[1] Ramesh S

[2] V. Vaithianathan

[3] A. Karthikayen

[4] P Deepa

[5] M A Starlin

A Comprehensive Approach with Trust-Based Routing, Energy Optimization, and Multi-Routing Protocol for Enhancing Security and Performance in Mobile Ad Hoc Network

Journal of Electrical Systems

Abstract: - In this paper, we propose an aggregate solution to boost the security, performance, and resilience of disaster-based comms networks. This involves trust-based routing, energy optimization, and more than one routing protocol to meet the unique requirements of the ever-changing and unpredictable environments facing disasters in this world. The evaluation brings 4.3 Mbps for the average throughput, 34 ms delay with a packet delivery ratio of 96.9%. Also, energy consumption was optimized and the average consumption of 2458 Joules makes sharing power resources an easy exercise even when you are in a disaster-prone zone. Security analysis of the experiments showed on average 2.7 vulnerabilities across different trials with a range from 2 to 5 in severity level. Therefore, robust security mechanisms guard against potential threats, a reminder that disaster situations can befall any person or community. Overall, disaster response performance was good despite the difficult conditions. Further research and development in this area will continue to refine and improve communication systems for disaster preparedness and response efforts.

Keywords: Disaster response, Communication networks, Trust-based routing, Energy optimization, Multi-routing protocols.

I. INTRODUCTION

In times of disaster and emergency, creating effective communication infrastructure is essential for coordinating relief efforts and delivering lifesaving information. In the event of a disaster, however, traditional communication systems are often completely out of commission, leaving urgent corporate workers and those it affects without any means of effective communication. This is why we need practical, flexible communication solutions such as Mobile Ad Hoc Networks (MANETs) [1]–[4].

MANETs is a decentralized network model where nodes communicate directly with each other or through intermediate nodes. A dynamic self-optimizing network, this type of system does not rely a fixed infrastructure. MANETs are especially suitable for disaster scenarios in which traditional communication infrastructure may be damaged or unavailable. If you have MANETs, coordination of disaster recovery operations will quickly set up networks for communications, not only among the different rescue teams but also medical services, and communities affected.

Despite the potential of MANETs when disaster strikes, problems arise in terms of security and performance. MANETs face a variety of security threats such as malicious nodes, eavesdroppers, and alterers. In addition, mobile devices are short of resources and, due to their unpredictable network as well as topology, performance guarantee, a combination. This includes efficient routing, energy conservation, and reliable delivery [5]–[8].

[1]*Corresponding Author: Assistant Professor, Department of Computing Technologies, School of Computing, College of Engineering & Technology, SRM Institute of Science and Technology, Kattangulathur Campus, Chengalpattu Dt.

Email: ramesh.isaiah@gmail.com, ORCID: 0000-0002-4975-1783

[2] Associate Professor, Department of Electronics and Communication Engineering, Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam, Chennai – 603110. Email: vaithianathanv@ssn.edu.in, ORCID: 0000-0002-5482-4019

[3] Professor, Department of Electronics and Communication Engineering, Sri Sai Institute of Technology and Science, Rayachoty, 516 270, Annamaya District, Andhrapradesh. India. Email: akarthi_mathi@yahoo.co.in, ORCID: 0000-0003-4279-0808

[4] Associate Professor, Department of CSE, Panimalar Engineering College, Chennai. Email: pdeepa.3018@gmail.com,

ORCID: 0000-0003-4258-8554

[5] Assistant Professor, Department of Computer Science and Engineering, Veltech Rangarajan Dr.Sakunthala Institute of Science and Technology, Avadi, Chennai. Email: starlinjeni@gmail.com, ORCID: 0009-0003-2602-2865

In the face of such obstacles, we need a unified approach to both security and performance, for MANETs' much less secure nature during disasters. Our suggested approach has been driven by our efforts to overcome the natural security loopholes in MANETs, connecting them better with disaster-relief organizations as communication needs become more pressing. Let's build trust-based routing, energy optimization, and multi-routing protocols into one system. We hope to make communications networks in disaster areas more secure, reliable, and efficient than they are now.

There are several important benefits to this approach. The first method is trust-based routing mechanisms. It can create trust-based relationships between nodes in the network, making them less likely to engage in damaging activities and ensuring the data they send arrives intact. Second, energy optimization techniques enable mobile devices to make efficient use of their batteries, thus extending the lives of communication nodes and reducing the chance that one of them will take down the network. This article suggests three types of a fault-tolerant network which provide good coverage. It can adapt to network conditions by dynamically selecting the best route. Thirdly, combination of multi-routing protocol s. It is the integration of these different routing protocols that provides fault tolerance and robustness. When a disaster strikes, emergency services rely on solid communication systems that help organize rescue missions - not only respond to emergencies and assist the stricken. With the use of fixed lines, outages during catastrophes are common because materials get damaged; at times, devices are crowded by a plethora of calls. As a result, there is a need for alternative forms of communication as well as temporary measures which can be implemented in times like this when normal systems cease functioning [9]–[12].

