IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 6, December 2026, pp. 5755~5763
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i6.pp5755-5763

An intelligent deep learning-driven multicast routing protocol for emergency-aware internet of things

Rashmi Shivaswamy[1], Naveen Lingaraju[2], M. Dhanalakshmi[3], Nandini G.[4]
[1]School of Computer Science and Engineering, RV University, Bengaluru, India
[2]Department of Computer Science and Engineering (Data Science), RNS Institute of Technology, Bengaluru, India
[3]Department of Computer Science and Engineering, New Horizon College of Engineering, Bengaluru, India
[4]Department of Computer Science and Engineering, BNM Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Jun 10, 2025
Revised Aug 22, 2026
Accepted Sep 20, 2026

Keywords:

Deep learning
Emergency
Intelligence
Internet of things
Multicast routing

ABSTRACT

There are various applications in internet of things (IoT) that demand highly reliable and timely delivery of critical data. Such an emergency event could arise for various reasons, e.g., health crises, gas leaks, and fires. Conventional multicast routing principles often treat the routing data equally, as they significantly lack any form of intelligence in a dynamic environment. Hence, this paper presents a novel multicast routing scheme that is capable of identifying an emergency event among emergencies by harnessing a deep learning model. Different from existing multicast routing schemes, the proposed scheme facilitates reclassification of priority nodes once the abnormal behavior of an IoT node is detected. This forms a multicast tree with real-time updates for facilitating efficient routing performance. The study outcome shows that the proposed scheme offers 25% enhanced data delivery in emergency conditions, 95% accuracy in detecting emergency conditions, 17% reduced delay, and 15% increased throughput.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Rashmi Shivaswamy
School of Computer Science and Engineering, RV University
Bengaluru, Karnataka 560059, India
Email: rashmineha.s@gmail.com

1. INTRODUCTION

A communication method termed multicast routing makes it possible for data to be effectively sent from one sender to numerous recipients at once. Multicast routing is essential to the internet of things (IoT) because it allows collaborative communication between devices like sensors as well as actuators, which frequently need to receive the same information or orders simultaneously [1]. This method is particularly useful in massive amounts or restricted in resources IoT networks since it saves bandwidth, lowers energy usage, and enhances scalability [2]. It is especially crucial in applications where fast and coordinated data distribution is essential, such as industrial automation, smart cities, and responses to emergencies. It makes it possible for public safety alerts, ecological monitoring data, and traffic updates to be efficiently distributed to numerous devices at once in smart cities. Multicast facilitates synchronized operation of sensors and machines in manufacturing automation, improving process synchronization and cutting down on latencies [3]. It enables the real-time distribution of vital information for rescue teams, healthcare units, and general communication networks during emergencies, including natural disasters.

When transmitting data in a critical situation, multicast routing in the IoT confronts a number of difficulties. First, frequent route breakdowns and erratic communication might result from network instability brought on by the movement of nodes, destruction, or overcrowding [4]. Second, standard multicast methods

might not ensure real-time data delivery, even though latency awareness is crucial in emergencies. Third, complicated multicast topologies are challenging to maintain due to resource limitations in IoT devices, such as restricted battery, memory, and processor power. Fourth, during crises, the number of devices and information packets rapidly grows, raising concerns about sustainability [5]. Last but not least, security and reliability of data are essential since leaked data during a crisis can have major repercussions [6]–[8]. However, protecting multicast transmissions without increasing overhead is still difficult.

Deep learning is especially well-suited to solving some of the multicast routing problems in the IoT [9]. Node movement, traffic spikes, and emergency breakdowns are examples of dynamic network circumstances that are difficult for traditional protocols to forecast. Deep learning helps overcome these difficulties by identifying temporal and spatial trends in previous data. Rule-based methods struggle to optimize routes in real-time in huge, complicated, and unpredictable networks; models based on deep learning, on the other hand, can automatically choose the best routes with little assistance from humans [10]. Furthermore, traditional techniques frequently fail to detect anomalies or malicious activity in multicast traffic, while deep learning may spot subtle, non-linear patterns that point to security risks.

