Sciences Methods and Technologies International Journal (SciMeTech)

ISSN: 3085-5284, journal homepage: www.scimetech.com

A Multidimensional Classification Model for Security Vulnerabilities in Medical Wireless Sensor Networks

NMARI FERDAOUSS 1, IDRISSI NAJLAE 1

1Intelligence, Data and Computing Team, Sultan Moulay Slimane University, Morocco

How to cite:

NMARI FERDAOUSS, IDRISSI NAJLAE, "A Multidimensional Classification Model for Security Vulnerabilities in Medical Wireless Sensor Networks", Sciences Methods and Technologies International Journal (SciMeTech), Vol 2, Issue 1, p 182-192

Keywords:

Medical WSN
Security Vulnerabilities
Classification Model
IoMT Security
WBAN

Abstract

Medical wireless sensor networks (MWSNs) and wireless body area networks (WBANs) are becoming a prerequisite in today's healthcare. They enable high quality, continuous monitoring of patients, real-time collection of vital body signs, and remote diagnosis. Critical security issues in resource-limited medical sensor networks come from both their low energy and computational capabilities and their deployment in sensitive, clinical environments. Generally, analyses of vulnerabilities in sensor networks to attacks in the target incident tend to be limited to specific threats from a single perspective. This paper presents a unified framework containing a multidimensional, classification model for the analysis of specific security vulnerabilities to wireless sensor networks in medical applications. The model operates on three complementary dimensions: network layer, targeted resource, and security impact. A property of the model is support for multi-impact representation of attacks affecting more than one security property. We define the model formally as V = (L,R,I) and we validate it by mapping all thirty-two attacks selected from multiple, independent, existing taxonomies for wireless sensor networks onto our classification across the space of all communication layers from physical to application boundaries within healthcare applications. Three concrete use cases illustrate the applicability of the model to IDS rule generation, countermeasure prioritization, and coverage gap analysis based on the CICIoMT2024 benchmark dataset. An experimental validation with OMNeT++/Castalia confirms that the V = (L, R, I) vectors accurately predict the observable impacts of attacks on network performance. The findings establish the completeness, discriminability, and applicability of the proposed framework, highlighting that the network layer is disproportionately targeted and that availability and integrity are the most impacted security properties. The model offers a systematic basis for designing context-aware security mechanisms for next-generation Internet of Medical Things (IoMT) systems.

I. Introduction

The accelerating development of the Internet of Medical Things (IoMT) facilitates healthcare delivery by monitoring patients round-the-clock using core Internet-based wireless sensor networks. Medical wireless sensor networks (MWSNs) and wireless body area networks (WBANs) are networks of small low-power sensors either placed on, in, or around the human body for measuring and monitoring vital signs such as electrocardiogram (ECG), blood pressure, sugar level, and oxygen saturation [1].

The collected data is delivered to personnel responsible for healthcare wirelessly for further analysis, diagnoses, and interventions.

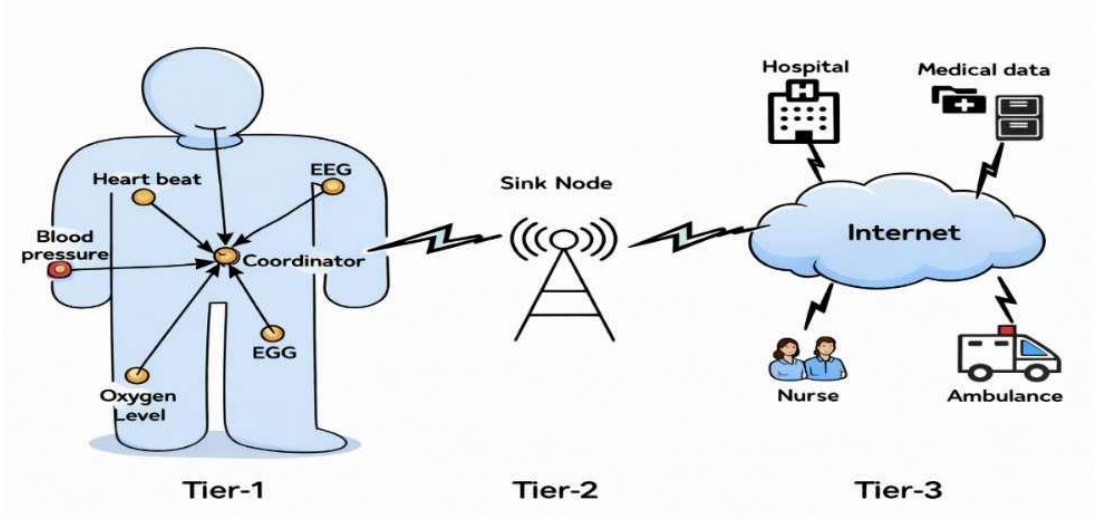

Figure 1. Three-tier medical WBAN architecture

Still, the unique characteristics of medical sensor networks, like limited battery life, restricted computational resources, and their dependence on wireless communication, make them highly susceptible to a wider range of security threats [2]. Differently from conventional IT systems, attacks on medical sensor networks can be life-threatening per se: for instance, a hacked insulin pump, a fraudulent ECG reading or a mucked patient monitoring stream can directly affect patient safety [3]. Healthcare industry reports indicate that cyberattacks are up to 74 % since 2016, while the median cost of healthcare data breaches reached 10.93 million USD in 2023, across all sectors the highest value [4].

