OPEN ACCESS
Kashf Journal of Multidisciplinary Research
Vol: 03 - Issue 03 (2026)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

CLIMATE CHANGE NOTIFICATION THROUGH PRIORITY-ROUTING NETWORKS USING IOT DEVICES: A STATISTICAL FRAMEWORK FOR REAL-TIME ENVIRONMENTAL MONITORING AND EARLY WARNING

Dr Anum Ali[1], Dr Muhammad Hussain[2]
[1, 2]*Department of Computer Science, Lahore Leads University, Pakistan*
[2]*Theo Giannopoulos, GTM Consultancy, UK*

[*]***Corresponding Author:*** (dranumali.cs@leads.edu.pk)
DOI: (*https://doi.org/10.71146/kjmr985*)

Article Info

Abstract

Climate change has increased the frequency and severity of environmental hazards, including floods, droughts, heatwaves, storms, and abnormal weather conditions. Conventional environmental monitoring and communication systems may experience network congestion and delayed transmission during critical events, reducing the effectiveness of early-warning mechanisms. This paper proposes a Climate Change Notification through Statistical Priority-Routing IoT Devices (CCN-PRIoT) framework for real-time environmental monitoring, intelligent event classification, and rapid emergency notification. The proposed system integrates distributed Internet of Things (IoT) sensors for collecting environmental parameters, including temperature, humidity, rainfall, atmospheric pressure, wind speed, water level, and air quality. The collected data are processed at edge or cloud nodes to detect abnormal environmental patterns and estimate climate-related risk levels. Based on event severity, urgency, location, and potential impact, a priority score is assigned to each notification. A priority-routing mechanism then selects communication paths that minimize delay and maximize reliability for high-priority alerts. Critical notifications are transmitted before routine monitoring traffic, allowing emergency information to reach disaster management authorities and affected communities more efficiently. The proposed framework supports multi-hop IoT networks, wireless sensor networks, edge computing, and cloud-based analytics. A performance evaluation model is developed using latency, packet delivery ratio, energy consumption, throughput, and priority-based notification success as key performance indicators. The framework can contribute to smart-city climate resilience and disaster risk reduction by improving the speed, reliability, and intelligence of environmental early-warning systems.

Keywords: *Climate Change, Internet of Things, Priority Routing, Environmental Monitoring, Early Warning System, IoT Networks, Statistical Disaster Management, Smart Cities*

1. Introduction

Climate change is one of the major global challenges affecting environmental stability, human communities, agriculture, infrastructure, and public safety. Rising temperatures and changing atmospheric patterns contribute to extreme weather events such as floods, droughts, heatwaves, cyclones, heavy rainfall, and severe storms. The consequences of these events can be reduced when accurate environmental information is collected and delivered to relevant stakeholders in real time.

The Internet of Things (IoT) has emerged as an important technology for environmental monitoring. IoT devices can continuously collect data from geographically distributed locations using sensors for temperature, humidity, rainfall, water level, air quality, wind speed, and other environmental variables. These devices can form large-scale monitoring networks that provide near-real-time information about changing environmental conditions.

However, an important challenge arises when a large number of IoT devices attempt to transmit data simultaneously. During an environmental emergency, network congestion can delay the delivery of critical notifications. For example, a rapidly increasing river water level should be communicated with higher priority than periodic temperature readings. Conventional routing systems may treat both types of information equally, potentially delaying life-critical alerts.

This research proposes a priority-routing network for climate change notification using IoT devices. The framework classifies environmental events according to their urgency and routes critical information through optimized communication paths. The proposed approach is intended to support real-time early-warning systems and improve the resilience of environmental monitoring networks.

The main contributions of this paper are:

1. A multi-layer IoT architecture for climate and environmental monitoring.
2. A priority classification model for environmental events.
3. A priority-routing mechanism for critical climate notifications.
4. An edge-based abnormal event detection system.
5. A performance evaluation framework for latency, reliability, energy consumption, and notification success.

2. Research Problem

Environmental monitoring systems generate large volumes of sensor data. Under normal network conditions, routine information can be transmitted without significant urgency. However, during extreme climate events, the communication infrastructure may experience congestion due to simultaneous sensor transmissions.

A major problem can therefore be expressed as:

How can IoT devices transmit high-priority climate and disaster notifications with minimum delay and maximum reliability during periods of network congestion?

The problem consists of three major components:

- detecting abnormal environmental conditions;
- determining the urgency of detected events;
- routing high-priority notifications efficiently through the communication network.

