A Self-Adaptive CBORF-IoT Dynamic Routing for Effective Disaster Management Operations

Sunita Rani[1], Sudesh Kumari Nandal[2,*], Sonal Beniwal[3], Pragya Chandi[4], and Vijender Singh[5]

ARTICLE INFO

Article history:
Received: 3 March 2024
Revised: 10 July 2024
Accepted: 17 September 2024
Online: 31 October 2025

Keywords:
Opportunistic internet of things
Connection based routing
History
Delivery probability and ONE

ABSTRACT

In the aftermath of a disaster, where traditional communication infrastructure is severely damaged or non-existent, establishing reliable communication among IoT devices, such as sensors, drones, and mobile units, is crucial for effective disaster management operations. Opportunistic IoT, also referred to as opportunistic Internet of Things (IoT), is a concept that leverages ephemeral and opportunistic network connections for IoT devices in disaster-prone areas. Conventional IoT networks rely on stable and reliable connections, whereas in opportunistic IoT, devices transmit messages and interact with other devices or systems by utilizing temporary, ad hoc, or ephemeral network opportunities. In this network, devices forward messages to their target devices according to the store-carry-forward principle. Various routing techniques, such as epidemic, prophetic, context-based, and history-based routing, are employed to transmit messages between devices, but none provides a solution for transmitting messages with acknowledgment. Moreover, there is another drawback: none of these routings provides a solution with lower end-to-end delay and high throughput simultaneously. In this paper, a Connection-Based Opportunistic Routing Framework (CBORF) is presented, wherein the connections of nodes are computed. The proposed framework calculates the duration of the connection and allows for the participation of different IoT devices. The value of the connection between the devices (CBD) is used to identify the next hop for data exchange on the way to the destination. The proposed framework was implemented in the ONE simulator. Three key performance indicators were thoroughly analyzed to assess the effectiveness of the projected mechanism: throughput, end-to-end latency, and overhead ratio. The proposed CBORF scheme outperformed two similar routing algorithms (CBR and HBR) with a remarkable throughput of 77%. It also demonstrates that the end-to-end latency of the proposed system is 4% lower than the state-of-the-art CBR and HBR methods that can manage disaster operations effectively.

1. INTRODUCTION

Consider a scenario where a natural disaster has caused widespread destruction in an urban area. IoT sensors deployed in the area collect data on various parameters like temperature, air quality, and structural integrity of buildings. Drones equipped with communication modules and the Connection-Based Opportunistic Routing Framework (CBORF) framework are dispatched to establish communication and coordinate rescue efforts. Mobile ad hoc networks facilitate devices to communicate with each other and exchange messages between them. There may be instances, however, in which the connection between the two devices is either permanently terminated or temporarily disrupted [1]. Taking into consideration the rapid development of IoT-connected devices, the significance of the number grows extremely immense and unintelligible. IoT refers to the current trend of providing objects with information processing, communication, and sensor technology so that they may be interacted with each other [2].

In recent years, extensive research on the opportunistic IoT has been provided, primarily from a business perspective [3]. Despite that, the corresponding interaction between humans and IoT, or the social aspect of IoT, has been rarely studied [4]. The conventional commencement of

[1]*Department of CSE & IT, BPSMV, Khanpur Kalan, Sonipat, India.*
[2]*Department of ECE, BPSMV, Khanpur Kalan, Sonipat, India.*
[3]*Department of CSE & IT, BPSMV, Khanpur Kalan, Sonipat, India.*
[4]*Department of CSE, UIET, KU, Kurukshetra, India.*
[5]*Department of CS & A, KU, Kurukshetra, India.*
**Corresponding author:* Sudesh Kumari Nandal; Email: sudesh_30@rediffmail.com.

the IoT focuses on establishing a global network of physical nodes as its essential strategy. Numerous personal devices, such as smartphones, wearables, and automobiles, can form the IoT when initiated with the required short-range communication. This is the primary reason why opportunistic IoT has gained so much popularity. Distinct devices in such networks are able to implement the store-and-carry-forward pattern [5]. A message can be stored at an intermediary device until it can be transmitted to its final destination. The major contribution of paper is to recommend a routing framework called CBORF that addresses the issue of information sharing and dissemination within and between opportunistic communities (consisting of pairs of devices) that are formed as a result of mobile and random interactions between devices. Furthermore, the proposed framework is simulatedwith ONE simulator, the proposed framework is analysed through throughput, end-to-end delay, and overhead ratio and compared with CBR and HBR existing strategies.

An opportunistic IoT architecture is a design strategy for IoT systems that employs opportunistic networking and communication techniques to enhance the connectivity and dependability of IoT devices. Opportunistic networking refers to the capability of devices to communicate when in close proximity or when network conditions are favourable, even in the absence of a stable and persistent network connection. This architecture is especially useful in remote or dynamic environments where traditional, always-on network connectivity is impractical. The opportunities of relationship amid device sensing and the IoT are depicted in Figure 1. This paper will demonstrate how the connection amid device sensing and Internet of Things (IoT) in disaster management operations has various avenues of opportunities for preparedness, response, and recovery. All nodes are mobile, and a message can reach any other node via any of the possible routes in an opportunistic network. Since the nodes interact in the network only for some time and may move from place to place, the connectivity of the nodes in the network is somewhat dynamic. Each single node can pull other nodes in the close proximity and can establish direct communications with them. Any node in contact with another node in the physical plane has the capability to send and or receive any type of data that is in the network. Based on findings from the analysis of device sensing and IoT technological applications in disaster management, stakeholders can enhance recovery programmes, response and preparedness, thus diminishing the cost of disasters in terms of human and economic losses.

Routing is very vital in disaster management because it enables comprehensive management of communication, resource, as well as the flow of information in disasters. It provides fast deliver of important alerts, help to deliver resources such as first aid kits, medical personnel and equipment, and keep connected in case of damaged infrastructure. However, routing poses other problems like, fluctuating and unpredictable topology of the network, fragmented routing paths due to breakdown of infrastructures, problems of high traffic congestion, power issues that is to do with energy beside restricted environments, and issues to do with the use of secure and interoperable communication amid substandard infrastructure. Therefore, it is imperative that new routing protocols for repertoire to be adaptive and efficient, secure and robust in order to support disaster response objectives and promote seamless cooperation between military, government and the public.

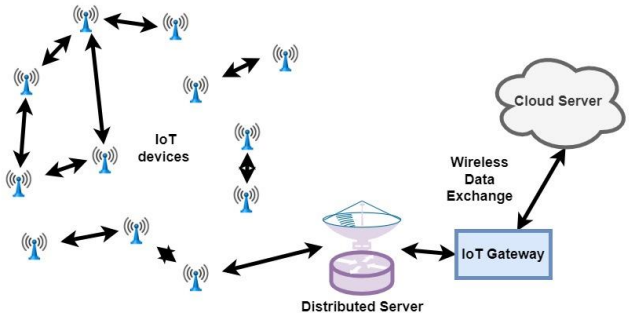

Fig. 1. Architecture of Opportunistic IoT.

