BLEGuard: Hybrid Detection Mechanism for Spoofing Attacks in Bluetooth Low Energy Networks (Research Proposal)

Hanlin Cai[1,2]

[1]National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland
[2]Key Laboratory of Industrial Automation Control Technology and Information Processing, China
Email: hanlin.cai.2021@mumail.ie

Abstract

As the most widely used low-power communication protocol, cybersecurity research on Bluetooth Low Energy (BLE) has garnered significant attention. Due to BLE's inherent security limitations and firmware vulnerabilities, spoofing attacks can easily compromise BLE devices and tamper with privacy data. In this paper, we proposed *BLEGuard*, a hybrid detection mechanism combined cyber-physical features judgment and learning-based models. We built a real-world network testbed to conduct attack simulations and capture advertising packages. Four different network features were utilized to implement detection and classification algorithms. Preliminary results have verified the feasibility of our proposed methods.

Introduction

Bluetooth Low Energy is one of the most widely used protocols for Internet of Things devices (e.g., smart lights, smart sensors and smart thermostats). It is expected that the number of BLE devices will reach 6.5 billion by 2025. Unfortunately, these devices are vulnerable to spoofing attacks since most of them have limited I/O capabilities and do not support firmware updates. To address the security challenge, an out-of-the-box detection method has been proposed, leveraging BLE's cyber-physical features to defend against advanced spoofing attackers without requiring any interference or updates (Wu et al. 2020). Additionally, several works rely on learning-based techniques to identify the malicious packages within BLE networks. A learning framework that integrates supervised and unsupervised learning was suggested to classify packets as benign or malicious inside each suspicious batch with high precision (Lahmadi et al. 2020). Nevertheless, most existing methods struggle to strike a balance high accuracy, low false alarm rate and low detection cost, which limits their applicability to a narrow range of scenarios. In this paper, we present *BLEGuard*, a hybrid detection mechanism based on cyber-physical features judgment and machine learning technology, which can identify advanced spoofing attacks through offline training and online analysis. Our contributions include: (i) physical BLE network testbed was built for attack simulations, (ii) detection algorithm was designed to recognize spoofing attacks, and (iii) experiments were conducted based on real-world advertising datasets.

This research proposal have been submitted to the **AAAI 2024** Student Abstract and Poster Program.

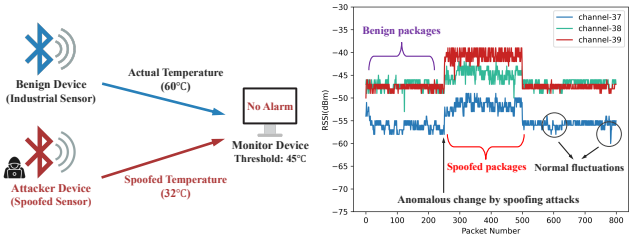

Figure 1: Left: Spoofing attack in BLE sensor network. Right: Observed RSSI values during attack simulation.

Experiment Setup

BLE Network Basics. The communication procedures between BLE devices and user devices can be categorized into four steps: advertising, connecting, pairing and accessing. However, most BLE network activities do not perform secure pairing and exchange data without conducting a secure authentication mechanism. This vulnerability can easily be exploited by attackers to inflict spoofing attacks. **Figure 1 (Left)** shows a typical spoofing attack case in BLE network.

Testbed Deployment. In this work, we built a physical BLE testbed in a typically noisy and complicated indoor office to evaluate our detection mechanism. We deployed twelve popular BLE devices covering various Bluetooth chips to set up our testbed. Additionally, we implemented three network sniffers based on the Raspberry Pi equipped with Ubertooth One, an open platform for capturing advertising package.

Feature Selection. Considering the specificity of BLE networks, four representative cyber-physical features were used for detection algorithm design and learning models training:

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

Attack Simulations. To generate multiple spoofing attacks, we utilized four distinct types of attacker platforms, each

with three identical samples at different locations. In the spoofing attack scenario, the cyber-physical features of BLE network will undergo noticeable affected, resulting in significant deviations from the benign scenario. For instance, the anomalous shift in the *RSSI* values of the advertising packets indicates the presence of spoofing attacks, as shown in **Figure 1 (Right)**. Currently, we have amassed a dataset comprising 902,890 advertising packets, with benign packets accounting for 85.2% and malicious packets for 14.8%.