There are various related works associated with the multicast routing scheme. Existing studies have witnessed the adoption of a standard multicast routing scheme known as multicast ad hoc on-demand vector (MAODV) that uses a tree-structured approach for performing data transmission (Pramitarini *et al.* [11], Farooq *et al.* [12], Chavan and Venkataram [13]). MAODV offers efficient bandwidth usage; however, it has higher control overhead due to frequent discovery of routes in IoT. The existing system has also witnessed the adoption of the on-demand multicast routing protocol (ODMRP) that uses a mesh scheme for dynamic routing, adopting a periodic flooding mechanism. This scheme has been noted in work carried out by Mohammadi [14], Park *et al.* [15], and Benazer *et al.* [16]. ODMRP offers increased robustness and reliability; however, its mechanism of periodic flooding maximizes the control overhead while transmitting data in large IoT networks.

Most recently, the adoption of deep learning-based architectures has been increasingly used towards enhancing data transmission in IoT. In this regard, a convolutional neural network (CNN) is used for optimizing the decision for routing by investigating patterns of the network, followed by predicting the multicast path with higher efficiency. The work carried out by various researchers (e.g. Chen *et al.* [17], Sagu *et al.* [18], Ding *et al.* [19], and Hussein *et al.* [20]) is proven to improve routing efficiency right from network behavior that contributes towards formulating intelligent decisions; however, potential computational resources are demanded for this purpose along with voluminous data for training. Similar to CNN, various existing researchers (Liu *et al.* [21], Albishari *et al.* [22], Gupta *et al.* [23]) have also experimented with gated recurrent unit (GRU) that assists in acquiring routing pattern with time dependency cost effectively; however, increased memory and processing power dependency becomes its prime shortcomings. Multi-layer perceptron (MLP) is also reported by authors Isabona *et al.* [24]) to assist in multicast data transmission, where a feedforward neural network is used for identifying the optimal routing path. MLP can significantly assist in enhancing the accuracy of path selection; however, it also suffers from significant computational resources and training data, hence unsuitable for lightweight devices in IoT.

The identified research problem is briefed as follows: during emergencies, existing multicast routing methods frequently have trouble sustaining dependable communication in extremely dynamic and resource-constrained IoT contexts. Many protocols are unable to adjust in real time to abrupt changes in topology or network congestion brought on by emergencies. Because ongoing route maintenance can rapidly deplete the batteries of IoT devices, conserving energy is a key concern. Furthermore, delivering data securely and with little latency in urgent circumstances continues to be a major research challenge.

The study aims to introduce a novel multicast routing scheme for facilitating data transmission in the dynamic environment of an IoT during emergency conditions as an extension to prior work [25]. The value-added contribution of the study are as follows: i) the model is capable of identifying the state of regularity and emergency using deep learning model that assists in prioritizing emergency information, ii) the study introduces an adaptive multicast routing integrated with deep learning for facilitating emergency data transmission with minimal latency and routing with context awareness, iii) the presented model is design to perfectly keep a balance in network performance as well as deep learning model performance, and iv) the introduced framework not only identify the state of emergency but also act according in different situation thereby making it scalable, robust, and yet cost-effective intelligent multicast routing.

2. METHOD

The goal of the proposed system is to design an innovative computational framework towards presenting an intelligent multicast routing scheme considering IoT as a use case. The architecture of the framework is shown in Figure 1, which is meant to identify the emergency conditions associated with

real-time applications. The study uses long short-term memory (LSTM) for this purpose. The model also assists in prioritizing the data transmission associated with the emergency information over the normal IoT traffic system for facilitating speedy data delivery operation more reliably during critical circumstances. The architecture also contributes towards controlling routing overhead with minimal score while adapting to the dynamic environment of the IoT network. This section presents detailed information about the core modules involved in the proposed architecture in Figure 1.

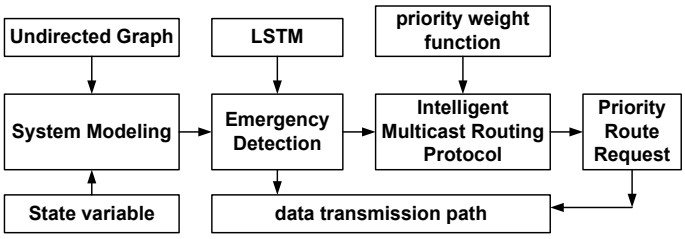


Figure 1. Architecture of proposed system

2.1. System modelling

This is the first module of the proposed study that aims to represent the network structure and IoT environment, encapsulating the dynamic behavior of IoT nodes. The proposed system uses a connected undirected graph G to model IoT networks as $G\ (V, E)$, where E and V represent edges and vertices. The edges E are represented as $E = \{(v_i, v_j) \in V \times V : d_{ij} \leq R\}$ and vertices V are represented as $V = \{v_1, v_2, \ldots, v_n\}$ where n depicts the set of IoT sensors, d_{ij} depicts the spatial distance between two IoT sensor nodes v_i and v_j, and the communication range is depicted by R. The scheme entails the use of state variables for each v_i IoT node as shown in (1).

