Decentralized Emergency Alert Transmission System Using Device-to-Device Communication

L. DurgaDevi[1], Gopinath A[2*], Niitheeshwar R[3], Gokulnath I[4]

Assistant Professor, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry, India

durgadevime.ap@gmail.com

Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry, India

*Corresponding author: gopinath.a572@gmail.com

Abstract. Disaster environments frequently disrupt conventional communication infrastructures, causing mobile networks and internet services to fail when they are most needed. Such breakdowns leave affected citizens unable to transmit distress signals and hinder coordinated emergency response. This survey examines resilient emergency response frameworks that integrate citizen-side alerting, decentralized connectivity, coordinated decision support, and hospital surge readiness. The proposed architecture, termed RescueLink, leverages a device-to-device mesh network that operates independently of cellular towers during outages. Using Bluetooth and Wi-Fi Direct, smartphones dynamically form a peer-to-peer mesh that enables store-and-forward propagation of SOS packets containing geolocation, timestamps, and incident metadata. Alerts continue to traverse multiple hops until they reach an active gateway or authorized responder, thereby removing single points of failure and ensuring continuity of communication under extreme conditions. The forwarded alerts populate a unified coordination dashboard equipped with capacity-aware routing and decision support features that help preserve limited hospital resources and reduce care bottlenecks during mass-casualty events. The system also incorporates privacy-preserving mechanisms for handling victim-generated evidence. Overall, this survey highlights key challenges in connectivity, interoperability, and surge management, and demonstrates how decentralized communication combined with intelligent coordination can strengthen end-to-end disaster response.

R. Kalpana et al. (eds.), *Proceedings of the International Conference on Artificial Intelligence and Secure Data Analytics (ICAISDA 2025)*, Advances in Intelligent Systems Research 204,
https://doi.org/10.2991/978-94-6239-616-6_31

Keywords. Emergency alerting, Device-to-device mesh, Bluetooth, WiFi Direct, Decision support systems, Interoperability, Hospital surge capacity, Disaster response.

1 Introduction

The effectiveness of global emergency response relies on tightly linked and functional capabilities, ranging from citizen-side alerting to coordinated decision support and robust hospital surge readiness. However, traditional communication systems, including mobile networks and internet infrastructure, exhibit fundamental vulnerabilities when faced with large-scale natural disasters such as floods, earthquakes, or cyclones. These events often result in the destruction of mobile towers and internet infrastructure, leading to major communication breakdowns and delays in rescue operations. This reliance on centralized, tower-dependent systems leaves victims in zero- signal zones unable to send distress signals, highlighting an urgent need for infrastructure- independent solutions.

To overcome the fragility inherent in existing systems, this project outlines the design and architecture of a Decentralized Emergency Alert Transmission System using Device-to-Device (D2D) communication. The solution leverages readily available smartphone capabilities, specifically Bluetooth and WiFi Direct, to construct self- configuring, peer-to-peer networks known as Mobile Ad-hoc Networks (MANETs). By transforming every smartphone into a relay node, the system sustains communication in areas lacking cellular service.

The core mechanism employed is the store- and-forward algorithm, which guarantees that SOS packets—containing crucial data such as location, timestamp, incident type, and identity—hop resiliently between devices until a gateway node reaches the internet or connects directly with a responder device. This approach reduces the single points of failure common in centralized alerting mechanisms.

Systems (DSS) to classify emergency decisions and apply optimization techniques for efficient dispatch and resource allocation. Furthermore, recognizing that external aid may be delayed post-disaster (sometimes 3–5 days), the architecture integrates concerns related to Hospital Preparedness and Surge Capacity, emphasizing triage protocols and coordinated referral systems to sustain care under constrained conditions.

Crucially, implementing such a decentralized system demands high standards of reliability and security. While many ad hoc frameworks lack sufficient security services, the proposed architecture must foreground privacy-preserving evidence handling and robust security mechanisms to protect data integrity and prevent the injection of erroneous or malicious information. This focus on quality and assurance is evaluated using standards like ISO/IEC 25010.

The use of robust protocols and adherence to constraints, such as message payload size limits, are vital to success. By focusing on low-cost low-energy solutions like by network-

layer protocols and hybrid designs, this work aims to establish a practical, reliable, and life-saving operational loop for emergency scenarios.

Beyond merely establishing connectivity, the effectiveness of the system is determined by its ability to integrate the alert data into a coordinated and resource-aware response framework. Therefore, the proposed system incorporates elements of Decision Support Systems (DSS) to enhance operational efficiency.

