Adaptive Protection Against Energy Depletion Attacks in Wearable Medical Devices

Shakir Mehdiyev
Institute of Information Technology of MSERA, Baku, Azerbaijan
shakir.mehtieff@gmail.com

***Abstract*—Wearable medical devices (WMDs), such as pacemakers, insulin pumps, and other implantable systems, are critically dependent on battery charge, making them vulnerable to various energy depletion threats. This article examines the causes of energy loss, including cyberattacks targeting sensor, computational, and communication modules. Based on a comprehensive literature review, adaptive power management methods and an intrusion detection system are proposed to enhance the resilience of these devices. The findings highlight the urgent need for proactive strategies to ensure the energy security of WMDs in the face of increasing cyber-physical threats.**

Keywords—wearable medical devices, sensors, energy vulnerabilities, battery failures, cyberattacks, energy monitoring

I. INTRODUCTION

The increasing prevalence of chronic diseases and the rise in life expectancy are driving the widespread adoption of wearable medical devices (WMDs) for continuous monitoring of physiological parameters. These devices help ensure autonomy and quality of life for individuals with disabilities or chronic health conditions. In addition, wearable devices are actively used in industry to monitor the physical condition of workers in extreme conditions, such as in the mining industry, on oil platforms, and in other challenging environments [1-3].

To ensure autonomous operation of WMD sensor nodes, integrated chemical power sources (e.g., lithium-ion batteries) with limited power consumption capabilities are typically used. The use of power consumption vulnerabilities as an attack vector opens a new dimension of cyber threats, which requires comprehensive research and development of effective defense mechanisms.

This article analyzes the energy consumption vulnerabilities of WMDs, their impact on reliability, and the potential risks they pose. Based on a thorough literature review, it classifies various types of attacks — ranging from physical to network-based — and proposes optimization methods, including ultra-low-power components, data processing algorithms, and energy-efficient wireless technologies.

The research aims to enhance the resilience of such devices to failures and security threats amid the growing role of technology in modern healthcare.

II. LITERATURE REVIEW ON ENERGY CONSUMPTION VULNERABILITIES

A. Energy Optimization in Wearable Medical Devices

Current research efforts aim to reduce the energy consumption of WMDs through both software algorithm optimization and hardware-level solutions. However, despite notable advancements, unresolved issues persist, particularly regarding the vulnerability of such systems to external threats, including cyberattacks designed to drain their energy resources.

One fundamental area of focus in energy efficiency is the development of ultra-low-power sensors. In [4], sensors for heart rate monitoring are presented that consume less than 10 μW, enabling power supply lifespans of several months even under continuous operation. These devices employ low-voltage circuitry and optimized materials; however, the authors note an inevitable trade-off between measurement accuracy and power consumption. For instance, reducing the sampling rate to conserve energy can result in missed anomalies in ECG data, which is unacceptable in critical medical scenarios such as arrhythmia diagnosis in patients with heart failure.

An even more advanced solution is described in [5], where an ultra-low-power sensor based on laser-induced graphene on a flexible PDMS substrate was developed. This three-dimensional strain sensor, designed for human motion tracking, consumes only 5 μW. Its high sensitivity (GF ≈ 225.1) and linearity (R^2 = 0.99062) within a 0–22% strain range make it ideal for WMDs. However, the complexity of the readout circuit could become a vulnerability under intensive computational loads triggered by external factors.

Advanced signal processing algorithms are employed to reduce computational load. Reference [6] describes the use of Compressed Sensing (CS), which enables the reconstruction of physiological signals, such as pulse or glucose levels, from a reduced number of samples, decreasing the volume of transmitted data by 40–60% compared to traditional methods. This is particularly beneficial for WMDs operating over bandwidth-constrained networks. Adaptive filtering, including Kalman filtering as demonstrated in [7], eliminates noise and redundant calculations, reducing processing-related energy consumption by up to 30%, as confirmed through experiments with wearable pressure sensors. Wavelet transform techniques, discussed in [8], provide multiscale data analysis, allowing ECG or motion signals to be compressed with minimal loss of informational value, making them highly suitable for patient activity monitoring systems.

