Secure and Intelligent DAWN-MANET Routing via AI and IoT Integration for Disaster Response

Khanista Namee [1,*], Rudsada Kaewsaeng-On [2], Karn Na Sritha[1], Pitpimon Choorod [1], and Jantima Polpinij [3]

[1] Faculty of Industrial Technology and Management, King Mongkut's University of Technology North Bangkok, Prachinburi, Thailand

[2] Faculty of Humanities and Social Sciences, Prince of Songkla University, Songkla, Thailand

[3] Faculty of Informatics, Mahasarakham University, Mahasarakham, Thailand

Email: Khanista.N@fitm.kmutnb.ac.th (K.N,); Rudsada.K@psu.ac.th (R.K.); Karn.N@itm.kmutnb.ac.th (K.N.S.); Pitpimon.C@itm.kmutnb.ac.th (P.C.); Jantima.P@msu.ac.th (J.P.)

*Corresponding author

***Abstract*—The Disaster Area Wireless Mesh Mobile Ad Hoc Network (DAWN-MANETs) face many challenges such as: moving topology, lack of pre-determined infrastructure and vulnerable to a variety of attacks which make it quite difficult in establishing the reliable and secure communication. Although current Ad hoc On-Demand Distance Vector (Secure-AODV) and AI-based MANET schemes are designed for addressing the security or adaptability problems only and do not have a disaster-aware decision-making model in place. In this paper, we present an integrated Artificial Intelligence-Internet of Things (AI-IoT) secure routing framework for DAWN-MANETs. The proposed approach successfully integrates management of IoT-assisted situational awareness and AI-based decision-making engine along with secure AODV routing protocol. This approach assures adaptive and secured routing under dynamic and adverse disaster situations. As network and environmental data can be monitored and analyzed in real-time, the approach can dynamically calculate routing paths which best balancing between reliability and security under the stochastic environment. Experimental results demonstrate that the proposed framework significantly improves the important network performance parameters as compared to traditional AODV and Secure-AODV protocols. The robustness of packet delivery, communication delay and security against attack scenarios have been well improved. With these strengths, it is believed that the integration disaster awareness and intelligent decision-making into secure routing protocols can greatly enhance the robustness and fitness for DAWN-MANETs. Despite focusing on simulation-based validation in the present research, the framework provides a scalable basis for actual application in disaster responses.**

***Keywords*—secure routing, Disaster Area Wireless Mesh Mobile Ad Hoc Network (DAWN-MANETs), disaster response, Artificial Intelligence (AI), Internet of Things (IoT), AODV protocol, Mobile Ad Hoc Networks (MANETs)**

I. Introduction

Traditional methods of communication frequently fail or become inaccessible during natural disasters and emergency scenarios. In these situations, establishing a temporary and rapidly deployable communication infrastructure is essential for the effective delivery of emergency services. Included in this category are Disaster Area Wireless Networks (DAWNs), which utilise Mobile Ad-hoc Networking (MANET). They stand out as one of the most reliable solutions due to their self-configuration and infrastructure-less characteristics. Nonetheless, there are considerable limitations associated with conventional MANET-based DAWNs when it comes to real-time decision-making, adaptability, and data security.

The integration of AI and IoT addresses the most complex issues arising from traditional DAWN-MANET based architectures. Lightweight machine learning models are employed to analyses dynamic network data in real-time, facilitating intelligent context-based routing decisions. This encompasses forecasting network congestion, identifying malicious routing activities, and adaptively re-optimizing paths based on situational awareness. Conversely, IoT peripherals such as temperature sensors, gas leak sensors, accelerometers, and GPS trackers function as edge-level environmental probes, providing crucial context regarding the surrounding environment and objects. The integration of AI and IoT systems allows DAWN-MANETs to transition from a reactive to a proactive mode of operation. This advancement facilitates predictive routing, early identification of threats—such as pinpointing unsafe areas through gas sensors—and real-time prioritization of emergency traffic. This integrated architecture establishes a secure and adaptive communication system that effectively meets the evolving demands of disaster scenarios, ensuring robust communications, context-awareness, and a strong survivability profile even in the face of hostile or unforeseen operating conditions.

This study presents an innovative integrated method that merges Artificial Intelligence (AI) with the Internet of Things (IoT) within a DAWN-embedded framework on top of MANETs to facilitate path migration for dynamic route optimization. The AI component utilizes lightweight classifiers and decision trees to monitor changes in various network metrics in real-time, including node density,

Manuscript received September 30, 2025; revised December 14, 2025; accepted January 29, 2026; published May 22, 2026.

mobility patterns, and residual energy levels, facilitating dynamic path discovery. The IoT layer incorporates distributed environmental sensors (e.g., gas, motion, temperature) that serve as context triggers for making intelligent routing decisions that priorities life-critical traffic and hazard alerts. The runtime of the AI-IoT system is decentralized and incorporates lightweight protection schemes, utilizing nonce-based packet verification and symmetric AES-128 encryption to enhance resilience against jamming, eavesdropping, and routing attacks. The performance of the proposed method is evaluated using simulations in NS-2.35, comparing standard AODV and Secure-AODV across various mobility and threat situations. The test findings indicate substantial enhancements in PDR, time delay, packet loss prevention, and energy efficiency, confirming the efficacy of the integrated architecture in facilitating context-aware, secure, and reliable communication during disaster response scenarios.

