Navigating the Trilemma: Security, Power, and Performance Trade-offs in Bluetooth Low Energy

***Abstract*—Over recent years, Bluetooth Low Energy (BLE) has found widespread applications in various sectors, including medical devices, smart home technologies, IoT sensors, and wearables. Despite its popularity driven by low power consumption, its security requirements have remained a critical concern. This study conducts a comprehensive examination on BLE security, assessing the effects of different security levels on power efficiency and performance in real-world scenarios. Unlike previous studies which often concentrate on singular aspects of security, power efficiency, or performance, our research adopts a holistic approach by incorporating these factors simultaneously. We bridge this gap by thoroughly exploring the interplay between these critical factors, offering insights into the trade-offs involved and conducting a comprehensive analysis of the cost of security in relation to power efficiency and transmission performance. We evaluate BLE's power consumption under realistic conditions and quantify the cost of security on perspectives of energy and transmission speed. The experimental results indicate that security settings can impact both energy consumption and performance. Moreover, our findings reveal that higher-performance protocol configurations can paradoxically lead to reduced energy consumption. This highlights the paramount importance of the security-power-performance trade-off in BLE protocol design.**

***Index Terms*—Bluetooth Low Energy, IoT, Power Consumption, Performance, Security.**

I. Introduction

The rapid expansion of Internet of Things (IoT) devices has increased the demand for energy-efficient and secure wireless communication technologies. Bluetooth Low Energy (BLE) has become a key solution due to its low power consumption, widespread adoption, and suitability for resource-constrained IoT applications. From smart home automation and wearable health monitors to industrial sensors and asset tracking, BLE enables seamless and continuous data exchange. However, BLE devices must navigate a fundamental trilemma between power efficiency, transmission performance, and security. While higher security settings protect against emerging threats such as man-in-the-middle (MITM) attacks and key recovery exploits, they often come at the cost of increased power consumption and reduced transmission speed. Similarly, optimizing performance for faster data transmission can lead to higher energy demands, impacting battery life in low-power IoT systems [1], [2].

In recent years, BLE technology has received significant attention in performance evaluation and power management. In particular, BLE was initially developed as a low-power alternative to traditional Bluetooth, addressing the specific requirements in resource-limited platforms [3]. The heightened interest in recent research on BLE stems from the essential need to optimize the performance and power efficiency of BLE-enabled devices to meet the demands of diverse IoT ecosystems. Extensive research efforts have been dedicated to evaluating the performance characteristics [4], [5], measuring power consumption [6], [7] and optimization [8], [9].

Furthermore, along with the application of BLE technology in more sensitive fields, such as medical devices, smart home control and industrial sensors, security emerges as a critical design concern [10]. Indeed, a myriad of security threats has surfaced, highlighting the vulnerability of BLE communication to malicious attacks. For instance, attacks targeting key recovery pose a risk to the confidentiality of data exchanged over BLE connections [11], [12]. Vulnerabilities enabling bypassing of authentication mechanisms can lead to unauthorized access and potential compromise of IoT devices [13]. To address security challenges in IoT, recent research has explored different lightweight security mechanisms [2], [14]–[16]. However, the impact of security defense strategies on power consumption and performance remains largely unexplored. To the best of our knowledge, there has been a notable absence of analysis and modeling studies regarding the comprehensive examination of the costs associated with various security features in BLE-enabled devices.

While considering the performance aspect, recent studies such as [17]–[19] have focused on direction determination, or Neighbor Discovery Process (NDP) [5], [20], leaving the general transmission performance during the connection interval largely unexplored. Although the theoretical maximum data throughput has been reported as 1.4 Mbps [21], real-world application scenarios often struggle to reach this peak speed. For instance, recent empirical studies, such as that conducted by Badihi et al. [4], have measured a maximum data throughput of only 341 Kbps, significantly lower than the theoretical limit. While the low data throughput is commonly attributed to factors like low signal strength or quality, other contributing factors have yet to be thoroughly explored. Despite advancements, the existing gap highlights the need for a comprehensive evaluation of BLE security mechanisms, examining their trade-offs with power efficiency and system performance to inform the design of optimized and resilient IoT solutions.

In this work, our primary objective is to *navigate the BLE Trilemma* and *thoroughly analyze the intricate interplay among security, power, and performance within the BLE protocol*, with an emphasis on the associated costs of security mechanisms. Unlike prior studies that often address these factors in isolation, our research takes a holistic approach, systematically evaluating their interactions under real-world conditions. By quantifying the impact of security on energy consumption and transmission speed, our findings offer key insights into optimizing BLE

protocol configurations to balance security and efficiency in IoT applications.

