



iSocialDrone: QoS aware MQTT middleware for social internet of drone things in 6G-SDN slice

Amartya Mukherjee^{1,2} · Nilanjan Dey³ · Atreyee Mondal⁴ · Debashis De¹ · Rubén González Crespo⁵

Accepted: 15 July 2021 / Published online: 2 August 2021

© The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2021

Abstract

The Internet of Things (IoT) paradigm is a predominant research domain for smart cities, smart villages, society, and industry 4.0. The introduction of Unmanned Aircraft Systems (UAS) in an ultra-low latency network with fog, dews, and edge computing gives the researcher ample scope to establish a decentralized architecture for ultra-high-speed message exchange between IoT devices. This work mainly focused on Social Internet of Things ecosystem and its design to efficiently handle large group social gatherings, events, and emergency service management. We propose a layered message transfer framework for the social IoT scenario. We also establish network connection through flying ad hoc network architecture. The standard IoT message transfer protocol is redesigned by amalgamating with an opportunistic routing mechanism and deployed within 6G software-defined network (SDN) slice. We use seven distinguished network slices for different services and corresponding access. The study reveals nearly 99% of message delivery rate with a latency upper bound of 2300 ms by opportunistic message transfer scheme in a dense network scenario for QoS 2. It also shows 95% of the bandwidth utilization per slice and 97% of network coverage under SDN in quality of service level 2.

Keywords SIoT · SIoDT · Opportunistic forwarding · MQTT-QoS · SDN · Network slice

Communicated by Oscar Sanjuán Martínez.

✉ Amartya Mukherjee
mamartyacse1@gmail.com

Nilanjan Dey
neelanjan.dey@gmail.com

Atreyee Mondal
atreyee.shakshi@gmail.com

Debashis De
dr.debashis.de@ieee.org

Rubén González Crespo
ruben.gonzalez@unir.net

¹ Maulana AbulKalam Azad University of Technology, Kalyani, West Bengal, India

² Institute of Engineering and Management, Kolkata, India

³ JIS University, Kolkata, India

⁴ Techno International, New Town, Kolkata, India

⁵ Universidad Internacional de La Rioja, Logroño, Spain

1 Introduction

Over the past few decades, Internet of Things (IoT), also recognized as the Internet of Everything, becomes an emerging technology domain in communication and embedded technology, where heterogeneous devices can globally interact with each other with built-in intelligence. Various industries are adopting IoT technology to build a global network of interconnected and integrated devices, including smartphones, body sensors, smart embedded objects, smart-watches, and many more. Heterogeneous interconnection between devices helps society grow a hyper-connected cyber-physical-social environment using heterogeneous and communication protocols (Gubbi et al. 2013). Recently, abstraction of the Internet of things and social networks is merging to form a socialized and collaborated integration of devices which is known a Social Internet of Things. SIoT is an emerging subset of IoT where globally interconnected devices establish a social relationship. SIoT is gaining significant attention from numerous industries for having wide application areas of hyper-connected smart societies such as smart city, smart community, healthcare and telemedicine, smart multimedia

streaming, and system (Ali 2015). The most fundamental and challenging SIoT-enabled smart system requirement is the relationship management and establishment of trustworthiness among the integrated smart objects (Afzal et al. 2019; Ruiz et al. 2021). We establish different types of relationships between connected objects such as ownership, and social object relation. These are further extended to provide on-demand services by enhancing network navigability (Gulati and Kaur 2021). SIoT-enabled smart heterogeneous devices globally connected and collaborated to achieve a common goal that is mutually beneficial for all the interconnected objects (Roopa et al. 2019). However, there are some major challenges faced by the developers while establishing social connectivity among objects. The SIoT objects support heterogeneous communication protocols with various deployment features, which is the fundamental concern for establishing a complex IoT-enabled society. Apart from the diversity of perspectives, there is also a growing demand to increase the number of devices under the same network causing scalability concerns. The autonomous interaction among devices, beneficial for human users, covers both human–object and object–object relationships (Marche et al. 2018). Trustworthiness is one of the key functionalities of SIoT architecture, which defines the good collaboration and socialization of SIoT devices (Bao et al. 2013). Some emerging subset of IoT includes Internet of Drone Things (IoDT) (Mukherjee et al. 2020a), Internet of Robotic Things (IoRT) (Simoens et al. 2018), Internet of Public Safety Things (IoPST) (Alsamhi et al. 2019; Kantarci and Mouftah 2014), Internet of Nano Things (IoNT) (Miraz et al. 2015), Internet of Underwater Things (IoUT) (Kao et al. 2017), Internet of Medical Things (IoMT) (Joyia et al. 2017), Internet of Cloud Things (IoCT) (Pawlick et al. 2018), and Internet of Mobile Things (IoMBT) (Nahrstedt et al. 2016).

Unmanned Aerial Vehicles, also known as drones, are the key part of IoDT. Drones are mainly equipped with remotely controllable IoT devices, provide services in different civilian sectors, monitor and surveillance in industrial areas, managing wildfire, etc. The Internet of Drone Technology refers explicitly to a layered network architecture that coordinates the sensor services and UAV navigation. The drones can be considered a node that stores and redirects the sensor's information by using an ad hoc attribute to the UAV. This feature is also known as flying ad hoc network (FANET). FANET (Bekmezci et al. 2015) is a specialized subset of MANET and VANET, which can be effectively used to establish a multi-layered UAV communication network because of its high degree of mobility. Three extensive networks layered approach is followed on the Internet of Drone Technology (IoDT), namely mobile network, aerial sensor network, and Internet

(Quaritsch et al. 2010). In SIoT, each UAV is considered a set of flying ad hoc network nodes interconnected and collaborates and socializes via sensors to perform a mutually beneficial specific task. With the invention of 6G networks, SIoT can reshape society with superior performance (Katz et al. 2018). IoT-enabled devices, such as multi-UAV systems, can communicate more effectively using sixth-generation networks. These technologies facilitate the Social Internet of Drone Thing (SIoDT) services via wireless media. It also enables maximum data transfer rate even in a sparse network scenario. The communication between 6G wireless networks facilitates multi-UAV communications with nearly zero infrastructures, specifically in an emergency (Song et al. 2020; Akyildiz et al. 2002).

1.1 Motivation and contribution

The primary contribution of this work is to design a UAV-enabled seamless communication framework that can sense and transfer data captured by the sensor or intelligent devices. We have developed a framework, which acts as middleware in this case. This framework leverages the features of core IoT protocols amalgamate with opportunistic routing phenomena, which can efficiently work in a highly dynamic and sparse network topology. The ultra-low latency 6G network architecture is an obvious choice for developing such an ecosystem because message transfer in a highly sparse network can only be possible with the ultra-low latency software-defined network (SDN). Therefore, we have critically included SDN in our work to validate the effectiveness of the proposed framework.

Rest of the article is organized as follows: Section 2 describes the related research; Sect. 3 emphasizes the Social Internet of Drone things modeling. Section 4 shows the experimental setup and the performance metrics. Section 5 describes the performance analysis of different methodologies. Finally, discussions and the conclusion are made in Sects. 6 and 7, respectively.

2 Related work

In recent decade, the Internet of Drone Things enhanced a significant research field where the integrated objects are always related to drones. All the associated works, such as globally interconnecting through sensors, and message transfer, are performed either explicitly or implicitly by the UAV(s). Social IoDT is an emerging subset of IoDT. A multi-UAV system acts as a heterogeneous group of devices where each device collaborates and socializes to perform the same task. An implementation named Dragnet for amateur drone surveillance using the cognitive Internet

of Things is done (Ding et al. 2018; García et al. 2019). The concept behind Dragnet is that the surveillance devices, i.e., drones, are interconnected and can learn, think, understand global decisions, and work like it have brains with minimum human intervention. In (Motlagh et al. 2017), an IoT-enabled UAV architecture is performed, focusing on crowd surveillance for suspicious activity monitoring. A cloud-based framework is proposed in Luo et al. (2015) to perform disaster monitoring with limited UAV resources. The power consumption and processing time of UAVs are more challenging for the developers in this domain. An energy-efficient UAV-based IoT framework is proposed in Motlagh et al. (2016); here, the authors highlight a selection technique of UAV for a specific goal. A comprehensive survey related to significant challenges and future perspectives of IoDT is illustrated in (Motlagh et al. 2016b). Mukerjee et al. (2020) propose a hybrid model named iGridEdgeDrone for building intelligent grid networks using IoDT.

IoDT comprises a layered network structure where each layer retrieves data from the previous layer (Gharibi et al. 2016). In another work, the author proposes an ad hoc network named FANET for the interconnection between multi-UAV system for communicating with the base station and satellites in a highly dynamic environment (Bekmezci et al. 2013). FANET is a subset of mobile ad hoc networks (MANET) and Vehicular ad hoc networks (VANET) with a superior mobility degree. A real-time CNN-based detection model named Dronet is proposed in Kyrkou et al. (2018) for UAV-based vehicle detection applications such as emergency response, and traffic monitoring. The concept of IoDT is much similar to IoD, but in IoDT the edge and fog layer are present with the perception layer. Aerial sensor network plays a vital role in the multi-UAV-based IoT system for localization, path planning, and sensor data aggregation (Mukherjee et al. 2020c). An aerial sensor network is used as a mobile sensor network that moves around the environment, senses using sensors present in UAVs and then finally, transfers the collected data to the ground base (Cabreira et al. 2018). In another work (Hua et al. 2018), authors propose an energy-efficient sensor network scheduling approach. Some factors like packet delivery ratio, low delay in delivery, and packet loss need to be considered for the increment of the collaborating devices. Several routing protocols are used in FANET, categorized as topology-based routing protocols, swarm-based routing protocols, and position-based routing protocols. A comprehensive study of different routing protocols is addressed in Oubbati et al. (2017). The routing in a UAV network is highly challenging due to the highly dynamic mobility of UAV nodes.