With the use of the Self-Adaptive CBORF Framework in this disaster management setting, IoT devices provide a solution to the obstacles caused by unstable communication structures and constantly changing environmental situations in order to coordinate rescue operations in this case efficiently. The paper is divided into 5 sections. In Section 1, introduction of opportunistic IoT provides the need for opportunistic IoT and its architecture in depth. Section 2 presents a review of the literature that provides the role of existing routing strategies in opportunistic IoT. In Section 3, a proposed framework is presented that provides a mathematical solution for data exchange between IoT devices in opportunistic scenarios. After that, proposed algorithms were presented. Furthermore, in Section 4, the results and analysis have been discussed. In Section 5, the conclusion of the paper and future research directions has been discussed.

2. LITERATURE REVIEW

In opportunistic IoT networks, routing is a challenging obstacle due to the need for effective message delivery and the transient nature of connections. Researchers have developed a variety of solutions to this issue. Opportunistic Routing (OR) is a strategy that employs streaming techniques to enhance the delivery performance and dependability of cellular networks [6]. Hidden Markov Model Routing (HMMR) is an additional proposed method that uses emission and transition probabilities to estimate the likelihood of routes successfully delivering a message [7, 8]. The ORPL-DT technique uses both uplink and downlink

traffic to update link quality information [8] in order to further improve packet delivery ratio and control overhead in multihop low power and lossy networks (LLN). Also, enhanced network throughput and packet latency have been proposed as a result of simultaneous opportunistic routing employing multiple wireless technologies in IoT networks as opposed to conventional routing's reliance on a single technology [9]. In addition, a secure and reliable routing protocol for OppIoT (dubbed RFCSec) has been projected; it defences the network from threats such as packet collusionand wormhole attack [10].

There exists a study that presents a hyperbolic routing strategy for the Information-Centric IoT [11] based on the concepts of Information-Centric Networking (ICN) and edge computing. A dynamic hop selection static routing protocol (DHSSRP) is devised in order to solve the issue of load balancing in IoT networks with a priority-based, non-congested communication architecture [12]. The authors recommended a three-phase enhanced ad hoc on-demand distance vector (enhanced-AODV) routing protocol for multi-WSNs [13], with phases 1 and 2 handling high-priority traffic and phases 3 handling low-priority and ordinary network traffic, respectively. The collected data of an AG-IoT network can be processed from origin to final destination using the network's multihop count and organizational distance-based communication infrastructure, as described in [14]. Using TD routing the associated SRv6 header (SRH) compression (CARD) technique, [15] proposes a decentralised storage mechanism. GMMR [16] integrates the advantages of context-aware routing approach by using ML-based approaches. A fish-inspired Multi-Adaptive Routing Protocol (MARP) for IoT-relied ad hoc networks that reduce latency and power consumption [17]. In [18] solution was proposed to the problem of rapidly determining the optimal path to the destination. It has taken protective measures to reduce its power and memory usage [19]. Using the Ring Loop Routing Protocol, node locations in IoT networks can be kept hidden. For optimal results across all domains, employ a backtracking technique [20,21].

Based on experimental findings, the proposed Opportunistic Context-Virtual Networks method reduces the resource usage of relaying nodes while increasing the overhead ratio and delivery probability in comparison to other well-known opportunistic routing algorithms [22]-[24]. Since IoT users have access to physical data, the proposed SecDL strategy prioritises IoT-user security while simultaneously attaining security, QoS, and energy efficiency in dynamic cluster-based WSN-IoT networks [25]. Similarly, in [26], the authors propose a context-based protocol (HiBOp) and evaluate it in light of two established approaches, Epidemic Routing and PROPHET. Findings indicate that HiBOp significantly reduces system resource utilisation. In addition, [27] states that a significant challenge between opportunistic societies is how to design an opportunistic network by identifying crucial links between individuals and smart devices [28]. In light of these facts, the study investigates certain fundamental applications, imminent obstacles in constructing opportunistic networks on an IoT background, and the organisation of opportunistic network forwarding operations. In addition, the SEER algorithm, which is based on social relationships, has been presented in order to facilitate efficient communication between smart devices in environments where such connection is unavailable [29]-[39]. Using similarities in human behaviour or mobility patterns to design a route is possible due to the social connections between individuals [40]-[56].

3. EXISTING ROUTING TECHNIQUES IN OPPORTUNISTIC IoT

In opportunistic IoT for disaster management, where traditional communication framework might be disrupted or unavailable, routing techniques play a crucial function in ensuring reliable and efficient data transmission. Opportunistic IoT provides numerous routing techniques that utilizes the pattern of store carry and forward. The very first routing technique was epidemic routing. It is a straightforward and reliable routing method. In this method, a node that encounters other nodes replicates data messages and distributes them throughout the network. This technique assumes that the message will ultimately reach its destination through message replication. Furthermore, the advancement in epidemic routing is called Spray and Wait which aims to decrease overhead. Initially, a fixed number (spray) of copies of a message are transmitted to various nodes. A copy is passed to the next node and with this, there is cutting down on one copy. Subsequently, the Prophet routing evaluates and assigns a delivery predictability value to each node based on the probability of receiving messages by the other nodes. Messages are delivered to nodes that are likely to deliver than other nodes with lower probability of doing so. This method is optimized towards message forwarding and reduced overhead. Compared with the other existing state-of-art protocols like epidemic, Prophet, history-based and encounter, Contact-based routing focuses on direct contact between nodes and the notion of proximity. Epidemic routing duplicates message transmission attempting to guarantee message delivery probability because nodes are expected to meet due to mobility. However, Prophet routing utilizes previous contact frequencies in order to estimate future meetings and then adjusts the message delivery intention to the nodes which are anticipated to be meeting in the near future. Utilising data based on past encounters of transport vehicles, history-based routing provides the best routes on one hand while using history on the other. The main idea of the contact-based routing is the direct transmission of data and the avoidance of the repetition of data transfers, making it highly energy efficient and suitable for constantly changing

and resource-scarce environments such as opportunistic networks and IoT. Every approach describes its benefits appropriate to selected network conditions and strengths and weaknesses reflecting on scale, power use, and flexibility to ensure the reliability of communication in various circumstances.