Our main contributions are outlined as follows:

- We conduct a comprehensive evaluation of the power consumption incurred by specific security features in a practical wearable device platform, thereby establishing a direct correlation between BLE security and power usage.
- Through systematic assessment of how different security-related protocol parameters affect the transmission speed, we establish a clear correlation between BLE security and performance.
- We examine the impact of performance-related parameters on power consumption, bridging the gap between power efficiency and performance optimization.
- We identify an optimal combination of security levels and transmission parameters from the perspective of power efficiency in BLE-enabled devices. Furthermore, considering the varied contexts in which BLE technology is deployed, we propose several combinations that strike a balanced trade-off, effectively meeting multiple requirements simultaneously.

The remainder of this paper is organized as follows. Section II provides a background introduction to BLE and presents related works. Our experiment settings are outlined in Section III. Section IV presents the evaluation results and findings. Subsequently, Section V concludes the paper.

II. Background and Related Studies

In this section, we present a discussion regarding current studies and related BLE background that will be used in the following sections.

A. Related Studies

The Internet of Things has become an integral part of modern technology, enabling seamless connectivity across diverse applications such as healthcare, smart homes, and industrial automation. Given its widespread adoption, ensuring security in IoT systems has been a major research focus, with numerous studies exploring lightweight security mechanisms tailored for IoT and resource-constrained devices [14]–[16], [22]–[28]. While significant progress has been made in securing IoT across various computing layers, the security of Bluetooth Low Energy, a key wireless communication protocol in IoT, along with its impact on power consumption and performance trade-offs, remains understudied.

In recent years, there has been considerable research focused on different aspects of BLE technology, particularly with respect to security, performance, and power consumption. Studies on BLE security have primarily addressed vulnerabilities and attack vectors, particularly in older BLE versions. [29], [30] highlights the susceptibility of BLE to attacks such as eavesdropping, key negotiation downgrades, and man-in-the-middle (MITM) attacks, and efforts have been made to mitigate these threats, particularly through the introduction of new security mechanisms, like Secure Connections in BLE 4.2 and BLE 5.0, which use stronger encryption algorithms.

Research	Security	Power	Performance	Interplay	Measurement
[29]	✓				
[30]	✓				
[6]			✓		✓
[31]			✓		✓
[17]			✓		
[32]			✓		
This Research	✓		✓		✓

TABLE I: Comparison of our study with state-of-the-art BLE research

Similarly, power consumption has been a central theme in BLE research, especially within the context of IoT devices, where energy efficiency is paramount. Studies such as [6], [31] focus on calculating energy usage across different operating modes, providing comparatively precise BLE power consumption estimation and valuable insights for optimizing battery life. However, these works tend to ignore the security mechanisms introduced by the BLE protocol and overlook the trade-offs between energy consumption and data transmission.

Performance evaluations have also garnered attention, particularly in the context of throughput, latency, and maximum reachability of BLE devices. Recent research [17], [32] on data transmission efficiency emphasizes the impact of connection intervals on throughput and energy consumption. While these findings are useful, they fail to integrate considerations of security settings, which could potentially alter transmission speed and device power consumption under real-world conditions.

Unlike previous studies that focus on isolated aspects of BLE technology, our work takes a comprehensive approach by examining the intricate interplay between security, power, and performance within the BLE protocol. Table I highlights the specific focus areas of existing research, emphasizing the uniqueness of our study in providing a holistic analysis of security, power, and performance trade-offs in BLE.

B. Terminology and Key Concepts

To facilitate a clearer understanding of the security-power-performance trade-offs in Bluetooth Low Energy systems, this section defines key parameters that influence data transmission, power consumption, and security. These concepts form the foundation of our experimental setup and analysis.

BLE operates using a structured communication model where devices exchange data periodically. One of the most important parameters governing this exchange is the *Connection Interval (CI)*, which defines the time between two consecutive data exchanges, known as connection events, between a BLE peripheral and a central device. This interval is measured in milliseconds (ms) and typically ranges from 7.5 ms (fastest) to 4,000 ms (slowest). A shorter connection interval leads to more frequent communication, resulting in higher throughput at the cost of increased power consumption. Conversely, a longer connection interval reduces the frequency of data exchange, thereby conserving energy but introducing higher latency.

Another critical parameter is the *GAP (Generic Attribute Profile) Data Length*, which determines the maximum size of a single BLE data packet. This value typically ranges from 27

