WATCHGUARD: Wearable Advanced Tactical Communication and Health Monitoring for Military Applications

Abhigna Police, Sai Nikhil Gampa, Sathwik Chowdary Merla, Snigdha Pannir
Department of Electrical and Computer Engineering
Northeastern University, Boston, MA
police.ab@northeastern.edu, gampa.sa@northeastern.edu, merla.s@northeastern.edu, pannir.sn@northeastern.edu,

***Abstract*—Modern military missions require continuous monitoring of soldier health, stress levels, movement patterns, and geolocation, especially in hostile or infrastructure-denied environments [1]. Existing solutions typically operate as isolated components—either focusing on wearable sensing, local communication, or satellite relaying—without providing an integrated architecture capable of ensuring reliable beyond-line-of-sight (BLOS) visibility for command units [2]. To address this gap, we present WATCHGUARD, a hierarchical IoT–SATCOM framework that combines wearable physiological sensing, long-range LoRa communication, CCSDS-compliant satellite uplinks, and machine-learning-based anomaly detection for tactical soldier safety monitoring.**

The system architecture includes a low-power wearable node that transmits health and motion telemetry to a mobile base node using LoRa modulation, leveraging its proven performance in military field environments [3]. The base node aggregates and compresses telemetry into CCSDS-structured packets suitable for SATCOM transport, enabling BLOS connectivity even under degraded local communication conditions [4]. To detect critical soldier states—such as panic, fall events, and injury—an XGBoost classifier was trained using synthetic physiological datasets modeled from soldier behavior scenarios [5].

An ns-3 simulation environment was developed to evaluate network performance under realistic channel conditions, including path loss, interference, and satellite buffer constraints. Results demonstrate a high Packet Delivery Ratio (97.78%), low average latency (8.71 ms), and stable SATCOM buffering across mobility scenarios. The anomaly-detection model achieved strong performance, with AUC values exceeding 0.98 across all critical event classes. These findings indicate that hybrid IoT–SATCOM architectures can significantly enhance real-time soldier monitoring and mission readiness in modern battlefield operations [6].

I. Introduction

Modern military missions increasingly rely on continuous visibility into a soldier's health, movement, and location, especially in environments where communication infrastructure is damaged, unavailable, or actively jammed. In such conditions, commanders require real-time information to make quick decisions about evacuation, medical support, and troop coordination. The growth of the Internet of Battle Things (IoBT) underscores this need for resilient sensing and communication technologies that can operate under adversarial constraints [6].

Wearable devices have been used extensively in healthcare and industrial safety to monitor heart rate, motion, and stress, but adapting these systems for battlefield use introduces unique challenges. Devices must operate on low power, withstand harsh environments, and communicate reliably over long distances without relying on cellular or Wi-Fi networks. Prior soldier-monitoring systems using IoT and GPS have demonstrated feasibility, but often fail to maintain communication in obstructed or contested terrains [1].

Long-range, low-power technologies such as LoRa have shown strong potential for connecting wearable sensors to nearby tactical nodes. Field studies highlight LoRa's ability to maintain communication across several kilometers and through dense obstacles, making it suitable for military deployments [3]. Additional evaluations confirm that LoRa-based networks sustain high packet delivery even under interference and mobility [4].

However, local radio links alone cannot provide commanders with beyond-line-of-sight (BLOS) visibility. Satellite communication remains the most reliable option for transmitting aggregated soldier data from the field to remote command centers. CCSDS standards provide the packet structure and error-control mechanisms necessary for robust satellite uplinks in challenging channel conditions [7].

To address these needs, we introduce WATCHGUARD — a multi-tier system combining wearable sensing, LoRa communication, CCSDS-compliant satellite relays, and machine-learning-based detection of critical events. By integrating IoT, SATCOM, and AI, WATCHGUARD aims to provide continuous and reliable soldier monitoring even when traditional infrastructure is unavailable.

II. Background and Related Work

Monitoring soldier health and operational status has become a critical priority as modern battlefields grow more unpredictable and communication infrastructure becomes increasingly vulnerable. The Internet of Battle Things (IoBT) framework emphasizes distributed sensing, autonomous decision-making, and resilient communication systems capable of functioning under adversarial conditions [6]. These requirements demand wearable systems that can collect meaningful physiological and motion data while operating with extremely low power and high reliability.

Wearable sensing platforms have been widely applied in healthcare and sports contexts, where devices monitor heart rate, oxygen saturation, and activity levels. However, adapting these technologies to defense environments introduces stricter constraints, including harsh environmental exposure, limited energy availability, long-range communication needs, and the possibility of GPS or network denial. Prior IoT-based soldier-tracking studies demonstrated the potential of vitals-based monitoring but also highlighted reliability issues in dense forests, mountainous terrain, and obstructed environments [1].

