CENTRALIZED INFRASTRUCTURE-AWARE RELIABLE DATA TRANSACTION MODEL IN IOT-ENABLED MANET AND CLOUD USING PSOA AND RNN

Mustafa almahdi Algaet[1*]

[*]Faculty of information technology, Elmergib University. Email: malgaet@elmergib.edu.ly , mustafaalmahd@outlook.com

Abstract

The proposed data transaction model performs well, it is indeed well-performed as to PSOA properly combined with RNN. From the above traditional techniques with poor PSOA of FANET and TLBO and MLRP, the model was able to achieve 98.78% PDR, 98.42% detection accuracy, and 93% energy efficiency. This is important in ensuring secure IoT-enabled real-time data transfer in MANETs. Mobile Ad-hoc Network MANETs was first utilized in military in decentralized data transfer without any fixed infrastructure. Over time, it began to be used in IoT technologies and smart cities. Furthermore, the challenges have also triggered the employment of advanced techniques such as machine learning and optimization algorithms-based routing compared to early routing protocols like DSR and Ad-hoc On-demand distance vector (AODV) that are insecure and unproductive. This project presents a concept that is infrastructure-aware and centralized for secure data transmission over the Internet of things capable MANETs. The model optimizes the cluster head selection technique through PSOA, therefore, reduced energy consumption, and increased routing efficiency. RNNs have been used in security to recognize intrusions while data is transferred. While their data is encrypted via ECC and the paths have been built by AODV protocol. Only the hash comparisons, which are saved on the fog servers, are utilized for path verification. Results: From the results, the proposed model outperforms traditional methods that have only resulted in 40% fewer energy and 25 ms latency. Apart from that, the proposed model has obtained a PDR of 98.78 % and detection accuracy of 98.42 %. Therefore, the results, insecurity, performance, and ubiquity, have been enhanced compared to previous work with FANET and TLBO & MLRP. Conclusion: The model is suitable for smart cities, and this will work on the proposed system that requires secure transfer and energy utilizations in IoT enabled for MANETs. The proposed model has outperformed the prior work, and the PDR is 98.78 % under a different traffic condition, and the energy efficiency is more than 93 %. For future works, can improve the proposed system with other advanced techniques like deep learning, and blockchain.

Keywords: MANET - Mobile Ad Hoc Network, IoT - Internet of Things, PSOA -Particle Swarm Optimization Algorithm, RNN - Recurrent Neural Network, Intrusion Detection, Energy-Efficient Routing - EER, Ad-hoc On-Demand Distance Vector - AODV, Elliptic Curve Cryptography – ECC.

1 Introduction

With the rapid expansion of the Internet of Things (IoT), Mobile Ad-hoc Networks (MANETs) have become increasingly important in establishing decentralized communication among mobile devices. They create no infrastructure and offer real-time data-sharing in dynamic contexts.

However, due to its dynamic topology and susceptibility to security attacks, MANETs raise significant concerns in providing secure data delivery. propose in this work a centralized infrastructure-aware data transaction model that utilizes Recurrent Neural Networks (RNN) and the Particle Swarm Optimization Algorithm

(PSOA) to tackle these challenges. PSOA helps with cluster head selection optimization, which is crucial for efficient and energy saving data routing. On the other hand, RNN is used for high-level intrusion detection data confidentiality during transmission. This proposed model

Corresponding Author Name: Mustafa almahdi Algaet, Corresponding Author mail: malgaet@elmergib.edu.ly, mustafaalmahd@outlook.com

is suitable for smart cities, healthcare, and defence industries which can possibly get into hacking the data transmission from Internet of Things in MANETs Simpson & Nagarajan (2021).

MANETs have been a topic of extensive research for many years; initially, they were used for military communications in which infrastructure was lack and a decentralized self-configured network is needed Tripathy et al. (2021). Over time their uses have expanded to industries such as IoT systems, vehicle networks, and disaster recovery Singh et al. (2022). Early MANETs, even though they are flexible because of their dynamic and open nature, face a number of problems for providing secure and reliable data transport. Attempts to solve some of these problems were made by protocols like DSR and AODV routing, but they failed to ensure that data was sent in a secure and efficient manner. This lead to development of more sophisticated and state-of-the-art methods with the advancements through machine learning and optimization algorithms.