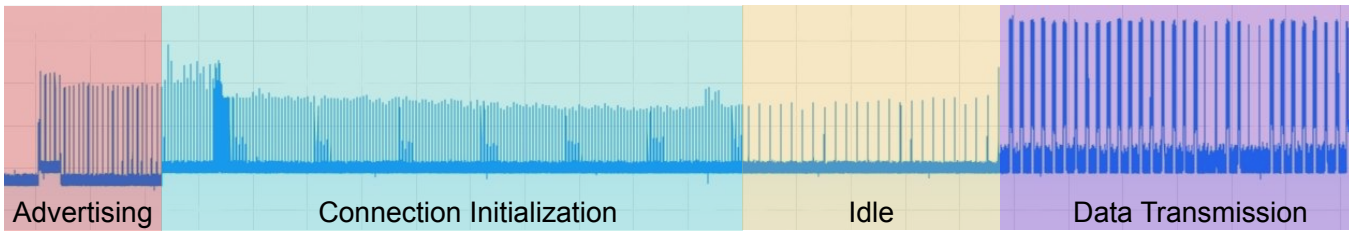


Fig. 1: Diagram of different stages of a BLE connection process.

bytes (minimum) to 251 bytes (default in BLE 5.0 and later). A larger data length allows more data to be transmitted in a single packet, reducing the overhead associated with multiple transmissions. While this improves transmission efficiency, it may lead to higher power consumption and time cost per packet due to the increased computational load on the BLE device.

Furthermore, the *GAP Event Length* defines the duration for which the BLE device remains active within each connection interval. If the event length is too short, the device may not have enough time to complete data transmission before entering an idle state, reducing efficiency. A longer event length allows for the transmission of larger amounts of data per connection event but increases the overall power consumption. The balance between these factors plays a crucial role in optimizing BLE power efficiency while maintaining reliable data transmission.

III. Proposed Methodology

In this section, we present details of our proposed methodology for security, power, and performance trade-off analysis in BLE-enabled devices. To comprehensively evaluate the power consumption of data transmission on a realistic platform, we conduct a series of experiments using different BLE security and performance settings. These experiments can be categorized to different parts: assessing the power-performance trade-off, evaluating the performance cost for security policies, and analyzing the power cost for security policies. In this work, we strictly define performance as the data transmission throughput (or transmission speed), and security as the different possible combinations of encryption and authentication policies.

A. Experiment Settings

Our experiments are conducted using a Nordic `nRF52840` [21]. This is a System-on-Chip (SoC) designed specifically for executing applications related to communication protocols like BLE and Bluetooth Mesh. This SoC features a 32-bit ARM Cortex-M4 processor with a floating point unit (FPU), supporting a maximum frequency of 64 MHz. We utilize Bluetooth 5.1 in our experiments, employing the LE 2M (low-energy, 2Mbit/s throughput) as the PHY mode. We use the IoT Power CC device [33] to perform power measurement. These experimental settings are summarized in Table II.

When measuring the actual power consumption, the result should be consistent and accurate. To verify whether the result we collect is consistent, multiple measurements were executed. If all measurements remain in a small range, then we know our results are consistent. For accuracy, since BLE protocols can be carried by various chips and formats, our experiments cannot lead to a generally applicable value. Therefore, our results would serve as a trend comparison of various operating modes.

Moreover, to guarantee the collected results are consistent and accurate, we either try to slice from the relatively same starting point or slice a long range measurement during the data transmission stage to minimize the noise. For example, in the connection initialization stage, there are always patterns present at the beginning and the end of the stage. For each measurement, we only slice the results in between these patterns to keep the consistency.

Control Variable	Set Value
Physical Layer mode	LE 2M
BLE version	Bluetooth 5.1 qualified [34]
Hardware	Nordic `nRF52840` [21]
Power Measurement Device	IoT Power CC [33]

TABLE II: Control Variables for Performance

B. BLE Security Configurations

Security in BLE communications is governed by encryption and authentication mechanisms that protect data integrity and prevent unauthorized access. In this study, we examine three security configurations that represent different levels of protection.

- C1 Just-Works paring, where encryption/decryption or authentication is not involved.
- C2 Encryption with unauthenticated pairing, selected to evaluate only the transmission events occurring within the connection interval.
- C3 Passkey bonding pairing, which requires a password during the connection initiation stage, incorporating the influence of authentication.

The first configuration, **C1**, represents a baseline scenario where no encryption or authentication is applied, commonly referred to as the ”Just-Works” pairing. In this setting, devices establish a connection without exchanging secure keys, making it vulnerable to eavesdropping and man-in-the-middle (MITM) attacks. Due to the lack of encryption overhead, this configuration provides the highest transmission speed and the lowest power consumption. However, it is only suitable for low-risk

applications where security is not a primary concern, such as simple environmental sensors.

The second configuration, **C2**, incorporates encryption but does not require authentication during pairing. This means that the transmitted data is encrypted using Legacy Pairing, providing a basic level of security against passive eavesdropping. However, without authentication, an attacker could potentially intercept the key exchange process, leading to compromised security, like MITM attacks. This configuration is commonly used in standard BLE applications where encryption is needed but strict authentication is not required, such as fitness trackers and smart home devices.