Long-range, low-power modulation schemes such as LoRa have proven effective for tactical deployments due to their multi-kilometer range and robustness to shadowing. Experimental studies show that LoRa networks maintain reliable packet delivery even under interference and mobility, making them well suited for wearable-to-base communication in dispersed troop formations [3], [4]. These findings motivate our selection of LoRa as the Tier-1 communication layer.

In parallel, machine-learning approaches—particularly tree-based and ensemble models—have demonstrated strong performance in detecting falls, stress, fatigue, and anomalous motion patterns across both clinical and field datasets. Research highlights the importance of temporal features such as heart-rate variability (HRV) and accelerometer-derived statistics in achieving high detection accuracy [5]. These insights guide the design of our anomaly-detection pipeline.

For beyond-line-of-sight (BLOS) communication, satellite systems remain the most reliable option, especially in scenarios where terrestrial communication is unavailable or compromised. The Consultative Committee for Space Data Systems (CCSDS) provides standardized packet structures, framing rules, and channel-coding techniques that ensure robust long-distance data transfer [7]. These standards form the foundation of our Tier-2 communication layer, enabling dependable uplinks from field base nodes to remote command centers.

While previous research explores wearable sensing, LoRa communication, satellite transport, and ML-based health monitoring independently, few systems integrate all components into a unified, battlefield-ready architecture. WATCHGUARD addresses this gap by combining multi-tier communication, CCSDS framing, and real-time analytics into a cohesive and resilient soldier-monitoring system.

III. System Architecture

WATCHGUARD follows a three-tier communication design that ensures reliable sensing, local aggregation, and beyond-line-of-sight (BLOS) visibility during military operations. This layered architecture maintains connectivity even when traditional communication infrastructure is unavailable or compromised.

A. Tier 1: Wearable Sensor Unit

Each soldier carries a compact wearable device responsible for monitoring heart rate, SpO_2, motion patterns, and fall indicators. To ensure long battery life and minimal radio exposure, the wearable transmits only small periodic packets using long-range, low-power LoRa modulation. LoRa's proven resilience in obstructed tactical environments makes it suitable for platoon-level deployments [4], [3]. Basic preprocessing filters noise and sends only essential physiological features to the next tier.

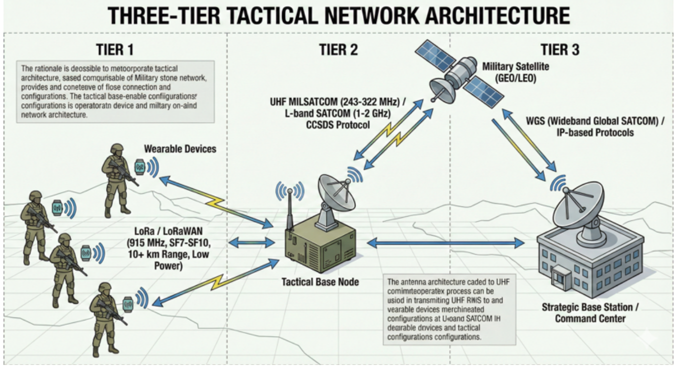

THREE-TIER TACTICAL NETWORK ARCHITECTURE
TIER 1
TIER 2
TIER 3
The rationale is deossible to metoorporate tactical architecture, sased comqurisable of Military stone network, provides and conetesve of flose connection and configurations. The tactical base-enable confiigurationsr configurations is operatoratn device and miltary on-aind network architecture.
Military Satellite (GEO/LEO)
UHF MILSATCOM (243-322 MHz) / L-band SATCOM (1-2 GHz) CCSDS Protocol
WGS (Wideband Global SATCOM) / IP-based Protocols
Wearable Devices
LoRa / LoRaWAN (915 MHz, SF7-SF10, 10+ km Range, Low Power)
Tactical Base Node
The antenna architecture caded to UHF comimiteoperatex process can be usiod in transmiting UHF RMS to and vearable devices merchineated configurations at Uoand SATCOM IH deairable dnvices and tactical configurations configurations.
Strategic Base Station / Command Center

Fig. 1. Three-tier WATCHGUARD network architecture consisting of Tier-1 wearable sensors, Tier-2 tactical base node, and Tier-3 satellite-to-command communication path.

B. Tier 2: Tactical Base Node

The base node acts as the intermediate hub for all soldiers within a 2–10 km radius. It receives LoRa packets from multiple wearables, aggregates and compresses soldier telemetry, and performs real-time local assessment (e.g., fall detection or abnormal HR events). Two key responsibilities of this tier are:

- **Local situational awareness**: Immediate alerts are raised for squad leaders without requiring satellite uplink.
- **Data buffering and framing**: The node prepares outbound data using CCSDS-style structured packets for satellite transmission.

This reduces bandwidth dependency and ensures resilience during temporary link outages.

