. 8. Training and testing of models reconstruction using TCN.

➢ TCN模型的优势

- 可以有效捕捉长期的时间依赖性
- 在较少的样本情况下获得更好的结果
- 在预测攻击流量行为时更为准
- 重构误差更低，并且具有更强的记忆效果
- 易于并行处理，训练速度快

TCN model in the Hybrid Structure

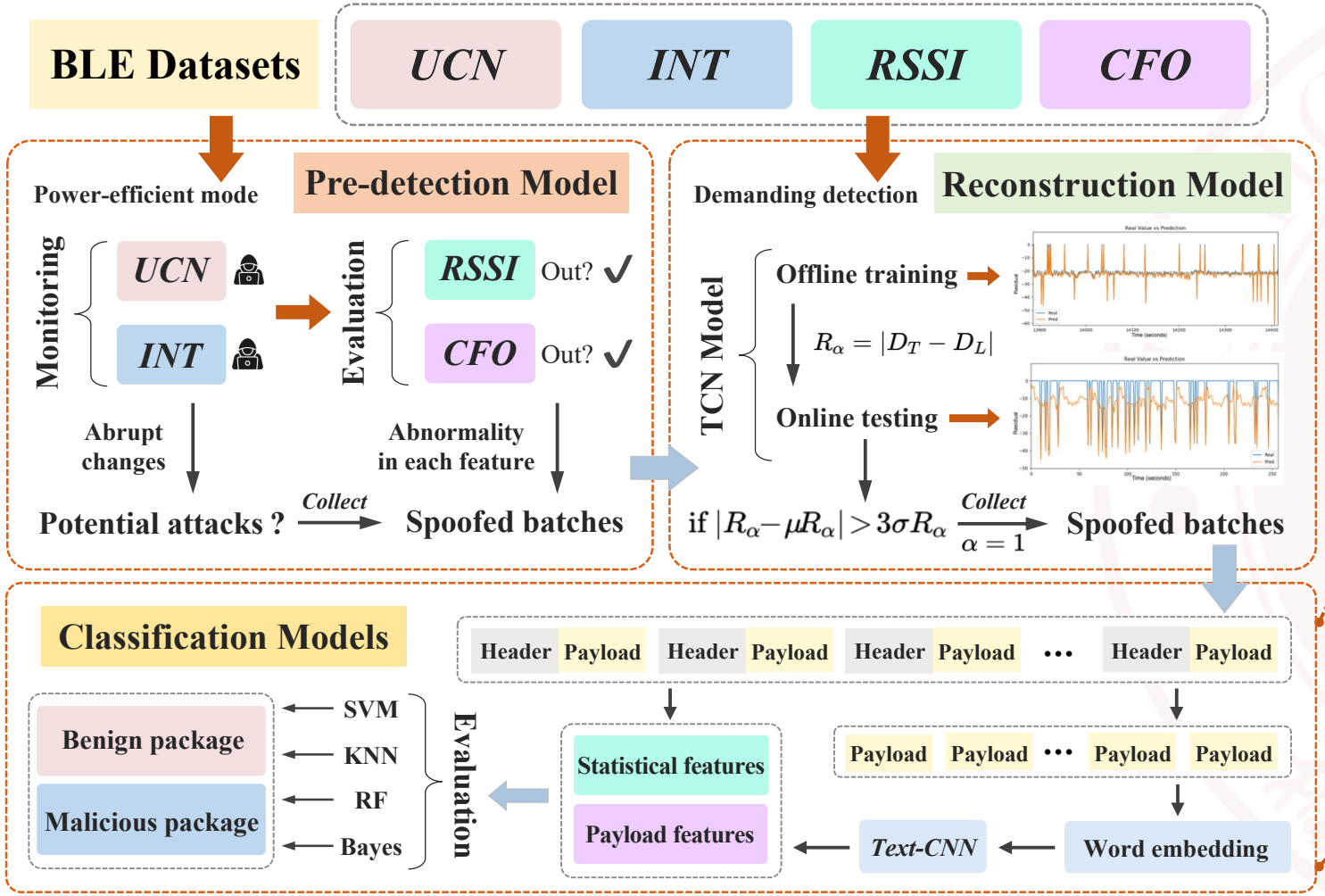




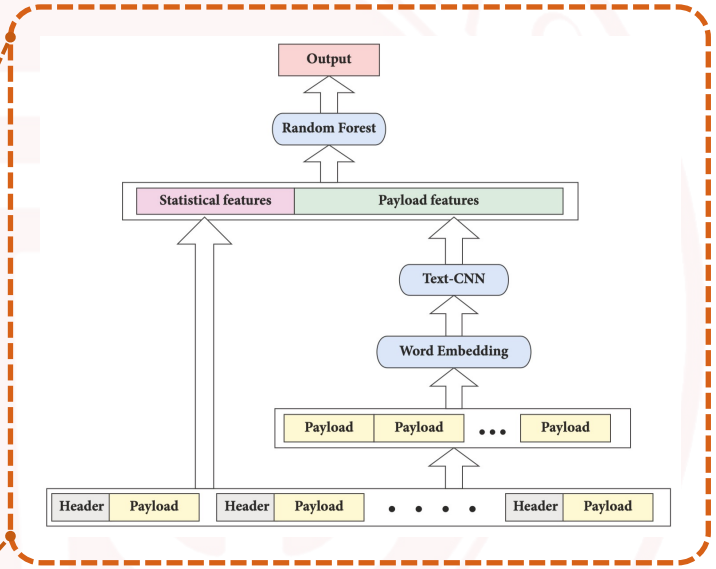
TCN Model

只能在批量级别检测异常，而不能精确到单个数据包的检测

Detection & Classification



text-CNN + Classifiers



精确到单个异常BLE数据包的检测，为系统提供动态反馈

Demo Time!

➢ 本科生，如何把毕设发表到领域权威期刊 / 会议？

① **选择大于努力：**实验 > 理论，迁移应用 > 架构更新（注意语境！）

② **故事感：**有意义的研究，佐以丰富的应用前景 + 清晰的论文写作

③ **工作量：**“三个臭皮匠，顶个诸葛亮”，用诚意打动审稿人

④ **努力，还是努力：**历经多次拒稿，终于抵达“最佳目的地”

Thank you for your Listening!

➢ Our Related Paper

[1] Hanlin Cai, Tozammel Hossain, Zhezhuang Xu*. "Securing Billion Bluetooth Devices leveraging Learning-based Technique". *The 38th Annual AAAI Conference on Artificial Intelligence. Undergraduate Consortium* (AAAI 24, Research Proposal)

[2] Hanlin Cai, Yuchen Fang, Meng Yuan, Tozammel Hossain, Zhezhuang Xu*. "BLEGuard: Hybrid Detection Mechanism for Spoofing Attacks in Bluetooth Low Energy Networks". Expect to submit to *the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (KDD 24, Preprint)

Our data and model can be found here: https://github.com/BLEGuard/supplement

Presenter: Hanlin Cai

April 2024

Supplements

```
.