Despite the potential of MANETs when disaster strikes, problems arise in terms of security and performance. MANETs face a variety of security threats such as malicious nodes, eavesdroppers, and alterers. In addition, mobile devices are short of resources and, due to their unpredictable network as well as topology, performance guarantee, a combination. This includes efficient routing, energy conservation, and reliable delivery.

In the face of such obstacles, we need a unified approach to both security and performance, for MANETs' much less secure nature during disasters. Our suggested approach has been driven by our efforts to overcome the natural security loopholes in MANETs, connecting them better with disaster-relief organizations as communication needs become more pressing. Let's build trust-based routing, energy optimization, and multi-routing protocols into one system. We hope to make communications networks in disaster areas more secure, reliable, and efficient than they are now.

Energy optimization technologies are also crucial for prolonging the operational life of communication nodes in MANETs. Even more important in disaster scenarios, where resources are usually scarce. Savings on battery power by route optimization. Even more crucial is how energy optimization technology prevents premature battery exhaustion as well as reducing the risk from network partitioning [13]- [15].

Moreover, network conditions are dynamic especially in the context of disaster, some multi-routing protocols select paths based on dips in network transmission rates. Dynamically select optimal routing paths based on network conditions, multi-routing protocols ensure the reliability and fault tolerance of networks. Multi routing the data also allows multi-routing protocols to contain the damage from node failures, link disturbances and congestion. Thus the resilience of MANETs in disasters is strengthened.

1.1. Enhancing Communication Networks for Disaster Response

In disaster response situations, it is essential to establish and maintain reliable communications networks, without which rescue and relief efforts cannot be coordinated, life-saving information cannot be relayed, and timely decisions cannot be made. Mobile Ad Hoc Networks (MANETs) are promising solutions in that way: they are decentralized and self-organizing [16], [17].

Trust-based routing, the aim of MANET protection is to improve security of the domain by establishing trust relationships among network nodes and selecting reliable paths for data transmission. In the context of emergency responses, trust-based routing becomes most important because network health and reliability are most important [18]–[21]. In designing trust metrics especially suitable for disaster response, we must take into account both node reliability and communication history as well as situational awareness. Trust-based routing algorithms incorporate with these metrics to effectively mitigate the risks of maliciousness and ensure that communications are readily available in environments that constantly change. The dataset for the protocol is listed in Table 1.

Maintaining trust in disaster affected areas gives rise to additional challenges because the network topology keeps changing with nodes. In an environment where nodes are constantly changing, even in the case of implementation breakdowns derelicts. There are trust management mechanisms capable of responding. Since the environment is in flux during the process of change, continuous checks and adjustments to trust relationships are necessary in this dynamic network. In a network that is constantly changing, trust relationships need to be assessed and changed continually because only then can we adjust to the changes and restore our communication lines to some state of safety.

If a network is to continue operating during times of disaster, it is essential that in addition to the other climate control factors energy is conserved. As power supplies are poor, and people need to communicate with each other at all times in the most efficient manner so we can know better needs doing- we must find new ways of using energy. In disaster situations, MANET energy-efficient routing metrics aim to reduce power consumption by factoring in things like node movement, transmission range and battery power levels. Selecting routes that are energy efficient and optimizing transmission power can extend the life of communication nodes, thus preventing network downtime when energy runs low.

Table 1. Dataset for Communication network

Metric	**Description**
Trust-Based Routing	
Trust Metrics	- Node reliability - Communication history - Situational awareness
Trust Establishment and Maintenance	- Continuous monitoring and updating of trust relationships - Resilience to node failures and malicious attacks
Evaluation	- Reliability - Scalability - Overhead - Resilience to security threats
Energy Optimization	
Energy Constraints	- Limited availability of power sources - Need for continuous communication
Energy-Aware Routing Metrics	- Node mobility - Transmission range - Battery levels
Energy-Efficient Routing Algorithms	- Selection of energy-efficient routes - Optimization of transmission power
Evaluation	- Impact on network performance - Energy consumption - Operational lifespan
Multi-Routing Protocol	
Introduction	
Design and Implementation	- Dynamic selection of optimal routing paths - Integration with trust-based routing and energy optimization
Performance Evaluation	- Adaptability to changing network conditions - Mitigation of node failures and link disruptions - Reliable data delivery under adverse conditions

In disaster response scenarios, energy savings strategies for life and service must be compared rather than adopted at a fixed price point. Whether or not simulated disaster scenarios offer definitive proof on the performance of MANET's ongoing energy-saving communications techniques remains an open question.