The main contributions of this paper are summarized as below. It provides the first AI–IoT-integrated secure routing framework which is customized for DAWN-MANETs. This architecture binds together the IoT-aided situational awareness, AI inspired decision-making and secure AODV based routing in a natural way. Second, the article introduces an AI-based utility decision model that can dynamically determine secure and efficient routing paths when confronted with rapidly changing and malicious environments seen in disaster situations. Third, the proposed approach is subjected to a thorough validation by extensive simulations under a range of mobility and attack settings. The results show substantial improvement in Packet Delivery Ratios (PDRs), decrease in end-to-end delay and resilience over traditional AODV and Secure-AODV protocol.

Accordingly, this study is guided by the following research questions:

RQ1: How can AI–IoT integration enhance routing resilience in DAWN-MANET under security threats?

RQ2: To what extent does the proposed framework improve packet delivery, delay, and packet loss compared to baseline Secure-AODV approaches?

RQ3: What are the trade-offs between routing performance and energy consumption in disaster scenarios?

II. Literature Review

The integration of AI and IoT into MANETs has been suggested as a transformative strategy to enhance the resilience and efficacy of communication systems in disaster response. Due to the dynamic nature and insufficient infrastructure in post-disaster settings, MANETs are ideally suited for decentralized and rapid deployment networks. Nonetheless, challenges pertaining to heterogeneity, latency, security, and data fusion remain unresolved and are currently the focus of extensive scholarly research.

Interoperability is a critical concern with the integration of AI/IoT with MANETs. The variety of equipment, communication protocols, and data architectures complicates the implementation of transparent networking on these nodes. Research has demonstrated that the issue can be effectively addressed by implementing blockchain frameworks to provide standardized, secure, and tamper-resistant protocols [1, 2]. The research conducted by Kumbhar and Ali [3] demonstrated a blockchain-based secure communication protocol that significantly improved inter-device communications across cross-platform devices in MANET environments.

Latency is a critical component, particularly for real-time applications such as emergency reporting and hazard warning. Traditional MANET routing systems, such as AODV and DSR, exhibit responsiveness that results in elevated communication latency in unstable networks. Fog computing and edge intelligence are frequently employed to mitigate latency difficulties by processing data near its source, hence reducing round-trip time [4, 5]. Trinh *et al.* [6] determined that implementing AI models at the edge resulted in a latency reduction of up to 38% in emergency communication scenarios compared to cloud-only methods.

Data fusion is essential for deriving significant judgements from multisensory inputs, including wearables, drones, structural sensors, and environmental monitors. Advanced data fusion methodologies, including the Kalman filter, Bayesian inference, and Dempster-Shafer theory, have been employed to reconcile contradictory sensor inputs into coherent situational awareness [7, 8]. Moreover, deep learning architectures like CNNs have been employed for multimodal input processing to enhance event classification and pattern identification [9].

Incorporating AI and IoT elements into a MANET exacerbates security concerns. The dynamic and distributed nature of these networks renders them susceptible to several attacks, including blackhole, wormhole, sybil, and eavesdropping [10]. Encryption may be insufficient in the event of a calamity. Consequently, AI-driven Intrusion Detection Systems (IDS) and anomaly prediction techniques have been implemented [11]. Techniques such as Support Vector Machines, Recurrent Neural Networks, and ensemble learning have been employed to detect malicious actions in real-time. Gopalakrishnan *et al.* [12] asserted that the integration of lightweight encryption with AI-driven behavior monitoring yields optimal performance in resource-constrained environments.

Blockchain and Distributed Ledger Technologies (DLTs) have emerged as effective methods for trust-centric applications and reliable data dissemination. These mitigate the need for centralized authentication systems, which are impractical in emergency scenarios. Gopalakrishnan *et al.* [13] proposed a hybrid blockchain-Internet of Things architecture for safe and traceable communication across mobile catastrophe nodes. Similarly, Tham *et al.* [14] introduced a trust architecture based on smart contracts to enhance collaboration across unfamiliar MANET nodes.

Software Defined Networking (SDN) and Network Function Virtualisation (NFV), in conjunction with

artificial intelligence technologies, represent some of the most promising and adaptable network concepts currently emerging. These paradigms enable dynamic network topology and functional adaptability using real-time analytics. Mouradian *et al.* [15] introduced an SDN-based MANET network that employed AI to alleviate traffic from crowded nodes, resulting in a 29% enhancement in throughput. Furthermore, fog computing can be integrated with Software-Defined Networking (SDN) to rapidly reallocate resources in response to network dynamics [16, 17].