├─dataset                          # sample set of our data
│   ├─profiles                     # sample data of BLE device.
│   └─RSSI                         # partly RSSI feature data recorded.
├─src                              # source code
│   ├─blemonitor                   # BLE device monitor code.
│   ├─machine-learning             # relative code includes: SVM, TextCNN etc.
│   │   ├─bayes
│   │   ├─cnn-svm
│   │   ├─cnn-text-classification-pytorch
│   │   ├─cnn-text-classification-tf
│   │   ├─knn
│   │   ├─logistic
│   │   ├─lstm
│   │   ├─random-forest
│   │   ├─svm
│   │   └─tcn
│   └─ubertooth                    # fixed ubertooth code for additional feature.
├─static                           # static resource.
├─README.md                        # README file for our supplements.
└─Supplement-Report.pdf            # The report you are reading now.
```

Our data and model can be found here: https://github.com/BLEGuard/supplement

Appendix 1

Table 1. The hyperparameters of the TCN neural network.

Hyperparameter	Value
Optimizer	Adam
Learning rate	0.001
Batch size	40
Epoch number	150
Loss function	MSE
Validation metric	Accuracy
Validation split	0.2
DL framework	Tensorflow 1.13.1, Keras 2.2.4, Keras-tcn 2.6.7

- 较小的卷积核：通常可以捕获短期的依赖关系。它允许模型关注输入数据中的精细模式和快速变化。对于快速变化的时间序列或在短时间尺度上需要检测异常的场景，较小的卷积核可能更合适。