In addition, Context-based routing involves information more about the nodes in the routing as well as their mobility patterns and other contextual factors in the selection process. Context may refer to positions of the node, the energy level, communication history of the nodes and so on. The idea is to nominate the most suitable further step or the following path for a message and considering the field of these context data regarding the current network situation. On top of that, the history based routing that is used in the Opportunistic IoT involves forwarding decisions tied to the previous interactions nodes/bundles have had [26]. It considers the history of previous communication attempts and the interactions amid nodes in order to choose the most probable path for data transmission. This method is particularly useful when the network architecture is unknown in real time and the connection is unreliable. When conveying a message using the history of come across and transitivity protocol, each node first determines, using the delivery predictability metric, the possibility that its message will be successfully delivered to each of its known recipients. This metric indicates the probability that a message will be sent from its originator to its intended recipient. Delivery Predictability is determined by analysing the frequency with which two nodes have previously met and visited the same locations.
When two nodes interact, they exchange their respective delivery predictability. Figure 2 depicts the message transmission in HBR where two nodes interact frequently, the delivery predictability between them will increase. Two nodes that have been attempting to communicate with each other for a long time without success may not be dependable forwarders. Therefore, their Delivery Predictability must reduce over the time, otherwise; their costs will offset their revenue streams. These routing techniques can be adjusted according to the characteristics of, and integrated with each other to fit disaster management scenarios and opportunistic IoT considering the challenges involved in such operational environments. In sporadic IoT networks for disaster response, regimes of conventional routing protocols may be inadequate because it exists in a dynamic environment. However, actual routing methods designed to operate in MANETs have been devised to cope with the problems caused by limited connection duration, mobility of the nodes, and constrained availability of resources.

In Cluster-Based Routing (CBR), communication is achieved by the cluster hierarchy where the nodes are grouped and one of them act as cluster head (CH). CH is expected to collate data from related nodes in a cluster and forward same to the subsequent node. The simplified message transmission process diagram of can be presented as depicted below; Figure 3. The diagram shows a packet delivery from the OW to the destination node within various clusters in between. From the OW it is transmitted to the CH that follows it to the next succeeding CH until it gets to the desired destination node. Because of this structure, message cascading can quickly get to the intended recipient with little or no forwarding, thus enhancing efficiency in the network. Also, CBR is able to minimize the network fluctuations since the group formation and routing discipline can respond to node mobility as well as the link quality.

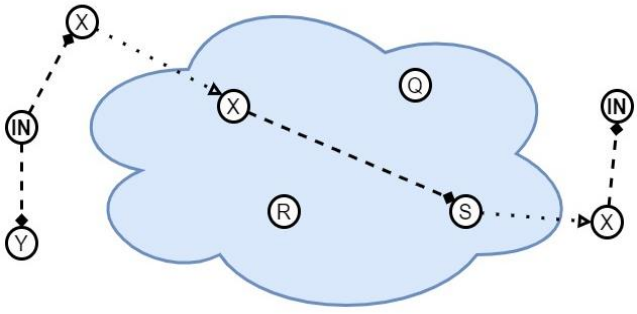

Fig. 2. Message transmission in HBR.

4. PROPOSED FRAMEWORK

Sophisticated routing systems for the forwarding of messages between IoT devices have been developed by researchers including History-based Routing (HBR), Content-based Routing (CBR) and others [26]. In the course of the HRM approach, a buffer memory of the IoT devices is employed to store details of their past communications. The log contains the acknowledgement number, sequence numberof the message. Message transmission between adjacent IoT devices could benefit from the context provided by this information. As a consequence, it is difficult to remember many past events, which increases the message latency rate and the overhead ratio. Using CBR, IoT objects' proximity, profile, and actions are recorded. The next IoT object requires information from the antecedent IoT object in order to convey the message to the inserted object, which creates a bottleneck during message transmission.

Objects in CBR are first configured into a virtual network topology in which one object is chosen as leader based on the energy contribution of the objects in the network, and then that object uses the same mechanism to select another object in its neighbour as next leader to forward the message to its final destination. The reasons of choosing the map-based movement model are explained below. First and foremost, it orients planners in the overall context with consideration to social bodies consisting of individuals and materiel in processes of mobility – so important in coordinating and ordering disaster operations. Secondly it makes it easy to recognize segregation and sharing spaces between different movements so that resource allocation is

better. Moreover, the use of map-based models can help represent simple, as well as subdivided systems and processes, using maps that can be easily analyzed to make improvements. This is especially so since one is able to determine the issues of congestion, delays, constraints and possible opportunities within the disaster management and response and recovery system. In addition, map-based models can improve movement and sensorimotor maps, which play a critical role in movement and action. In summary, there are few strengths that make the movement model a map based one; flexibility, coverage, and visual appeal which are essential in the enhancement of demanding systems including disaster management operations. Here, for each object, two tables are maintained: one that pertains to the distance between the destination and the object under consideration and the other that concern the content of the intersecting objects that can be used to reach a given destination and accomplishment of the particular task. Although this will mean keeping so much information for each item, it will also mean more time needed to transmit messages because of the overhead. However, the energy reduction rate is ineffective due to the high transmission time and high computation time necessary for the construction and maintenance of the virtual topology presented by in the CBR. In this paper, a connection-based opportunistic routing framework (CBORF) has been presented for obtaining optimal data exchange between mobile devices with high throughput and a low overhead ratio. In the proposed scenario, we consider D devices, S sender, and an R receiver. The sender and receiver devices communicated through IN intermediate devices. The value of IN ⊆ D. once data exchange initiated, the probability of message delivery between two devices when they are in the range of each other is computed using equation 1. It shows the computation of the present delivery probability on the basis of the initial probability and the past delivery probability of the device.

$$P_{(x,y)} = P_{(x,y)\,prev} + \left(1 - P_{(x,y)\,prev}\right) * P_{beg} \quad (1)$$

$P_{(x,y)}$: It denotes the present delivery probability of device.

$P_{(x,y)\,prev}$: It denotes the past delivery probability of device.

P_{beg}: It denotes initial probability of node.

Furthermore, the optimal energy (OE) is computed using equation 2. OE is the sum of the total energy of all devices from the perspective of the total number of devices. OE can be beneficial for computing the overhead ratio of a network.

$$Optimal\ Energy\ (OE) = \frac{\sum sum\ of\ remaining\ energy\ of\ all\ nodes}{No.of\ devices} \quad (2)$$

In the proposed framework, each device maintains an N*N matrix with a dynamic nature that contains the record of all connections that occurred between devices in order to calculate the CBD (connection between devices) valuethat will be used for selecting the next hop for data exchange to achieve high throughput. This CBD is derived from the number of messages each node generates, sends, and receives from its neighbouring nodes. The numbers range from zero to one. Messages are not sent across the nodes with values less than 0 in this algorithm.The proposed algorithms are as follows:

Algorithm I: compute the connection duration in terms of seconds between IoT objects

i,j : Indexing countersof IoT device

d: Devices

T_i: Time taken by device to deliver message

TDoC: Time duration of connection between two devices

1. Start.
2. Initialise number of IoT devices.
3. For(i=1;i<=d;i^{++})

{

4. for (j=1;j<=d;j^{++})

{

5. Compute connection between device(CBD) value of each device.
6. TDoC= T_i-T_j;

}

}

7. Maintain N*N matrix to store CBD values of each device for obtaining next hop for forwarding messages.
8. Return max TDoC.
9. Stop.