Recent studies also examine federated learning, which facilitates dispersed intelligence while safeguarding data privacy. In contrast to centralized methods, federated learning allows MANET nodes to collaboratively train AI models while preserving the confidentiality of sensitive sensor data. Mangla *et al.* [18] discovered that it not only enhanced privacy compliance but also improved model generalization in mobile contexts. Privacy-preserving neural networks (PPNNs) demonstrate promise in enhancing the performance of Mobile Ad Hoc Networks (MANETs) while mitigating the dangers of data leakage [19].

Unmanned Aerial Vehicles (UAVs) function as mobile data collectors, routers, and monitoring nodes inside Mobile Ad Hoc Networks (MANET). The synergistic application of AI and IoT in UAV-MANET nodes has enhanced network accessibility and robustness in geographically inaccessible areas. UAV-assisted routing systems can establish Line-of-Sight (LoS) communications to reduce communication delay and enhance bandwidth efficiency. Chandran and Vipin [20] illustrated the application of swarm intelligence and drone coordination algorithms for maintaining stable networks in rapidly evolving crisis situations.

The research indicates an agreement about the integration of AI-IoT into MANETs for disaster management. However, it also highlights ongoing trade-offs that entail increased computing complexity and energy consumption, alongside the efficient utilization of the spectrum. Future tasks involve optimizing lightweight AI algorithms, developing energy-efficient communication protocols, and validating models through hardware-in-the-loop simulations or field experiments.

This survey provides a comprehensive examination of the essential and advanced techniques for securing, optimizing, and deploying AI-IoT-enabled MANETs. These elements are crucial for the methodology suggested in this paper to integrate optimal adaptive routing, context-aware security, and decentralized intelligence methods to enhance disaster response systems.

However, despite remarkable progress made by existing Secure-AODV mobile ad hoc networks, AI-induced and IoT-efficient routing solutions for MANETs remain few insufficiencies unsolved. Most secure routing approaches mainly focus on cryptography or trust model, and very little flexibility in dynamic disaster environment can be offered. AI-based routing schemes, on the other hand are more adaptable but they, often times do not consider integrated security aspects and real-time situational awareness is required. IoT-aided paradigms help to facilitate environmental sensing, whilst its reliance on regular routing protocols results in suboptimal performance under adversarial conditions [21]. Moreover, the majority of previous works did not sufficiently study scalability, energy cost and real deployment practicability in terms to-scalable IDS. Such deficiencies call for an integrated framework accommodating security, flexibility and disaster supported services. In this context, we are going to present a new AI–IoT-based secure routing methodology for Disaster-Aware Wireless Mobile Ad Hoc Networks and which addresses clearly all the forthcoming constraints related to coordinated sensing, intelligent decision-making as well as secure routing optimization [22].

III. Proposed Framework

The suggested architecture comprises three overlay layers to facilitate the seamless integration of AI and IoT technologies with MANET protocols, enhancing communication in crisis scenarios. The layers comprise the IoT sensor layer, the AI decision engine, and the secure routing mechanism. Collectively, they offer context-sensitive routing and security in a highly dynamic PoD environment. Fig. 1 presents the overall architecture, highlighting the interaction between environmental sensors and the routing module.

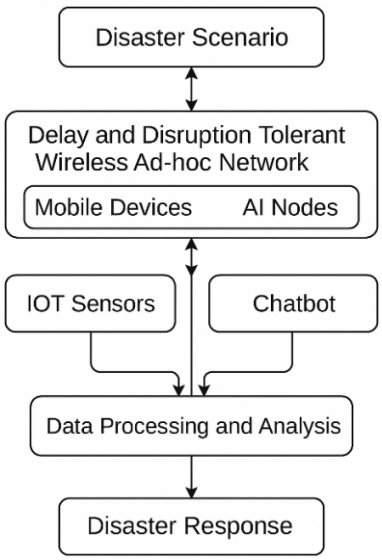

Fig. 1. Integrated framework of AI and IoT in DAWN-MANET for secure disaster response.

A. IoT Sensing Layer

This layer consists of various situational sensors, optimized for near real-time hazard detection and situational awareness tasks. Sensors such as temperature sensors, gas leak detectors, vibration devices, motion detectors, and GPS modules are sparsely distributed around the simulation area to simulate ground-level measurements in disaster-affected regions. The captured data is transmitted at intervals via a straightforward protocol, together with location and priority information.

These measurements are aggregated and converted into contextual triggers that inform routing decisions [2, 3].

B. AI-Based Decision Engine

The decision engine functions as a global cognitive module within each node. It utilises contextual data from IoT sensors and employs local neighbour routing statistics. A mixed machine learning model that integrates decision trees and fuzzy logic is employed to award utility scores to the available routing paths. This utility score U_i for a path i is calculated using the following formula:

$$U_i = w_1.A_i + w_2.S_i + w_3.R_i + w_4.C_i \quad (1)$$

where:
A_i: Available energy of the node
S_i: Signal strength of the link
R_i: Historical route stability
C_i: Contextual priority from IoT input (e.g., hazard alert)
w_1, w_2, w_3, w_4: Tunable weights for each parameter

This adaptive scoring approach enables the framework to priorities routes that pass through stable, secure, and resource-efficient nodes [17]. For instance, in the event of harmful gas detection, routes traversing vulnerable areas are dynamically deprioritized.