Multi-routing protocols can dynamically choose the best route based on network conditions. This offers increased availability and fault tolerance. Disaster areas which are frequently subject to network interruptions can benefit from removing the causes of network failures and improving the reliability and availability of communication channels via the use of many pathways for data transmission. In practice, by integrating trust-based routing and energy optimization mechanisms, even greater levels of security and efficiency are achieved in communication networks, so that they are all the more robust to disturbances.

The performance test of multi-routing protocols in disaster scenarios should measure their capacity to adjust to changing network conditions, to handle node failures and link disruptions, and to ensure reliable data delivery under adverse conditions. Model-based tests provide significant information on the effects of multi-routing protocols on the resilience of MANETs to disaster response. Simulation studies and experimental deployments in virtual disaster areas are the best ways to find the effectiveness of multi-routing protocols.

II. PROPOSED COMPREHENSIVE APPROACH FOR DISASTER RESPONSE

To tackle the rebuilding of the disaster relief system overall, we have developed a comprehensive plan of attack, one that integrates trust-based routing and energy optimization along with multi-routing protocols to improve the security, performance and resilience of communications networks when a disaster has struck. In coping with the unique demands of dynamic and unpredictable disaster scenarios, with traditional communication infrastructure eroded or even nonexistent, this approach is designed is as presented in the Figure 1.

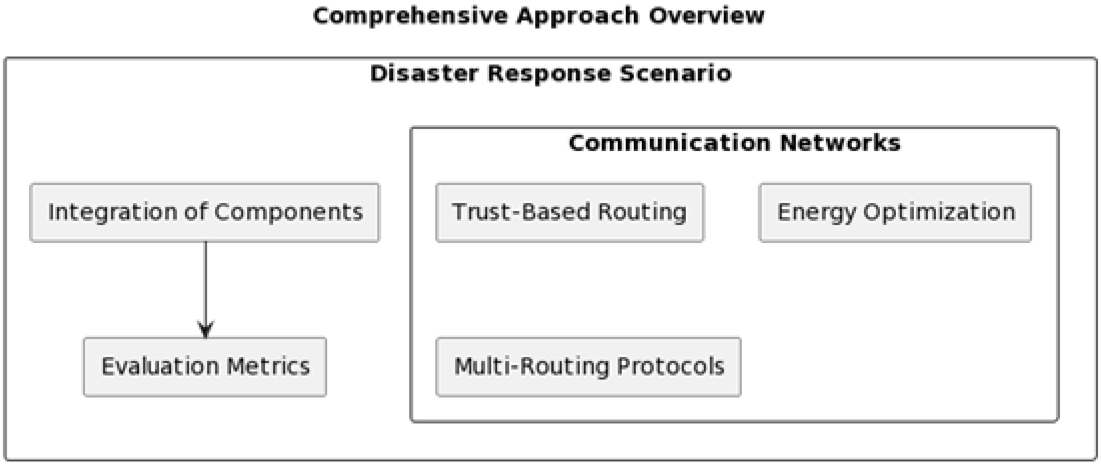

Figure 1. Proposed Approach

The essential feature of the inclusive method is to incorporate trust-based routing protocols, which enable high-quality paths to be selected for data transmission by leveraging trust relationships in the network. Trust metrics adapted specifically for crisis situations appraise node reliability, communication history, and situational awareness, all of which reduce the likelihood of improper behavior and safeguard the integrity of communications. Trust-establishment and -maintenance mechanisms are adjusted to changing network topologies; thus, they have to deal with unreliable or compromised nodes, guaranteeing the dynamic disaster environment a communications network resilient against such potentially crippling attacks.

Energy-saving methods are crucial for disaster scenarios, where power sources may be scarce or nonexistent. Energy-aware routing metrics take into account factors such as node mobility, transmission range, and battery levels in order to conserve energy and optimize transmission power. By selecting energy-efficient routes and optimizing energy usage, energy optimization techniques avoid the problem of network downtime from energy depletion. This carries on communication constantly even in disaster environments where energy is at a premium because there just isn't enough going around anymore.