DOI: 10.25045/SPCDH4.0.2025.14

Energy-efficient communication protocols complement these approaches by optimizing data transmission in WMD networks. Clustering techniques, as implemented in protocols such as LEACH, HEED, and others [9], distribute the communication load among sensors by selecting relay nodes based on residual energy levels, reducing overall network energy consumption by 20–40% compared to direct transmission. Energy-aware routing strategies, described in [10], utilize load prediction algorithms for dynamic sensor switching, minimizing redundant traffic, and extending battery life. Data aggregation methods also discussed in [11] eliminate redundant information, reducing transmission volume by 25–35%, a crucial factor for WMDs operating under limited bandwidth conditions such as Bluetooth Low Energy (BLE).

A review of modern solutions for WMDs, including exoskeletons, confirms the relevance of the aforementioned methods. In [12], it is emphasized that lower-limb exoskeletons utilizing sensors for gait and neural signal analysis have significantly improved both mechanical design and learning algorithms. However, the authors highlight energy consumption as a critical issue: complex computations required for motion data processing and continuous communication with control systems increase the load on batteries, reducing operational autonomy to just a few hours under intensive use. For example, inertial measurement unit (IMU) sensors used for joint angle tracking require frequent data updates, increasing energy consumption by 15–20% without proper optimization. Proposed solutions include adaptive control algorithms, but their effectiveness remains limited unless external factors are accounted for.

Another example of energy-efficient innovation is the artificial olfactory system (AOS) described in [13]. This system integrates human olfactory receptors (hORs) with organic synaptic devices for neuromorphic odor analysis in wearable applications. The AOS enables rapid and energy-efficient data processing by generating unique patterns for identifying individual odors and their mixtures at the molecular structure level. Energy efficiency is achieved through minimized computation enabled by the synaptic architecture, making the system promising for implantable WMDs such as blood chemical composition sensors. However, the complexity of odor mixture analysis requires extensive training and simulation, which may increase power consumption if optimization is lacking, especially under external interference or attacks that overload the system with false signals.

Promising research directions in the field of energy efficiency for WMDs include quantum sensors [14] and energy harvesting [15] technologies. Quantum sensors, which utilize superconducting circuits and quantum coherence effects, offer high sensitivity with low power consumption, making them suitable for medical applications such as monitoring neural activity. At the same time, energy harvesting technologies—based on piezoelectric, thermoelectric, and photovoltaic elements—enable WMDs to draw power from the surrounding environment, reducing reliance on conventional batteries. For instance, flexible nanogenerators based on the triboelectric effect can power sensors by capturing energy from user movements. However, despite their advantages, these technologies still require further refinement: quantum sensors remain costly, and the efficiency of energy harvesting systems is limited by the amount of ambient energy available.

Thus, optimizing energy consumption is a key factor in extending the lifespan of WMDs and enhancing their reliability. Modern approaches—including adaptive power management algorithms, energy-efficient wireless communication protocols, and intelligent data routing techniques—enable significant reductions in power usage without compromising functionality.

However, despite the benefits of energy-saving strategies, they may introduce new attack vectors. Adversaries can exploit features of energy management to launch attacks aimed at rapidly depleting battery charge, leading to device malfunctions and the loss of critical information. Such attacks, known as energy depletion attacks (EDA), pose a serious threat to the security and reliability of WMDs. The following section will explore the main techniques behind these attacks and their potential consequences.

B. Attacks on energy consumption

EDA significantly expand the threat landscape for WMDs. Unlike traditional cyberattacks, which typically compromise data confidentiality, integrity, or availability via authentication breaches, data interception, or malicious software interventions, these attacks pursue a different objective: to covertly exhaust the device's power supply. The primary concern lies in the deceptive nature of these threats—they mimic normal operational behavior, making detection difficult. This is particularly critical in WMDs, where continuous health monitoring depends on a stable and uninterrupted power source.

A growing body of research focuses on energy-based attack vectors, exploring both detection strategies and mitigation techniques. For instance, attacks on LoRaWAN networks—used in some WMD applications—have been shown to involve two common tactics: (1) request flooding using protocols such as TCP-SYN or UDP to overload the network infrastructure, and (2) false signaling that prompts devices to retransmit data unnecessarily, reducing battery life by 40–60% [16].