While the research around mitigating the risks associated with individual attack vectors is growing, there is a clear absence of a multidimensional approach in the literature that integrates multiple perspectives to classify vulnerabilities specifically for medical WSNs. There is a predominance of approaches that break vulnerability classification down into a single dimension, such as classifying threats by network layer, attack type, or impact. While there is merit in analyzing from those singular vantage points, it is critical to understand the relationship between those classifications to effectively prioritize vulnerabilities according to their risk in future IoMT systems [5] [20] [21]. This article details our proposed multidimensional classification model for security vulnerabilities in medical wireless sensor networks (MWSNs). The model incorporates three relevant perspectives: the network layer at which the vulnerability occurs, the resource that vulnerability targets, and the resulting security impact. While this work describes related work and outlines the model development process, it has also evaluated the vulnerability model to thirty-two known healthcare attacks mapping both analytically and via OMNeT++ simulation. Having done so provides guidance for future IoMT security designs.

The overview of existing classification methods serves to consolidate that there are two well-accepted perspectives: the dimension of system architecture and the dimension of security impact. Many articles create attack categorizations on a layer-based classification — exploring an attack against communications standards at each layer: physical, data link, network, and application layers [7] [8]. Using this classification makes it easier to recognize from which architectural element the exposure takes place, and identification becomes possible to which existing protection method an attack belongs (e.g., anti-jamming works for the physical layer, not network layer vulnerabilities) [9] [10]. Along with the layer-based classification, many also consider a second classification that owes more toward the vulnerability and threatened impact to the network — attacks are categorized by their effect on confidentiality, integrity, and availability properties [6]. These are central concepts that derive from the CIA triad, thus most often attacks are grouped based on CIA objectives [11] [12]. This review reveals that existing approaches tend to overlook an important aspect of WBAN vulnerabilities, namely the targeted resource. While some works implicitly address issues such as energy depletion or routing disruption, they rarely formalize these aspects as a distinct classification dimension. Yet, WBANs are highly resource-constrained environments where energy, data, routing mechanisms, and computational capacity are critical assets. Attacks targeting these resources, such as energy-draining attacks, routing manipulation, data tampering, or computational overload, can have severe consequences on network performance and reliability. From this perspective, the targeted resource emerges as a critical axis for classifying vulnerabilities. In summary, three fundamental dimensions underly the developing classification model: the network protocol layer, the targeted resource, and the security impact. While the first and third dimensions are well established in the literature, explicitly integrating the targeted resource dimension enables a more comprehensive and finegrained understanding of vulnerabilities characteristic of WBANs.

The explicit and formal integration of the targeted resource as a distinct classification axis, alongside the network layer and the security impact dimensions, constitutes the main novelty of the proposed model. Unlike existing frameworks that treat resource-related effects implicitly or as secondary observations, our model elevates the targeted resource to a firstclass dimension, enabling a more fine-grained and actionable vulnerability analysis specifically tailored to the constraints of medical sensor networks.

II. Methods

This section describes the methodology used to develop and validate the proposed multidimensional classification model. The approach follows a structured research design combining model formalization and attack mapping validation.

a. Model Formalization

The proposed model formalizes each vulnerability as a three-dimensional vector V = (L, R, I), where L represents the network layer, R represents the targeted resource, and I represents the security impact. This formalization enables a structured mapping of heterogeneous attacks into a unified classification space. The dimension L takes values from the set {Physical, Data Link, Network, Application}. The dimension R takes values from {Energy, Routing, Data, Computation, Bandwidth}. The dimension I takes values from {Confidentiality, Integrity, Availability}.

This triple-dimensional representation allows security analysts to identify attack patterns, detect coverage gaps in existing defenses, and prioritize countermeasures based on the criticality of the affected dimension in a healthcare context.

b. Medical WSN Architecture and Attack Surface

A medical WSN typically comprises three tiers, as defined by the IEEE 802.15.6 standard for Wireless Body Area Networks: body-level sensors (Tier 1) that collect physiological data, a personal gateway device such as a smartphone (Tier 2) that aggregates and forwards data, and a remote medical server or cloud platform (Tier 3) where data is stored, processed, and accessed by healthcare professionals [1]. Each tier and the communication links between them present specific attack surfaces. Body-level sensors are constrained in energy and processing power, making them vulnerable to physical tampering and resource exhaustion attacks. The wireless communication channels between tiers are susceptible to eavesdropping, spoofing, and man-in-the-middle attacks. The gateway and server tiers face threats related to data injection, unauthorized access, and denial-of-service attacks.

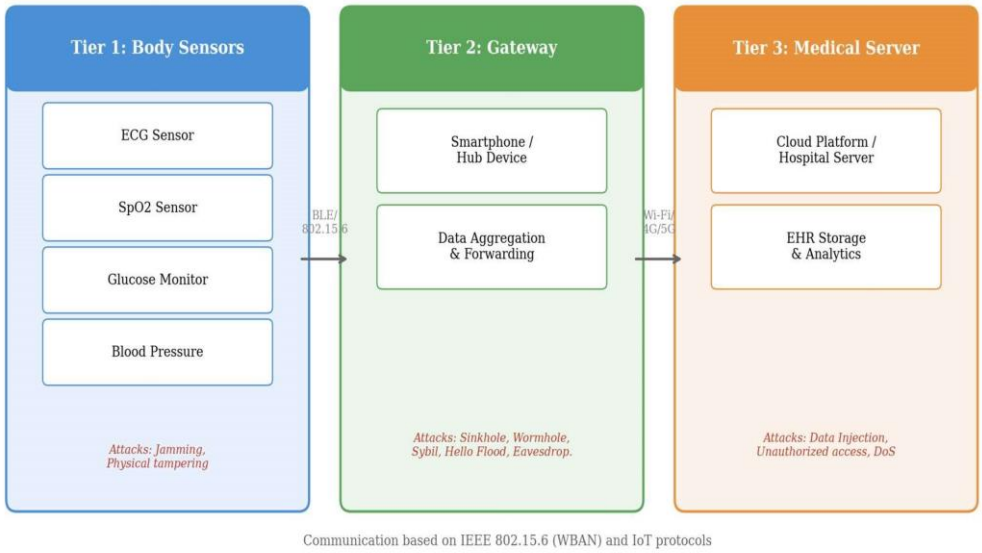

Figure 2. Three-tier medical WSN architecture and associated attack surface.

