IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 26 June 2024, accepted 8 July 2024, date of publication 11 July 2024, date of current version 19 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3427013

RESEARCH ARTICLE

SAFE-GF-NOMA: Social Autonomous Flocking to Enhance GF-NOMA for Massive Internet of Things Uplink Access Contention

FAROOQUE HASSAN KUMBHAR[1], (Member, IEEE), SALAHUDDIN UNAR[2], (Member, IEEE), WESSAM MESBAH[1,3], (Senior Member, IEEE), AND DANIEL BENEVIDES DA COSTA[1,3], (Senior Member, IEEE)

[1]Center for Communication Systems and Sensing, King Fahd University of Petroleum & Minerals, Dhahran 31261, Saudi Arabia
[2]School of Computer and Information Engineering, Qilu Institute of Technology, Jinan, Shandong 250200, China
[3]Electrical Engineering Department, King Fahd University of Petroleum & Minerals, Dhahran 31261, Saudi Arabia

Corresponding author: Farooque Hassan Kumbhar (farooque.kumbhar@ieee.org)

This work was supported in part by the Deanship of Research Oversight Coordination; and in part by the Interdisciplinary Research Center for Communication Systems and Sensing (IRC-CSS), King Fahd University of Petroleum and Minerals, Saudi Arabia.

ABSTRACT The swift progress of 6G cellular networks responds to the urgent demand for seamlessly integrating Internet of Things (IoT) devices on a large scale. Among various emerging technologies, grant-free non-orthogonal multiple access (GF-NOMA) emerges as a standout, offering distinct advantages over traditional networks in accommodating extensive connectivity needs. GF-NOMA optimizes resource usage by reallocating each time-frequency slot to multiple devices with different power levels. Furthermore, it reduces the coordination burden typically associated with uplink communication by broadcasting random access channels. Nonetheless, GF-NOMA faces a significant challenge: the risk of multiple devices inadvertently selecting the same resource and power, resulting in data loss, particularly problematic during emergencies marked by uncoordinated communications. Additionally, the expanding deployment of IoT devices demands a proportional increase in resources, despite advancements in network technology. To address these challenges, this paper introduces an innovative architecture aimed at significantly boosting spatial capacity through the establishment of autonomous social interactions among IoT devices. The proposed SAFE-GF-NOMA aggregation scheme facilitates resource sharing in an independent and ad-hoc trust management environment by ensuring trustworthy sharing. The proposed Social IoT (SIoT) framework reduces uplink access by grouping devices based on trust metrics, resulting in a notable 50% reduction in collision probability, and over a 50% increase in success probability, and a threefold capacity increase compared to conventional systems. Additionally, our system achieves a substantial reduction in energy consumption, cutting it from 17 J to just 5 J per device within the cluster.

INDEX TERMS Clustering, GF-NOMA, random access, social Internet of Things, uncoordinated access.

I. INTRODUCTION

The sixth generation (6G) of cellular networks aims to revolutionize connectivity by accommodating billions of devices in the Internet of Things (IoT) and massive Machine Type Communications (mMTC). IMT 2030 outlines enhanced capabilities for 6G networks, with various features targeting significant improvements over current 5G cellular networks [1]. It is envisioned that 6G networks will support connection densities ranging from 10^6 to 10^8 devices per square kilometer, while also delivering peak data rates with less than 1 millisecond latency and high reliability [2]. While 6G networks hold great potential for enabling unprecedented levels of connectivity and innovation, addressing

The associate editor coordinating the review of this manuscript and approving it for publication was Nan Wu.

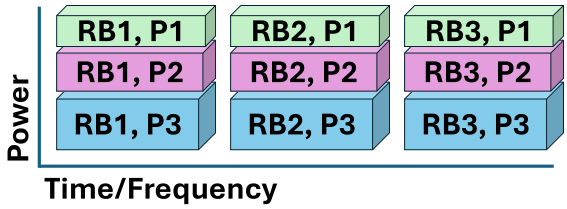

FIGURE 1. Power domain frequency reuse in NOMA.

the challenges associated with massive access and uplink transmission collisions is crucial for realizing their full potential and delivering on their promises of ultra-fast, reliable, and ubiquitous connectivity.

The futuristic IoT network promises numerous technological advancements, enabling autonomous connectivity and facilitating innovative applications across various domains. However, the massive device network also brings forth significant challenges, particularly in terms of resource allocation and energy consumption. Various multiple-access technologies in the envisioned 6G wireless claim to accommodate a higher number of devices with minimum overhead. Grant-Free Non-Orthogonal Multiple Access (GF-NOMA) is a promising access scheme proposed for 6G networks, aiming to efficiently accommodate the massive connectivity demands while mitigating interference and collision issues. Moreover, it significantly reduces the communication overhead required for a battery-constrained device to have successful uplink access. However, as the number of devices increases exponentially, managing access and minimizing collisions becomes increasingly complex. This necessitates the development of sophisticated algorithms and protocols to ensure efficient resource utilization and optimal performance in 6G GF-NOMA networks.

