Poster: Hybrid Detection Mechanism for Spoofing Attacks in Bluetooth Low Energy Networks

Hanlin Cai[1,3], Yuchen Fang[1], Jiacheng Huang[1], Meng Yuan[2,3], Zhezhuang Xu[3*]
[1]National University of Ireland, Maynooth, [2]Chalmers University of Technology, [3]Fuzhou University
{hanlin.cai.2021, yuchen.fang.2021, jiacheng.huang.2022}@mumail.ie, {meng.yuan, zzxu}@fzu.edu.cn

ABSTRACT

As the foremost protocol for low-power communication, Bluetooth Low Energy (BLE) significantly impacts various aspects of our lives, including industry and healthcare. Given BLE's inherent security limitations and firmware vulnerabilities, spoofing attacks can readily compromise BLE devices and jeopardize privacy data. In this paper, we introduce ***BLEGuard***, a hybrid mechanism for detecting spoofing attacks in BLE networks. We established a physical Bluetooth system to conduct attack simulations and construct a substantial dataset (***BLE-SAD***). *BLEGuard* integrates pre-detection, reconstruction, and classification models to effectively identify spoofing activities, achieving an impressive preliminary accuracy of 99.01%, with a false alarm rate of 2.05% and an undetection rate of 0.36%.

CCS CONCEPTS

• **Security and privacy** → *Mobile and wireless security*.

KEYWORDS

Mobile Systems, Security and Privacy, Deep Learning

ACM Reference Format:
Hanlin Cai[1,3], Yuchen Fang[1], Jiacheng Huang[1], Meng Yuan[2,3], Zhezhuang Xu[3*] . 2024. Poster: Hybrid Detection Mechanism for Spoofing Attacks in Bluetooth Low Energy Networks. In *Proceedings of The 22nd ACM International Conference on Mobile Systems, Applications, and Services (MobiSys '24).* ACM, New York, NY, USA, 2 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Named after the Viking King Harald Bluetooth, Bluetooth is one of the most popular protocols for short-range wireless communications. The advent of the Bluetooth Low Energy (BLE) standard has further solidified its dominance in the era of IoT and 5G. By 2027, the deployment of BLE devices is anticipated to burgeon to 7.5 billion [4]. Despite their widespread adoption, these devices remain prone to spoofing attacks due to their limited I/O capabilities and lack of support for firmware upgrades. To combat these security threats, a device-neutral monitoring framework has been introduced, capitalizing on BLE's cyber-physical attributes to fortify defenses against spoofing attackers [5]. Furthermore, various research initiatives employ machine learning techniques to detect anomalous patterns within BLE network traffic. A proposed learning framework that amalgamates reconstruction and classification models promises to discern packets as either benign or malicious with remarkable precision [1]. However, the prevalent challenge lies in harmonizing accuracy, false positive rates, and resource utilization for detection, a triad that presents substantial obstacles to real-world application.

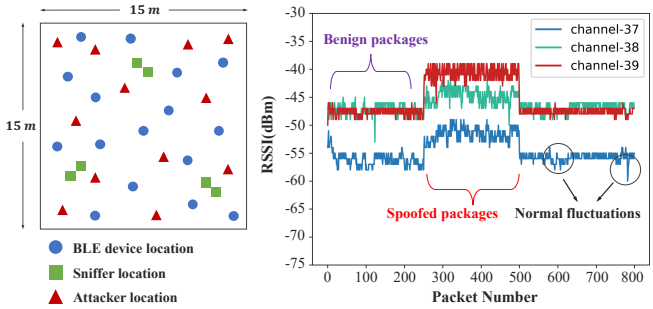

Figure 1: (a) Proposed BLE network testbed and (b) observed RSSI values during attack simulation.

In this paper, we present *BLEGuard*, a hybrid detection mechanism based on cyber-physical analysis and deep learning techniques. *BLEGuard* is capable of pinpointing intricate spoofing attacks by integrating offline training with real-time analysis. **Our contributions are threefold:** (i) the compilation of *BLE-SAD*, a large-scale dataset encompassing in excess of 1.2 million packets, specifically curated for model evaluation, (ii) the conceptualization and empirical validation of *BLEGuard*, engineered to proficiently detect spoofing intrusions, (iii) the capacity for *BLEGuard* to seamlessly integrate within BLE networks, ensuring detection is accomplished without causing interference or taxing the network's resources.

2 SYSTEM DESIGN

2.1 Testbed Deployment

In this work, we built a physical network testbed within a typical noisy indoor office environment. Nine mainstream BLE devices, featuring a range of Bluetooth chips such as nRF52840 and DA14585, were deployed to establish our testbed, as depicted in **Fig. 1**. Besides, three network sniffers were deployed using Raspberry Pi equipped with BLE-Analyzer-PRO to monitor and capture network activity.

***BLE-SAD* Dataset**: To generate multiple spoofing attacks, we utilized four 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 Received Signal Strength Indicator (RSSI) of advertising packets indicates the presence of spoofing activities (**Fig. 1**). Currently, we have accumulated

MobiSys '24, June 03–07, 2024, Tokyo, Japan

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/XXXXXXX.XXXXXXX

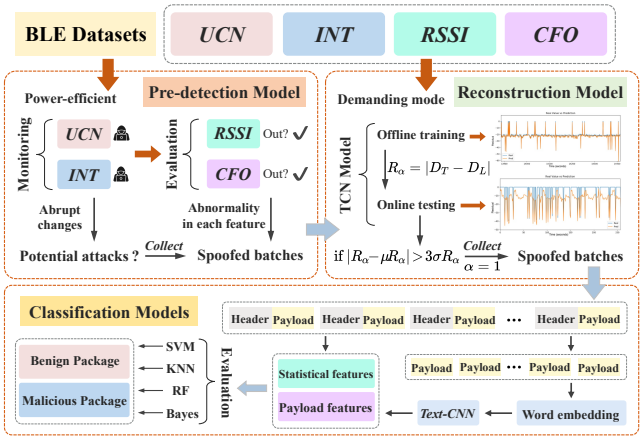

Figure 2: The workflow of *BLEGuard* detection mechanism.

a dataset comprising 1,209,200 advertising packets, with benign packets accounting for 80.3% and malicious packets for 19.7%.