In some cases, the connections become intermittent, and the chance of message loss is high. In such a scenario, the

traditional routing mechanism fails most of the time. Therefore, another most critical challenge in a multi-UAV system is trustworthiness. A fuzzy-based system is presented in Singh and Verma (2018) to control the behavioral unpredictability of FANET nodes, i.e., UAVs. Furthermore, the author proposes a topology construction model based on a nature-inspired particle swarm optimization algorithm (Srivastava and Prakash 2021) for end-to-end communication between UAVs and ground control stations.

UAVs have broadly three communication architectures, named UAV ad hoc Network, multi-group UAV ad hoc network, and multi-layer UAV ad hoc network (Khan et al. 2021; Pereira et al. 2019). SIoDT majorly follows a robust multi-layer UAV ad hoc network where UAVs' heterogeneous connection is natural without a single point of failure. With the invention of the 6G network development, almost everything is connected, and we are moving a step forward toward a fully digital society. An emerging technology integrated into 6G networks, known as software-defined networks (SDN), is used for network flexibility, centralized network control, and program the network for application development (Alomari et al. 2021). SDN plays a significant role in future Internet by solving significant challenges like ubiquitous accessibility, excessive bandwidth, and dynamic instantiation (Zhang et al. 2019).

Furthermore, 6G networks play an essential role in establishing communication in multi-UAV systems by overcoming the power consumption issue caused by propulsion and direction adjustment. In research (Alzenad et al. 2018), the authors introduce an approach where they use point-to-point free-space optics (FSO) to transmit information between UAVs with excessive data rates in different weather situations. However, due to high mobility, network security management is a critical concern in UAVs, which requires software-defined networking. Network function virtualization (NFV) is a cost-effective solarization technique to fulfill network security to vulnerable UAVs at less expense. Furthermore, NFV provides flexible, dynamic, and instant decision capabilities to the UAVs by using user authentication, access control mechanisms for effective and secure communication (Kumari et al. 2020).

3 Social internet of drone things modeling

Internet of Drone is a new paradigm in the recent advancement of the IoT era. Internet of Drone Things (IoDT) is the specialized concept where the drones can make an ad hoc network connection and have additional features like sensing, and local level processing as an edge device. The idea of social IoT fundamentally deals with the

massive cluster of people’s social behaviors and social gatherings in a closed area (Cheng et al. 2019).

We can often realize a social structure like a crowded football ground, congested traffic, a crowded shopping mall before Christmas, Durgapuja, emergency evacuation of mob due to fire, and earthquake (López-Quintero et al. 2018). The deployment of FANET-based SIOdT is highly relevant in this context for better signal coverage. Figure 1 depicts situations where we can physically build several network slices under a single 6G backbone. Each slice, in this case, provides a dedicated service and comprises the network of drones to transfer and stream the messages effectively.

In the proposed work, the concept of SIOdT comprises three distinct components. In the first part, the primary concern is drone mobility and routing. To achieve this, we establish a group of Flying ad hoc networks of ‘n’ nodes in the perception layer. Here, the key role is to sense and gather the data based on the social relationship of the people and the community within a society and city. In such cases, the ecosystem assigns a dedicated FANET for data gathering. We primarily deployed FANETS that are under ‘n’ ultra-low latency massive MIMO network considered the network layer. The network is segregated into several software-defined networks (SDN) slices based on

the social feature and utility. The FANET nodes are part of IoDT. The data gathered by the node also can process the drone nodes. Therefore, an edge sub-layer is considered a part of the network layer that can perform processing within the network’s edge. The processed information is then transmitted to the higher layers (dew, fog, and cloud layers) using the same low latency network. Finally, the network itself also comprises static hardware infrastructure on which we use virtualization. The core part of the software-defined network slice illustrates SIOdT in Fig. 2. SDN controller, access and core network, virtual computation, and storage infrastructure, and slice controller are the key components here. We have discussed more on SDN in Sect. 3.2.

As mentioned previously, the fundamental objective of our work incorporates the selection of the proper message transfer strategy in a highly dynamic topology for social FANET so that they can perform data gathering and social action of the objects. In addition to that with proper Quality of Service in routing is another crucial objective. In a FANET, IoDT nodes often form a sparse network topology. Therefore, to efficiently perform the message relay with a proper QoS, an enhancement of the standard protocol is highly required. Consequently, we re-engineered the standard MQTT messaging policy so that they can

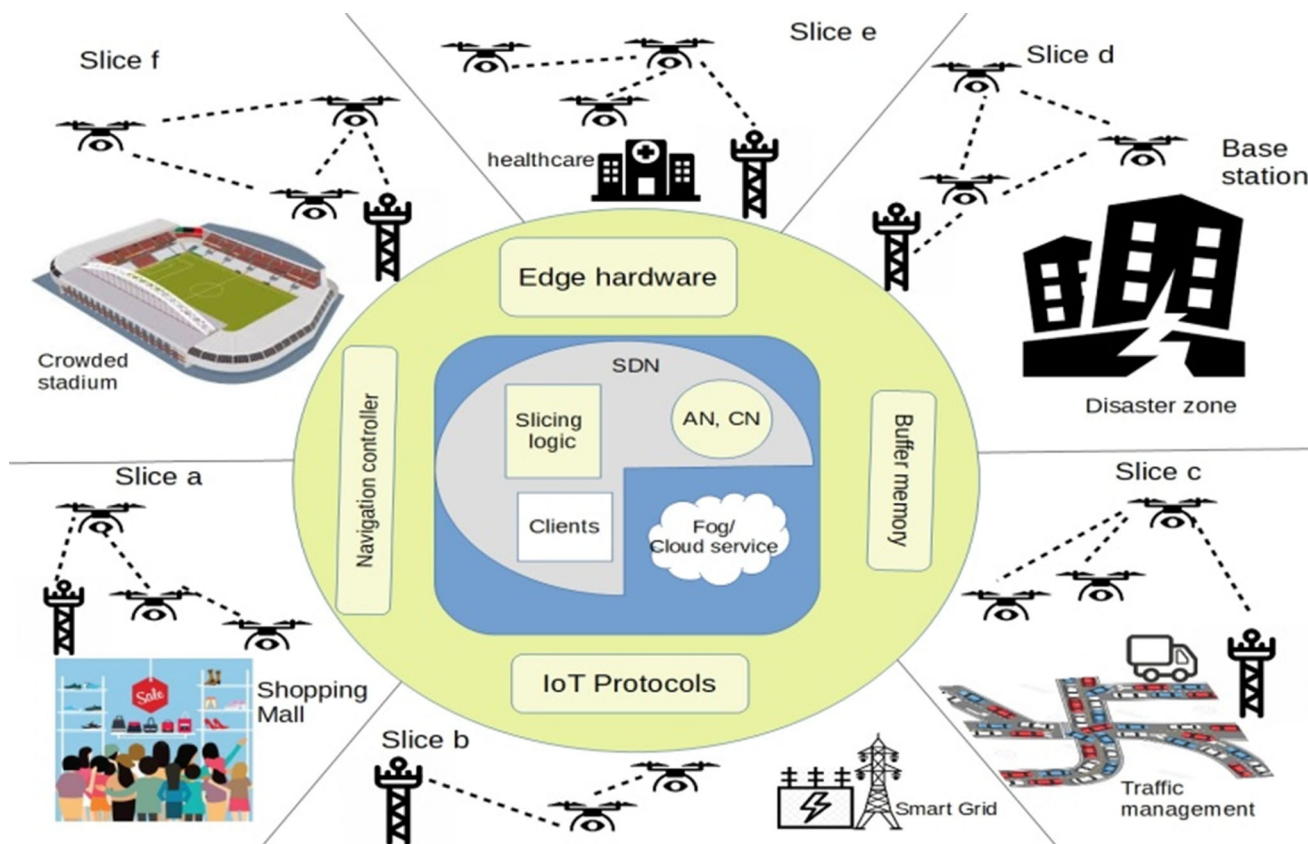


Fig. 1 FANET-based Social IoDT deployment scenario under 6G network infrastructures