To gain an in-depth understanding of the research challenge, note that GF-NOMA already utilizes two important aspects of Power-domain NOMA (PD-NOMA): frequency reuse and grant-free uplink access. PD-NOMA represents a significant advancement in wireless communication, leveraging transmission power differences to decode multiple signals, superimposed on the same frequency stream [3]. As illustrated in Figure 1, PD-NOMA allocates a frequency block to multiple devices with varying channel gains and transmission powers during each time slot. For instance, if two users employ the same frequency but with different transmission powers, the BS decodes the signal with higher power first, treating the other as noise. Subsequently, the decoded message is utilized to eliminate the high-power signal from the superimposed uplink, enabling the decoding of the low-power transmission [4]. This approach facilitates the simultaneous access of multiple data transmissions over the same frequency streams, thereby enhancing spectral efficiency.

Traditional PD-NOMA typically involves multiple control message exchanges between the BS and the requesting device, a process termed grant-based resource allocation.

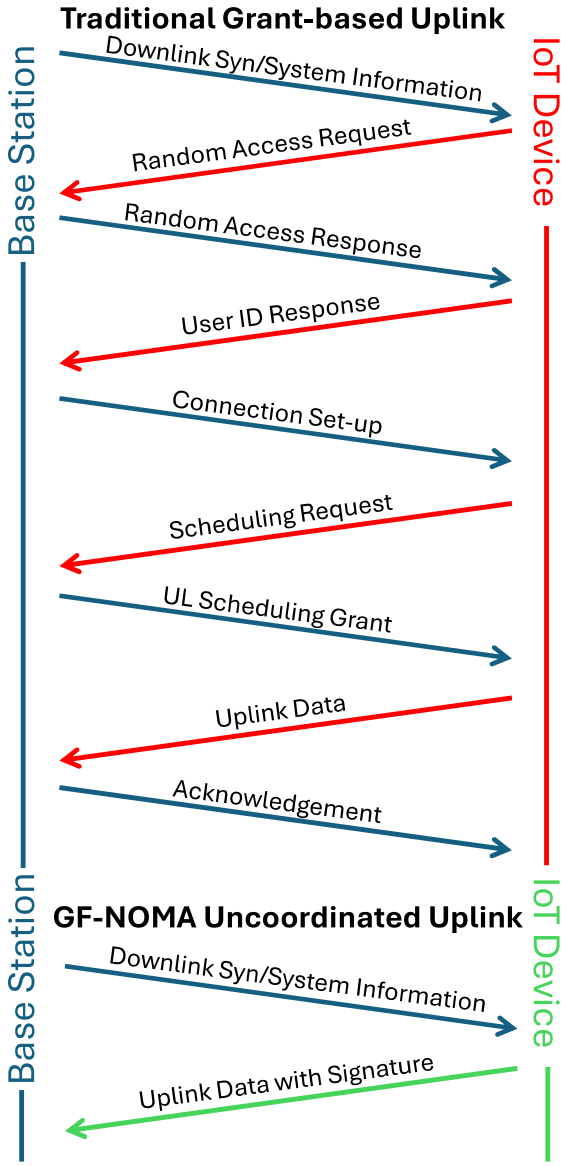

FIGURE 2. GB-NOMA vs GF-NOMA access mechanism.

In contrast, grant-free NOMA (GF-NOMA) streamlines this process by minimizing message exchanges, as depicted in Figure 2. GF-NOMA offers uncoordinated resources over random channels, unlike Sparse Code Multiple Access (SCMA). A unique take in [5] investigates advanced techniques to enhance spectral efficiency in mobile communications by using NOMA schemes, specifically focusing on SCMA in a downlink MIMO (Multiple-Input Multiple-Output) system over frequency-selective fading channels. In GF-NOMA, IoT devices initiate uplink data transmission by selecting a resource block based on preambles broadcast by the BS. This reduces the complexity and resource overhead associated with identifying active devices and allocating resources individually [6], [7]. However, the lack of coordination in resource and power selection among

IoT devices in GF-NOMA can lead to contention and collision of data transmissions, which results in subsequent re-transmissions that degrade network efficiency.