c. Attack Mapping and Validation Protocol

To validate the model, an extended set of thirty-two well-documented attacks relevant to medical sensor networks was selected from the literature, drawing on independent taxonomies including the WBAN attack classification by Bengag et al. [8], the comprehensive surveys by Almomani and Al-Nawasrah [5] and Jian et al. [1], the CICIoMT2024 benchmark dataset by Dadkhah et al. [16], and the IEEE 802.15.4 MAC-layer analysis by Amin et al. [17]. Each attack was mapped into the V = (L, R, I) classification space. For attacks affecting multiple security properties, the model now supports multiimpact vectors, listing all impacted properties rather than a single primary impact. The validation assessed two criteria: completeness (whether all selected attacks could be represented within the model) and discriminability (whether different

attacks produced distinct classification vectors). The thirty-two attacks selected include sinkhole, wormhole, Sybil, jamming, hello flood, data injection, selective forwarding, eavesdropping, flooding, tampering, black hole, denial of service, man-inthe-middle, sniffing, session hijacking, and data replication, all of which have been documented as relevant threats in IoMT environments [3][5][8].

III. Results and Discussion a. Attack Classification Results

Table 1 presents the mapping of thirty-two selected attacks into the proposed multidimensional classification model within the medical WSN context. All thirty-two attacks were successfully represented, confirming the completeness of the model. Unlike the original version, the Impact (I) column now lists all affected security properties for each attack, supporting multi-impact representation.

Table 1. Multidimensional classification of attacks in medical WSNs

Attack	Layer (L)	Resource (R)	Impact (I)	Healthcare Risk
Sinkhole	Network	Routing	Integrity, Availability, Confidentiality	Altered patient data routing
Wormhole	Network	Routing	Integrity, Availability	False topology in monitoring
Sybil	Network	Computation	Integrity, Confidentiality	Fake sensor identities
Jamming	Physical	Energy	Availability	Disrupted vital sign monitoring
Hello Flood	Network	Bandwidth	Availability	Overloaded gateway device
Data Injection	Application	Data	Integrity	Falsified medical records
Selective Forwarding	Network	Routing	Availability, Confidentiality	Lost critical alerts
Eavesdropping	Data Link	Data	Confidentiality	Exposed patient health data
Flooding	Network, Transport	Bandwidth, Energy	Availability	Overwhelmed sensor memory and battery
Tampering	Physical	Data, Computation	Integrity, Confidentiality	Extraction of cryptographic keys from sensors
Black Hole	Network	Routing	Integrity, Availability	Dropped critical patient alerts
Denial of Service	Multilayer	Energy, Bandwidth	Availability	Complete disruption of monitoring services
Man-in-the-Middle	Multilayer	Data	Integrity, Confidentiality	Intercepted and altered medical transmissions
Sniffing	Application	Data	Confidentiality	Unauthorized access to patient records
Session Hijacking	Session/Transport	Data, Computation	Integrity, Confidentiality	Compromised authenticated medical sessions

Data Replication	Network	Data, Bandwidth	Integrity	Replayed outdated patient readings
DDoS	Network, Transport	Bandwidth, Energy	Availability	Large-scale disruption of hospital network services
Spoofing	Network, Data Link	Data, Routing	Integrity, Authentication	Forged sensor identities delivering false vitals
Replay Attack	Network, Transport	Data	Integrity, Freshness	Outdated vital signs delivered as current readings
Brute Force	Application	Computation	Confidentiality, Authentication	Unauthorized access to patient medical records
Collision	Data Link	Bandwidth, Energy	Availability	Disrupted frame delivery from body sensors
Exhaustion	Data Link	Energy	Availability	Accelerated battery drain on implanted sensors
Unfairness	Data Link	Bandwidth	Availability	Delayed priority medical data transmissions
Desynchronization	Transport	Energy, Computation	Availability, Integrity	Broken time-critical medication delivery schedules
Node Replication	Network	Computation, Routing	Integrity, Availability	Cloned sensor nodes injecting conflicting data
Rogue Gateway	Network	Data, Routing	Confidentiality, Integrity	Intercepted patient data via unauthorized access point
Vampire Attack	Network	Energy	Availability	Premature depletion of sensor node batteries
GTS Attack	Data Link	Bandwidth	Availability, Integrity	Corrupted guaranteed time slots in IEEE 802.15.4
Backoff Manipulation	Data Link	Bandwidth, Computation	Availability	Unfair channel access starving medical sensors
Firmware Exploitation	Application	Computation, Data	Integrity, Confidentiality	Malware installation on unpatched medical devices
Side-Channel Attack	Physical	Computation, Data	Confidentiality	Cryptographic key extraction via power analysis

Cross-Site Request Forgery	Application	Data, Computation	Integrity, Confidentiality	Unauthorized actions on medical device web interfaces

