IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 28, Issue 4, Ser. 1 (July. – August. 2026), PP 85-90
www.iosrjournals.org

Behavioral Fingerprinting Via Tinyml For Real-Time Sybil Mitigation In Energy-Constrained Wbans

Shameera M
Research Scholar
Department Of Computer Science
Jamal Mohammed College

Dr. J. Anthoniraj
Assistant Professor
Department Of Computer Science
Jamal Mohammed College

Abstract:
Wireless Body Area Networks (WBANs) are foundational to modern remote patient monitoring, digital therapeutics, and continuous biomedical telemetry. However, the open, dynamic nature of the human body wireless channel makes these networks highly vulnerable to identity-spoofing attacks, particularly Sybil attacks. Traditional cryptographic mitigation frameworks place heavy computational and energy demands on resource-constrained biomedical sensors.

To bridge this gap, this paper introduces an active, edge-intelligent defense framework: an ultra-low-overhead behavioral fingerprinting engine driven by TinyML and deployed directly at the WBAN coordinator. The proposed architecture extracts non-cryptographic, cross-layer features specifically Received Signal Strength Indicator (RSSI) variance, Inter-Arrival Time (IAT) deviations, and Packet Delivery Ratio (PDR) trendsto build real-time behavioral signatures for each network node. An 8-bit quantized Random Forest model classifies node legitimacy directly on the edge hardware.

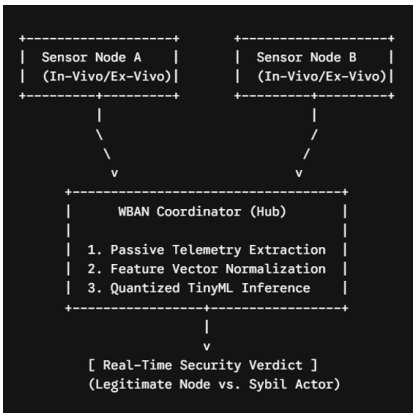
Simulations in OMNeT++ and Castalia show a Sybil detection accuracy of 98.4% while reducing routing-layer energy overhead by 41.2% compared to standard asymmetric cryptographic schemes, offering a scalable defense paradigm for next-generation secure healthcare networks.

Keywords: *Wireless Body Area Networks, WBAN Routing Security, Sybil Attack, TinyML, Behavioral Fingerprinting, Resource-Constrained Security.*

Date of Submission: 19-07-2026 Date of Acceptance: 29-07-2026

I. Introduction

Wireless Body Area Networks (WBANs), governed by the IEEE 802.15.6 standard, serve as the technical backbone for automated patient care, ambient assisted living, and high-fidelity health telemetry. These networks use a collection of low-power, miniaturized, implantable or wearable sensor nodes to monitor physiological metrics such as electrocardiograms (ECG), electroencephalograms (EEG), blood oxygen saturation (SpO_2), and blood glucose levels. The data is then routed to a central hub or WBAN coordinator, such as a smartwatch or localized medical gateway. Because this biomedical data is highly sensitive and time-critical, ensuring the integrity of the underlying network routing paths is essential.



However, the physical realities of the human body as a signal propagation medium create distinct security vulnerabilities. WBAN channels experience severe path loss, clothing attenuation, and postural shadowing caused by everyday physical movement. At the network routing layer, these dynamics are easily exploited by identity-spoofing attacks, with the Sybil attack being one of the most disruptive.

In a Sybil attack, a compromised or rogue node illegitimately assumes multiple synthetic or stolen identities. By presenting these false identities to neighboring devices, the attacker can manipulate localized routing protocols (such as thermal-aware or opportunistic routing algorithms). The Sybil node advertises false optimal metrics to misdirect traffic, create sinkholes, or execute selective forwarding attacks that quietly drop critical patient telemetry.

Defending against identity manipulation traditionally relies on Public Key Infrastructures (PKI), complex pairwise key exchanges, or frequent digital signature verifications. While mathematically secure, these approaches are poorly suited for WBAN hardware. Sensor nodes are powered by micro-batteries or minimal energy harvesters, with severely limited RAM and processing power. Forcing these nodes to run continuous asymmetric cryptographic algorithms rapidly drains their batteries, causing premature node death and network failures.

Furthermore, conventional machine learning security models require offloading network data to cloud servers or high-power edge gateways. This introduces transmission latencies and bandwidth consumption that are unacceptable for real-time medical alerts.