Specifically, uncoordinated mass access and uplink collisions are the immediate challenges in GF-NOMA for IoTs. With the promise of providing service to the massive IoT networks, GF-NOMA faces a major issue whereby each IoT device independently transmits over a random access channel, leading to contention and data loss. To address these challenges, we propose leveraging the Social Internet of Things (SIoT) principles for autonomous device network-based clustering. SIoT represents the convergence of social networks (SN) and IoT, aimed at establishing navigable, scalable, and trustworthy autonomous IoT networks [8]. Unlike conventional social perspectives that rely on user social ties, SIoT fosters social relationships among devices, resulting in dynamic and trustworthy communities. These communities are formed based on device similarities such as common ownership or shared functionalities, facilitating information exchange and enhancing trustworthiness. In our approach, we utilize SIoT traits to develop an autonomous and trustworthy clustering scheme, considering factors such as device centrality, previous interactions, and relationships with neighboring devices.

In this paper, we propose SAFE-GF-NOMA: Social Autonomous Flocking to Enhance GF-NOMA, where the IoT devices create local clusters by establishing social trust locally .[1] Our major focus is on enabling autonomous clusters, where trust management ensures that the relayed data transmissions are not exploited maliciously. Our innovative, autonomous, and independent SIoT-based flocking requires no communication between the device and the BS, over the existing GF-NOMA resource allocation process. To the best of the authors' knowledge, there exists no research that has utilized the full potential of autonomous SIoT and its respective relations to reduce uplink access without imparting additional delays. The major contribution of the paper are given below:

1) Identification and exploration of autonomous communication for clustering in GF-NOMA to facilitate resource sharing.
2) Considering the probability of the malicious nature in IoT devices, we discuss and analytically model a local trust management module that establishes social relationships between devices without a central authority.
3) Analytical modeling of success and collision probabilities for both existing and proposed schemes in GF-NOMA.
4) Subsequently, we propose the SAFE-GF-NOMA solution that aggregates IoT devices using their social autonomous relations. Each cluster is formed with a certain level of trust among the devices. A novel mechanism is designed for cluster head (CH) selection and maintenance using trust and residual energy, to ensure reliable and capable CH identification.
5) Extensive performance evaluation through simulation and analytical experiments, demonstrating a significant reduction in uplink access without incurring additional delays.

The paper is structured as follows: In Section II, we review the existing literature on active device detection and GF-NOMA contention, as well as the background and relevant works on SIoT. Section III outlines the proposed SAFE-GF-NOMA aggregation scheme, detailing its components and operation. Following this, in Section IV, we provide an in-depth analysis of the aggregation scheme, discussing its theoretical underpinnings and practical implications. Section V presents the performance evaluation and results, where we empirically assess the proposed scheme. Finally, in Section VI, we offer concluding remarks and insights from our study.

II. LITERATURE REVIEW

The problem of contention in GF-NOMA is a significant challenge in providing widespread and massive connectivity in 6G cellular networks. To improve access technology, there has been substantial research on device activity detection, barring, or collision avoidance strategies. In this context, we highlight important research conducted in the GF-NOMA domain and outline the latest innovations and solutions in the SIoT domain. It is worth noting that the proposed SAFE-GF-NOMA is the first research work that combines SIoT with GF-NOMA to address uplink access contention.

A. UNCOORDINATED IOT ACCESS OF GF-NOMA

Two novel random access schemes are introduced in [3], tailored for facilitating simultaneous inter and intra-cluster transmissions among IoT devices within MIMO-NOMA networks. The authors explicitly delineated that their scope excluded clustering and beamforming, with their primary focus dedicated to the design of effective random access techniques. The authors in [4] addressed the challenge of maximizing uplink sum rates within NOMA clustering methods and NB-IoT systems. The article introduced an efficient heuristic algorithm designed to tackle the joint optimization of NOMA clustering and resource allocation for MTC devices. The literature review provided in [7] highlighted several key aspects of a proposed solution within a Single Input Single Output (SISO) GF-NOMA network context for diverse IoT devices. The authors identified three contributions: addressing the lack of consideration for diverse IoT traffic in GF-NOMA, introducing device-specific reward modeling for Reinforcement Learning (RL) models, and proposing advanced access mechanisms to accommodate Industrial IoT (IIoT) devices with flexibility and reduced overhead. The devices are categorized into periodic, triggered, and hybrid types, and a Q-learning algorithm is

[1]Please note that the proposed solution majorly operates on the user equipment side to reduce contention.

TABLE 1. State-of-the-art solutions to reduce contention in uncoordinated GF-NOMA.