$$s_i(t) \in \{0,1\}\ where \begin{cases} s_i(t) = 0 & when\ IoT\ node\ is\ in\ normal\ state\ at\ t - time \\ s_i(t) = 1 & when\ IoT\ node\ is\ in\ emergency\ state\ at\ t - time \end{cases} \quad (1)$$

It can be noted that the proposed system considers the heterogeneous IoT nodes for forming a wireless IoT network that are randomly distributed in a specific deployment area. The environmental parameters are consistently monitored by each IoT node, which further yields data packets to the central sink node adopting multicast routing. The study also uses multivariate time series to represent the sensory readings at τ for each IoT node as (2).

$$X_i^\tau = \{x_i^1, x_i^2, \ldots, x_i^\tau\}, x_i^\tau \in R^m \quad (2)$$

The proposed study framework uses dynamic environmental changes, energy constraints, and node mobility. Now it is feasible for the IoT nodes to carry out a transition between two states of normal and emergency. It is dependent on subsequent classification and sensed data using a deep learning module. In (2), the computation of the sensory reading depends upon the number of m types of sensors and x_i^τ As a sensor vector at the *t*-th time. Different from the conventional static network model that considers all traffic flows of data and IoT nodes equally, the proposed system distinguishes them on the basis of the classification state of emergency. This operation facilitates adaptive behavior of the network for providing dynamic prioritization of critical data. This module contributes towards modelling states of IoT nodes along with understanding their impact on network behavior.

2.2. Emergency detection using deep learning

This is the second module of implementation that aims to determine emergency conditions originating from raw sensor data that prompts the routing scheme to emphasize critical data transmission. The study uses an LSTM network for extracting information related to temporal dependencies present within IoT traffic data. The input sliding windows associated with readings of multiple sensors (e.g., gas concentration and temperature) are fed to the LSTM, followed by generating a binary classification as the outcome. This output depicts either the absence or presence of an emergency condition of an IoT node. The study uses an LSTM network for classifying the $s_i(t)$ state of an IoT node that is subjected to training to perform a binary classification. The function *f* for this purpose is mathematically represented as (3).

$$f_\theta = X_i^\tau \longrightarrow \hat{s}_i(t) \epsilon \{0,1\} \quad (3)$$

In (3), the variable f_θ represents an LSTM framework where the θ weight is used for parameterizing the model. A labelled dataset is used to train the model offline. Different from conventional anomaly detection schemes using a threshold in IoT, the proposed system uses LSTM for learning the subtle alterations in the environment and sophisticated temporal patterns. The window of the input sequence is represented as X_i^τ For the *i*-th node, the predicted state is represented as $\hat{s}_i(t)$ at *t*-th time. The operation carried out by LSTM towards processing the sequence is as shown in expression (4).

$$ht = LSTM(xt, ht-1;\ \theta) \quad (4)$$

Expression (4) contributes to early and precise detection of the emergency state. It also contributes to the minimization of false alarms that are essential for retaining maximum network efficiency. To perform binary classification, a sigmoid function is implemented on the outcome as exhibited in expression (5). Apart from this, the system uses a loss function while performing the training operation, as exhibited in (6).

$$\hat{s}_i(t)\sigma(Wh_\tau + b), where\ \sigma = 1/(1+e^{-z}) \quad (5)$$

$$L(\theta) = \frac{1}{N}\sum_{i=1}^{N} s_i.\log(\hat{s}_i) + (1-s_i).\log(1-\hat{s}_i) \quad (6)$$

In (6), the training samples are denoted by N. The proposed system combines a deep learning-based method within the IoT network for facilitating the layer of data transmission for dynamically fine-tuning priorities on the basis of event classification reliably. This approach also contributes towards improving the emergency responsiveness and situational awareness of IoT nodes, unlike conventional schemes.