Without priority-based communication, critical alerts may compete with routine sensor data for the same network resources.

3. Objectives of the Study

The objectives of this research are:

1. To design an IoT-based climate change monitoring framework.
2. To collect real-time environmental data using distributed sensors.
3. To identify abnormal climate and environmental conditions.
4. To classify detected events according to severity and urgency.
5. To develop a priority-routing mechanism for emergency notifications.
6. To minimize the delay of high-priority climate alerts.
7. To improve packet delivery reliability during network congestion.
8. To evaluate the energy efficiency and scalability of the proposed network.

4. Proposed Climate Change Notification Framework

The proposed system is called the **Climate Change Notification Priority Routing IoT Framework (CCN-PRIoT)**.

The architecture consists of five major layers.

4.1 Environmental Sensing Layer

This layer contains distributed IoT sensors responsible for collecting environmental information.

Monitored Parameters

The system can monitor:

- Temperature
- Humidity
- Rainfall
- Wind speed
- Atmospheric pressure
- Air quality
- Carbon dioxide levels
- River and water levels
- Soil moisture
- Solar radiation

Each IoT node periodically records environmental values and transmits the collected information to nearby gateways or edge devices.

4.2 Communication Layer

The communication layer connects IoT devices to gateways and data-processing nodes.

Possible communication technologies include:

- Wireless sensor networks
- Wi-Fi
- LoRaWAN
- 5G and cellular networks
- Zigbee
- Satellite communication

The network may operate as a multi-hop system in which sensor nodes forward data through intermediate devices.