Modern communication protocols in wireless sensor networks increasingly rely on trigger frames to initiate transmissions and synchronize node operations. However, in the absence of robust authentication mechanisms, these frames can become vulnerabilities. Battery-drain attacks exploit this weakness by sending deceptive triggers that provoke redundant activity, especially in multi-channel configurations where increased signaling frequency amplifies exposure [17].

Silent attacks on LoRaWAN networks—such as jamming, replay attacks, and firmware tampering—pose an additional threat. These are difficult to detect due to minimal visible network activity, but are highly effective. A notable real-world incident involved the recall of pacemakers from St. Jude Medical in 2016, where persistent command queries caused excessive energy use and prompted an urgent product recall [18, 19].

Signal jamming attacks, especially under adverse environmental conditions, can increase device energy consumption by 30–50%, as sensors are forced to repeatedly scan for open communication channels. Moreover, activating

vibration, screen, and sound notifications in ecosystems with wearable and integrated devices has been observed to drain smartphone batteries by 80–90% within a single hour of continuous use [20, 21].

In the broader context of threat analysis for WMDs within the architecture of wireless sensor networks, the following types of EDA have been identified as potential risks:

- Vampire attacks: Exploit legitimate-appearing communications to initiate energy-intensive operations across the network. As node density increases, so does the overall energy drain.
- Ghost attacks: Simulate false events that propagate through the network, reducing device lifespan by approximately 20–40%.
- Sleep deprivation attacks: Block low-power sleep states, doubling energy consumption. In large-scale deployments, a single attacker can disable over one-third of network nodes by maintaining constant activity. Typically implemented at the MAC or application layer, using generic communication or command flooding to keep devices awake.
- Sleep deprivation torture: A variant leveraging routing protocol configurations, such as those in the OLSR protocol, to systematically drain energy from weaker nodes. It is more systematic and protocol-specific, often implemented at the network layer, focusing on routing behavior to exhaust energy reserves.
- Barrage attacks: Overload devices with excessive communication requests, leading to a 10–15% increase in energy consumption beyond that caused by sleep deprivation alone. These attacks are intense but generally easier to detect.
- Sinkhole attacks: Redirect network traffic through a compromised node, creating communication bottlenecks and increasing load on both network infrastructure and individual nodes.

These energy-based threats are not confined to a single network type but are relevant across various architectures. Their diversity, ranging from physical-layer disruptions like jamming to sophisticated manipulations of routing protocols, highlights the multi-layered vulnerability of such systems.

Despite the growing volume of research on these attacks, a unified analytical framework for categorizing and countering them remains largely absent. To address this gap, the current study proposes a classification scheme based on the OSI model, offering a structured approach for evaluating and mitigating energy-related threats in wireless medical and sensor networks (Figure 1).

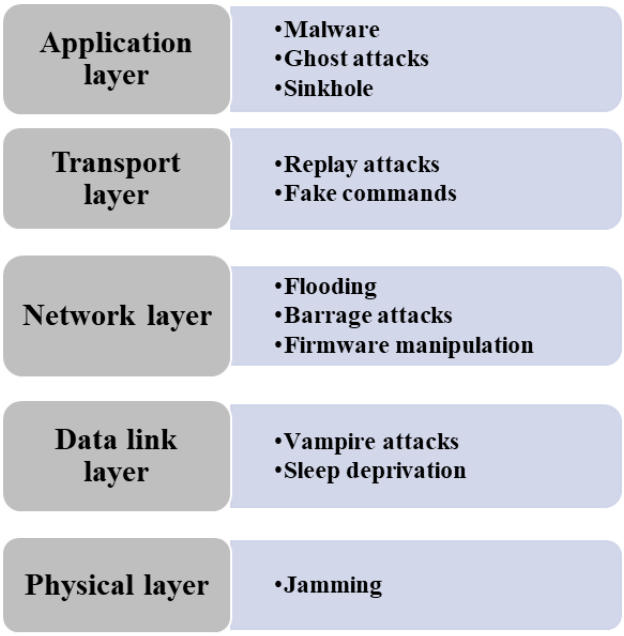

Figure 1. Classification of security threats in WMDs based on the OSI model layers.