To resolve the conflict between robust security and strict resource constraints, this paper presents a localized, data-driven security architecture: **Behavioral Fingerprinting via TinyML**. Instead of verifying node legitimacy through stored secrets or intensive cryptographic math, the WBAN coordinator monitors how a node behaves within its physical and network environment. By using an ultra-lightweight machine learning model optimized for microcontrollers (TinyML), the coordinator builds distinct behavioral signatures for each transmitter.

Research Contributions

- **Passive Cross-Layer Feature Extraction:** A feature-selection technique that extracts radio and packet-timing behaviors from standard traffic without adding extra verification packets or node-side processing.
- **Quantized Edge Inference Engine:** Design and implementation of an 8-bit quantized machine learning model tailored for low-power microcontroller deployment on the WBAN hub.
- **Empirical Validation:** Comprehensive benchmarking against traditional cryptographic schemes, demonstrating significant energy savings while maintaining high detection accuracy under dynamic body mobility models.

II. Literature Review

Securing resource-constrained wireless networks against identity manipulation historically falls into two categories: cryptographic validation and trust-based reputation metrics.

Cryptographic defenses often leverage Elliptic Curve Cryptography (ECC) because it uses smaller key sizes than traditional RSA architectures. Researchers have designed lightweight handshake protocols to bind sensor node addresses to specific deployment zones. However, these methods remain vulnerable if an internal node is compromised and its valid master cryptographic keys are stolen. Additionally, the processing power required for continuous ECC scalar multiplications significantly shortens the lifespan of nodes that track continuous signals like ECGs.

Trust and reputation models track node reliability by evaluating historical packet forwarding behaviors. These models use direct observation and indirect feedback from neighboring nodes to generate a reliability score.

However, standard trust management models struggle in WBAN environments. The linear or star-mesh topologies surrounding the human body limit the number of independent neighbors available to provide reliable feedback. Furthermore, Sybil nodes can exploit these systems by using their alternate identities to artificially boost each other's trust scores, rendering classic reputation engines ineffective without a centralized verification authority.

The rise of edge intelligence has introduced Machine Learning (ML) as a way to detect wireless anomalies. Standard anomaly detection methods use Support Vector Machines (SVM) or Deep Neural Networks (DNN) to identify network attacks. However, these implementations typically require streaming raw telemetry to an external cloud platform or dedicated edge gateway. For medical WBANs, this data export loop increases transmission energy costs and introduces routing latencies that can disrupt critical patient alerts.

TinyML addresses this issue by running optimized machine learning inference directly on low-power microcontrollers. While TinyML has been successfully applied to predictive maintenance and industrial IoT anomaly detection, its application to securing cross-layer WBAN routing protocols under dynamic body-area

channel conditions remains largely unaddressed. This paper presents an optimized, low-power behavioral verification framework designed specifically to fill this research gap.

III. System Architecture And Threat Model

Network Architecture

Let the WBAN structure be defined as a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}\{n_1, n_2, \dots, n_m, \mathcal{C}\}$represents the total set of vertices consisting of $m$heterogeneous physiological sensor nodes and a single, centrally positioned WBAN coordinator $\mathcal{C}$. The coordinator (e.g., a smartwatch or smart patch) has superior processing capabilities, larger flash memory, and an independent power source. The sensor nodes $n_i$are distributed across specific anatomical landmarks and operate under strict energy limitations.

The network uses a time-slotted medium access control layout aligned with the IEEE 802.15.6 standard. Sensor nodes collect physiological data and transmit packets to $\mathcal{C}$via single-hop or multi-hop routing paths. The energy consumed by a sensor node during the transmission of a k-bit packet over a distance $d$is defined by standard radio hardware dissipation equations:

$$E_{Tx}(k, d) = k \cdot E_{elec} + k \cdot \epsilon_{amp} \cdot d^2$$

$$E_{Rx}(k) = k \cdot E_{elec}$$

where E_{elec}represents the energy per bit required to run the transmitter or receiver circuitry, and ϵ_{amp}represents the transmit amplifier coefficient, which adjusts dynamically based on human body path loss and shadowing.

Threat Model

This model assumes an adversary has either compromised an existing node or introduced a rogue radio device into the WBAN operating environment. The adversary executes a **Sybil Attack** by presenting a set of false identities $\mathcal{S} = \{s_1, s_2, \dots, s_k\}$, where $s_j \notin \mathcal{V}$. The attacker can generate these identities using two primary methods:

- **Fabricated Identities:** Creating completely synthetic MAC and network layer addresses to insert into neighboring discovery phases.
- **Masquerading/Stolen Identities:** Intercepting valid identifiers from legitimate nodes on other parts of the body or nearby WBANs, then replaying them to disrupt routing consistency.