Reference	Main idea and novelty	Simulation or Analytical	Device or BS	Uplink or Downlink	Shortfalls or overhead
A. Kumar *et al*. [3]	Design of random access techniques for inter and intra-cluster transmissions	Simulations	Both	Uplink	No in-depth consideration of cluster formation, no trust-based relaying.
A. Shahini *et al*. [4]	Maximizing uplink sum rates within NOMA clustering methods and NB-IoT systems	Analytical	Both	Uplink	The proposed ranking within the cluster using the same frequency requires heavy control and processing overhead.
D. Wu *et al*. [7]	Reinforcement Learning (RL) models and advanced access mechanisms to accommodate Industrial IoT (IIoT)	Simulation	BS	Uplink	Only two IoT devices per resource block (RB) considered and requires extensive training data for the Q-learning model.
F. Kilinc *et al*. [9]	Optimizing user pairing, Reconfigurable Intelligent Surface (RIS) assignment, and phase shift alignment to enhance the performance of NOMA systems	Analytical	Both	Both	Requires centrally known environment details, including BS, users, and RIS positioning.
Y. Liu *et al*. [10]	Maximization of the long-term average uplink success, taking into account stringent latency and reliability requirements	Simulation	Both	Uplink	High processing and complexity, which is not considered by the authors.
C. Yuan *et al*. [11]	Closed-form power allocation and user pairing based on linear programming relaxation, to maximize the sum secrecy rate	Simulation	BS	Downlink	Requires perfect channel state information.
L. Wu *et al*. [12]	Device sleep mode proposed to reduce energy consumption, along with a power barring method that reduces uplink access	Simulation	Device	Uplink	Incurs additional delays by barring from uplink access.
M. Fayaz *et al*. [13]	Proposed "transmit power pool" for open-loop power control using RL, for devices to reuse frequency in GF-NOMA	Simulation	Both	Uplink	Requires a multi-agent model to be trained and distributed to all the devices.
D.-D. Tran *et al*. [14]	Proposed maximizing the long-term average energy efficiency while ensuring reliability and latency for URLLC-enabled GF-NOMA systems	Simulation	BS	Both	Requires extensive training of the deep Q-learning models.
Our proposed SAFE-GF-NOMA	Using SIoT for autonomous trust establishment and aggregation to reduce uplink access	Both	Device	Uplink	Requires established SIoT network.

proposed for stationary mode access and an AdaUpdate-aided Priority-based Deep Q-Network (PA-DQN) algorithm for overload mode access. However, the study noted two major challenges: the limitation of considering only two IoT devices per resource block (RB), despite GF-NOMA's potential to accommodate multiple devices for uplink, and the necessity for extensive training data for the Q-learning model, which might not guarantee optimal solutions. Additionally, the study considered factors such as instantaneous success probability and long-term successful access probability in evaluating the proposed techniques.

The primary focus of the study outlined in [9] revolved around optimizing user pairing, Reconfigurable Intelligent Surface (RIS) assignment, and phase shift alignment to enhance the performance of NOMA systems with RIS assistance. The introduction of GF-NOMA alleviated the need for pre-scheduled time slots, thereby enhancing spectral efficiency by allowing users to transmit data without specific time allocations. The paper proposed strategies for effectively pairing users in NOMA systems to maximize both system throughput and fairness. Additionally, it delved into the allocation of RIS elements to users and the optimization of phase shifts within the RIS to enhance signal quality and mitigate interference. The problem was further dissected into two main components: User Equipment (UE) clustering and RIS assignment subproblems, providing a comprehensive approach to addressing the complexities of optimizing NOMA systems with RIS assistance. Overall, the paper contributed to the advancement of communication systems by leveraging RIS and NOMA to enhance spectral efficiency, system throughput, and fairness, particularly in scenarios where grant-free communication was preferred or necessary. In the paper, the parameters for user pairing in the context of RIS-assisted GF-NOMA were likely to include several factors that influenced the performance and efficiency of the communication system.

The study in [10] delved into the intricate task of dynamic resource configuration within GF-NOMA networks, taking into account stringent latency and reliability requirements. The authors aimed to maximize the long-term average number of successfully served users while adhering to latency constraints. One of the prominent challenges highlighted in their work was the contention resolution at the base station, particularly concerning random access collisions of preambles. This contention posed a significant obstacle in ensuring efficient resource allocation and optimal network performance within GF-NOMA systems. Another notable contribution outlined in [11] emphasized the significance of

secure communications within multi-user NOMA downlink systems, primarily attributed to the decoding nature essential for message recovery. Recognizing the potential threat posed by eavesdroppers, the authors concentrated on resource allocation strategies aimed at maximizing the sum secrecy rate while accommodating data requirements and power constraints. The problem at hand was divided into two distinct components: closed-form power allocation and user pairing based on linear programming relaxation. The outcomes of the study encompassed secrecy sum-rate metrics, shedding light on the effectiveness of the proposed approaches in enhancing the security of NOMA downlink systems. An interesting strategy in [12] proposed a combined solution where they innovated with the addition of a sleep mode to reduce energy consumption, along with a power barring method that reduces the uplink access. A coverage cell was divided into multiple power layers, and a device chose to conserve energy and/or skip uplink data with added delay. The device received the channel broadcast and switched active mode on. With a $P_t^{n,l}$, the device participated and selected a random resource to uplink data. The proposed scheme improved energy consumption for devices and reduced uplink access for the base station but with a cost of delay for the device. Moreover, the efficient use of resources being under or overused was not possible in an uncoordinated network. The research conducted by Wu et al. is considered a reference point due to its compatibility with our proposed scheme. Similar to *Wu et al.'s* work, we also utilized multiple resources with varying power levels for uplink access in uncoordinated GF-NOMA. Given the performance evaluation settings, [12] serves as a better state-of-the-art benchmark compared to other existing schemes.

