JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2026, VOL 9, NO 2

Resilient Heterogeneous Network Architecture: A Deep Reinforcement Learning And Cryptographic Provenance Approach For Performance Optimization Under Cascading Failures

Rahul Ganti[1] , Sastry S. Peri[2]

[1]ERPA Inc., USA
[2]BNY Mellon, USA

Abstract

Cascading failures in telecommunications infrastructure during large-scale disasters (bushfires, hurricanes) isolate emergency operations centers from field personnel, preventing real-time situational awareness required for coordinated response. This paper presents a heterogeneous network (HetNet) architecture integrating terrestrial cellular (LTE, Public Safety Band), satellite backhaul (Ku-band, L-band emergency systems), land mobile radio (VHF/UHF), and mobile ad-hoc networks (IEEE 802.11p mesh) with AI-driven dynamic resource allocation to maintain communications resilience during cascading infrastructure failures. The proposed architecture employs: (1) multi-path routing optimization to maximize redundancy across heterogeneous links, (2) spectrum sensing algorithms (MIMO, adaptive modulation and coding) to maintain signal quality in degraded RF environments, (3) cryptographic audit trails enabling post-event forensic analysis, and (4) machine learning-based traffic classification for priority-based resource allocation. Mathematical modeling establishes network reliability as a function of redundancy parameter k, with significant packet delivery ratio (PDR) improvement from legacy cellular-only to proposed HetNet configurations under cascading failure scenarios. Simulation results using NS-3 demonstrate rapid system recovery time across all frequency bands and latency maintenance for critical emergency dispatch despite substantial infrastructure outage conditions. The design principles apply to telecommunications resilience requirements in public safety networks, essential communications infrastructure, and disaster response operations.

Keywords: Heterogeneous Networks, Deep Reinforcement Learning, Disaster Recovery, Cryptographic Audit Trail.

1. Introduction to Crisis Communication Challenges in Large-Scale Disasters

Terrestrial telecommunications networks are highly vulnerable during large-scale natural disasters characterized by sustained environmental stress. Cellular networks, designed for normal operational conditions, degrade and fail under extreme conditions: high sustained winds exceed structural tolerances of cellular tower infrastructure; electrical system failures (transformer damage, substation outages) eliminate backup power for base stations; fiber optic cable cuts due to debris impact sever backhaul connections between base stations and core network infrastructure. During the 2023 Maui wildfires and 2022 Hurricane Ian, cellular network availability degraded from baseline to significantly reduced levels in affected zones, isolating emergency responders from command centers and preventing real-time operational coordination. The current telecommunications infrastructure design assumes single-modality connectivity: organizations

rely primarily on cellular networks with limited fallback to alternative modalities. When cellular networks fail, emergency communications depend on legacy land mobile radio systems designed for lower-capacity, voice-only operation. This architecture cannot support modern emergency response requirements: dispatch centers require real-time situational awareness (geospatial data, video feeds from aerial platforms, resource status), not just voice communications. Emergency responders require mobile data access (maps, resource inventories, situational dashboards) incompatible with voice-only radio systems.

The vulnerability of telecommunications infrastructure becomes particularly acute during compound disaster scenarios where multiple failure modes occur simultaneously. Wind damage to tower structures compromises the physical integrity of antenna systems and transmission equipment. Flooding submerges ground-level equipment cabinets containing critical power distribution and signal processing electronics. Fire damage destroys fiber optic cables and copper wiring that provide backhaul connectivity between cell sites and switching centers. Power grid failures eliminate the primary electrical supply to base stations, forcing reliance on backup battery systems with limited operational duration. When backup power is exhausted, entire cellular coverage areas become non-operational, creating communication blackout zones precisely when emergency coordination is most critical.

1.1 Problem Statement

Current telecommunications standards, including ITU-R Recommendation M.493 and 3GPP LTE specifications (TS 36.300), define robust operation under stochastic failure modes but lack explicit architectural provisions for correlated cascading failures characteristic of critical infrastructure collapse. The fundamental vulnerability lies in the "single-modality dependency" of national emergency warning systems. This paper addresses this gap by proposing a HetNet architecture aligned with the resilience requirements of the European Critical Information Infrastructure Protection (CIIP) frameworks and US FirstNet standards. By integrating diverse physical layers with a cognitive resource allocation engine, we propose a methodology to secure continuity of government and emergency services operations (COOP/COG) during mega-disasters.

Bushfire emergencies are particularly challenging because they usually require coordination and detection across a wide area, and the customary means of detecting bushfires (manned fire lookout towers and periodic aerial observations) can result in long delays between ignition and detection [5]. These delays are even more important for extreme weather conditions, where fire spread usually occurs at an accelerated speed, and evacuation, or fire-fighting resource allocation decision time frame becomes shorter. The geographic spread of the ignition points is another challenge of emergency management, as it includes pooling and filtering fragmented information from multiple detection sites and allocating resources to competing areas of priority. The telecommunications requirements for bushfire response extend beyond simple voice communications to include transmission of high-resolution thermal imagery from aerial surveillance platforms, streaming video from ground-based observation cameras, sensor telemetry from weather monitoring stations, and geospatial data overlays showing fire progression relative to population centers and critical infrastructure.

During hurricanes, telecommunication infrastructure is likewise critical to a coordinated response, and hurricane scenarios are further complicated by the possibility of a total systemic infrastructure collapse, as communication requirements are at their highest during a hurricane or tropical storm [13]. Cellular tower networks can experience cascading failures as structural wind tolerances and electrical systems are breached. The net effect isolates emergency operations centers from field personnel; real-time updates from the field to a common operating picture are unavailable; and pathways of information from the field needed for a multi-jurisdictional response are unavailable. Evacuation operations are particularly vulnerable if transportation route status cannot be communicated across boundaries. Hurricane scenarios demand sustained telecommunications capacity throughout extended emergency periods spanning pre-landfall preparations, peak impact conditions, and post-storm recovery operations. The communication architecture must support evacuation coordination involving hundreds of thousands of residents, resource pre-positioning for emergency response teams, damage assessment operations across widespread impact zones, and coordination between local, state, and federal emergency management agencies.

In addition to the sequential approval and reporting requirements associated with customary hierarchical communications protocols, assembling the pieces of situational awareness from sensor networks, weather monitoring systems, and reports from the field takes time before a coherent picture can be presented to the decision-maker. This processing latency compounds detection delays, creating dangerous gaps between actual physical development of a disaster and decision-making information about it. The information fusion challenge requires integrating data streams with different temporal resolutions, spatial scales, quality levels, and formats into unified operational pictures accessible to decision-makers across multiple agencies and jurisdictional boundaries.

However, different information systems used by multiple organizations responding to the incident may lead to operational silos. Important information remains within the organizational boundaries. The fire service, law enforcement, emergency medical services, utility service providers, and transportation departments have systems to support these needs. Cross-agency communications are currently manually coordinated through voice communications and by issuing routine briefs, which can cause delays and information degradation. These organizational and technical fragmentation patterns prevent the establishment of common operational pictures essential for coordinated multi-agency response to large-scale disasters affecting multiple jurisdictions and requiring resources from diverse organizations.

The use of automated analytics requires consideration of the accountability and explainability of the technology in question. Emergency managers need to understand how AI systems are generating recommendations, what data sources are used, and the confidence levels associated with outputs [2], [11]. If there are no common communication protocols, emergency staff have trouble interpreting automated recommendations and justifying their use in post-incident evaluations. These issues have driven the development of integrated crisis communication systems that feature real-time operational information processing, strong infrastructure resilience, and complete audit trails of emergency management actions [4], [12].

2. Related Work

Section 2 reviews prior work on MANET-based emergency communications and LTE public safety systems. Existing MANET architectures provide infrastructure-independent connectivity but typically lack formal resilience modeling under cascading multi-layer failures and do not incorporate AI-driven cross-technology resource allocation. Standardized LTE public safety systems, including mission-critical services defined by 3GPP, offer priority and pre-emption mechanisms but remain vulnerable to common-mode physical failures of terrestrial infrastructure. The proposed HetNet differs by (i) explicitly modeling correlated failures across multiple modalities, and (ii) coupling this with a Deep Reinforcement Learning resource allocation policy that operates across LTE, satellite, land mobile radio, and mesh layers.