The third and most secure configuration, **C3**, implements both encryption and authentication through passkey bonding. In this setting, a passkey must be exchanged between devices before a connection is established, significantly reducing the risk of MITM attacks. This configuration ensures a higher level of security but introduces additional computational overhead, leading to increased power consumption and a reduction in transmission speed. This configuration is typically used in security-sensitive applications such as medical devices, financial transactions, and enterprise authentication systems where unauthorized access must be strictly prevented.

C. Performance Configuration

The selected BLE performance configurations, P1 to P4, represent a spectrum of trade-offs between power efficiency and data transmission speed, covering both low-power and high-performance applications.

P1 is designed for ultra-low-power applications like environmental sensors, where energy conservation is critical, using long connection intervals (400 ms) and small packets to minimize power consumption. **P2** balances power and speed for devices like wearable and smart home systems, reducing the connection interval (200 ms) while increasing packet size.

P3 represents a performance-driven but energy-conscious setting for applications like health monitoring and industrial sensors, using 100 ms intervals and large packet sizes to ensure efficient data exchange. Finally, **P4** is optimized for latency-sensitive applications like real-time streaming, minimizing the connection interval (30 ms) and maximizing data throughput at the cost of higher power usage.

	Connection Interval	GAP Length	GATT Data Length	GAP Event Length
P1 (Slowest)	400 ms	27	23	7.5 ms
P2 (Slow)	200 ms	107	103	10 ms
P3 (Fast)	100 ms	207	203	20 ms
P4 (Fastest)	30 ms	251	247	30 ms

TABLE III: Performance settings

D. Experiment Design and Tradeoffs

1) Power vs. Performance: In this section, we aim to investigate the relationship between power consumption and transmission performance in BLE. We begin by verifying that our proposed performance configurations (P1-P4) directly influence transmission speed. To accomplish this, we measure the transmission speed under configurations P1-P4, with security configured to C1 (no security) and compare the distribution of transmission speeds. Subsequently, we collect both average power and accumulative energy consumption under P1-P4 and compare the results to establish the connections between power and performance.

2) Performance vs. Security: To evaluate the impact of security on performance, we first conduct experiments to measure the transmission speeds under different security settings (C1-C3). We select P3 and P4 as our performance configurations. This experiment design enables us to: (1) Evaluate the impact of security settings on performance; (2) Determine if the impact is consistent across different performance configurations. We then configure security to C2 and change the key lengths to examine the impact on performance.

As shown in Figure 1 , the encryption process occurs during the pre-processing stage. When the encryption process lengthens due to the inclusion of encryption and authentication operations or extended key length, the remaining stages could potentially be compressed, resulting in a shorter transmission period, hence causing the performance to drop. Our proposed set of experiments and trade-off considerations aims to verify this assumption.

3) Power vs. Security: Evaluating the impact of security on power consumption requires an analysis of both the connection initialization and data exchange stages. To precisely measure the power consumed by security configurations, we maintain consistency in performance by using the same configuration, namely P3, across all experiments. This ensures uniformity in performance and allows for a direct comparison of power consumption during data transmission operations. Therefore, the measured total power consumption can be leveraged to present how much extra power would be consumed by security configurations. We utilize this method to measure both energy consumption and average power of security configurations during both connection initialization and data exchange stages.

Furthermore, for data exchange stage, we employ C1 (no security) as the baseline to quantify the additional power consumption attributed to other security settings (C2, C3). Since both C2 and C3 can encrypt transmitted data, we specifically select C2 with varying key lengths (7 and 16 bytes) to evaluate the impact on power consumption. This experiment design enhances our understanding of the cost of security and enables observation for the additional power consumed.

During the connection initialization stage, the security protocol specifies the pairing or bonding method and the key for subsequent encryption. While power consumption during this stage is minimal as these operations are executed only once throughout the entire connection process, it is crucial to consider that certain peripheral devices may need to report frequently to various host devices. Over time, the accumulation of these operations could lead to significant power consumption. At the data exchange stage, the security protocol consumes additional power for encryption operations. Our experimental analysis and results will provide insights into the impact of security on power consumption, aiding in the evaluation and

optimization of BLE systems.

IV. Evaluation and Discussion

In this section, we present our evaluation results using the described methodology and experiment settings. We delve into our findings, offering detailed insights into the interplay between security configurations, power consumption, and performance in BLE-enabled devices.

A. Power vs. Performance

We first measure the actual transmission speed under the four performance settings (P1-P4) outlined in Section III. Figure 2 demonstrates the substantial impact of our selected parameter sets (P1-P4) on transmission speed, with P1 being the slowest (∼320 Bytes/s) and P4 being the fastest (over 1Mb/s, approaching the theoretical limit). This verifies the effectiveness of the chosen protocol parameter sets in precisely controlling transmission speed in BLE.