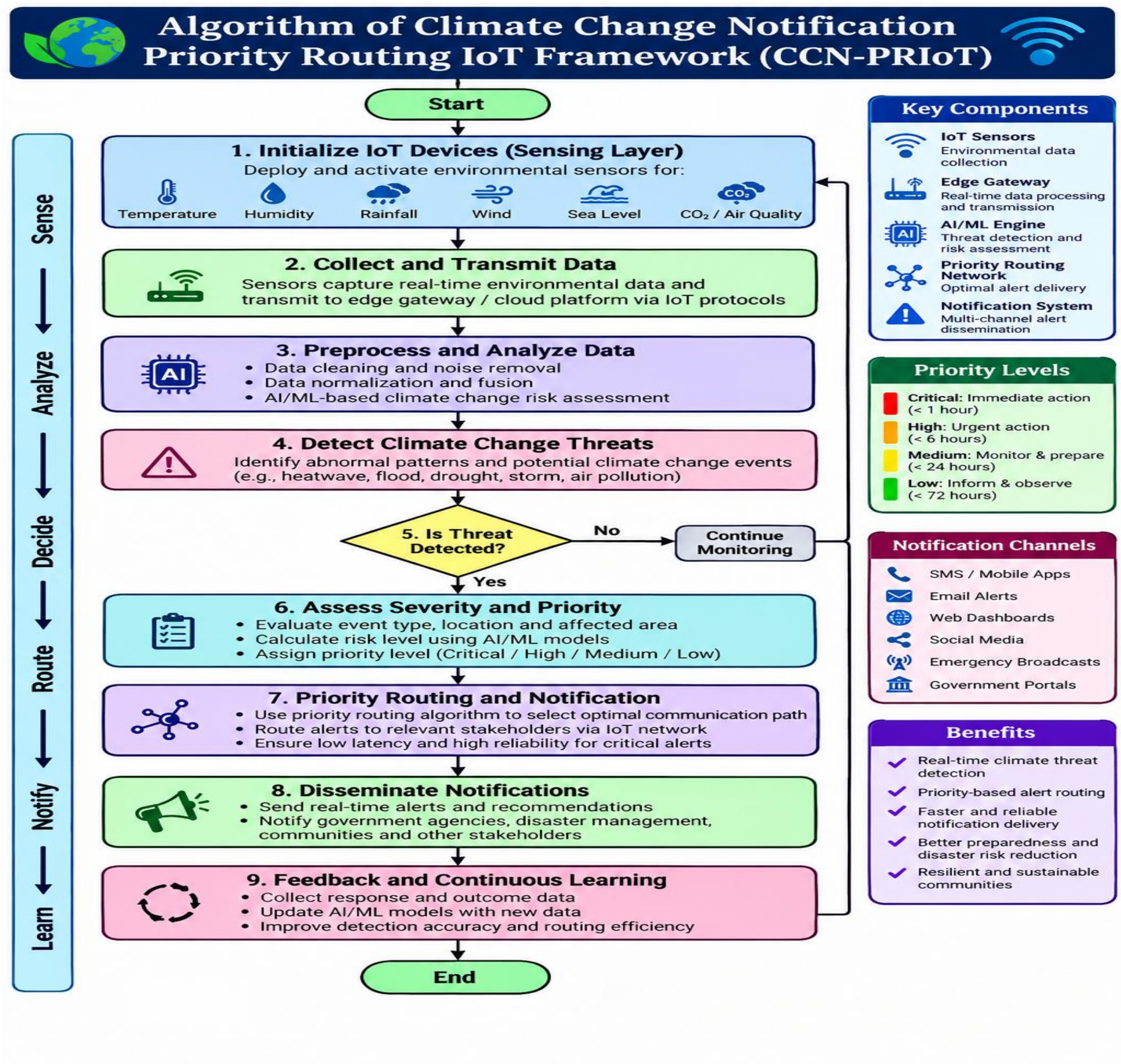

Fig 1: CCN-PrioT framework

4.3 Edge Intelligence Layer

Edge computing devices process sensor information close to the data source. This reduces the need to transmit every raw sensor measurement to a remote cloud server.

The edge layer performs:

- Data filtering
- Data cleaning
- Abnormal event detection
- Threshold analysis
- Priority classification
- Local alert generation

For example, a water-level sensor detecting a sudden increase beyond a defined threshold can generate an immediate emergency event.

4.4 Priority Routing Layer

The priority-routing layer determines the communication strategy for each notification.

The priority of an event depends on:

- Severity of the environmental condition
- Rate of environmental change
- Number of affected people
- Geographic location
- Infrastructure vulnerability
- Probability of disaster occurrence
- Urgency of response

High-priority notifications receive preferential access to network resources and are routed through low-latency and reliable communication paths.

4.5 Application and Notification Layer

The final layer delivers alerts to:

- Disaster management authorities
- Government agencies
- Emergency response teams
- Local communities
- Mobile applications
- Smart-city management centers

Notifications may be delivered through:

- SMS alerts

- Mobile applications
- Emergency dashboards
- Public warning systems
- Automated control systems

5. Priority Classification Model

The proposed system assigns a priority score to every detected environmental event.

Let the priority score be represented by:
$$P_i = w_sS_i + w_uU_i + w_rR_i + w_lL_i$$
Where:

- P_i = priority score of event i
- S_i = severity score
- U_i = urgency score
- R_i = risk probability
- L_i = location impact
- w_s, w_u, w_r, w_l = weighting factors

The priority score is divided into four categories.

Priority Level	Event Type	Routing Action
P1	Critical emergency	Immediate priority routing
P2	High risk	Fast transmission
P3	Moderate risk	Normal priority
P4	Routine monitoring	Standard transmission

Example

A sudden flood event may receive a P1 classification, while a routine hourly temperature measurement may receive P4.

6. Proposed Statistical Priority-Routing Algorithm

The routing mechanism evaluates available network paths according to delay, reliability, congestion, and energy consumption.

The routing cost of a path can be represented as:
$$C_{path} = D + (1-R) + Q + E$$
Where:

- D = transmission delay
- R = route reliability
- Q = network congestion
- E = energy consumption

- (, , ,) = optimization weights

The system selects the path with the minimum routing cost for high-priority events.

A priority-aware routing decision can be represented as:
[Route_i =]

7. System Workflow

The proposed framework follows the following operational process:

1. Environmental sensors collect climate-related data.
2. Data are transmitted to a local IoT gateway.
3. The edge node preprocesses the data.
4. Abnormal conditions are detected.
5. The system calculates an environmental risk score.
6. A priority level is assigned.
7. The routing algorithm evaluates available communication paths.
8. High-priority events are transmitted first.
9. Notifications are delivered to relevant users and authorities.
10. The event and network performance are recorded for future analysis.

8. Algorithm

Algorithm 1: Priority Climate Notification Routing

Input: Environmental sensor data

Output: Priority-based climate notification

1. Initialize IoT sensor network.
2. Collect environmental parameters.
3. Remove incomplete or erroneous data.
4. Analyze sensor values.
5. Detect abnormal environmental conditions.
6. Calculate severity and urgency.
7. Assign priority score (P_i).
8. If (P_i) is critical:

   - Search for the fastest reliable route.
   - Allocate priority network resources.
   - Transmit emergency notification.
9. Otherwise:
   - Route data through the normal network.
10. Record network performance.
11. Repeat the monitoring process.

