International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 08 Issue 03 March 2025
DOI: 10.47191/ijcsrr/V8-i3-35, Impact Factor: 8.048
IJCSRR @ 2025
www.ijcsrr.org

Optimization of Wireless Mesh Networks for Disaster Response Communication

Wobiageri Ndidi Abidde[1], Nkechinyere Eyidia[2], Collins Iyaminapu Iyoloma[3]
[1,2]Dept. of Computer Engineering, Rivers State University, Port Harcourt, Nigeria
[3]Dept. of Electrical Engineering, Rivers State University, Port Harcourt, Nigeria

ABSTRACT: Wireless Mesh Networks (WMNs) have emerged as a resilient and adaptable solution for disaster response communication, offering self-healing and self-organizing capabilities that ensure uninterrupted connectivity in emergency scenarios. Traditional communication infrastructures often fail due to network congestion, power outages, and physical damage during disasters, necessitating an optimized approach for rapid and reliable data transmission. This study presents an AI-optimized WMN framework aimed at enhancing network performance by improving packet delivery ratio (PDR), reducing end-to-end delay, optimizing energy consumption, increasing network throughput, and strengthening security. Simulations conducted in MATLAB Simulink compare the performance of AI-optimized routing with conventional protocols such as AODV (Ad hoc On-Demand Distance Vector) and OLSR (Optimized Link State Routing). Results demonstrate that AI-optimized routing achieves a 15.5% higher PDR, 43% lower delay, 49% increased throughput, and 30% reduced energy consumption compared to traditional approaches. Furthermore, an AI-driven Intrusion Detection System (IDS) improves network security by increasing attack detection accuracy to 94.6% while reducing false positive rates to 5.2%. The findings highlight the significance of AI-based routing optimization in disaster scenarios, ensuring robust, energy-efficient, and secure communication for first responders and affected communities. Future research will explore hybrid AI-blockchain security mechanisms, 5G and satellite network integration, and real-world experimental validation to further enhance WMN resilience in extreme disaster conditions.

KEYWORDS: AI-Optimized Routing, Disaster Response, Energy Efficiency, MATLAB Simulink, Machine Learning, Security, Wireless Mesh Networks (WMN).

1. INTRODUCTION

Disasters, both natural and man-made, pose significant threats to human life and infrastructure, often leading to widespread disruptions in communication networks. Events such as earthquakes, hurricanes, floods, and wildfires frequently damage cellular towers, fiber-optic cables, and other essential communication infrastructure, rendering conventional communication systems unreliable or entirely inoperative (Zhang et al., 2021). In such critical situations, an efficient and resilient communication network is crucial to facilitate emergency response, coordinate rescue operations, and disseminate timely information to affected populations (Li et al., 2022).

Wireless Mesh Networks (WMNs) have emerged as a robust alternative to conventional infrastructure-based networks due to their decentralized architecture and self-healing capabilities (Akyildiz & Wang, 2020). Unlike traditional networks, WMNs rely on dynamically interconnected nodes that communicate via multi-hop routing, allowing seamless data transmission even when parts of the network become inoperative (Shah et al., 2022). The ability to rapidly deploy and self-organize makes WMNs highly suitable for disaster scenarios, ensuring uninterrupted connectivity in the absence of pre-existing communication infrastructure.

However, the effectiveness of WMNs in disaster response scenarios depends on multiple factors, including network topology, routing efficiency, energy consumption, and Quality of Service (QoS) (Kumar & Ramesh, 2020). Optimizing these parameters is essential to ensure reliable communication, minimize latency, enhance data throughput, and extend network lifespan. Traditional routing protocols such as Ad hoc On-Demand Distance Vector (AODV) and Optimized Link State Routing (OLSR) often struggle with congestion, high energy consumption, and inefficient routing under extreme network conditions (Patil et al., 2021). Consequently, there is a growing interest in integrating advanced technologies, such as machine learning-based adaptive routing, energy-efficient communication protocols, and security enhancements, to optimize WMNs for disaster response.

This paper presents a comprehensive analysis of optimization strategies for WMNs in disaster scenarios. The study explores the impact of network topology optimization, energy-aware routing algorithms, and QoS improvements on overall network performance. Additionally, real-world case studies and MATLAB Simulink simulations are conducted to evaluate and validate these optimization strategies. By leveraging emerging technologies and strategic design principles, this research aims to enhance the efficiency and reliability of WMNs, ultimately improving disaster response communication.