The study conducted in [13] shed light on a crucial limitation encountered in GF-NOMA networks, particularly concerning short-packet IoT applications, where closed-loop power control was unavailable. To address this challenge, the authors proposed a novel approach termed ''transmit power pool'' for open-loop power control. In this mechanism, IoT users obtained their transmit power levels from a shared power pool based on their respective distances from the base station. The determination of the power pool was facilitated by a multi-agent deep Q-network (DQN)-aided GF-NOMA framework, wherein each user served as an agent and learned a policy through interactions with the environment. Initially, the base station broadcasted the power pool to all IoT users, who subsequently randomly selected a power level from the pool. This innovative power selection strategy significantly reduced control overhead and communication requirements. Moreover, the allocation of RBs was based on the distance of users from the base station, ensuring efficient resource utilization. However, a notable challenge arose from the possibility of multiple users at the same distance selecting the same RB with identical power levels. While resource sharing occurred in both frequency and power domains, there was no mechanism for releasing or reallocating

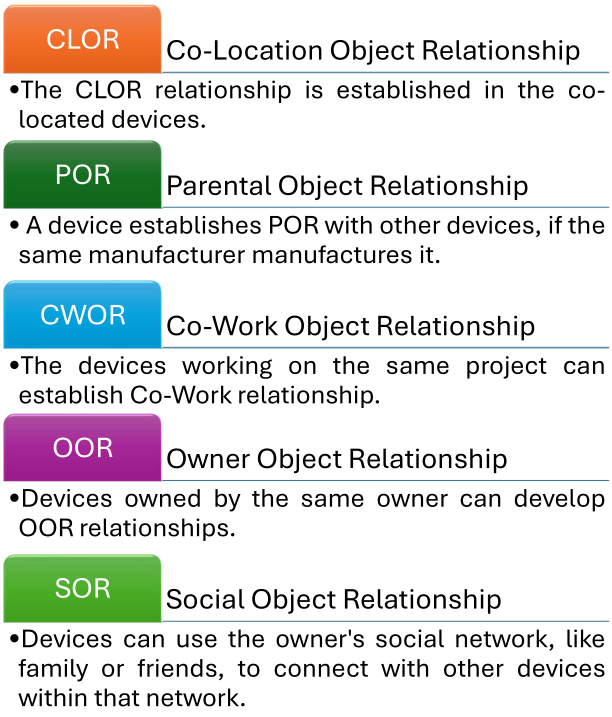

FIGURE 3. Social relationships in SIoT.

resources in GF-NOMA networks once they had been shared. The study suggested further exploration of exploiting time-division considerations in conjunction with frequency and power-domain resource allocation, albeit requiring pre-planned coordination. In their study, Tran et al. [14] highlighted the critical requirements of Ultra-Reliable Low Latency Communication (URLLC) messages, which were characterized by their ultra-short duration and the necessity for massive connectivity. Within the context of GF-NOMA solutions, effective resource allocation emerged as a crucial factor in mitigating contention in RB selection. The potential for multiple users to select the same RB could result in collisions and interference, ultimately undermining system performance. To address this challenge, the authors proposed a framework aimed at maximizing the long-term average energy efficiency while ensuring the fulfillment of user requirements regarding reliability and latency for URLLC-enabled GF-NOMA systems. The paper presented a novel approach to maximize energy efficiency, simultaneously optimizing sum rate maximization and power consumption minimization by utilizing Deep Q Learning techniques. Three distinct solutions were proposed: MA Dueling Double Deep Q Network, MA Double Deep Q Network, and MA Deep Q Network. An interesting take on non-orthogonality in [15] proposed the unified non-orthogonal waveform (uNOW) scheme, which integrated non-orthogonal waveforms with NOMA to enable efficient data transmission across different users. The authors proposed a receiver design based on variational inference, which is a probabilistic method for