2.3. Intelligent multicast routing protocol

This is the final module of implementation, which is responsible for facilitating the transmission of emergency data at reduced latency in the IoT network. It is done dynamically for fine-tuning the multicast routing as per the state of the IoT node's emergency. Consider T to represent a tree for multicast routing where $T = (VT, ET)$ and is a subset of graph *G*. The system adjusts the tree dynamically in accordance with the state vector $s(t) = [s1(t), s2(t), \ldots, sn(t)]$ while the priority weight function for each IoT node is represented as (7).

$$w_i(t) = \begin{cases} \alpha & if\ s_i(t) = 1(emergency) \\ \beta & if\ s_i(t) = 1(normal) \end{cases}, \alpha > \beta > 0 \quad (7)$$

The study initially constructs a foundation for multicast routing, followed by introducing a new form of data transmission scheme with emergency awareness. The deep learning module classifies the emergency sources of IoT nodes, starting to forward priority-based route requests. A distinct multicast tree is maintained by the protocol towards regular and emergency forms of an IoT traffic system. The system optimizes the data transmission path for emergency data with reduced delay and reduced number of hops, while regular dynamic updating is carried out for the routing table once the system witnesses a node to change its state. The study also uses selective packet duplication and prioritized queuing in order to ensure proper data delivery. It is to be noted that the routing protocol targets towards creating a multicast tree T with minimal weight that gives more importance to an IoT node with increased weight $w_i(t)$. The mathematical representation of this multicast tree T is as in (8).

$$T*(t) = \arg \min_{T \subseteq G} \sum_{(v_i,v_j)\in E_\tau} c_{ij}.\left(\frac{1}{w_i(t)} + \frac{1}{w_j(t)}\right) \quad (8)$$

In expression (8), the delay or the cost of communication on the edge (v_i, v_j) is represented as c_{ij}. While $T*(t)$ represents the optimal routing tree at the *t*-th time. In the event of detection of an emergency node, the system activates a priority route request (PREQ), which either takes the value of 1 if $s_i(t)$ and $s_i(t-1)$ are equivalent to 1 and 0, respectively, or otherwise, it takes the value of 0. This operation renders the updating of the data transmission path for the vertices $\hat{v}_i \epsilon V_T$ .Where the value of state $s_i(t)$ is equivalent to 1. This significantly assists in reducing the delay D_i, which is computed as (9).

$$D_i = \sum_{(v_i,v_j)\in P_i} d_{jk} \quad (9)$$

In (9), the variable P_i represents the data transmission path leading to the sink node from the origination point of v_i. Different from conventional multicast schemes that don't possess context awareness and consider all data equivalently, the proposed system uses emergency classification, intellectually adapting routing structures on the go. It also reduces control overhead by restricting route updates only to nodes assigned with priority, something that is not noted in any conventional multicast routing scheme.

3. RESULTS AND DISCUSSION

3.1. Results

The implementation of the proposed system is carried out considering 50-100 nodes deployed in a 1,000 × 1,000 m^2 simulation area with random waypoint with 300 s of simulation time. Multicast constant bit rate (CBR) has been used for a traffic type with a 512-byte packet. The complete analysis of the outcome is carried out from two perspectives, viz., assessing network-level performance and deep learning model evaluation. The assessment is carried out using the gas sensor array drift dataset [26], which consists of timestamped sensory readings from 16 chemical sensors that are meant to capture information on heterogeneous gas concentration under different environmental conditions. This dataset is usually considered for studying anomaly detection and gas classification in IoT-based sensor networks, which makes it highly suitable for studying emergency detection in IoT.

3.1.1. Network-level assessment

The proposed system undergoes network-level assessment by comparing itself with the standard routing scheme of MAODV and ODMRP while maintaining a similar test environment. A latest hybrid routing protocol (hybrid energy-aware adaptive routing (HEAR 2024)) has also been compared, which is known for its adaptive and energy-aware routing scheme [27]. The assessment is carried out considering throughput, end-to-end delay, and routing overhead as the performance metrics. A simulation is carried out considering 100 IoT nodes, while 10% of these IoT nodes are assigned randomly to an emergency state. The observed numerical values are shown in Table 1. The outcome in Table 1 showcases that the proposed model has accomplished approximately 15% increased throughput in contrast to MAODV, along with 17% minimized delay. The outcome also shows minimized overhead on routing due to selective priority-based routing and the adaptive updating process of routes.