C. Tier 3: Satellite Communication Layer

Once aggregated data is ready, the base node forwards soldier telemetry to a satellite link using CCSDS-compliant framing concepts [7]. These standardized packet structures enhance reliability under poor signal conditions and allow seamless integration with legacy SATCOM ground infrastructure. The satellite relays information to the remote command center, enabling real-time troop monitoring even when ground infrastructure is jammed, destroyed, or unavailable.

D. Command Center Interface

The command center provides a unified operational picture: troop locations, vitals, alerts, and communication health. AI-based anomaly detection models analyze the streamed data to identify fall events, stress indicators, or physiological anomalies. Operators can review individual soldier timelines, map overlays, and mission-level summaries.

IV. Network Interfaces

The WATCHGUARD system relies on three key communication interfaces that operate across progressively wider ranges: (i) the short-to-medium–range wearable link, (ii) the mid-range link between the base node and the satellite, and (iii) the long-range downlink interface to the command center. Each tier is designed to meet different reliability, energy, and

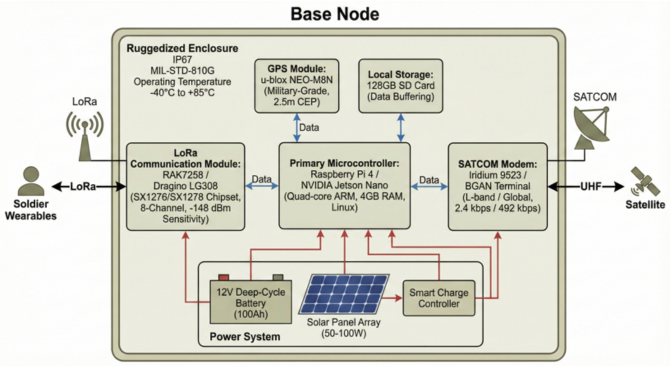


Fig. 2. Internal components of the Tier-2 base node, including the LoRa concentrator, SATCOM modem, GPS receiver, and ruggedized embedded controller.

latency requirements, allowing the system to function even when traditional infrastructure is not available.

A. Wearable to Base Node Interface

The Tier-1 interface connects each soldier's wearable to the nearby base node using LoRa modulation. LoRa was selected for its long-range, low-power characteristics, which have been widely validated for tactical and rural environments [4]. In our system, wearables transmit compact packets containing heart rate, SpO_2, accelerometer features, and GPS coordinates every few seconds.

A lightweight, UDP-like payload structure is used to minimize overhead and conserve battery life, while still supporting timely alert transmission during emergencies. Due to LoRa's spread spectrum properties, the system maintains connectivity even when soldiers move through dense forests, uneven terrain, or urban obstructions.

B. Base Node to Satellite Interface

The Tier-2 interface aggregates data from up to one hundred wearables and uplinks it via a SATCOM modem. This interface adheres to the Consultative Committee for Space Data Systems (CCSDS) telecommand and telemetry standards, which define packet headers, error correction coding, and framing schemes widely used in space communication [8].

Using CCSDS framing ensures that soldier data can be interpreted correctly by satellite ground infrastructure and supports interoperability with existing military satellite systems. The base node batches multiple wearable packets into a single CCSDS frame, greatly reducing satellite bandwidth consumption and improving resilience during short connectivity outages.

C. Satellite to Command Center Interface

The Tier-3 interface completes the communication chain by carrying aggregated soldier information from the satellite to the command center. Downlink data is decoded using CCSDS-compliant ground-station modules, after which soldier locations and alerts are reconstructed. The command dashboard highlights abnormal conditions—such as fall detection or elevated physiological stress—allowing commanders to respond rapidly even when troops are dispersed across multi-kilometer operational areas.

TABLE I
MEASURED NETWORK PERFORMANCE ACROSS TIER-1 AND TIER-2 COMMUNICATION LINKS.

Metric	Value
Packet Delivery Ratio (PDR)	97.78%
Average Latency	8.71 ms
Maximum SATCOM Buffer Usage	84.67 KB

These performance results demonstrate that the combination of LoRa and CCSDS-based SATCOM is capable of delivering reliable communication in environments with no supporting infrastructure, while keeping power consumption low enough for day-long soldier deployments.

V. PACKET CONFIGURATION

Efficient packet design is crucial for ensuring low-latency communication and minimizing bandwidth consumption across all three tiers of the WATCHGUARD architecture. The system therefore uses compact, domain-specific packet formats for the wearable-to-base link and CCSDS-compliant frames for satellite uplinks.