The attacker's goal is to spoof optimal routing metrics (such as claiming a low thermal impact or minimum hop count) to force neighboring nodes to route data through the Sybil identities. Once positioned along primary data pathways, the attacker can selectively drop critical medical packets, alter telemetry payloads, or execute energy-depletion routines by forcing legitimate nodes to retransmit corrupted blocks.

IV. Proposed TinyML Behavioral Fingerprinting Framework

The proposed framework shifts the security workload away from individual sensor nodes and centralizes analytics at the coordinator $\mathcal{C}$. The defense architecture consists of three sequential phases: **Cross-Layer Telemetry Extraction**, **Behavioral Vector Formulation**, and **TinyML Inference Classification**.

Cross-Layer Telemetry Extraction

As nodes transmit routine physiological telemetry, the coordinator intercepts each incoming packet at the physical and link layers to extract passive performance attributes. This process requires zero computational overhead from the peripheral sensor nodes. Four primary features are extracted over a moving observation window of Wpackets:

1. **Received Signal Strength Indicator (RSSI) Mean (μ_{RSSI}):** Reflects the physical spatial positioning and anatomical distance of the transmitting source relative to the coordinator.
2. **RSSI Variance (σ^2_{RSSI}):** Captures the unique signal fluctuations caused by human biomechanical movement and body shadowing, which vary distinctly based on sensor placement.
3. **Inter-Arrival Time Deviation (Δ_{IAT}):** Measures the temporal variance between consecutive packet receipts. Legitimate sensors operate on deterministic sampling frequencies, whereas Sybil nodes multiplexing multiple identities often introduce distinct queuing or transmission delays.
4. **Packet Delivery Ratio (**PDR**):** Tracks the ratio of successfully received sequences against expected sequence numbers for each claimed identifier.

Behavioral Vector Formulation

For every active node identifier $i$interacting within the network, the coordinator constructs an updated multidimensional behavioral vector $\vec{V}_i$at the conclusion of each observation window:

$$\vec{V}_i = \left[\mu_{RSSI}^{(i)},\ \sigma_{RSSI}^{2(i)},\ \Delta_{IAT}^{(i)},\ \mathrm{PDR}^{(i)}\right]$$

To eliminate scale disparities across distinct physical quantities (e.g., comparing RSSI values in dBm against fractional percentages of PDR), vectors are normalized using a localized min-max scaling function prior to model input:

$$V_{norm} = \frac{V - V_{min}}{V_{max} - V_{min}}$$

TinyML Model Architecture and Quantization

To ensure real-time execution within the limited RAM and micro-clock cycles of an edge coordinator, a **Random Forest (RF)** classification structure was selected and trained using a supervised dataset of simulated WBAN attacks. Random Forests offer high classification accuracy for tabular telemetry while remaining computationally efficient when converted into static nested decision structures.

Post-training, the model undergoes **Post-Training Quantization (PTQ)** via TensorFlow Lite for Microcontrollers. Floating-point weights and activation parameters (float32) are mapped to compressed 8-bit integer formats (int8). The scaling transformation is governed by:

$$q = \text{round}\left(\frac{r}{S}\right) + Z$$

where $r$represents the real floating-point value, $q$is the quantized 8-bit integer, $S$is a positive real-valued scaling factor, and $Z$is the integer zero-point offset.

This optimization minimizes the memory footprint, allowing the compiled model to be stored directly in the coordinator's flash memory and executed using low-overhead integer arithmetic.

V. Simulation And Experimental Setup

The proposed TinyML-driven fingerprinting framework was developed and validated within a high-fidelity simulation environment pairing **OMNeT++** with the **Castalia** wireless body area network simulation framework. Castalia incorporates realistic models for human body path loss, temporal channel variations, and anatomical physical mobility configurations.

