2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS) | 979-8-3503-3071-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICPADS60453.2023.00135

FingerBLE: A Device Fingerprint Identification Scheme for BLE devices

Xikai Sun
Department of Automation
Tsinghua University
Beijing, China
sxk23@mails.tsinghua.edu.cn

Fan Dang
Global Innovation Exchange
Tsinghua University
Beijing, China
dangfan@tsinghua.edu.cn

***Abstract*—With the increasing popularity of industrial networks, driven by the development of the Internet of Things, cloud computing, and big data, there are still security threats when it comes to using wireless communication technologies, including BLE, in these networks. This is primarily due to the heterogeneity and resource limitations of the devices. To address the issues of device cloning and enhance BLE device access authentication, a device authentication mechanism based on physical features can be employed. By leveraging the uniqueness and nonreplicability of physical attributes, such as fingerprints, this mechanism effectively mitigates attacks. Therefore, this paper proposes a BLE device authentication scheme called FingerBLE, which relies on the physical fingerprints of devices at the physical-layer. In terms of system design, this article also introduces a fingerprint database authentication mechanism that utilizes the aforementioned fingerprints for node recognition and legitimacy authentication. Experimental results demonstrate that FingerBLE is capable of successfully extracting corresponding device fingerprints and accurately identifying nodes across a wide range of tests.**

***Index Terms*—BLE network, device fingerprint, feature extraction**

I. Introduction

With the development of the Internet of Things (IoT), cloud computing, and big data, the application of the Industrial Internet of Things (IIoT) is becoming increasingly widespread, leading to a rapid increase in industrial network devices like BLE and Wi-Fi devices. However, this increase in the number of devices also implies a significant increase in the potential for attacks. For example, in 2017, the Reaper IoT botnet successfully exploited publicly disclosed vulnerabilities to infect IoT devices [1]. In 2018, the IoT malware, HideNSeek, successfully achieved device persistence even after a reboot, causing irreparable infections [2]. These continuously emerging and novel network attacks amplify the challenges and urgency associated with network security.

Meanwhile, due to its advantages such as low power consumption, cost efficiency, and high compatibility, Bluetooth Low Energy (BLE) is becoming a widely adopted infrastructure in Industrial Internet of Things (IIoT) [3]. However, BLE applications often employ a "just works" security method, which leaves BLE devices vulnerable to eavesdropping attacks and other risks. For example, NCC Group, a company specializing in information security, successfully carried out a relay attack targeting the BLE link layer to breach the keyless entry system of the Tesla Model 3 and Model Y, which relies on BLE-based authentication mechanisms, as illustrated in Fig. 1 [4]. Traditional BLE authentication and network access processes take place in the broadcast channel, making authentication information easily captured and vulnerable to malicious activities such as signal replay and device cloning. These vulnerabilities pose potential threats to the entire network. Fortunately, BLE devices commonly possess certain inherent physical imperfections known as device fingerprints, which are unique and nonreproducible. By incorporating device fingerprints into the BLE authentication process, the security of the authentication mechanism can be significantly enhanced, solving attacks such as signal replay and device cloning.

Insighted by the opportunity, we propose a BLE device authentication scheme called FingerBLE, which is based on device fingerprints of the physical layer. The scheme consists of two stages: the registration stage and the recognition stage. In the registration stage, we extract features from the BLE device's broadcast signal and assess the specificity of the physical characteristics. High-specificity features are selected as device fingerprints and added to the fingerprint database. The nodes registered in the database will be referred to as legitimate nodes. In the recognition stage, when the BLE nodes are applied to join the BLE network, we employ similar feature extraction methods to match and identify device fingerprints. Only nodes that successfully match will be considered legitimate and allowed to access the BLE network. In summary, this paper makes the following contributions:

- We present the FingerBLE scheme, which utilizes physical layer device fingerprints for BLE device authentication in industrial networks.
- We develop a matching and identification mechanism based on these extracted features to authenticate BLE devices in an industrial setting.
- We systematically evaluate the effectiveness of the FingerBLE scheme through extensive experiments.

Fan Dang is corresponding author.