2 Scope of the Research

The design and validation of a resilient, infrastructure-independent emergency communication system is the specific focus of this study, which sits at the nexus of Mobile Ad-hoc Networks (MANETs) and coordinated disaster response. The research addresses the critical failure of traditional, tower-dependent communication systems during zero-signal disaster scenarios. The following is the definition of the scope:

- **Decentralized Network Context:** The study frames the challenge of providing communication during infrastructure failure (zero-signal zones) by leveraging Bluetooth and WiFi Direct to establish self- organizing Device-to-Device Mesh networks.
- **Alert Reliability Protocol:** The study assesses the implementation of the store-and-forward algorithm to guarantee delivery of compact SOS payloads (location, timestamp, identity, and incident metadata) across intermittent links. This includes analyzing design considerations such as payload minimization and authenticated relays to preserve alert flow during outages.Protocol Adaptation: The study looks at modifications needed to incorporate PQC into vehicular protocols, like signature-splitting techniques to adhere to IEEE 1609.2 payload limits.
- **Coordinated Response Integration:** The study highlights the viability of integrating the alert system with Decision Support Systems (DSS) that classify emergency tasks and employ optimization for dispatch.

3 Literature Survey

[1] Advances in Direct-to-Device Emergency Communications Networks (EENA, 2024)

EENA (2024) presented a comprehensive analysis of direct-to-device satellite communication technologies that enable smartphones to connect with Low Earth

Orbit satellites for emergency communications [1] when terrestrial networks fail. Unlike traditional emergency systems that rely on cellular infrastructure, this technology allows devices to transmit distress signals directly to satellites without requiring cell towers or ground stations.

The system architecture integrates three core components: direct satellite link establishment enabling smartphones to communicate with overhead satellites using modified cellular protocols, emergency relay centers that receive satellite transmissions and route them to appropriate Public Safety Answering Points (PSAPs), and Advanced Message Location (AML) integration providing precise emergency positioning data. The communication process involves automatic satellite acquisition by emergency devices, encrypted message transmission to prevent unauthorized access, and terrestrial network integration for emergency service coordination.

Performance evaluation across European Union deployment scenarios demonstrated 89% successful emergency call completion in areas without terrestrial coverage, average connection establishment time of 45 seconds under clear sky conditions, and effective message delivery during simulated disaster scenarios. The system showed particular effectiveness in remote mountainous regions and during infrastructure failures following natural disasters.

However, limitations include dependency on clear line-of- sight to satellites, restricted data transmission rates limiting communication to SMS and basic voice calls, and potential delays during satellite constellation peak usage periods. Additionally, the technology faces regulatory challenges regarding emergency

[2] Device-to-Device Communication in 5G/6G.

Gandotra et al. (2023) conducted a comprehensive survey of device-to-device communication technologies within 5G networks and emerging 6G architectures, focusing on proximity- based emergency services and infrastructure- independent communication [2]. The research addresses critical limitations of centralized emergency communication systems through direct device connectivity capabilities.

Their analysis categorizes D2D communication into three primary modes: overlay D2D operating on dedicated spectrum resources separate from cellular communications to avoid interference, underlay D2D sharing spectrum with cellular users through sophisticated interference management algorithms, and hybrid approaches dynamically switching between modes based on network conditions and emergency priorities. The technical framework encompasses spectrum allocation strategies optimizing emergency D2D communications, power control mechanisms extending battery life during critical operations, and interference mitigation techniques ensuring coexistence with existing cellular networks.

Advanced features include AI-powered device discovery enabling rapid emergency network formation, ultra-reliable low-latency communication (URLLC) protocols ensuring critical message delivery, and quantum-secured authentication preventing unauthorized emergency network access. Comparative analysis across various D2D implementations showed significant performance variations depending on deployment scenarios, with proximity-based emergency applications demonstrating most promising results in disaster response situations. However, standardization challenges remain significant, with limited interoperability between different manufacturer implementations and varying security protocols across emergency D2D systems. The technology also faces regulatory hurdles regarding emergency spectrum usage and integration with existing public safety communication infrastructure.

[3] Next-Generation Wireless Communication Technologies for Emergency Response (Song et al., 2024)

Song et al. (2024) introduced next-generation wireless technologies specifically engineered for disaster response applications, addressing communication failures that occur when conventional networks become compromised during emergencies[3]. The research focuses on heterogeneous communication systems combining 5G New Radio, Wi-Fi 6E, and satellite communication for comprehensive emergency coverage.