2.2 Detection Mechanism

Pre-detection Scheme: The suspicious activities can be identified based on the atypical fluctuations in cyber-physical features, like Used Channel Numbers (UCN), Advertising Interval (INT), Carrier Frequency Offset (CFO) and Received Signal Strength Indicator (RSSI). In *BLEGuard*, three network sniffers are deployed to capture the values of these four features within a lookback window, establishing a baseline for normal behavior. Subsequently, the system scrutinizes the corresponding values of advertising packets within an observation window. An alarm is triggered upon detecting any deviation from the established norms in any of these features. This straightforward scheme can be seamlessly integrated into BLE networks without causing any disruption and internal consumption.

Learning-based Detection: Upon detecting suspicious activities, we embark on a comprehensive analysis of anomalous data batches. A Temporal Convolutional Network (TCN) [2] is utilized to reconstruct traffic patterns, facilitating the isolation of aberrant data through comparative analysis. During the offline training phase, our aim is to minimize the error between the learned data D_L and the original dataset D_T. In the online testing phase, the presence of malicious packets in the input data leads to an increase in the reconstruction error. The residual is defined as $R(D_T, D_L) = |D_T - D_L|$ with $D_L = f(D_T)$, where f denotes the transformation function of the TCN auto-encoder. We assess this residual to determine the anomaly score α for each data batch, as depicted in Equation (1), with R_α representing the corresponding residual, μ as the mean value of the residual, and σ as its standard deviation.

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

Packet Classification: After pinpointing suspicious batches, the subsequent step is to classify these packets into two categories: benign or malicious. In this study, a text-convolutional neural network (text-CNN) [3] is utilized for traffic feature extraction, while packet classification is performed using four cost-efficient classifiers (SVM, KNN, Random Forest, and Naïve Bayes) to avoid bias in text analysis. Network payload-based features are generated by converting the payload bytes into low-dimensional vectors using *Word2Vec* techniques. These vectors serve as the input for the text-CNN, and the extracted key features are concatenated with statistical features for input into the final classification models.

Table 1: Detection performance of *BLEGuard*

ID	Device (Number)	Accuracy	FAR	UND
1	Xiaomi Sensor (*3)	99.06%	2.24%	0.29%
2	Xiaomi Locker (*2)	99.10%	2.04%	0.33%
3	Xiaomi Speaker (*2)	98.92%	1.84%	0.36%
4	Apple HomePod (*1)	99.03%	2.13%	0.34%
5	Dell Speaker (*1)	99.05%	2.52%	0.31%
6	Lenovo Speaker (*1)	98.85%	1.82%	0.61%
7	August Smart Lock (*2)	99.01%	2.41%	0.19%
8	Nutale Key Finder (*2)	99.04%	1.46%	0.52%
9	Nordic nRF52 DK (*2)	99.06%	1.97%	0.36%
Overall		**99.01%**	**2.05%**	**0.36%**

System Overview: *BLEGuard* is designed to strike a balance between detection accuracy and power overhead in BLE networks. As illustrated in **Fig. 2**, when GPU resources are constrained, the pre-detection algorithm can be efficiently implemented with minimal online consumption. Conversely, reconstruction models are activated when achieving high detection accuracy is of utmost importance. Furthermore, the classification models can reliably pinpoint specific malicious advertising packets and offer precise feedback to enhance the performance of the detection modules.

3 PRELIMINARY RESULTS

We evaluate the performance of *BLEGuard* through large-scale, imbalanced data collected from nice different BLE devices, as illustrated in **Table 1**. The results revealed a high level of effectiveness, achieving an average accuracy of 99.01%, with a false alarm rate of 2.05% and an un-detection rate of 0.36%. We have provided our code and data for the reproducibility of experiments[1].

ACKNOWLEDGMENTS

This project was supported by the Chinese National Undergraduate Innovation Training Program (No. 202310386056) and AAAI 2024 Undergraduate Consortium Scholarship.

REFERENCES

[1] Abdelkader Lahmadi, Alexis Duque, Nathan Heraief, and Julien Francq. 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*. Springer, 149–164.
[2] Colin Lea, Michael D Flynn, Rene Vidal, Austin Reiter, and Gregory D Hager. 2017. Temporal convolutional networks for action segmentation and detection. In *proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*.
[3] Erxue Min, Jun Long, Qiang Liu, Jianjing Cui, and Wei Chen. 2018. TR-IDS: Anomaly-based intrusion detection through text-convolutional neural network and random forest. *Security and Communication Networks* 2018 (2018).
[4] Bluetooth SIG. 2024. Bluetooth Market Update. Online: https://bluetooth.com/2024-market-update/.
[5] Jianliang Wu, Ruoyu Wu, Dongyan Xu, Dave Tian, and Antonio Bianchi. 2023. SoK: The Long Journey of Exploiting and Defending the Legacy of King Harald Bluetooth. In *2024 IEEE Symposium on Security and Privacy (S&P)*.

[1]Link: https://github.com/BLEGuard/supplement