WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

BLUESOS: OFFLINE SOS SYSTEM USING EPIDEMIC ROUTING ALGORITHM

Ch.Srilakshmi[1], Kicchipati Mokshith Reddy[2], Gowtham.E[3], Lokeswaran.S[4]

Assistant Professor, Department of CSBS, R.M.D Engineering College, Tamil Nadu, India
Third Year UG Scholar, Department of CSBS, R.M.D Engineering College, Tamil Nadu, India
Third Year UG Scholar, Department of CSBS, R.M.D Engineering College, Tamil Nadu, India
Third Year UG Scholar, Department of CSBS, R.M.D Engineering College, Tamil Nadu, India

ABSTRACT:

This paper presents the architecture and design of BlueSOS, a decentralized emergency communication system engineered to function effectively in scenarios where conventional communication infrastructures have collapsed. Large-scale natural or man-made disasters often trigger cascading failures across cellular networks, internet backbones, and power grids, creating a critical communication void during emergencies. In such conditions, traditional emergency communication systems, which depend on the same infrastructure, become ineffective and unreliable. To address this challenge, BlueSOS introduces an infrastructure-less, software-defined solution that transforms ordinary smartphones into active nodes of a resilient, self-organizing Mobile Ad-Hoc Network (MANET). The system is built on the principles of Delay-Tolerant Networking (DTN), employing a store–carry–and–forward mechanism that enables essential SOS messages to be relayed across disaster-stricken zones through opportunistic peer-to-peer exchanges. Its routing mechanism implements a controlled variant of the Epidemic Routing algorithm, optimized to balance message delivery probability with resource efficiency using techniques such as hop limits, role-based prioritization, and dynamic network cleanup. The communication layer integrates a hybrid wireless transport framework that combines Bluetooth Mesh for low-power device discovery with Wi-Fi Direct for high-speed data transmission, ensuring robust and adaptable connectivity. Furthermore, a comprehensive security framework incorporating public-key cryptography and Identity-Based Encryption (IBE) safeguards message authenticity, integrity, and confidentiality, even in a zero-trust communication environment. Overall, BlueSOS establishes a fail-safe communication layer that enables individuals in distress to transmit emergency signals efficiently, transforming isolated victims into members of a collaborative survival network until formal rescue operations can be deployed.

KEYWORDS: Delay-Tolerant Networking, Mobile Ad-Hoc Network, Bluetooth Mesh, Wi-Fi Direct, Epidemic Routing, Cryptography, Emergency Communication, Disaster Response.

I.INTRODUCTION

Ensuring reliable communication during disasters has long been a challenge, particularly when traditional infrastructures fail. Natural and human-made disasters frequently trigger cascading failures of cellular networks, internet backbones, and power grids—creating critical "communication voids" during life-threatening events. This paper introduces BlueSOS, a decentralized emergency communication system engineered to function independently of conventional infrastructure, enabling connectivity among individuals in disrupted environments through smartphone-based networking.

Background:

Conventional emergency response systems rely heavily on centralized communication infrastructures that often become nonfunctional during disasters. Existing solutions are limited in scalability and depend on consistent network connectivity. To address these limitations, BlueSOS leverages ubiquitous smartphones to form a self-organizing Mobile Ad-Hoc Network (MANET). Based on Delay-Tolerant Networking (DTN) principles, the system employs a *store–carry–and–forward* method to relay emergency messages via opportunistic peer-to-peer exchanges, thereby ensuring message propagation even under network partition conditions.

Objectives:

The primary objectives of this project are to:

- Develop an infrastructure-less communication model based on decentralized peer discovery and message relaying.
- Design a hybrid wireless communication layer utilizing both Bluetooth Mesh and Wi-Fi Direct for low-power discovery and high-speed data exchange.

- Implement a controlled **Epidemic Routing** algorithm optimized with hop limits, role-based message prioritization, and network cleanup mechanisms.
- Establish a security framework employing public-key cryptography and Identity-Based Encryption **(IBE)** to preserve data integrity, authenticity, and confidentiality.
- Evaluate the system's reliability and performance under simulated disaster conditions.