2690-5965/23/$31.00 ©2023 IEEE
DOI 10.1109/ICPADS60453.2023.00135

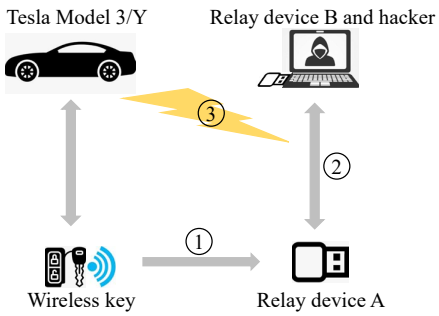

Fig. 1. The process of Tesla being attacked. The hacker employs a technique in which a relay device A is secretly placed within a 14-meter range of a Tesla owner's wireless key fob. This device aims to intercept and capture the signals emitted by the wireless key fob. Additionally, another relay device B is connected to a laptop and strategically placed in proximity to the vehicle. By establishing communication between these two relay devices, the captured BLE signals from the wireless key fob acquired by device A are effectively replayed and amplified, allowing the vehicle to recognize and perceive them. Consequently, even if the genuine wireless key fob is physically distant from the vehicle's designated communication range, the car can still receive the key's signals, enabling the unlocking and ignition processes to ensue.

Overall, this paper contributes to the advancement of secure authentication solutions for BLE devices in the IIoT.

The remainder of this paper is structured as follows: In Section II, we provide a comprehensive review of the current state of relevant research in the field. In Section III, we present FingerBLE scheme in detail. The effectiveness of the scheme will be evaluated in Section IV. Finally, Section V concludes this paper and provides a discussion of the findings.

II. Related Work

There have been many relevant research works in the field of IIoT device authentication. Xie et al. [5] propose an active scanning-based network access control scheme that periodically scans the connected devices, effectively preventing IP/MAC spoofing attacks. Another study [6] suggests a comprehensive port scanning approach for IIoT devices, optimizing the scanning rate to maximize device security and ensure long-term accuracy of device identification. In order to prevent attackers from impersonating damaged devices, an automatic encoder [7] is proposed to detect compromised or infected devices in the network, denying access to higher-level networks from these devices. To reduce computational and energy pressures on the recipient side, a trust evaluation mechanism for node devices [8] is transplanted to the edge network, significantly improving the identification efficiency.

With the advancement of machine learning, novel efforts have been made to analyze the fingerprint features of data packets in network traffic using machine learning models. This approach aims to detect and identify whether a data packet originates from a legitimate device, thereby defending against malicious data intrusion based on packet traffic analysis. For instance, in the study by [9], deep neural networks are employed for deception attack detection. [10] utilizes support vector machines (SVM) for offline defense against deception attacks, while [11] employs Gaussian mixture models to enhance identity verification privacy. In [12], an anomaly-based intrusion detection solution is proposed to dynamically and proactively analyze and monitor all connected devices, with the aim of detecting device tampering attempts and suspicious network transactions. This solution calculates out-of-bounds network profile behaviors by continuously monitoring the network traffic of each device with expensive hardware infrastructure, effectively recognizing vulnerabilities and abnormal traffic. In [1], a method is proposed that utilizes a set of sparse auto-encoders to detect anomalous network communication. By learning legitimate communication profiles for each node device type, it can automatically differentiate between malicious and legitimate packets, preserving legitimate communication while discarding anomalous communication. The trained model is embedded within the recipient's device, eliminating the need for additional hardware infrastructure. Similar approaches can also be applied to software-defined networks (SDNs). For example, [13] introduces an SDN-based proactive alert manager solution deployed in gateways. It classifies traffic at the gateway and utilizes an ensemble model to identify attacks within the network, thus detecting and mitigating malicious traffic. Since these machine learning-based security mechanisms are established at the information level, they do not necessarily require the legitimacy of the node devices. This allows for the existence of malicious nodes disguised as legitimate nodes. The key lies in observing the changes in traffic at upper-layer devices to automatically filter out the data traffic generated by these malicious nodes. These approaches ensure the dynamic scalability of the network while safeguarding device security.

For BLE devices, a study [14] proposes the prevention of device deception and device cloning attacks by monitoring the operational lifecycle of devices. Unique network flow characteristics are extracted from the link layer and the ATT / GATT service layer to generate fingerprint features for device authentication. Prior to establishing a connection with a BLE device, the network observes the link layer transmission signatures and checks them against a global blacklist database for potential deception attacks. To improve the accuracy of authentication, a study [15] suggests using more complex authentication schemes that incorporate not only device fingerprints, but also passwords and user information for verification. The aim is to increase the diversity of authentication information and further improve anticounterfeiting measures.