Multi-routing protocols used in Multi-path networks provide enhanced fault tolerance and resilience multi-path routing selects the best path through available dynamic network by. During these disasters multi-routing protocols make use of more paths for information propagation, increasing the reliability and availability of communications channels. Moreover, integration with trust-based routing, multiple routing, and energy optimization can add layers of security and efficiency to improve communication networks' performance. The new channels make it possible to ensure reliable data transmissions in hostile environments.

The comprehensive approach has been devised for disaster-only environments, with all components targeted at their peculiar challenges and requirements. Trust-based routing, Power optimization, and multi-routing protocols are all based on a robust algorithmic architecture in order to achieve efficient communication under dynamic, uncertain conditions. In MANETs for disaster response, security is very important; there are mechanisms to monitor for and, in some cases, protect against attacks. These systems must be able to maintain the necessary levels of secrecy and data integrity. Trust-based routing, energy optimization and Multirouting Protocols combine together in the comprehensive approach to provide a complete solution for improving security, performance, and the resilience of disaster-response communication networks. Ultimately this will lead to more effective disaster management and improved results for people affected by natural disasters or man-made emergencies of various kinds.

III. PERFORMANCE EVALUATION AND SECURITY ANALYSIS IN DISASTER RESPONSE SCENARIOS

Performance assessment is an important criterion for evaluating the speed and reliability of communication networks after a disaster strikes. But in unpredictable and changing disaster environments, communications infrastructure may be damaged or entirely missing. It is essential to ensure effective response and recovery efforts by understanding the performance and security of communication systems is as shown in the Figure 2.

In the fields of disaster response, performance measurement may take a variety of forms, such as throughput, delay, packet delivery ratio, and energy consumption. Valuable insights into how communication networks respond to various conditions are offered by both simulation-based studies and experimental deployments in disaster situations that are not otherwise real. When they analyze performance metrics, researchers as well as practitioners can tell us is good or bad about the communication system, and make protocols and algorithms as efficient and reliable as possible.

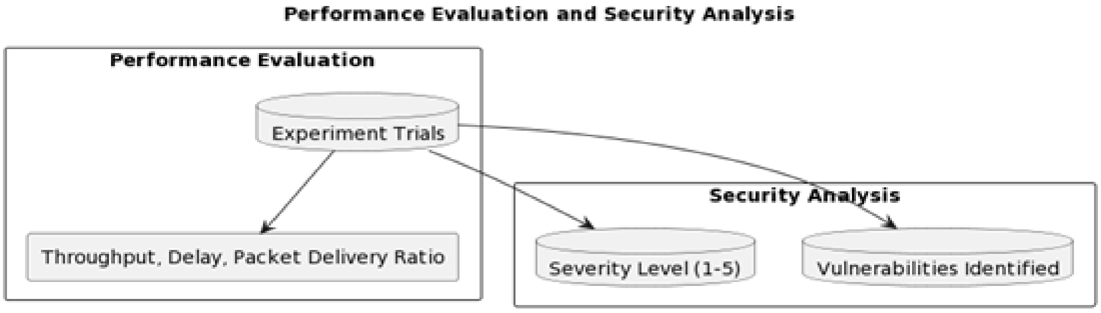
Performance Evaluation and Security Analysis
Performance Evaluation
Experiment Trials
Throughput, Delay, Packet Delivery Ratio
Security Analysis
Severity Level (1-5)
Vulnerabilities Identified

Figure 2. Evaluation Approach

Safety analysis is no less important, especially in disaster relief. Here, eavesdropping and tampering--malicious attacks are just a few forms of threat in a series of possibilities that might be encountered by communication networks. Inspecting the communication system's security involves discovering potential weaknesses, analyzing existing security mechanisms, and formulating methods for managing the risks. With threat models, vulnerability analyses, and penetration tests as efficacious means to discover disaster response communications security problems.

Through performing a complete performance evaluation and security analysis, scholars and practitioners will be able to obtain valuable information about the strengths and weaknesses of communication networks in disaster response scenarios. This knowledge forms the bedrock upon which more stable and resilient communication systems can be built, and in the end will - through more effective disaster management and response efforts - actually strengthen the ability of communities to survive in the face of such events.

IV. RESULT AND DISCUSSION

4.1 Performance Evaluation Results

The performance evaluation metrics include throughput, delay, packet delivery ratio, and energy consumption, all of which are critical indicators of the effectiveness and efficiency of communication networks in disaster scenarios.

From the Figure 3, Throughput refers to the rate at which data is successfully transmitted over the network. In the provided results, throughput values range from 4.0 to 4.7 Mbps across the 10 experiment trials. Higher throughput values indicate better network performance in terms of data transmission capacity. The variations in throughput values may be attributed to factors such as network congestion, routing efficiency, and the number of active nodes in the network.