C. Secure Routing Layer

This layer employs a lightweight security protocol that implements Secure-AODV to address security concerns in MANETs. Principal improvements comprise:

- Nonce-based request validation to mitigate replay attacks.
- Packets are encrypted using AES-128 to guarantee confidentiality.
- Node authentication utilizing a symmetric pre-distributed shared key among the rescue devices.
- Dynamic blacklist to isolate rogue nodes that disrupt or inundate the route.

These three levels function concurrently. A superior routing path is automatically refreshed in real-time to accommodate fluctuations in operational conditions and node status [11]. Fig. 2 illustrates the overall architecture of the system, emphasizing the interconnections among IoT sensors, the AI decision engine, and the secure routing core.

D. Proposed System Architecture

From scalability and practical deployment perspectives, the proposed AI–IoT-integrated architecture is tailored for the emerging densely deployed nodes faced by disaster-response ecosystems. The routing algorithm is based on localized IoT sensing incorporating lightweight AI inferences, resulting the least overhead control at network expansion [23]. While the AI decision engine imposes additional computation overhead, this is maintained at low cost due to periodical inference and route-level optimization rather than per-packet ones. Deployment wise, the framework is intended to work with off-the-shelf IEEE 802.11-based Mobile Ad Hoc Network (MANET) hardware, no centralized infrastructure is necessary and the nodes can be quickly deployed in disaster areas [24]. There are practical issues to be resolved, however: these include energy constraints and the existence of heterogenous IoT devices as well as featuring real-time inference latency factor, all necessary to overcome for successful deployment at scale on the ground.

E. AI Decision-Making

The AI-driven decision engine is a utility-based approach to route selection that takes factors related to the network and its security profile into account in a dynamic manner. The input features include node mobility, remaining energy, link quality and packet-forwarding behavior as well as attack indications discovered by means of IoT-assisted situational sensing. These characteristics are integrated into a single utility function used to allow scoring for candidate routes. The routing path with the maximum utility is selected, achieving an optimal compromise between security, reliability and efficiency under dynamic disaster scenarios. Such decision making is made periodically and not for each individual packet, thereby minimizing computational efforts along with providing adaptation- and context-awareness to routing optimization.

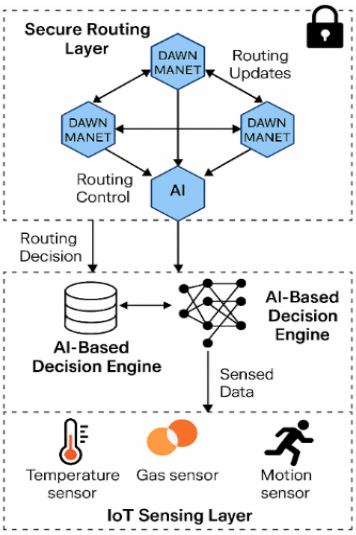

Fig. 2. The system ARC biotecture.

IV. Materials and Methods

A simulation environment utilizing NS-2.35 was established for the performance examination of the proposed AI-IoT integrated DAWN-MANET framework. The network was designed to simulate genuine post-disaster scenarios characterized by a lack of infrastructure and mobile nodes. The simulation was conducted to evaluate the new architecture in comparison to established protocols like AODV and Secure-AODV across various mobility patterns and danger levels. The underlay communication layer assumes IEEE 802.11-based wireless links operating at 2.4 GHz, consistent with typical MANET and disaster-response deployments.

The AI unit employs lightweight supervised learning methods, specifically decision trees and fuzzy logic inference, to categories routes based on diverse network characteristics, including residual energy, mobility

prediction, and link stability. The IoT layer comprises simulated sensors, including temperature, gas, and motion detection, integrated within the simulation space. These monitors provide context-sensitive inputs that influence routing decisions by signaling hazardous or high-priority zones. The AI decision engine is trained using simulation-generated routing and network state datasets derived from NS-2.35 under varying node mobility and attack conditions.

The proposed system addresses common MANET security threats including black hole attacks, selective packet dropping, route falsification, and denial-of-service behavior. Security procedures included nonce-based request verification and symmetric encryption using AES-128 [11, 13]. The procedures for updating the routing table were altered to respond to replayed packets and black hole modules when jamming symptoms are identified. The efficacy of four in-network processing methods was assessed based on Packet Delivery Ratio, End-to-End Delay, Energy Consumption, and Packet Loss in the context of security assaults.