Detection Mechanism

Features Judgment Algorithm. The specificity features of advertising packages can be used to determine malicious activities within BLE networks. The abrupt changes of *UCN* and *INT* can be attributed to the occurrence of potential attacks. Additionally, to detect the advanced spoofing attacks, *RSSI* and *CFO* are utilized to implement a continuous judgment mechanism. In BLEGuard, three network sniffers are utilized to collect the value of *RSSI* and *CFO* in the lookback window to infer valid ranges, and then inspect relevant values of advertising packets in the observation window. Once the system detects an abnormality in either of these two features, an alarm is raised. This detection algorithm can be easily deployed in BLE network without any interference.

Unsupervised Reconstruction Model. The reconstruction method involves learning the benign behavior of BLE packet exchanges. In offline training phase, we aim to minimize the error between learned data D_L and original dataset D_T. In online testing phase, if input data contains any malicious package, the reconstruction error will obviously increase. In this paper, network reconstructions are conducted using a temporal convolutional network. The residual is defined as $R(D_T, D_L) = |D_T - D_L|$ with $D_L = f(D_T)$ and f represents the transformation of *TCN* auto-encoder. Afterwards, we evaluate the residual to determine the anomaly score α for each data batch, as illustrated in Equation (1), where R_α represents the corresponding residual, μ is the mean value of residual, and σ is its standard deviation. In a word, reconstruction methods are employed to detect suspicious data batches, in next step, we will utilize the classification model to identify the malicious packets involved in network traffic.

$$\alpha = \begin{cases} 0, \ when \ |R_\alpha - \mu R_\alpha| \leq 3 * \sigma R_\alpha \\ 1, \ otherwise \end{cases} \quad (1)$$

Supervised Classification Models. Upon the identification of suspicious batches, the next stage is to categorize these packages into different classes: benign or malicious. In this study, we employed the text-convolutional neural network (text-CNN) (Chen et al. 2022) for traffic features extraction and we evaluated the performances of four different classifiers (SVM, KNN, Random Forest and Naïve Bayes) in package classification. In particular, the payload based features are extracted by converting the payload bytes into low dimensional vectors utilizing the *Word2Vec* technique. These vectors served as the input for the text-CNN model, and the generating features were concatenated with statistical network features and provided for the final classification.

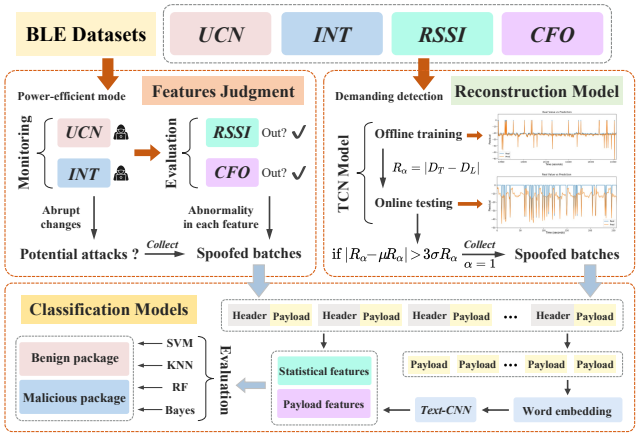

Figure 2: The workflow of BLEGuard detection mechanism.

Hybrid Detection Mechanism. Overall, BLEGuard system aims to balance the detection precision and power overhead within BLE networks. As shown in **Figure 2**, when GPU resources are not abundant enough, features judgment algorithm can be deployed online with very low consumption, while reconstruction models can be utilized when detection correctness is highly demanding. In addition, the classification models can identify specific malicious advertising packets very reliably. Preliminary experimental results verified the feasibility and non-interference of BLEGuard[1]. We will provide our code for the reproducibility of experiments[2].

Future Works

To improve BLEGuard system, future plans are as follows:

- More advertising package datasets need to be collected.
- Learning models' training and testing will be expanded.
- Optimal configurations between high precision and low power cost will be explored and verified in real datasets.

References

Chen, X.; Hao, Z.; Li, L.; Cui, L.; Zhu, Y.; Ding, Z.; and Liu, Y. 2022. Cruparamer: Learning on parameter-augmented api sequences for malware detection. *IEEE Transactions on Information Forensics and Security*, 17: 788–803.

Lahmadi, A.; Duque, A.; Heraief, N.; and Francq, J. 2020. MitM attack detection in BLE networks using reconstruction and classification machine learning techniques. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*, 149–164. Springer.

Wu, J.; Nan, Y.; Kumar, V.; Payer, M.; and Xu, D. 2020. {BlueShield}: Detecting spoofing attacks in bluetooth low energy networks. In *23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*.

[1]Supplement: https://www.researchgate.net/publication/374977587

[2]Code: https://github.com/BLEGuard/supplement