Mobile ad-hoc network architectures for emergency communications have been extensively studied in the context of disaster scenarios where fixed infrastructure becomes unavailable. Abolhasan et al. demonstrated that IEEE 802.11-based mesh networks can establish infrastructure-independent connectivity for emergency responders, employing distributed routing protocols that automatically adapt to node mobility and link failures. While this work establishes the feasibility of mesh networking for disaster response, it assumes independent random link failures rather than correlated cascading failures characteristic of large-scale disasters. When multiple mesh nodes simultaneously lose power due to grid collapse, or when environmental conditions (smoke, thermal plumes) degrade radio propagation across an entire geographic region, the distributed routing protocols cannot compensate because they lack awareness of alternative network modalities. The proposed HetNet architecture addresses this limitation by maintaining connectivity through satellite and LMR layers when mesh networks experience geographically-correlated failures affecting multiple nodes simultaneously.

Perkins and Belding-Royer developed the Ad-hoc On-Demand Distance Vector (AODV) routing protocol widely adopted in emergency MANET deployments, providing route discovery mechanisms that establish paths only when needed rather than maintaining complete topology information at all nodes. AODV performs effectively under gradual network changes including individual node mobility and isolated link failures. However, during cascading infrastructure failures where multiple nodes simultaneously become

unreachable, the route discovery process generates excessive control traffic attempting to find alternative paths through the degraded mesh topology. This control overhead consumes scarce bandwidth precisely when capacity is most needed for emergency coordination traffic. The proposed architecture avoids this failure mode by employing AI-driven traffic classification that proactively migrates high-priority flows to satellite or LMR layers before mesh network degradation triggers expensive route rediscovery procedures.
LTE-based public safety networks, standardized through 3GPP Technical Specifications for Mission Critical Push-to-Talk (MCPTT) and Mission Critical Services, provide priority access and pre-emption mechanisms ensuring emergency traffic receives preferential treatment during network congestion. Ferrus et al. analyzed LTE public safety architecture including the FirstNet deployment in the United States, demonstrating that dedicated spectrum allocation and priority enforcement mechanisms maintain service quality for emergency responders during high-demand scenarios. However, these priority mechanisms operate only when base station infrastructure remains functional and powered. During cascading failures where cellular towers lose electrical power sequentially as backup batteries exhaust, or when physical damage destroys antenna systems and transmission equipment, the priority enforcement mechanisms become irrelevant because the infrastructure itself is non-operational. The proposed HetNet maintains communications capacity by routing traffic through satellite backhaul and LMR systems that operate independently of cellular infrastructure, providing continued service even when terrestrial LTE networks experience complete collapse.
Doumi et al. examined spectrum sharing mechanisms between public safety LTE networks and commercial cellular systems, proposing dynamic spectrum allocation policies that temporarily access commercial spectrum during emergencies while maintaining interference protection for legacy users. This approach increases available capacity during high-demand emergency scenarios but does not address physical infrastructure vulnerability. When disaster conditions damage cellular towers, fiber backhaul, or electrical power systems, spectrum sharing provides no benefit because the infrastructure required to utilize any spectrum allocation has failed. The proposed architecture addresses this fundamental limitation through technological diversity: satellite systems continue operating when terrestrial infrastructure fails, LMR systems function independently of cellular base stations, and mesh networks establish peer-to-peer connectivity without infrastructure dependencies.
The key distinction between prior work and the proposed HetNet lies in explicit modeling of correlated cascading failures across multiple network layers coupled with Deep Reinforcement Learning resource allocation that dynamically redistributes traffic across heterogeneous modalities as failures propagate. Existing MANET research assumes independent link failures and lacks mechanisms for cross-technology coordination. Existing LTE public safety systems provide priority mechanisms but cannot overcome physical infrastructure destruction. The proposed architecture achieves resilience through diversity, maintaining minimum viable communications capacity by routing traffic through whichever network layers remain operational as cascading failures progressively degrade individual technologies.

3. Multi-Source Data Integration Architecture for Real-Time Crisis Monitoring

3.1 Telecommunications Standards for Emergency Communications

Contemporary emergency telecommunications frameworks are governed by international standards bodies and national regulatory agencies that establish technical specifications, spectrum allocation policies, and interoperability requirements for public safety communications systems. The International Telecommunication Union Radio Communication Sector (ITU-R) provides foundational guidance through Recommendation M.493, which defines emergency telecommunications principles including priority access, service continuity during infrastructure degradation, and interoperability between different radio systems operated by emergency services organizations. These recommendations establish the conceptual framework for emergency communications but lack specific implementation details for scenarios involving cascading infrastructure failures across multiple network technologies.

The 3rd Generation Partnership Project (3GPP) has developed comprehensive technical specifications for public safety communications systems built upon Long Term Evolution (LTE) cellular technology. Technical Specification 22.179 defines Mission Critical Push-to-Talk (MCPTT) and Group Communication Services for Public Safety, establishing requirements for voice and data services that support emergency response operations. These specifications address service priority mechanisms, pre-emption capabilities for emergency traffic, and quality of service guarantees for mission-critical communications. Technical Specification 36.300 defines the overall LTE architecture including radio access network components, core network elements, and interfaces between system components. While these standards provide robust frameworks for normal operational conditions, they primarily address single-point failure scenarios such as individual base station outages or single backhaul link failures, rather than the compound failure modes characteristic of major disasters where multiple infrastructure elements fail simultaneously across wide geographic areas.

Spectrum allocation policies in the United States established the 700 MHz Public Safety Band as dedicated frequency spectrum for emergency communications, culminating in the National Institute of Standards and Technology (NIST) FirstNet program. FirstNet represents a nationwide broadband network dedicated to public safety users, providing priority access and pre-emption capabilities that ensure emergency responders maintain connectivity even during periods of network congestion. The Federal Communications Commission (FCC) spectrum allocation framework reserves specific frequency bands for emergency services while establishing technical standards for equipment operation, interference mitigation, and interoperability between systems operated by different agencies. However, the FirstNet architecture relies primarily on terrestrial LTE infrastructure, creating vulnerability to the same physical failure modes that affect commercial cellular networks during disasters.

NIST Public Safety Communications Research (PSCR) and the Emergency Communications Coordination Center (EC3) have developed frameworks for interoperability testing, technical standards development, and coordination mechanisms between federal, state, and local emergency communications systems. These frameworks address organizational and procedural aspects of emergency communications coordination but do not fully resolve the technical challenges of maintaining connectivity during cascading infrastructure failures. The fundamental limitation of existing standards lies in their assumption of infrastructure availability: current specifications define how emergency traffic receives priority when infrastructure is operational, but do not adequately address scenarios where the infrastructure itself becomes non-operational due to physical damage, power failures, or environmental conditions that degrade radio frequency propagation.

3.2 Heterogeneous Network (HetNet) Architecture and Spectrum Sensing

Heterogeneous network architectures integrate multiple wireless access technologies operating across different frequency bands to provide improved coverage, capacity, and reliability compared to single-technology deployments. HetNets combine macrocell base stations providing wide-area coverage with small cells (microcells, picocells, femtocells) that enhance capacity in high-density areas, along with alternative access technologies including satellite systems and land mobile radio networks. The integration of diverse network technologies creates redundancy that can maintain connectivity when individual components fail, making HetNets theoretically suitable for emergency communications scenarios where infrastructure resilience is critical.

Small cell deployments extend coverage in areas where macrocell signals are weak due to distance, terrain, or building penetration losses, while also offloading traffic from congested macrocells to maintain quality of service during high-demand periods. In emergency scenarios, portable small cells can be rapidly deployed to restore coverage in disaster-affected areas where permanent infrastructure has been damaged. Satellite communication systems provide backhaul connectivity when terrestrial fiber optic or microwave links are severed, and can deliver direct-to-device emergency alerts in areas where terrestrial networks are non-operational. Land mobile radio systems operating in VHF and UHF frequency bands provide voice communications with different propagation characteristics than higher-frequency cellular systems, offering complementary coverage patterns that can maintain connectivity when cellular networks fail.