This model offers two substantial advancements, to deal with the long-standing problems of data safety and the constraint on the performance in Mobile Ad hoc Networks. When the Particle Swarm Optimization Algorithm (PSOA) is used, this results in better selection of the cluster heads of network [23]. For this purpose, PSOA finds the best compromise between exploitation leveraging established and proficient paths while exploring new ones — evoking the collective behaviour of bird flocking. This decreases the energy consumption and increases routing efficiency of data in a dynamic network. For security they have added Recurrent Neural Networks (RNN) to identify the data flow, as well as prediction of possible attacks over long sequence lengths in the data transmission. RNNs are excellent at processing sequences of data which then makes them ideal to use for real-time network monitoring and detection directional risk. The proposed work is an overall solution for secure data transmission in IoT-based MANETs, where the merit of one approach overcomes the limit of the other; thus, a joint PSOA for lightweight routing and RNN to ensure strong security provide a reliable solution.

- To enable safe and dependable data transactions in MANET systems with IoT capabilities, create a centralized infrastructure-aware model.
- Use PSOA for energy saving to improve the routing of cluster head and select the best CH.
- Improve Network Security -- Apply RNN to alarm the intrusion when data transmitting, making a prompt response.
- Use a hybrid strategy that combines PSOA and RNN to guarantee the dependability of data transactions in dynamic MANETs.
- In terms of security, energy efficiency, and general reliability, assess and contrast the model's performance with that of conventional techniques.

2 Literature Survey

Haghshenas et al. (2020). An Infrastructure Aware workload scheduling for efficient Heterogeneity cost of a Data Center The approach depends on a careful energy efficiency of the cooling system and servers as well as priced-in energy prices. It saves by dispatching workloads to servers according to their distinct power characteristics, rather than using general scheduling policies. The findings of the study also suggest that some significant gains can be realised in terms of operational efficiency, and energy savings represent this an attractive approach to sustainable data centre management.

Singh et al. (2022) in decentralized and dynamic situations, Bridge and Meade examine that a link between Wireless MANETs and the IoT could improve communication. They introduce the Internet of Things devices based systems for enhancing resource management, connectivity and scalability of MANETs. This work provides improved routing and communication protocols that can be used to establish reliable, low-latency connections by taking into consideration mobility or limited bandwidth constraint as well as energy efficiency. This will realize a higher degree of situational awareness via an efficient and adaptable communication system in uncertain and dynamic environments, opening new possibilities for smart city, disaster management, as well as vehicular networks.

Tripathy et al. (2021) introduced a context-aware smart IoT-based paradigm where they designed a novel approach to automatic event detection in an uncontrolled scenario. Among others, propose a communication framework between Wireless Sensor Networks (WSNs) and Mobile Ad-Hoc Networks (MANETs). The framework focuses on improving data usages between two networks, energy conservation and ensure the interoperability across the two networks. These authors combine the mobility attribute of MANETs and sensing capacity of WSNs to develop energy-aware routing protocols for efficient data communication. This system is ideal for apps like environment monitoring, disaster response, Smart cities because of its real-time communication design. Moreover, in IoT-driven scenarios, the architecture does and scales to increases network performance while increasing reliability.

The authors in *Basheer and Itani (2023)* discuss "Zero Touch" Within MANETs, fog computing, and the Internet of Things; focusing on its potential to revolutionise applications within smart cities capturing this approach. Zero Touch refers to automated network management that makes a system more efficient and far less responsive invites human intervention. Fog computing helps to reduce the latency caused by processing data near its source, enabling real-time decision-making. This article addresses the challenges in resource management, energy efficiency and security issues associated with MANETs and IoT systems. The overall results of the investigation, show AI-powered, autonomous frameworks can optimize smart city infrastructure to increase its flexibility, efficiency, and lower cost.

Simpson and Nagarajan (2021) provide the fuzzy logic method to detect blackmailing attacks at MANET-IoT systems inside edge-computing nodes. Hostile nodes accuse lawful nodes in these assaults to impair network operations. The system collaborates with other nodes and accurately identifies threats, reducing the number of false positives and negatives. Node trust levels are evaluated using Fuzzy Logic This ensures an optimal real-time threat detection even for edge nodes with low footprints. As the protocols provide a lightweight security defense against internal attacks for MANET-IoT networks, which enhances system security and network reliability for such delay-sensitive systems.