Table 1. Network level assessment of routing protocols

Protocol	Throughput (kbps)	End-to-end delay (ms)	Routing overhead (%)	Statistical significance vs the proposed
MAODV	185.2	112.6	23.4	$p < 0.01$
ODMRP	178.7	124.3	25.1	$p < 0.01$
HEAR 2024	198	101.5	20.2	$p < 0.05$
Proposed system	213.5	89.4	17.6	-

3.1.2. Deep learning model evaluation

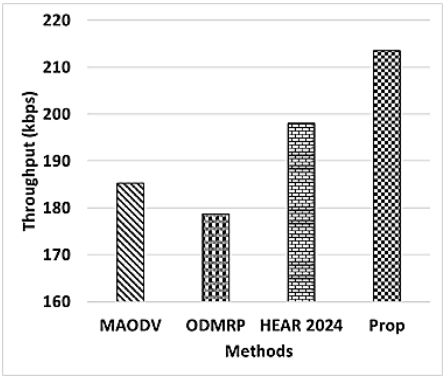
The study assesses the LSTM module for gauging its effectiveness during an emergency. For this purpose, the proposed model has been compared with frequently used deep learning models adopted for anomaly detection, viz. GRU, CNN, MLP. A similar dataset with time-series sensory features has been used for testing the model for unseen scenarios of emergencies. Table 2 showcases the numerical table where accuracy, training time, and response time have been assessed to testify to the effectiveness of the deep learning model. The trend of numerical outcomes from Table 2 showcases that the based model in proposed system achieves the maximum accuracy score (acc = 95.4%), followed by a highly reduced response time (res = 9.3s). This outcome is found to be quite appropriate for the detection task of real-time emergencies. Further, a competitive training time is observed for the proposed system, excelling much better in contrast to GRU and CNN. The enhancement in the network layer in IoT in the proposed system is due to route reconfiguration with emergency awareness and adaptive prioritization.

Table 2. Assessment of deep learning model

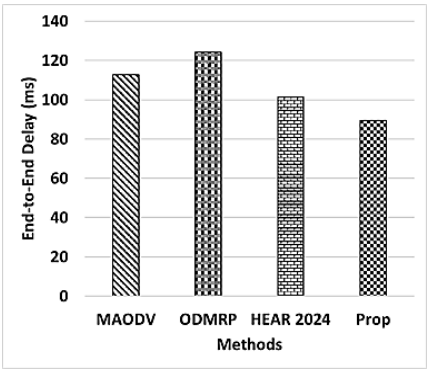
Model	Accuracy (%)	Training time (s)	Response time (ms)
CNN	91.3	52.1	14.8
GRU	92.7	48.9	13.2
MLP	89.6	41.3	11.7
Proposed (LSTM)	95.4	46.7	9.3

3.2. Discussion

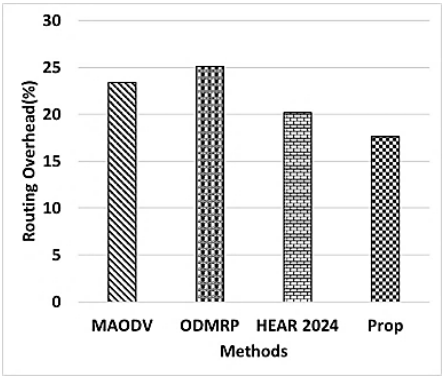
From the perspective of network-level assessment (Figure 2), it can be noted that conventional multicast routing schemes of ODMRP and MAODV underperform consistently in contrast to the proposed model. This is mainly because of the identification capability of the proposed scheme in dynamic conditions, while the affected nodes are prioritized by reconfiguring the multicast tree, offering higher throughput (Figure 2(a)). Further, adoption of LSTM offers faster and more reliable detection of emergency conditions, which significantly controls the overhead (Figure 2(b)) and delay (Figure 2(c)). Figure 3 show the outcome shows that the proposed model accomplishes a significantly increased throughput of around 7.6% higher, as well as offers 11.9% reduced delay in contrast to HEAR 2024. The proposed system also records higher accuracy (Figure 3(a)), minimized training time (Figure 3(b)), and reduced response time (Figure 3(c)). This will eventually mean that deep learning model inclusion doesn't increase the computational complexity while performing data transmission in both normal and emergency states.