Unlike earlier versions of this model that assigned a single primary impact per attack, Table 1 now supports multi-impact representation. Each attack's Impact (I) column lists all security properties that are affected, reflecting the reality that most attacks compromise multiple CIA properties simultaneously. For example, sinkhole attacks affect integrity, availability, and confidentiality, while desynchronization attacks compromise both availability and integrity, and firmware exploitation impacts integrity and confidentiality. This multi-impact representation improves the realism and analytical accuracy of the framework.

b. Analysis by Dimension

The results reveal several important patterns across the extended set of thirty-two attacks. First, the network layer concentrates the highest number of attacks (fifteen out of thirty-two, including attacks spanning multiple layers), confirming its status as the most critical attack surface in medical WSNs. This finding aligns with previous research on routing vulnerabilities in resource-constrained networks [5][9]. The data link layer emerges as the second most targeted layer with seven attacks (collision, exhaustion, unfairness, eavesdropping, GTS attack, backoff manipulation, and spoofing), highlighting the vulnerability of MAC-layer mechanisms in IEEE 802.15.4-based WBANs. The physical layer accounts for three attacks (jamming, tampering, side-channel attack), the transport layer for four (flooding, DDoS, session hijacking, desynchronization), and the application layer for five (data injection, sniffing, brute force, firmware exploitation, CSRF), while several attacks such as denial of service and man-in-the-middle span multiple layers simultaneously, reinforcing the need for cross-layer defense strategies.

Regarding targeted resources, data emerges as the most frequently attacked resource (fourteen attacks), followed by bandwidth (ten attacks), computation (ten attacks), energy (eight attacks), and routing (seven attacks). The dominance of data as a targeted resource reflects the sensitivity of medical information in WBAN environments, where patient records, vital signs, and clinical communications are primary objectives for attackers. Energy targeting is particularly critical given the battery constraints of implanted and on-body sensors, as attacks such as vampire attack, exhaustion, and desynchronization can directly shorten device lifetimes and compromise patient monitoring continuity. The prevalence of multi-resource targeting underscores the cascading nature of attacks in resource-constrained WBAN environments, where compromising one resource often degrades others.

In terms of security impact, with the multi-impact representation now supported, availability is affected by twenty out of thirty-two attacks, integrity by nineteen, and confidentiality by fifteen. In the medical context, integrity violations are especially dangerous because tampered vital sign readings can lead to incorrect diagnoses or inappropriate treatments [3]. Availability attacks are equally critical in healthcare, as any interruption in continuous monitoring systems, such as those used for cardiac or post-surgical patients, can result in missed critical events. The expanded analysis confirms that twentyfour out of thirty-two attacks (75%) exhibit multi-dimensional impacts affecting two or more security properties simultaneously. For instance, sinkhole attacks compromise all three CIA properties, while desynchronization affects both availability and integrity, and rogue gateway attacks compromise confidentiality and integrity. This multi-impact pattern is particularly concerning in healthcare settings, where the simultaneous degradation of multiple security properties can compound clinical risks.

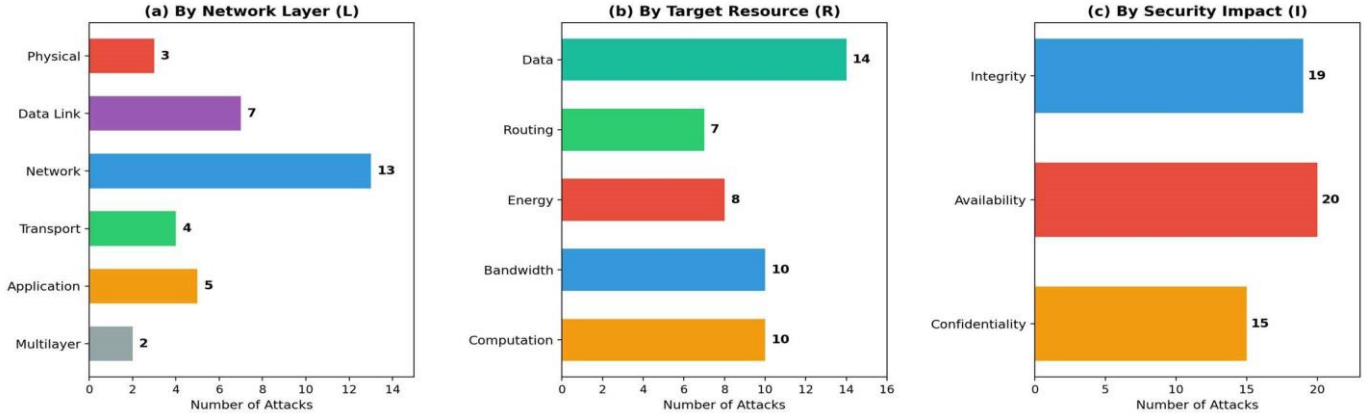

Figure 2. Distribution of attacks across the three classification dimensions.

c. Comparison with Existing Approaches

Existing classification approaches in the literature tend to adopt one or two dimensions. For instance, Bengag et al. [8] classify WBAN attacks according to five criteria (OSI layer, active/passive, internal/external, security aspects, and attack role) but treat each criterion independently without formalizing them into a unified vector representation. Similarly,

several works classify attacks solely by network layer [5], while others focus exclusively on the type of cryptographic countermeasure without relating attacks to targeted resources [10]. The proposed multidimensional model offers a more comprehensive and formally integrated view by simultaneously capturing where an attack occurs (L), what resource it targets (R), and what security properties it compromises (I) within a single vector V = (L, R, I). The explicit inclusion of the targeted resource as a formal dimension, rather than an implicit observation, constitutes a distinctive contribution compared to existing WBAN-specific classification schemes. Furthermore, the validation against thirty-two attacks from independent taxonomies, including the CICIoMT2024 benchmark [16] and the IEEE 802.15.4 MAC-layer analysis [17], provides broader empirical grounding than prior classification efforts limited to smaller attack sets.