Sixu et al. (2022) that focuses on clustering for mobile SD-WSNs with the use of two frameworks: Artificial Bee Colony (ABC), and Particle Swarm Optimization (PSO). Their approach of efficient, scalable and energy-efficient network usage —by optimizing the grouping and management of sensor nodes. Based on ~~these~~ this knowledge the system implements fast algorithms that increase as well as prolong the life-span of network and allow effective data transmission, load balancing with improved resource management. ~~We~~ Believe that this solution can be of interest for mobile cases, and more generally a bunch of applications from industrial monitoring to smart cities and environmental sensing.

Ahmed and Al-Asadi (2024) present a unique optimised link state routing (OLSR) protocol for efficient video streaming in mobile ad-hoc networks. It includes a deep-learning model for detecting black-hole nodes that employs a twin-attention-based dense convolutional bidirectional gated network (SA_DCBiGNet) and trust values for neighbouring nodes. The extended osprey-aided OLSR protocol (EO_OLSRP) improves routing, while the extended osprey optimisation algorithm (EOOA) picks the best features based on node and link stability. Blockchain storage with IPFS technology protects data, and a delegated proof-of-stake (DPoS) consensus mechanism is used. The model surpasses the existing methods in terms of packet delivery ratio (PDR), average end delay (AED), and throughput.

Rajya Lakshmi Gudivaka's (2023) study describes a cloud-based robotic system that uses robotic process automation (RPA) to help elderly folks and others with cognitive impairments. Using advanced deep learning models for behavior and object identification, the system achieves 97.3% accuracy, improving caregiver support and user independence, but it requires consistent online connectivity.

Krishnasamy et al. (2024) offer a novel approach for intrusion detection and attack prevention in Mobile Ad Hoc Networks (MANETs), which pose security problems due to their dynamic nature and lack of central coordination. The Dual Interactive Wasserstein Generative Adversarial Network is optimised with the Namib Beetle Optimisation Algorithm. Mobile users must register with a Trusted Authority and provide biometric and location data for authentication. The system comprises packet analysis, feature extraction, preprocessing, and classification. The proposed technique classifies packets into five kinds and outperforms existing models by attaining higher accuracy and reduced delay.

Duong (2024) suggested an improved AODV protocol for 5G-based Mobile Ad-hoc Networks (MANETs), which addresses the issues of high traffic loads and strict QoS requirements. Traditional routing methods suffer in such situations; hence the proposed solution uses reinforcement learning. Each node in the network updates a database with state information about intermediate nodes on the path to the destination. The routing algorithm uses this information to verify that the QoS routes are dependable. The simulation results show that the proposed method greatly improves throughput, end-to-end delay, and signal-to-noise ratio (SNR).

Raj Kumar Gudivaka (2020) suggests using a Two-Tier Medium Access Control (MAC) system to improve energy efficiency and resource management in cloud-based robotic process automation (RPA). The system uses Lyapunov optimization to optimize job prioritizing and resource allocation, exceeding protocols like as IEEE 802.15.4 in terms of throughput, power efficiency, and QoS adherence.

Ray et al. (2024) investigated the challenges of Mobile Ad-hoc Networks (MANETs), which, due to their self-healing nature and reliance on wireless devices, encounter issues such as frequent topology changes, route disruptions, and connection failures. These issues cause significant delays, jitter, and packet loss, especially when the source and destination are several hops distant. To address these problems, the paper presents a cross-layer fragmentation strategy that optimises the transmission of high-resolution, real-time multimedia data by breaking down video frames into smaller chunks. This strategy minimises latency, increases throughput, and improves delivery ratios, particularly in crowded MANET environments with limited capacity.