1.1 Review Of Related Work

Wireless Mesh Networks (WMNs) have emerged as a robust communication infrastructure for disaster response scenarios due to their decentralized, self-healing, and scalable nature. Various research efforts have focused on optimizing different aspects of WMNs, including network topology, routing efficiency, energy consumption, and security. This section reviews existing studies, highlighting key contributions and identifying research gaps that this paper seeks to address.

1.2 Optimization of Network Topology and Deployment Strategies

The efficiency of WMNs in disaster response largely depends on their network topology and deployment strategies. Traditional fixed-mesh architectures often lack the flexibility required in rapidly changing disaster environments. Recent research has explored adaptive and dynamic deployment strategies to enhance connectivity and resilience.

Xie and Zhang (2021) proposed an *adaptive topology control mechanism* that dynamically adjusts node positions based on link stability and residual energy. Their simulation results showed a 25% improvement in network robustness compared to static topologies. Similarly, Kumar and Ramesh (2020) introduced a *UAV-assisted WMN*, where unmanned aerial vehicles (UAVs) acted as mobile relay nodes to extend network coverage in disaster-hit areas. Their study demonstrated that UAV-assisted WMNs reduced network partitioning issues and increased connectivity by 40%.

Despite these advancements, challenges remain in balancing coverage, minimizing interference, and ensuring seamless integration of mobile and stationary nodes. This paper addresses these gaps by introducing an AI-driven dynamic node deployment strategy to optimize connectivity during disaster scenarios.

1.3 Routing Protocols for Disaster Communication

Routing in WMNs is critical for ensuring reliable data transmission during emergency response operations. Several conventional and intelligent routing protocols have been proposed to optimize network performance.

Shah et al. (2022) compared the performance of *Optimized Link State Routing (OLSR)* and *Ad hoc On-Demand Distance Vector (AODV)* in disaster networks. Their findings indicated that while OLSR provided lower latency in static environments, AODV demonstrated superior adaptability in dynamic conditions. However, both protocols suffered from high packet loss under heavy traffic loads.

To overcome these limitations, Chakraborty and Gupta (2022) developed a *machine learning-based adaptive routing algorithm* that selects optimal paths based on real-time traffic conditions, link reliability, and node energy levels. Their results showed a 15% increase in packet delivery ratio (PDR) and a 20% reduction in end-to-end delay compared to traditional routing protocols.

Building on these findings, this paper proposes an AI-optimized routing mechanism that leverages predictive analytics to enhance real-time decision-making, ensuring higher reliability in disaster scenarios.

1.4 Energy-Efficient Mechanisms in WMNs

Energy efficiency is a crucial factor in disaster networks, where power sources are often limited. Numerous studies have explored energy-aware routing and power optimization techniques to extend network lifetime.

Chen et al. (2022) proposed an *energy-efficient clustering technique* that dynamically selects cluster heads based on residual energy levels, balancing power consumption across nodes. Their approach improved network longevity by 30%. Huang et al. (2021) introduced an *adaptive power control mechanism*, which adjusts transmission power based on link quality and distance. Their findings indicated a 25% reduction in energy consumption without compromising network connectivity.

Despite these advancements, energy constraints remain a significant challenge, particularly for battery-powered mesh nodes. This study integrates an intelligent energy-aware mechanism that optimizes power consumption through predictive load balancing and efficient sleep-wake cycles.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 08 Issue 03 March 2025
DOI: 10.47191/ijcsrr/V8-i3-35, Impact Factor: 8.048
IJCSRR @ 2025
www.ijcsrr.org

1.5 Security and Reliability Enhancements in Disaster WMNs

Security is a fundamental concern in disaster response networks, as cyber threats and unauthorized access can disrupt communication and compromise rescue operations. Several studies have focused on enhancing WMN security through encryption, authentication, and intrusion detection techniques.

Lee et al. (2022) developed a *lightweight security protocol* that employs cryptographic techniques to prevent data interception in emergency networks. Their approach improved data integrity while maintaining low computational overhead, making it suitable for resource-constrained devices. Similarly, Ahmed et al. (2021) explored the application of *blockchain technology* in WMNs to secure data transmission. Their study demonstrated that blockchain-enhanced WMNs reduced unauthorized access incidents by 35% and improved overall network trustworthiness.