Although the aforementioned works have conducted in-depth research to ensure the legitimacy of industrial network devices, there are still some challenges:

- **Limited applicability**: Due to the heterogeneity of devices in the IIoT, many studies cannot be applied directly to the authentication and identification of BLE network devices.
- **Closed nature of BLE technology**: The achievements

in BLE device authentication are primarily limited to the link layer and the ATT/GATT service layer, and the data frames used for authentication still have the possibility of being forged.

These challenges have also served as one of the key motivations for the development of FingerBLE. By leveraging the inherent uniqueness and nonreplicability of the physical characteristics of BLE devices, FingerBLE enables highly accurate identification of BLE devices.

III. Scheme Design

When a BLE device joins the network, the registration request information of the node is bound to its unique and tamper-proof physical characteristics. This approach utilizes the non-reproducibility of device physical features to prevent network attacks such as device cloning. Based on the aforementioned notion, the specific workings of FingerBLE are shown in Fig. 2. In the FingerBLE scheme, the BLE networking process can be divided into two stages: the registration stage and the identification stage. It should be noted that registering a BLE device in the device fingerprint database does not imply immediate joining of the BLE network. During the registration stage, users can extract device fingerprints for new BLE devices and add these fingerprints to the device fingerprint database, thus completing the verification of the node's legitimacy. In the identification stage, when a new node wants to join an existing BLE industrial network, the following process must be completed.

(1) The BLE node initiates a network access request to the master node of the BLE industrial network.
(2) The device fingerprint extractor of the physical layer captures the physical signals from the BLE node and extracts the specified device fingerprint.
(3) The master node sends the BLE device fingerprint to the database terminal.
(4) The database terminal compares the fingerprint of the device with the fingerprints of the nodes registered in the database and returns the result of the comparison.
(5) When the comparison result is true, the joining node is considered legitimate and the master node sends the network access information to the node. Otherwise, the network access request is rejected.

In this section, we will sequentially discuss the processes of feature extraction from BLE signals, how to evaluate those features, and the registration and identification stage of the fingerprint database.

A. Feature Extraction and Evaluation

BLE utilizes the GFSK modulation waveform, allowing decoding without the need for precise calibration of carrier frequency offset (CFO) and I/Q imperfections [16]. Meanwhile, these imperfections may exhibit desirable specificity, which ensures the effectiveness of FingerBLE. However, traditional BLE receivers only provide a coarse estimation of these

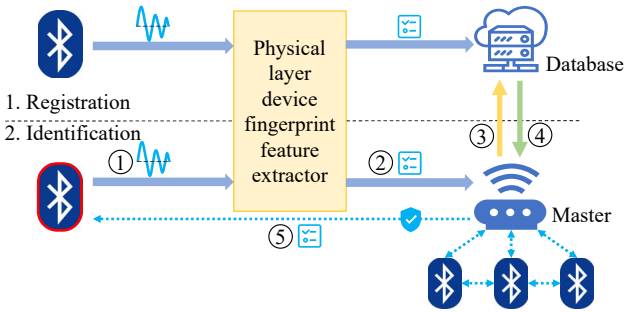

Fig. 2. The overview of FingerBLE.

physical characteristics by examining the preamble of the BLE signal, rendering the estimation results inadequate for node identification [17]–[19]. To accurately estimate these features from the BLE physical signal, we adopt the Joint Estimation Algorithm proposed in [16]. The general procedure of this algorithm is shown in Fig. 3. The specific details of the Joint Estimation Algorithm will be explained in the following text.

After sampling a BLE physical signal, we can decode it to obtain the corresponding binary sequence, which represents the encoded form of the data packet. For valid BLE sequences, the decoded output typically includes a valid CRC that can be used for packet verification. Then we can reconstruct the waveform of the signal with GFSK encoding (i.e., by constructing the corresponding waveform function). The resulting ideal unbiased baseband waveform signal, denoted as y, is as follows:

$$y = e^{i\omega(t)t}, \tag{1}$$

where $\omega(t)$ represents the baseband frequency generated by the decoded binary sequence according to GFSK modulation. Since the reconstruction process is conducted in a mathematical sense rather than generating an actual physical signal, the reconstructed waveform is theoretically unbiased and unaffected by hardware-related physical impairments in signal generators and the like. After obtaining the unbiased signal function, we can introduce offset parameters representing physical impairments to intentionally distort the waveform, resulting in a biased signal denoted as y' as follows [16]:

$$\begin{aligned} y'(t) =& A\left(\left(1-\frac{\epsilon}{2}\right) cos\left(\omega(t)t-\frac{\phi}{2}\right)+I\right. \\ &\left.+j\left(\left(1+\frac{\epsilon}{2}\right) sin\left(\omega(t)t+\frac{\phi}{2}\right)+Q\right)e^{j(\phi_0+2\pi f_0 t)}, \end{aligned} \tag{2}$$

where the parameters f_0, ϕ_0, A, $\frac{1-\epsilon}{1+\epsilon}$, ϕ, I and Q respectively represent the carrier frequency offset (CFO), phase offset, normalized amplitude of the signal, I/Q amplitude imbalance, I/Q phase imbalance, I-component offset, and Q-component offset. To determine suitable values for these parameters, in the Joint Estimation Algorithm, the distorted waveform is

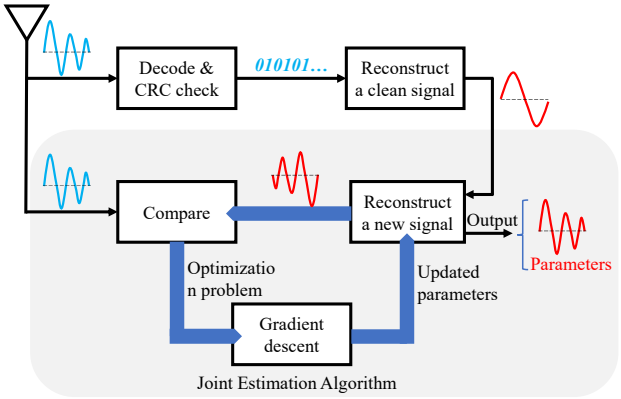

Fig. 3. The Joint Estimation Algorithm [16].

compared with the original physical waveform. Thus, the following optimization problem needs to be solved:

$$\min_{f_0,\phi_0,A,\epsilon,\phi,I,Q} L(f_0,\phi_0,A,\epsilon,\phi,I,Q) = ||y' - y||_2. \quad (3)$$

To accelerate the exploration of the parameters, this method uses a gradient descent algorithm to iteratively seek the optimal solution for the optimization problem. Ultimately, the iterative process aims to align the distorted waveform with the original input BLE physical signal in terms of its fundamental shape.

Compared to the traditional approach of using preamble-based estimation, the Joint Estimation Algorithm relies on the complete RF signal of the entire data packet, which offers richer information. Therefore, the accuracy of the estimation is significantly higher than the former. For example, the accuracy of the CFO estimation using the latter is 50 Hz, whereas for the former, it is only 2 kHz [16]. Within a channel bandwidth of 2 kHz, such precision is sufficient to provide ample distinction for hundreds of BLE nodes.

In order to obtain the global optimum solution for the optimization problem, the Joint Estimation Algorithm requires estimation of all possible offset parameters instead of just a subset of parameters. Furthermore, prior to the estimation results, we cannot assess the specificity of these parameters. However, for the following reasons, it is not necessary to consider all parameters as the final device fingerprints.

- Several highly specific features are sufficient for identifying nodes. Introducing low-specificity features (resulting from environmental factors, computational errors, etc.) may actually lower the accuracy.
- Having more features means an increase in computational and storage cost, which is disadvantageous for rapid registration and identification of device fingerprints.

Therefore, we employ the robust Maximal Information Coefficient (MIC) as an evaluation metric to assess the association between different features and node categories. Features with high MIC values are chosen as device fingerprints.

The mutual information $I(X,Y)$ is defined as follows:

$$I(X,Y) = \sum_{X,Y} p(X,Y) \log_2 \frac{p(X,Y)}{p(X)p(Y)}, \quad (4)$$

where $p(X,Y)$ represents the joint probability of the feature X and label Y. However, in general cases, the calculation of $p(X,Y)$ for all variables X and Y can be complex. To address the relationship between two variables, we can discretize them in a two-dimensional space. By dividing the x-axis and y-axis into different intervals in this two-dimensional space, each grid interval will contain a certain number of discrete points (X,Y). In this case, the joint probability simplifies the observation of the distribution of discrete points in different grid intervals. Thus, the MIC value between X and Y can be calculated using the formula:

$$MIC(X,Y) = \min_{a \cdot b < B} \frac{I(X,Y)}{\log_2 min(a,b)}, \quad (5)$$

where a represents the number of intervals in the horizontal axis, b represents the number of intervals in the vertical axis, and B is an empirical value, typically around 0.6 times the data size. The resulting MIC value lies in the range $[0,1]$, where a higher $MIC(X,Y)$ indicates a stronger correlation between the variables X and Y. By comparing the MIC values of different physical features, we can select more specific features as device fingerprints for node identification.