Figure 3a illustrates the total energy consumption required to transmit 122,000 bytes of data across different performance configurations. A surprising finding from this experiment is that slower transmission speeds do not necessarily lead to lower energy consumption. In fact, the slowest configuration (P1) consumes significantly more energy than the higher-performance configurations (P2-P4), with the fastest configuration (P4) using the least energy overall.

The reason for this trend becomes clearer when considering average power consumption, as shown in Figure 3b. As the transmission speed increases from P1 to P4, the average power also rises. However, the total energy consumption decreases because higher-speed configurations complete data transmission in a much shorter time, reducing the duration for which power is drawn. This finding holds true in scenarios where a large amount of data needs to be sent as quickly as possible.

In real-world IoT applications, however, devices often do not generate such large amounts of data in a short time. If the same amount of data were spread over a longer period, the average power consumption shown in Figure 3b would better reflect the power efficiency of each configuration. In this case, higher-performance configurations would consume significantly more energy over time compared to slower configurations.

Finding 1: The transmission speed can be directly controlled by our proposed protocol parameter sets. When transmitting a large amount of data in a short period, higher-performance configurations can be more energy-efficient due to the reduced transmission duration. However, for typical IoT applications that transmit data intermittently, lower-performance configurations may be more power-efficient over time.

Thus, while high-speed configurations can be more energy-efficient for large data transmissions, they may not be the best choice for typical IoT applications that transmit data intermittently. For such cases, a lower-performance configuration should be selected to optimize power efficiency.

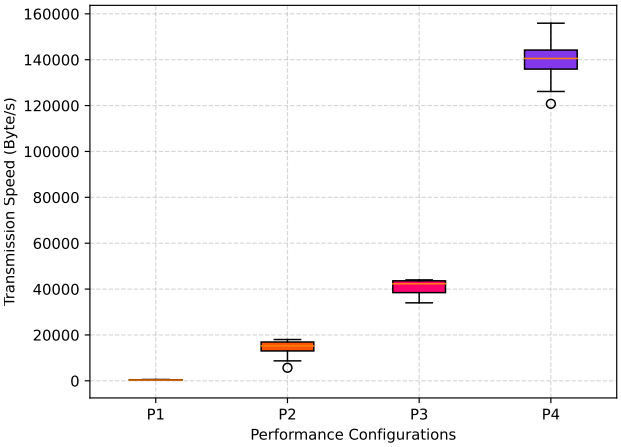
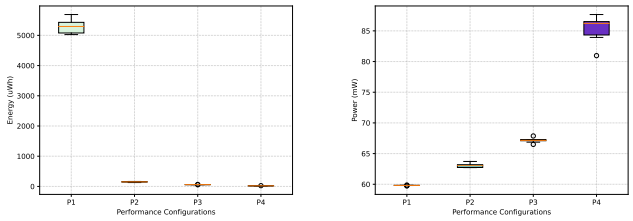


Fig. 2: Measured transmission performance under configurations P1-P4.



(a) Measured energy consumption under different performance settings.

(b) Measured average power under different performance settings.

Fig. 3: Energy and power data during data transmission under different performance configurations.

By examining Table III, one can observe that transmission speeds are determined by (1) Connection Interval (i.e. how often the BLE device connects to the host); (2) GAP Length and GATT Data Length (i.e. size of each data packet); and (3) GAP Event Length (i.e. the active time within each connection interval).

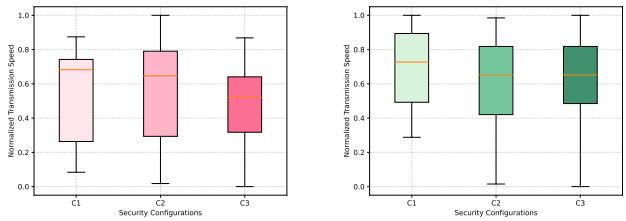
Lower speed is obtained by setting a longer Connection Interval, shorter packet length and shorter active time, which result in the device to be in Idle status more frequently. Transmitting at a lower speed will hence cause the device to spend more time idling. Assuming the energy consumption of sending the same amount of data is the same, since staying in Idle status also consumes energy, the total energy consumption will be higher.

B. Performance vs. Security

In Figure 4, we present the measured transmission performance. Figure 4a depicts the distribution of measured transmission rates under performance configuration P4 (Fastest), while Figure 4b shows results under a slower performance configuration (P3, Fast). Examining Figure 4a and Figure 4b, it is observed that applying encryption during the data transmission stage influences BLE performance.

The transmission speed shows a slight decrease as the security configuration changes from C1 to C2 and C3. Moreover, comparing Figure 4a and Figure 4b, we observe that the drop in the transmission speed is related to the base speed determined by the configuration. When we use a higher performance configuration P4, the transmission speed tends to drop more compared with a slower configuration P3. Based on our measurement, the performance drops 36% more when applying configuration P4.