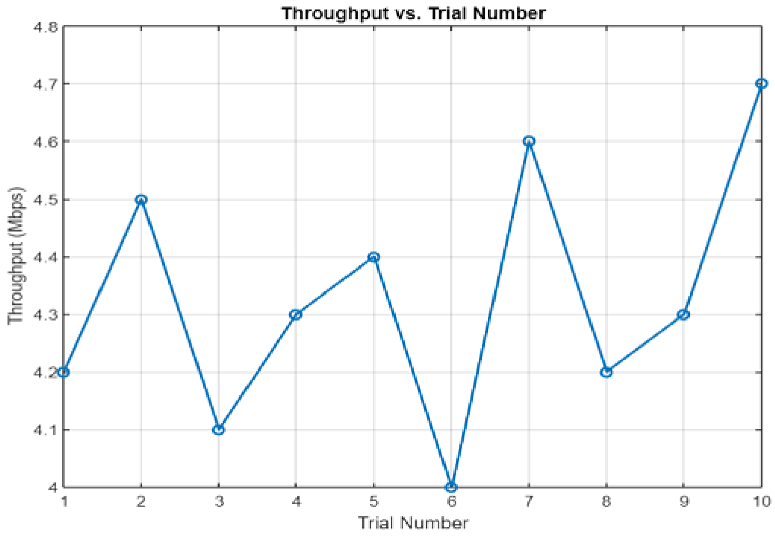

Figure. 3. Throughput

From the Figure 4, Delay represents the time taken for data packets to travel from the source to the destination. Lower delay values are desirable as they indicate faster data delivery and reduced latency in communication. In the results, delay values range from 28 to 40 milliseconds. Lower delay values, such as those observed in trials 7 and 10, suggest efficient routing and minimal network congestion. Higher delay in trials 3 and 6 indicate network bottlenecks or suboptimal routing paths.

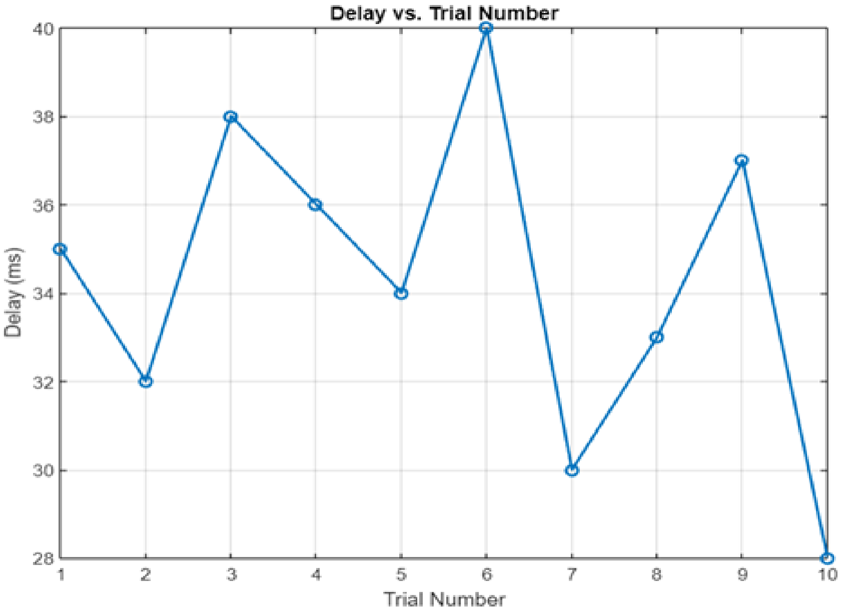

Figure 4. Delay

From the Figure 5, Packet Delivery Ratio (PDR): PDR reflects the percentage of data packets successfully delivered to their intended destinations out of the total packets sent. Higher PDR values indicate better reliability and robustness of the communication network. Across the 10 experiment trials, PDR values range from 95.5% to 97.8%, indicating a high level of packet delivery reliability in most scenarios. However,