- 较大的卷积核：可以捕获更长期的依赖关系。这对于包含长期趋势或模式的时间序列尤其重要，例如在异常检测中，异常行为可能在较长的时间跨度内逐渐表现出来。

Appendix 2

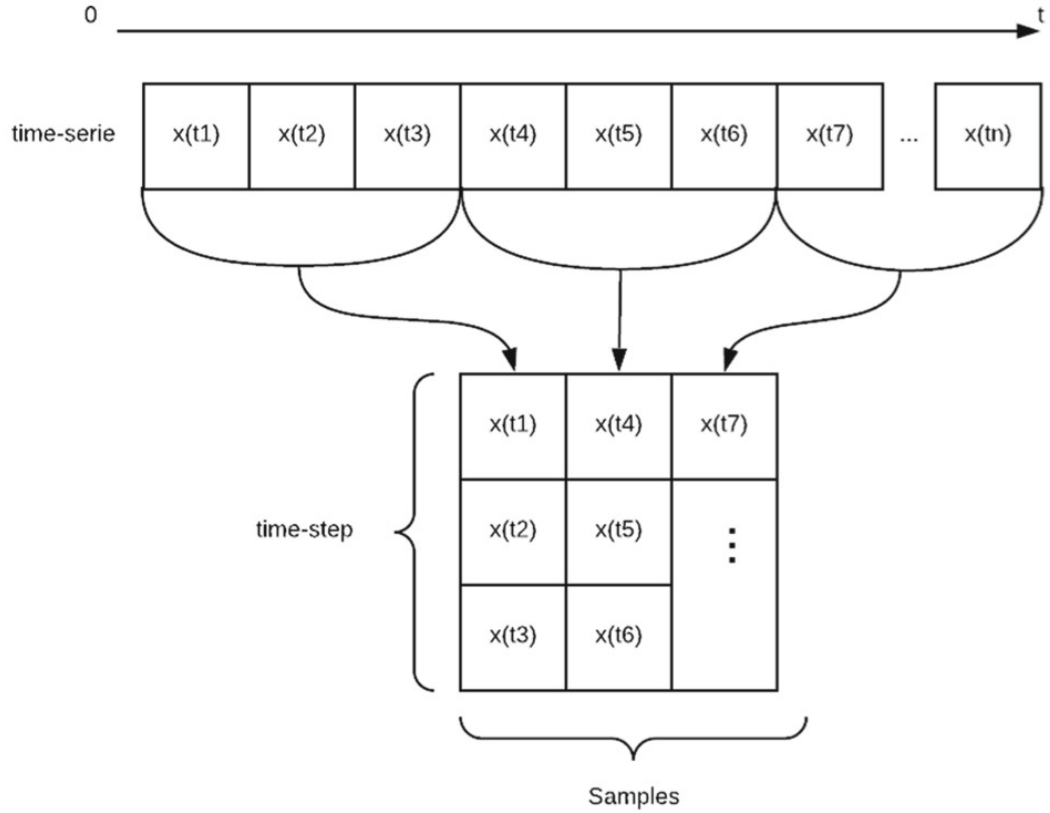


Fig. 5. Transformation of time series into training samples with a time-step = 3.