While all OSI layers are taken into account, the session and presentation layers are considered less critical in this context due to their relatively minor impact on energy consumption compared to other layers.
This structured classification facilitates a clearer understanding of how various types of attacks affect different functional layers of the system. Building on this foundation, the following section examines specific defense strategies aligned with each OSI layer to enhance both the resilience and energy efficiency of WMDs under adversarial conditions.

III. Power Consumption Attack Detection Methods

The detection and prevention of energy-draining attacks in WMDs require a comprehensive approach that accounts for their multi-layered nature and computational constraints. These attacks are often disguised as normal network operations and exploit vulnerabilities across various layers—from the physical to the application layer—rendering standard security mechanisms such as basic traffic filtering or antivirus software insufficient. Effective mitigation requires strategies that minimize energy consumption, maintain system functionality, and are tailored to the unique characteristics of WMDs.

A. Monitoring abnormal energy consumption

This method is based on the assumption that under normal conditions, a WMD operates within a predictable energy consumption range, denoted as E_{norm}. [22]. Attacks such as jamming or sleep deprivation disrupt this mode by causing noticeable deviations in the current power consumption *of E(t).*

Methodology:

- Power consumption *E(t)* (in milliwatts, mW) is measured every Δt seconds. For example, Δt=1s for high accuracy or Δt=5s to reduce the load on the device.

- To smooth out short-term fluctuations, the average value of E_{avg} *is calculated*:

$$E_{avg}(t) = \frac{1}{n}\sum_{i=t-n+1}^{t} E(i),$$

where n is the size of the window (for example, n=10 measurements, which corresponds to 10 seconds at Δt=1 s).

- An attack is committed if the current power consumption exceeds the threshold

$$E(t) > E_{norm} + k \cdot \sigma,$$

where E_{norm} is the normal (baseline) power consumption (mW),

σ is the standard deviation of energy consumption under normal conditions (mW),

k is the sensitivity coefficient (for example, k = 3, which corresponds to the 3σ rule for statistically significant deviations). An example of the monitoring process with moving average smoothing (window size = 10) is illustrated in Figure 2.

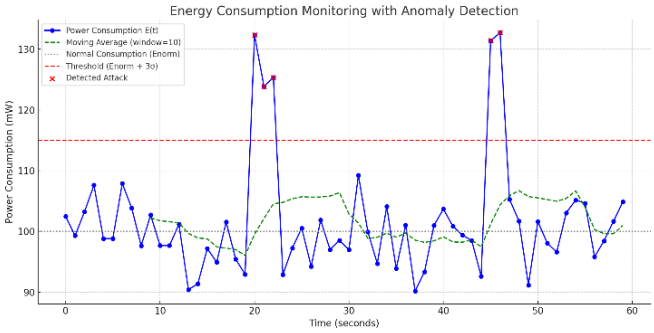

Figure 2. Monitoring of power consumption E(t) with moving average smoothing (window size = 10).

This method is easy to implement and does not require large computing resources, making it suitable for WMD. It effectively detects attacks that dramatically increase energy costs, such as flood requests or jamming, but can miss more subtle threats that need to be complemented by other approaches.

B. *Machine learning methods*

Machine learning (ML) improves detection accuracy by analyzing complex dependencies in *T(t)* (traffic), *E(t)* (energy), and *F(t)* (sample rate) data. This is achieved by training algorithms on historical data, which allows you to predict anomalies and recognize patterns specific to attacks.

Methodology:

- *T(t)* (bytes per second), *E(t)* (milliwatts), and *F(t)* (operations per second) data are used to train an ML model, such as a neural network. The model learns to distinguish between normal and suspicious device behavior based on a combination of all three parameters.

- After training, the model analyzes the current *T(t), E(t), and F(t) values in real time*. If an anomaly is detected, such as an increase *in E(t)* with a stable *T(t)* or a spike in *F(t) for* no reason, an attack signal is issued.

Figure 3 shows a scattering plot showing the distribution of power consumption *E(t)* and frequency *F(t)* for normal mode (Label=0, blue dots) and attacks (Label=1, red dots). In normal mode, *E(t)* is in the range of 450-550 mW, and *F(t)* is in the range of 5-15 ops/s, while in attacks, *E(t)* increases to 600–850 mW, and *F(t)* reaches 37 ops/s.