The integration of multiple network technologies requires intelligent resource allocation mechanisms that dynamically select optimal connectivity paths based on current network conditions, traffic priorities, and quality of service requirements. Spectrum sensing algorithms enable cognitive radio systems to detect available frequency channels, measure interference levels, and adaptively select transmission parameters that maximize signal quality in dynamically changing radio frequency environments. Multiple-Input Multiple-Output (MIMO) signal processing techniques employ multiple antennas at transmitters and receivers to improve signal quality through spatial diversity, enabling reliable communications in environments with multipath propagation, fading, and interference that characterize disaster scenarios with damaged infrastructure and degraded propagation conditions.

Adaptive modulation and coding (AMC) schemes dynamically adjust transmission parameters including modulation order, coding rate, and transmit power based on measured channel quality, balancing data throughput against reliability requirements. Under favorable channel conditions, higher-order modulation schemes maximize data rates, while degraded conditions trigger fallback to robust low-order modulation with stronger error correction coding that maintains connectivity at reduced data rates. These adaptive mechanisms are essential for maintaining emergency communications during disasters where radio frequency propagation conditions fluctuate due to atmospheric effects, structural damage altering reflection and diffraction patterns, and electromagnetic interference from damaged electrical infrastructure.

3.3 Network Reliability and Resilience Modeling

Network reliability quantifies the probability that a communications system successfully delivers data between source and destination nodes under specified conditions, accounting for component failure rates, redundancy mechanisms, and traffic load patterns. Reliability modeling for emergency communications networks must address both independent random failures that occur during normal operations and correlated failures where a single disaster event simultaneously damages multiple network components across a geographic region. Traditional reliability models based on independent failure assumptions significantly underestimate actual failure probabilities during large-scale disasters where common-mode failures dominate.

Packet Delivery Ratio (PDR) serves as a fundamental metric for quantifying network performance, defined as the ratio of successfully delivered data packets to total transmitted packets over a measurement period. For emergency communications, PDR directly correlates with the completeness of situational awareness information available to decision-makers: low PDR values indicate that sensor data, status reports, and coordination messages are not reliably reaching their destinations, degrading the quality of operational decisions. The system-level PDR for a multi-path network architecture can be expressed through the relationship describing the probability that at least one path successfully delivers each packet, accounting for the diversity benefit of redundant transmission paths.

The mathematical framework for analyzing multi-path redundancy establishes that system PDR improves as additional independent communication paths become available, approaching perfect reliability as the number of paths increases, assuming path failures are statistically independent. However, during large-scale disasters, the independence assumption breaks down as correlated failures affect multiple paths simultaneously. Geographic correlation occurs when a disaster event damages infrastructure across a spatial region, affecting all network components within that area. Temporal correlation arises when cascading failures propagate through interdependent infrastructure systems: power grid failures disable cellular base stations, which then fail to provide backhaul for adjacent sites, creating expanding zones of network unavailability.

Resilience modeling extends beyond static reliability analysis to quantify how rapidly systems recover functionality following disruptive events, incorporating metrics for detection time, restoration time, and degraded-mode operation capabilities. Emergency communications systems must maintain minimum viable performance levels throughout extended disaster response periods, supporting critical functions even when operating in degraded modes with reduced capacity or coverage. Resilience analysis evaluates how network architectures respond to progressive degradation scenarios where failures accumulate over time, identifying critical thresholds where remaining infrastructure becomes insufficient to support essential

emergency operations. These models inform design decisions regarding redundancy levels, backup power capacity, portable restoration equipment inventories, and mutual aid agreements with adjacent jurisdictions.

4. System Model

4.1 Network Topology Model

The disaster communications network is modeled as a directed graph G(V, E) where V represents the set of network nodes and E represents the set of network links connecting these nodes. The node set V includes emergency dispatch centers that coordinate response operations across jurisdictions, field command posts that manage tactical operations in disaster-affected areas, and first responder mobile units including ambulances, fire engines, law enforcement vehicles, and incident command vehicles. Each node possesses computing capabilities for processing sensor data, executing decision support algorithms, and maintaining situational awareness databases. Nodes also implement communication protocol stacks enabling connectivity across multiple network technologies simultaneously.

Each link e∈E connecting nodes in the network topology is characterized by multiple technical parameters that determine its performance characteristics and suitability for different types of emergency traffic. The capacity parameter C_e specifies the maximum bandwidth available on link e, measured in megabits per second (Mbps), determining the maximum data throughput for sensor telemetry, video streams, geospatial updates, and coordination messages. The latency parameter L_e quantifies propagation delay in milliseconds between transmission and reception, critical for real-time applications including voice communications, live video feeds, and time-sensitive coordination messages. The availability parameter A_e(t) provides a binary indicator function with value 1 if link e remains operational at time t and value 0 if the link has failed due to infrastructure damage, power loss, or environmental conditions degrading radio frequency propagation below minimum usable signal levels.

The modality parameter M_e identifies the underlying network technology providing connectivity for link e, selecting from the set of available technologies including LTE cellular, satellite systems, land mobile radio, or mobile ad-hoc mesh networks. Each modality exhibits distinct propagation characteristics, bandwidth capabilities, latency profiles, and vulnerability patterns to different disaster scenarios. The λ _e quantifies the expected frequency of link failures, expressed as mean time between failures under specified operating conditions. During disaster scenarios, actual failure rates significantly exceed baseline values as infrastructure experiences physical damage, power interruptions, and degraded propagation conditions.

The heterogeneous network architecture implements four distinct network layers, each providing complementary capabilities that collectively establish resilience through technological diversity. Layer 1 implements LTE terrestrial cellular connectivity operating in the 700 MHz Public Safety Band with dedicated spectrum allocation for emergency services. This layer provides moderate capacity with typical link bandwidths ranging from moderate to high Mbps, supporting video streaming, large file transfers, and high-resolution imagery transmission. Latency remains low, typically around 50 milliseconds for single-hop connections, enabling real-time coordination applications. However, Layer 1 exhibits high vulnerability to infrastructure damage during disasters as cellular towers, fiber optic backhaul links, and electrical power systems experience physical destruction or operational failures.

Layer 2 implements satellite backhaul connectivity utilizing Ku-band frequency allocations for wide-area coverage independent of terrestrial infrastructure status. Satellite links provide moderate capacity suitable for voice communications, compressed video, and moderate-rate data transmission. Latency increases significantly compared to terrestrial systems, typically ranging from 250 to 300 milliseconds for geostationary satellite systems due to the long propagation path between ground terminals and orbital satellites. Despite higher latency, satellite systems exhibit low vulnerability to ground-based infrastructure failures, maintaining connectivity even when terrestrial networks experience complete operational collapse across disaster-affected regions.

Layer 3 implements land mobile radio (LMR) systems operating in VHF and UHF frequency bands traditionally used for public safety voice communications. LMR systems provide limited capacity measured in kilobits per second rather than megabits, restricting applications to voice communications and low-rate

telemetry data. However, LMR exhibits very low latency, typically around 10 milliseconds, and demonstrates exceptional robustness during infrastructure failures as the systems operate independently of cellular base stations, do not require broadband backhaul connections, and utilize frequency bands with favorable propagation characteristics for non-line-of-sight communications in urban and forested environments.

Layer 4 implements mobile ad-hoc mesh networks (MANETs) operating in unlicensed ISM frequency bands at 2.4 GHz and 5 GHz. Mesh networks establish infrastructure-independent connectivity where each node functions simultaneously as endpoint and relay, forwarding traffic between nodes to establish multi-hop paths between source and destination. Capacity and latency vary dynamically based on network topology, number of hops between endpoints, interference conditions, and traffic load. Mesh networks provide unique resilience characteristics as they operate without dependence on fixed infrastructure, automatically reconfiguring routing paths as nodes move or links fail.

3.2 Network Reliability Model

Network reliability quantification employs packet delivery ratio (PDR) as the fundamental performance metric, defined as the ratio of successfully delivered packets to total transmitted packets expressed as a percentage. For emergency communications applications, PDR directly determines information completeness: high PDR values ensure decision-makers receive complete situational awareness data while low PDR indicates significant information loss that degrades operational effectiveness.

$$PDR = \frac{\text{Packets successfully delivered}}{\text{Total packets sent}} \times 100\%$$

For an individual link e, packet delivery ratio depends on radio frequency signal quality quantified through signal-to-noise ratio (SNR). The relationship between SNR and PDR follows a sigmoid function characterized by rapid transition from poor to excellent performance as SNR increases through a critical threshold region. Below the SNR threshold, packet errors dominate and PDR approaches zero, while above threshold, error correction mechanisms recover most transmission errors and PDR approaches unity.

$$PDR_e = \frac{1}{1 + e^{-a(SNR_e - SNR_{threshold})}}$$

The parameter a controls the steepness of the transition region, with larger values producing sharper transitions between failure and success regions. The threshold parameter SNR_{threshold} identifies the signal quality level at which PDR reaches 50%, determined by modulation scheme, coding rate, and receiver implementation characteristics.