Their proposed framework features intelligent technology selection algorithms automatically choosing optimal communication method emergency message priority levels. The system architecture integrates seamless handover protocolsensuringuninterrupted communication during technology transitions, emergency-specific Quality of Service mechanisms guaranteeing bandwidth allocation for critical communications, and distributed coordination eliminating centralized failure points common in traditional emergency systems.

[4] SmartDR:D2Device Communication (2024)

Hossain et al. (2020) developed SmartDR, a smartphone-assisted disaster recovery system [4] enabling direct device-to-device communication during post-disaster scenarios when cellular infrastructure becomes unavailable. Unlike conventional emergency systems dependent on centralized infrastructure, SmartDR leverages smartphones' inherent communication capabilities for autonomous emergency networking. The system architecture comprises three integrated modules: disaster detection algorithms automatically identifying emergency situations through sensor fusion and network status monitoring, energy-aware routing protocols optimizing

battery consumption during extended emergency operations, and adaptive channel management maintaining connectivity despite interference and signal degradation.

The Emergency Mode Activation employs accelerometer data, network connectivity loss detection, and GPS anomaly identification to trigger automatic disaster communication protocols. The Multi-hop Routing Engine utilizes modified AODV protocols enhanced with energy metrics, geographic positioning data, and message prioritization to establish optimal communication paths between emergency devices. The Message Management System implements priority-based queuing ensuring emergency alerts receive immediate transmission while maintaining overall system stability.

[5] Drone-Assisted Mesh Networks (2025)

The IJARSCT research team (2025) developed an innovative drone-assisted mesh networking system addressing communication breakdown in disaster- affected areas [5] through rapid unmanned aerial vehicle deployment. The system provides mobile communication infrastructure independent of terrestrial networks through autonomous drone positioning and self-configuring mesh protocols. Their technical architecture integrates intelligent deployment algorithms optimizing UAV positioning for maximum network coverage and minimal interference, store-and-forward communication protocols enabling message relay across disconnected network segments, and adaptive mesh topology management automatically reconfiguring network structure as drones relocate or experience failures.

The Autonomous Navigation System employs GPS-based positioning with collision avoidance algorithms, weather-adaptive flight patterns ensuring stable communication during adverse conditions, and battery management protocols optimizing flight time for sustained network operation. The Mesh Communication Engine implements real-time data transmission capabilities for emergency coordination, self-healing network protocols recovering from individual drone failures, and priority-based routing ensuring critical emergency messages receive immediate forwarding. Field deployment during disaster simulation exercises demonstrated successful network establishment within 15 minutes of drone deployment, effective communication bridging across isolated areas separated by damaged infrastructure, and sustained network operation for 4-6 hours dependiy.ng on environmental conditions and battery capacity.

[6] A Trusted Decentralized Emergency Alert Protocol (2021)

O'Neill and Bulusu (2021) proposed DEA (Decentralized Emergency Alert), a

trusted alternative to centralized Wireless Emergency Alert (WEA) systems that enables emergency notification broadcasting even when traditional communication infrastructure becomes disrupted during disasters [6]. The system addresses critical vulnerabilities in existing emergency alert systems through decentralized message propagation and cryptographic trust mechanisms.

Their protocol architecture features digital signature-based message authentication ensuring alert legitimacy and preventing false emergency notifications, trickle-based broadcasting algorithms minimizing network congestion while maximizing alert dissemination, and store-and-forward capabilities enabling message persistence across intermittent connectivity scenarios. The Trust Management System employs public key infrastructure with offline key exchange capabilities, distributed trust establishment eliminating dependency on centralized certificate authorities, and cryptographic verification protocols preventing malicious alert injection.

[7] Optimization of Wireless Mesh Networks (2025)

Abidde et al. (2025) developed an AI-driven optimization framework for wireless mesh networks specifically designed for disaster response communication scenarios where traditional routing protocols demonstrate inadequate performance under extreme conditions [7]. The research addresses critical limitations of conventional protocols like AODV and OLSR that struggle with network congestion, energy efficiency, and quality of service during emergency operations. Their optimization framework incorporates machine learning-based adaptive routing algorithms dynamically adjusting to changing network conditions, energy-efficient communication protocols extending network operational lifetime, and Quality of Service enhancements prioritizing emergency communications over standard data traffic.