9. Machine Learning Integration

Machine learning can improve the ability of the proposed system to identify climate-related anomalies.

The input feature vector can be represented as:
[X = [T, H, R, W, P, AQ, WL, SM]]
Where:

- (T) = temperature
- (H) = humidity
- (R) = rainfall
- (W) = wind speed
- (P) = atmospheric pressure
- (AQ) = air quality
- (WL) = water level
- (SM) = soil moisture

Potential machine-learning models include:

- Random Forest
- Support Vector Machine
- Gradient Boosting
- Long Short-Term Memory networks
- Deep Neural Networks

The machine-learning model can predict an event probability:

[Pr(Event) = f(X)]
The predicted probability can then be incorporated into the priority score.

10. Performance Evaluation Metrics

The proposed framework can be evaluated using the following metrics.

10.1 End-to-End Delay

[Delay = T_{received} - T_{generated}]

The goal is to minimize delay, particularly for critical notifications.

10.2 Packet Delivery Ratio

[PDR =]

A high packet delivery ratio indicates reliable notification delivery.

10.3 Throughput

[Throughput =]

10.4 Energy Consumption

[E_{total} = _{i=1}^{n} E_i]

Energy efficiency is important because many IoT devices operate on limited battery power.

10.5 Priority Notification Success Rate

[PNSR = {}]

The proposed system aims to maximize the delivery success rate of P1 and P2 alerts.

11. Expected Results

The priority-routing approach is expected to provide better performance than conventional routing networks, particularly during environmental emergencies.

Expected improvements include:

- Reduced delay for critical alerts
- Higher packet delivery ratio
- Improved reliability
- Better management of network congestion
- Efficient allocation of communication resources
- Faster disaster response
- Improved energy utilization

The expected relationship can be expressed as:

[Delay_{Priority} < Delay_{Conventional}]
and:
[PDR_{Priority} > PDR_{Conventional}]
particularly for critical climate notifications.

12. Discussion

The proposed framework combines environmental sensing and intelligent communication. Traditional IoT networks generally focus on collecting and transmitting sensor data, while the CCN-PRIoT framework introduces an additional decision layer that considers the importance of information.

The framework is particularly useful for areas vulnerable to climate-related disasters. For example, IoT water-level sensors can detect possible flooding. If the water level increases slowly, the system may classify the event as moderate. However, if rapid water-level growth occurs, the system can increase the event priority and immediately route the notification through the most reliable network path.
The same concept can be applied to:

- Heatwaves detection
- Flood monitoring
- Drought prediction

- Forest fire monitoring
- Severe storm notification
- Air pollution alerts

13. Challenges and Limitations

Several challenges must be addressed before large-scale deployment.

13.1 Network Infrastructure

Remote areas may have limited communication coverage.

13.2 Energy Limitations

Battery-powered sensors require energy-efficient communication.

13.3 Data Quality

Incorrect sensor readings may produce false alerts.

13.4 Cybersecurity

Environmental monitoring networks may be vulnerable to cyber-attacks, data manipulation, or denial-of-service attacks.

13.5 Scalability

Large-scale deployments may contain thousands or millions of IoT devices.

Future work should include secure routing, block chain-based data integrity, federated learning, and adaptive artificial intelligence.

14. Conclusion

This paper proposed the Climate Change Notification through Priority-Routing IoT Devices framework for real-time environmental monitoring and emergency communication. The system integrates IoT sensors, edge intelligence, priority classification, and optimized network routing to improve the delivery of critical climate-related notifications. Unlike conventional IoT communication systems, the proposed approach assigns priority levels according to environmental severity, urgency, risk probability, and geographic impact. High-priority events are routed through low-latency and highly reliable communication paths, while routine monitoring data are transmitted through standard or energy-efficient routes.

The proposed framework has potential applications in smart cities, disaster management, environmental protection, agriculture, and remote community monitoring. Future research can focus on implementing the framework using real sensor data, developing machine-learning models for event prediction, and evaluating the routing protocol through network simulation or real-world test beds.

References

1. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks*, *38*(4), 393–422.
2. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660.
3. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376.
4. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. *IEEE Internet of Things Journal*, *1*(1), 22–32.
5. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, *57*(10), 2266–2279.
6. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, *3*(5), 637–646.
7. IPCC. (2023). *Climate Change 2023: Synthesis Report*. Intergovernmental Panel on Climate Change.
8. UNDRR. (2022). *Global Assessment Report on Disaster Risk Reduction*. United Nations Office for Disaster Risk Reduction.