We attribute this phenomenon to the competition between the transmission and security. As outlined in the previous section, in a standard BLE connection session, there's a limitation on the duration each device can remain active. Therefore, during a single transmission session, as the security level increases, the peripheral device may spend more time in the pre-processing stage due to encryption requirements, leaving less time for data transmission. As a result, applying a security configuration that requires encryption introduces time competition, reducing the number of transmitted data packets and ultimately decreasing performance.



(a) Measured transmission performance under configuration P4. (b) Measured transmission performance under configuration P3.

Fig. 4: Measured transmission performance.

Furthermore, we conduct an experiment to examine how encryption key length affects performance and to validate our previous explanation. Intuitively, a longer key would cause a longer encryption stage. Due to the competition between pre-processing and data transmission in an active period, the BLE device will have less time to transmit data packets, resulting in decreased performance.

As shown in Figure 5, we can see that the transmission rate decreases when the key length increases, which matches our prediction. When using a key length of 16 bytes, the mean transmission speed drops 7 kB/s, compared to a 7-byte key. Given the cost of performance, it might be more efficient to use a shorter key and frequently change it in certain circumstances.

Finding 2: Higher security levels negatively impact performance, as the additional encryption stages compete with the data transmission stage during an active period. This effect is more pronounced when BLE devices operate under a high-performance configuration.

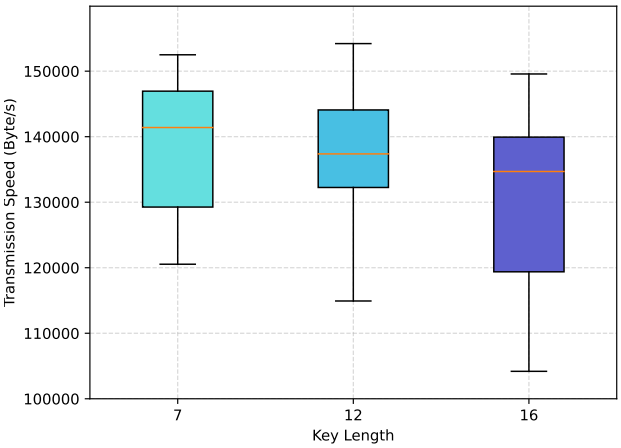
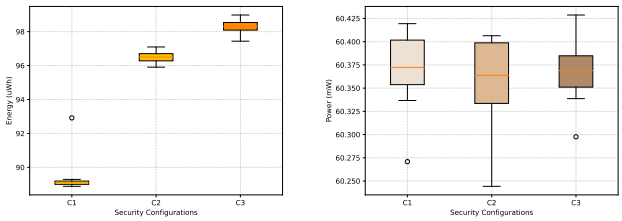


Fig. 5: Measured transmission performance under different key length configurations.

C. Power vs. Security

We further examine power, another important cost factor of security. Figure 6 depicts the energy consumption data of the connection initialization period, in which the central device and peripheral device pair, exchange encryption keys and other connection parameters. From Figure 6, a significant difference between the power consumption can be observed. In Figure 6a, the energy consumption significantly increases from C1 (i.e. no security policies enforced) to C3 (i.e. both encryption and authentication enforced).

However, due to the extended time brought by encryption and authentication, along with the periodic idle status of BLE devices, the average power measurements of the three configurations are similar, as shown in Figure 6b. One noteworthy observation is that our evaluation results tend to represent lower bounds in real-world scenarios. In our measurement, we simulate the key input and automate the pairing acceptance. However, in wearable device scenarios, due to the slower human-interfered authentication steps like keyboard passkey input, the total power consumption would be higher.



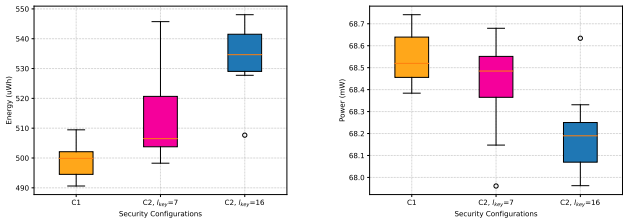
(a) Measured energy consumption. (b) Measured average power.

Fig. 6: Energy and power data during connection initialization.

Figure 7 shows the power consumption measurement of the data exchange process. In this experiment, we keep consistent performance and total transmitted data size settings to enforce

an identical number of connection intervals. Thus, any differences in energy consumption across measurements are solely attributed to the encryption steps.

Figure 7a shows that higher security levels consume more power. However, as shown in Figure 7b, the averaged power decreases. This occurs because, compared to data transmission, encryption consumes less power, as shown in Figure 1. Higher security levels will cause the BLE device to spend more time on the pre-processing stage in each active cycle, causing the average power to decrease.



(a) Measured energy consumption. (b) Measured average power.

Fig. 7: Energy and power data during data transmission.