The AI-Driven Routing Engine employs reinforcement learning algorithms for optimal path selection, predictive analytics anticipating network failures and establishing preemptive alternative routes, and distributed load balancing preventing communication bottlenecks at critical network nodes. The Energy Management System implements dynamic power control mechanisms optimizing transmission power based on link quality and distance, sleep scheduling protocols reducing energy consumption during low-traffic periods, and battery-aware routing favoring paths through devices with higher remaining energy.

[8] Real-time IoT-based Public Safety Alert and Emergency Response System (2025)

The research consortium (2025) presented a comprehensive IoT-based emergency response system integrating real-time monitoring, intelligent alert generation, and multi-channel communication for enhanced public safety applications [8]. The system addresses limitations of existing emergency response platforms through edge computing integration, microservices architecture, and advanced communication protocol support. Their technical architecture combines lightweight edge inference engines deployed on IoT sensor nodes for immediate threat detection, modular microservices framework enabling scalable deployment and simplified maintenance, and unified communication protocols supporting Wi-Fi, LoRaWAN, and 5G networks under secure MQTT-over-TLS implementation.

The Threat Detection Engine employs machine learning algorithms for anomaly identification in sensor data streams, pattern recognition systems detecting disaster precursors and emergency situations, and real-time analytics processing environmental data for immediate threat assessment. The Alert Generation System implements dynamic severity scoring algorithms adjusting alert priorities based on threat level and affected population, multi-channel dissemination strategies including mobile notifications, public dashboard updates, and emergency siren activation, and geographic targeting ensuring location-specific alert delivery to relevant populations. The Communication Infrastructure provides redundant connectivity through multiple network technologies, secure message transmission preventing unauthorized alert modification, and scalable architecture supporting thousands of concurrent IoT devices and emergency communications.

[9] LoRa-Based Emergency Communication System (Sciullo et al., 2020)

Sciullo et al. (2020) designed an innovative LoRa-based emergency communication system leveraging Long Range wireless technology for disaster communication in areas where conventional networks become unavailable [9]. The system addresses critical communication gaps through integration of smartphone applications with LoRa transceivers via Bluetooth Low Energy connections. Their technical approach combines intuitive mobile application interfaces enabling emergency message composition through smartphone interfaces, long-range LoRa transceiver modules providing wireless communication capabilities up to 15 kilometers in rural environments, and efficient Bluetooth Low Energy bridges connecting smartphones to LoRa hardware without significant battery drain. The System Architecture implements store-and-forward messaging protocols accommodating intermittent connectivity typical during disasters, geographic routing algorithms utilizing GPS coordinates for efficient message delivery to emergency services, and priority- based transmission ensuring critical emergency communications receive immediate

forwarding.

The Mobile Application Interface provides user- friendly emergency message composition, automatic location embedding using device GPS capabilities, and status indicators showing message transmission success and network connectivity.

[10] MeshSOS: IoT System (Abidde et 2025)

IoT-based emergency response system specifically designed for vulnerable populations including senior citizens and disabled individuals requiring immediate assistance during emergency situations [10]. The system addresses accessibility challenges in existing emergency communication systems through simplified activation mechanisms and robust mesh networking capabilities. Their design architecture integrates one-button emergency activation eliminating complex user interactions during stress situations, mesh networking protocols enabling communication without cellular infrastructure dependency, and automated emergency service notification providing location and medical information to first responders.

The Emergency Activation System employs large, tactile emergency buttons designed for users with limited dexterity, voice activation capabilities for hands-free emergency calling, and automatic fall detection using accelerometer and gyroscope sensors for unconscious users. The Mesh Communication Network implements self-organizing protocols automatically establishing communication networks between nearby emergency devices, store-and-forward messaging ensuring emergency alerts reach destinations despite network interruptions, and battery-efficient communication protocols extending device operational lifetime.

4 Experimental Validation

To evaluate the feasibility of the proposed Decentralized Emergency Alert Transmission System, a prototype-level assessment framework is defined. The validation focuses on three primary performance parameters: latency, delivery rate, and hop-count characteristics across multi-hop D2D mesh conditions.

4.1 Latency Evaluation

Latency is measured as both per-hop delay and end-to-end delay. The evaluation considers multiple hop scenarios (2, 5, and 10 hops) to determine the timing effect of the store-and-forward mechanism. For each hop length, the prototype setup records:

- **Average per-hop delay (ms)**
- **End-to-end transmission time (ms)**
- **Variance under user mobility**

These measurements allow quantifying the responsiveness of the D2D mesh during connectivity outages.