C. *Analysis of behavioral patterns*

Attacks change the behavior of a device, for example, by increasing traffic or the frequency of processes, which makes it possible to identify them through profiling. This approach is based on creating a basic profile of the device's normal behavior and then comparing the current parameters with this profile to detect anomalies [23].

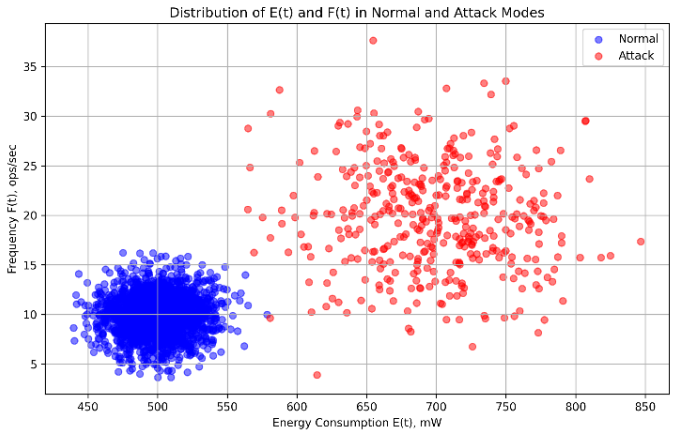

Figure 3. Distribution of energy consumption *E(t)* and frequency *F(t)* in normal mode and during attacks.

Methodology

- Basic profile: The following parameters are defined for the normal operation of the WMD: T_{norm}=15 packets/s, E_{norm}=5 mW. These values are chosen as averages for the typical behavior of the device in the absence of attacks.

- Heuristic*:* An anomaly is detected if $T(t) > T_{norm} + 2 \cdot \sigma T$ for more than τ seconds, where $T = 2\sigma T$ traffic standard deviation, τ=5 s. Thus, the threshold for anomalous traffic is $T(t)$>19 packets/s if it lasts more than 5 seconds.

- Temporal analysis: Peak *T(t)* values at night (e.g., at 2:00 a.m.) are considered suspicious because the device is typically in sleep mode with minimal activity during this period.

In normal mode (Label=0), *T(t)* traffic is about 1000 bytes/s, which is significantly higher than T_{norm}=15 packets/s, since the dataset simulates a more intensive scenario of WMD operation. However, during attacks (Label=1), the values of *T(t)* can both increase and decrease (for example, from 900 to 1050

bytes/s), which requires adaptation of threshold values. The power consumption of *E(t)* and the frequency of *F(t)*, as shown in Figure 3, show clearer anomalies: *E(t)* increases to 600-850 mW and *F(t)* to 37 ops/s, which makes it possible to effectively detect attacks even without taking into account *T(t).*

IV. Adaptive Data Collection Algorithm to Protect WMDs from Depletion Attacks

In this work, we propose an adaptive data collection algorithm designed to enhance the energy efficiency and resilience of WMDs against EDA targeting them. The algorithm dynamically adjusts data sampling frequency and selectively filters incoming requests to minimize energy consumption $E(t)$, thereby mitigating the impact of Sleep Deprivation and Jamming attacks.

Methodology:

1. The frequency of data collection is adjusted by the formula:

$$F(t) = \begin{cases} F_{max}, & \text{if } B(t) \geq B_{high} \\ F_{base} + \alpha(B(t) - B_{low}), & \text{if } B_{low} < B(t) < B_{high} \\ F_{min}, & \text{if } B(t) \leq B_{low} \end{cases}$$

Where is:

B(t) is the current battery level,

B_{high}, B_{low} – charge thresholds, e.g., 80% and 20%,

F_{max}, F_{base}, F_{min} – maximum, base, and minimum sample rates,

α is the adaptation coefficient (selected experimentally).