B. Fingerprint Registration and Identification

After selecting J highly distinctive physical features as device fingerprints, we have designed a prototype of a fingerprint library-based authentication system. The entire fingerprint authentication process consists of two stages: registration and identification.

In the registration stage, considering the variability of device fingerprint distributions, the registered fingerprint is defined by the following equation:

$$f_j^i = \frac{\sum_{n=1}^{N} f_{jn}^i}{N}, \quad (6)$$

where f_j^i represents the registered value of device fingerprint j for node i, f_{jn}^i represents the estimated value of device fingerprint j computed from registration sample n of node i, and N is the number of registration samples. These average registered fingerprints will be added to the registration database, representing the identity information of the node.

Considering the impact of environmental factors on registration samples, we need to evaluate the samples by calculating the sample standard deviation, denoted as std_j:

$$std_j = \sqrt{\frac{\sum_{n=1}^{N} \left(f_{jn}^i - f_j^i\right)^2}{N-1}}. \quad (7)$$

If std_j exceeds a predefined threshold, we perform a DBSCAN clustering analysis on the current set of device fingerprints used for registration. We only select samples from a larger cluster as registration samples, thereby accomplishing the removal of these outlier samples.

In the identification stage, we extract the device fingerprints of the signal sample from unknown node, compare those fingerprints with the registered fingerprints in the fingerprint database, and identify the unknown node as the registered node with the closest similarity. This can be achieved with high accuracy through a straightforward comparison using weighted Manhattan distance, as represented by the following equation:

$$y_{pred}(t) = \begin{cases} \underset{i \in N^+[1,N]}{argmin} & \sum_{j=1}^{J} \alpha_j \left| f_j^t - f_j^i \right|, \\ & \text{if } \underset{i \in N^+[1,N]}{min} \sum_{j=1}^{J} \alpha_j \left| f_j^t - f_j^i \right| < \beta, \\ \text{unknown}, & \text{otherwise}, \end{cases} \tag{8}$$

where α_j represents the weight of the j-th fingerprint (with $\alpha_1 \equiv 1$). It can be obtained through techniques such as gradient descent or manual tuning that maximize the accuracy on the test set. β is the set confidence threshold, and y_{pred} denotes the predicted label for the node under test.

IV. Evaluation

A. Experimental Testbed

In the experiment, we use 51 COTS BLE nodes for the test. These nodes are from the Silicon EFR32BG22C224F512 model. The physical characteristics of BLE nodes are primarily determined by their inherent hardware flaws and are generally independent of the transmitted data packets. Therefore, the extracted physical features of any transmitted data packet should be relatively consistent. Therefore, the specific communication task performed by the BLE nodes is not of concern. For our experiment, we selected iBeacon broadcasting as the task executed by the BLE nodes. We developed a signal acquisition program using Gun Radio software and employed the HackRF One device to sample the RF signals. Finally, we collected over 20 physical signal sequences for each node. Considering the potential influence of the environment on the physical flaws of the nodes, we randomly selected 20 sequences from each node as registration samples, reserving the remainder as the test set for evaluating the scheme's performance.

B. Feature Extraction

Through the Joint Estimation Algorithm, we eventually extracted 25 candidate physical features. In order to select features with higher specificity as device fingerprints, the MIC values of these features were calculated, shown in Table I. By comparing the MIC values, it was found that features 2, 3, and 24 exhibit strong specificity, representing CFO, I phase offset, the average signal amplitude, respectively. However, the feature 24 is not strictly caused by physical hardware; it is also influenced by factors such as sampling distance and environmental noise, making it unsuitable for some scenarios of mobile networks. Therefore, in order to make the solution compatible with a wider range of network scenarios, features 2 and 3 were ultimately selected as the device fingerprints.