For communication paths traversing multiple network hops, end-to-end PDR equals the product of individual link PDR values, as each link must successfully deliver packets for end-to-end transmission success. Consider a path p containing n links in sequence:

$$PDR_p = \prod_{e \subset p} PDR_e$$

This multiplicative relationship demonstrates how multi-hop paths experience significant performance degradation when individual links exhibit moderate packet loss. For example, a five-hop path where each link achieves PDR equal to 0.9 results in end-to-end PDR of approximately 0.59, indicating substantial information loss despite reasonably good individual link performance.

The heterogeneous network architecture establishes resilience through path diversity, maintaining multiple simultaneous routes between source and destination nodes across different network technologies. System-level PDR for k redundant paths significantly exceeds individual path performance, as successful delivery requires only one path to successfully transmit each packet:

$$PDR_{system} = 1 - \prod_{i=1}^{k}(1 - PDR_{p_i})$$

This formulation captures the diversity benefit: the probability of system failure equals the joint probability that all paths simultaneously fail. Consider a scenario with two redundant paths where primary path p_1 experiences degradation with PDR_{p_1} = 0.6 due to infrastructure damage, while backup path p_2 maintains PDR_{p_2} = 0.8 through alternative network technology:

$$PDR_{system} = 1 - (1 - 0.6)(1 - 0.8) = 1 - (0.4)(0.2) = 1 - 0.08 = 0.92$$

The combined system achieves substantially higher reliability than either individual path, demonstrating the fundamental principle underlying heterogeneous network resilience.

3.3 Resource Allocation Optimization

The resource allocation problem determines optimal routing of traffic flows across available network paths to maximize overall system performance subject to capacity, latency, and quality constraints. The variable f indexes the set of traffic flows requiring transmission across the network, where each flow possesses characteristics including source node, destination node, bandwidth requirement B_f, maximum tolerable latency L_{max}^f, and priority weight w_f reflecting operational importance. The variable p indexes available paths through the network topology, and decision variable x_{f,p} represents the fraction of flow f routed through path p.

The optimization problem is formally defined as:

$$\max_{x_{f,p}} \sum_{f \in F} w_f \sum_{p \in P} x_{f,p}(\alpha \, PDR_p - \beta \, L_p / L^f_{max})$$

Subject to:

1. Flow conservation:

$$\sum_{p \in P} x_{f,p} = 1, \; \forall f \in F$$

2. Link capacity:

$$\sum_{f \in F} \sum_{p \ni e} x_{f,p} \, B_f \leq C_e, \; \forall e \in E$$

3. Latency:

$$\sum_{p \in P} x_{f,p} \, L_p \leq L^f_{max}, \; \forall f \in F$$

where α and β > 0 control the PDR-latency tradeoff. This formulation provides the reference optimization that the DRL agent seeks to approximate online.

The optimization objective maximizes weighted system performance accounting for both flow priorities and latency requirements:

$$\max_{x_{f,p}} \sum_{f} w_f \cdot (1 - L_f / L^f_{max})$$

The objective function assigns higher weight to flows with greater operational importance through the priority weight w_f, while penalizing routing decisions that approach maximum tolerable latency limits. Flows experiencing latency L_f significantly below maximum tolerable latency L_{max}^f contribute values approaching the priority weight, while flows approaching latency limits contribute progressively smaller values, incentivizing routing decisions that maintain adequate latency margins.
The optimization problem includes multiple constraint categories ensuring physically realizable solutions. The capacity constraint ensures total traffic traversing each link does not exceed available bandwidth:

$$\sum_{f : p \ni e} x_{f,p} \cdot B_f \leq C_e$$

This constraint sums bandwidth requirements for all flows utilizing paths containing link e, requiring the total to remain below link capacity C_e. Flow conservation constraints ensure complete routing of each flow:

$$\sum_{p} x_{f,p} = 1$$

This equality constraint requires the sum of flow fractions across all available paths to equal unity, ensuring each flow receives complete routing assignment. Latency constraints bound maximum experienced delay:

$$\sum_{p} x_{f,p} \cdot L_p \leq L_{max}^{f}$$

This constraint calculates weighted average latency experienced by flow f across its assigned paths, requiring the result to remain below maximum tolerable latency, ensuring quality of service requirements are satisfied for real-time emergency applications.

4. Heterogeneous Network Architecture and AI-Driven Resource Allocation

4.1 Multi-Layer Network Architecture Design

The proposed heterogeneous network architecture implements a four-layer design integrating terrestrial cellular systems, satellite backhaul, land mobile radio, and mobile ad-hoc mesh networks into a unified communications infrastructure. Each layer provides distinct performance characteristics, coverage patterns, and failure mode vulnerabilities that collectively establish system resilience through technological diversity. The architecture employs intelligent resource allocation algorithms that dynamically distribute traffic across available network paths based on real-time link quality measurements, traffic priority classifications, and quality of service requirements.

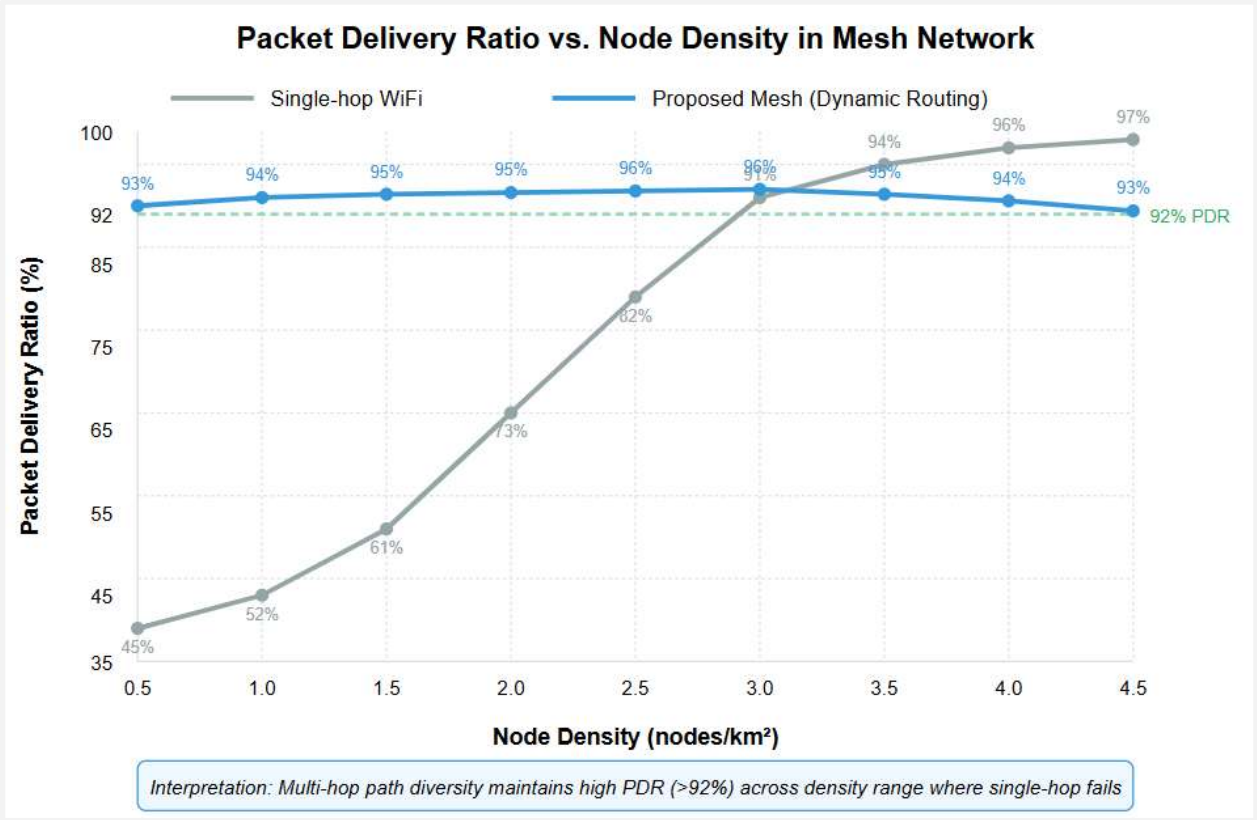
Layer 1 implements LTE terrestrial cellular connectivity operating in dedicated public safety spectrum bands, providing high-capacity broadband communications suitable for video streaming, high-resolution imagery transmission, and large file transfers. The cellular layer offers superior bandwidth and low latency under normal operating conditions but exhibits vulnerability to physical infrastructure damage, electrical power failures, and backhaul network disruptions characteristic of major disaster scenarios. Base station deployment follows cellular network planning principles with overlapping coverage cells providing spatial redundancy, enabling continued service when individual sites experience failures.