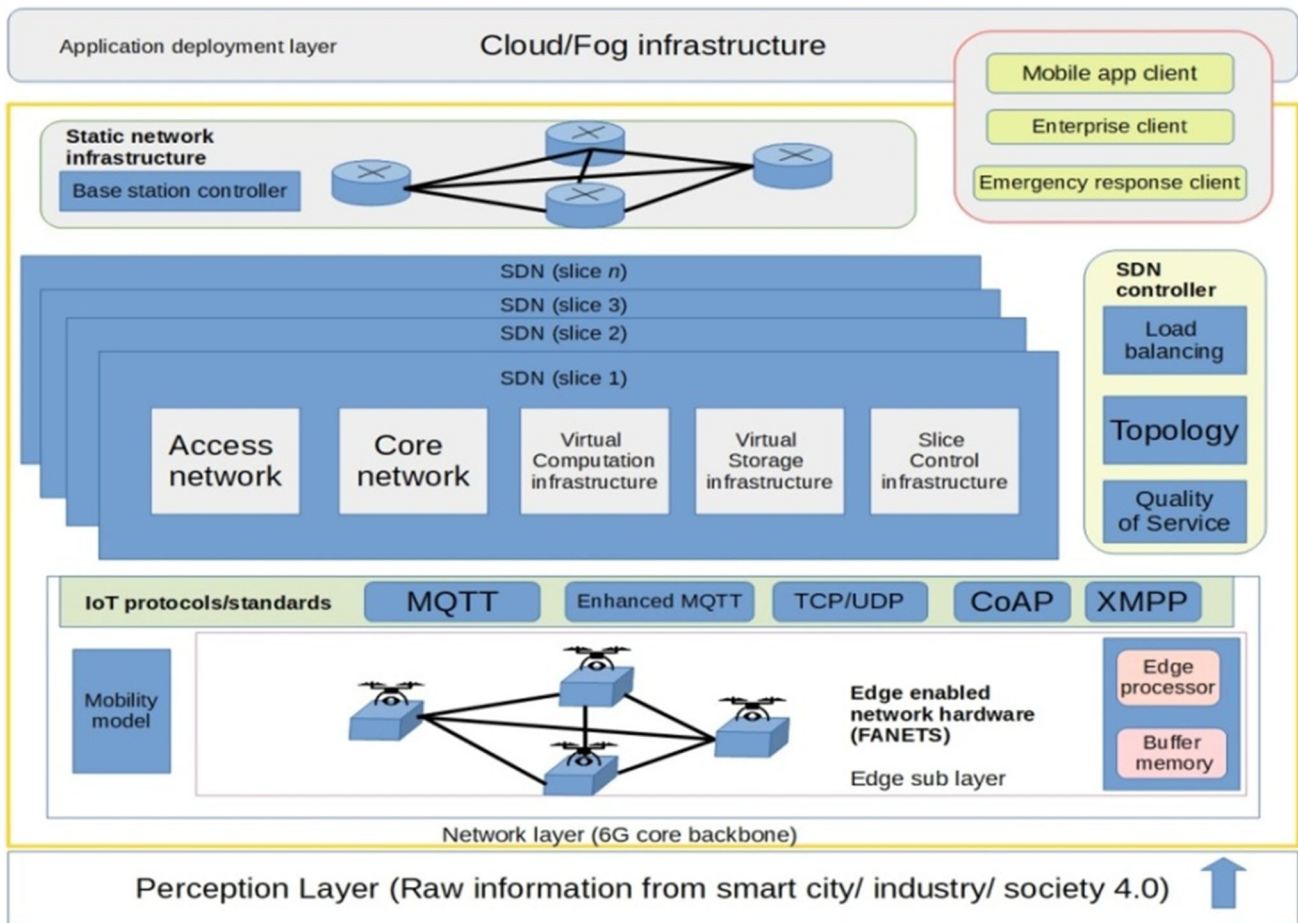


Fig. 2 Social IoDT ecosystem with SDN slices comprises of services, access network, and the core networks

work optimally in a dense and sparse, and highly dynamic network scenario.

3.1 Opportunistic IoDT design

We choose an appropriate selection of the opportunistic routing for the message transfer under IoDT. The performance of the standard MQTT protocol gets sacrificed in a FANET due to its high degree of mobility. In such a case, broadcast messages from one node to another node may not reach in proper time. Thereby the time to live (TTL) gets expired, and the message gets dropped. This problem becomes even more critical when the network is sparse. The opportunistic routing scheme is the best approach for precise message transfer. The enhanced protocol, in this case, ensures a high message delivery probability. We have employed two renowned message routing mechanisms, namely MaxProp and Spray and Focus (Mukherjee et al. 2019; Avasalcai et al. 2019). Therefore, we amalgamate the existing functionality of the MQTT protocol with the opportunistic message transfer scheme to improve the QoS in a highly dynamic network topology. The new

terminology for those message transfer mechanisms is termed MP-MQTT and SF-MQTT, respectively. The MaxProp strategy increases the chance of delivering the message in a challenging scenario where network coverage is low. Three key things are involved: neighbor discovery, data transfer, and storage management, which we can explain with the standard mathematical model. If 'n' is the number of nodes, each of the nodes $i \in n$ keeps tracking the contact probability $\in n$. Now, we have to set $f_j^i = \frac{1}{|n|+1}$ where f_j^i is considered as the likelihood of a connection between i and j . Each time i encounters j , $f_j^i \leftarrow f_j^i + 1$. The cost to each path along d direction has computed as

$$c(i, i + 1, \dots, y) = \sum_{x=i}^{y-1} (1 - (f_{x+1}^x)) \tag{1}$$

Therefore, we can compute the cost of transferring the message toward the destination y as

$$(y) \leftarrow \min(c(i, i + 1, \dots, y)) \tag{2}$$

The second message transfer scheme that works with MQTT will also significantly improve message delivery by

utilizing maximum bandwidth and minimum forwarding latency (Bao et al. 2013; Kumari et al. 2020). The transfer scheme maintains a summary vector between nodes based on the rapid flooding rule. Each time before the message transfer, a timestamp token has to be sent to all nodes present within the communication range in a particular instance of time. The model then chooses the best message forwarder as a subscriber of the message in such a case based on the timestamp and the forwarder distance. For example, if p and q are two nodes considered a publisher and the subscriber, the encounter distance Δ_{pq} and the timer τ_m have to be computed with an incremental timestamp value.

While a node encounters with a source node, the model immediately checks the timestamp value, and the minimum timestamp valued nodes are considered a better forwarder based on the following relation

$$\tau_m(N) = \tau_m(j) - \tau_m(i) + \Delta_{pq} \quad (3)$$

where $\tau_m(N)$ can be considered as the newly computed times value for the encounter to the forwarder. In this way, the best forwarder or subscriber of the message has to be chosen based on the relation

$$\tau_m(sub) = \min[\tau_m(N_1), \tau_m(N_2), \dots, \tau_m(N_x)] \quad (4)$$

where x is the number of subscriber nodes encountered within a particular instance of time, algorithm 1 is showing

Algorithm 1: Opportunistic message transfer strategy 1 (MP-MQTT)

```

1. input : msg,  $\alpha \leftarrow 0.5$ ,  $n\_node \leftarrow \{nodeset, \phi\}$ 
2. output:  $c\_msg$ (message tx/rx cost),  $sub\_id$ ,  $sv()$  (summary vector)
3. start
4. for  $t$  until  $end\_sim\_time \wedge remove(n\_node) \neq \phi$ 
5.    $node(i) \leftarrow node(j) \leftarrow next(\{nodeset\})$ 
6.   for  $i = 1$  to  $node(i)$ 
7.     for  $j = 1$  to  $node(j)$ 
8.        $prob(sv(node(i-j))) \leftarrow prob_{old}(sv(node(i-j))) + \alpha$ 
9.        $f = \frac{1}{|prob(sv(node(i-j)))| + 1}$ 
10.       $dst = \sqrt{loc(node(i))^2 + loc(node(j))^2}$ 
11.      if ( $dst < 0.5$ )
12.         $f \leftarrow f + 1$ 
13.      end if
14.      for  $x = node(i)$  to  $node(j)$ 
15.         $c(i) = c(i-1) + (1-f)$ 
16.      end for
17.    end for
18.  end for
19.  $c\_msg \leftarrow \min(c[1 \dots x])$ 
20.  $sub\_id \leftarrow format(c\_msg)$ 
21. update ( $sv(node(sub\_id))$ )
22.  $mqtt\_call(sub\_id)$ 
23. defmqtt_call:
24.   call pub (broker, QoS, topic)
25.   if  $sub\_id = sv(node(sub\_id))$ 
26.     call sub(broker, topic)
27.   end

```

Algorithm 2: Opportunistic message transfer strategy 2 (SF-MQTT)

```

1. input :  $p, q, init\_tm, n\_node \leftarrow \{nodeset, \phi\}, loc(p), loc(q)$ 
2. output:  $tm(sub)(timestamp), sub\_id, sv()(summary\ vector)$ 
3. start
4. for  $t$  until  $end\_sim\_time \wedge remove(n\_node) \neq \phi$ 
5.    $tm_x \leftarrow init\_tm$ 
6.    $broadcast(tm_x)$ 
7.    $buffer(state)$ 
8.    $receive(tm_y)$ 
9.    $dst = \sqrt{loc(p)^2 + loc(q)^2}$ 
11.   $tm_n = tm_x - tm_y + dst$ 
12. end for
13.  $tm(sub) \leftarrow \min[tm_n(n\_node)]$ 
14.  $sub\_is \leftarrow format(tm(sub))$ 
15.  $sub\_id \leftarrow format(c\_msg)$ 
16.  $mqtt\_call(sub\_id)$ 


---


17. defmqtt call:
18.  $call\ pub(broker, QoS, topic)$ 
19. if  $sub\_id = sv(node(sub\_id))$ 
20.    $call\ sub(broker, topic)$ 
21. end

```

the message transfer strategy 1. Algorithm 2, on the other hand, reflects the message transfer strategy 2.

3.2 Implementation of SDN

The SDN fundamentally comprises of slices that logically share the channels and the network resources (Nguyen et al. 2017). The slicing of the network enables the heterogeneity of the functions and operations within a shared infrastructure. We have created seven distinguished Network Slice Instance (NSI) under a single MIMO infrastructure in this work. We have generated SDN through NFV, and each network has its own virtualized resources shared across the slice. The cross-domain network slices (Gligoroski and Kravlevska 2019; Zhirnov et al. 2019; Luo et al. 2018) provide seven services: smart-grid communication, healthcare, transport, e-commerce, education, disaster response application, and infotainment for society 4.0. The SDN slices are distinctively identified as a combination of the services (SR), core networks (CN), and access networks (AN). While assigning the service under a slice, we have to consider it as a Latin rectangle table to identify the benefits under a particular AN and CN quickly and distinctly. There are two different cases we can consider to slice the network and allocate the services.

Firstly, we can have dedicated CN and the AN for each service so that one particular service can able to avail the functionality of the CN and AN. Secondly, an imbalance in resource allocation happens when we assign more than one service within a single AN or CN. Obviously, in such

cases, either the resource of either AN or CN or both have been shared. Such an approach is often called soft slicing. Tables 1, 2 depict the hard and soft slicing through the Latin square method considered in our scenario.