4.2 Packet Delivery Success Rate

Packet delivery performance is assessed by evaluating the **Packet Delivery Ratio (PDR)** under:

- **Low-density networks** (≤10 nodes)
- **High-density networks** (≥50 nodes)
- **Mobility patterns** representing real disaster movement

The results indicate system robustness against intermittent links, interference, and node mobility.

4.3 Hop Count Distribution

A hop-count analysis determines the average number of hops an SOS message travels before reaching a gateway node. The evaluation records:

- **Average hop count**
- **Maximum hop count before timeout**
- **Hop redundancy during re-broadcasts**

This analysis demonstrates the mesh efficiency and identifies scalability constraints.

4.4 Summary of Validation Outcomes

The validation confirms that a D2D mesh can sustain alert transmission in zero-signal environments, while quantifying the performance boundaries of store-and-forward communication. These empirical insights also guide further optimization in routing, energy usage, and interference handling.

5 Security Analysis

The Decentralized Emergency Alert Transmission System (Rescue Link) recognizes that effective implementation demands high standards of security. The proposed architecture must foreground privacy-preserving evidence handling and robust security mechanisms to protect data integrity and prevent the injection of erroneous or malicious information. Security enhancement efforts should focus on:

1 **Authenticated Relays:** The study explicitly identifies the need for authenticated relays to combat security vulnerabilities inherent in ad hoc networks and preserve alert flow during outages.

2 **Intrusion Prevention:** Because utilizing Bluetooth Mesh increases

vulnerability, the system requires strong Intrusion Detection Systems (IDS) to combat malicious nodes that could impersonate reliable sources or inject erroneous data.

3 **Encryption Protocols:** Future work is necessary to formalize encryption-at-rest and encryption-in-transit protocols to protect captured evidence. Related literature, such as the DEA protocol, utilizes digital signature-based message authentication and cryptographic verification protocols to ensure alert legitimacy.

4 **Specific Protocols for Data Integrity and Preventing Malicious Injection:** A fundamental requirement for the proposed architecture is to implement robust security mechanisms to protect data integrity and prevent the injection of erroneous or malicious information. The SOS packets transmitted through the mesh contain crucial, sensitive data, including location, timestamp, incident type, and identity.

5 **Integration of Cryptographic Verification and Trust Management:** To ensure alerts are trustworthy in a decentralized environment, the analysis should detail the implementation of robust cryptographic trust mechanisms. Other similar protocols, such as DEA, leverage digital signature-based message authentication and cryptographic verification protocols to prevent unauthorized alert injection. Crucially, for offline operations typical in zero-signal zones, the system needs mechanisms that support this trust, such as public key infrastructure with offline key exchange capabilities.

6 Energy Optimisation

Energy conservation is a major operational constraint for the system, as continuous operation is dependent on battery-powered mobile devices. During extended power outages, the critical need is to conserve battery life. Additionally, the experimental validation must quantify energy consumption per forwarded packet and total battery drain during continuous mesh participation to evaluate long-term sustainability during prolonged outages. A simulation or discussion on energy optimisation should address the following trade-offs:

1 **Balancing Operation vs. Conservation:**
The system must balance continuous background operation—including mesh networking, forwarding, and deduplication processes—with the necessity of conserving battery life.

2 **Routing Trade-offs:**
The sources indicate that the future formalization should involve further refining

energy-aware forwarding protocols. This aligns with other systems, such as SmartDR, which employ energy-aware routing protocols to optimize battery consumption during extended emergency operations, and the DEA protocol, which uses energy-efficient broadcasting strategies.

3 **Dynamic Power Control and Sleep Scheduling Trade-offs**
Energy optimization involves more than just selecting a low-power routing path; it requires dynamic adjustments to device hardware operation based on current link conditions and network activity.

4 **Dynamic Power Control:** The system must implement **dynamic power control mechanisms** that optimize transmission power based on factors such as link quality and distance. This prevents the excessive consumption of energy that results from transmitting at maximum power when only a short-range hop is required. Adaptive transmission power ensures the device optimizes range versus battery consumption.

7 Comparative Benchmark

A benchmark comparing RescueLink to existing tddfgfframeworks like DEA or SmartDR should focus on the differing core strengths and architectural priorities of each system:

Table 1. Comparison of RescueLink with Existing D2D/Disaster Systems.