TABLE I
MIC values of physical level features

feature	MIC	feature	MIC	feature	MIC
0	0.1710	10	0.1040	20	0.1773
1	0.2232	11	0.1940	21	0.1964
2	0.9068	12	0.2012	22	0.3057
3	0.6044	13	0.1941	23	0.2936
4	0.1372	14	0.2019	24	0.7486
5	0.1818	15	0.2555		
6	0.1769	16	0.2574		
7	0.1089	17	0.1924		
8	0.1447	18	0.2263		
9	0.1216	19	0.1596		

C. Fingerprint Authentication

The fingerprint extraction was performed on the test set and the fingerprint recognition was performed using the equation 8. With α_1 set to 1, α_2 set to 0.002, and β set to 1000, the resulting normalized confusion matrix is visualized in Fig. 4. The depth of color within each (i, j) coordinate represents the proportion of test samples with label i that were identified as label j, relative to the total number of test samples with label i. Clearly, the higher the proportion in the diagonal grids resembling a "\" shape, the higher the recognition accuracy of the samples from the corresponding node. From Fig. 4, it can be observed that:

- For most of the test samples, a simple shortest weighted Manhattan distance method is sufficient for effective recognition. This further validates that the selected features possess good specificity and affirms the effectiveness of the fingerprint-based authentication mode based on the physical layer.
- The recognition results for some test samples are concentrated on a few labels. Possible reasons for this could include close similarity in the registered fingerprints of these labels' corresponding nodes or an impact of noise on the test samples.

The overall accuracy of the test set is 89.10%. Precision, recall and F1 score under micro-average, macro-average, and weighted average conditions are calculated as shown in Table II, where "Support" represents the number of test samples used in calculating the evaluation metrics. Due to the imbalance in sample distribution, the results based on the weighted average (where the proportion of each class's sample is used as a weight in computing metrics) generally provide a more fair reflection of the test results. Under the weighted average condition, those metrics maintain good results, further validating the specificity of the selected device fingerprints and the effectiveness of the fingerprint database authentication mechanism.

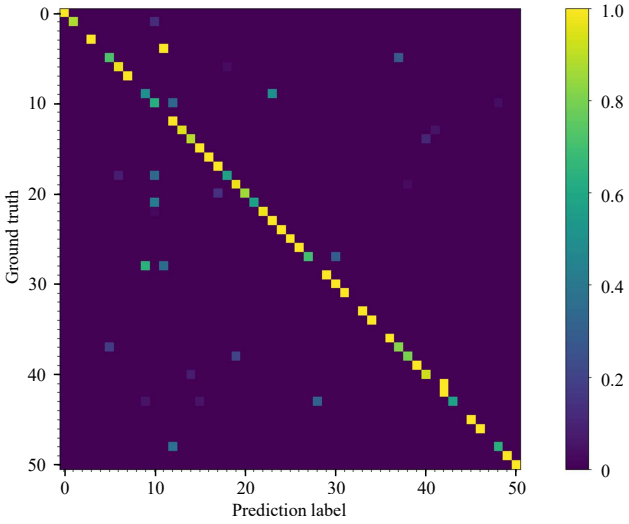

Fig. 4. Normalized confusion matrix in test set.

TABLE II
EVALUATION METRICS FOR IDENTIFICATION RESULTS IN TEST SETS

	Precision	Recall	F1-score	Support
micro avg	0.89	0.89	0.89	1046
macro avg	0.72	0.72	0.71	1046
weighted avg	0.90	0.89	0.89	1046

V. CONCLUSION

In this paper, we propose the FingerBLE, a BLE device authentication scheme based on physical layer device fingerprints. We utilize the Joint Estimation Algorithm to extract the parameter CFO and I-phase offset, which serve as device fingerprints. In the prototype design of the authentication system, FingerBLE employs a fingerprint database authentication mechanism, enabling node recognition and verification of legitimacy. Experimental results demonstrate that FingerBLE can effectively extract corresponding device fingerprints and achieve high accuracy in node identification. Using the inherent uniqueness and specificity of device fingerprints at the physical level, FingerBLE offers an effective solution to the issue of device cloning in IIoT networks.

ACKNOWLEDGMENT

The findings of this paper benefit from the work [16] published in 2022. We acknowledge the valuable insights and contributions of its authors. This work is supported in part by the National Key R&D Program of China under grant No. 2021YFB2900100, the National Natural Science Foundation of China (NSFC) under grants No. 62302259.