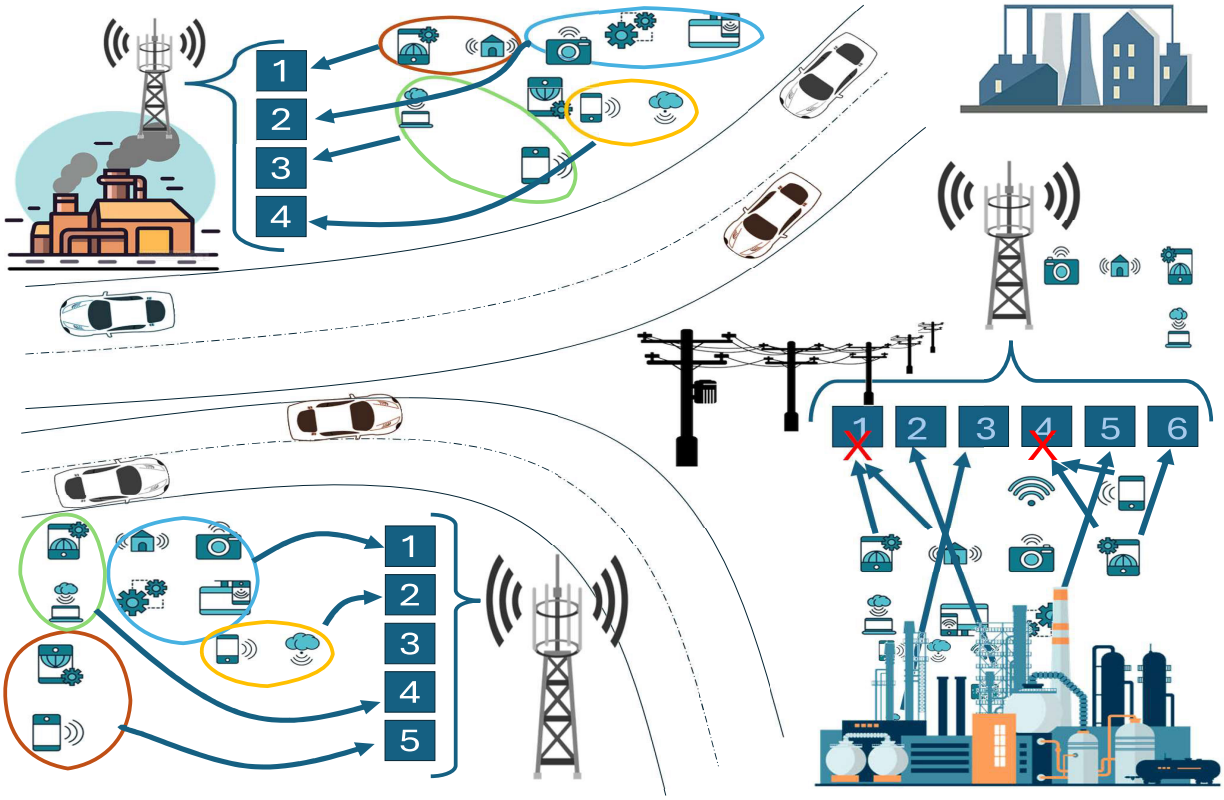

FIGURE 4. Enabling SIoT aggregation in the GF-NOMA uncoordinated IoT network uplink access.

approximating complex posterior distributions. The proposed equalization can successfully balance complexity and bit error rate performance. Moreover, the authors in [16] introduced an innovative resource allocation scheme designed to enhance the energy efficiency (EE) of Pattern Division Multiple Access (PDMA)-based Simultaneous Wireless Information and Power Transfer (SWIPT) systems. The approach addresses the challenge of maintaining quality of service (QoS) while optimizing resource allocation. These methodologies offered innovative strategies to enhance the performance and efficiency of GF-NOMA systems while meeting the stringent demands of URLLC communications. We have summarized the existing literature on uncoordinated GF-NOMA in Table 1.

B. STATE OF THE ART IN SIOT

IoT envisions providing ubiquitous computing, where smart or non-smart objects like coffee makers, fridges, and etc., autonomously communicate and exchange information [17]. Subsequently, SIoT offers a navigable, scalable, and autonomous architecture for massive IoT networks, by incorporating relationships between devices. Another advantage of social relations in autonomous devices is trustworthiness, which provides secure networking. SIoT enables devices to identify and establish dynamic relationships with nearby devices, and eventually to provide efficient resource and service discovery [18], [19]. Khan et al. introduced the SIoT structure, where relationships in devices are discussed [8]. These social relations in autonomous IoT networks are formed using existing sociology and anthropology theories in SNs [20], [21]. A device can establish one or more relationships with other devices, as listed in Figure 3. These SIoT relationships are explained below:

1. Co-Location Object Relationship (CLOR): The CLOR relationship is established between the co-located devices, which can communicate over capillary communication (Bluetooth, Zigbee, etc.).