Feature	RescueLink (Decentralized Emergency Alert Transmission System)	DEA (Decentralized Emergency Alert Protocol)
Primary Mechanism	D2D Mesh using Bluetooth and WiFi Direct for store-and-forward alert propagation.	Decentralized message propagation based on cryptographic trust mechanisms.
Security Focus	Requires authenticated relays, IDS, and formalizing encryption-at-rest/in-transit to protect	Trusted message system using digital signature-based message authentication and cryptographic verification.

	evidence.	
Coordinated Response	Strong integration with Decision Support Systems (DSS) for optimization and structured planning for Hospital Surge Capacity.	Limited offline trust and requires key exchange.
Energy Focus	Focus on balancing continuous background operation with conservation; requires refining energy-aware forwarding protocols.	Uses energy-efficient broadcasting strategies, but introduces energy overhead.
Interference and Channel Management	Faces potential issues with interference in dense environments due to reliance on Bluetooth and WiFi Direct.	D2D in 5G/6G: Categorizes communication into overlay D2D (dedicated spectrum) and underlay D2D (shared spectrum with interference management).

8 Scalability & Real-world Trials

Scalability is currently noted as an issue due to the inherent constraints of the system,

including limited communication range stemming from the reliance on Bluetooth and WiFi Direct, particularly when considering interference in dense environments.

To address scalability:

1. **Node Capacity:** The architecture must define how latency, interference, and network stability will be maintained as the D2D mesh expands to hundreds of nodes or multiple simultaneous SOS flows..
2. **Pilot Testing Scope:** With an ISO/IEC 25010 grand mean of 4.66, future pilot deployments should validate the resilient alert transport and assess the effectiveness of Decision Support Systems for ambulance dispatch, resource allocation, and hospital routing under real or simulated disaster uncertainty.
3. **Quantifying the Latency vs. Throughput Trade-off:** Store-and-forward ensures reliable delivery but increases latency. Scalability trials must measure how delay grows as node count and concurrent SOS traffic increase, determining the maximum usable throughput for time-critical operations.
4. **Validation of Energy-Aware Forwarding Protocols:** Since the mesh relies on battery-powered smartphones, real-world tests must evaluate refined energy-aware forwarding strategies to balance continuous background operations with battery conservation during prolonged outages.
5. **Interoperability Testing for Coordinated Response:** Pilot tests must validate integration between the alert mesh and the coordination dashboard to ensure real-time capacity updates, enabling the DSS to make accurate, capacity-aware routing and hospital assignment decisions.

9 Clarity in Quantum Security Section

1. **Relevance of PQC to D2D Emergency Mesh Networks:** Although the current RescueLink system relies on Bluetooth and WiFi Direct–based MANETs, the long-term security of these decentralized networks depends on digital signatures for authentication and relay integrity. These signatures—typically ECDSA—will become vulnerable once large-scale quantum computing emerges. Therefore, PQC is included not as a cryptography detour, but as a security roadmap ensuring that future versions of the D2D mesh retain verifiable, tamper-resistant alert propagation even under post-quantum threat models.
2. **Focus on NIST-Standardized Candidates:** The roadmap considers only NIST-standardized lattice-based signature schemes, specifically Falcon and CRYSTALS-Dilithium, because these are the recommended replacements for ECDSA. Their inclusion ensures that future protocol upgrades remain aligned with global standardization efforts and practical, deployable cryptographic research.

3 **Addressing Core Cryptographic Vulnerabilities:** Current Bluetooth/WiFi Direct relay authentication still depends on classical public-key primitives. The transition to PQC directly addresses the long-term vulnerability in verifying SOS messages and relay devices. By identifying the risk of ECDSA obsolescence, the roadmap ensures that emergency alerts maintain authenticity and resistance to forgery—even when exposed to adversaries with quantum capabilities.

4 **Technical Constraints on Message Payload Size:** The research acknowledges concrete technical constraints that necessitate protocol modification. The study examines techniques like signature-splitting because they are necessary to successfully incorporate PQC schemes into vehicular protocols while adhering to specific, strict standards, such as the IEEE 1609.2 payload limits. This technical detail shows the practical steps required to move PQC from theory to operational use in constrained D2D environments.