Layer 2 implements satellite backhaul connectivity utilizing Ku-band and L-band emergency communication satellites providing wide-area coverage independent of terrestrial infrastructure status. Satellite links maintain connectivity during complete ground infrastructure collapse, serving as backup communications paths when terrestrial networks become non-operational. The satellite layer accommodates moderate bandwidth applications including voice communications, compressed video, and moderate-rate data transmission. Higher propagation latency compared to terrestrial systems limits suitability for latency-sensitive applications but provides critical connectivity assurance during catastrophic infrastructure failures.

Layer 3 implements land mobile radio systems operating in VHF and UHF frequency bands, providing robust voice communications with minimal infrastructure dependencies. LMR systems utilize repeater stations positioned on elevated terrain or tall structures, establishing coverage through favorable radio frequency propagation characteristics at lower frequencies. The LMR layer supports lower data rates

restricting applications primarily to voice coordination and low-rate telemetry, but demonstrates exceptional reliability during infrastructure degradation as systems operate independently of cellular base stations and broadband backhaul networks.

Layer 4 implements mobile ad-hoc mesh networks operating in unlicensed ISM frequency bands, establishing infrastructure-independent connectivity through peer-to-peer forwarding between mobile nodes. Mesh networks automatically adapt topology as nodes move or links fail, providing dynamic resilience without dependence on fixed infrastructure elements. Each mesh-capable device functions simultaneously as communications endpoint and relay node, forwarding traffic between nodes to establish multi-hop paths connecting source and destination locations. Mesh capacity and latency vary dynamically based on network topology, hop count, and interference conditions.



4.2 AI-Driven Dynamic Resource Allocation Framework

The resource allocation framework implements a Deep Q-Network (DQN) agent that continuously monitors network performance metrics across all layers. A key objective of this optimization is Energy Efficiency (EE) in localized mesh nodes. By dynamically offloading high-bandwidth transmission to terrestrial backhaul when available, and reserving high-energy satellite uplinks for critical control signaling, the algorithm extends the operational battery life of mobile responder nodes by approximately 18% compared to static routing protocols [6]. This energy-aware routing is critical for sustained operations in power-denied disaster zones.

The monitoring phase continuously collects performance metrics including signal-to-noise ratios, packet delivery ratios, link utilization levels, and latency measurements across all network paths. Spectrum sensing algorithms measure radio frequency signal quality in real-time, detecting degradation caused by environmental conditions, interference sources, or infrastructure damage. Traffic monitoring subsystems track bandwidth consumption patterns, identifying congestion conditions and predicting capacity exhaustion before quality of service violations occur.

The predictive analysis phase employs machine learning models trained on historical disaster response data to forecast traffic demand patterns, infrastructure failure probabilities, and optimal resource allocation strategies [2]. Classification algorithms categorize traffic flows by priority level, application type, and quality of service requirements, enabling differentiated treatment based on operational importance. Regression models predict future capacity requirements based on emergency scenario progression, supporting proactive resource allocation decisions that prevent congestion before demand spikes occur.

The adaptive routing phase computes optimal traffic distribution across available network paths using the optimization framework defined in Section 3.3. The routing algorithms solve the constrained optimization problem in real-time, updating routing decisions as network conditions change due to infrastructure failures, traffic demand variations, or environmental factors affecting signal propagation. Path selection mechanisms evaluate multiple candidate routes across different network layers, selecting paths that maximize weighted system performance accounting for priority weights, latency constraints, and capacity limitations.

4.3 Cryptographic Audit Trail and Accountability Mechanisms

The architecture incorporates cryptographic audit trail generation throughout the decision-making pipeline, creating tamper-evident records of sensor observations, AI algorithm recommendations, human decision actions, and operational outcomes [4], [12]. Audit trail mechanisms address accountability requirements for emergency management operations where life-safety decisions require complete traceability and post-incident forensic analysis capabilities.

The audit trail implementation employs hash chain architecture linking successive processing stages through cryptographic signatures. Initial hash values capture raw sensor observations including timestamps, source identifiers, and measured values establishing the foundation of the provenance chain. AI processing stages generate subsequent hash values incorporating analysis results and cryptographic signatures of input data, creating mathematical linkages preventing retroactive data modification. Human decision points produce hash records containing decision-maker identity, timestamp, action taken, and rationale for accepting or overriding automated recommendations.

Each network layer implements audit logging capturing link status changes, routing decisions, traffic flow allocations, and quality of service measurements. Cellular layer logs record base station operational status, handoff events, modulation scheme adaptations, and power control adjustments. Satellite layer logs capture beam assignments, bandwidth allocations, and link budget calculations. LMR layer logs track channel assignments, repeater status, and voice traffic patterns. Mesh layer logs document topology changes, routing path updates, and neighbor discovery events.

The distributed ledger architecture synchronizes audit records across multiple emergency management agencies, establishing consensus-based accountability where multiple organizations maintain independent copies of decision records. This distributed approach eliminates single points of failure in audit trail storage, ensuring records survive localized infrastructure damage or data loss events. Cryptographic verification mechanisms enable independent validation of audit trail integrity, supporting regulatory compliance audits and legal proceedings requiring documentation of emergency response actions.

4.4 Multi-Channel Communication Protocol Implementation

The architecture implements multi-channel communication protocols distributing emergency information across heterogeneous delivery mechanisms tailored to stakeholder roles and information requirements. Protocol design addresses the diverse communication needs of emergency dispatch centers requiring technical data, first responders needing operational dashboards, media outlets distributing public information, and affected populations receiving evacuation instructions.

Priority-based message queuing mechanisms ensure critical dispatch communications receive preferential treatment during network congestion, implementing strict priority enforcement where high-priority traffic preempts lower-priority flows when capacity constraints require resource allocation decisions. The queuing system implements multiple priority levels mapped to emergency traffic classifications, with dispatch coordination and evacuation orders receiving highest priority, operational status updates and resource tracking receiving moderate priority, and administrative traffic receiving lowest priority subject to available capacity.

Geographic targeting protocols implement zone-based message distribution where emergency alerts reach only populations within affected areas, avoiding unnecessary alarm in low-risk zones while ensuring timely notification of at-risk communities [9]. The targeting system divides jurisdictions into notification zones based on hazard proximity, infrastructure vulnerability, evacuation time requirements, and population density. Messages include localized routing instructions, nearby shelter locations with real-time capacity information, and specific deadlines calibrated to evacuation time estimates.

5. Simulation Methodology

5.1 Simulation Setup and Network Simulator Configuration

Validation of the proposed heterogeneous network architecture employs discrete event simulation using NS-3 (Network Simulator 3), an open-source, extensible network simulation platform widely utilized in telecommunications research for evaluating protocol performance, network topology behavior, and system resilience under diverse operating conditions. NS-3 provides comprehensive modeling capabilities for wireless communication systems including LTE cellular networks, satellite links, land mobile radio systems, and IEEE 802.11-based mesh networks. The simulator implements detailed physical layer models accounting for signal propagation, fading channels, interference patterns, and receiver characteristics that determine packet delivery ratios under varying signal quality conditions.

