Securing Billion Bluetooth Devices leveraging Learning-based Techniques

Keywords: Bluetooth Low Energy, Security and Privacy, Deep Learning

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. It is expected that BLE will be empowering up to 7.5 billion devices by 2027 [1]. This exponential adoption, however, is overshadowed by BLE's inherent security limitations and firmware vulnerabilities, which render devices susceptible to spoofing attacks, compromising not only the integrity of myriad BLE-enabled systems but also the confidentiality of sensitive data in transit [2].

Background: In response to the security challenges, an out-of-the-box detection method has been proposed, leveraging BLE's cyber-physical features to defend against spoofing attackers without requiring any interference or updates [3]. Additionally, several works rely on learning-based techniques to identify the malicious packets within BLE network traffic. A learning framework that integrates reconstruction and classification models was suggested to classify packets as benign or malicious inside each suspicious batch with high precision near 99.0% [4]. However, most existing methods struggle with the challenge of reconciling high detection accuracy with low computational cost, which limits their applicability across a more expansive range of real-world situations [5, 6].

Prior Work by the Applicant: During my internship at State Key Laboratory of Industrial Automation Control Technology and Information Processing in my college, I spearheaded a research initiative focused on detecting spoofing attacks in BLE networks through cyber-physical feature judgment. To evaluate the judgment algorithm, I established a physical BLE testbed by deploying 16 mainstream consumer BLE devices like smart thermometers and door locks, as well as four simulated attacker platforms. By collecting approximately 902,980 benign advertising packets and 107,546 spoofed advertising packets, the dataset used for detection algorithm validation was formed. Experimental results show that our proposed algorithm achieved an average accuracy of over 98.7% and can be deployed on low-cost off-the-shelf platforms. This prior work can contribute substantial data and code [7] and valuable experience to support my forthcoming research.

Proposal: I propose to further explore the challenge of advanced spoofing attacks detection through combining the reconstruction model and classification model for efficient large-scale online detection. Previous works [4, 8] have verified the effectiveness of extracting characteristic features of BLE networks for learning, these statistical features include used channel numbers (*UCN*), advertising interval (*INT*), received signal strength (*RSS*), and carrier frequency offset (*CFO*). However, two essential enhancements must be made to existing learning strategy for a better balance between high accuracy and low detection cost. These focus on pre-detection and key feature extraction.

Pre-detection: The extensive computational overhead of current reconstruction models hinder their suitability for real-time online detection. To improve this, I propose a novel pre-detection algorithm derived from my prior work, which promises to substantially decrease the computational load, making continuous online detection feasible without incurring exorbitant processing costs.

Feature Extraction: While the all-feature end-to-end models like Transformer have demonstrated outstanding performance in network text-classification tasks [9], their substantial resource requirements render it impractical for deployment within BLE networks. Thus, I propose to circumvent this by embedding key feature extraction into cost-efficient classification models, striking an optimal balance between computational resource demands and network packet analysis efficacy.

Method: In this study, I plan to develop a novel hybrid detection mechanism for BLE spoofing attack detection in three stages: (i) pre-detection, (ii) reconstruction, and (iii) classification.

Pre-detection Algorithm: The specificity features of advertising packets can be used to determine malicious activities within BLE networks. The abrupt changes in *UCN* and *INT* can be attributed to the occurrence of potential attacks. Additionally, to detect advanced spoofing attacks, *RSS* and *CFO* are utilized to implement a continuous pre-detection mechanism. In my work, three network sniffers will be deployed to collect the value of *RSS* 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 network features, an alarm will be raised. This pre-detection algorithm can be deployed in BLE devices without any interference.

Reconstruction Model: Following the pre-detection stage, where the system potentially identifies malicious activities and triggers an alarm, the focus shifts to the reconstruction analysis. In the offline training phase, I aim to minimize the error between learned data D_L and original dataset D_T. In the online testing phase, if the input data batches contain any malicious packet, the reconstruction error will obviously increase. In this research, network reconstructions are conducted using a lightweight temporal convolutional network (TCN) [10]. 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. Subsequently, I will 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 the residual, and σ is its standard deviation. In a word, the reconstruction model is employed to detect suspicious data batches within network traffic. In the next step, classification models will be utilized to identify the malicious packets involved in each suspicious batch.

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

Classification Models: Upon the identification of suspicious batches, the next stage is to categorize these packets into different classes: benign or malicious. In this study, the text-convolutional neural network (text-CNN) [11] is employed for traffic feature extraction while the packet classification will be conducted using four cost-efficient classifiers (SVM, KNN, Random Forest and Naïve Bayes) to prevent bias in text analysis [12]. The network payload-based features are generated by converting the payload bytes into low dimensional vectors utilizing the *Word2Vec* techniques. These vectors served as the input for the text-CNN model, and the extracted key features were concatenated with statistical features and provided for the final classification models.