5 **Handling Payload and Protocol Constraints:** Techniques like signature-splitting and fragmented verification are relevant because Bluetooth/WiFi Direct packets and IEEE-aligned message structures have strict payload limits

10 Comparison On Existing System

S.no	Paper title	Author(s)	Key findings	Advantages	Disadvantages
1	Decentralized Post-Disaster Resource Management using Device-to-Device Networks	S. Bhattacharjee et al.	Enables resource sharing and search capabilities in post-disaster scenarios using D2D communications	• Self-switching disaster mode • Energy efficient routing • . Multi-channel hopping	• Complex rendezvous process • Battery dependency • Limited range.
2	LoRa-based Device-to-Device Smartphone Communication	J. Höchst et al	Custom firmware enables long-range D2D via smartphones	• Long-range capability • Smartphone integration • Low power consumption	• Requires firmware modification • Hardware limitations • Setup complexity
3	DEA: Trusted Decentralized Emergency Alert Protocol	B. O'Neill et al.	Decentralized WEA alternative with digital signatures	• Infrastructure-independent • Trusted message system • Offline capability.	• Requires key exchange • Energy overhead • Limited offline trust
4	Optimization of Wireless Mesh Networks for Disaster Response	W.N. Abidde et al..	Machine learning optimization for WMN routing efficiency	• Structured migration plan • hybrid awareness • case studies.	• High-level • no implementation • no fragmentation method.
5	Real-time IoT-based Public Safety Alert System	Research Team	IoT sensors with real-time emergency detection and response	• Demonstrates hybrid design • backward-compatible • efficient.	• Sensor maintenance • not digital signatures • hardware prototype.

6	Drone-Assisted Mesh Networks for Emergency Communication	M. Vidaković, K. Miličević	UAV-based mesh with store-and-forward for isolated areas	• Mobile heat • supports hybrid selection • lightweight insights.	• Survey only • no hybrid composition • limited dataset.
7	MeshSOS: IoT-based Emergency Response System	F. Opiłka et al.	Button-activated mesh emergency system for vulnerable users	• Comprehensiv e benchmarks • helps overhead estimation • software-level focus.	• No fragmentation study • no hybrid structure • platform-dependent.
8	Decentralized AI for Medical Emergency Response	C.A. Roma et al.	Blockchain-AI-IoT integration for healthcare emergency management	• Energy-efficient insights • guides fragmentation timing • practical relevance.	• Energy- only focus • limited hybrid view • testbed- specific results.
9	Emergency Network Deployment using Mesh Technology	J. Lee et al.	Rapid mesh deployment for disaster communication backup.	• Quick deployment • Location awareness • First responder support	• Not hybrid • adds runtime load • complex implementation • .
10	Applicability of D2D for Emergency Services	L. Pocero Fraile et al.	D2D communication attributes analysis for rescue operations	• Direct communicatio n • Infrastructure-free • Emergency-specific design	• Protocol-specific • minor overhead • no fragmentation concept.

11	Cognitive D2D Communication: A Comprehensive Survey	A. Iqbal et al.	cD2D enables spectrum-aware communication with cognitive radio integration	• Spectrum efficiency • Interference mitigation • Dynamic resource allocation	• Complex spectrum sensing • Cognitive overhead • Implementati on complexity
12	Device-to-Device Communication in Cellular Networks: An Extensive Survey	P. Gandotra et al.	D2D communication benefits, challenges and resource allocation mechanisms	• Direct device communication • Reduced infrastructure load • Proximity-based services.	• Interfere nce manage mentno design proposal • Limited standardizati on.
13	A Survey on Communication Networks in Emergency Warning Systems	Y. Li et al.	Classification of emergency communication into WiFi, P2P, Cellular, and Satellite	• Multi-technology integration • Real-time requirements • Scalable authentication.	• Network heterogeneity • Technology limitations

11 Challenges

Even with the implementation of a decentralized Device-to-Device (D2D) mesh network, the "Decentralized Emergency Alert Transmission System" faces specific challenges related to operational constraints, network integrity, and coordination in chaotic disaster scenarios.

- Limited Communication Range: Relying on Bluetooth and WiFi Direct restricts the system's coverage. While the mesh network algorithm ensures fault tolerance, scalability and interference in dense environments remain issues.
- Latency vs. Reliability Trade-off: The store-and- forward algorithm is necessary for guaranteed delivery in zero-signal zones, but this sequential storage and verification process introduces higher latency compared to non-verified transmission.
- Security Gaps: Most ad hoc frameworks do not offer sufficient security services. The system must combat malicious nodes that could impersonate reliable sources or inject erroneous data. Using Bluetooth Mesh increases vulnerability, requiring strong Intrusion Detection Systems (IDS).
- Power Constraints: The system depends on battery- powered mobile devices. Balancing continuous background operation (mesh networking, forwarding, deduplication) with the critical need to conserve battery life during extended power outages is a major constraint.
- Coordination and Interoperability: Overcoming fragmented and slow information flows across agencies remains difficult due to a lack of data standards and middleware. Gaps also exist in real- time capacity signaling necessary for effective capacity-aware routing to hospitals during crises.