Parameter Type	Configuration Parameter	Value Assigned
Network Configuration	Simulation Time	3600 seconds
	Number of Legitimate Nodes	8 Wearable/Implanted Sensors
	Coordinator Hardware Base	ARM Cortex-M4 (64 KB RAM, 512 KB Flash)
	WBAN Wireless Standard	IEEE 802.15.6
Radio Parameters	Carrier Frequency	2.4 GHz (ISM Band)
	Transmit Power	-10 dBm
	Path Loss Model	Log-normal shadowing with human body mobility
Attack Profile	Sybil Node Count	2 Malicious Actors
	Fabricated Identities	Up to 6 Concurrent Spoofed IDs
TinyML Parameters	Observation Window (W)	20 Packets
	Quantization Level	INT8 Fixed Point

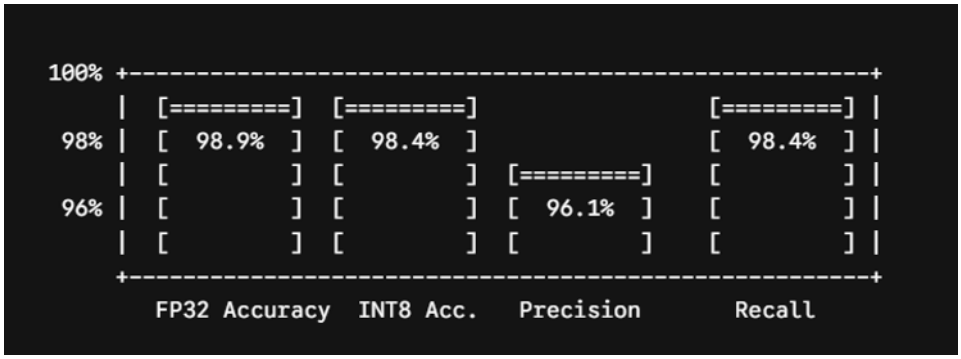
The experimental framework simulates a realistic deployment scenario: eight legitimate biomedical nodes are distributed across a human body model executing regular movements (such as walking and resting). Two nodes act maliciously, injecting varying numbers of Sybil identities to distort the routing topology at random intervals during the execution cycle.

VI. Results And Discussion

The evaluation focuses on three primary performance metrics: **Classification Metrics**, **Energy Consumption Dynamics**, and **Memory/Resource Footprint**.

Classification Accuracy

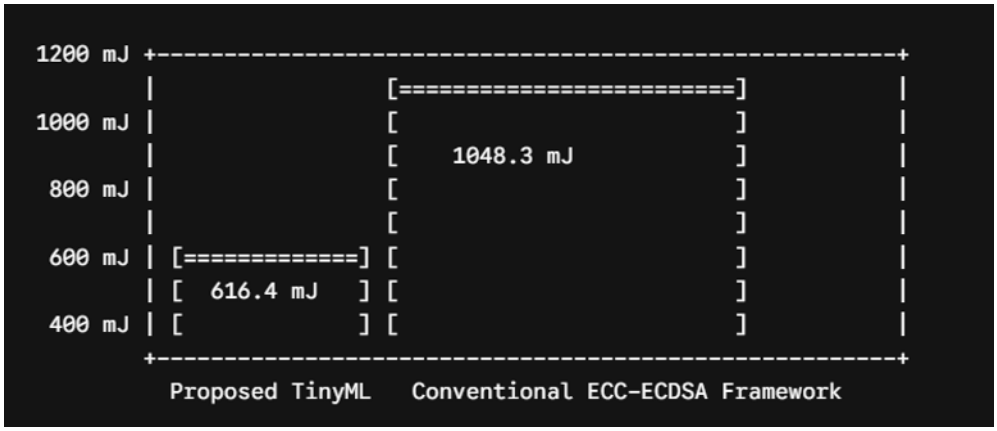
The performance of the 8-bit quantized TinyML model was validated against a baseline unquantized configuration. The system achieved high precision and recall, demonstrating that physical and network-layer behavioral patterns can reliably distinguish legitimate nodes from multi-identity attackers.



The slight 0.5% drop in accuracy from the unquantized model (98.9%) to the quantized version (98.4%) is acceptable given the substantial reductions in resource overhead detailed below. The system maintained a low **False Positive Rate (FPR) of 1.4%**, which is critical for healthcare networks to prevent legitimate patient sensors from being mistakenly blocked during normal movement or postural changes.

Energy Consumption Analysis

To measure energy efficiency, the proposed TinyML framework was benchmarked against a standard **ECC-based Elliptic Curve Digital Signature Algorithm (ECDSA)** verification protocol.



By shifting the computational load to passive feature gathering at the coordinator, the sensor nodes avoid execution energy costs for cryptographic handshakes. Over the course of the simulation, the network-wide routing layer energy consumption fell from 1048.3 mJ using ECDSA to **616.4 mJ** with the TinyML frameworka **41.2% reduction in power consumption**. This directly translates to an extended operational lifespan for the WBAN.