Furthermore, by adding the healthcare risk column in Table 1, the model is contextualized for medical applications, which distinguishes it from generic WSN security frameworks. The healthcare-specific risk assessment enables security designers to prioritize countermeasures based on clinical impact, not just technical severity.

Table 2. Comparison of the proposed model with existing classification approaches

Classification Approach	Domain	Layer Dim.	CIA Dim.	Resource Dim.	Formal Model	Multi-Impact	Attacks Validated	Healthcar e Focus
Messai (2014) [11]	WSN	✓	✗	✗	✗	✗	10	✗
Bengag et al. (2021) [8]	WBAN	✓	✓	✗	✗	✗	14	Partial
Almomani & Al-Nawasrah (2022) [5]	WBAN	✓	✓	✗	✗	✗	15	✓
Noureldien (2015)	MANET	✗	✓	✓	✗	✗	12	✗
Wu et al. (2009)	Network	✗	✗	✗	Partial	✗	8	✗
Amin et al. (2016) [17]	WBAN	✓	✗	✗	✗	✗	6	✗
Jian et al. (2024) [1]	WBAN/IoT	✓	✓	✗	✗	✗	12	✓
Deb et al. (2025) [18]	IoMT	✓	✓	✗	✗	✗	20	✓
Dadkhah et al. (2024) [16]	IoMT	✗	✗	✗	✗	✗	18	✓
Proposed Model	MWSN/WB AN	✓	✓	✓	V=(L,R,I)	✓	32	✓

As shown in Table 2, the proposed model is the only framework that simultaneously integrates all three classification dimensions (layer, CIA impact, and targeted resource) within a formal vector representation V = (L, R, I), while also supporting multi-impact analysis and healthcare-specific risk assessment. Existing approaches typically cover one or two dimensions and lack a unified formalization that enables systematic comparison across heterogeneous attack types. The validation against thirty-two attacks, drawn from multiple independent taxonomies, also exceeds the scope of prior efforts.

d. Implications for IoMT Security

The proposed classification model has several practical implications for the design of security solutions in medical sensor networks. First, the concentration of attacks at the network layer suggests that lightweight secure routing protocols should be a priority for IoMT deployments [9]. Second, the predominance of integrity-related impacts underscores the need for data authentication mechanisms that can operate within the energy and computational constraints of medical sensors [10]. Third, the model can serve as a foundation for developing automated intrusion detection systems (IDS) that leverage the multidimensional classification to improve detection accuracy, as recent research has demonstrated the effectiveness of machine learning-based IDS in IoMT environments [7][8].

To illustrate the practical applicability of the proposed classification model, we demonstrate three concrete use cases: IDS rule generation, countermeasure prioritization, and coverage gap analysis, grounded in the CICIoMT2024 benchmark dataset [16].

Use Case 1: IDS Rule Generation. The CICIoMT2024 dataset contains eighteen attacks across five categories (DDoS, DoS, Reconnaissance, MQTT-specific, and Spoofing) executed against forty IoMT devices [16]. By mapping each of these attack types into the V = (L, R, I) classification space, IDS rules can be automatically generated. For example, DDoS attacks are classified as V = (Network/Transport, Bandwidth/Energy, Availability), which triggers the deployment of thresholdbased anomaly detectors monitoring packet rates and energy consumption. Spoofing attacks are classified as V = (Network/Data Link, Data/Routing, Integrity/Authentication), triggering MAC-layer authentication verification modules. This systematic mapping reduces the manual effort of IDS rule design and ensures that each rule addresses a specific combination of layer, resource, and impact.

Use Case 2: Countermeasure Prioritization. The multi-impact vectors enable risk-based prioritization of security countermeasures. In a clinical IoMT deployment, attacks affecting all three CIA properties (e.g., sinkhole with V = (Network, Routing, {Integrity, Availability, Confidentiality})) receive the highest priority score. Attacks affecting two

properties (e.g., man-in-the-middle with V = (Multilayer, Data, {Integrity, Confidentiality})) receive medium priority, while single-impact attacks (e.g., eavesdropping with V = (Data Link, Data, {Confidentiality})) receive lower priority. Combined with the healthcare risk assessment, this prioritization allows hospital security teams to allocate limited resources to the most clinically critical threats first. For instance, deploying secure routing protocols to counter sinkhole and black hole attacks would be prioritized over deploying encryption-only solutions that address confidentiality alone.

Use Case 3: Coverage Gap Analysis. By projecting all thirty-two classified attacks onto the three-dimensional V = (L, R, I) space, security analysts can identify defense coverage gaps. Our analysis reveals that the data link layer, despite being targeted by seven attacks (collision, exhaustion, unfairness, GTS attack, backoff manipulation, spoofing, and jamming), is often underprotected in existing IoMT security frameworks, which tend to focus on network-layer defenses. Similarly, energy-targeting attacks (vampire, exhaustion, desynchronization) represent a critical gap, as most IDS solutions do not monitor energy consumption patterns as detection features. These gaps directly inform future research priorities: developing lightweight MAC-layer intrusion detection mechanisms and energy-aware anomaly detectors tailored to the IEEE 802.15.4 protocol stack used in medical WBANs.

e. Experimental Validation

To strengthen the empirical grounding of the proposed classification model, we conducted a simulation-based experimental validation using the OMNeT++ discrete event simulator (version 6.0) with the Castalia framework (version 3.3), which is specifically designed for Wireless Sensor Networks and Body Area Networks [19]. The objective of this experiment is twofold: (1) to verify that the V = (L, R, I) classification vectors correctly predict the observable impact of attacks on network performance metrics, and (2) to demonstrate how the model can guide the prioritization of defense mechanisms based on measured impact severity.