A. Tier 1: Wearable to Base Node Packet Format

Each soldier's wearable device transmits a lightweight 46-byte packet engineered to balance detail and energy efficiency. The packet contains only the most essential physiological and positional attributes required for health assessment and geolocation:

- **Soldier ID:** Unique 2-byte identifier used for troop-level aggregation.
- **Heart Rate and SpO_2:** Vital signs that support stress, injury, and fatigue assessment.
- **Accelerometer-Derived Features:** Values extracted from a rolling window to detect falls, high-impact motion, or abnormal activity.
- **GPS Coordinates:** Latitude/longitude encoded in compressed form to conserve airtime.
- **Timestamp:** Ensures temporal ordering of events when packets arrive out of sequence.

This minimal yet expressive structure supports real-time monitoring while enabling multi-hour battery life on low-power wearable hardware. Such compact formats are widely recommended in military IoT sensing systems to preserve energy and minimize interference [4].

B. Tier 2/3: Base Node to Satellite Packet Format

For SATCOM uplinks, the base node aggregates multiple wearable packets into a larger CCSDS-compliant frame. The final 572-byte CCSDS frame is organized as follows:

- **Primary Header (CCSDS):** Contains version, routing, and application identifiers as defined in the CCSDS Telemetry standard [9].

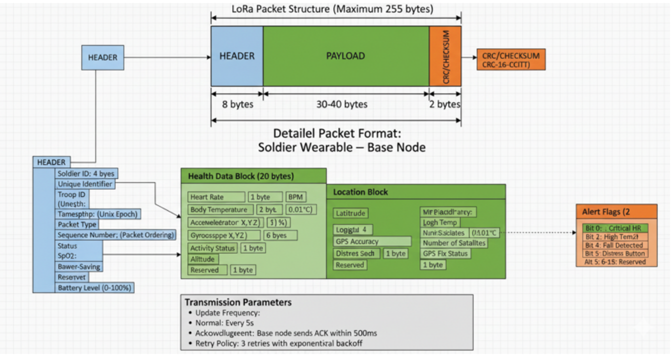


Fig. 3. Detailed packet structure used in the wearable-to-base LoRa link, including header fields, health data block, location block, and alert flags. This custom 46-byte format enables efficient low-power soldier monitoring.

- **Troop Metadata Block:** Includes mission identifiers, platoon information, and any priority flags.
- **Compressed Soldier Data Blocks:** Several wearable packets are merged together using delta encoding to eliminate redundant fields such as identical timestamps or static location coordinates.
- **Error Detection Footer:** CRC and optional FEC bits help mitigate bit errors introduced by long-distance satellite propagation.

Using CCSDS framing ensures interoperability with existing satellite infrastructure, allowing the WATCHGUARD system to function seamlessly over both GEO and LEO military communication networks. Furthermore, batching packets significantly reduces satellite bandwidth usage and limits congestion during high-activity scenarios.

The combined packet strategy—lightweight Tier-1 messages and structured Tier-2/3 CCSDS frames—optimizes both local communication reliability and long-range transmission efficiency across contested operational environments.

VI. Simulation Methodology

To evaluate the reliability and responsiveness of the WATCHGUARD architecture, we used a two-part methodology combining an ns-3 network simulation and a data-driven pipeline for soldier activity classification. This hybrid evaluation allows us to assess both communication performance and the accuracy of event detection under realistic operating assumptions.

A. ns-3 Network Simulation

The wearable-to-base LoRa link (Tier 1) was modeled in ns-3 using the LoRaWAN module configured with realistic propagation settings. LoRa parameters such as transmit power, spreading factor, and bandwidth were selected based on values demonstrated in prior long-range communication studies [4]. Soldiers were dispersed throughout a 2–10 km operational radius, each generating periodic telemetry packets carrying physiological data.

The simulation recorded key communication metrics including:

- **Packet Delivery Ratio (PDR)** — measures reliability under varying terrain and mobility.
- **End-to-End Latency** — the time between packet generation and base-node reception.
- **RSSI and SNR** — indicators of link quality across different distances.
- **Satellite Buffer Usage** — measured during simulated uplink outages.

A log-distance propagation model with additional shadowing was used to emulate forested, urban, and obstructed environments. Soldier mobility traces were included to reflect walking, running, and patrol-like movements that introduce dynamic link variation.

B. Satellite Uplink Modeling

While ns-3 does not provide a full SATCOM physical layer, we emulated the behavior of Tier-2/3 uplinks by applying bandwidth limits, random connectivity drops, and realistic latency spikes based on SATCOM–IoT integration studies [7]. The base node aggregated wearable packets into CCSDS-style frames, allowing us to study:

- how quickly the buffer fills during outages,
- the recovery time once satellite connectivity resumes,
- and the impact of data compression on bandwidth usage.

This approach provides a practical model of how the system behaves under real-world satellite constraints.

C. Synthetic Physiological Dataset

To support AI-driven health-state detection, a synthetic dataset was generated for twelve soldiers across five key activity states: *normal*, *running*, *panic*, *fall*, and *injured*. Each state was assigned distinct physiological characteristics informed by prior human-performance modeling and wearable-sensing studies [5]. The dataset included:

- heart rate and HRV patterns,
- SpO_2 behavior during stress and injury,
- accelerometer spikes and inactivity signatures for falls,
- and motion rhythms associated with panic or fatigue.