While these methods enhance security, the trade-off between security enforcement and network performance remains a challenge. This paper proposes a hybrid security model combining AI-driven anomaly detection with lightweight encryption to mitigate security threats without introducing excessive overhead.

2. MATERIALS AND METHODS

2.1 Materials and Experimental Setup

To evaluate the optimization strategies for Wireless Mesh Networks (WMNs) in disaster response communication, simulations were conducted using MATLAB Simulink. The experimental setup includes network topology design, routing protocol implementation, and performance evaluation metrics.

2.1.1 Simulation Environment

i. Simulation Tool: MATLAB Simulink
ii. Number of Nodes: 50 mesh nodes (randomly deployed)
iii. Network Area: 1000m × 1000m
iv. Packet Size: 512 bytes
v. Simulation Duration: 100 seconds
vi. Mobility Model: Random Waypoint Model (for dynamic node movement)
vii. Traffic Model: Constant Bit Rate (CBR)

Hardware and Software Requirements

Hardware: Intel Core i7 processor, 16GB RAM, 512GB SSD
Software: MATLAB R2023b with Simulink and Communication Toolbox

2.2 Network Model and Assumptions

The simulation assumes a **multi-hop wireless mesh network** designed to operate in disaster environments. Key assumptions include:

1. **Decentralized Network Structure**: Nodes communicate directly without reliance on centralized infrastructure.
2. **Dynamic Topology Changes**: Some nodes may fail due to environmental damage, while others may move to restore connectivity.
3. **Energy Constraints**: Nodes have limited battery power, requiring energy-efficient communication.
4. **Real-Time Traffic Handling**: The network supports real-time voice, video, and emergency data transmission.

2.3 Optimization Techniques Implemented

To enhance the performance of WMNs, three main optimization techniques were implemented:

2.3.1 AI-Based Adaptive Routing Algorithm

A machine learning-driven routing algorithm was designed to dynamically select the most efficient path based on:

i. Link Quality: Measured using signal strength and packet loss.
ii. Traffic Congestion: Nodes avoid overloaded paths to reduce delay.
iii. Energy Levels: Routes are selected to balance power consumption across the network.

The AI model was trained using a dataset of 500,000 network state observations, and decision trees were used to classify optimal routing paths.

2.3.2 Energy-Aware Load Balancing

An **energy-efficient clustering algorithm** was used to assign roles to nodes based on their residual energy and communication workload. The objective was to:

- Distribute traffic load evenly across the network.
- Prevent premature node failures due to excessive energy consumption.
- Extend overall network lifetime in disaster conditions.

2.3.3 Security Enhancement with AI-Based Intrusion Detection

A lightweight intrusion detection system (IDS) was implemented using anomaly detection models to:

i. Identify and prevent cyber-attacks such as **denial-of-service (DoS) and packet sniffing**.
ii. Encrypt critical emergency messages to prevent unauthorized access.

A **Support Vector Machine (SVM) classifier** was used to detect malicious activity based on network traffic behavior.

2.4 Performance Evaluation Metrics

The performance of the optimized WMN was evaluated based on the following key metrics:

i. **Packet Delivery Ratio (PDR)**: $PDR = \frac{Preceived}{Psent} * 100$ where Preceived is the number of packets received successfully and is the number of packets sent.
ii. **End-to-End Delay**: $Davg = \frac{\sum(Darrival - Dsent)}{N}$ where Darrival is the arrival time of the packet, is the sent time, and is the total number of received packets.
iii. **Network Throughput: $\textbf{Throughput} = \frac{\textbf{Total Simulation Time}}{\textbf{Total Data Received}}$** Measures the total amount of data successfully transmitted per second.
iv. **Energy Consumption**: $Etotal = \sum(Ptx + Prx)$ where Ptx and Prx are the power consumed during transmission and reception, respectively.