Evaluation: I will conduct experiments based on the dataset collected from real-world BLE networks. In prior work, I have built a physical BLE testbed with 16 user BLE devices, 4 attacker platforms, and 3 network sniffers. This testbed will be further expanded and be used to generate large-scale data for model training and online testing. Also, I will perform experiments based on known real-world attacks like InjectaBLE [13] and Btlejack [14]. The results of my method will be compared to baseline models, including BLE-guardian [15], BlueShield [3], and BLEDiff [16].

Broader Impact: This proposal addresses a crucial challenge in Bluetooth security and provides a substantial dataset for wireless security research. Beyond security improvements, the approach encourages interdisciplinary collaborations and sets a precedent for deploying deep learning models in resource-constrained environments. Successful outcomes can significantly reduce the global economic and social repercussions of attacks on billions of Bluetooth devices, influencing not only the field of cybersecurity but also the daily lives of countless users dependent on these technologies.

References

[1] Bluetooth SIG. Bluetooth market update. Online: https://bluetooth.com/2023-market-update/, November 2023.

[2] Andrea Lacava, Valerio Zottola, Alessio Bonaldo, Francesca Cuomo, and Stefano Basagni. Securing bluetooth low energy networking: An overview of security procedures and threats. *Computer Networks*, 211:108953, 2022.

[3] Jianliang Wu, Yuhong Nan, Vireshwar Kumar, Mathias Payer, and Dongyan Xu. {BlueShield}: Detecting spoofing attacks in bluetooth low energy networks. In *23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*, 2020.

[4] Abdelkader Lahmadi, Alexis Duque, Nathan Heraief, and Julien Francq. 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*, pages 149–164. Springer, 2020.

[5] Arup Barua, Md Abdullah Al Alamin, Md Shohrab Hossain, and Ekram Hossain. Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey. *IEEE Open Journal of the Communications Society*, 3:251–281, 2022.

[6] Jianliang Wu, Ruoyu Wu, Dongyan Xu, Dave Tian, and Antonio Bianchi. Sok: The long journey of exploiting and defending the legacy of king harald bluetooth. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 23–23. IEEE Computer Society, 2023.

[7] Hanlin Cai, Yuchen Fang, Meng Yuan, and Zhezhuang Xu. Bleguard: Hybrid detection mechanism for spoofing attacks in bluetooth low energy networks. Online: https://github.com/BLEGuard/supplement, November 2023.

[8] Muhammad Yaseen, Waseem Iqbal, Imran Rashid, Haider Abbas, Mujahid Mohsin, Kashif Saleem, and Yawar Abbas Bangash. Marc: A novel framework for detecting mitm attacks in ehealthcare ble systems. *Journal of medical systems*, 43:1–18, 2019.

[9] Ting Jiang, Deqing Wang, Leilei Sun, Huayi Yang, Zhengyang Zhao, and Fuzhen Zhuang. Lightxml: Transformer with dynamic negative sampling for high-performance extreme multi-label text classification. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 35, pages 7987–7994, 2021.

[10] Zumin Wang, Jiyu Tian, Hui Fang, Liming Chen, and Jing Qin. Lightlog: A lightweight temporal convolutional network for log anomaly detection on the edge. *Computer Networks*, 203:108616, 2022.

[11] Xiaohui Chen, Zhiyu Hao, Lun Li, Lei Cui, Yiran Zhu, Zhenquan Ding, and Yongji Liu. Cruparamer: Learning on parameter-augmented api sequences for malware detection. *IEEE Transactions on Information Forensics and Security*, 17:788–803, 2022.

[12] Maede Zolanvari, Marcio A Teixeira, Lav Gupta, Khaled M Khan, and Raj Jain. Machine learning-based network vulnerability analysis of industrial internet of things. *IEEE Internet of Things Journal*, 6(4):6822–6834, 2019.

[13] Romain Cayre, Florent Galtier, Guillaume Auriol, Vincent Nicomette, Mohamed Kaâniche, and Géraldine Marconato. Injectable: Injecting malicious traffic into established bluetooth low energy connections. In *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 388–399. IEEE, 2021.

[14] Damien Cauquil. Defeating bluetooth low energy 5 prng for fun and jamming. *DEF CON*, 27, 2019.

[15] Kassem Fawaz, Kyu-Han Kim, and Kang G Shin. Protecting privacy of {BLE} device users. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 1205–1221, 2016.

[16] Imtiaz Karim, Abdullah Al Ishtiaq, Syed Rafiul Hussain, and Elisa Bertino. Blediff: Scalable and property-agnostic noncompliance checking for ble implementations. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 3209–3227. IEEE, 2023.