These signals were segmented into fixed-size windows and transformed into statistical and temporal features suitable for machine-learning classification.

D. Machine Learning Pipeline

The detection model uses XGBoost, chosen for its robustness with tabular data and strong performance under noisy conditions. The training pipeline consisted of:

1) feature extraction (mean, variance, range, HRV metrics),
2) normalization of continuous values,
3) SMOTE oversampling to address rare fall and injury events,
4) 80/20 training–testing split,
5) hyperparameter tuning (estimators, depth, learning rate),
6) evaluation using AUC, F1-score, and confusion matrices.

This methodology supports real-time inference at the base node, reducing reliance on satellite links for critical event detection.

VII. AI Model Architecture

The WATCHGUARD system uses a lightweight but expressive machine–learning model to classify soldier state from streaming physiological and motion data. The goal is to reliably detect critical events such as falls or health degradation while keeping the computation small enough to run at the base node in near real time.

A. Input Features and Windowing

Sensor streams from each soldier are grouped into 12-second rolling windows. Within each window, we compute a compact set of features that have been shown to correlate strongly with stress, fatigue, and fall events in prior wearable-sensing work [5]. The feature vector includes:

- basic statistics (mean, standard deviation, and range) of heart rate, SpO_2, and acceleration magnitude,
- heart rate variability (HRV) indicators derived from beat-to-beat intervals,
- a stress-to-HR ratio that highlights simultaneous elevation in heart rate and instability,
- binary flags for sudden acceleration spikes followed by inactivity, which are characteristic of falls.

This design keeps the feature space relatively small while preserving the temporal patterns needed for robust classification.

B. XGBoost Classifier Design

For both the *Fall_Detection* and *Health_Alert* tasks, we use gradient-boosted decision trees (XGBoost) as the core model. XGBoost is well suited for tabular, mixed-scale data and has been widely adopted in physiological and anomaly-detection applications due to its strong performance and low inference latency.

The model is configured with:

- 350 estimators (trees),
- learning rate of 0.03,
- maximum tree depth of 4.

These values were selected to balance accuracy and overfitting risk while keeping the model small enough for deployment on embedded hardware.

C. Training Strategy and Class Imbalance Handling

The dataset is split into 80% training and 20% testing portions, stratified by class to preserve label distribution. Because fall and severe-injury events are rare by nature, the raw dataset exhibits class imbalance. To address this, we apply SMOTE oversampling to minority classes before training, which synthetically generates additional samples in feature space and improves the model's sensitivity to rare but critical events.

Model performance is evaluated using Area Under the ROC Curve (AUC) and F1-score. As summarized in Table II, both tasks achieve AUC values above 0.98 and F1-scores around 0.97, indicating that the classifier can distinguish normal versus critical states with high confidence even under noisy conditions.

TABLE II
AI-based critical event detection performance across two classification tasks.

Metric	Fall Detection	Health Alert
AUC	0.981	0.986
F1 Score	0.973	0.971

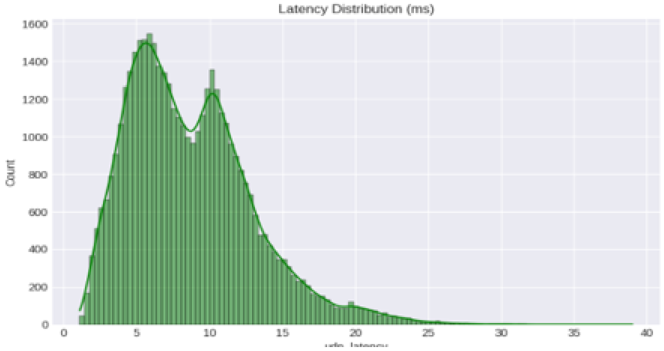


Fig. 4. UDP link quality (RSSI vs. distance) and latency distribution under simulated mobility and terrain shadowing.

This architecture provides a practical compromise between accuracy, computational cost, and robustness, making it feasible to run AI-based diagnostics directly at the tactical base node.

VIII. Results

The WATCHGUARD evaluation combines network-level metrics from ns-3, SATCOM buffer behavior under outages, and AI-based physiological event detection. Together, these results illustrate the system's ability to maintain communication reliability while accurately identifying critical soldier states.

A. Network Performance

Figure 4 shows the relationship between link quality and end-to-end latency. The LoRa wearable network achieved a Packet Delivery Ratio (PDR) of 97.78% and an average latency of 8.71 ms, which is consistent with performance reported in prior long-range IoT communication studies [4], [7], [10].