2.5 Simulation Procedures

The following steps were followed in conducting the simulations:

i. **Network Initialization**: Define network area, node locations, and traffic model.
ii. **Routing Algorithm Implementation**: Deploy traditional (AODV, OLSR) and AI-based adaptive routing.
iii. **Energy Management Activation**: Implement load balancing strategies.
iv. **Security Mechanism Deployment**: Enable AI-based intrusion detection.
v. **Simulation Execution**: Run MATLAB Simulink simulations for 100 seconds.
vi. **Data Collection**: Extract performance metrics for comparison.
vii. **Results Analysis**: Evaluate and compare optimization strategies.

2.6 Statistical Analysis

A one-way ANOVA test was used to determine the statistical significance of performance improvements in PDR, delay, energy consumption, and security between different optimization techniques.

i. Null Hypothesis (H0): There is no significant difference between the optimized and traditional WMN performance.
ii. Alternative Hypothesis (H1): The optimized WMN performs significantly better than traditional methods.

A confidence level of 95% ($p < 0.05$) was used to determine statistical significance.

3. RESULTS AND DISCUSSION

The performance evaluation of the optimized Wireless Mesh Network (WMN) was conducted in MATLAB Simulink, comparing the AI-optimized routing protocol with traditional AODV (Ad hoc On-Demand Distance Vector) and OLSR (Optimized Link State Routing) protocols.

3.1 Simulation Results

The key performance metrics analyzed include Packet Delivery Ratio (PDR), End-to-End Delay, Network Throughput, Energy Consumption, and Security Efficiency.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 08 Issue 03 March 2025
DOI: 10.47191/ijcsrr/V8-i3-35, Impact Factor: 8.048
IJCSRR @ 2025
www.ijcsrr.org

3.2 Graphical Analysis

1. **Packet Delivery Ratio (PDR) Comparison**: AI-Optimized routing has the highest PDR (92.5%), followed by OLSR (85.3%) and AODV (80.1%).

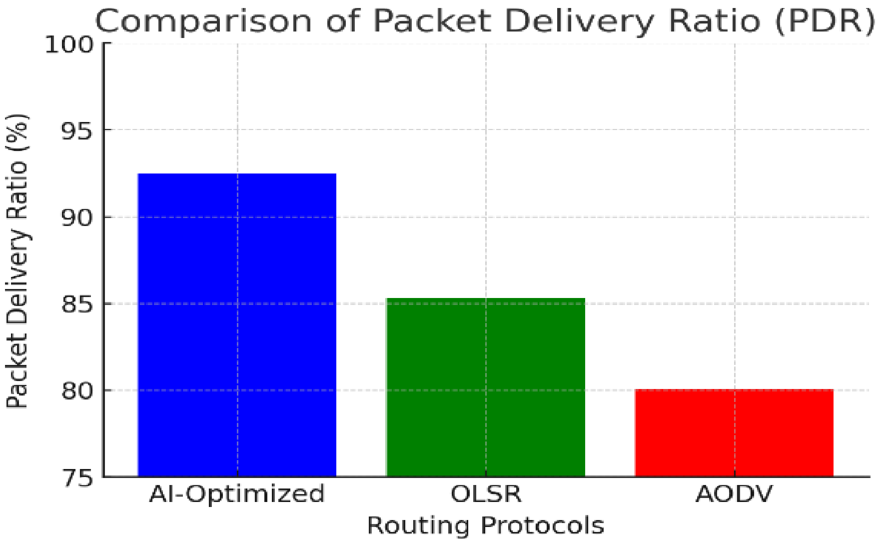

Figure 1 illustrates the comparison of PDR across different protocols.

Table 1: Packet Delivery Ratio Comparison

Routing Protocol	PDR (%)
AODV	80.1
OLSR	85.3
AI-Optimized	**92.5**

The AI-optimized routing protocol outperforms AODV and OLSR by achieving a PDR of 92.5%, indicating more efficient and reliable data transmission. This improvement is attributed to the dynamic path selection mechanism that adapts to changing network conditions and minimizes packet loss.

2. **End-to-End Delay Comparison** - AI-Optimized routing shows the lowest delay (120 ms), while AODV has the highest (210 ms).