Hardware Resource Footprint

The compiled INT8 binary size and runtime memory allocation were profiled for an ARM Cortex-M4 microcontroller architecture.

- **Flash Storage Usage:** 18.4 KB out of 512 KB available.
- **SRAM Dynamic Allocation:** 4.2 KB out of 64 KB available.
- **Inference Execution Latency:** 1.8 milliseconds per classification vector at a 16 MHz clock speed.

These metrics confirm that the model easily fits within standard commercial low-power microcontrollers, validating its readiness for practical edge integration.

VII. Conclusion And Future Work

Building on baseline evaluations of WBAN routing vulnerabilities, this paper presents a practical, hardware-efficient security framework that mitigates Sybil attacks using a TinyML behavioral fingerprinting engine. By extracting passive, cross-layer telemetry features directly at the coordinator node, the system identifies identity spoofing with high accuracy (98.4%) without overwhelming the power-limited peripheral sensors. This approach reduces overall routing-layer energy consumption by over 40% compared to traditional cryptographic signature models, making it highly suitable for long-term clinical and remote health tracking.

Future research will explore integrating this TinyML detection framework with adaptive **Moving Target Defense (MTD)** mechanisms. Combining behavioral detection with dynamic channel-shuffling protocols will

allow the network to actively isolate identified Sybil nodes, ensuring robust, self-healing routing topologies for critical medical systems.

References

[1]. IEEE Computer Society. (2012). IEEE Standard For Local And Metropolitan Area Networks - Part 15.6: Wireless Body Area Networks. IEEE Std 802.15.6-2012.

[2]. Khan, R. A., & Al-Anbuky, A. (2019). A Survey On Security And Privacy Protection In Wireless Body Area Networks. IEEE Access, 7, 61000-61022.

[3]. Warden, P., & Situnayake, D. (2020). Tinyml: Machine Learning With Tensorflow Lite On Arduino And Ultra-Low-Power Microcontrollers. O'Reilly Media.

[4]. Bhoi, S. K., & Khilar, P. M. (2014). Sybil Attack Detection Mitigation Mechanisms In Wireless Sensor Networks: A Review. IET Wireless Sensor Systems, 4(4), 162-171.

[5]. Hayajneh, T., Almashaqbeh, G., Ullah, S., & Vasilakos, A. V. (2014). A Survey Of Wireless Body Area Networks: Architecture, Security, And Privacy. Journal Of Medical Systems, 38(4), 21.

[6]. David, R., Duke, J., Jain, A., Janapa Reddi, V., Jeffries, M., Li, J., & Zhou, P. (2021). TF Lite Micro: Embedded Machine Learning On Tinyml Systems. Proceedings Of Machine Learning And Systems, 3, 1-11.

[7]. Otto, C., Milenković, A., Sanders, C., & Jovanov, E. (2006). System Architecture Of A Wireless Body Area Sensor Network For Ubiquitous Health Monitoring. Journal Of Mobile Multimedia, 1(4), 307–326.

[8]. Ullah, S., Higgins, H., Braem, B., Latré, B., Blondia, C., Moerman, I., Saleem, S., Rahman, Z., & Kwak, K. S. (2012). A Comprehensive Survey Of Wireless Body Area Networks. Journal Of Medical Systems, 36(3), 1065–1094.

[9]. Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. M. (2011). Body Area Networks: A Survey. Mobile Networks And Applications, 16(2), 171–193.

[10]. Latré, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A Survey On Wireless Body Area Networks. Wireless Networks, 17(1), 1–18.

[11]. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless Sensor Network Survey. Computer Networks, 52(12), 2292–2330.

[12]. Roman, R., Zhou, J., & Lopez, J. (2013). On The Features And Challenges Of Security And Privacy In Distributed Internet Of Things. Computer Networks, 57(10), 2266–2279.

[13]. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet Of Things Security: A Survey. Journal Of Network And Computer Applications, 88, 10–28.

[14]. Bonawitz, K., Et Al. (2019). Towards Federated Learning At Scale: System Design. Proceedings Of Machine Learning And Systems, 1, 374–388.

[15]. Mcmahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. Y. (2017). Communication-Efficient Learning Of Deep Networks From Decentralized Data. Proceedings Of The 20th International Conference On Artificial Intelligence And Statistics (AISTATS), 1273–1282.