Finding 3: Security configurations can slightly impact the total consumed energy both during connection initiation and data transmission. During the connection initialization, additional security-related operations lead to an increase in the total energy consumption to increase. Moreover, these operations contribute to higher energy consumption during data transmission. However, as the less energy-intensive pre-processing steps occupy larger portion of each active cycle, the average power reduces as security levels increase.

D. Discussion on Design Choices

Our findings provide valuable insights into robust and efficient design choices of BLE protocols. In terms of the power-performance trade-off, if energy and power are paramount considerations, users only need to configure the protocol to operate at maximum speed which increases the energy efficiency of data transmission. However, this approach may lead to power spikes, and in a certain circumstance, a less aggressive protocol setting may be more suitable.

When considering the security-performance trade-off, users need to assess whether the increased security level justifies the resulting performance reduction, especially when the protocol is configured to run at a higher data transmission speed. Furthermore, it is notable that the security configurations can influence power consumption in both connection initialization and data transmission stages. It is essential to calculate whether the increased energy consumption resulting from improved security is worthwhile, especially in power-constraint IoT devices.

Future efforts should focus on developing software and hardware solutions aimed at enhancing the power efficiency of security mechanisms in BLEs while minimizing the performance overhead. This includes, but is not limited to: (1) Performance engineering to fine-tune encryption/decryption software libraries for optimal efficiency. (2) Integration of heterogeneous hardware components, such as ASIC accelerators, to streamline security and communication operations within these systems.

V. Conclusion and Future Work

In this paper, we perform a comprehensive evaluation of energy consumption and transmission speeds under varying security and performance configurations within the Bluetooth Low Energy (BLE) protocol. Our findings shed light on the intricate relationships and importance of considering balanced trade-offs among security, power, and performance requirements within the BLE ecosystem. Notably, we observe that security settings within the BLE protocol can exert a significant impact on both performance and energy efficiency. Additionally, we uncover a counter-intuitive finding wherein more aggressively performant protocol configurations can paradoxically lead to lower energy consumption.

Overall, our experimental results highlight the paramount importance of the security-power-performance trade-offs consideration. Consequently, striking an optimal balance among security, power efficiency, and performance emerges as the key consideration in designing a high performance, robust, and cost-efficient BLE system. Future work will expand the power analysis into a comprehensive characterization by systematically quantifying BLE power consumption across various configurations. Additionally, we will develop machine learning-based power prediction models to enable real-time power estimation, facilitating dynamic optimization of BLE settings for enhanced energy-efficiency.

References

[1] A. Nikoukar, S. Raza, A. Poole, M. Güneş, and B. Dezfouli, "Low-power wireless for the internet of things: Standards and applications," *IEEE Access*, vol. 6, pp. 67893–67926, 2018.

[2] S. M. P. Dinakarrao, X. Guo, H. Sayadi, C. Nowzari, A. Sasan, S. Rafatirad, L. Zhao, and H. Homayoun, "Cognitive and scalable technique for securing iot networks against malware epidemics," *IEEE Access*, vol. 8, pp. 138508–138528, 2020.

[3] B. S. I. Group, "Bluetooth core specifications 4.0," 2010.

[4] B. Badihi, M. U. Sheikh, K. Ruttik, and R. Jäntti, "On performance evaluation of ble 5 in indoor environment: An experimental study," in *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–5, IEEE, 2020.

[5] B. Luo, Y. Yao, and Z. Sun, "Performance analysis models of ble neighbor discovery: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8734–8746, 2020.

[6] P. H. Kindt, D. Yunge, R. Diemer, and S. Chakraborty, "Energy modeling for the bluetooth low energy protocol," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 19, no. 2, pp. 1–32, 2020.

[7] J. J. Treurniet, C. Sarkar, R. V. Prasad, and W. De Boer, "Energy consumption and latency in ble devices under mutual interference: An experimental study," in *2015 3rd International Conference on Future Internet of Things and Cloud*, pp. 333–340, IEEE, 2015.

[8] M. Dodangeh, M. S. O. Alink, and B. Nauta, "Quantifying the trade-off between latency and power consumption in bluetooth low energy and its mitigation by using a wake-up receiver," in *2022 IEEE 8th World Forum on Internet of Things (WF-IoT)*, pp. 1–8, IEEE, 2022.

[9] M. J. Chaudhry, S. Murawwat, F. Saleemi, S. Tariq, M. Saleemi, and F. J. Chaudhry, "Power optimized secure bluetooth communication," in *2008 IEEE International Multitopic Conference*, pp. 182–188, IEEE, 2008.

[10] J. Wu, R. Wu, D. Xu, D. Tian, and A. Bianchi, "Sok: The long journey of exploiting and defending the legacy of king harald bluetooth," in *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 23–23, IEEE Computer Society, 2023.