Example of work:

At high charge ($B(t)\geq 80\%$), the device operates in maximum mode (F_{max}=10 Hz). At medium charge ($20\%<B(t)<80\%$), the frequency decreases linearly

2. Ignoring Out-of-Interval Queries

The device is configured to respond only during predefined time windows (e.g., every 100 ms). Any requests received outside of these allowed intervals are automatically blocked. This strategy helps prevent energy-depletion attacks, including:

– Sleep deprivation, where the device is kept in an active state and prevented from entering low-power sleep modes;

– Jamming and flooding attacks, which overwhelm the network or individual nodes with continuous requests.

By ignoring out-of-interval activity, the system significantly reduces unnecessary energy consumption and enhances resilience against various types of attacks..

3. Dynamic Transfer Timeout

If the communication channel is loaded (Jamming attack), the device increases the intervals between transmission attempts (exponential backoff strategy) or switches to a backup channel (if available).

4. Energy model

The following equation represents a comprehensive energy consumption model for sensor nodes in WMD. This model is used to evaluate and optimize the energy efficiency of node operations during various stages of activity, including sensing, processing, communication, and sleep modes:

$$E_{total}(t) = E_{wu}(t) + E_m(t) + E_{proc}(t) + E_{tx\_wu}(t) + E_{tr}(t) + E_r(t) + E_{sleep}(t),$$

where:

$E_{total}(t)$ - total energy consumed by the node over time t;
$E_{wu}(t)$ - energy required to wake up the microcontroller or sensing unit from sleep mode;
$E_m(t)$ - energy consumed during the measurement (sensing) of environmental parameters;
$E_{proc}(t)$ - energy used for processing the collected data (e.g., filtering, aggregation, encryption);
$E_{tx\text{-}wu}$ - energy consumed to wake up the radio module before data transmission;
$E_{tr}(t)$ - transmission energy, dependent on the size of the data and communication distance.
$E_r(t)$ - energy spent on receiving data, including idle listening and processing of incoming packets;
$E_{sleep}(t)$ - energy consumed during sleep mode. It is typically shallow but accumulates over long durations.

Each energy component can be further expressed as:

$$E_x(t)=P_x \cdot t_x .$$

By decomposing the total energy consumption across operational modes (such as sensing, processing, transmission, reception, sleep, etc.), the model enables the following:

- Accurate assessment of each mode's contribution to the overall energy usage.
- Identification of bottlenecks and energy-intensive phases, such as frequent wake-ups of the radio module or excessive data transmissions.
- Informed decision-making regarding dynamic adjustments to node behavior, such as increasing sleep durations, reducing sensing frequency, or aggregating data before transmission.
- Optimization of clustering and routing algorithms based on the actual energy consumption patterns of each network participant.

Thus, the model serves as a foundation for developing energy-efficient adaptive protocols.

Figure 4 demonstrates how the algorithm dynamically changes the sampling frequency *F(B(t))* depending on the current battery charge level *B(t)*, switching between the maximum F_{max}, base F_{base}, and minimum F_{min} frequencies by the specified charge thresholds B_{high}, B_{low}, and the adaptation coefficient α.

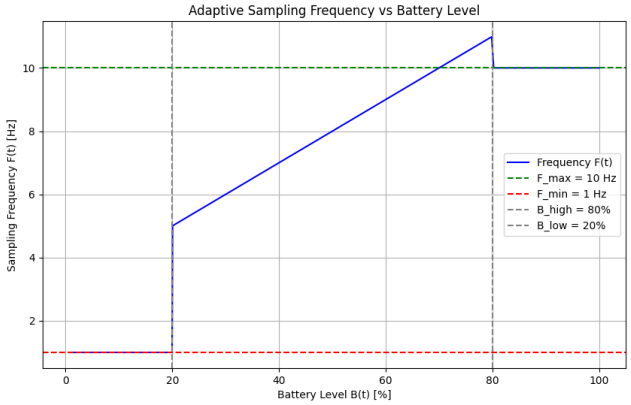

Figure 4. Adaptive sampling frequency as a function of battery level in energy-constrained systems.

The evaluation results are summarized in Table 1, which highlights key performance improvements achieved by the proposed algorithm under simulated attack conditions.