We present two algorithms based on the above-mentioned discussion. Initialise the IoT devices with some temporary memory or buffer to store messages in the first step of algorithm I. Further, calculate the total number of connections that occurred between devices for each IoT device. The CBD value shown is derived from the connection time between each subsequent pair of IoT devices. The connection duration can be calculated by subtracting the total amount of time it took device A to send a message to device B from the start of message initiation. This CBD value is used to determine the responsive IoT device through which messages will be delivered.

Furthermore, Algorithm II is used to compute energy consumption of all IoT devices. This algorithm will first set the initial energy level for each IoT device. After that, we examine the IoT's current state. We considered a number of states, including off-state, on-state, and scanning states. Now compute the total amount of energy used by the item, including the energy used to initialise it. Thus, CBORF has operated by initially calculating the time and second calculating the energy of the devices according to their stats and behaviors.

Algorithm II: To check the energy of IoT object

i: Indexing counter of IoT device.

d: Devices.

IN_i = Intermediate devices used during message transmission. If the value is 0, it shows that there are no intermediate devices involved between the source and destination, and if it is 1, it indicates that intermediate devices are involved.

S_i= status of the i^{th}device.

T_d = Time delay

T_w = Waiting time in buffer

T_c = Carrying time;

1. Start.
2. for (i=1;i<=d;i^{++})
{
3. Check the status of the device.
4. If(IN_i=0)
5. Si is in off state.
else
If(IN_i=1)
then
6. Si is in active state.
else
7. Si is in scanning state.
}
8. Check energy for all device
9. For(i=1;i<=d;i^{++})
{
10. Utilized energy= T_d=T_w+T_c
11. $Optimal\ Energy\ (OE) = \frac{\sum sum\ of\ remaining\ energy\ of\ all\ nodes}{No.of\ devices}$
12. }
13. Stop.

This technique, Self-Adaptive CBORF-IoT Dynamic Routing for Effective Disaster Management Operations, will automatically adjust to the changing topography of the network in real time, thus determining the best path without any necessity for human interferes. This makes it possible for the chosen architecture to adapt to different node mobility, topological changes and traffic flows. It highlights that due to this context awareness in the algorithm communication can be established and remains operational in disaster situations, threat stemming from obstacles, node failures, or problematic connectivity. it is also flexible because it can be used in small networks as well as in large networks making it important in a wide range of disaster management. Further, the technique is performed with an energy-saving context, where the routing-based paths are found to prolong the lifetime of the network that is essential for the constrained IoT settings. All these self-adaptive features make a common evaluation to ensure that the CBORF-IoT dynamic routing technique offers a proficient and trustworthy converged communication that fits the demanding and volatile environment characteristic of disaster management operation.

4.1 Map-Based Movement Model:

The reasons for the selection of the map-based movement model include. First, it offers a possibility to know the key incoming/outcoming contingents and resources, which is critical in disaster management operations, as better coordination and common action are provided. Secondly, it gives the coordination since it shows the relation between the movements at a horizontal level and how much they do overlap or do not overlap at all thus facilitating the coordinative and allocating of resources. Thirdly, map-based models represent theoretical and practical systems and processes and their optimization as clear and understandable maps. This is more so in disaster management where, a record is made of all the low moments, hurdles, and obstacles in the response and recovery cycles. In addition, map-based models can improve movement while some may improve on sensorimotor maps which are highly crucial to movement and action. In general, the map based movement model covers all essential elements of the objects under study that specifies its advantages when studying complex systems such as disaster management operations, in detail.

The proposed framework can not only be mapped out in the format of a flow chart but also be represented through a type of thematic map characterized by the use of linear symbols to depict movement. The flow chart presented illustrates the relation between individual frames of the framework and the sequence of its steps, as well as the process of transferring the data from device to device and calculation of the CBD value. The flow chart is therefore unlike a map but a civil flow diagram in that it captures several dynamics involved in the framework.

Time-to-Live (TTL): Network Herbalizers are very important concepts in networking and TTL is used to control the life span of packets in a network. In the framework in question TTL is utilized to specify time for which each packet should remain on computer or network before being deleted. This is important for avoiding that data packets are

transmitted throughout network and create congestion. TTL value can be set by administrators and they can set any value between the TTL range of 1-255. Whenever a packet arrives on a router interface, router decrease TTL value of packet by 1; if value of TTL becomes 0, then router will discard packet. This generates Internet Control Message Protocol (ICMP) message that is directed back to the host of origin. The TTL value is also employed in other areas such as content delivery network caching and Domain Name System (DNS) caching to determine data caching and enhance performance.

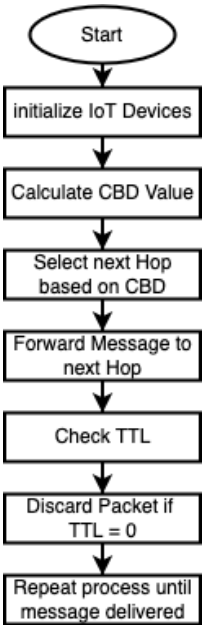

Fig. 3. Flow Chart of the Proposed Framework.

5. RESULTS AND DISCUSSION

One of the simulators is intended to carry out simulation exercises with reference to the projected framework. Static node simulation and dynamic node simulation are provided through this open-source simulation. ONE simulator version 1.5.1 is used because it is stable and has all features necessary to simulate an opportunistic network. This version consists of multiple mobility models and routing protocols and supports the analysis to provide a correct representation of low-layer issues and is suitable for simulations in realistic and diverse scenarios. For the purpose of illustrating the proposed framework, simulation factors as shown in the Table 2 below were used for simulation. In order to model the mobility of IoT devices in a geographic space we have used a map-based movement model. This model allowed us to realistically model the movement patterns of devices and assess the recital of our projected CBORF framework in a more realistic and dynamic environment. We use three performance metrics to analyses the recital of the projected framework and two other state-of art techniques, such as average message delay, throughput, and overhead ratio. The average message delay is used for analyzing the performance of the network. It is measured in seconds. Furthermore, the overhead ratio mainly occurs due to factors like network congestion, scarcity of resources, etc. and is used to compute the excessive resources needed by the routing protocol for data delivery. Moreover, throughput is used to determine the network output. Throughput is calculated by dividing number of messages delivered by number of messages created.