Simulations were conducted for three scenarios involving 30, 50, and 70 nodes. One of the benchmark cases was defined by varying mobility and Constant Bit Rate (CBR) situations, integrated with stochastic models. The simulation area was established at 1000 m × 1000 m, with node velocities varying from 0 to 20 m/s for a duration of 500 seconds as shown in Table I.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Simulation Tool	NS-2.35
Simulation Area	1000 m × 1000 m
Number of Nodes	30, 50, 70
Traffic Model	Constant Bit Rate (CBR)
Node Mobility	Random Waypoint
Node Speed	0–20 m/s
Packet Size	512 bytes
Simulation Time	500 seconds
Routing Protocols	AODV, Secure-AODV, Proposed
Attack Models	Replay, Jamming, Blackhole

To model energy consumption for each transmission, we used the simplified linear energy model:

$$E_{tx} = E_{elec} \times k + E_{amp} \times k \times d^2 \quad (2)$$

where:

E_{tx} is the total energy consumed for transmitting a packet.

E_{elec} is the energy dissipated per bit to run the transmitter or receiver circuitry.

E_{amp} is the energy used by the transmit amplifier.

k is the size of the message in bits.

d is the distance between transmitter and receiver.

This model was used to estimate the energy profile of the proposed protocol compared to baseline AODV and Secure-AODV under identical conditions.

To improve reproducibility, the AI decision model was trained by simulation-based datasets retrieved from NS-2.35; including different node mobilities and attack models. The training and validation data was split 80:20. The model parameters were tuned offline before evaluation. In order to increase the robustness of the results, each simulation scenario is run several times with different random seeds and the reported performance metrics correspond to the average ones over those replications [25]. Statistical validation was conducted to obtain the average and standard deviation of the important metrics which are packet delivery ratio, end-to-end delay and packet loss rate respectively.

V. RESULTS

All performance results presented in this section are obtained from multiple independent simulation runs performed with similar parameters. To account for stochastic fluctuations, each scenario was run multiple times with different random seeds and the values below are obtained as average results. Variability across different runs was investigated through consistent overall performance trends of important metrics like Packet Delivery Ratio, End-to-end delay and Packet loss rate.

In order to assure fair and accurate performance evaluation the considered framework was evaluated on common simulation scenario with the baseline protocols: AODV and Secure-AODV. All simulations utilized NS-2.35 under different node mobility patterns and attack scenarios. Every experimental setting was repeated several times with different random seeds to alleviate stochastic noise, and we show the average performance scores. Statistical verification was also assured by recording the average and standard deviation of key parameters such as PDR, EED and PLR. This enables the performance trends of the various routing schemes to be compared more rigorously.

The simulation results illustrate the performance, security robustness, and energy efficiency characteristics of our AI-IoT Secure-AODV system. Four performance evaluation criteria were established: Packet Delivery Ratio (PDR), End-to-End Delay, Energy Consumption, and Packet Loss Rate. The experiment evaluates the number of nodes with varying densities (30, 50, and 70 nodes) in an adversarial environment characterised by replay, jamming, and blackhole attacks. The computational complexity of the AI decision process grows linearly with the number of candidate routes, while communication overhead remains comparable to Secure-AODV with marginal additional control packets.

A. Packet Delivery Ratio (PDR)

The suggested AI-IoT Secure-AODV demonstrated a superior Packet Delivery Ratio (PDR) relative to existing protocols across all scenarios. In the scenario with 70 nodes, the suggested protocol attained a Packet Delivery Ratio (PDR) of 92.6%, compared to 88.1% for Secure-AODV and 83.4% for AODV. This enhancement results from intelligent routing selection based on sensor context and priority hierarchy utilizing an AI system.

B. End-to-End Delay

The suggested protocol, utilizing context-aware decision-making and congestion avoidance, reduced the average end-to-end delay to 140 ms, compared to 165 ms for Secure-AODV and 160 ms for AODV.

C. Energy Consumption

The proposed approach demonstrated enhanced energy efficiency by circumventing unreliable paths and reducing retransmissions. The average energy per node was around 2.38 J, just above that of AODV (2.10 J), although demonstrating significantly greater reliability.

D. Packet Loss Rate

The suggested protocol demonstrates resilience against simulated attack scenarios. The packet loss ratio was recorded at 7.4% for blackhole and jamming attacks, but it was elevated for Secure-AODV (11.9%) and AODV (16.6%) as shown in Table II.

TABLE II. PERFORMANCE COMPARISON

Protocol	PDR (%)	Delay (ms)	Energy (J)	Packet Loss (%)
AODV	83.4	160	2.10	16.6
Secure-AODV	88.1	165	2.22	11.9
AI-IoT Secure-AODV	92.6	140	2.38	7.4

Figs. 3 and 4 visually depict the enhancements in Packet Delivery Ratio (PDR) and the reduction in packet loss, respectively, highlighting the advantages of AI-driven IoT integrated catastrophe communication scenarios.

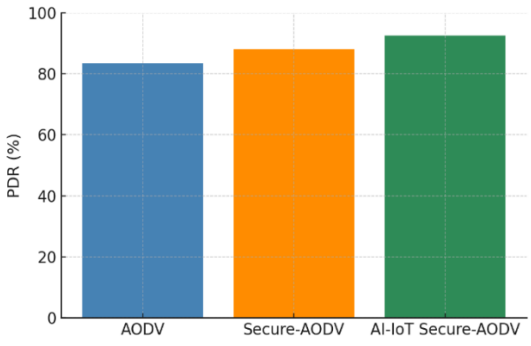

Fig. 3. Packet Delivery Ratio (PDR) comparison.