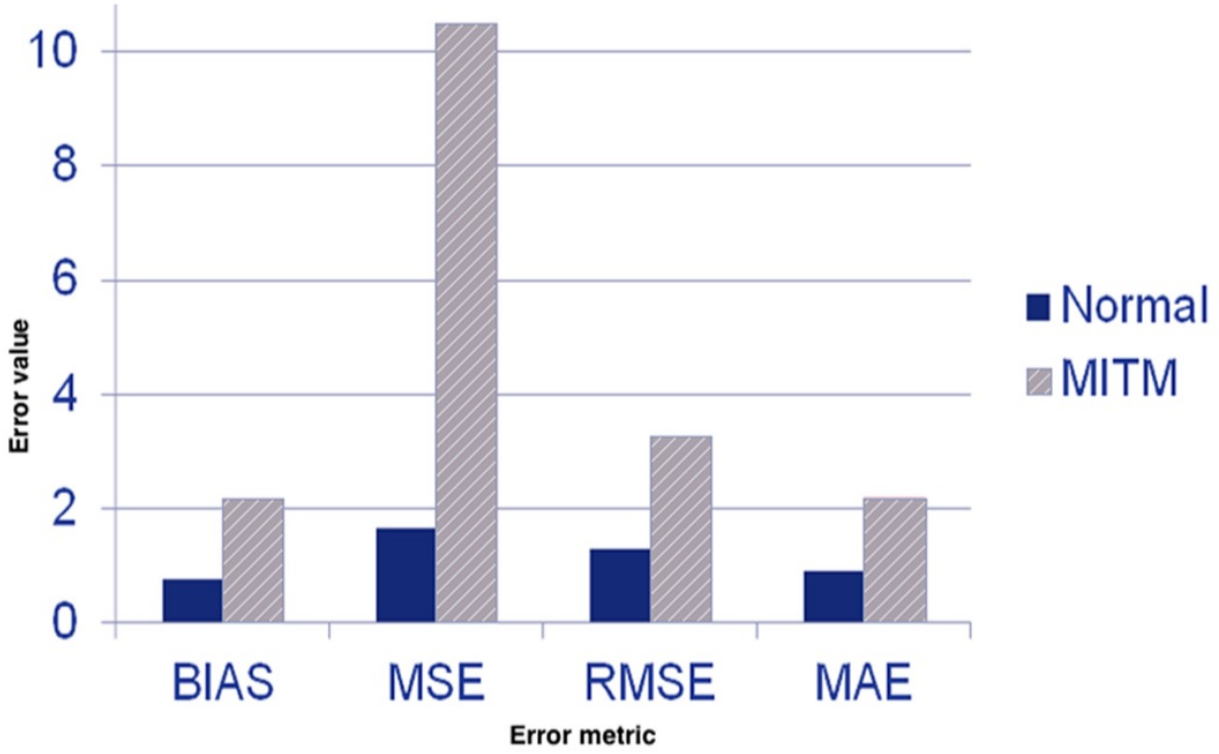


Fig. 9. Reconstruction error between normal and attack patterns using TCN.

Appendix 4

Table 1: An illustrative sample of characteristics of a BLE device recorded during the profiling phase.

Characteristic	Value
Device ID & Name	1, n097w
MAC Address	0xD1 76 A3 1A F4 7F
Advertising Data	0x06 09 4E 30 39 37 57
Advertising Pattern	Intermittent
Lower Bound of INT	1280 ms

Table 3. Statistical features of BLE traffic data.

Features
Number of packets per second
Number of bytes per second
Max, min and average packets length
Max, min and average time interval between 2 packets
Number of packets for each BLE packets type (ADV, DATA, etc.)

Table 6: Sample data of BLE devices recorded during the collecting phase.

Device ID	MAC Address	Advertising Data	Advertising Pattern	Low Bound of *INT* (ms)
1, n075w	02:4f:19:02:c8:f2	06 09 4e 30 39 37 57	Intermittent	1282
2, b3s97	08:7f:2a:1c:5e:b3	0a 18 54 28 6d 81 45	Continuous	1376
3, tfb7a	0e:2b:65:9f:3d:a7	0f 3a 73 59 21 4c 60	Continuous	923
4, r672y	0b:19:0c:7f:8e:2d	0d 0e 76 45 93 82 1a	Continuous	1149
5, o3aqe	01:98:4d:6a:f7:3c	04 13 28 6b 94 3e 77	Intermittent	1423
6, 7wzfy	0c:57:6f:8b:a2:4e	07 23 58 17 9f 02 3d	Continuous	1445
7, 3v9nl	0a:aa:32:ef:1d:80	0b 88 49 2e 76 51 3C	Intermittent	1055
8, 42xpz	03:ef:1a:58:c4:9d	05 47 9d 0a 86 2b 1e	Intermittent	1290
9, qtpv5	09:6d:84:23:5f:ca	0c 6f 3b 0c 98 74 21	Continuous	1178
10, l348y	04:31:2e:7d:0f:6a	0e 67 a1 05 9d 3f 7a	Continuous	1264

Appendix 5

Table 9: Detection results for features judgment algorithm and classification models (using SVM).

Device ID	Device Name	Accuracy	Overall	
			FAR	UND
1	Smoke detector	97.40	0.09	0.85
2	Indoor camera	99.20	0.07	1.49
3	Nest mini	97.86	0.07	1.96
4	Temperature sensor	97.58	0.09	0.93
5	Tempi temperature sensor	97.26	0.07	1.07
6	Smart lock	98.07	0.14	1.26
7	Door & window sensor	97.49	0.11	0.96
8	Button remote control	98.19	0.05	1.39
9	Energy socket	97.61	0.08	0.74
10	Smart light bulb	98.15	0.12	1.94
11	Mi smart scale	96.96	0.13	1.49
12	Mi band 8	98.62	0.08	1.70
13	Mijia hygrometer 2	99.44	0.08	0.97
14	Key finder	97.05	0.09	1.48
15	Otbeat sport band	98.54	0.04	1.15
16	HomePod 2	98.73	0.12	1.13
	Average	**98.01**	**0.09**	**1.28**