To understand the mathematical model, we can consider the slice as Σ , which is a three-variable tuple, and we can represent it as $\Sigma = \{S, A, C\}$ where $S = \{s_1, s_2, \dots, s_n\}$, $A = \{a_1, a_2, \dots, a_n\}$, and $C = \{c_1, c_2, \dots, c_n\}$ is the set of service, AN and CN, respectively. Therefore, the hard-core network slicing can be obtained by

$$\Sigma_{HCS} = \{ (s_i, a_i, c_i) : s_i \in S, a_i \in A, c_i \in C \} \quad (5)$$

where minimum two tuple $\{(s_1, a_1, c_1) \text{ and } (s_2, a_2, c_2)\} \in \Sigma_{HCS}$ and the following condition should hold:

Table 1 Hard slicing of seven different services under specified AN and CN

Access network	Core network						
	C ₁	C ₂	C ₃	C ₄	C ₅	C ₆	C ₇
A ₁	S ₁						
A ₂		S ₂					
A ₃			S ₃				
A ₄				S ₄			
A ₅					S ₅		
A ₆						S ₆	
A ₇							S ₇

$$\forall s_i = s_j : a_i \neq a_j \wedge c_i \neq c_j$$

$$\forall a_i = a_j : s_i \neq s_j \wedge c_i \neq c_j$$

where s_i, a_i, c_i are the i th instances and s_j, a_j, c_j are the j th instances of service, AN, and CN, respectively.

In the same way, we can perform the AN slicing using $\Sigma_{HAS} = \{ (s_i, a_i, c_i) : s_i \in S, a_i \in A, c_i \in C \}$ where minimum two tuple $\{(s_1, a_1, c_1) \text{ and } (s_2, a_2, c_2)\} \in \Sigma_{HCS}$ and the following condition should hold:

$$\forall s_i = s_j : a_i \neq a_j \wedge c_i \neq c_j$$

$$\forall c_i = c_j : s_i \neq s_j \wedge a_i \neq a_j$$

Also, it is possible to prove that if $\Sigma_{HS} = \{ (s_i, a_i, c_i) : s_i \in S, a_i \in A, c_i \in C \}$ is a hard network slice, then $\exists a^- (\acute{S}, \acute{A}, \acute{C})$ such that $\acute{S} \subseteq S, \acute{A} \subseteq A,$ and $\acute{C} \subseteq C$.

It is evident that while creating a hard slice Σ_{HAS} , we can consider a vector of services λ that maps to AN and CN. In such case, the service set $\acute{S} \subseteq S$, will always hold. The AN and CN set also flows the same rule. Therefore, the list λ contains either an empty cell $\{\phi\}$ or have a single symbol $\in S$. Hence, we can conclude the conjugate $^- (\acute{S}, \acute{A}, \acute{C})$ exists so that $\acute{S} \subseteq S, \acute{A} \subseteq A,$ and $\acute{C} \subseteq C$ holds. Algorithm 3 presents the slicing mechanism under dedicated AN and CN.

Table 2 Soft slicing of seven different services under specified AN and CN

Access network	Core network						
	C ₁	C ₂	C ₃	C ₄	C ₅	C ₆	C ₇
A ₁	S ₁						
A ₂		S ₂					
A ₃			S ₃				
A ₄				S ₄			
A ₅				S ₅	X		
A ₆					S _{6, S₇}	X	
A ₇							X

4 Experimental setup and performance metric

We have carried out the simulation experiment in two phase. Firstly, we deploy the IoDT nodes in a smart city scenario through an opportunistic network simulator. We have segmented the client nodes into seven distinct social groups, and the dedicated IoDT networks are assigned to each group. We choose the shortest path map-based mobility for each group to realize more accurate social behavior. The reason behind that is to find out the optimal sequence of the path to reach a particular destination. The time complexity of such a model lies in between $O(e \log v)$ to $O(v^2)$. Table 3 shows the simulation parameters for IoDT nodes under the smart city scenario. In phase 2, we

Algorithm 3: Slicing under dedicated AN and CN

```

1. Input: user, rad, cent; output : active_slice, a(cov_ratio)
2. active_slice ← {ϕ}
3. rej_clinet ← {ϕ}
4. start
mod1:
5. for t = 0 to sim_time - 1
6.   req ← get_req(si, ai, ci)
7.   for req = (si, ai, ci) ∈ (S, A, C)
8.     if index(ci) ∧ index(ai) = index(si)
9.       active_slice ← active_slice ∪ req
10.    else
11.      req_count ← req_count + 1
12.    rej_client ← rej_client ∪ req
mod2:
13.  cov = √(∑1active_slice (rad - cent)2)
14.  covpu = cov/user
15.  a = covpu/active_slice
16.  return a
17. end
    
```


Table 3 Standard simulation parameters for IoDT nodes

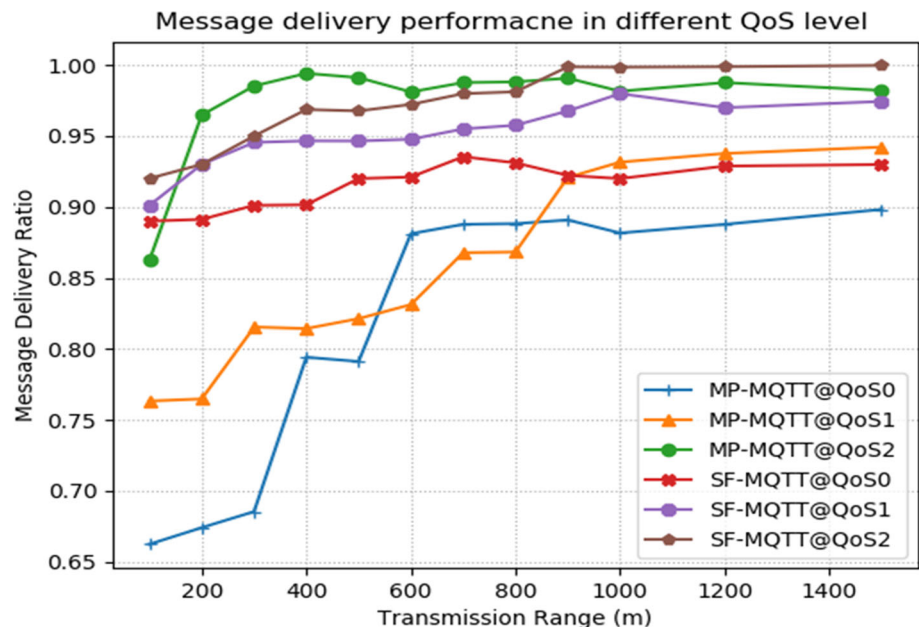
Parameter	Value
Simulation time	43, 200 (12 h)
Number of IoDT node	100–2000
Number of social groups	7
Low-speed interface transmission range	100 m
High-speed interface transmission range	500–1500 m
Low-speed interface transmission speed	500 Mbps
High-speed interface transmission speed	2–4Gbps
Message Buffer size	0.5 GB–3 GB
IoDT node Speed	2kmph–75kmph
Simulation Area	3, 920, 400 (m ²)

Table 4 Simulation parameters for SDN

Parameter	Value
Simulation time (min)	100
Number users	200–6000
QoS level	0, 1, 2
Assigned bandwidth (GHz)	10 ⁸ G
Number of slices	7
Delay tolerance (sec)	20 s
Simulation area (m)	1980 × 1980

assign the dedicated frequency slot to each of the seven groups in the form of an SDN slice.

Fig. 3 Message delivery performance of enhanced message transfer strategies in various Quality-of-Service levels under varying transmission ranges

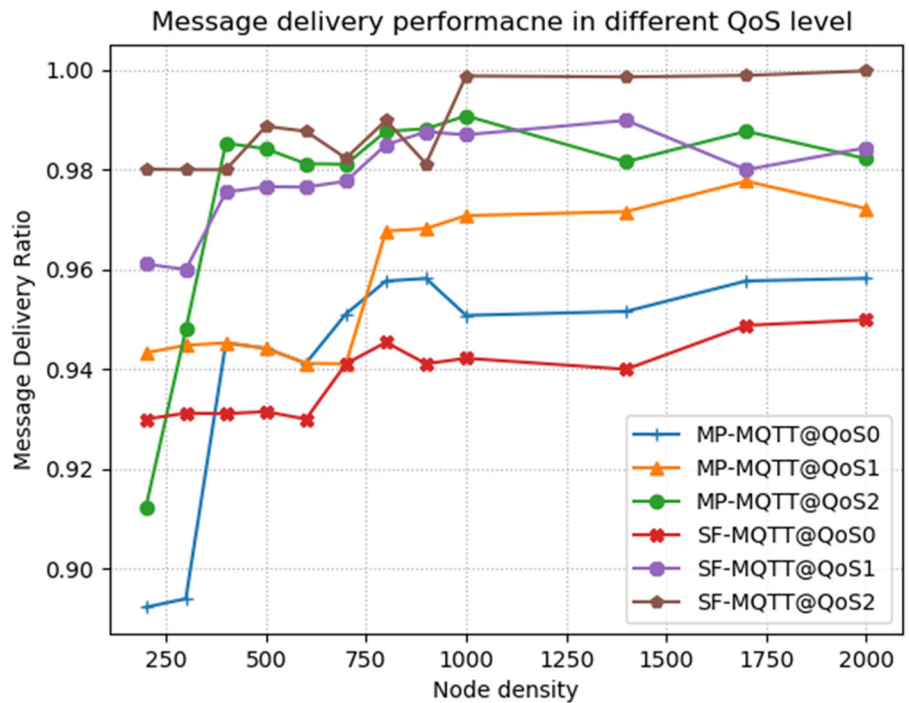


The slices, in this case, are considered hard slices. In our experimental scenario, we have statically created seven slices for seven different services. We distribute the size of each slice equally with the equal segment and incremental frequency values. Furthermore, each slice has its own dedicated AN and CN. As the philosophy of 6G ensures network availability anywhere irrespective of ground, underground /underwater, and deep space, ultra-low latency opportunistic message transfer is the key ingredient. We have modeled the system to achieve an opportunistic capability by leveraging an ultra-high-frequency band. Table 4 depicts the functional parameters of the SDN slice. To simulate SDN, we have used the Slicsim simulator. The simulator is a python-based open-source simulator where we create a slicing scheme as a script and give all parameters into a yaml script file to execute.