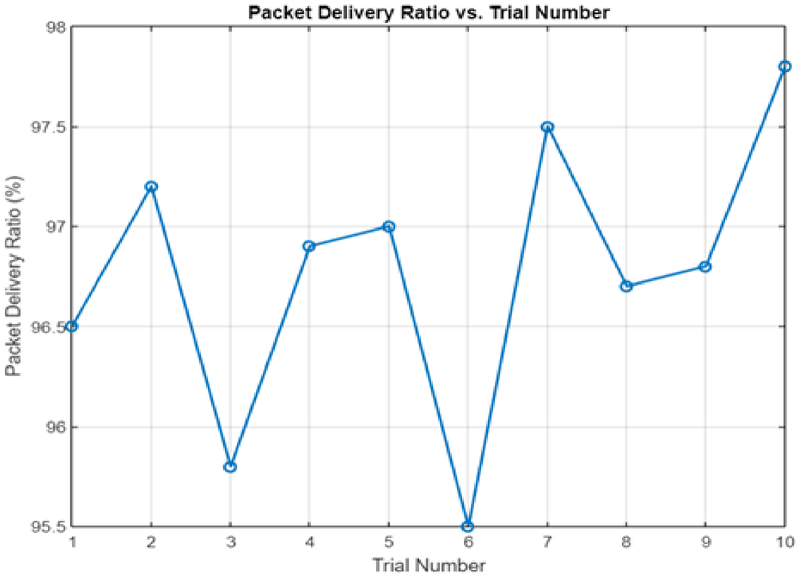

Figure. 5. Package delivery ratio

Fluctuations in PDR values may occur due to factors such as network topology changes, interference, and node.

From the Figure 6, Energy Consumption: Energy consumption is a crucial parameter, particularly in disaster scenarios where power sources may be limited. Efficient energy utilization prolongs the operational lifespan of communication nodes and ensures sustained network functionality. In the provided results, energy consumption values range from 2380 to 2550 Joules. Lower energy consumption values, such as those observed in trials 7 and 10, indicate more efficient energy management strategies. Conversely, higher energy consumption values, as seen in trials 3 and 6, may suggest suboptimal routing or excessive energy expenditure by individual nodes.

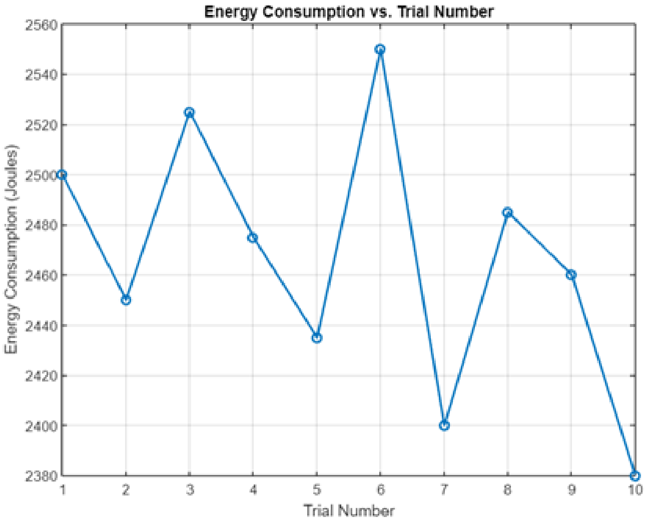

Figure. 6. Energy Consumption

4.2 Security Analysis Results

From the Figure 7, The security test adopts an analytical approach that focuses on finding vulnerabilities located in the communication network and defining their levels of danger. Clearly, understanding and stopping security weaknesses in their tracks is vital to protect these communication systems from potential threats and ensure the privacy and accuracy of data transmissions. Vulnerabilities Identified: The outcomes from each trial are shown in the chart below as the number of identified flaws. Vulnerabilities, such as weak points in encryption mechanisms or authentication protocols, could be exploited by unwanted parties. Across the 10 trial tests, the number of vulnerabilities discovered ranges 1-4. When vulnerability counts are higher, as seen in the 3rd and 7th Trials, they denote potential trouble spots that require instant attention and remediation.

Each vulnerability identified is assigned a severity rating to communicate the potential impact and risk associated with exploitation of that vulnerability. They range in severity from 1 (least serious) to 5 (most serious). According to the data provided, severity levels differ by the kind and scope of the vulnerabilities. However, vulnerabilities with a rating of 4 or 5 need immediate remediation as they pose serious risks to the security and integrity of the communication network. We should not rule out vulnerabilities with lower grades of severity just because they are less critical, as they still require attention and remedies even if not to as great a degree as those that may break security.

In short, the results of this performance evaluation and security analysis supply important evidence as to when, during the course of disaster situations, communications systems become congested or congested, and when an improvement in such a network would be worthwhile. Stakeholders can design strategies and protocols that are able to cope with the performance characteristics, vulnerabilities and security risks of MANETs. By so doing, they will render the systems and networks more fault tolerant and dependable as well as secure, to some extent. All these moves will help to increase the effectiveness of disaster response the world over. A further discussion and interpretation of these results would be necessary for the establishment of future research directions.