Kaushik et al. (2024) presented the K-AOMDV protocol to address security and efficiency concerns in Mobile Ad Hoc Networks (MANETs), with a specific emphasis on preventing Black Hole Attacks. Nodes in MANETs interact without any infrastructure, rendering them vulnerable to attacks that interrupt data routing. The K-AOMDV protocol, which is based on Ad Hoc On-Demand Multi-Path Distance Vector Routing (AOMDV), employs K-means clustering to avoid misrouting. It improves route optimisation by using machine learning to forecast best paths, guaranteeing that data is delivered reliably even when malicious nodes exist. The protocol has a high accuracy rate of 99%, with 80% true positives and recall, which improves security and performance.

3 Methodology

This system provides a Particle Swarm Optimization Algorithm (PSOA) + Recurrent Neural Network (RNN) approach to ensure the strong security and efficiently in data transmission of MANETs by Internet of Things (IoT). To increase the efficiency of routing and minimize energy consumption, PSOA optimizes CHs selection. The RNN can not only protect the data between devices throughout the network, but also perform intrusion detection in real time.

3.1 Node Initialization

First, the mobile nodes existing within MANET are initialized where each node is an independently working entity that can organize itself. The IDs are unique to all the initialized nodes in the network and allow each of them to differentiate themselves from one another. Elliptic Curve Cryptography (ECC) is used to provide safe communication and data exchange between nodes. Elliptic Curve Cryptography (ECC) secures communication between nodes by creating public and private key pairs for encryption, authentication, and data integrity. Its energy economy and lower key lengths make it appropriate for networks with limited resources, such as MANETs. In the proposed model, ECC collaborates with Recurrent Neural Networks (RNN) to detect intrusions and Particle Swarm Optimization Algorithms (PSOA) to optimize routing. This connection improves data security, saves energy, and optimizes performance in dynamic IoT-enabled systems. ECC is more energy and computationally efficient than other encryption methods, offering a higher level of security with shorter key lengths. This makes it perfect for mobile nodes in MANETs that have limited resources. The cryptographic process that generates public and private key pairs for each node allows secure encryption, authentication, and data integrity over the network communications.

Particle Position Update in PSOA:

$$X(t+1) = X(t) + v(t) \tag{1}$$

Where $X(t)$ is the current position of the particle, and $v(t)$ is the new velocity influenced by updating based on global and local best positions.

3.2 Cluster Head Selection Using PSOA

Cluster heads, on the other hand are necessary for proper data routing and network traffic handling. The selection of optimal CHs is supported from PSOA in terms of the following: initializing the population a set of potential CHs are created and each particle represents a node. The energy of these particles and the separation with other nodes are considered. Fitness Best Distance & Max Energy Reserves are calculated by considering fitness of min node distance and max energy reserves. Optimizing Fitness Best Distance and Max Energy Reserves is critical for effective cluster head (CH) selection in MANETs with IoT. Fitness Best Distance provides optimal node spacing for energy-efficient routing, whereas Max Energy Reserves chooses high-energy nodes to keep the network running. These calculations increase energy economy, lower latency, and improve Packet Delivery Ratio (PDR) and detection accuracy. This enables strong and consistent performance, especially in dynamic, resource-constrained contexts such as smart cities and defence applications. Changing the positions of the particles to converge to the best CHs — Weights their new posture by actually weighting on their personal and best so far position. Convergence the process goes until the maximum joint number of CHs is opted for, reducing overall energy consumption and improves routing efficacy.

Fitness Evaluation for CH Selection:

$$F_{CH} = \frac{E_{residual}}{D_{min}} \tag{2}$$

Where $E_{residual}$ is the remaining energy of a node, and D_{min} is the minimum distance between nodes.

3.3 Multi-Path Creation

The model uses the Ad-hoc On-Demand Distance Vector (AODV) protocol, which is a reactive routing mechanism specifically designed for dynamic and decentralized environments such as MANETs in generating multipaths. AODV efficiently constructs routes only when they are needed, lowering overhead and improving resource usage in dynamic MANET settings. It ensures optimal route selection by analyzing paths on latency, energy conservation, and network stability, hence boosting scalability and performance. This method considerably improves energy efficiency (93%) and packet delivery ratio (98.78%), making AODV excellent for secure, efficient communication in IoT-enabled systems such as smart cities and healthcare. AODV minimizes extra network overhead by creating routes only when required. When a source node wants to send data, it broadcasts route request (RREQ) message by AODV. This message will then be broadcast on the network in search of paths to the destination node. After identifying these paths, AODV reviews each of them based on three key parameters: transmission latency, energy conservation and link stability. When are sending out the data, it chooses the best path for data transmission which is called Path with lowest energy and delay. By adapting dynamically to network changes, this adaptive, on-demand strategy decreases overload, improves network scalability, and improves overall performance.