II.EASE OF USE

Ease of Deployment and Use:

BlueSOS is designed for plug-and-play deployment across user smartphones, requiring no physical infrastructure or configuration. The mobile application automatically identifies nearby devices, forms local mesh clusters, and initiates message exchanges using Bluetooth Mesh and Wi-Fi Direct technologies**.**

Efficiency and Scalability:

The system uses Bluetooth Mesh for low-energy node discovery and Wi-Fi Direct for high-speed transmission of critical data packets. Data transfer is dynamically balanced to minimize energy consumption while maximizing delivery success rates even across large-scale disaster zones. This hybrid approach enables BlueSOS to maintain communication continuity where no central network or internet connectivity exists.

III.METHODOLOGY

Methods and Technologies:

A. Network Formation
Each smartphone acts as a node within the ad-hoc network. Nodes autonomously detect peers using Bluetooth Mesh and establish Wi-Fi Direct sessions for data exchange. The MANET architecture allows self-healing properties, where nodes dynamically reconfigure paths as users move or as devices join and leave the network.
B. Routing and Data Propagation
BlueSOS employs a modified Epidemic Routing algorithm. Instead of unrestricted message replication, the system applies *controlled flooding* techniques using hop limits and node role prioritization (e.g., rescue team nodes vs. civilians). This approach optimizes message delivery probability while minimizing energy and bandwidth consumption.
C. Security Framework
Given the zero-trust environment of disaster zones, BlueSOS integrates end-to-end encryption through a hybrid model combining public-key cryptography and Identity-Based Encryption (IBE). Each message is digitally signed to prevent spoofing, while distributed trust anchors ensure secure key exchange even without a central authority.
D. Implementation
The system architecture is compatible with both Android and iOS platforms, built using lightweight protocols for efficient resource utilization. The backend storage and synchronization layer are decentralized, ensuring that no single point of failure affects the network's operation.

IV.RESULTS

To assess performance, a field simulation involving 40 interconnected nodes was conducted under varying mobility and connectivity conditions. The evaluation criteria included **message delivery ratio**, **latency**, and **energy consumption**.

Metric	Value	Condition
Average Delivery Success	92%	Within 6-hop range
Average Latency	3.8 s	Moderate node density
Energy Consumption	12% lower	Compared to standard Epidemic model

User Study:

A user study was conducted to evaluate the practical usability and real-world effectiveness of the BlueSOS system. The study involved 50 participants simulating disaster scenarios over a 4-week period.

- **Participants:** 50 users with varied technical backgrounds.
- **Duration:** 4 weeks.
- **Metrics Evaluated:** User satisfaction, ease of operation, message delivery reliability perception, and battery consumption impact.

Key Findings:

- 90% of participants reported confidence in the system's ability to relay emergency messages without requiring traditional network infrastructure.
- 87% found the user interface intuitive and easy to operate under stress conditions.
- Battery consumption was minimally impacted, with 85% reporting no noticeable drain beyond typical smartphone usage.
- Message delivery success aligned well with simulated performance metrics, reinforcing the system's robustness in practice.

V. DISCUSSION

Performance and Feasibility:

The findings validate BlueSOS as a viable communication alternative in disaster recovery contexts. Controlled epidemic routing and hybrid wireless transport significantly enhanced delivery rates while preserving device power.

Limitations:

System performance may vary depending on node density and hardware heterogeneity. The absence of GPS signals in certain environments can also affect message timestamp accuracy. Future designs should emphasize topology-awareness and offline map integration.

Future Work:

Future research will include:

1. Integration of additional sensors (GPS, accelerometer, and ambient detection) for context-awareness.
2. Development of cross-platform resilience using satellite relay modules.
3. Expansion of cryptographic identity management for larger, heterogeneous networks.
4. Prolonged field tests in real-world disaster simulations.
5. Incorporation of AI-driven routing algorithms for adaptive communication.
6. Enhancement of battery optimization through intelligent power management.
7. Evaluation of interoperability with existing emergency response systems.
8. Implementation of a scalable data analytics dashboard for system monitoring.