[11] D. Antonioli, N. O. Tippenhauer, and K. B. Rasmussen, "The {KNOB} is broken: Exploiting low entropy in the encryption key negotiation of bluetooth {BR/EDR}," in *28th USENIX security symposium (USENIX security 19)*, pp. 1047–1061, 2019.

[12] D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "Key negotiation downgrade attacks on bluetooth and bluetooth low energy," *ACM Transactions on Privacy and Security (TOPS)*, vol. 23, no. 3, pp. 1–28, 2020.

[13] D. Antonioli, N. O. Tippenhauer, and K. Rasmussen, "Bias: Bluetooth impersonation attacks," in *2020 IEEE symposium on security and privacy (SP)*, pp. 549–562, IEEE, 2020.

[14] S. M. P. Dinakarrao, H. Sayadi, H. M. Makrani, C. Nowzari, S. Rafatirad, and H. Homayoun, "Lightweight node-level malware detection and network-level malware confinement in iot networks," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 776–781, IEEE, 2019.

[15] V. A. Thakor, M. A. Razzaque, and M. R. Khandaker, "Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28177–28193, 2021.

[16] J. Hwang, G. Kale, P. P. Patel, R. Vishwakarma, M. Aliasgari, A. Hedayatipour, A. Rezaei, and H. Sayadi, "Machine learning in chaos-based encryption: Theory, implementations, and applications," *IEEE Access*, vol. 11, pp. 125749–125767, 2023.

[17] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, and D. Formica, "Performance evaluation of bluetooth low energy: A systematic review," *Sensors*, vol. 17, no. 12, p. 2898, 2017.

[18] M. Qian, K. Zhao, A. Seneviratne, and B. Li, "Performance analysis of ble 5.1 new feature angle of arrival for relative positioning," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. 46, pp. 155–161, 2022.

[19] C. Huang, Y. Zhuang, H. Liu, J. Li, and W. Wang, "A performance evaluation framework for direction finding using ble aoa/aod receivers," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3331–3345, 2020.

[20] J. Siva, J. Yang, and C. Poellabauer, "Connection-less ble performance evaluation on smartphones," *Procedia Computer Science*, vol. 155, pp. 51–58, 2019.

[21] N. Semiconductor, "Bluetooth low energy data throughput," Accessed May 2024.

[22] H. Sayadi, H. M. Makrani, O. Randive, S. M. PD, S. Rafatirad, and H. Homayoun, "Customized machine learning-based hardware-assisted malware detection in embedded devices," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, pp. 1685–1688, IEEE, 2018.

[23] Z. Sheng, H. Wang, C. Yin, X. Hu, S. Yang, and V. C. Leung, "Lightweight management of resource-constrained sensor devices in internet of things," *IEEE internet of things journal*, vol. 2, no. 5, pp. 402–411, 2015.

[24] Z. He and H. Sayadi, "Image-based zero-day malware detection in iomt devices: A hybrid ai-enabled method," in *2023 24th International Symposium on Quality Electronic Design (ISQED)*, pp. 1–8, IEEE, 2023.

[25] H. Sayadi, Z. He, C. W. Fernandes, and T. Miari, "Cyber-immunity at the core: Securing biomedical devices through hardware-level machine learning defense," in *2023 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, pp. 1–5, IEEE, 2023.

[26] S. Yılmaz, E. Aydogan, and S. Sen, "A transfer learning approach for securing resource-constrained iot devices," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4405–4418, 2021.

[27] Z. He, H. Homayoun, and H. Sayadi, "Beyond conventional defenses: Proactive and adversarial-resilient hardware malware detection using deep reinforcement learning," in *Proceedings of the 61st ACM/IEEE Design Automation Conference*, pp. 1–6, 2024.

[28] H. Wang, H. Sayadi, S. M. P. Dinakarrao, A. Sasan, S. Rafatirad, and H. Homayoun, "Enabling micro ai for securing edge devices at hardware level," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 4, pp. 803–815, 2021.

[29] Y. Zhang, J. Weng, R. Dey, and X. Fu, *Bluetooth Low Energy (BLE) Security and Privacy*, pp. 1–. 10 2019.

[30] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain, "Security and privacy threats for bluetooth low energy in iot and wearable devices: A comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 251–281, 2022.

[31] P. Bulić, G. Kojek, and A. Biasizzo, "Data transmission efficiency in bluetooth low energy versions," *Sensors*, vol. 19, no. 17, p. 3746, 2019.

[32] H. Xu, Z. Yan, B. Li, and M. Yang, "Modelling and analysis of the performance for bluetooth low energy," *IEEE Communications Letters*, 2024.

[33] luatOS team, "Iot power power consumption test artifact." https://wiki.luatos.org/iotpower/index.html, Accessed May 2024.

[34] B. S. I. Group, "Bluetooth core specifications 5.1," 2019.