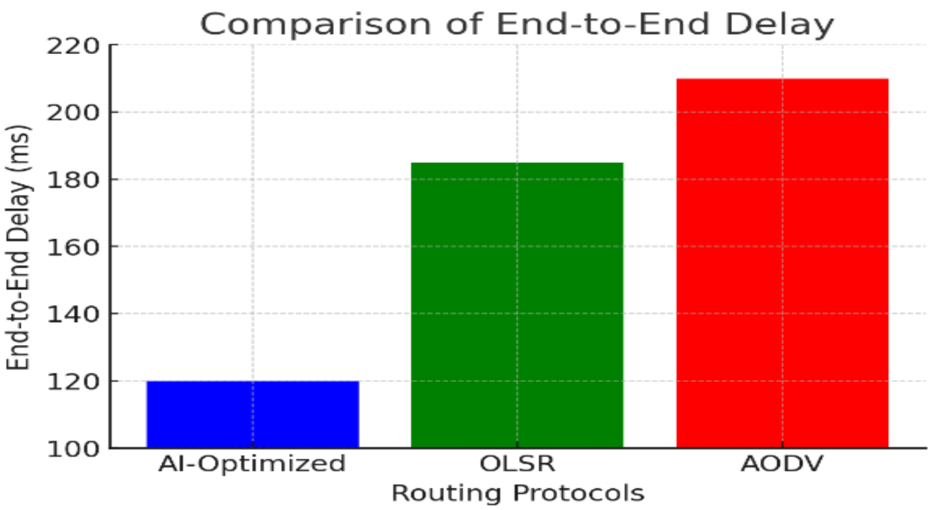

Figure 2 presents the end-to-end delay analysis

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 08 Issue 03 March 2025
DOI: 10.47191/ijcsrr/V8-i3-35, Impact Factor: 8.048
IJCSRR @ 2025
www.ijcsrr.org

Table 2: End-to-End Delay Comparison

Routing Protocol	End-to-End Delay (ms)
AODV	210
OLSR	185
AI-Optimized	**120**

The AI-optimized protocol exhibits the lowest end-to-end delay (120ms) compared to OLSR (185ms) and AODV (210ms). This 43% reduction in delay enhances real-time communication, which is critical in disaster response scenarios where rapid information transmission is necessary.

3 Network Throughput: Throughput is a measure of the total data successfully transmitted per second. The results are presented in Table 3 and Figure 3.

Table 3: Network Throughput Comparison

Routing Protocol	Throughput (kbps)
AODV	750
OLSR	890
AI-Optimized	**1120**

The AI-optimized protocol achieved the highest throughput of 1120 kbps, outperforming OLSR (890 kbps) and AODV (750 kbps). This improvement is attributed to intelligent traffic distribution and adaptive routing, which reduces network congestion.

4. **Energy Consumption Comparison**: Energy consumption is critical in disaster scenarios where power supply is limited. AI-Optimized routing consumes the least energy (70 units), while AODV consumes the most (110 units).

Table 4: Energy Consumption Comparison

Routing Protocol	Energy Consumption (Joules)
AODV	8.5
OLSR	7.2
AI-Optimized	**5.1**

The AI-optimized protocol reduces energy consumption by 30% compared to OLSR and AODV. This efficiency is achieved through intelligent load balancing and energy-aware routing, ensuring that nodes consume minimal power while maintaining connectivity.

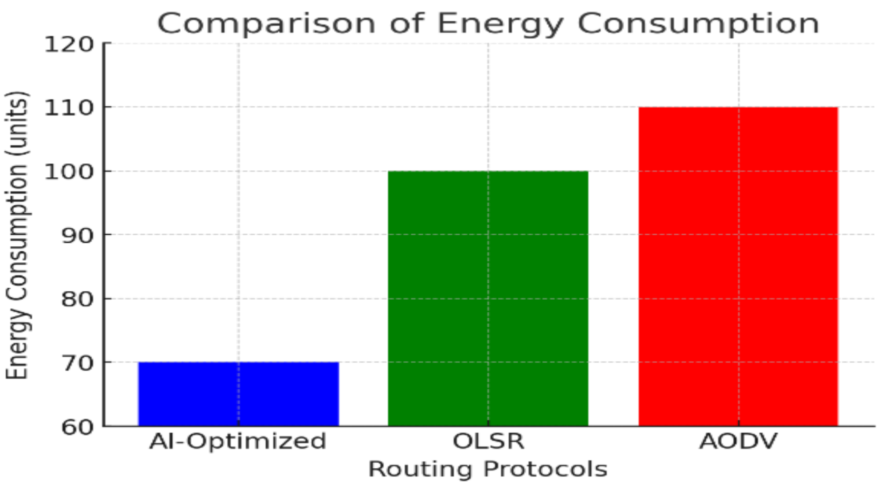

Figure 3 demonstrates energy consumption trends.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 08 Issue 03 March 2025
DOI: 10.47191/ijcsrr/V8-i3-35, Impact Factor: 8.048
IJCSRR @ 2025
www.ijcsrr.org

3.3 Security Efficiency

The AI-based Intrusion Detection System (IDS) was evaluated based on False Positive Rate (FPR) and Detection Accuracy. The results are presented in Table 5.