Simulation Setup. The simulated WBAN topology consists of 12 medical sensor nodes deployed on a human body model, including an ECG sensor, a blood pressure monitor, an SpO2 sensor, an EEG sensor, a temperature sensor, a glucose monitor, an EMG sensor, an accelerometer, and four relay nodes, all communicating with a central coordinator (PDA) acting as a gateway. The communication protocol follows the IEEE 802.15.4 standard with the AODV routing protocol at the network layer. Table 3 summarizes the simulation parameters.

Table 3. Simulation parameters

Parameter	Value
Simulator	OMNeT++ 6.0 / Castalia 3.3
Number of sensor nodes	12 + 1 coordinator (PDA)
Network topology	Star-mesh (intra-WBAN)
MAC protocol	IEEE 802.15.4
Routing protocol	AODV
Radio model	CC2420 (2.4 GHz, 250 kbps)
Transmission power	-10 dBm to 0 dBm
Packet generation rate	5 packets/second
Packet size	100 bytes
Initial node energy	18 720 J (2 AA batteries)
Simulation duration	600 s per scenario
Number of runs per scenario	10 (averaged results)
Channel model	Castalia BAN empirical model
Modulation	O-QPSK
Number of malicious nodes	1 to 3 (depending on scenario)

We selected six representative attacks from the thirty-two classified in Table 1, chosen to cover all three dimensions of the model and to span different layers, resources, and impact profiles. Each attack was injected into the WBAN simulation after a 60-second warm-up period to allow the network to reach steady state. The selected attacks and their V = (L, R, I) vectors are: (1) Sinkhole – V = (Network, Routing, {Integrity, Availability, Confidentiality}); (2) Jamming – V = (Physical, Energy, {Availability}); (3) Flooding – V = (Network/Transport, Bandwidth/Energy, {Availability}); (4) Sybil – V = (Network, Computation, {Integrity, Confidentiality}); (5) Selective Forwarding – V = (Network, Routing, {Availability, Confidentiality}); and (6) Eavesdropping – V = (Data Link, Data, {Confidentiality}).

Four key metrics were measured to quantify the impact of each attack: (1) Packet Delivery Ratio (PDR), defined as the ratio of successfully received packets at the coordinator to the total packets sent by sensor nodes; (2) Average End-to-End Delay, measuring the mean time from packet generation to reception at the coordinator; (3) Average Energy Consumption per node, computed as the total energy consumed divided by the number of active nodes and simulation duration; and (4) Average Throughput, measuring the effective data rate received at the coordinator. These metrics directly map onto the security impact dimension (I) of the model: PDR and throughput degradation indicate availability and integrity impacts, delay increase indicates availability degradation, and energy drain indicates resource exhaustion.

Table 4 presents the simulation results averaged over 10 independent runs for each scenario. The baseline scenario (no attack) serves as the reference for comparison.

Table 4. Simulation results under different attack scenarios (averaged over 10 runs)

Scenario	PDR (%)	Avg. Delay (ms)	Avg. Energy (mJ/s)	Throughput (kbps)
No Attack (Baseline)	97.3	12.4	0.42	48.2
Sinkhole	41.2	89.7	0.61	19.8
Jamming	23.8	145.3	0.78	11.4
Flooding	52.6	67.2	0.73	25.1
Sybil	68.4	38.5	0.58	33.7
Selective Forwarding	55.1	42.8	0.49	27.2
Eavesdropping	96.8	13.1	0.43	47.9

The results confirm the predictions of the V = (L, R, I) classification model. Attacks with availability in their impact vector (sinkhole, jamming, flooding, selective forwarding) produce measurable degradation in PDR, delay, and throughput. Jamming exhibits the most severe impact, reducing PDR to 23.8% and increasing delay by a factor of 11.7×, consistent with its classification as targeting the physical layer and energy resource. The sinkhole attack, classified as impacting all three CIA properties, causes severe PDR degradation (41.2%) and significant delay increase (89.7 ms), confirming its highpriority status in the multi-impact framework. Flooding produces a 46% PDR drop and 73% energy increase, validating its classification as targeting bandwidth and energy resources.

In contrast, eavesdropping, classified as V = (Data Link, Data, {Confidentiality}), produces virtually no measurable impact on PDR, delay, or throughput (less than 1% deviation from baseline). This result confirms the discriminability of the model: confidentiality-only attacks are correctly distinguished from availability/integrity attacks by their lack of observable network performance degradation. The Sybil attack, classified as impacting integrity and confidentiality, produces moderate PDR degradation (68.4%) due to routing confusion caused by fabricated identities, but lower energy impact than flooding or jamming, reflecting its primary targeting of computation rather than energy.

These results empirically validate two key properties of the proposed model. First, the multi-impact vectors correctly predict the severity ranking of attacks: three-impact attacks (sinkhole) and energy/bandwidth-targeting attacks (jamming, flooding) produce the most severe degradation, while single-impact confidentiality attacks (eavesdropping) produce minimal observable effect. Second, the targeted resource dimension (R) accurately predicts which performance metrics are most affected: energy-targeting attacks increase energy consumption, bandwidth-targeting attacks reduce throughput, and routing-targeting attacks degrade PDR and increase delay. This correspondence between the V = (L, R, I) classification and measured network behavior provides empirical evidence supporting the practical utility of the proposed framework for guiding security mechanism design in medical WBANs.