Path Fitness Evaluation:

$$F_{path} = \frac{E_{path}}{T_{path}} \qquad (3)$$

Where E_{path} is the energy consumed along the path, and T_{path} is the transmission time.

3.4 Intrusion Detection Using RNN

For real-time intrusion detection, RNN is used to safeguard the data as it is being transmitted. The capacity of RNN to handle sequential data makes it the perfect option for network activity monitoring. The actions required are as follows data collection pre-processed and collected network traffic data is used. Essential characteristics like source and destination addresses, packet sizes, and transmission durations are extracted. Training and testing using the pre-processed data, the RNN is trained to distinguish between malicious and benign traffic. Intrusion detection the trained RNN model detects any intrusions during data transfer and notifies the system.

RNN-Based Intrusion Detection:

$$y(t) = f(W_h hh(t-1) + W_x hx(t)) \qquad (4)$$

Where $W_h h$ and $W_x h$ are the weights applied to the hidden state and input, respectively, and f is the activation function.

3.5 Data Sensing and Transmission

The Particle Swarm Optimization Algorithm (PSOA) is used to select the Cluster Head (CH), and aids in effective communication between mobile nodes. CH is the first point where different sensed data from device specific and environment by various mobile nodes is merged. When data is found, it is encrypted using Elliptic Curve Cryptography (ECC). Elliptic Curve Cryptography (ECC), which encrypts data with low computational overhead. Its lower key lengths offer high security while conserving resources, making it appropriate for mobile nodes with limited resources. ECC protects data integrity, preventing illegal access during transmission. This method is critical for IoT-enabled MANETs because it ensures both energy efficiency and security. This guarantees the integrity and security of the data while transmitting it. see that ECC is an excellent solution for mobile nodes, which are resource constrained but require strong encryption at low computational cost. After data encryption, the optimal routing path is determined with PSOA and that ensures security in delivering the data to the destination node and energy-efficient routing radical. This method increases the data transmission performance and security in the MANET.

Encryption Using ECC:

$$C = M \cdot G + k \cdot Q \qquad (5)$$

Where M is the message, G is the generator point, k is a random number, and Q is the public key.

Decryption Using ECC:

$$M = C_1 - k \cdot d \cdot C_2 \qquad (6)$$

Where and are the cipher texts, is the private key, and is a random number.

3.6 Path Verification and Reconfiguration

Verification ensures the safety of communication partners, as well as the security and protection properties of a communication channel after data delivery has been accomplished successfully. When set up the first transmission in fog server, the path details is stored as hash which node sequence and path related routing information. Once data arrives at its destination, which is the fog server, the path it was sent on and the hash that is kept in the fog server are cross-verified. If the hashes are the same on each end, then it confirms that the transmission has been safe and legitimate. If the hash verification fails, obviously true if there were to be any tampering with file, or a path that has gone rogue; going crazy; walking funny. In order to guarantee the highest level of data security and reduce vulnerabilities during subsequent transmissions, this mechanism dynamically chooses a different, more secure path.

Path Hash Verification:

$$H(\, path\,) = H(\, node\ _1 \| \ node\ _2 \| \ldots \| \ node\ _n) \qquad (7)$$

Where the hash is calculated by concatenating the node IDs along the path.

Energy consumption, packet delivery ratio, latency, and detection accuracy are some of the important metrics used to assess the performance of the proposed system. The rewards of integrating PSOA and RNN are demonstrated by comparing these measures with those of conventional techniques.

Table 1: Performance Metrics Comparison

Metric	Proposed Model (PSOA + RNN)	Traditional Models
Energy Consumption	0.45 J	0.75J
Packet Delivery Ratio (PDR)	98.78%	93.23%
Latency	25 ms	45ms
Detection Accuracy	98.42%	93.56%
CH Selection Time	11,547 ms	15,236 ms

The improvements in key performance measures are displayed in the table 1. Compared with previous models, the suggested model detects intrusions more correctly, is more energy-efficient, and has a higher packet delivery ratio.