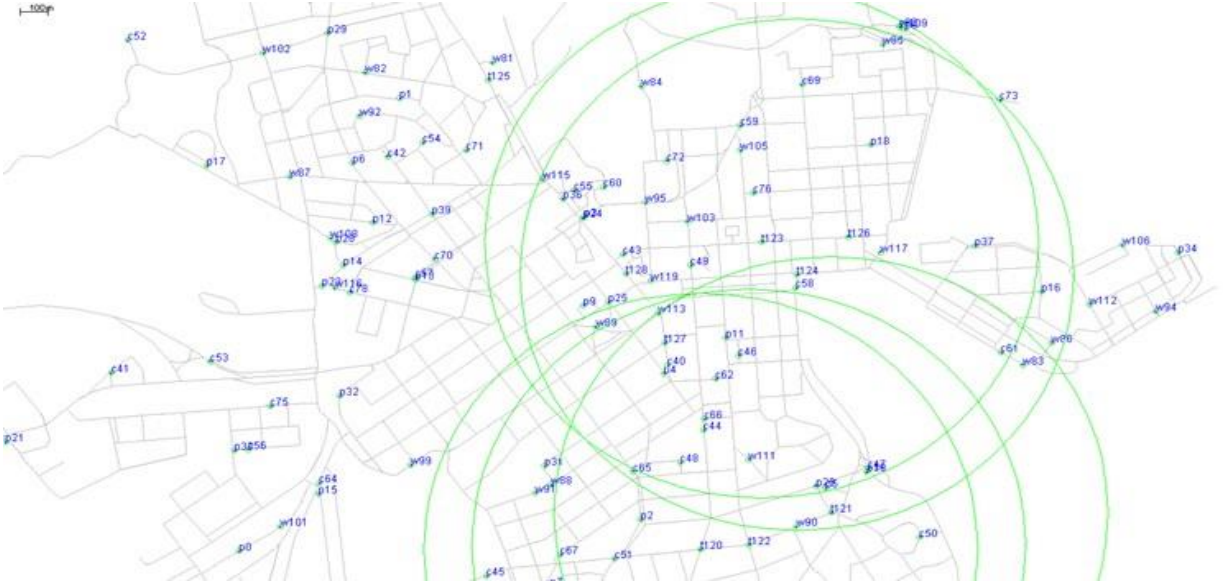

Fig. 4. Data exchange between devices.

Table 2. Simulation parameter table

Parameter Used	Value
Area of Simulation	4500mX3400m
Time duration of Simulation	55000sec
Buffer Size	5MB
Transmission Range	10mtrs
Warm-up Period	1000sec
Nodes	100;150;200;250
Movement model	Map Based Movement
Routing Schemes	[CBORF, CBR and HBR]
Time to Live	300 sec

Figure 4 shows our suggested framework's simulation setup using a Helsinki simulation map. Time to Live (TTL), buffer capacity for transient message storage, wampum time (used for device setup for message transmission), and a map-based movement model for device mobility are among the critical characteristics that are first implemented on 100 devices. The simulation evaluates device variations between 100 and 250 in order to compare our framework's performance with other methods already in use.

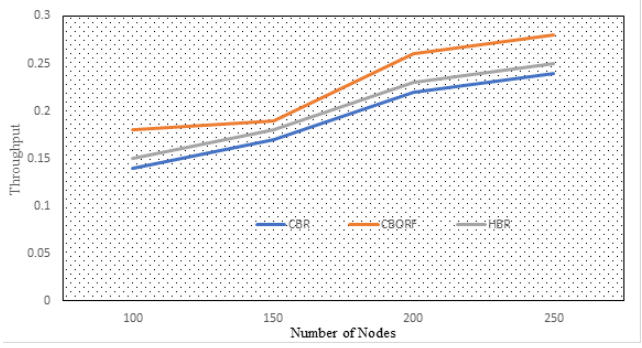

Fig. 5. Throughput comparison between proposed CBORF and existing HBR and CBR in perspective of devices.

Fig. 6. Overhead ratio comparison between proposed CBORF and existing HBR and CBR in perspective of devices.

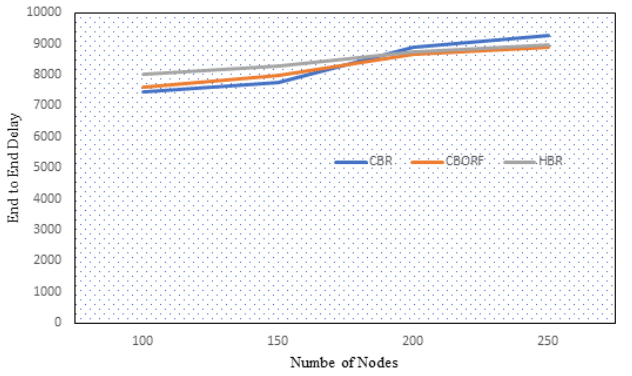

Fig. 7. End to end delay comparison between proposed CBORF and existing HBR and CBR in perspective of devices.

The throughput comparison of our suggested CBORF with traditional CBR and HBR routing techniques, based on simulation findings, is shown in Figure 4. A 16% improvement over CBR and a 12% increase over HBR throughput are shown by the CBORF. The use of CBD values by the CBORF, the creation of links between devices to choose the best hop for message delivery, the reduction of message drop rates, and the increase in throughput are all responsible for this improved performance.

The overhead ratio comparison of CBORF, CBR, and HBR is shown in Figure 6. To further demonstrate its efficiency, our suggested framework shows reduced overhead ratios when contrasted to the other two state-of-the-art methods. Furthermore, a comparison of CBORF, CBR, and HBR in terms of end-to-end latency is shown in Figure 6. CBORF performs better than CBR, with a 2% improvement over HBR and a 4% delay reduction. The total efficacy and efficiency of CBORF in message transmission is enhanced by this reduced latency.

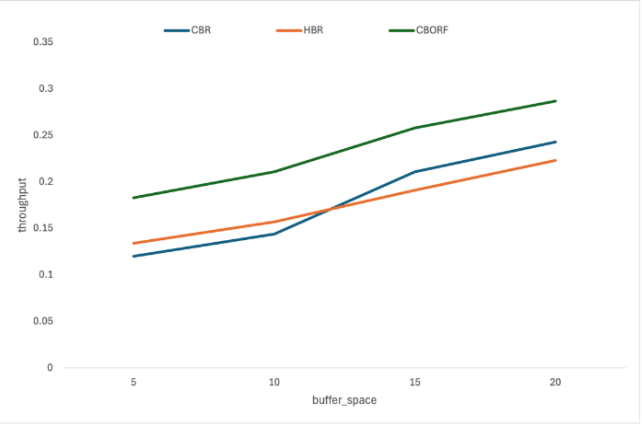

Fig. 8. Throughput comparison between proposed CBORF and existing HBR and CBR in perspective of devices.

The Figure 8 shows assessment of the performance of three routing protocols - CBR, HBR, and CBORF - in terms of throughput and buffer space. It is evident from the

computed results that our proposed CBORF has more efficiency compared to CBR and HBR for all the buffer space values. In particular, the throughput of CBORF increases from 0.183 to 0.287 when the size of buffer space is increased from 5 to 20, which means that the network performance of our proposed CBORF has also been enhanced. CBR and HBR on average are however characterized by lower throughput values, and the values ranges from 0.12-0.243 for CBR and 0.134-0.223 for HBR. These outcomes indicate that CBORF is more efficient in tuning the network operational capacity especially when implementing applications having restricted buffer sizes.