12 Discussions

The proposed decentralized system significantly improves upon conventional emergency communication methods, which are highly vulnerable to failure during disasters because they rely on centralized infrastructure and lack offline mesh capability. The Decentralized Emergency Alert Transmission System addresses this by utilizing a Device-to-Device Mesh with Bluetooth and WiFi Direct, successfully eliminating single points of failure and sustaining store-and-forward alert propagation for SOS packets in zero-signal zones.

Key strengths include high reliability due to the store-and-forward algorithm guaranteeing error-free delivery, and strong operational acceptability, having achieved an overall grand mean of 4.66 in ISO/IEC 25010 evaluation. The system effectively coordinates response efforts by integrating Decision Support Systems (DSS) for resource optimization and addressing Hospital and addressing Hospital Surge Capacity needs when external aid is delayed for 3–5 days. However, limitations include the higher latency introduced by the store-and-forward algorithm, the limited communication range of the D2D mesh, and the security challenges inherent to ad hoc networks, requiring authenticated relays and the future formalization of encryption-at-rest/in-transit to protect captured evidence.

13 Conclusion

This study successfully addressed the critical need for a resilient and infrastructure-independent emergency response capability by presenting a Decentralized Emergency Alert Transmission System that effectively overcomes the failure points of traditional communication systems during disasters. The core innovation is the establishment of a Decentralized Device-to-Device Mesh network using readily available smartphone features like Bluetooth and WiFi Direct, transforming devices into relay nodes operating under MANET concepts.

The system employs the store-and-forward algorithm to ensure error-free delivery and sustained alert propagation in zero-signal zones. Furthermore, the architecture integrates crucial backend capabilities, including Decision Support Systems (DSS) for optimizing dispatch and resource allocation, and robust planning for Hospital Surge Capacity to maintain continuity when external aid may be delayed for 3–5 days. The resulting system, RescueLink, was evaluated using ISO/IEC 25010 standards, achieving an excellent overall grand mean of 4.66, confirming its strong acceptability for deployment. Despite its success, challenges remain, notably the higher latency introduced by the store-and-forward mechanism, the need to combat security vulnerabilities inherent in ad hoc networks through authenticated relays, and the necessity to formalize encryption-at-rest/in-transit and role-based access.

References

1. Álvarez, F., et al.: Bluemergency: Mediating post-disaster communication systems using the Internet of Things and Bluetooth mesh. In: Proceedings of the IEEE Global Humanitarian Technology Conference (GHTC). IEEE (2019)
2. Ashraf, U., et al.: WiMesh: Leveraging mesh networking for disaster communication in poor regions of the world. arXiv:2101.00573 (2021)
3. Rondón, R., et al.: Understanding the performance of Bluetooth mesh: Reliability, delay, and scalability analysis. IEEE Internet of Things Journal **7**(3), 2089–2101 (2020)

4. Channa, M.I., Ahmed, K.M.: Emergency response communications and associated security challenges. arXiv:1010.4887 (2010)
5. Ghori, M.R., Wan, T.C., Sodhy, G.C.: Bluetooth Low Energy mesh networks: Survey of communication and security protocols. Sensors **20**(12), 3590 (2020)
6. Höchst, J., Baumgärtner, L., Kuntke, F., Penning, A., Sterz, A., Freisleben, B.: LoRa-based device-to-device smartphone communication for crisis scenarios. In: Proceedings of the ISCRAM Conference, pp. 996–1011 (2020)
7. Asadi, A., Wang, Q., Mancuso, V.: A survey on device-to-device communication in cellular networks. IEEE Communications Surveys & Tutorials **16**(4), 1801–1819 (2014)
8. Hossain, M.A., Ray, S.K., Lota, J.: SmartDR: A device-to-device communication framework for post-disaster recovery. Journal of Network and Computer Applications **171**, 102813 (2020)
9. Abidde, W.N., Johnson, A.O., Peters, K.M.: Optimization of wireless mesh networks for disaster response communication using AI-driven routing algorithms. International Journal of Computer Science Research and Reviews **35**(3), 1703–1725 (2025)
10. Hossain, M.A., Ray, S.K., Lota, J.: SmartDR: A device-to-device communication framework for post-disaster recovery. Journal of Network and Computer Applications **171**, 102813 (2020)