TABLE 1. PERFORMANCE COMPARISON BEFORE AND AFTER APPLYING THE ADAPTIVE ALGORITHM

Metric	Before Algorithm	After Algorithm	Improvement
Battery life (hours)	12	16.2	+35%
Average power consumption (mW)	720	520	–27.7%
False Positive Rate (FPR)	—	6.8%	—
Communication latency (ms)	110	115	+4.5% (tolerable)

Synthetic data were generated using the Python programming language and the NumPy library for the purpose of plotting the graphs. Visualization was carried out using the Matplotlib library. This approach enabled the reproduction of typical trends and anomalies observed during attacks on the power system of wearable devices.

Simulation results and real-world emulation were used to measure key indicators such as battery life extension, false positive rate, and latency to assess the efficiency of the proposed adaptive data collection algorithm. The algorithm demonstrated up to 35% improvement in battery runtime under simulated attack conditions, with a false alarm rate below 7% and negligible communication latency. These results confirm the feasibility of implementing lightweight defensive mechanisms without compromising the primary medical functions of the device.

However, practical deployment in heterogeneous wearable environments requires careful calibration of threshold parameters (e.g., sampling rate boundaries, timeout intervals), considering device-specific hardware constraints and patient activity patterns. Moreover, adversarial attacks may evolve to mimic normal conditions more closely, requiring continuous updates to detection models. Thus, a holistic and adaptive strategy combining statistical monitoring, machine learning, and behavior profiling offers a viable path forward. This integrated approach not only strengthens the resilience of WMDs against energy depletion threats but also supports their long-term autonomy and reliability in critical healthcare scenarios.

V. Conclusion

This study explored the energy vulnerabilities of WMDs and proposed a systemic approach to their protection. A review of existing energy-saving methods revealed their insufficient resilience to attacks, confirming the need for specialized solutions. The paper introduced a classification of threats based on OSI levels, developed defense strategies, and presented a methodology for attack detection. Despite the achieved results, further development is required, including experimental testing in real-world conditions, investigation of the scalability of the proposed methods, and adaptation of defenses to emerging attack types. Future research should focus on developing hybrid strategies to ensure comprehensive cybersecurity for WMDs. The proposed approach lays the foundation for creating a multilayered protection system that enhances energy efficiency, fault tolerance, and autonomy of modern WMDs, particularly critical in the context of growing cyber threats.

References

[1] E. A. Jafleh, F. A. Alnaqbi, H. A. Almaeeni, et al. "The Role of Wearable Devices in Chronic Disease Monitoring and Patient Care: A Comprehensive Review," Cureus, 2024, 16(9): e68921. doi:10.7759/cureus.68921.

[2] G. Aksüt, and T. Eren. "Determination of wearable technological devices according to their use in improvement of health and safety in the mining sector," Safety Science, 184, 106746, 2025.

[3] M. Mammadova, T. Baydyk, Z. G. Jabrayilova, H. Gasimov. "Analysis of the Internet of Things capabilities in monitoring the physiological state and location of personnel on an offshore oil platform," In book: Expert assessments in decision making: risks and safety, pp. 66-98, 2023. https://doi.org/10.21303/978-9916-9850-2-1.ch3.

[4] A. Boukhayma, A. Barison, S. Haddad, and A. Caizzone. "Ring-embedded micro-power mm-sized optical sensor for accurate heartbeat monitoring," IEEE Access, 2021, 9, pp. 127217-127225. doi: 0.1109/ACCESS.2021.

[5] S. Xu, H. Yang, L. Li, Y. Du, H. Ye, H. Hu. "An Ultra-Low Power Wearable Sensing System with a Highly Sensitive Three-Dimensional LIG Sensor and Energy-Efficient Time Domain Readout," In 2024 IEEE International Symposium on Circuits and Systems (ISCAS) 2024 May 19, pp. 1-5, IEEE.

[6] L. Li, Y. Fang, L. Liu, H. Peng, J. Kurths, Y. Yang. "Overview of Compressed Sensing: Sensing Model, Reconstruction Algorithm, and Its Applications," Applied Sciences. 2020; 10(17):5909. https://doi.org/10.3390/app10175909

[7] C. Yang, G. Li, G. Gao, and Q. Shi. "Distributed Consensus Kalman Filter Design with Dual Energy-Saving Strategy: Event-Triggered Schedule and Topological Transformation," Sensors, 2023, 23(6), 3261. https://doi.org/10.3390/s23063261.