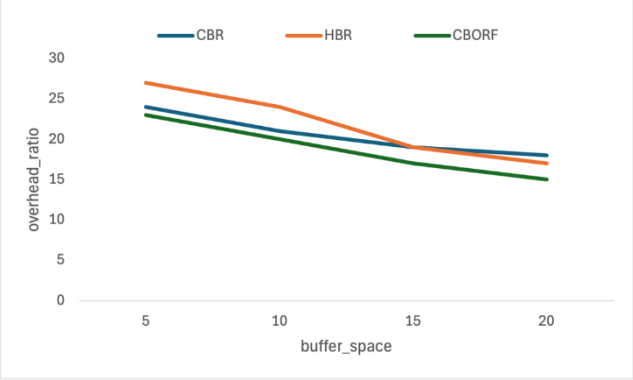

Fig. 9. Overhead ratio comparison between proposed CBORF and existing HBR and CBR in perspective of devices.

It appears from the figure 9 that at different buffer space, the overhead ratio values of three routing protocols including CBR, HBR and CBORF varies. The results suggested that CBORF had a lower overhead ratio compared with CBR and HBR across the whole range of buffer space. The overhead ratio is 5 for CBORF at buffer space of 5 and is 24 for CBR and 27 for HBR. When buffer space is at 10 overhead ratios for CBORF is 20 while that of CBR and HBR are 21 and 24 respectively. This trend is maintained at buffer spaces of 15 and 20 and from the graph, it is clear that CBORF has a smaller overhead ratio than both CBR and HBR. Based on the outcomes of our simulations, CBORF seems to have a better overhead cost controlling capability compared to PARF in periods where there is little buffer space is available. This might be because of the flexibility provided to CBORF in responding to network conditions and make routing decisions according to connected nodes' mobility and other features of the links.

Figures 10 indicates the end-to-end delay results for three routing protocols CBR, HBR and CBORF for different sizes of buffer space. The results also show that CBORF obtains superior overall throughput to CBR and HBR in all the buffer space values with lower end-to-end delay. When buffer space is 5, the CBORF has an end-to-end delay of 7216µs and CBR and HBR are 7120µs and 7340µs respectively. As the buffer space increases to 10, the end to end delay for CBORF is 8673 microseconds and for CBR and HBR only 7901 microseconds and 8123 microseconds respectively. This trend is also observed at buffer spacing of 15 and 20 where CBORF offers lower end to end delay than CBR and HBR. These results confirm that CBORF is better placed in reducing end-to-end delay especially in systems characterized by restricted buffer size. This may be caused due to, potentially, high dynamic characteristics of the CBORF in terms of adjusting the routing decisions to the current state of the network with regards to the mobility pattern, and quality of the links.

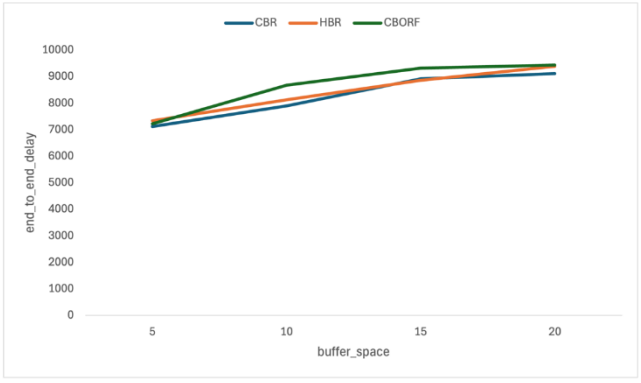

Fig. 10. End to end delay comparison between proposed CBORF and existing HBR and CBR in perspective of devices.

6. CONCLUSION AND FUTURE DIRECTIONS

Therefore, the concepts of a Self-Adaptive CBORF Framework developed for opportunistic IoT networks, but especially for disaster management operations, optimise communication with the target environment and the coordination of rescue operations. Through dynamic message routing based on its content, network condition adaptation and opportunity-based communication, the framework makes IoT systems more efficient, robust and proactive in disaster scenarios. Traditional IoT vision targets at integrating every physical object in the global network. To achieve efficient high throughput with low end-to-end delay a CBORF has been introduced in this paper where a CBD value is obtained by considering number of messages transmitted by the devices from which desired CBD value is selected for determining next hop for data transmission.The proposed system is implemented in the ONE simulator. The results show that in the proposed CBORF, the throughput is high, the end-to-end delay is low, and the overhead ratio is low compared to the state-of-the-art CBR and HBR techniques used. In the future, priority will be given to the development of energy-efficient routing protocols, especially in IoT networks where many devices are battery-powered.

The Self-Adaptive CBORF Framework holds great promise for revolutionizing disaster management operations by enabling more resilient, efficient, and adaptive communication among IoT devices. Future research should focus on optimizing routing strategies to reduce energy

consumption in order to extend device lifetime and reduce maintenance costs. Improve routing by incorporating information about the social interactions and mobility patterns of users in disaster-prone areas. Continued research, innovation, and collaboration across interdisciplinary domains are essential to realize its full potential and address the evolving challenges of disaster preparedness for integration with edge computing, enhanced security, and privacy measures.

REFERENCES

[1] Guo, B., Zhang, D., Wang, Z., Yu, Z., & Zhou, X. (2013). Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things. *Journal of Network and Computer Applications*, *36*(6), 1531-1539.

[2] Ayele, E. D., Meratnia, N., & Havinga, P. J. (2018, February). Towards a new opportunistic IoT network architecture for wildlife monitoring system. In *2018 9th IFIP international conference on new technologies, mobility and security (NTMS)* (pp. 1-5). IEEE.

[3] Wu, J., Xia, J., & Gou, F. (2022). Information transmission mode and IoT community reconstruction based on user influence in opportunistic social networks. *Peer-to-Peer Networking and Applications*, *15*(3), 1398-1416.

[4] Dede, J., & Förster, A. (2017). Comparative analysis of opportunistic communication technologies. In *Interoperability, Safety and Security in IoT: Second International Conference, InterIoT 2016 and Third International Conference, SaSeIoT 2016, Paris, France, October 26-27, 2016, Revised Selected Papers 2* (pp. 3-10). Springer International Publishing.

[5] Sharma, A., Goyal, N., & Guleria, K. (2021). Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes. *The Journal of Supercomputing*, *77*, 6036-6055.

[6] Sharma, A. (2019). Resource utilization of DTN routing protocols by calculating energy consumption of mobile nodes. *Pervasive computing: A networking perspective and future directions*, 47-52.

[7] Sharma, A., & Singh, A. (2019, February). A Contact Based Routing Protocol for High Mobility Scenario in DTN. In *2019 Amity International Conference on Artificial Intelligence (AICAI)* (pp. 371-379). IEEE.

[8] Kalaivani, D., Srinivasan, L., & Saravanan, K. (2022, January). Using multipath TCP and opportunistic routing in IoT network. In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 94-104). IEEE.

[9] Srinidhi, N. N., Sharath, J., & Kumar, S. D. (2021). HMMR: Hidden Markov Model prediction-based routing in opportunistic IoT scenario. *International Journal of Computing and Digital Systems*, *10*(1), 443-454.