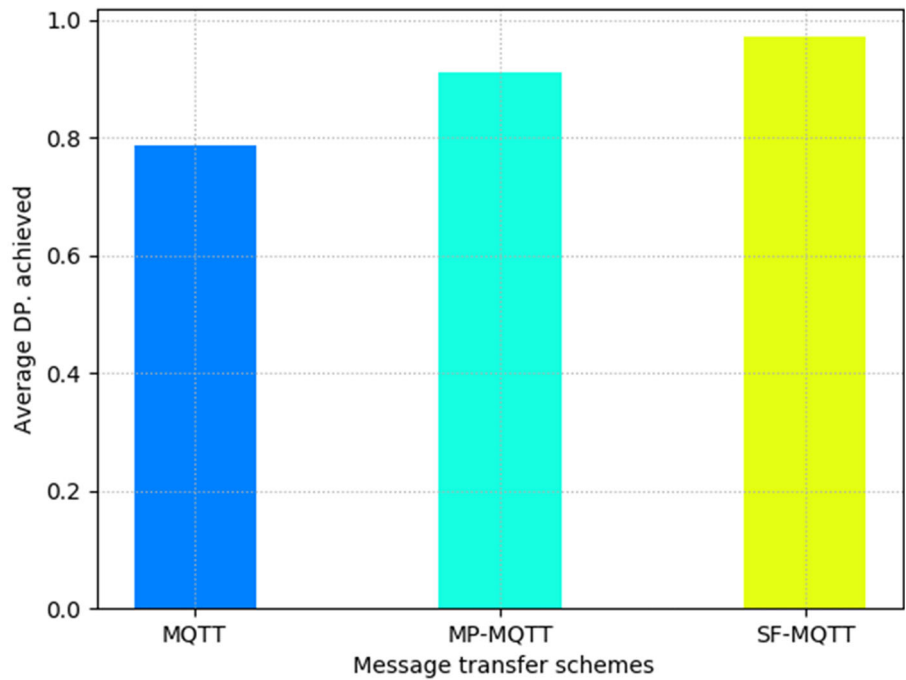
5 Performance analysis

We have made the performance analysis in two phases. In the first phase, we analyze the performance of the enhanced message transfer strategy over the proposed ecosystem. Then, we have done the simulation. We have considered the IoDT nodes here as the subset of the entire node group. Majorly, they are either fixed-wing or multi-rotor lightweight drones. Other nodes are in the class of human nodes, vehicular nodes, and base stations.

Fig. 4 a The impact of node density on the message delivery probability under various QoS values. **b** Average message DP for the standard and the proposed message transfer models.

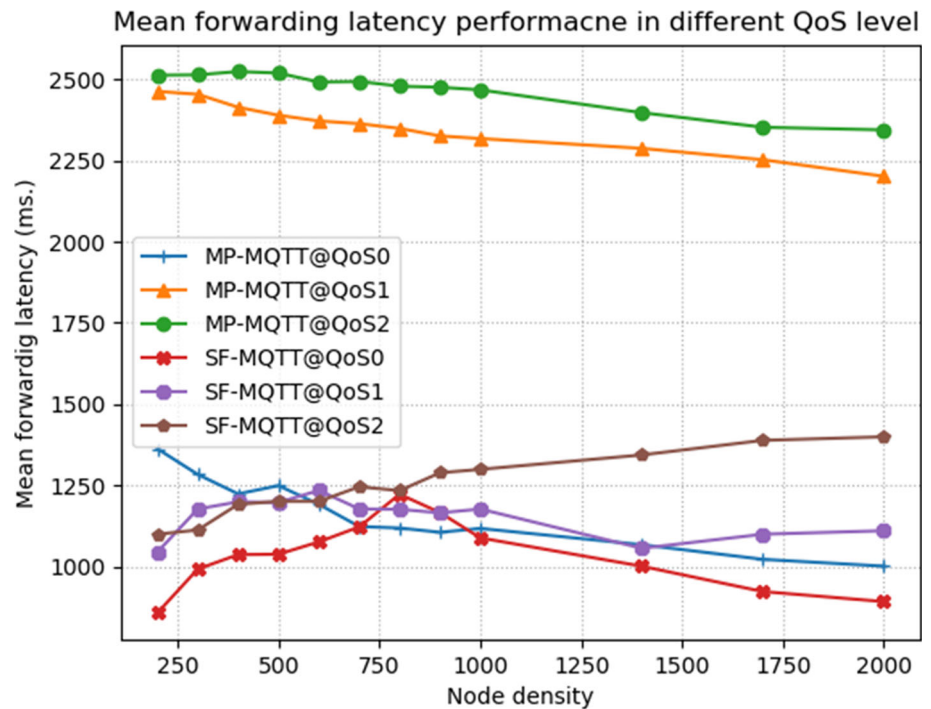


(a) The Impact of node density on the message delivery probability under various QoS values



(b) average message DP for the standard and the proposed message transfer models

Fig. 5 Mean forwarding latency performance with varying node density under different QoS level



5.1 Performance of IoDT nodes under social scenario

Figure 3 represents the message delivery performance of the enhanced message transfer models under various MQTT-QoS levels in varying transmission ranges. The figure illustrates an increasing rate of delivery probability (DP) in both cases. It is evident that change in the transmission range proportionally affects the DP. For example, in Spray- and Focus-based message transfer, the QoS 2 ensures the highest benchmark of DP, which is at around 0.99. The acknowledgment at each step made by the publisher, subscribe, and a broker causes this phenomenon.

Figure 4 show message delivery probability with varying node density. In a typical opportunistic scenario, we report that the DP may decrease as the number of clients increases within a particular network due to the limited bandwidth. The message routing strategies do not perform well in such a case. However, under ultra-low latency 6G network scenario, this performs quite well. As the number of hosts increases, message delivery also increases with the number of nodes.

As the number of hosts expands, the higher number of the node gets selected for potential message forwarder. In Spray and Focus, we can choose more message subscribers with a smaller number of tokens. Thereby delivery ratio reaches a higher benchmark. As the number of subscribers increases, the DP is also increasing proportionally and reaches up to 0.99. MaxProp obeys the same rule because the higher the number of nodes, the better the delivery

predictability. In the case of MaxProp, the QoS 0 gives a minimum benchmark due to the significant amount of packet loss. The decreasing number of nodes makes this chance pretty high which is at about 0.67.

Figure 5 illustrates the forwarding latency corresponding to varying node densities. The increasing number of nodes in the smart city here shows a falling latency. The introduction of more base stations and the relay nodes into the network results in a phenomenon that ensures the near-real-time message forwarding capability.

On the other hand, Fig. 4 shows a comparative study between the average message delivery performance of the standard MQTT protocol and the proposed MP-MQTT, SF-MQTT model, respectively. The classic MQTT scheme is generally designed to transfer the packet to a stationary node or a mobile node that is always connected with the backbone. In the case of IoDT scenario, the node is flying with a variable altitude and speed. Therefore, the performance of the standard MQTT is not satisfactory as in most cases. The figure shows that the average delivery ratio for MQTT, in that case, reaches 0.78. On the other hand, the SF-MQTT offers its best performance and reaches a maximum benchmark of 0.97.

5.2 Performance of SDN under social scenario

Figure 6 shows the simulation snapshot that shows the varying node density under seven different SDN slices. The increasing amount of bandwidth involves the

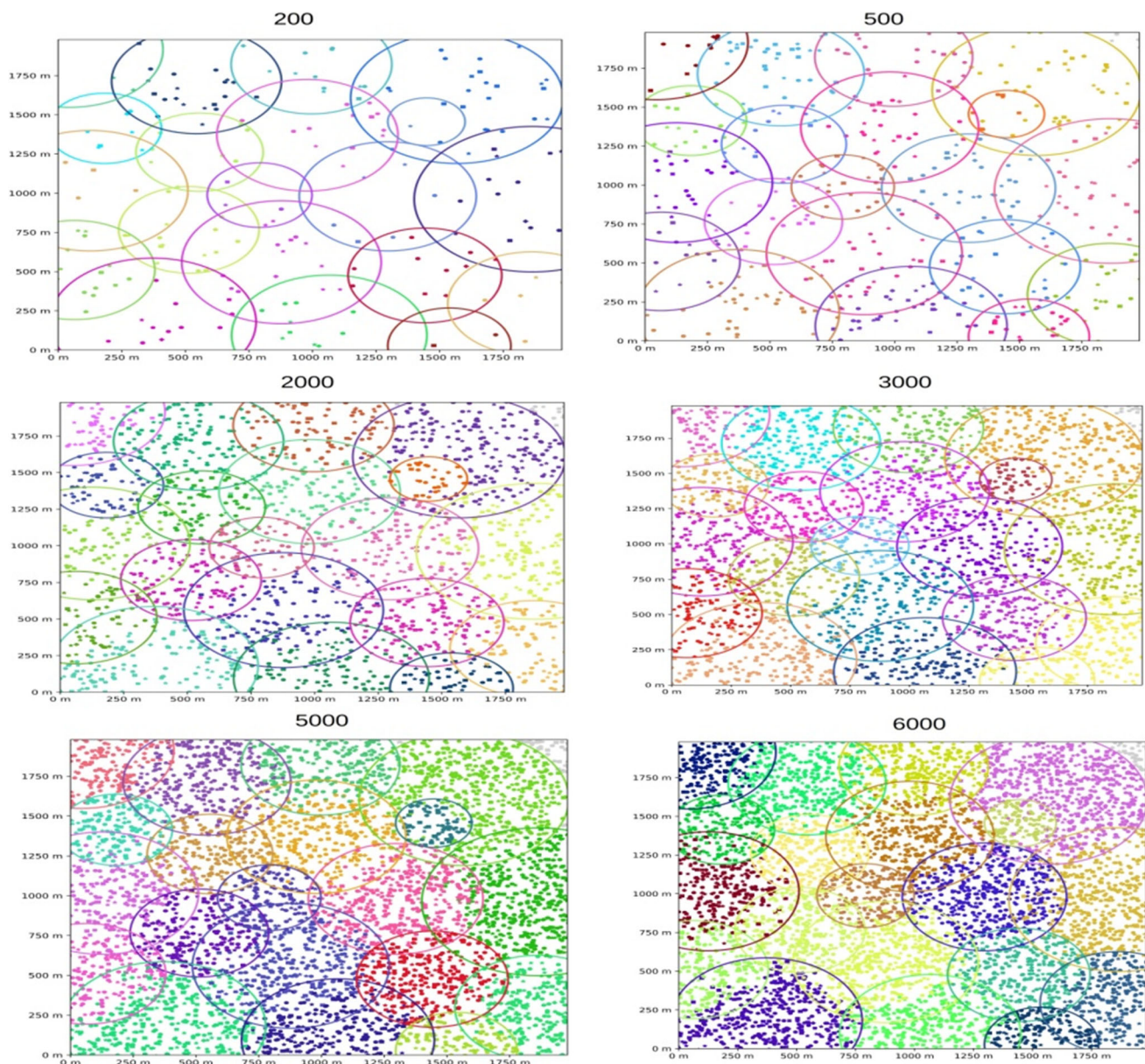


Fig. 6 Simulation snapshot of SDN slicing. The initial number of nodes: 200. The final number of nodes: 6000