(a)

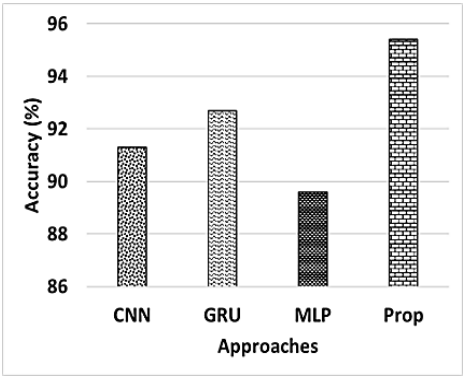


(b)

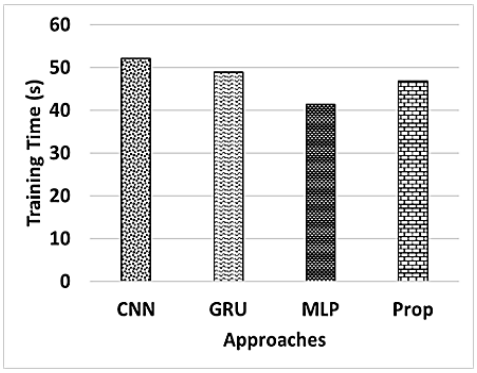


(c)

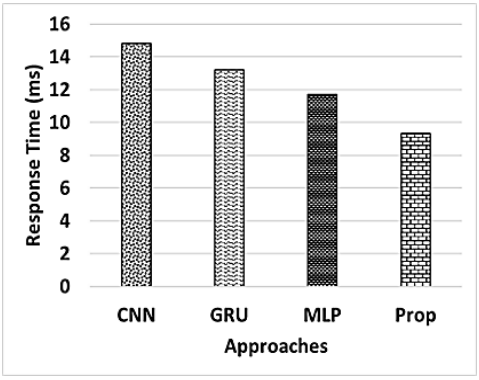
Figure 2. Graphical outcome for network-level assessment: (a) throughput, (b) end-to-end delay, and (c) routing overhead



(a)



(b)



(c)

Figure 3. Graphical outcome for deep learning model evaluation: (a) accuracy, (b) training time, and (c) response time

On the contrary, CNN, GRU, and MLP still lag slightly behind the proposed scheme in this regard. Apart from this, the proposed scheme permits adjustment of routing regularly, integrating adaptive communication using modified multicast routing and deep learning. Further, the network is never overwhelmed with unnecessary control packets when it performs selective prioritization, which is not observed in conventional schemes of multicast routing.

4. CONCLUSION

The current paper has presented a deep learning-based multicast routing scheme that is capable of performing data transmission during the time of emergency in an IoT environment. The novel accomplishment of this work is i) a dual-layer framework is designed integrating adaptive multicast routing with a deep learning model, ii) a novel routing strategy with emergency awareness is presented for potentially enhancing transmission of critical information alongside minimal overhead retention, iii) a highly responsive and scalable system design has been presented with optimal multicasting routing performance in IoT. The future work of this work will be towards incorporating multiple types of emergency conditions to model more complicated environments in IoT. The idea will be to adopt federated learning to construct another version of intelligent multicast routing in IoT.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Rashmi Shivaswamy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	
Naveen Lingaraju		✓			✓	✓	✓	✓	✓	✓	✓	✓		
M. Dhanalakshmi	✓		✓	✓			✓			✓	✓		✓	✓
Nandini G.		✓		✓	✓		✓	✓	✓	✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [RS], upon reasonable request.

REFERENCES

[1] I. E. Lakhlef, B. Djamaa, and M. R. Senouci, "A comprehensive study of multicast routing protocols in the internet of things," in *Artificial Intelligence and Its Applications (AIAP 2021)*, 2022, pp. 325–335, doi: 10.1007/978-3-030-96311-8_30.

[2] Y. Rbah *et al.*, "Hybrid software-defined network-based deep learning framework for enhancing internet of medical things cybersecurity," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 3, pp. 3599–3610, 2024, doi: 10.11591/ijai.v13.i3.pp3599-3610.

[3] D. Careglio, F. Agraz, and D. Papadimitriou, "A multicast routing scheme for the internet: simulation and experimentation in large-scale networks," *Applied Sciences*, vol. 11, no. 18, 2021, doi: 10.3390/app11188645.