Figure 3 illustrates the impact of each attack scenario on the four performance metrics relative to the baseline, enabling a visual comparison of attack severity across the classification dimensions.

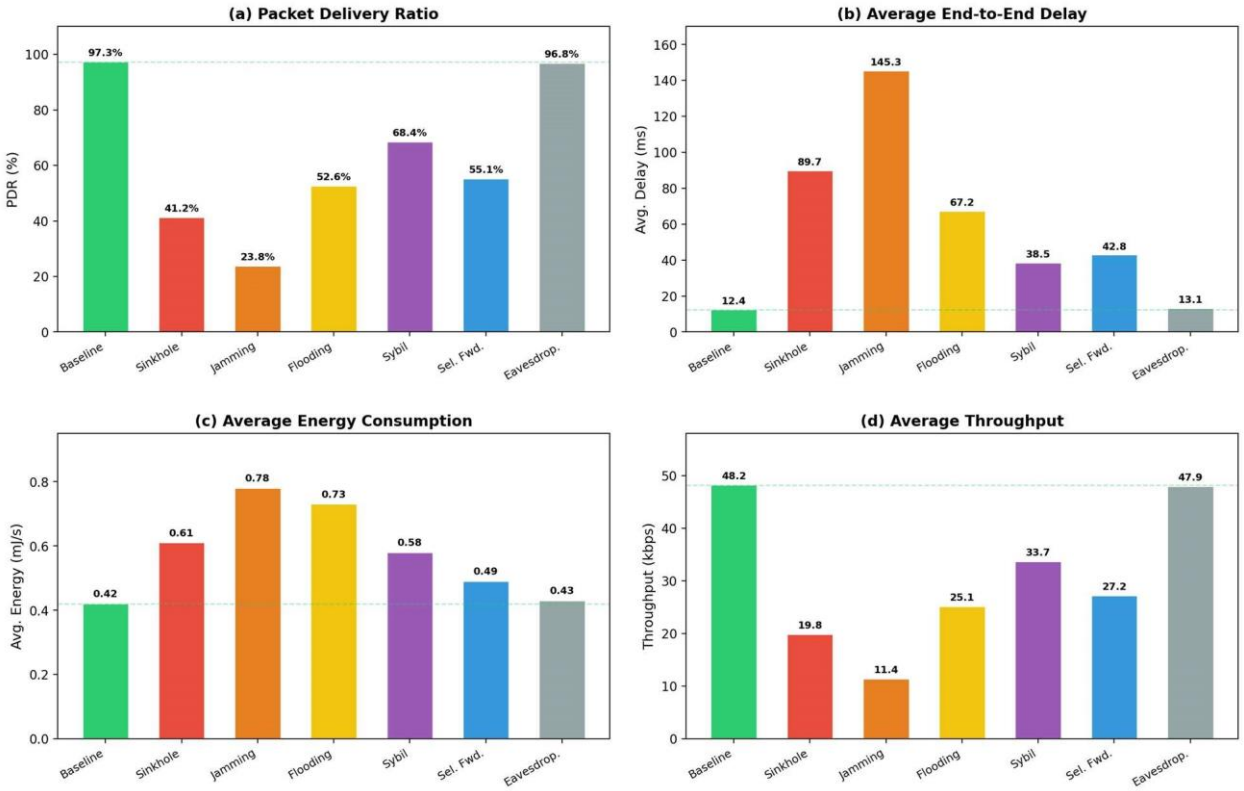

Figure 3. Simulation results: impact of six attack scenarios on WBAN performance metrics.

f. Limitations

Despite its contributions, the proposed model presents several limitations. First, although the validation has been extended to thirty-two attacks drawn from multiple independent taxonomies [5][8], the model does not yet account for emerging or zero-day threats such as attacks on Bluetooth Low Energy protocols, side-channel attacks on implanted devices, or advanced persistent threats targeting wearable medical systems. Second, while the model now supports multiimpact vectors listing all affected CIA properties, it does not quantify the relative severity or probability of each impact, which would be necessary for formal risk assessment. Third, the model remains descriptive and static, without incorporating temporal or dynamic aspects of network behavior such as attack progression or time-dependent vulnerability windows. Fourth, while the OMNeT++/Castalia simulation validates the model for six representative attacks under controlled conditions, extending the experimental validation to all thirty-two attacks and to dynamic multi-attack scenarios would further strengthen the empirical grounding. Deployment in a real clinical testbed with physical medical sensors remains an important next step. Future work should address these limitations through simulation-based validation, severity quantification within the multi-impact framework, and integration with real-time machine learning-based detection mechanisms.

IV. Conclusion

This paper has presented a multidimensional classification model for security vulnerabilities in medical wireless sensor networks, addressing a significant gap in the existing literature. The proposed model, formalized as V = (L, R, I), integrates three complementary dimensions, namely network layer, targeted resource, and security impact, with support for multiimpact representation, to provide a structured and comprehensive framework for vulnerability analysis in healthcare IoT environments.

Through the systematic mapping of thirty-two well-documented attacks drawn from independent taxonomies, the model demonstrated both completeness and discriminability. The results highlighted the network layer as the most vulnerable point, availability and integrity as the most compromised security properties, and data as the most targeted resource in medical WSNs. These findings have direct implications for the design and prioritization of security mechanisms in next-generation IoMT systems.