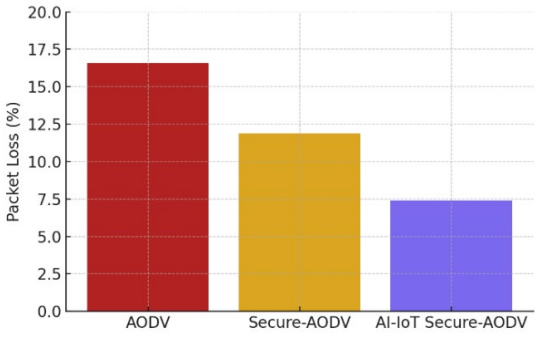

Fig. 4. Packet loss rate comparison.

VI. DISCUSSION

The simulations indicate that the integration of AI and IoT within the DAWN-MANET architecture significantly enhances network robustness and performance during disasters. This section examines the ramifications of the results and delineates the performance trends alongside the strengths vs trade-offs observed during simulation.

A. Interpretation of Results

This increase in the PDR for AI-IoT Secure-AODV verifies enhanced route stability and sophisticated traffic management. The optimal alarms are relayed by a central control center processor, generating the specific base station through which individual addressable smoke detectors communicate with the control center or an inflation indicator included in each alarm. Moreover, the reduction in end-to-end time indicates a potential to minimize routing costs and circumvent overloaded or compromised links. This is crucial for emergencies, as real-time communication could determine life or death.

Energy usage exceeds that of standard AODV, and this trade-off is deemed acceptable due to significant enhancements in reliability and safety. The rise in energy consumption is mostly attributed to cryptographic overhead and additional AI processing demands; nevertheless, the benefits in reliability far outweigh the expenses. The performance findings indicate that the suggested protocol has markedly diminished packet loss, demonstrating its resilience to routing attacks and dynamic topology alterations, which is essential for post-disaster scenarios.

B. Comparative Advantage

The suggested approach has demonstrated much greater resilience compared to traditional AODV and Secure-AODV. It adapts to ambient conditions and network dynamics by employing real-time sensor data and a learning-based route selection process. The supplementary server pass enhances both packet confidentiality and node authentication, addressing the deficiencies present in conventional MANET protocols.

Fig. 2 illustrates a notable increase in Packet Delivery Ratio (PDR) from AODV to AI-IoT Secure-AODV, while Fig. 3 concurrently shows a reduction in packet loss. These trends confirm that the planned improvements are beneficial. The secure routing add-ons successfully mitigated simulated replay, jamming, and blackhole attacks.

C. Limitation and Future Improvements

Nevertheless, there are certain compromises that must be made. Especially when implemented on resource-limited devices, the heightened complexity of the routing process may result in extended computation delays. Additional model size optimization or the introduction of computations with edge nodes may be considered in future work, given that light AI models were retained. Furthermore, improved adaptability can be accomplished by further expanding the diversity of depth sensors and conducting research on routing decisions that are based on deep learning.

The performance analysis presented in this paper is based on extensive simulations with NS-2.35. While simulation-based studies allow a controlled study under multiple disaster and attack scenarios, these studies disregard contact with practical limitations faced in real world deployments such as resource-constrained hardware, noise from the environment and disparate behaviors of heterogeneous devices--all factors which

significantly impact bottom-line performance measures. As a result, the results discussed above mainly show relative performance trends and comparisons to previous levels of advisors rather than concrete real-world performance evaluation. Hardware emulation and field deployment should be taken as key tracks for future validation activities.

The demonstrated improvements in performance validate the effectiveness of combining AI-based decision-making with IoT-supported situational awareness in disaster MANETs. However, these enhancements are not without trade-offs, especially with respect to the computational and energy requirements of AI's decision-making process. Despite its higher packet delivery ratio and decreased delay against attack cases, the additional processing overheads could be impractical for heavily resource-constrained nodes. These compromises suggest that the proposed approach is most suited for scenarios when it is more important to be sure of deploying a fault-tolerant application than to minimize energy consumption.

VII. Conclusion and Future Work

In this paper, we propose a secure routing model based on AI and IoT for DAWN-MANETs. More precisely, the framework is dedicated to enhance routing security in a dynamic and adversarial context. Through joint use of the situation sensing with IoT support, AI enabled decision making and secure routing method to enable adaptive and security aware for optimization-based routing without relying on centralize infrastructure.

Simulation results show that the proposed scheme outperforms both baseline AODV and Secure-AODV protocols in terms of important metrics such as packet delivery ratio, end-to-end delay, and packet loss. This is especially so in the case of attacks while maintaining energy overhead at reasonable level. These results also demonstrate the effectiveness of combining intelligent decision-making and real-time environmental awareness for disaster communication network.