[4] F. Li, "Improving the efficiency of network controllability processes on temporal networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 3, 2024, doi: 10.1016/j.jksuci.2024.101976.

[5] S. Ding, H. Ward, and A. Tukker, "How internet of things can influence the sustainability performance of logistics industries – a Chinese case study," *Cleaner Logistics and Supply Chain*, vol. 6, 2023, doi: 10.1016/j.clscn.2023.100094.

[6] R. Mishra and A. Mishra, "Current research on internet of things (IoT) security protocols: a survey," *Computers and Security*, vol. 151, 2025, doi: 10.1016/j.cose.2024.104310.
[7] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 167–185, 2024, doi: 10.1016/j.iotcps.2023.12.003.
[8] Y. Na *et al.*, "Enhancing the reliability of IoT data marketplaces through security validation of IoT devices," in *Proceedings - 16th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2020*, 2020, pp. 265–272, doi: 10.1109/DCOSS49796.2020.00050.
[9] M. V. Sudhakar, P. R. Reddy, U. Penchalaiah, and P. R. Reddy, "A deep learning based latency aware predictive routing model for network-on-chip architectures," *International Journal of Communication Systems*, vol. 36, no. 17, 2023, doi: 10.1002/dac.5602.
[10] Z. Ke, Q. Zou, J. Liu, and S. Qian, "Real-time system optimal traffic routing under uncertainties — can physics models boost reinforcement learning?," *Transportation Research Part C: Emerging Technologies*, vol. 173, 2025, doi: 10.1016/j.trc.2025.105040.
[11] Y. Pramitarini, R. H. Y. Perdana, K. Shim, and B. An, "DLSMR: deep learning-based secure multicast routing protocol against wormhole attack in flying ad hoc networks with cell-free massive multiple-input multiple-output †," *Sensors*, vol. 23, no. 18, 2023, doi: 10.3390/s23187960.
[12] W. Farooq, S. U. Islam, M. A. Khan, S. Rehman, U. A. Gulzari, and J. Boudjadar, "UGAVs-MDVR: a cluster-based multicast routing protocol for unmanned ground and aerial vehicles communication in VANET," *Applied Sciences*, vol. 12, no. 23, 2022, doi: 10.3390/app122311995.
[13] C. P. Chavan and P. Venkataram, "Design and implementation of event-based multicast AODV routing protocol for ubiquitous network," *Array*, vol. 14, 2022, doi: 10.1016/j.array.2022.100129.
[14] R. Mohammadi, "Multicast reliable traffic engineering technique for SDN-Fog based IoUT," *Scientific Reports*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-93383-w.
[15] C. Park, S. Lee, H. Joo, and H. Kim, "Empowering adaptive geolocation-based routing for UAV networks with reinforcement learning," *Drones*, vol. 7, no. 6, 2023, doi: 10.3390/drones7060387.
[16] S. S. Benazer, M. S. Dawood, G. Suganya, and S. K. Ramanatha, "Performance analysis of modified on-demand multicast routing protocol for MANET using non-forwarding nodes," *Materials Today: Proceedings*, vol. 45, pp. 2603–2605, 2021, doi: 10.1016/j.matpr.2020.11.342.
[17] H. Chen, D. Liu, S. Li, S. Huai, X. Luo, and W. Liu, "MUGNoC: a software-configured multicast-unicast-gather NoC for accelerating CNN dataflows," in *Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC*, 2023, pp. 308–313, doi: 10.1145/3566097.3567846.
[18] A. Sagu, N. S. Gill, P. Gulia, N. Alduaiji, P. K. Shukla, and M. A. Shah, "Advances to IoT security using a GRU-CNN deep learning model trained on SUCMO algorithm," *Scientific Reports*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-025-99574-9.
[19] C. Ding, Z. Liu, A. Zhou, J. Yu, Y. Li, and S. Wang, "A resource-efficient multiple recognition services framework for IoT devices," *IEEE Transactions on Services Computing*, vol. 18, no. 1, pp. 29–42, 2025, doi: 10.1109/TSC.2024.3512949.
[20] T. D. H. Hussein, M. Frikha, S. Ahmed, and J. Rahebi, "BA-CNN: bat algorithm-based convolutional neural network algorithm for ambulance vehicle routing in smart cities," *Mobile Information Systems*, vol. 2022, pp. 1–14, 2022, doi: 10.1155/2022/7339647.
[21] J. Liu, J. Albrethsen, L. Goh, D. Yau, and K. H. Lim, "Spatial-temporal graph representation learning for tactical networks future state prediction," in *Proceedings of the International Joint Conference on Neural Networks*, 2024, pp. 1–8, doi: 10.1109/IJCNN60899.2024.10650266.
[22] M. Albishari, M. Li, M. Ayoubi, A. Alsanabani, and J. Tian, "Federated deep learning models for detecting RPL attacks on large-scale hybrid IoT networks," *Computer Networks*, vol. 254, 2024, doi: 10.1016/j.comnet.2024.110837.
[23] B. B. Gupta, K. T. Chui, A. Gaurav, V. Arya, and P. Chaurasia, "A novel hybrid convolutional neural network- and gated recurrent unit-based paradigm for IoT network traffic attack detection in smart cities," *Sensors*, vol. 23, no. 21, 2023, doi: 10.3390/s23218686.
[24] J. Isabona *et al.*, "Development of a multilayer perception neural network for optimal predictive modeling in urban microcellular radio environments," *Applied Sciences*, vol. 12, no. 11, 2022, doi: 10.3390/app12115713.
[25] G. Nandini and J. Anitha, "Performance chronicles of multicast routing protocol in wireless sensor network," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 9, 2017, doi: 10.14569/ijacsa.2017.080941.
[26] N. Dennler, S. Rastogi, J. Fonollosa, A. V. Schaik, and M. Schmuker, "Drift in a popular metal oxide sensor dataset reveals limitations for gas classification benchmarks," *Sensors and Actuators B: Chemical*, vol. 361, Jun. 2022, doi: 10.1016/j.snb.2022.131668.
[27] J. Yang, W. Li, C. Li, L. Zhang, and L. Liu, "An energy-efficient and transmission-efficient adaptive routing algorithm using deep reinforcement learning for wireless sensor networks," *IEEE Internet of Things Journal*, vol. 12, no. 23, pp. 50414–50426, 2025, doi: 10.1109/JIOT.2025.3609624.