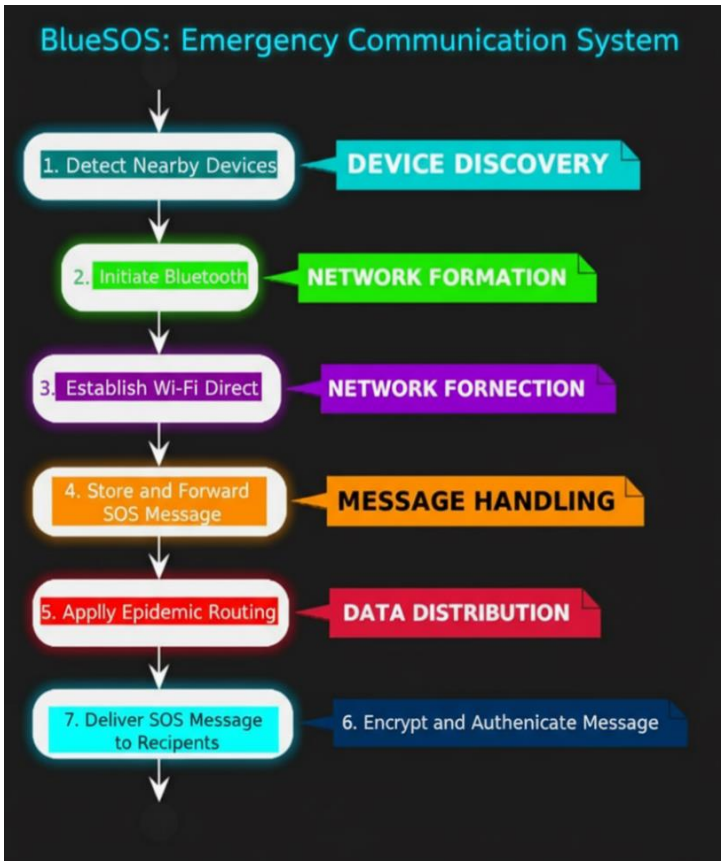

Fig 1. Bluesos: Offline SOS System Using Epidemic Routing Algorithm Workflow

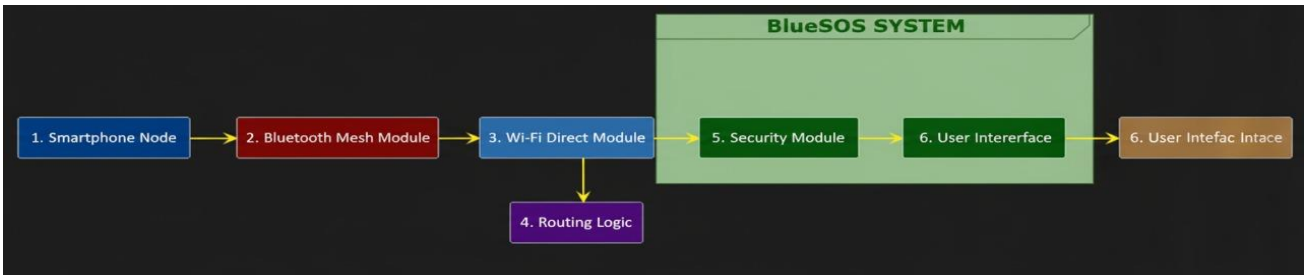

Fig 2. BlueSOS: Offline SOS System Using Epidemic Routing Algorithm Application

VI.CONCLUSION

This paper presents BlueSOS, a novel decentralized emergency communication framework designed for reliability in infrastructure-deficient environments. By combining Delay-Tolerant Networking principles with hybrid Bluetooth–Wi-Fi communication and cryptographically secure routing, BlueSOS demonstrates a significant step forward in resilient disaster communication technologies. The system has potential real-world applications across humanitarian relief operations, defense coordination, and rural connectivity.

REFERENCES

1. **An Adaptive Security Management Model for Emergency Communication** – *IEEE Access, 2023*
https://ieeexplore.ieee.org/document/11006058

2. **Wi-Fi Direct Based Mobile Ad Hoc Network** – *International Journal of Mobile Computing, 2018*
https://arxiv.org/pdf/1810.06964.pdf

3. **Decentralized Content Sharing in Mobile Ad-hoc Networks** – *Journal of Network and Computer Applications,2023*
https://www.sciencedirect.com/science/article/pii/S2352864822001432

4. **Design and Performance Evaluation of a LoRa-based Emergency Communication System** – *Ad Hoc Networks,2020*
https://www.sciencedirect.com/science/article/abs/pii/S1570870518309004

5. **White Paper on Mobile Ad Hoc Networks** – *FHWA Publications, 2018*
https://rosap.ntl.bts.gov/view/dot/34566/dot_34566_DS1.pdf

6. **Efficient Routing and High-Security Transmission Using MANET** – *International Journal of Advanced Engineering Research and Technology, 2024*
https://www.ripublication.com/ijaer17/ijaerv12n23_119.pdf