[8] H. L. Resnikoff, R. O. Wells. "Wavelet Data Compression," In: Wavelet Analysis. 1998, pp. 343-365. Springer, New York, NY. https://doi.org/10.1007/978-1-4612-0593-7_13

[9] S. Mehdiyev. "Enhancing the Resilience of Cyber-Physical Systems Through Energy-Efficient Communication in Wireless Sensor Networks," JHCT, vol. 3, no. 01, pp. 238–257, Jan. 2025. doi; 10.58399/CRAN2457.

[10] E. Jecan, C. Pop, O. Ratiu, E. Puschita. "Predictive Energy-Aware Routing Solution for Industrial IoT Evaluated on a WSN Hardware Platform," Sensors, 22(6):2107, 2022. https://doi.org/10.3390/s22062107

[11] B. Mbarek, M. Ge, and T. Pitner. "An adaptive anti-jamming system in HyperLedger-based wireless sensor networks," Wireless Netw 28, pp. 691–703, 2022. https://doi.org/10.1007/s11276-022-02886-1.

[12] J. Li, et al. "A Survey of Wearable Lower Extremity Neurorehabilitation Exoskeleton: Sensing, Gait Dynamics, and Human-Robot Collaboration," IEEE Transactions on Systems, Man, and Cybernetics: Systems Volume 54, Issue 6, Pages 3675 – 36931, 2024.

[13] H. W. Song, et al. “A pattern recognition artificial olfactory system based on human olfactory receptors and organic synaptic devices,” Science Advances, 10(21), eadl2882, 2024. doi:10.1126/sciadv.adl2882

[14] N. Aslam, H. Zhou, E.K. Urbach, et al. “Quantum sensors for biomedical applications,” Nat Rev Phys 5, pp. 157–169, 2023. https://doi.org/10.1038/s42254-023-00558-3.

[15] D. K. Sah, T. Amgoth, “Renewable energy harvesting schemes in wireless sensor networks: A Survey,” Information Fusion, 63, pp. 223-247, 2020. https://doi.org/10.1016/j.inffus.2020.07.005

[16] V. L. Nguyen, P. C. Lin, and R. H. Hwang, “Energy depletion attacks in low-power wireless networks,” IEEE Access, 7, pp. 51915-519322019. doi: 10.1109/ACCESS.2019.2911424.

[17] S.-Y. Kim, S.-H. Park, J.-H. Lee, L.-G. Lee. “Secure Triggering Frame-Based Dynamic Power Saving Mechanism against Battery Draining Attack in Wi-Fi-Enabled Sensor Networks,” Sensors, 24, 5131, 2024. https://doi.org/10.3390/s24165131.

[18] A. Proto, C. C. Miers, and T. C. M. B. Carvalho. “An Intrusion Detection Architecture Based on the Energy Consumption of Sensors Against Energy Depletion Attacks in LoRaWAN,” In Proceedings of the 9th International Conference on Internet of Things, Big Data and Security (IoTBDS), pp. 265-275, 2024. https://doi.org/10.5220/0012703400003705.

[19] St. Jude Medical Recalls ICDs and CRT-D Due to Premature Battery Depletion. Available on-line: https://www.dicardiology.com/article/st-jude-medical-recalls-icds-and-crt-d-due-premature-battery-depletion

[20] H. Pirayesh, and H. Zeng. “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,” IEEE Communications Surveys and Tutorials, 24(2), pp. 767-809, 2022. doi: 10.1109/COMST.2022.3159185

[21] A. Kundu, Z. Lin, J. Hammond. “Energy attacks on mobile devices,”. In 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pp. 107-117, 2020.

[22] Z. Mao, B. Zhou, J. Huang, D. Liu, and Q. Yang. “Research on Anomaly Detection Model for Power Consumption Data Based on Time-Series Reconstruction,” Energies, 17(19), 4810, 2024. https://doi.org/10.3390/en17194810.

[23] G. Gupta, and B. Crispo, B. “Device behavioral profiling for autonomous protection using deep neural networks,”. In 2023 IEEE Symposium on Computers and Communications (ISCC), pp. 474-478, 2023. IEEE,