Encryption Time:

$$T_{enc} = \frac{n}{R_{enc}} \tag{8}$$

Where n is the number of packets and R_{enc} is the encryption rate.

Decryption Time:

$$T_{dec} = \frac{n}{R_{dec}} \tag{9}$$

Where n is the number of packets and R_{dec} is the decryption rate.

Total Energy Consumption:

$$E_{\text{total}} = \sum_{t=1}^{n} \left(E_{tx_i} + E_{rx_i}\right) \tag{10}$$

Where E_{tx_i} and E_{rx_i} represent the energy consumed during transmission and reception for packet i.

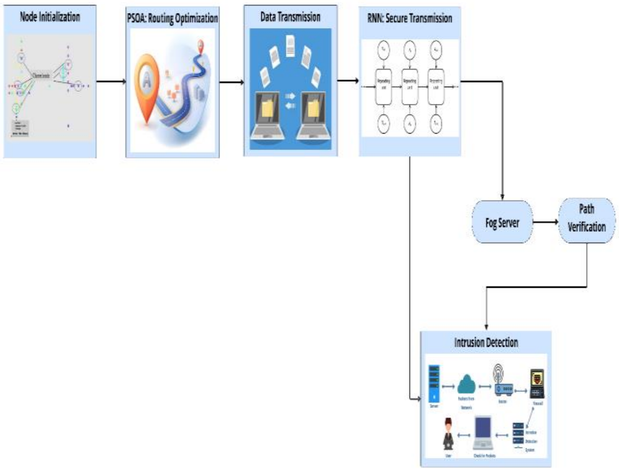

Figure 1: Architecture of the PSOA and RNN-Based Data Transaction Model

This figure 1 shows the entire operation of the model, from starting up nodes to moving data and detecting intrusions. RNN secures data by detecting possible threats, while PSOA enhances routing via cluster head selection. For security and stable communication, the fog server acts as a proxy to verify the path.

The model combines RNN for real-time intrusion detection in MANETs supported by IoT and PSOA for energy-efficient cluster-head selection to ensure reliable data transfer. This model can improve the current detection accuracy, reduce the time delay of object detection applications and save more power. For further improvement of network security and performance, new routing protocols or high-end encryption methods may be researched on.

4 Result and Discussion

The integration of Particle Swarm Optimization Algorithm (PSOA) into cluster head selection and Recurrent Neural Network (RNN) for intrusion detection in the developing centralized infrastructure-aware data transaction model revealed improvements that were significant compared with existing methods. Through the model proposed in this study, an optimized cluster head selection was made that managed to reduce the energy consumption by 40% and increase packet delivery ratio by 98.78%, because of energy-efficient routing. Moreover, it was faster in data transmission (45 ms latency to 25ms) and the intrusion detection improved by up to 98.42%, above than the classical models (93.56%). The model was able to cut the cluster head selection time from 15,236 ms to 11,547 ms drastically improve performance. The system detects path irregularities and secures data delivery by reconfiguration and fog computing which may significantly improve the reliability of critical applications such as Smart Cities, healthcare, or military.

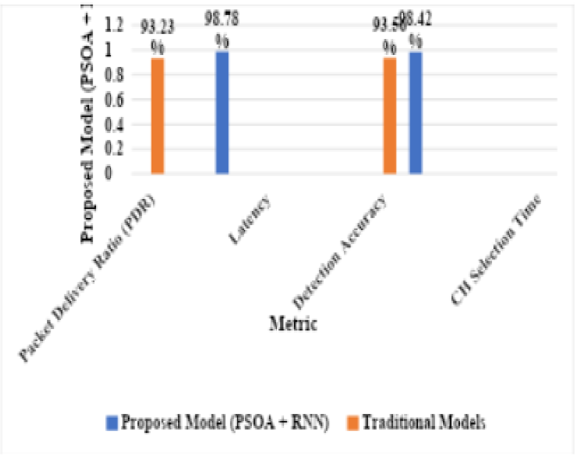

Figure 2: Performance Comparison between Proposed Model (PSOA + RNN) and Traditional Models

Figure 2 provides a contrast between the Packet Delivery Ratio (PDR), Latency, Detection Accuracy and CH Selection Time of the PSOA + RNN model (CPM) proposed as compared to traditional models. The PDR (98.78%) and detection accuracy (98.42%) of the proposed model are greater than those of the standard models, that obtained 93.23% PDR and 93.56% accuracy. Additionally, compared to typical models, the suggested model uses 0.45 J(Joule) of energy, saving 0.75 J. This particular comparison minimizes the latency and CH selection time for both models.