[10] Kang, D. K., Kim, H. S., & Bahk, S. (2017, December). ORPL-DT: opportunistic routing for diverse traffic in multihop IoT networks. In *GLOBECOM 2017-2017 IEEE Global Communications Conference* (pp. 1-6). IEEE.

[11] Singh, F., Vijeth, J. K., & Murthy, C. S. R. (2016, April). Parallel opportunistic routing in IoT networks. In *2016 IEEE Wireless Communications and Networking Conference* (pp. 1-6). IEEE.

[12] Kandhoul, N., Dhurandher, S. K., & Woungang, I. (2021). Random forest classifier-based safe and reliable routing for opportunistic IoT networks. *International Journal of Communication Systems*, *34*(1), e4646.

[13] Yang, W., Qin, Y., & Wu, B. (2021). A hyperbolic routing scheme for information-centric internet of things with edge computing. *Wireless Networks*, *27*, 4567-4579.

[14] Adil, M., Song, H., Ali, J., Jan, M. A., Attique, M., Abbas, S., & Farouk, A. (2021). Enhanced-AODV: A Robust Three Phase Priority-Based Traffic Load Balancing Scheme for Internet of Things. *IEEE Internet of Things Journal*, *9*(16), 14426-14437.

[15] Ma, D., Wang, P., Song, L., Chen, W., Ma, L., Xu, M., & Cui, L. (2023). A lightweight deployment of TD routing based on SD-WANs. *Computer Networks*, *220*, 109486.

[16] Vashishth, V., Chhabra, A., & Sharma, D. K. (2019). GMMR: A Gaussian mixture model based unsupervised machine learning approach for optimal routing in opportunistic IoT networks. *Computer Communications*, *134*, 138-148.

[17] Ramkumar, J., & Vadivel, R. (2021). Multi-adaptive routing protocol for internet of things based ad-hoc networks. *Wireless Personal Communications*, *120*(2), 887-909.

[18] Pan, M. S., & Yang, S. W. (2017). A lightweight and distributed geographic multicast routing protocol for IoT applications. *Computer Networks*, *112*, 95-107.

[19] Vrince Vimal, Kamred Udham Singh, Abhishek Kumar, Sachin Kr Gupta, Mamoon Rashid, R.K. Saket, P. Sanjeevikumar, "Clustering Isolated Nodes to Enhance Networks Life Time of WSNs for IoT Applications", IEEE Systems Journal, 15(4), 5654 – 5663, 2021, 10.1109/JSYST.2021.3103696.

[20] Shah, S. B., Chen, Z., Yin, F., Khan, I. U., & Ahmad, N. (2018). Energy and interoperable aware routing for throughput optimization in clustered IoT-wireless sensor networks. *Future Generation Computer Systems*, *81*, 372-381.

[21] Wang, H., Han, G., Zhou, L., Ansere, J. A., & Zhang, W. (2019). A source location privacy protection scheme based on ring-loop routing for the

IoT. *Computer Networks*, *148*, 142-150.

[22] Farooq E., Sahu A., Gupta S. K. "*Survey on FSO Communication System Limitations and Enhancement Techniques*" Optical and Wireless Technologies, Lecture Notes in Electrical Engineering (LNEE), Springer Nature Singapore, Vol. 472, pp. 255-264, 2018. DOI: 10.1007/978-981-10-7395-3_29.

[23] Sharma, D. K., Rodrigues, J. J., Vashishth, V., Khanna, A., & Chhabra, A. (2020). RLProph: a dynamic programming based reinforcement learning approach for optimal routing in opportunistic IoT networks. *Wireless Networks*, *26*, 4319-4338.

[24] Vashishth, V., Chhabra, A., Khanna, A., Sharma, D. K., & Singh, J. (2018). An energy efficient routing protocol for wireless Internet-of-Things sensor networks. *arXiv preprint arXiv:1808.01039*.

[25] Galán-Jiménez, J., Berrocal, J., Garcia-Alonso, J., & Azabal, M. J. (2019). A novel routing scheme for creating opportunistic context-virtual networks in IoT scenarios. *Sensors*, *19*(8), 1875.

[26] Hanif, S., Khedr, A. M., Al Aghbari, Z., & Agrawal, D. P. (2018). Opportunistically exploiting internet of things for wireless sensor network routing in smart cities. *Journal of Sensor and Actuator Networks*, *7*(4), 46.

[27] Sujanthi, S., & Nithya Kalyani, S. (2020). SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT. *Wireless Personal Communications*, *114*, 2135-2169.

[28] Boldrini, C., Conti, M., Jacopini, J., & Passarella, A. (2007, June). Hibop: a history-based routing protocol for opportunistic networks. In 2007 IEEE international Symposium on a world of wireless, mobile and multimedia networks (pp. 1-12). IEEE.

[29] Anuradha Banerjee, Sachin Kumar Gupta, Parul Gupta, Abu Sufian, Ashutosh Srivastava, Manoj Kumar, "UAV-IoT Collaboration: Energy and Time-Saving Task Scheduling Scheme", International Journal of Communication Systems, Wiley, 36(14), 1-24, 2023, (SCIE, IF=2.1) https://doi.org/10.1002/dac.5555

[30] Anuradha Banerjee, Abu Sufian, Ashutosh Srivastava, Sachin Kumar Gupta, Saru Kumari, Sachin Kumar, "An Energy and Time-Saving Task Scheduling Algorithm for UAV-IoT Collaborative System," Microprocessors and Microsystems, Elsevier, 2023, doi.org/10.1016/j.micpro.2023.104875 (SCI, IF=3.503).

[31] Vinay Pathak, Karan Singh, Radha Raman Chandan, Sachin Kumar Gupta, Manoj Kumar, Shashi Bhushan, Sujith Jayaprakash, "Efficient Compression Sensing Mechanism based WBAN System", Security and Communication Networks, Hindawi, 2023, Article ID 8468745, 1-12 https://doi.org/10.1155/2023/8468745

[32] Malik, A., Bhushan, B., Kumar, A., & Chaganti, R. (2022). Opportunistic internet of things (OIoT): elucidating the active opportunities of opportunistic networks on the way to IoT. In *New Trends and Applications in Internet of Things (IoT) and Big Data Analytics* (pp. 209-224). Cham: Springer International Publishing.

[33] Malik, A. (2023). A social relationship-based energy efficient routing scheme for Opportunistic Internet of Things. *ICT Express*, *9*(4), 697-705.

[34] Roopashree S, Anitha J, Sathiyamoorthi V, B Aruna Devi, Ashutosh Srivastava, Sachin Kr. Gupta, Manoj Kumar, "An IoT and Machine Learning based Intelligent System for the Classification of Therapeutic Plants", Neural Processing Letters, Springer, 1-29, 2022, DOI: 10.1007/s11063-022-10818-5.