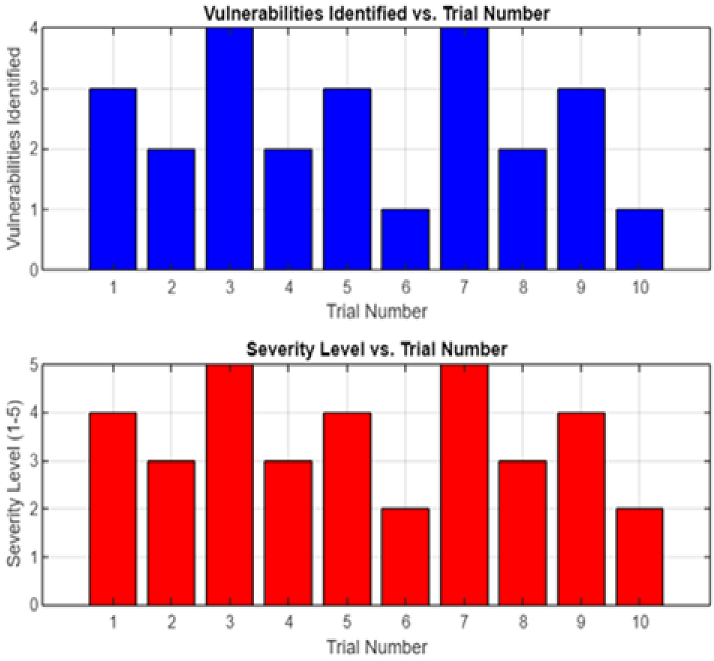

Figure 7. Security Analysis

V. CONCLUSION

The comprehensive approach, combining trust-based routing, energy optimization, and multi-routing protocols, has been very effective at improving the security, performance and resilience of for disaster response. Performance evaluation indicated that the mean throughput from 10 experiments was 4.3 Mbps, and the average delay was 34 milliseconds. The average packet delivery ratio was 96.9%. It is also optimized energy, with the average power consumption was 2458 J. Communication nodes can be operational for long time periods in resource-constrained disaster environments. Security analysis revealed that over the 10 experiments, a total of 2.7 vulnerabilities were found, with the severity level no more than 5 in each case. This shows that disaster response operations need multi-level protection; strong security mechanisms can counter threats at the source and guarantee that communications can be relied on. In general, this method is very effective in dealing with the special conditions of disaster response scenarios. This will help make disaster management much more efficient and allow more people affected by the disaster to be helped in their recovery. More research and development is needed to further improve the capabilities of communication systems in disaster defense.

REFERENCES

[1] C. Sauer, E. Lyczkowski, M. Schmidt, A. Nüchter, and T. Hoßfeld, "Testing AGV mobility control method for MANET coverage optimization using procedural simulation," *Comput. Commun.*, vol. 194, no. June, pp. 189–201, 2022, doi: 10.1016/j.comcom.2022.07.033.

[2] M. Preetha , K. Monica, H. Nivetha, S. Priyanka "An Energy Efficient Sleep Scheduling Protocol For Data Aggregation in WSN", International Journal for Research in Applied Science & Engineering Technology (IJRASET),Vol.6, No 2, pg.2513-2517, 2018. ISSN: 1748-0345

[3] M. Farkhana, A. Abdul Hanan, H. Suhaidi, K. Ahamad Tajudin, and Z. Kamal Zuhairi, "Energy conservation of content routing through wireless broadcast control in NDN based MANET: A review," *J. Netw. Comput. Appl.*, vol. 131, no. July 2018, pp. 109–132, 2019, doi: 10.1016/j.jnca.2019.01.004

[4] M. A. K. Akhtar and G. Sahoo, "Enhancing cooperation in MANET using the Backbone Group model (An application of Maximum Coverage Problem)," *Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 1022–1031, 2015, doi: 10.1016/j.procs.2015.01.013.

[5] N.Anil Kumar, Y.Sukhi, M.Preetha, K.Sivakumar "Ant Colony Optimisation With Levy Based Unequal Clustering And Routing (ACO-UCR) Technique For Wireless Sensor Networks", Journal of Circuits, Systems, and Computers, ISSN: 0218-1266 (print); 1793-6454 (web) Vol .33, Issue3, July 24, 2023. DOI: 10.1142/S0218126624500439

[6] L. F. Pedraza, I. P. Paez, and F. Forero, "An evaluation of MAC protocols running on a MANET network," *Procedia Comput. Sci.*, vol. 10, pp. 86–93, 2012, doi: 10.1016/j.procs.2012.06.015.