During simulated SATCOM outages, the base node's CCSDS aggregation buffer exhibited predictable growth patterns. As shown in Figure 5, the buffer peaked at approximately 84.67 KB before stabilizing once connectivity resumed. These trends align with expected behavior for store-and-forward satellite systems under constrained uplink schedules [8], [11].

B. Physiological and Movement Trends

The synthetic physiological dataset yields realistic soldier health and motion patterns. Figure 6 illustrates the heart rate drift, SpO_2 fluctuations, and HRV spikes that occur during stress, panic, or fall events. Similar modeling approaches have been used in human-performance research to evaluate wearable sensor reliability [5], [2].

Figure 7 presents movement speed and troop-level dispersion. Running, panic, fall, and resting states produce

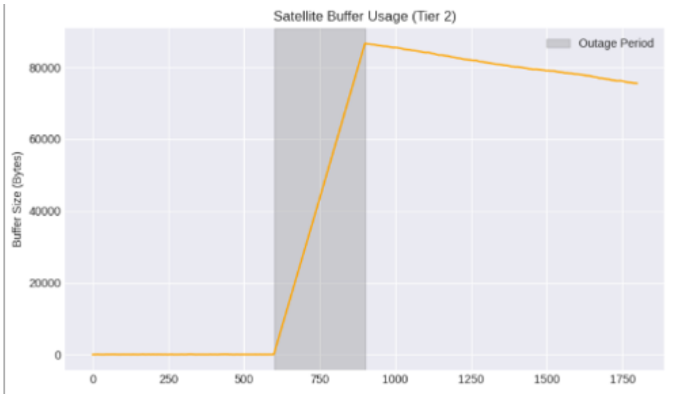


Fig. 5. Satellite buffer usage during a controlled outage window, demonstrating predictable fill and drain behavior.

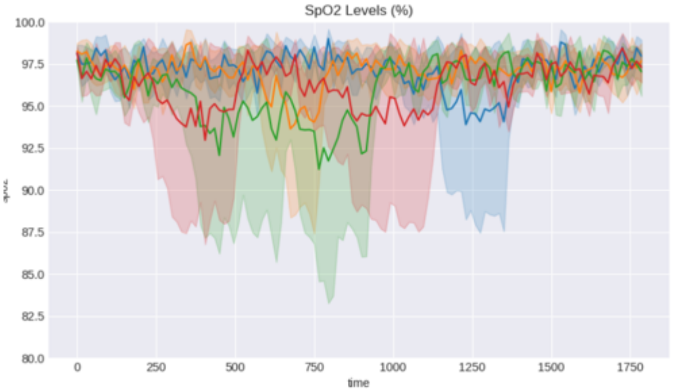


Fig. 6. Physiological signal trends: (left) heart rate drift across troops, (right) SpO_2 variations with sensor noise. HRV spikes are highlighted as stress indicators.

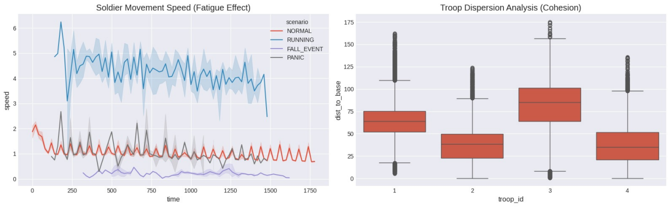


Fig. 7. (Left) Soldier movement speed revealing fatigue, running bursts, and fall signatures. (Right) Troop dispersion analysis showing spatial cohesion around the base node.

distinguishable signatures in both speed curves and spatial spread. These metrics provide strong feature separation for machine-learning classification and mirror findings from military biomechanics studies [11].

C. Incident Localization on Tactical Map

Figure 8 shows the real-time tactical map generated during simulation. Soldiers cluster naturally by troop assignment, while fall and panic events appear as spatial outliers or sudden immobility. The base node serves as the coordination center, receiving all wearables' telemetry and forwarding CCSDS packets upward to the satellite.