Although the present analysis is limited to simulation-based work, the design provides a scalable framework for eventual real-world application. Future work will be focused on the verification of this framework using hardware implementation, the exploration of federated learning for distributed intelligence and integration with lightweight blockchain solutions to improve security and trust in large-scale disaster-response MANETs.

Despite its promising results, the current study is not without limitations. The performance evaluation is based on simulations running through NS-2.35, an option that allows for controlled experimentation but does not capture important real-world factors including power and hardware constrains, wireless interference with other VIMs (and the operator) when different configurations are applied to the network and variability of devices in disaster scenarios. What is more, the decision-making model powered by AI also introduces a certain amount of computational and energy overhead load to each node which may deleteriously influence scalability in large-scale deployments with severely resource-constrained nodes. Accordingly, the results are indicative of comparative performance trends and do not describe performance in actual operating situations.

There are however several limitations to this study despite the encouraging outcomes. The performance is evaluated by performing simulations using NS-2.35. While this is a good way of conducting controlled experiments with different disaster types, and attack cases, but it does not represent real-word scenarios including hardware constraints, wireless interference, diverse behaviors across heterogeneous devices. Moreover, AI based decision making process introduces moderate computation and energy overhead which may become a challenge in massive deployments with very low resource nodes. Subsequent research will focus on the validation of the proposed framework based on a hardware testbed. It will also investigate the use of federated learning to enable distributed and privacy-centric model training, and the inclusion of lightweight blockchain approaches to enhance trust management and security in large-scale DAWN-MANET deployments.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Khanista Namee conceptualized the research, designed the AI–IoT integrated secure routing framework, supervised the experiments, interpreted the results, wrote the manuscript, and approved the final version; Rudsada Kaewsaeng-On conducted the literature review, contributed to disaster scenario analysis, and reviewed the manuscript; Karn Na Sritha implemented the simulation environment, performed data preprocessing and performance evaluation, and validated the experimental results; Pitpimon Choorod developed the IoT data integration components, collected and analyzed experimental data, and drafted parts of the methodology; Jantima Polpinij validated the AI decision model, provided technical feedback on routing security, and assisted in manuscript revision; all authors have read and approved the final version of the manuscript.

Funding

This research was funded by the National Science, Research and Innovation Fund (NSRF) and King Mongkut's University of Technology North Bangkok, under Project No. KMUTNB-FF-68-B-20.

Acknowledgment

The authors wish to express their sincere gratitude for the financial and institutional support that made this work possible.

References

[1] D. Goyal, A. Sharma, K. D. Garg, B. Sharma, and I. B. Dhaou, "The Internet of Things (IoT) contribution to natural disaster management: Review," in *Proc. 2023 20th ACS/IEEE International*

Conference on Computer Systems and Applications (AICCSA), 2023, pp. 1−7. doi: 10.1109/aiccsa59173.2023.10479272

[2] M. B. Begum, B. Suganthi, P. Sivagamasundhari, S. Arunmozhi, and S. Suhail, "An enhanced heterogeneous local directed acyclic graph blockchain with recalling enhanced recurrent neural networks for routing in secure MANET—IoT environments in 6G," *International Journal of Communication Systems*, vol. 38, no. 4, Jan. 2025. doi: 10.1002/dac.6110

[3] F. H. Kumbhar and S. T. Ali, "Hyper metamorphism: Hyper secure and trustworthy 5G networks using blockchain with IoT," in *Proc. 2023 International Conference on Frontiers of Information Technology (FIT)*, 2023, pp. 166−171. doi: 10.1109/fit60620.2023.00039

[4] R. Lai, G. Zhao, Y. He, and Z. Hou, "A robust sharding-enabled blockchain with efficient hashgraph mechanism for MANETs," *Applied Sciences*, pp. 166−171. Jul. 2023. doi: 10.3390/app13158726

[5] S. Zhang, H. Yan, X. Li, W. Bao, and J. Wang, "Joint resource optimization of mobile edge computing in disaster areas based on 5G communication network," in *Proc. 2023 International Conference on Artificial Intelligence of Things and Systems (AIoTSys)*, 2023, pp. 125−132. doi: 10.1109/aiotsys58602.2023.00041

[6] H. Trinh *et al*., "Energy-aware mobile edge computing and routing for low-latency visual data processing," *IEEE Transactions on Multimedia,* vol. 20, no. 10, pp. 2562-2577 Aug. 2018. doi: 10.1109/TMM.2018.2865661.