accommodation of the more significant number of IoT nodes. The modeling of the SDN under the social IoT scenario involves seven different network slices for various services. Each service receives dedicated access and the core network in this case. Network configuration with 200 to 6000 nodes is identifiable in Fig. 6. We can consider the drone nodes as part of the SDN slice, and the SDN forwards the message in the form of MQTT pub/sub mechanism with an enhanced opportunistic phenomenon. Figure 7 shows the coverage ratio of the SDN slice under different QoS levels. The coverage ratio here gets computed as coverage per user divided by the number of the active slice.

We can observe from Fig. 7 that the coverage ratio decreases drastically in QoS 0 for an increasing number of nodes at about 0.86. As a result, more nodes are out of coverage. In the case of QoS 0, the message delivery chance is minor. A dedicated frequency band is allocated for each node; therefore, the node with less delivery probability moves out of coverage. On the other hand, QoS 2 shows the highest benchmark of coverage which reaches beyond 99% at the number of nodes 1000. The number of connected client ratio per slice and the connection probability is illustrated in Figs. 8 and 9, respectively.

We can obtain the connected client ratio β as the difference between the total available client in slice and the

Fig. 7 Coverage ratio under various QoS levels under proposed SDN

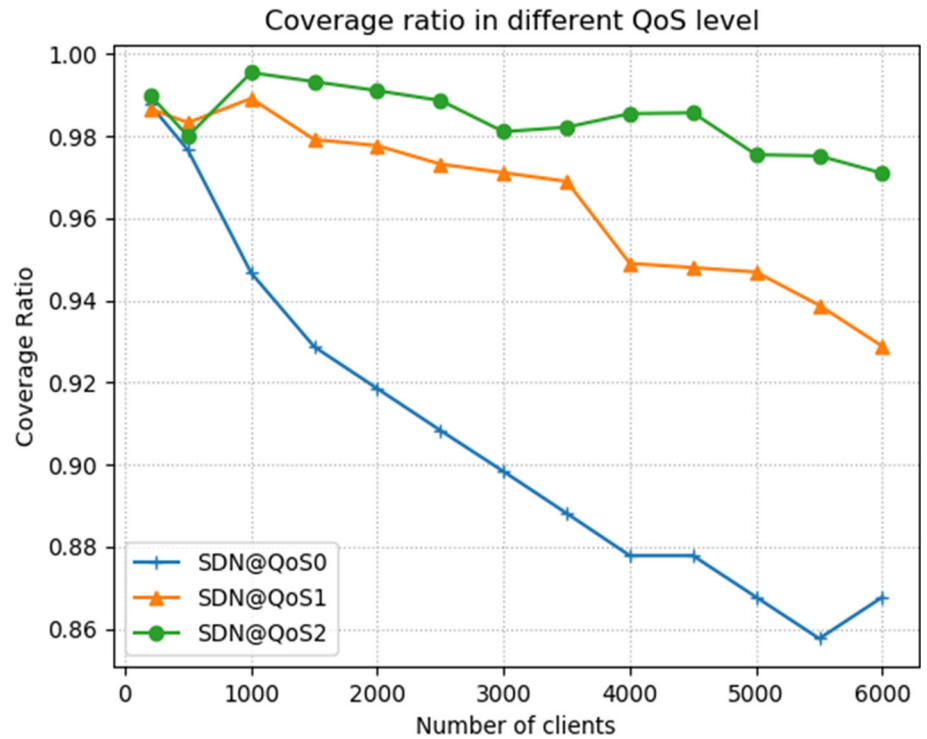
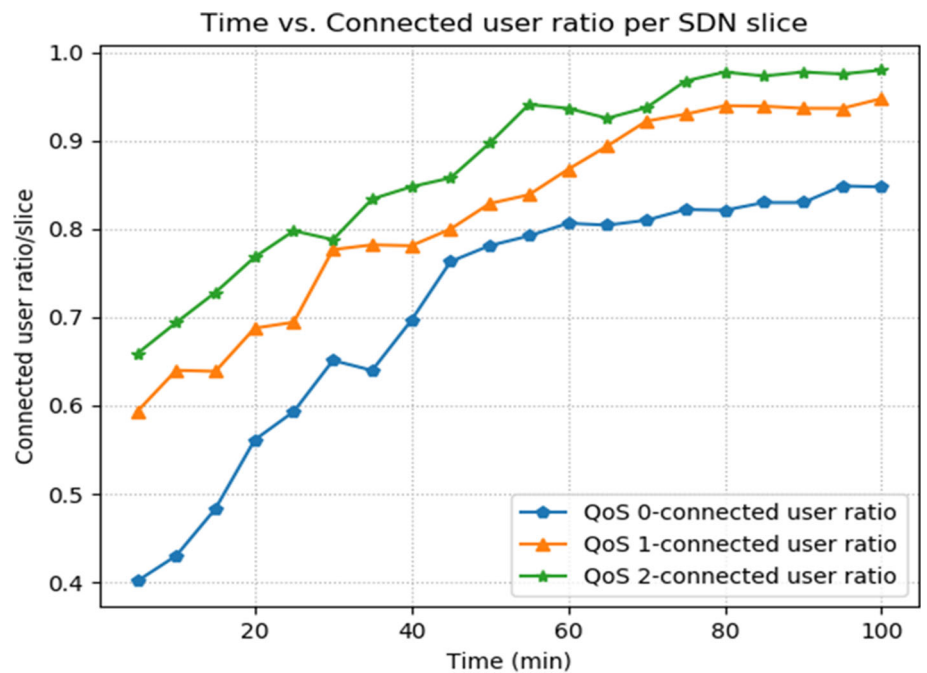


Fig. 8 Connected user ratio (β) per SDN slice within the simulation time



total rejected client plus total handed-off clients with the total available client in the slice. Therefore, we can write as:

$$\beta = \{TACS - (TCH + TCR)\} / TACS \tag{6}$$

TACS is the total number of available clients in the slice, TCH, TCR, handoff clients, and rejected clients. It is noticed from Fig. 8 that as time elapsed, the connected

client ratio per slice increases. Based on the time, the more users got the chance to connect the slice, and the SDN itself schedules this connection. In QoS 2, the ratio reaches more than 0.98; therefore, the users with QoS 2 will get the best connectivity and uninterrupted services from the network. Further, we have observed that the increasing number of clients is inversely proportional to the client connection probability. As the number of users increases, the clients'

Fig. 9 Connection probability of clients under various QoS levels

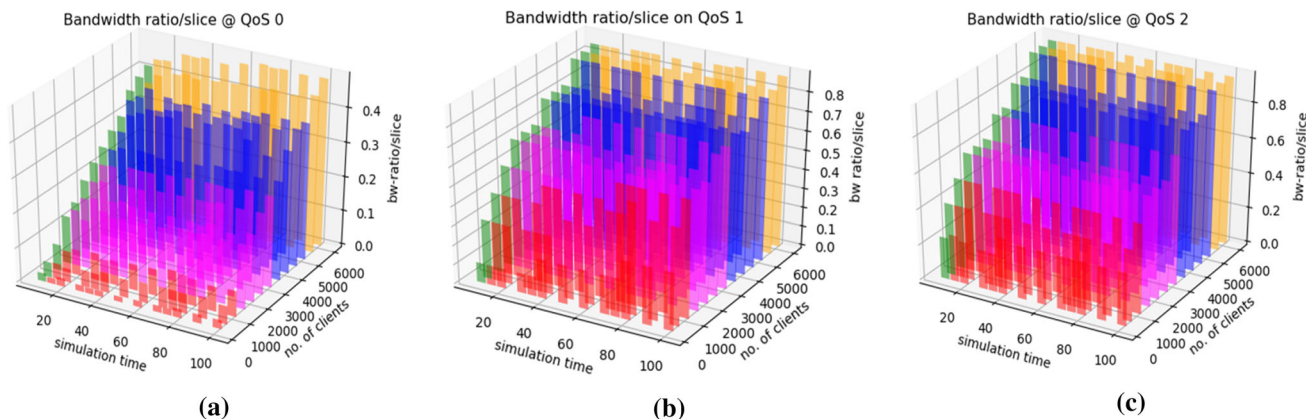
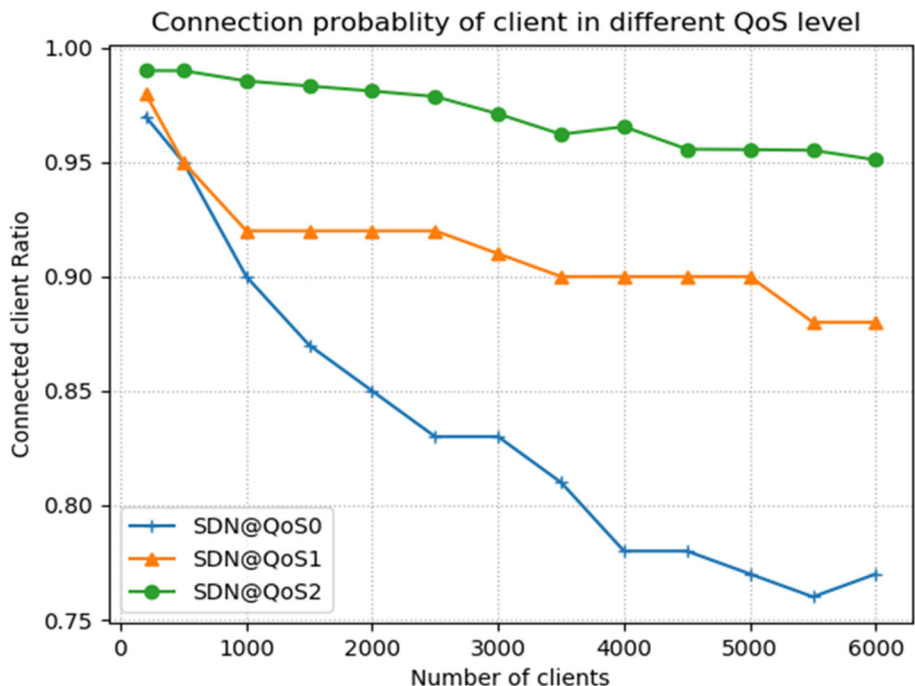