2. Parental Object Relationship (POR): A device establishes a POR with other devices if they are manufactured by the same manufacturer. Similar products mimic a family with the same parents.

3. Co-Work Object Relationship (CWOR): Devices working on the same project can establish a Co-Work relationship. A multi-agent, goal-oriented project can highly benefit from CWOR.

4. Owner Object Relationship (OOR): Multiple devices owned by a single person can communicate and develop an autonomous relationship that makes things easier for the owner. A relation fostered based on the same owner similarity is termed an owner-object relationship (OOR).

5. Social Object Relationship (SOR): An owner might share services (printer information, etc.) with friends, where devices can utilize the owner's social circle information and establish relationships with these external devices.

Social relationships establish an autonomous SN of devices, where interactions between device SNs and human SNs may also exist [22]. Communication with human SNs enables context awareness in devices, and they can also benefit from efficient data acquisition and quality decisions [23]. The establishment and maintenance of social relationships in IoT devices require various control communications, which can be achieved using a centralized entity, i.e. an SIoT Server [24]. However, an independent peer-to-peer (P2P) network perfectly mimics a human SN, where devices can directly communicate and establish social relationships dynamically [24].

III. PROPOSED SAFE-GF-NOMA SCHEME

We introduce a distributed device network and propose a graph theory-based clustering mechanism that ensures trustworthiness in the CH.[2] We believe that a trustworthy cluster where devices are familiar with each other can be utilized in several applications. GF-NOMA faces a severe hurdle in its uncoordinated and random but massive access to IoT networks, in the form of uplink collisions. The proposed trustworthy aggregation can provide resource sharing, leading to a substantial reduction in uplink access without incurring any additional delays or data loss. Subsequently, the reduced uplink access substantially reduces collisions and contentions. Moreover, for every transmission, a large number of IoT devices in the proposed scheme opt to transmit via a CH which enhances the battery life and reduces the uplink interference. The proposed SIoT-based aggregation scheme relies on relationship establishment and independent trust management. Figure 4 illustrates a GF-NOMA environment where resources are shared over a broadcast channel and the IoT devices carry out random selection. However, the massive access contains mostly short messages or data transmission, and the collisions due to the same resource selection can easily degrade the overall system performance. On the other hand, the proposed scheme reduces the uplink access with the help of SIoT-based aggregation, where devices share resources by establishing trust among themselves. The proposed autonomous process requires careful modeling and design for efficient cooperative aggregation.

A. SYSTEM MODEL

Let a network be described as a directed graph $\upsilon = \{\delta, \varepsilon\}$, where $\delta = \{\rho_1, \rho_2, \ldots, \rho_k\}$ is the set of k nodes. An edge $\varepsilon_{i,j}$ is a representation of a physical wireless direct communication link between devices, ρ_i and ρ_j. We propose

[2]The proposed scheme operates on MAC and higher layers to enable two-hop message delivery with trustworthiness. However, the impact of reduced uplink access also improves the physical layer metrics such as signal strength and data rate, as demonstrated in our results.

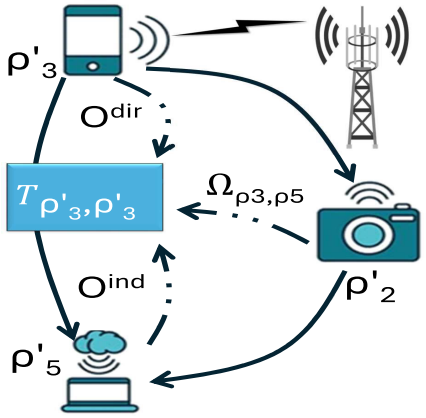

FIGURE 5. Trust model.

an overlaying social graph $\upsilon' = \{\delta', \varepsilon'\}$, where $\upsilon' \subseteq \upsilon$, $\delta' \subseteq \delta$ and $\varepsilon' \subseteq \varepsilon$. Given $\upsilon = \{\delta, \varepsilon\}$, our aggregation model generates a social graph $\upsilon' = \{\delta', \varepsilon'\}$, where each social edge $\varepsilon'_{i,j}$ represent a trust between ρ'_i and ρ'_j. Two nodes establish an edge $\varepsilon'_{i,j}$ in the social graph if there exists a valid $\varepsilon_{i,j}$ and a level of trustworthiness ($T_{i,j}$), as formulated below:

$$\upsilon' = \{\delta', \varepsilon'\} \mid \forall\ \varepsilon'_{i,j}\ \exists\ \varepsilon_{i,j}\ \textit{and}\ T_{i,j} > T_{\text{Thresh}}, \tag{1}$$

where $T_{i,j}$ is the trust value of ρ_i and T_{Thresh} is a threshold of trustworthiness, a value to limit the amount of information sharing with trustworthy devices.