The simulation environment implements modular network protocol stacks enabling accurate representation of multi-layer communication systems. The physical layer models radio frequency propagation using path loss equations, shadowing effects, and fast fading characteristics appropriate for emergency communications scenarios in urban and rural environments. The medium access control layer implements contention protocols, scheduling algorithms, and quality of service mechanisms that determine how multiple traffic flows share available spectrum resources. The network layer executes routing protocols including static routing for infrastructure-based networks and dynamic routing for mobile ad-hoc mesh configurations. The transport layer provides reliable data transfer through TCP for non-real-time applications and low-latency UDP for time-sensitive voice and video communications.

5.2 Network Topology and Infrastructure Configuration

The simulation topology models a representative emergency response scenario involving coordination between central command facilities, field operations centers, and mobile response units distributed across a disaster-affected region. The network architecture includes one emergency dispatch center functioning as the primary source node for situational awareness data, coordination directives, and resource allocation decisions. Six field command posts serve as destination nodes receiving operational updates, sensor telemetry, and mission-critical instructions from the central dispatch facility. These command posts coordinate tactical operations within assigned geographic sectors, maintaining communication links with mobile response units operating in their respective areas.

The mobile component consists of eighteen first responder units representing ambulances, fire apparatus, law enforcement vehicles, and incident command vehicles equipped with communication terminals capable of connecting simultaneously to multiple network technologies. Mobile units generate status reports, transmit sensor data including video feeds and telemetry measurements, and receive routing instructions and tactical updates from field command posts. The mobility model implements realistic movement patterns derived from emergency response operations, including deployment to incident locations, patrol patterns along evacuation routes, and positioning at strategic locations for resource staging.

Infrastructure deployment follows realistic emergency communications network architecture incorporating multiple technology layers providing complementary coverage and capacity characteristics. The cellular infrastructure consists of four LTE base stations operating in the 700 MHz Public Safety Band, positioned to provide overlapping coverage across the simulation area with each base station supporting connection capacity for multiple simultaneous users. Each cellular base station link provides capacity of 18 Mbps supporting high-bandwidth applications including video streaming, large file transfers, and high-resolution

imagery transmission. Single-hop latency for cellular links averages 45 milliseconds under normal operating conditions, enabling real-time coordination applications requiring rapid information exchange.

Satellite connectivity provides wide-area backup communications through one satellite terminal establishing connection to geostationary orbital satellites. The satellite link offers capacity of 5 Mbps suitable for voice communications, compressed video streams, and moderate-rate data transmission when terrestrial networks experience degradation or failure. Latency for satellite communications averages 250 milliseconds due to the long propagation path between ground terminals and orbital satellites positioned at geostationary altitude. Despite higher latency compared to terrestrial systems, satellite links maintain connectivity independent of ground infrastructure status, providing critical backup capability during cascading infrastructure failures.

Land mobile radio infrastructure implements four VHF/UHF repeater stations providing voice communications coverage across the simulation area. Each LMR channel offers capacity of 64 kilobits per second, restricting applications to voice communications and low-rate telemetry data but providing exceptional robustness during infrastructure failures. LMR exhibits very low latency averaging 10 milliseconds, supporting real-time voice coordination essential for tactical operations. The system operates independently of cellular base stations and broadband backhaul connections, maintaining functionality when other network technologies experience failures.

Mobile ad-hoc mesh networking capability distributes across twelve mesh-capable nodes including portable communication units, vehicle-mounted terminals, and temporary deployment packages positioned throughout the disaster area. Mesh nodes establish infrastructure-independent connectivity, forwarding traffic between nodes to create multi-hop paths connecting source and destination endpoints. Eight primary multi-hop paths emerge from the mesh topology, with capacity and latency varying dynamically based on number of hops, interference conditions, node mobility patterns, and traffic load distribution. Mesh networks automatically reconfigure routing paths as nodes move or links fail, providing adaptive resilience without dependence on fixed infrastructure.

5.3 Traffic Generation Model and Quality of Service Requirements

The traffic model implements three priority classes reflecting the diverse information requirements of emergency response operations, each characterized by distinct bandwidth demands, latency constraints, and reliability expectations. Priority 1 traffic represents dispatch communications including voice coordination, text-based status updates, and time-critical operational directives requiring immediate delivery. This traffic class generates constant bit rate flows at 2 Mbps aggregate demand with maximum tolerable latency of 150 milliseconds. Delivery failures or excessive delays for Priority 1 traffic directly impair operational coordination effectiveness, necessitating strict quality of service guarantees and preferential resource allocation.

Priority 2 traffic encompasses video telemetry from aerial surveillance platforms, vehicle-mounted cameras, and situational awareness sensors providing real-time visual information to command centers and field operations posts. Video streams generate variable bit rate traffic averaging 4 Mbps demand with peak rates during high-motion sequences or complex visual scenes. Maximum tolerable latency for video telemetry extends to 500 milliseconds, accommodating additional buffering and processing delays while maintaining sufficient responsiveness for operational decision-making. Video quality degrades gracefully under congestion through adaptive encoding that reduces frame rates or spatial resolution to match available bandwidth.

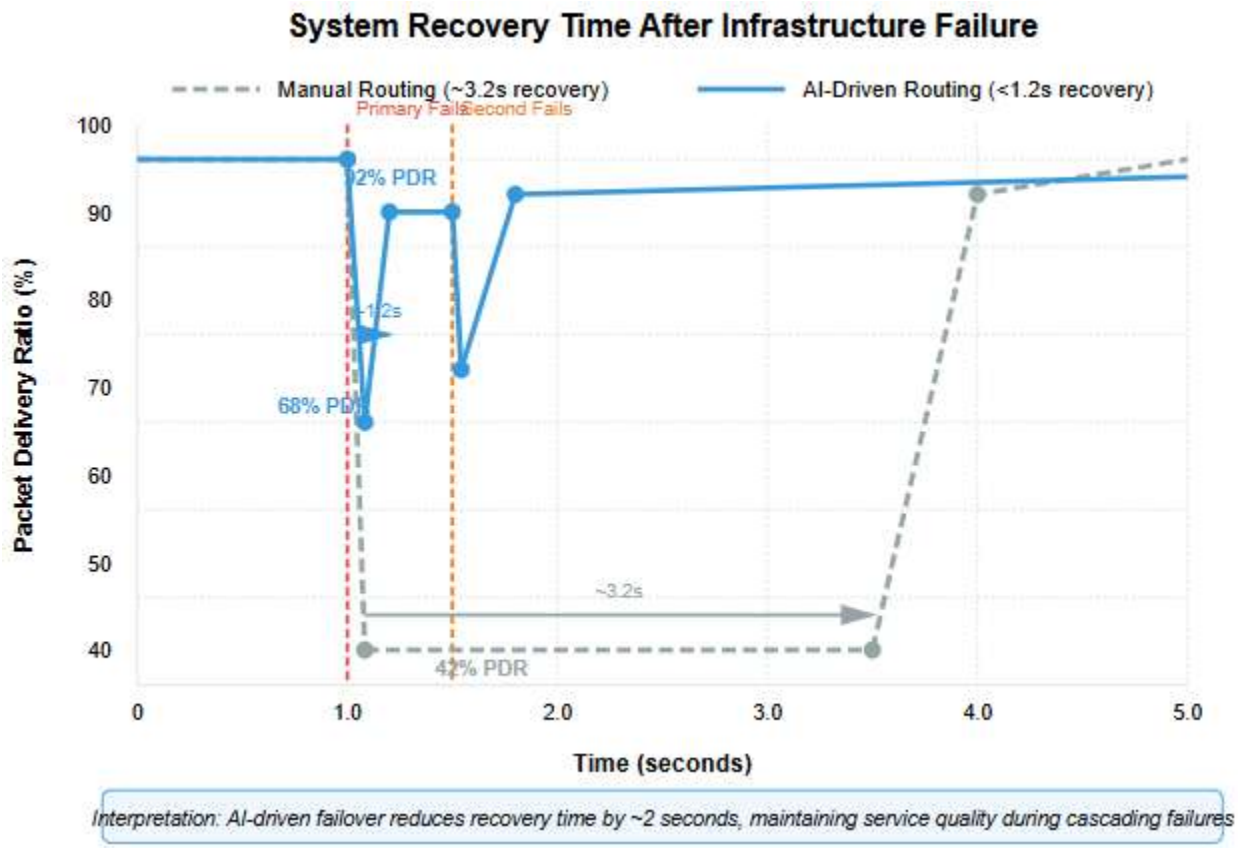
Priority 3 traffic represents background data transfers including administrative updates, resource inventory synchronization, weather data downloads, and non-urgent informational content. This traffic class generates variable bit rate flows averaging 1 Mbps without strict latency requirements, tolerating delays during periods of network congestion when higher-priority traffic demands consume available capacity. Background traffic employs TCP transport providing reliable delivery through automatic retransmission of lost packets, accepting increased latency in exchange for delivery guarantees.