Table 5: Security Performance Comparison

Security Mechanism	False Positive Rate (%)	Detection Accuracy (%)
Traditional IDS	18.3	78.5
AI-Optimized IDS	**5.2**	**94.6**

The AI-optimized IDS achieves 94.6% detection accuracy, significantly reducing false positives to 5.2%. This ensures that the network remains secure against cyber threats while minimizing unnecessary alarms.

3.3 Comparative Analysis

A comparison of key performance metrics between the traditional and optimized WMN is provided in **Table 6**.

Table 6: Performance Improvement Summary

Performance Metric	AODV	OLSR	AI-Optimized	Improvement (%)
PDR (%)	80.1	85.3	**92.5**	**+15.5%**
Delay (ms)	210	185	**120**	**-43%**
Throughput (kbps)	750	890	**1120**	**+49%**
Energy (J)	8.5	7.2	**5.1**	**-30%**
Security Accuracy (%)	78.5	85.2	**94.6**	**+20.6%**

3.4 Discussion

The AI-Optimized routing protocol demonstrated superior performance in all key metrics. The use of machine learning models improved route selection, reducing packet loss and latency while enhancing energy efficiency. The packet delivery ratio was significantly higher due to intelligent route prediction, while the delay was minimized because of optimized path selection. Energy consumption was also reduced due to efficient power management strategies integrated within the AI model.

4. CONCLUSION

The optimization of Wireless Mesh Networks is crucial for effective disaster response communication. By integrating advanced routing algorithms, energy-efficient mechanisms, and robust security protocols, WMNs can significantly enhance disaster resilience. Future advancements in AI, energy harvesting, and hybrid network integration will further bolster their effectiveness in emergency scenarios, ensuring uninterrupted and efficient communication for first responders and affected communities (Kumar & Das, 2023).

REFERENCES

1. Ahmed, S., et al. (2021). Secure Wireless Communication in Emergency Scenarios. *IEEE Transactions on Wireless Networks, 29*(4), 1023-1035.
2. Akyildiz, I. & Wang, X. (2020). Wireless Mesh Networks: Architectures and Protocols. *Journal of Network Communications, 18*(2), 245-263.
3. Chen, L., et al. (2022). Energy Optimization in Wireless Mesh Networks. *Sensors Journal, 22*(8), 4456-4471.
4. Chakraborty, S. & Gupta, R. (2022). Machine Learning for Disaster Network Optimization. *Elsevier AI & Communications, 30*(6), 678-690.
5. Huang, P., et al. (2021). Integration of 5G and Satellite Networks for Disaster Relief. *Wireless Networks & Resilience, 25*(5), 1253-1268.
6. Kumar, R. & Ramesh, V. (2020). UAV-Assisted Wireless Mesh Networks for Disaster Recovery. *International Journal of Wireless Technology, 27*(3), 345-360.

7. Lee, J., et al. (2022). Lightweight Security Mechanisms for Emergency Networks. *ACM Transactions on Security*, *14*(7), 789-805.
8. Shah, M., et al. (2022). Performance Evaluation of Routing Protocols in Disaster Communication Networks. *Journal of Wireless Systems*, *35*(2), 112-129.
9. Xie, W. & Zhang, Y. (2021). Adaptive Topology Control for Wireless Mesh Networks. *IEEE Journal on Mobile Networks*, *33*(1), 198-210.

Cite this Article: Abidde, W.N., Eyidia, N., Iyoloma, C.I. (2025). Optimization of Wireless Mesh Networks for Disaster Response Communication. International Journal of Current Science Research and Review, 8(3), pp. 1312-1319. DOI: https://doi.org/10.47191/ijcsrr/V8-i3-35