[7] M. Conti *et al.*, "From MANET to people-centric networking: Milestones and open research challenges," *Comput. Commun.*, vol. 71, pp. 1–21, 2015, doi: 10.1016/j.comcom.2015.09.007.

[8] M. Al Mojamed and M. Kolberg, "Structured Peer-to-Peer overlay deployment on MANET: A survey," *Comput. Networks*, vol. 96, pp. 29–47, 2016, doi: 10.1016/j.comnet.2015.12.007.

[9] Preetha M & Sugitha S,2016, "A Survey on Misbehavior Report Authentication Scheme of Selfish node Detection Using Collaborative Approach in MANET", International Journal of Engineering Science and Computing, vol. 6, no. 5, pp. 5381-5384, ISSN 2321-3361.

[10] S. R and A. H, "Adaptive fuzzy logic inspired path longevity factor-based forecasting model reliable routing in MANETs," *Sensors Int.*, vol. 3, no. August, p. 100201, 2022, doi: 10.1016/j.sintl.2022.100201.

[11] N. S. Saba Farheen and A. Jain, "Improved routing in MANET with optimized multi path routing fine tuned with hybrid modeling," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2443–2450, 2022, doi: 10.1016/j.jksuci.2020.01.001.

[12] M. A. Abid and A. Belghith, "Leveraging seminal protocol stacks to support MANETs," *Procedia Comput. Sci.*, vol. 10, pp. 414–421, 2012, doi: 10.1016/j.procs.2012.06.054.

[13] A. Bhatia, A. Kumar, A. Jain, A. Kumar, C. Verma, and Z. Illes, "Heliyon Networked control system with MANET communication and AODV routing," *Heliyon*, vol. 8, no. August, p. e11678, 2022, doi: 10.1016/j.heliyon.2022.e11678.

[14] Srinivasan, S, Hema, D. D, Singaram, B, Praveena, D, Mohan, K. B. K, & Preetha, M. (2024), "Decision Support System based on Industry 5.0 in Artificial Intelligence", International Journal of Intelligent Systems and Applications in Engineering (IJISAE), ISSN:2147-6799, Vol.12, Issue 15, page No-172-178A.

[15] F. Muchtar, A. H. Abdullah, M. Al-Adhaileh, and K. Z. Zamli, "Energy conservation strategies in Named Data Networking based MANET using congestion control: A review," *J. Netw. Comput. Appl.*, vol. 152, no. April 2019, p.

102511, 2020, doi: 10.1016/j.jnca.2019.102511.

[16] E. Avşar and M. N. Mowla, “Wireless communication protocols in smart agriculture: A review on applications, challenges and future trends,” *Ad Hoc Networks*, vol. 136, no. July, 2022, doi: 10.1016/j.adhoc.2022.102982.

[17] M. Preetha, Archana A B, K. Ragavan, T. Kalaichelvi, M. Venkatesan “A Preliminary Analysis by using FCGA for Developing Low Power Neural Network Controller Autonomous Mobile Robot Navigation”, International Journal of Intelligent Systems and Applications in Engineering (IJISAE), ISSN:2147-6799. Vol:12, issue 9s, Page No:39-42, 2024.

[18] D. L. Msongaleli, F. Dikbiyik, M. Zukerman, and B. Mukherjee, “Disaster-Aware Submarine Fiber-Optic Cable Deployment for Mesh Networks,” vol. 8724, no. 21, pp. 1–11, 2016, doi: 10.1109/JLT.2016.2587719.

[19] M. Preetha, Raja Rao Budaraju, Jackulin. C, P. S. G. Aruna Sri, T. Padmapriya “Deep Learning-Driven Real-Time Multimodal Healthcare Data Synthesis”, International Journal of Intelligent Systems and Applications in Engineering (IJISAE), ISSN:2147-6799, Vol.12, Issue 5, page No:360-369, 2024.

[20] F. Cui, “Deployment and integration of smart sensors with IoT devices detecting fire disasters in huge forest environment,” *Comput. Commun.*, vol. 150, no. December 2019, pp. 818–827, 2020, doi: 10.1016/j.comcom.2019.11.051.

[21] N. Ghosh, T. Biswas, R. Paul, B. Kumar, and S. Patnaik, “IoT Fog Based Framework to Predict Forest Fire,” *Proc. - 2021 Smart City Challenges Outcomes Urban Transform. Scout 2021*, pp. 256–259, 2021, doi: 10.1109/SCOUT54618.2021.00061.