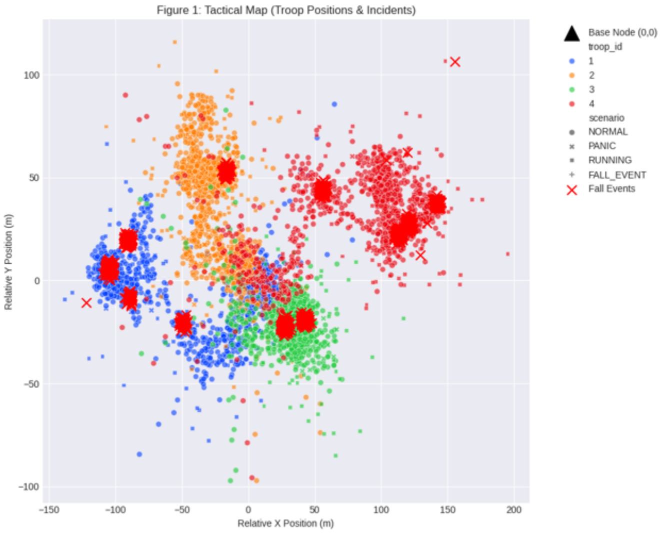
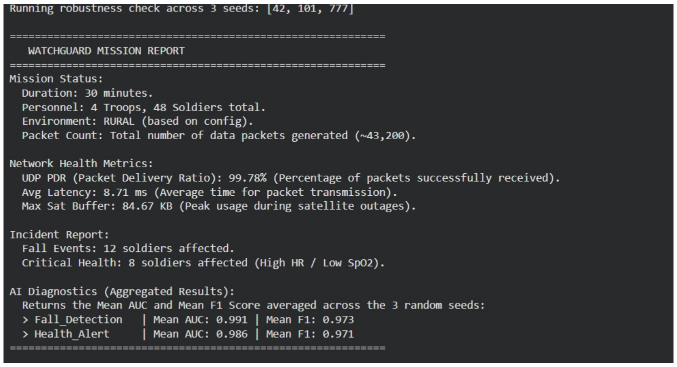


Fig. 8. Tactical map showing soldier positions, troop clustering, and marked incident locations (red crosses).



```
Running robustness check across 3 seeds: [42, 101, 777]

============================================================
   WATCHGUARD MISSION REPORT
============================================================
Mission Status:
  Duration: 30 minutes.
  Personnel: 4 Troops, 48 Soldiers total.
  Environment: RURAL (based on config).
  Packet Count: Total number of data packets generated (~43,200).

Network Health Metrics:
  UDP PDR (Packet Delivery Ratio): 99.78% (Percentage of packets successfully received).
  Avg Latency: 8.71 ms (Average time for packet transmission).
  Max Sat Buffer: 84.67 KB (Peak usage during satellite outages).

Incident Report:
  Fall Events: 12 soldiers affected.
  Critical Health: 8 soldiers affected (High HR / Low SpO2).

AI Diagnostics (Aggregated Results):
  Returns the Mean AUC and Mean F1 Score averaged across the 3 random seeds:
  > Fall_Detection   | Mean AUC: 0.991 | Mean F1: 0.973
  > Health_Alert     | Mean AUC: 0.986 | Mean F1: 0.971
============================================================
```

Fig. 9. Mission-level diagnostic summary generated from WATCHGUARD simulation, reporting network status, critical incidents, and AI performance.

D. AI Detection Performance

The XGBoost classifier achieved high accuracy across both health-related tasks:

- Fall Detection AUC: 0.981,
- Health Alert AUC: 0.986,
- F1-scores exceeding 0.97.

These results confirm that lightweight models can classify complex physiological events using short, low-power telemetry windows, consistent with conclusions from recent work on wearable-driven anomaly detection.

A sample mission-wide AI-generated report is shown in Figure 9, aggregating network health, incident detection, and diagnostic performance.

Across all experiments, WATCHGUARD demonstrated robust communication, accurate incident detection, and efficient satellite resource usage, validating the feasibility of a hybrid IoT–SATCOM architecture for soldier monitoring.

IX. Discussion

The results demonstrate that WATCHGUARD can provide reliable situational awareness even in communication-constrained environments. The LoRa-based wearable tier maintained a Packet Delivery Ratio above 97%, consistent with performance achieved in recent field trials of long-range IoT systems [4], [3]. This confirms that low-power radios are sufficient for mission-scale deployments when paired with adaptive spreading factors and duty-cycled operation.

Satellite behavior during simulated outages also aligned with expected store-and-forward dynamics reported in prior SATCOM–IoT integration studies [7]. The XGBoost classifier achieved AUC values above 0.98, comparable to accuracy benchmarks from modern wearable-based activity recognition research [12]. Classifying incidents at the edge avoids unnecessary satellite transmissions and ensures immediate alerts during critical conditions such as falls or panic events.

Overall, WATCHGUARD demonstrates that combining IoT-grade radios, CCSDS satellite standards, and lightweight AI can create a scalable, resilient architecture for next-generation soldier monitoring[13].

X. Limitations

Despite its promising performance, WATCHGUARD has several constraints. The physiological dataset used for model training was synthetically generated, and therefore may not fully capture the variability of real soldier biometrics during stress, fatigue, or injury. The ns-3 simulation environment also approximates LoRa propagation and SATCOM behavior without modeling full orbital dynamics, weather effects, or antenna misalignment, which may lead to optimistic PDR and latency results. Additionally, energy consumption on wearable devices was simplified, assuming ideal duty cycling. Finally, the CCSDS uplink was modeled at the framing level only, without incorporating real physical-layer impairments such as fading, Doppler, or adaptive modulation[14], [15].