REFERENCES

[1] Mustafizur R. Shahid, Gregory Blanc, Zonghua Zhang, and Hervé Debar. Anomalous communications detection in iot networks using sparse autoencoders. In *2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*, pages 1–5, 2019.

[2] Adrian Şendroiu and Vladimir Diaconescu. Hide'n'seek: an adaptive peer-to-peer iot botnet. *architecture*, 3:5, 2018.

[3] Junjie Yin, Zheng Yang, Hao Cao, Tongtong Liu, Zimu Zhou, and Chenshu Wu. A survey on bluetooth 5.0 and mesh: New milestones of iot. *ACM Transactions on Sensor Networks (TOSN)*, 15(3):1–29, 2019.

[4] NCC Group. Tesla bluetooth hack opens doors and start cars. Website, 2022.

[5] Wanjuan Xie, Junhua Yu, and Guoqiang Deng. A network access control scheme for iot terminals based on active scanning. In *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, pages 47–51, 2022.

[6] Shikhar Verma, Yuichi Kawamoto, and Nei Kato. A network-aware internet-wide scan for security maximization of ipv6-enabled wlan iot devices. *IEEE Internet of Things Journal*, 8(10):8411–8422, 2021.

[7] Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. N-baiot—network-based detection of iot botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, 17(3):12–22, 2018.

[8] Tian Wang, Guangxue Zhang, Anfeng Liu, Md Zakirul Alam Bhuiyan, and Qun Jin. A secure iot service architecture with an efficient balance dynamics based on cloud and edge computing. *IEEE Internet of Things Journal*, 6(3):4831–4843, 2019.

[9] H. Liu C. Shi, J. Liu and Y. Chen. Smart user authentication through actuation of daily activities leveraging wifi-enabled iot. In *18th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, pages 1–10, 2017.

[10] Mete Ozay, Iñaki Esnaola, Fatos Tunay Yarman Vural, Sanjeev R. Kulkarni, and H. Vincent Poor. Machine learning methods for attack detection in the smart grid. *IEEE Transactions on Neural Networks and Learning Systems*, 27(8):1773–1786, 2016.

[11] Liang Xiao, Qiben Yan, Wenjing Lou, Guiquan Chen, and Y. Thomas Hou. Proximity-based security techniques for mobile users in wireless networks. *IEEE Transactions on Information Forensics and Security*, 8(12):2089–2100, 2013.

[12] Joseph R Rose, Matthew Swann, Gueltoum Bendiab, Stavros Shiaeles, and Nicholas Kolokotronis. Intrusion detection using network traffic profiling and machine learning for iot. In *2021 IEEE 7th International Conference on Network Softwarization (NetSoft)*, pages 409–415, 2021.

[13] Pankaj Thorat, Niraj Kumar Dubey, Kunal Khetan, and Rajesh Challa. Sdn-based predictive alarm manager for security attacks detection at the iot gateways. In *2021 IEEE 18th Annual Consumer Communications Networking Conference (CCNC)*, pages 1–2, 2021.

[14] Tianbo Gu and Prasant Mohapatra. Bf-iot: Securing the iot networks via fingerprinting-based device authentication. In *2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pages 254–262, 2018.

[15] Mohammad Wazid, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Mauro Conti, and Minho Jo. Design of secure user authenticated key management protocol for generic iot networks. *IEEE Internet of Things Journal*, 5(1):269–282, 2018.

[16] Hadi Givehchian, Nishant Bhaskar, Eliana Rodriguez Herrera, Héctor Rodrigo López Soto, Christian Dameff, Dinesh Bharadia, and Aaron Schulman. Evaluating physical-layer ble location tracking attacks on mobile devices. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1690–1704, 2022.

[17] Vladimir Brik, Suman Banerjee, Marco Gruteser, and Sangho Oh. Wireless device identification with radiometric signatures. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 116–127, 2008.

[18] KÖSE Memduh, Selçuk TAŞCIOĞLU, and Ziya TELATAR. Wireless device identification using descriptive statistics. *Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering*, 57(1):1–10, 2015.

[19] Tien Dang Vo-Huu, Triet Dang Vo-Huu, and Guevara Noubir. Fingerprinting wi-fi devices using software defined radios. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 3–14, 2016.