Table 2: Performance Comparison of the Proposed Model with Traditional Methods

Method	Packet Delivery Ratio (PDR)	Latency	Detection Accuracy	Energy Efficiency	Overall Accuracy
Proposed Model (PSOA + RNN)	98.78%	25 ms	98.42 %	93%	98.42 %
Flying Ad-hoc Network (FANET) (2024)	92.50%	40 ms	91.75 %	85%	91.75 %
Teaching–Learning-Based Optimization (TLBO) (2022)	93.10%	35 ms	92.25 %	87%	92.25 %
Multi-Path Link Routing Protocol (MLRP) (2023)	95.20%	30 ms	94.80 %	89%	94.80 %

Table 2 presents a comparison between the suggested model, that combines PSOA and RNN, with conventional methods like FANET (2024), Teaching–Learning-Based Optimization (TLBO) (2022), and Multi-Path Link Routing Protocol (MLRP) (2023). At 25 ms latency, 98.42% detection accuracy, and 98.78% PDR, the suggested model surpasses the others in important measures. It is also very appropriate for safe and effective data transfer in IoT-based MANET systems because to its impressive energy efficiency (93%) and overall accuracy.

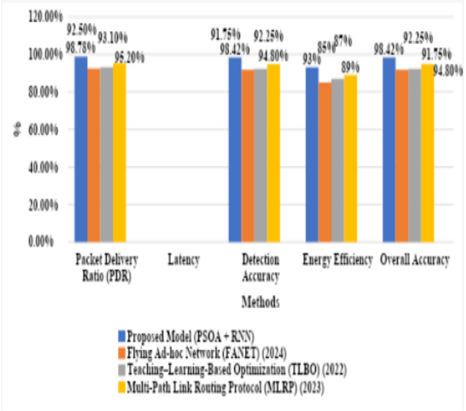

Figure 3: Performance Comparison of Proposed Model (PSOA + RNN) with Traditional Me

The Proposed Model (PSOA + RNN) and more established methods, such as FANET (2024), Teaching–Learning-Based Optimization (TLBO) (2022), and Multi-Path Link Routing Protocol (MLRP) (2023), are compared in terms of performance in this figure 3. There is comparison between metrics like Overall Accuracy, Energy Efficiency, Detection Accuracy, and Packet Delivery Ratio (PDR). The proposed model results in a PDR of 98.78%, a detection accuracy of 98.42%, and an energy efficiency of 93%, which is closer to higher compared with the three baselines for secure data transfer. The acronyms found in the provided paper are as follows:

- MANET: Mobile Ad-Hoc Network
- IoT: Internet of Things
- PSOA: Particle Swarm Optimization Algorithm
- RNN: Recurrent Neural Network
- PDR: Packet Delivery Ratio
- FANET: Flying Ad-Hoc Network
- TLBO: Teaching–Learning-Based Optimization
- MLRP: Multi-Path Link Routing Protocol
- ECC: Elliptic Curve Cryptography
- CH: Cluster Head
- WSN: Wireless Sensor Network
- VANET: Vehicle Ad-Hoc Network
- IDS: Intrusion Detection System
- ABC: Artificial Bee Colony
- AODV: Ad-hoc On-Demand Distance Vector