[35] Internet of Things (IoT): Concept and Applications, pp: 473-489, 2020, DOI: 10.1007/978-3-030-37468-6_25, Publisher: Springer International Publishing, Springer Nature Switzerland AG, Mamoon Rashid, Shabir Ahmad Parah, Aabid Rashid Wani, Sachin Kr. Gupta "Securing E-Health IoT Data on Cloud Systems using Novel Extended Role Based Access Control Model.

[36] Anuradha Banerjee, Abu Sufian, Krishna Keshob Paul, Sachin Kr Gupta, "EDTP: Energy and Delay Optimized Trajectory Planning for UAV-IoT Environment", Computer Networks, Elsevier, 202(2022), pp: 1-17, 108623, https://doi.org/10.1016/j.comnet.2021.108623.

[37] Akshita Gupta, Sachin Kr Gupta, "A Survey on Green UAV-based Fog Computing: Challenges and Future Perspective", Transactions on Emerging Telecommunications Technologies, Wiley, 33(11), pp: 01-29, 2022. Doi:10.1002/ett.4603.

[38] Akshita Gupta, Sachin Kr Gupta "Flying through the Secure Fog: A Complete Study on UAV-Fog in Heterogeneous Networks", International Journal of Communication Systems, Wiley, 35(13), pp: 1-41, 2022, https://doi.org/10.1002/dac.5237

[39] Amina Khan, Sumeet Gupta, Sachin Kr. Gupta, "Emerging UAV Technology for Disaster Detection, Mitigation, Response, and Preparedness" Journal of Field Robotics, Wiley, 39(6), pp: 905–955, 2022 https://doi.org/10.1002/rob.22075.

[40] Amina Khan, Sumeet Gupta, Sachin Kr. Gupta, "Multi-UAV Integrated HetNet for Maximum Coverage in Disaster Management" Journal of Electrical Engineering, 73(2), pp: 116-123, 2022.

[41] Amina Khan, Sumeet Gupta, Sachin Kr Gupta, "Unmanned aerial vehicle-enabled layered architecture-based solution for disaster management," Transactions on Emerging Telecommunications Technologies, Wiley, 32(12), pp: 1-29, 2021. DOI: 10.1002/ett.4370.

[42] Arun Kumar, Sharad Sharma, Nitin Goyal, Sachin Kr. Gupta, Saru Kumari, Sachin Kumar, "Energy Efficient Fog Computing in Internet of Things based on Routing

Protocol for Low Power and Lossy Network with Contiki," International Journal of Communication Systems, Wiley, 35(4), pp: 1-21, 2021, doi.org/10.1002/dac.5049.

[43] Amina Khan, Sumeet Gupta, Sachin Kr. Gupta, "Multi-hazard Disaster Studies: Monitoring, Detection, Recovery, and Management, based on Emerging Technologies and Optimal Techniques", International Journal of Disaster Risk Reduction, Elsevier, 47 (2020), pp: 1-34, 101642, (SCIE, IF=5), https://doi.org/10.1016/j.ijdrr.2020.101642

[44] Saeed Mohammed, Ou Ma, Samar Ansari, Sachin Kr. Gupta, "Collaboration of Drone and Internet of Public Safety Things in Smart Cities: An Overview of QoS and Network Performance Optimization", *Drones*, MDPI, 3(1), 1-18, 2019. https://doi.org/10.3390/drones3010013.

[45] Saeed H. Alsamhi, Ou Ma, M. Samar Ansari, Sachin Kr. Gupta "*Tethered Balloon Technology in Design Solutions for Rescue and Relief Team of Emergency Communication Services*", Disaster Medicine And Public Health Preparedness, Cambridge University Press, Vol. 13, No. 2, pp. 203-210, 2019.

[46] Amina Khan, Sumeet Gupta, Sachin Kr Gupta, "UAV-Enabled Disaster Management: Applications, Open Issues, and Challenges," GMSARN International Journal, 18(1), 44-53, 2024.

[47] Susmita Mondal, Mehak Shafi, Sumeet Gupta, Sachin Kr Gupta, "Blockchain based Secure Architecture for Electronic Healthcare Record Management," GMSARN International Journal, 16 (4), 413-426, 2022.

[48] Amina Khan, Sumeet Gupta, Sachin Kr. Gupta, "Disaster management solution based on collaboration between SAR team and multi-UAV", Futuristic Communication and Network Technologies. VICFCNT 2021. Lecture Notes in Electrical Engineering, Springer, Singapore, 471-481, vol 995, 2023. https://doi.org/10.1007/978-981-19-9748-8_44.

[49] Amina Khan, Sumeet Gupta, Sachin Kr. Gupta, "Cooperative Control between Multi-UAVs for Maximum Coverage in Disaster Management: Review and Proposed Model," IEEE 2nd International Conference on Computing and Information Technology (ICCIT), University of Tabuk, Tabuk, Saudi Arabia, pp: 271 – 277, 25-27 Jan. 2022, DOI: 10.1109/ICCIT52419.2022.9711627.

[50] Sachin Kumar Gupta, Parul Gupta, Pawan Singh, "Enhancing UAV-HetNet Security Through Functional Encryption Framework," Concurrency and Computation: Practice and Experience, Wiley, 00(00), pp: 01-22, 2024, https://doi.org/10.1002/cpe.8206.

[51] Akshita Gupta, Sachin Kumar Gupta, "UAVs in collaboration with Fog computing network for improving QoS", International Journal of Communication Systems, Wiley, 37(9), pp: 01-19, 2024, https://doi.org/10.1002/dac.5759.

[52] Itika Sharma, Sachin Kumar Gupta, "SFL-MDrone: Synchronous Federated Learning Enabled Multi Drones", Journal of Intelligent & Fuzzy Systems, 46(04), pp: 8543-8562, 2024, DOI:10.3233/JIFS-235275.

[53] Farheen Syed, S. H. Alsamhi, Sachin Kumar Gupta, Abdu Saif, "LSB-XOR Technique for Securing Captured Images from Disaster by UAVs in B5G Networks", Concurrency and Computation: Practice and Experience, Wiley, 36(12), pp: 01-13, 2024, https://doi.org/10.1002/cpe.8061.

[54] Itika Sharma, Sachin Kumar Gupta, "Channel Tracking in IRS-based UAV Communication Systems using Federated Learning", Journal of Electrical Engineering, 74(06), pp: 521-531, 2023.

[55] Madhumitha Kulandaivel, Ganesh Kumar, V. Sathiyamoorthi, Sachin Kumar Gupta, "A Novel Sensitive DDoS Attacks against Statistical Test in Network Traffic Fusion", Transactions on Emerging Telecommunications Technologies, Wiley, 34(12), pp: 01-19, 2023, Doi: 10.1002/ett.4867.

[56] Vinod Kumar, Sachin Kumar Gupta*, Abid Hussain, Amit Sharma, "A systematic approach to prevent threats using IDS in IoT based devices", GMSARN International Journal, 19(01), 107-112, 2025.