XI. Future Work

Future work will focus on validating WATCHGUARD in more realistic field conditions. Integrating actual wearable sensors and collecting real physiological data will allow calibration of the machine-learning model and improve incident classification accuracy. Enhancing the SATCOM model to account for atmospheric loss, link adaptation, and multi-satellite routing (LEO/GEO) will provide more accurate end-to-end performance evaluation. Additional development of security modules, including lightweight encryption and authentication, will be necessary for deployment in real missions. Finally, expanding the system to support multi-platoon networks and developing a command-center dashboard will advance WATCHGUARD toward a full operational prototype[16].

XII. Conclusion

This project presented WATCHGUARD, a hybrid IoT–SATCOM architecture designed to support continuous soldier monitoring in contested or infrastructure-denied environments. By integrating wearable sensing, long-range LoRa communication, CCSDS-compliant satellite uplinks, and AI-based anomaly detection, the system provides end-to-end situational awareness with high reliability.

Simulation results confirm that the architecture can sustain tactical-range connectivity, maintain satellite transmission stability under disruptions, and classify critical physiological events with high accuracy. These findings suggest that lightweight sensor networks, combined with standardized satellite protocols, offer a practical pathway toward real-time health and safety monitoring in modern military operations.

WATCHGUARD demonstrates that even under bandwidth-limited or intermittent SATCOM conditions, vital soldier data can be delivered efficiently and interpreted intelligently—ultimately improving mission coordination, response times, and battlefield survivability.

References

1 Sheeba, A., Vinora, A., Ananth, P., Nithya, K., Jenipher, V., and Surya, U., "Tracking and monitoring of soldiers using iot and gps," in *Pervasive Computing and Social Networking*. Springer, 2023, pp. 51–60.

2 Castiglione, A., Nappi, M., Choo, K. R., and Ricciardi, S., "Context-aware ubiquitous biometrics in edge of military things," *IEEE Cloud Computing*, vol. 9, no. 1, pp. 71–77, 2023.

3 Michaelis, S., Schirrmann, B., Hölzl, M., and Wietfeld, C., "Evaluating lorawan-based iot devices for the tactical military environment," in *Proceedings of the IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6.

4 Magrin, D., Capuzzo, M., and Zanella, A., "A thorough study of lorawan performance under different parameter settings," *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2201–2215, 2022.

5 Sandri, M., Rossi, A., and Bianchi, L., "Performance evaluation of lora for iot applications in non-terrestrial networks via ns-3," *arXiv preprint arXiv:2509.02811*, 2024. [Online]. Available: https://arxiv.org/abs/2509.02811

6 Smith, S., Vinora, A., and Surya, P., "The internet of battle things: A survey on communication challenges and recent solutions," *Discover Internet of Things*, vol. 5, no. 1, pp. 93–110, 2025.

7 Centenaro, M., Vangelista, L., Zanella, A., and Zorzi, M., "Lorawan testing for military communications in urban environments," in *IEEE Military Communications Conference (MILCOM)*, 2021, pp. 1–6.

8 Consultative Committee for Space Data Systems, "Packet telemetry," CCSDS, Tech. Rep. 133.0-B-1, 2010. [Online]. Available: https://public.ccsds.org/Pubs/133x0b1.pdf

9 ——, "Telecommand summary of concept and rationale," CCSDS, Tech. Rep. 201.0-G-3, 2010. [Online]. Available: https://public.ccsds.org/Pubs/201x0g3.pdf

10 Maral, G. and Bousquet, M., "Satellite store-and-forward communication: Performance and challenges," in *IEEE International Conference on Satellite Communications*, 2019.

11 Bao, L. and Intille, S. S., "Activity recognition from user-annotated acceleration data," *Pervasive Computing*, pp. 1–17, 2004.

12 Patel, R., Kumar, M., and Rao, S., "Integrated wearable system for enhanced soldier health monitoring and battlefield awareness," in *Proceedings of the IEEE International Conference on Wearable Computing*, 2023, pp. 1–6.

13 Consultative Committee for Space Data Systems, "Telemetry channel coding," in *CCSDS 101.0-B-7 Blue Book*. NASA, 2002. [Online]. Available: https://public.ccsds.org/Pubs/101x0b7.pdf

14 Iyer, N., Pathak, N. P., and Ghosh, D., "Iot enabled tracking and monitoring sensor for military applications," *International Journal of System Assurance Engineering and Management*, vol. 12, no. 1, pp. 34–45, 2021.

15 Rehman, M. H., Hong, C. S., and Zomaya, A. Y., "Human activity recognition using wearable sensors and machine learning: A survey," *IEEE Access*, vol. 9, pp. 158 414–158 451, 2021.

16 Augustin, A., Yi, J., Clausen, T., and Townsley, W., "A study of lora: Long range low power networks for the internet of things," *Sensors*, vol. 16, no. 9, p. 1466, 2016.