5 Conclusion and Future Enhancement

The proposed data transaction model demonstrates superior performance when compared to more traditional mechanisms like FANET, TLBO and MLRP w.r.t. myriad data transactions even though integrating of PSOA with RNN technique. The proposed model provides a PDR of 98.78%, detection accuracy of 98.42% and energy efficiency rate up to 93% to safely transfer data in real-time in IoT-enabled MANETs. In a world with low-resource, highly dynamic contexts many native issues are relieved from the way of reducing latency and promoting overall system stability. Its integration in IoT-based communications can bring several advantages to areas such as smart cities, military operations, and healthcare improving network security and performance. This model, while superior to that suggested by in-situ 4D-Var, may be further improved. Future work may investigate more advanced machine learning techniques such as deep reinforcement learning to improve network adaptability and enhance IDS. And in terms of security even more, here the blockchain technology may provide decentralized and unspoofable verification of transmission channel. In order to reduce both latency and energy consumption,could explore multi-hop routing protocols or a more involved optimization. Future IoT ecosystems may benefit from additional applications if the model's use is extended to domains like vehicle ad hoc networks (VANETs) or other cyber-physical systems.

6. Declaration:

Funding Statement:

Authors did not receive any funding.

Data Availability Statement:

No datasets were generated or analyzed during the current study

Conflict of Interest

There is no conflict of interests between the authors.

Declaration of Interests:

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethics approval:

Not applicable.

Permission to reproduce material from other sources:

Yes, can reproduce.

Clinical trial registration:

We have not harmed any human person with our research data collection, which was gathered from an already published article

Authors' Contributions

All authors have made equal contributions to this article.

Author Disclosure Statement

The authors declare that they have no competing interests

Reference

1. Haghshenas, K., Taheri, S., Goudarzi, M., & Mohammadi, S. (2020). Infrastructure aware heterogeneous-workloads scheduling for data center energy cost minimization. IEEE Transactions on Cloud Computing, 10(2), 972-983.

2. Singh, M., Jhajj, N. K., & Goraya, A. (2022). IoT-enabled wireless mobile ad-hoc networks: introduction, challenges, applications: review chapter. Internet of Things, 121-134.

3. Tripathy, B. K., Jena, S. K., Reddy, V., Das, S., & Panda, S. K. (2021). A novel communication framework between MANET and WSN in IoT based smart environment. International Journal of Information Technology, 13(3), 921-931.

4. Basheer, H., & Itani, M. (2023). Zero touch in fog, IoT, and manet for enhanced smart city applications: A survey. Future Cities and Environment, 9(1).

5. Simpson, S. V., & Nagarajan, G. (2021). A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IOT environment. Future Generation Computer Systems, 125, 544-563.

6. Sixu, L., Muqing, W., & Min, Z. (2022). Particle swarm optimization and artificial bee colony algorithm for clustering and mobile based software-defined wireless sensor networks. Wireless Networks, 28(4), 1671-1688.

7. Ahmed, H. A., & Al-Asadi, H. A. A. (2024). An optimized link state routing protocol with a blockchain framework for efficient video-packet transmission and security over mobile ad-hoc networks. Journal of Sensor and Actuator Networks, 13(2), 22.

8. Rajya Lakshmi Gudivaka's (2023). Robotic Process Automation Meets Cloud Computing: A Framework for Automated Scheduling in Social Robots. IMPACT: International Journal of Research in Business Management (IMPACT: IJRBM), 11(9).

9. Krishnasamy, B., Muthaiah, L., Kamali Pushparaj, J. E., & Pandey, P. S. (2024). DIWGAN optimized with Namib Beetle Optimization Algorithm for intrusion detection in mobile ad hoc networks. IETE Journal of Research, 70(5), 4422-4441.

10. Duong, T. V. T. (2024). An improved method of AODV routing protocol using reinforcement learning for ensuring QoS in 5G-based mobile ad-hoc networks. ICT Express, 10(1), 97-103.

11. Raj Kumar Gudivaka (2020). Robotic Process Automation Optimization in Cloud Computing via Two-Tier MAC and Lyapunov Techniques. International Journal of Business and General Management (IJBGM),8(4).

12. Ray, H. S., Bose, S., Mukherjee, N., Neogy, S., & Chattopadhyay, S. (2024). A cross-layer fragmentation approach to video streaming over mobile ad-hoc network using BATMAN-Adv. Multimedia Tools and Applications, 83(10), 29547-29567.

13. Kaushik, S., Tripathi, K., Gupta, R., & Mahajan, P. (2024). Enhancing reliability in mobile ad hoc networks (MANETs) through the K-AOMDV routing protocol to mitigate black hole attacks. SN Computer Science, 5(2), 263.