Fig. 10 Bandwidth ratio per SDN slice for three different QoS level under varying node density **a** QoS 0 **b** QoS 1 **c** QoS 2

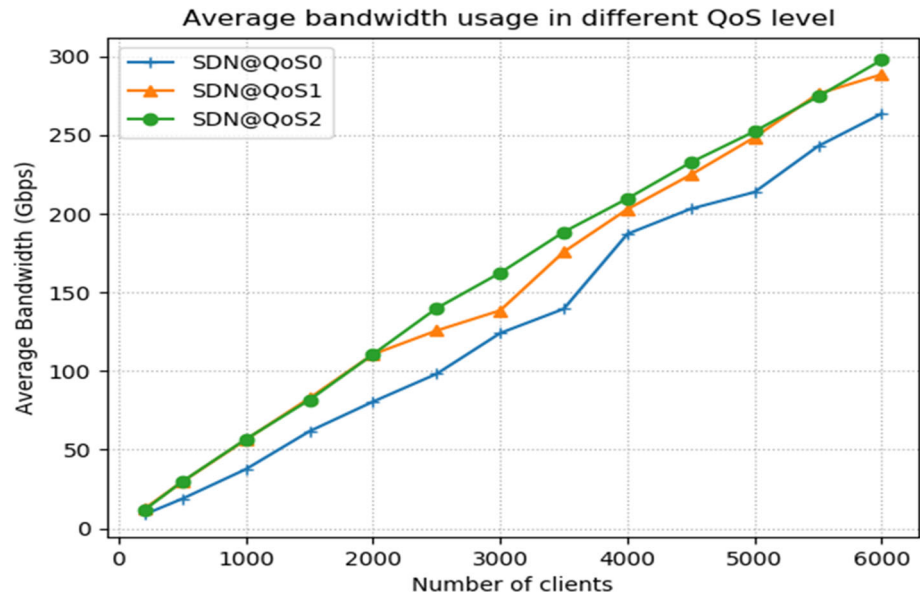
chance to move into the rejection list also increases rapidly. This phenomenon is even more critical while the client uses QoS 0. In such cases, we report that the connection probability is 0.76, which is the minimum benchmark. The bandwidth utilization is perhaps the most crucial factor in the case of a social IoT scenario. As the channels are considered an ultra-low latency transmission capability, the data transmission under slices will happen in order of gigabits per second.

The bandwidth utilization within the SDN slice is linearly increasing as the numbers of nodes are increasing. As shown in Fig. 11, the bandwidth utilization of both QoS 1 and 2 is almost similar, growing linearly. The enormous number of messages and the acknowledged transfer within

the network is the reason behind this phenomenon. On the other hand, QoS utilizes a minimum bandwidth of about 250 Gbps. Figure 10a also shows the bandwidth utilization ratio per slice, which also clearly mentions that the QoS 0 utilizes low bandwidth compared to QoS 1 and 2. From Fig. 10a, b, and c, it is understandable that the bandwidth utilization/slice is increasing as the number of nodes increases. We also report that the QoS 0 message transfer bandwidth ratio per slice is significantly low for the lower value of node density reflected in the red region of Fig. 10a.

On the other hand, the magenta region shows the bandwidth ratio/slice while the node density is between 3000 and 4000. In this scenario, we observe that the

Fig. 11 Average bandwidth usage of the nodes under various QoS levels



bandwidth utilization for QoS 1 and 2 is almost similar, where the ratio increases drastically as the number of nodes increases. This characteristic significantly illustrates that with the introduction of more clients in slices, the performance is not degraded but shows stability.

6 Discussion

The study reveals that the opportunistic message transfer scheme designed to enhance the capability of the MQTT pub/sub messaging scheme is considered highly effective in a situation where there is a lack of coverage. In such cases, the node having a high chance of encountering is automatically chosen as the best forwarder or subscriber. Due to that extended feature, message delivery probability drastically increases. And this reaches its top benchmark while the MQTT protocol is using QoS level 2. We also observe that the Spray and Focus perform best among two of the message forwarding techniques.

In contrast, we record the delivery ratio of MaxProp in QoS 0 to be the worse, which is 66%. In the latency point of view, QoS 0 for both the strategy shows a better performance which is 1000 and 1100 ms, respectively, and QoS 2, in this case, takes more time in comparison with this. Next, the study on the generated SDN slices divulges at about 95% of bandwidth utilization per slice, while the node density is about 6000 and the QoS level is 2. We also observe that the coverage ratio is drastically decreasing in QoS 0 in an increasing number of nodes, which may negatively impact the network. The lightweight devices with low power, which are preferred to transfer messages in QoS 0 level, must shift to QoS 1 in such a case to avoid

the coverage issue. From the bandwidth utilization characteristics study, it is also evident that real-time mission-critical applications like remote surgery, disaster management, and real-time traffic congestion management systems must strictly use quality of service level 2. In contrast, near-real-time IoT applications like live streaming and augmented-reality-based recommendation systems for smart malls may use QoS 1 or 2 depending on bandwidth availability. However, some of the limitations can be observed in this methodology like the limitation of the QoS availability. This might affect the high bandwidth data in some cases. Further, the study mainly emphasizes the telemetry transport protocols. Implementation of the same methodology for the streaming protocols like real-time streaming protocol (RTSP) can be considered as a future work for the proposed methodology.

7 Conclusion

In this work, we propose a message transfer framework for the Social Internet of Drone Things ecosystem. We have tested the framework for different services under a 6G network scenario, and we have set up seven slices for seven distinct slots. We assign the core and the access network for each slice. The standard MQTT message transfer mechanism modification has also been performed at the IoT level by introducing an additional opportunistic feature on message transfer that utilizes opportunistic behavior. We amalgamate the two different opportunistic routing techniques with the MQTT publish-subscribe mechanism. In the first case, the subscriber is chosen based on the message delivery predictability. In the second case, the

timestamp-based forwarding token-based approach selects the best subscriber and the relay node to transfer the message into the destination. We have made the testbed under both mechanisms with varying quality of service, and the latency and delivery performance are measured. The results show that the timestamp-based Spray and Focus approach performs the best among them. Secondly, the performance SDN slices have also measured user connection support, coverage of the network, and the bandwidth utilization by the clients under QoS 0, 1, and 2. We observe that the MQTT QoS2 technique is the best mechanism for achieving the best performance from the network slices under 6G networks. In our belief, the enhanced message transfer mechanism and the SDN network slices implementation give way forward to establish a research direction toward an ultra-low latency data communication. These mechanisms are beneficial for mission-critical social scenarios like disaster management and mobile crowd-sensing. We can also introduce an intelligent network slice selection methodology for precise slice allocation to the mission-critical services.

Authors' contributions AM contributed to conceptualization, methodology, software, investigation, formal analysis, writing—original draft, visualization, validation. ND contributed to formal analysis, investigation, methodology, resources, data curation, project administration, writing—review and editing, supervision, visualization. AM contributed to methodology, formal analysis, writing—original draft, visualization, validation. DD contributed to conceptualization, formal analysis, investigation, writing—original draft, writing—review and editing, supervision, validation, project administration, visualization. RGC contributed to formal analysis, methodology, resources, project administration, writing—review and editing, supervision.

Funding Not applicable.

Availability of data and material Not applicable.

Code availability Not applicable.

Declarations

Conflicts of interest Author declares that they have no conflict of interest.

Ethical approval No ethical approval required.

Informed consent Consent is not required for this article.

Human and animal rights statement This article does not contain any studies with human participants or animals performed by any of the authors.