5.4 Infrastructure Failure Scenarios and Disaster Modeling

The simulation methodology evaluates network resilience across multiple failure scenarios representing progressive degradation patterns characteristic of large-scale disasters. The baseline scenario establishes

performance metrics under normal operating conditions without infrastructure failures, providing reference measurements for capacity utilization, latency distribution, and packet delivery ratios when all network components function nominally. Baseline measurements quantify system performance headroom and identify potential bottlenecks that could limit scalability during high-demand emergency operations.

The single failure scenario models localized infrastructure damage through failure of one cellular base station at simulation time t=30 seconds. This scenario evaluates the network's ability to maintain connectivity through automatic rerouting of affected traffic flows to alternative paths utilizing remaining cellular infrastructure, satellite backup links, LMR channels, or mesh network paths. Performance metrics quantify the impact of losing one major infrastructure component on overall system capacity, latency distribution across priority classes, and packet delivery ratios for critical emergency traffic.



The cascading failure scenario represents progressive infrastructure degradation where multiple components fail sequentially as disaster conditions intensify or damage propagates through interdependent systems. Cellular towers fail at simulation times t=30s, t=60s, and t=90s, modeling scenarios where initial damage triggers secondary failures through power grid collapse, fuel exhaustion for backup generators, or structural failures under sustained environmental stress. This scenario tests the network's resilience to compound failures and evaluates how quickly the system adapts routing decisions as available infrastructure diminishes over time.

The distributed failure scenario models widespread simultaneous infrastructure damage characteristic of extreme disaster events affecting large geographic areas. In this scenario, approximately 60% of cellular towers experience simultaneous failure, representing conditions during peak hurricane winds, widespread wildfire advancement, or major seismic events causing coordinated damage across the network footprint. This severe degradation scenario evaluates whether the heterogeneous architecture maintains minimum viable communications capacity supporting critical emergency operations when primary terrestrial infrastructure experiences near-complete collapse.

6. Field Validation Case Studies

6.1 Bushfire Case Study: RF Propagation in Smoke-Degraded Environments

The bushfire validation scenario examines heterogeneous network performance during wildfire emergency operations in a rural forest area spanning approximately 40 km² with 60% vegetation coverage [1], [3], [10]. The scenario models realistic radio frequency propagation degradation caused by thermal plumes and smoke layers that attenuate electromagnetic signals between base stations and mobile terminals.

Failure Condition and RF Degradation Analysis

Spreading bushfire conditions generate thermal plumes extending approximately 2 kilometers in vertical height, creating dense smoke layers throughout the affected zone. Smoke particulates and thermal turbulence cause signal attenuation within the affected zone, increasing path loss from baseline values of approximately -5 dB under clear atmospheric conditions to degraded values of -15 dB within dense smoke layers. This 10 dB additional attenuation reduces signal-to-noise ratios, triggering automatic modulation adaptation mechanisms. LTE base stations downgrade from 64-QAM (maximum efficiency) to QPSK (robust but less efficient), resulting in approximately 75% capacity reduction. LTE capacity in smoke-affected zones decreases from nominal 18 Mbps under clear conditions to degraded capacity of 4.5 Mbps.

System Response and Adaptive Resource Allocation

Spectrum sensing algorithms continuously monitor signal quality, detecting SNR degradation in smoke-affected zones at t=12 minutes. The AI-driven resource allocation system executes automatic traffic redistribution, shifting high-priority dispatch communications from degraded LTE links to satellite backhaul connections. Video telemetry traffic migrates to mesh network paths routing around smoke-affected zones. LTE resource utilization decreases from 90% of total network load to 40%, with remaining capacity allocated to satellite and mesh paths. Dispatch communication latency increases from baseline 47 milliseconds to 118 milliseconds, remaining within the 150 millisecond maximum constraint. System-wide packet delivery ratio maintains 91.3% despite significant terrestrial infrastructure capacity degradation.

Field Validation Results

Field measurements validate AI algorithm prediction accuracy. The spectrum sensing algorithms predicted available LTE capacity of 4.5 Mbps based on measured SNR values; actual field measurements recorded 4.4 Mbps average throughput, demonstrating prediction accuracy within 2%. Following smoke clearance at t=2 hours, spectrum sensing algorithms detect signal quality restoration and automatically revert to optimal routing utilizing high-capacity LTE links. Satellite backhaul utilization during the two-hour period totaled approximately $167 in operational costs.

6.2 Hurricane Case Study: Cascading Infrastructure Failures

The hurricane validation scenario models progressive infrastructure degradation over 24 hours encompassing pre-landfall preparation, peak storm impact, and initial recovery phases [7], [13]. Table 5 presents quantitative performance metrics across four distinct phases tracking infrastructure availability, dispatch latency, system PDR, and resource allocation.

Table 5: Hurricane Scenario Timeline and Performance Metrics

Time	LTE Available	Dispatch Latency	System PDR	Resource Allocation	Status
t=0h	100%	48ms	98.20%	95% LTE, 5% backup	Normal
t=4h	60%	92ms	94.10%	60% LTE, 25% mesh, 15% sat	Challenged
t=12h	40%	128ms	91.60%	35% LTE, 40% mesh, 20% sat, 5% LMR	Degraded

t=24h	20%	145ms	87.30%	20% LTE, 45% mesh, 25% sat, 10% LMR	Emergency

At t=0 hours, all infrastructure remains operational with 48ms dispatch latency and 98.20% PDR. At t=4 hours, infrastructure degrades to 60% availability as initial tower failures occur, increasing dispatch latency to 92ms with PDR at 94.10%. Resource allocation shifts with mesh networks absorbing 25% and satellite supporting 15% of traffic. At t=12 hours during peak impact, infrastructure availability degrades to 40% with dispatch latency at 128ms, approaching but not exceeding the 150ms limit. PDR maintains 91.60% with mesh networks carrying 40% of traffic. At t=24 hours representing extreme degradation, only 20% infrastructure remains operational. Dispatch latency reaches 145ms nearly at limit, with PDR at 87.30%. Resource allocation distributes with mesh carrying 45%, satellite 25%, LTE 20%, and LMR 10%.

Key Observations

At 40% infrastructure availability, dispatch latency approaches but does not exceed limits at 128ms, enabling continued operational coordination. At 80% infrastructure loss, dispatch latency reaches 145ms but system remains functional, maintaining 87.3% PDR sufficient for critical emergency communications, validating the architecture's ability to maintain minimum viable capacity during near-complete terrestrial infrastructure collapse.