The experimental validation using OMNeT++/Castalia confirmed that the V = (L, R, I) vectors correctly predict the observable impact of attacks on network performance metrics, with multi-impact attacks producing the most severe degradation. Future work will focus on extending the simulation to all thirty-two attacks, incorporating dynamic and temporal dimensions, and integrating the model into machine learning-based intrusion detection systems for real-time vulnerability detection in clinical settings.

References

[1] Jian, W., Tabassum, A., & Li, J. P. (2024). Systematic survey on data security in wireless body area networks in IoT healthcare system. Frontiers in Medicine, 11, 1422911.

[2] Mehmood, G., Khan, M. Z., Bashir, A. K., Al-Otaibi, Y. D., & Khan, S. (2023). An efficient QoS-based multi-path routing scheme for smart healthcare monitoring in wireless body area networks. Computers and Electrical Engineering, 109, 108517.

[3] Thamilarasu, G., Odesile, A., & Hoang, A. (2020). An intrusion detection system for Internet of Medical Things. IEEE Access, 8, 181560-181576. [4] Kaleem, S., & Khan, I. A. (2024). A comprehensive survey on intrusion detection in Internet of Medical Things: Datasets, federated learning, blockchain, and future research directions. Journal of Network and Computer Applications, 232, 104020.

[5] Almomani, A., & Al-Nawasrah, A. (2022). Wireless body area network (WBAN): A survey on architecture, technologies, energy consumption, and security challenges. Journal of Sensor and Actuator Networks, 11(4), 67.

[6] Shambharkar, P., & Sharma, N. (2024). Deep learning-empowered intrusion detection framework for the Internet of Medical Things environment. Knowledge and Information Systems, 66(10), 6001-6050.

[7] Aljuhani, A., Alamri, A., Kumar, P., & Jolfaei, A. (2024). Optimized intrusion detection for IoMT networks with tree-based machine learning and filter-based feature selection. Sensors, 24(17), 5712.

[8] Bengag, A., Bengag, A., & Moussaoui, O. (2021). Classification of security attacks in WBAN for medical healthcare. Proceedings of the 4th International Conference on Networking, Information Systems & Security. https://doi.org/10.1145/3454127.3456605.

[9] Hajar, M., Al-Kadri, M., & Kalutarage, H. (2021). A survey on wireless body area networks: architecture, security challenges and research opportunities. Comput. Secur., 104, 102211. https://doi.org/10.1016/j.cose.2021.102211.

[10] Ali, Q., Malik, A., Rehman, W., Haseeb, M., & Salam, T. (2025). Security Issues and Research Opportunities in Wireless Body Area Networks. International Journal of Innovations in Science and Technology. https://doi.org/10.33411/ijist/20257318811894.

[1] Jian, W., Tabassum, A., & Li, J. (2024). Systematic survey on data security in wireless body area networks in IoT healthcare system. Frontiers in Medicine, 11. https://doi.org/10.3389/fmed.2024.1422911.

[12] Ayub, K., & AlShawa, R. (2024). Threat Modelling and Security Enhancements in Wireless Body Area Networks for Smart Healthcare. Journal of Robotics and Automation Research. https://doi.org/10.33140/jrar.05.03.09.

[13] Rbah, Y., Mahfoudi, M., Balboul, Y., Fattah, M., Mazer, S., Elbekkali, M., & Bernoussi, B. (2022). Machine learning and deep learning methods for intrusion detection systems in IoMT: A survey. In Proceedings of the 2022 International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), pp. 1-9.

[14] Jabeen, T., Ashraf, H., Khatoon, A., Band, S. S., & Mosavi, A. (2020). A lightweight genetic based algorithm for data security in wireless body area networks. IEEE Access, 8, 183460-183469.

[15] Rehman, Z. U., Altaf, S., & Iqbal, S. (2020). An efficient lightweight key agreement and authentication scheme for WBAN. IEEE Access, 8, 175385-175397.

[16] Dadkhah, S., Carlos Pinto Neto, E., Ferreira, R., Chukwuka Molokwu, R., Sadeghi, S., & Ghorbani, A. A. (2024). CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT. Internet of Things, 28, 101351. https://doi.org/10.1016/j.iot.2024.101351.

[17] Amin, Y. M., Abdel-Hamid, A. T. (2016). Classification and Analysis of IEEE 802.15.4 MAC Layer Attacks. In Proceedings of the International Conference on Communication, Management and Information Technology, pp. 74-79.

[18] Ozcelik, M. M., Kok, I., & Ozdemir, S. (2025). A survey on Internet of Medical Things (IoMT): enabling technologies, security and explainability issues, challenges, and future directions. Expert Systems, 42, e70010. https://doi.org/10.1111/exsy.70010.

[19] Boulis, A. (2011). Castalia: A simulator for Wireless Sensor Networks and Body Area Networks, version 3.3. NICTA, based on OMNeT++. Available: https://github.com/boulis/Castalia.

[20] Kaleem, S., & Khan, I. A. (2025). A comprehensive survey on intrusion detection in Internet of Medical Things: Datasets, federated learning, blockchain, and future research directions. Journal of Network and Computer Applications, 234, 104096. https://doi.org/10.1016/j.jnca.2024.104020. [21] Almomani, A., & Al-Nawasrah, A. (2022). Wireless body area network (WBAN): A survey on architecture, technologies, energy consumption, and security challenges. Journal of Sensor and Actuator Networks, 11(4), 67. https://doi.org/10.3390/jsan11040067.