BIOGRAPHIES OF AUTHORS



Dr. Rashmi Shivaswamy is an academician and researcher with over two decades of experience in computer science and engineering. Currently a professor at RV University, Bengaluru, and also pursuing her postdoctoral degree at Lincoln University College, Malaysia, she has held several academic and leadership roles, including head of the Department and Chairman of Boards of Studies and Examiners at reputed institutions. She guides research scholars, authors impactful journal publications, and files patents in assistive technology and healthcare innovation. She is a recognized IEEE senior member. Her main research interests include cloud computing, cybersecurity, IoT, machine learning, and blockchain technology. She can be contacted at email: rashmineha.s@gmail.com.



Dr. Naveen Lingaraju obtained his Ph.D. in Computer Science and Engineering from VTU, and then he obtained his master's degree in Computer Science and Engineering from VTU and Bachelor's degree in Information Science and Engineering from Visvesvaraya Technological University (VTU), Belgaum, Karnataka, India. He is working as associate professor in the Department of Computer Science and Engineering (Data Science) at RNS Institute of Technology, Bengaluru. He has 14 years of total experience, including 8 years of industry experience and 6 years of teaching experience. His areas of interest are neural networks, artificial intelligence, data mining, big data, wireless sensor, and cellular networks. He has published and presented papers in journals and at international and national-level conferences. He can be contacted at email: naveenlingaraju@gmail.com.



Dr. M. Dhanalakshmi is currently serving as a professor in the Department of Computer Science and Engineering at New Horizon College of Engineering, Bengaluru. She has over 2 decades of experience in the field of computer science and engineering, serving in different roles in various academic institutions. She has also presented and published research papers in both national and international conferences and peer-reviewed journals. Her main research interests include cloud computing, cybersecurity, IoT, and machine learning. She can be contacted at email: mdhanalak72@gmail.com.



Dr. Nandini G. is currently working as an associate professor in the Department of Computer Science and Engineering at BNM Institute of Technology, Bengaluru, Karnataka, India. She received her bachelor of engineering (B.E.), master of technology (M.Tech.), and doctor of philosophy (Ph.D.) from Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India. Her research interests include wireless sensor networks, IoT, artificial intelligence, and machine learning. Actively involved in professional organizations like IEI and ISTE. She can be contacted at email: nandinig@bnmit.in.