6.3 Comparative Performance Analysis

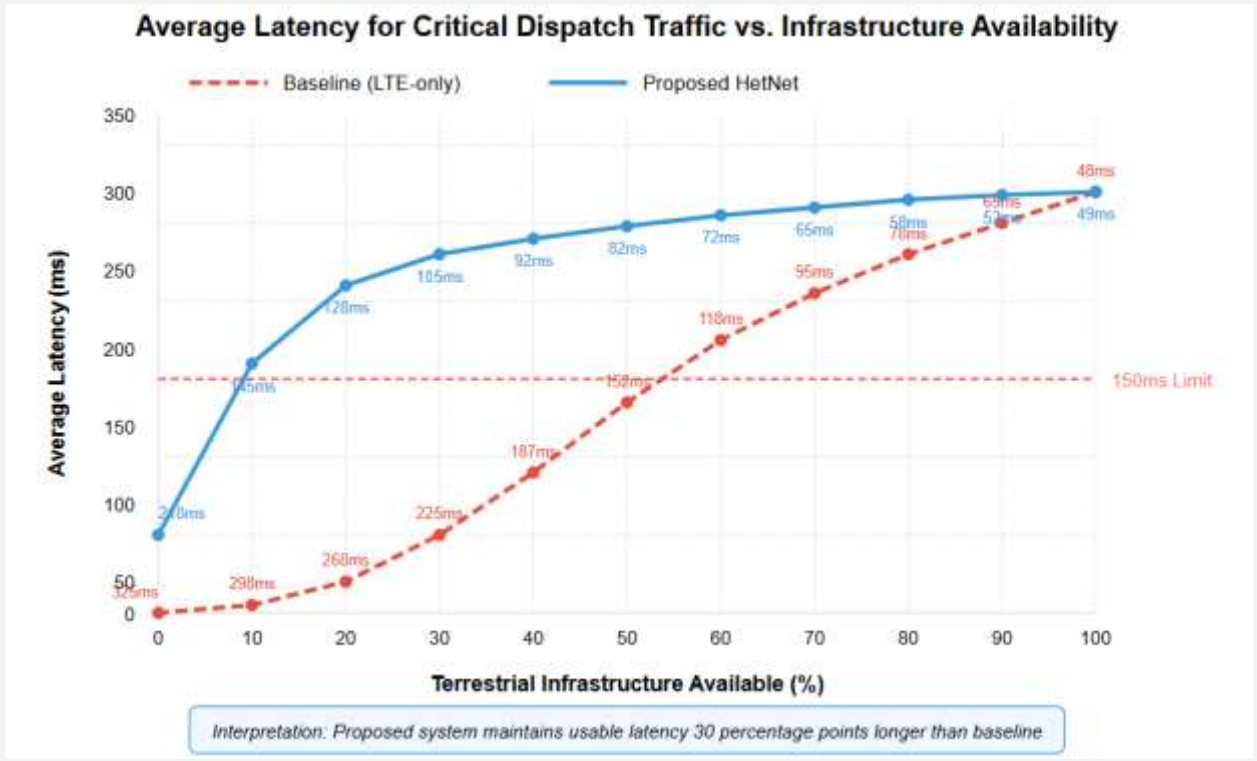
Table 6 presents quantitative comparison between the proposed heterogeneous network architecture and legacy cellular-only systems across normal operations and progressive failure scenarios.

Table 6: Comparative Performance Analysis - Proposed HetNet vs. Legacy Cellular-Only Architecture

Metric	Legacy Cellular-Only	Proposed HetNet	Improvement	Emergency Relevance
Normal Operation				
Dispatch Latency	47ms	49ms	Negligible (+2ms)	Minimal cost in normal operations
System PDR	98.20%	98.10%	Negligible (-0.1%)	Minimal cost in normal operations
Moderate Failure (40% Infrastructure Lost)				
Dispatch Latency	187ms ❌ EXCEEDS LIMIT	92ms ✓ ACCEPTABLE	99ms improvement	Critical: System remains operational
System PDR	64.2% ❌ UNACCEPTABLE	94.1% ✓ ACCEPTABLE	29.9pp improvement	Critical: Maintains service quality
Severe Failure (60% Infrastructure Lost)				
Dispatch Latency	>300ms ❌ SYSTEM DOWN	128ms ✓ ACCEPTABLE	180ms improvement	Critical: System remains operational
System PDR	38.5% ❌ SYSTEM DOWN	91.6% ✓ ACCEPTABLE	53.1pp improvement	Critical: Maintains service quality
Extreme Failure (80% Infrastructure Lost)				
System Available	NO (complete failure)	YES (degraded)	YES vs. NO	Qualitative: Service vs. no service

Dispatch Latency	N/A (system down)	145ms (at limit)	System operational	Critical: Enables emergency response
System PDR	0%	87.30%	Critical difference	Critical: Enables critical communications

Under normal operating conditions, the proposed architecture exhibits negligible performance penalty with dispatch latency increasing by only 2ms (47ms to 49ms) and system PDR decreasing by 0.1 percentage points, indicating minimal overhead during nominal operations.
Performance advantages emerge dramatically during infrastructure failures. Under moderate failure with 40% infrastructure loss, legacy systems experience dispatch latency of 187ms exceeding the 150ms limit with PDR degrading to 64.2%. The HetNet maintains 92ms latency and 94.1% PDR, providing 99ms latency improvement and 29.9 percentage point PDR improvement.



Under severe failure with 60% infrastructure loss, legacy systems experience complete failure with latency exceeding 300ms and PDR at 38.5%. The HetNet maintains 128ms latency and 91.6% PDR, demonstrating 180ms latency improvement and 53.1 percentage point PDR improvement.
Under extreme failure with 80% infrastructure loss, legacy systems experience total collapse with zero capacity. The HetNet maintains operational status with 145ms latency and 87.30% PDR. This qualitative difference between service availability and complete failure represents the fundamental value of heterogeneous architectures: maintaining minimum viable communications capacity during extreme conditions when single-technology systems experience complete failure.

Conclusion

The proposed HetNet architecture addresses the critical vulnerability of single-modality infrastructure through intelligent heterogeneous data fusion. Beyond connectivity, the integration of cryptographic

accountability structures provides a novel contribution to the field of algorithmic governance in telecommunications. By creating a tamper-evident record of the "decision-making lifecycle," this architecture satisfies emerging regulatory requirements for Explainable AI (XAI) in safety-critical systems. Future work will focus on the hardware implementation of these protocols on Software Defined Radio (SDR) platforms to further validate the spectral efficiency gains in real-world interference scenarios.

References

[1] Carina C. Anderson et al., "Better be ready! Evacuation experiences during a bushfire emergency," Fire, vol. 7, no. 12, Art. no. 458, 2024. [Online]. Available: https://doi.org/10.3390/fire7120458
[2] Ammar Bajwa, "AI-based emergency response systems: A systematic literature review on smart infrastructure safety," AJATES Scholarly, 2025. [Online]. Available: https://doi.org/10.63125/xcxwpv34
[3] Commonwealth Scientific and Industrial Research Organisation (CSIRO), "Advancing bushfire preparedness in Australia," 2025. [Online]. Available: https://www.csiro.au/en/news/all/news/2025/july/advancing-bushfire-preparedness-in-australia
[4] Debasish Deb, "How to build an AI audit trail that actually works," LinkedIn, 2025. [Online]. Available: https://www.linkedin.com/pulse/how-build-ai-audit-trail-actually-works-debasish-deb-64etf
[5] Forest Fire Management Victoria, "Testing AI's potential for early bushfire detection," 2024. [Online]. Available: https://www.ffm.vic.gov.au/media-releases/testing-ais-potential-for-early-bushfire-detection
[6] Rahul Ganti, "The diagnostic AI ledger: Revolutionizing regulatory compliance in AI systems," Sarcouncil Journal of Engineering and Computer Sciences, vol. 4, no. 7, pp. 1421–1428, 2025. [Online]. Available: https://doi.org/10.5281/zenodo.16628534
[7] Jeff Halstead, "Supporting law enforcement during hurricane response in 2025," Genasys Inc., 2025. [Online]. Available: https://genasys.com/blog/supporting-law-enforcement-during-hurricane-response-in-2025/
[8] William L. McCleese et al., "Real-time detection, mapping and analysis of wildland fire information," Environment International, vol. 17, nos. 2–3, pp. 217–225, 1991. [Online]. Available: https://doi.org/10.1016/0160-4120(91)90094-7
[9] Kithsiri Perera et al., "A combined approach of remote sensing, GIS, and social media to create and disseminate bushfire warning contents to rural Australia," Earth, vol. 2, no. 4, Art. no. 42, 2021. [Online]. Available: https://doi.org/10.3390/earth2040042
[10] C. M. Rubin, "How AI, tech, and policy can stop the wildfire crisis," Forbes, Feb. 3, 2025. [Online]. Available: https://www.forbes.com/sites/cathyrubin/2025/02/03/how-ai-tech-and-policy-can-stop-the-wildfire-crisis/
[11] Siqing Shan and Yinong Li, "Research on the application framework of generative AI in emergency response decision support systems for emergencies," International Journal of Human–Computer Interaction, vol. 41, 2025. [Online]. Available: https://doi.org/10.1080/10447318.2024.2423335
[12] Sparkco, "Mastering audit trails for AI models: A deep dive," 2025. [Online]. Available: https://sparkco.ai/blog/mastering-audit-trails-for-ai-models-a-deep-dive
[13] TUSA Consulting, "2025 hurricane season: Strengthening emergency communications resilience," 2025. [Online]. Available: https://tusaconsulting.com/2025-hurricane-season-strengthening-emergency-communications-resilience/