[7] C. R. Umeike, X. Guo, T. Dao, S. V. Croope, X. Hong, and A. Johnston, "A standards-based approach to enhancing interoperability of low-cost industrial IoT flood sensors for transportation system resilience," vol. 20, no. 10, pp. 2562−2577. Aug. 2023. doi: 10.1088/1757-899x/1289/1/012022

[8] K. Wrona, M. Tortonesi, M. Marks, and N. Suri, "Leveraging and fusing civil and military sensors to support disaster relief operations in smart environments," in *Proc. 2019 IEEE Military Communications Conference (MILCOM)*, 2019, pp. 790−797. doi: 10.1109/MILCOM47813.2019.9021004

[9] A. M. Raivi and S. Moh, "JDACO: Joint data aggregation and computation offloading in UAV-enabled internet of things for post-disaster scenarios," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 16529−16544, 2024. doi: 10.1109/jiot.2024.3354950

[10] S. Hafeez, R. Cheng, L. Mohjazi, Y. Sun, and M. Imran, "Blockchain-enhanced UAV networks for post-disaster communication: A decentralized flocking approach," arXiv preprint, arXiv:2403.04796, 2024. doi: 10.48550/arxiv.2403.04796

[11] S. J. Patil, L. Admuthe, A. S. Patil, and S. R. Prasad, "Secure MANET routing with blockchain-enhanced latent encoder coupled GANs and BEPO optimization," arXiv preprint, arXiv:2403.04796, 2024. doi: 10.1080/23080477.2024.2355750

[12] S. Gopalakrishnan, E. D. K. Ruby, D. Hemanand, A. Roy, D. Suresh, and S. B. Choubey, "Leveraging AI and blockchain in MANETs to enhance smart city infrastructure and autonomous vehicular networks," *Babylonian Journal of Machine Learning*, pp. 112−120, 2024. doi: 10.58496/bjml/2024/011

[13] D. Cordova, A. Laube, T. M. T. Nguyen, and G. Pujolle, "Blockgraph: A blockchain for mobile ad hoc networks," in *Proc. 2020 4th Cyber Security in Networking Conference*, 2020, pp. 1−8. doi: 10.1109/CSNET50428.2020.9265532

[14] M. L. Tham, Y. Wong, B. H. Kwan, and Y. Owada, "Artificial Intelligence of Things (AIoT) for disaster monitoring using wireless Mesh network," in *Proc. 2023 6th International Conference on Software Engineering and Information Management*, 2023, pp. 234−239. doi: 10.1145/3584871.3584905

[15] J. I. Zahid, F. Hussain and A. Ferworn, "A model of computing and communication for public safety integrating FirstNet, edge computing, and internet of things," in *Proc. 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC, Canada, 2019, pp. 619−623, doi: 10.1109/IEMCON.2019.8936153

[16] C. Mouradian, N. T. Jahromi, and R. Glitho, "NFV and SDN-based distributed IoT gateway for large-scale disaster management," *IEEE Internet of Things Journal*, Aug. 2018. doi: 10.1109/JIOT.2018.2867255

[17] A. Munir *et al*., "FogSurv: A fog-assisted architecture for urban surveillance using artificial intelligence and data fusion," *IEEE Access*, vol. 9, pp. 111938−111959. Aug. 2021. doi: 10.1109/ACCESS.2021.3102598

[18] L. Campioni, N. Fontana, A. Morelli, N. Suri, and M. Tortonesi, "A federated platform to support IoT discovery in smart cities and HADR scenarios," in *Proc. 2020 15th Conference on Computer Science and Information Systems (FedCSIS)*, 2020, pp. 511−519. doi: 10.15439/2020F48

[19] R. Ghoni and T. Ibrahim, "Integration of emergency response management system with internet of things," *Journal of Physics: Conference Series*, 2021, vol. 1874, no. 1, 012074. doi: 10.1088/1742-6596/1874/1/012074

[20] I. Chandran and K. Vipin, "Multi-UAV networks for disaster monitoring: Challenges and opportunities from a network perspective," *Drone Systems and Applications*, vol. 12, pp. 1−28, 2024. doi: 10.1139/dsa-2023-0079

[21] M. Tosun, U. C. Cabuk, O. Dagdeviren and Y. Ozturk, "DAWN-sim: A distributed algorithm simulator for wireless ad-hoc networks in python," in *Proc. 2023 International Conference on Computing, Networking and Communications (ICNC)*, 2023, pp. 635−639. doi: 10.1109/ICNC57223.2023.10074218

[22] K. K and D. N, "Efficient and secured routing management for internet of vehicles using AI," in *Proc. 2025 International Conference on Emerging Technologies in Engineering Applications (ICETEA)*, 2025, pp. 1−5. doi: 10.1109/ICETEA64585.2025.11099968

[23] A. Patekhede, S. Warule, S. Rathod, S. Sultan and V. Pimprale, "A smart disaster management system for emergency hospital allocation," in *Proc. 2025 International Conference on Modern Sustainable Systems (CMSS)*, 2025, pp. 229−238. doi: 10.1109/CMSS66566.2025.11182469

[24] S. Majumdar, L. A. Szolga, and S. Kirkley, "IoT-enabled autonomous vehicles for wildfire relief: A system of systems approach," in *Proc. 2025 13th International Electrical Engineering Congress*, 2025, pp. 1−6. doi: 10.1109/iEECON64081.2025.10987618

[25] Y. I. Mohammed *et al*., "Revolutionizing FANETs with reinforcement learning: Optimized data forwarding and real-time adaptability," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 4295−4310, 2025. doi: 10.1109/OJCOMS.2025.3565471