References

- Afzal B, Umair M, Shah GA, Ahmed E (2019) Enabling IoT platforms for social IoT applications: vision, feature mapping, and challenges. *Futur Gener Comput Syst* 92:718–731
- Akyildiz IF, Su W, Sankarasubramanian Y, Cayirci E (2002) Wireless sensor networks: a survey. *Comput Netw* 38(4):393–422
- Alomari A, Subramaniam SK, Samian N, Latip R, Zukarnain Z (2021) Resource management in SDN-based cloud and SDN-based fog computing: taxonomy study. *Symmetry* 13(5):734
- Ali, D. H. (2015). A social Internet of Things application architecture: applying semantic web technologies for achieving interoperability and automation between the cyber, physical, and social worlds (Doctoral dissertation).
- Alsamhi SH, Ma O, Ansari MS, Gupta SK (2019) Collaboration of drone and Internet of public safety things in smart cities: An overview of qos and network performance optimization. *Drones* 3(1):13
- Alzenad M, Shakir MZ, Yanikomeroglu H, Alouini MS (2018) FSO-based vertical backhaul/fronthaul framework for 5G+ wireless networks. *IEEE Commun Mag* 56(1):218–224
- Avasalcai C, Dustdar S (2019) Latency-aware distributed resource provisioning for deploying iot applications at the edge of the network“ In: Future of information and communication conference, pp 377–391. Springer, Cham
- Bao F, Chen R, Guo J (2013) Scalable, adaptive, and survivable trust management for community of interest-based Internet of things systems. In: 2013 IEEE eleventh international symposium on autonomous decentralized systems (ISADS). IEEE, pp 1–7
- Bekmezci I, Sahingoz OK, Temel Ş (2013) Flying ad-hoc networks (FANETs): a survey. *Ad Hoc Netw* 11(3):1254–1270
- Bekmezci I, Sen I, Erkalkan E (2015) Flying ad hoc networks (FANET) test bed implementation. In: 2015 7th international conference on recent advances in space technologies (RAST). IEEE, pp 665–668
- Cabreira TM, Di Franco C, Ferreira PR, Buttazzo GC (2018) Energy-aware spiral coverage path planning for uav photogrammetric applications. *IEEE Robot Auto Lett* 3(4):3662–3668
- Cheng L, Liu J, Xu G, Zhang Z, Wang H, Dai HN, Wu Y, Wang W (2019) SCTSC: a semicentralized traffic signal control mode with attribute-based blockchain in IoVs. *IEEE Trans Comput Soc Syst* 6(6):1373–1385
- Ding G, Wu Q, Zhang L, Lin Y, Tsiftsis TA, Yao YD (2018) An amateur drone surveillance system based on the cognitive Internet of Things. *IEEE Commun Mag* 56(1):29–35
- García CG, Núñez-Valdez ER, García-Díaz V, Bustelo CPG, Lovelle JMC (2019) A review of artificial intelligence in the internet of things. *Int J Interactive Multimedia ArtifIntell* 5(4): 9–20
- Gligoroski D, Kravlevska K (2019) Expanded combinatorial designs as tool to model network slicing in 5g. *IEEE Access* 7:54879–54887
- Gharibi M, Boutaba R, Waslander SL (2016) Internet of drones. *IEEE. Access* 4:1148–1162
- Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of things (IoT): a vision, architectural elements, and future directions. *Futur Gener Comput Syst* 29(7):1645–1660
- Gulati N, Kaur PD (2021) FriendCare-AAL: a robust social IoT based alert generation system for ambient assisted living. *J Ambient Intell Humaniz Comput*, pp 1–28.
- Hua M, Wang Y, Zhang Z, Li C, Huang Y, Yang L (2018) Power-efficient communication in UAV-aided wireless sensor networks. *IEEE Commun Lett* 22(6):1264–1267

- Joyia GJ, Liaqat RM, Farooq A, Rehman S (2017) Internet of Medical Things (IOMT): applications, benefits and future challenges in healthcare domain. *J Commun* 12(4):240–247
- Kantarci B, Mouftah HT (2014) Trustworthy sensing for public safety in cloud-centric Internet of things. *IEEE Internet Things J* 1(4):360–368
- Kao CC, Lin YS, Wu GD, Huang CJ (2017) A comprehensive study on the Internet of underwater things: applications, challenges, and channel models. *Sensors* 17(7):1477
- Katz M, Matinmikko-Blue M, Latva-Aho M (2018) 6Genesis flagship program: Building the bridges towards 6G-enabled wireless smart society and ecosystem. In: 2018 IEEE 10th Latin-American conference on communications (LATINCOM). IEEE, pp 1–9
- Khan MA, Ullah I, Kumar N, Oubbati OS, Qureshi IM, Noor F, Khanzada FU (2021) An efficient and secure certificate-based access control and key agreement scheme for flying Ad-Hoc networks. *IEEE Trans Veh Technol* 70(5): 4839–4851.
- Kumari A, Gupta R, Tanwar S, Kumar N (2020) A taxonomy of blockchain-enabled softwarization for secure UAV network. *Comput Commun*
- Kyrkou C, Plastiras G, Theocharides T, Venieris SI, Bouganis CS (2018). DroNet: Efficient convolutional neural network detector for real-time UAV applications. In: 2018 design, automation and test in Europe conference and exhibition (DATE). IEEE, pp 967–972
- Luo C, Nightingale J, Asemota E, Grecos C (2015). A UAV-cloud system for disaster sensing applications. In: 2015 IEEE 81st vehicular technology conference (VTC Spring). IEEE, pp 1–5
- Luo C, Ji J, Wang Q, Chen X, Li P (2018) Channel state information prediction for 5G wireless communications: a deep learning approach. *IEEE Trans Netw Sci Eng*
- López-Quintero F, Lovelle JMC, Crespo RG, García-Díaz V (2018) A personal knowledge management metamodel based on semantic analysis and social information. *Soft Comput* 22(6):1845–1854
- Marche C, Atzori L, Nitti, M (2018) A dataset for performance analysis of the social Internet of things. In: 2018 IEEE 29th annual international symposium on personal, indoor and mobile radio communications (PIMRC). IEEE, pp 1–5
- Miraz MH, Ali M, Excell PS, Picking R (2015) A review on internet of things (IoT), internet of everything (IoE), and internet of nano things (IoNT). In: 2015 internet technologies and applications (ITA). IEEE, pp 219–224
- Motlagh NH, Baga M, Taleb T (2016) Uav selection for a uav-based integrative iot platform. In: 2016 IEEE global communications conference (GLOBECOM). IEEE, pp 1–6
- Motlagh NH, Taleb T, Arouk O (2016b) Low-altitude unmanned aerial vehicles-based Internet of things services: Comprehensive survey and future perspectives. *IEEE Internet Things J* 3(6):899–922
- Motlagh NH, Baga M, Taleb T (2017) UAV-based IoT platform: A crowd surveillance use case. *IEEE Commun Mag* 55(2):128–134
- Mukherjee A, Dey N, Kumar R, Panigrahi BK, Hassanién AE, Tavares JMRS (2019) Delay-tolerant network assisted flying Ad-Hoc network scenario: modeling and analytical perspective. *Wireless Netw* 25(5): 2675–2695.
- Mukherjee A, Mukherjee P, De D, Dey N (2020). iGridEdgeDrone: hybrid mobility aware intelligent load forecasting by edge enabled internet of drone things for smart grid networks. *Int J Parallel Programm*, pp 1–41.
- Mukherjee A, Dey N, De D (2020a) EdgeDrone: QoS aware MQTT middleware for mobile edge computing in opportunistic Internet of Drone Things. *Comput Commun* 152:93–108
- Mukherjee A, Panja AK, Dey N (2020c) a beginner’s guide to data agglomeration and intelligent sensing. Academic Press, Cambridge
- Nahrstedt K, Li H, Nguyen P, Chang S, Vu L (2016) Internet of mobile things: mobility-driven challenges, designs, and implementations. In: 2016 IEEE first international conference on internet-of-things design and implementation (IoTDI). IEEE, pp 25–36
- Nguyen V-G, Brunstrom A, Grinnemo K-J, Taheri J (2017) SDN/NFV-based mobile packet core network architectures: a survey. *IEEE Commun Surv Tutor* 19(3):1567–1602
- Oubbati OS, Lakas A, Zhou F, Güneş M, Yagoubi MB (2017) A survey on position-based routing protocols for Flying Ad hoc Networks (FANETs). *Veh Commun* 10:29–56
- Pawlick J, Chen J, Zhu Q (2018) iSTRIC: An interdependent strategic trust mechanism for the cloud-enabled Internet of controlled things. *IEEE Trans Inf Forensics Secur* 14(6):1654–1669
- Pereira AA, Espada JP, Crespo RG, Aguilar SR (2019) Platform for controlling and getting data from network connected drones in indoor environments. *Futur Gener Comput Syst* 92:656–662
- Quaritsch M, Kruggl K, Wischounig-Strucl D, Bhattacharya S, Shah M, Rinner B (2010) Networked UAVs as aerial sensor network for disaster management applications. *e & iElektrotechnik und Informationstechnik* 127(3):56–63
- Roopa MS, Pattar S, Buyya R, Venugopal KR, Iyengar SS, Patnaik LM (2019) Social internet of things (SIoT): foundations, thrust areas, systematic review, and future directions. *Comput Commun* 139:32–57
- Ruiz JG, Torres JM, Crespo RG (2021) The application of artificial intelligence in project management research: a review. *Int J Interactive Multimedia Artif Intell* 6(6):54–66
- Simoens P, Dragone M, Saffiotti A (2018) the internet of robotic things: a review of concept, added value and applications. *Int J Adv Rob Syst* 15(1):1729881418759424
- Singh K, Verma AK (2018) A fuzzy-based trust model for flying ad hoc networks (FANETs). *Int J Commun Syst* 31(6):e3517.
- Song Q, Zeng Y, Xu J, Jin S (2020) A survey of prototype and experiment for UAV communications. *arXiv preprint: arXiv:2007.00905*.
- Srivastava A, Prakash J (2021) Future FANET with application and enabling techniques: anatomization and sustainability issues. *Comput Sci Rev* 39:100359.
- Zhang T, Chen M, Wei X, Chen B, Chao Hu (2019) Sdnms: A software defined network measurement system for nfv networks. *China Communications* 16(4):59–74
- Zhirnov NS, Lyakhov AI, Khorov EM (2019) Mathematical model of a network slicing approach for video and web traffic. *J Commun Technol Electron* 64(8):890–899

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.