The SIoT-based trustworthiness framework enables autonomous trust establishment and management in IoT devices. The trust process is initiated between two nodes by considering similar traits or properties, e.g. Co-Owner, Co-Work, etc. However, the trustworthiness of a device does not depend only on the type of relationship, but it is a function of multiple attributes. A device calculates the trustworthiness of a neighboring device $T_{i,j}$ by considering the centrality in the network $\Omega_{i,j}$, previous experience of direct transactions O^{dir}, and the opinions of common devices O^{ind}. The centrality of a device j is defined as the ratio of connections with j to the total number of devices, given by: $\Omega_j = \frac{N^{\delta_j}}{N^{\delta}}$. A higher Ω_j value indicates that the device j is well-connected and can provide access to other nearby resources. The direct transaction experience O^{dir} depends on the ratio of messages sent to j to the total, expressed as $O^{\text{dir}} = \frac{M_{i,j}}{M_i}$. This direct experience reflects previous messages, bug reports, software updates, and communications. Nearby devices with higher O^{dir} values are considered trustworthy and reliable for future transmissions. The neighbor opinion (O^{ind}) is the average of direct transaction experiences of all common neighbors with target devices j, estimated as: $O^{\text{ind}} = \frac{\sum_k^{\text{CLOR}_i} O^{\text{dir}}_{k,j}}{\text{CLOR}_i}$. This value O^{ind} is used in the trust calculation to avoid relying solely on personal experience. A trustworthy device must be well-connected and well-communicated with other nearby devices. We consider the trustworthiness calculation as an existing function of SIoT, where the device establishes and

Algorithm 1 Device Periodic Trust Management

Require: $\delta = \{\rho_1, \rho_2, \ldots \rho_k\}$
for Device i in $\delta = \{\rho_1, \rho_2, \ldots \rho_k\}$ **do**
  for CLOR$_i$ **do**
    if $T_{i,j} \geq T_{\text{Thresh}}$ **then**
      Register in TT
    end if
  end for
  Participate in SAFE-GF-NOMA aggregation and resource allocation
end for

Algorithm 2 Aggregation Communication Algorithm

Initiate the process by I_j
Broadcast the aggregation request
for each response i **do**
  Calculate $T_{j,i}$ using Equation 1
  if $T_{j,i} > T_{\text{Thresh}}$ **then**
    Register in TT
  end if
end for
Select a resource out of M, broadcast from the BS
Identify transmit power level P_j
Transmit over selected resource with the selected power

maintains relationships. Figure 5 shows an example of node ρ_3' calculating T_{ρ_3,ρ_5} (trust value for ρ_5'), utilizing $\Omega_{i,j}$, O^{dir}, and O^{ind}.

The trust value $T_{i,j}$ in the range of [0, 1] is finally calculated using a weighted sum model. The autonomous trust $T_{i,j}$ can be estimated as:

$$T_{i,j} = (1 - \alpha - \beta)\Omega_{i,j} + \alpha O_{i,j}^{\text{dir}} + \beta O_{i,j}^{\text{ind}}, \qquad (2)$$

where $\Omega_{i,j}$ indicates the centrality of node ρ_j', as viewed from ρ_i', and previous transaction experience is represented by O^{dir} and O^{ind}.

Smart and connected IoT applications, such as healthcare, smart homes, consumer electronics, intelligent transportation systems, and smart cities, are prime targets for our proposed SIoT-based trustworthiness. Trust establishment and management in all these applications are crucial. Let us consider a scenario in healthcare where devices within the same room or area can establish trust and share information. For any patient, devices such as wearable health monitors, smart infusion pumps, digital stethoscopes, and bedside tablets, are deployed to provide comprehensive patient care. These devices must communicate and collaborate to monitor the patient's health and provide real-time data to healthcare providers. Our trust mechanisms ensure that sensitive patient data is shared only with trustworthy devices. For a smart city scenario, our trust procedure can be easily integrated to enhance traffic management and ensure public safety with smart devices such as traffic lights, surveillance cameras, smart parking meters, air quality sensors, and emergency response units. In this paper, we consider a generalized trust management model using Equation (2), where a device can quantify, calculate and store the trust value of another device, regardless of the application.

B. SIoT-BASED AGGREGATION MODEL

In an independent and autonomous IoT paradigm, a device can calculate trust for other devices using Equation (2), which can be used for various applications. We propose a SAFE-GF-NOMA, SIoT-based aggregation scheme for GF-NOMA contention, where trustworthiness is a crucial component. An autonomous device can communicate and keep track of periodic trust among devices using Equation (2), as outlined in Algorithm 1. The trust information of the nearby devices is stored locally in a "Trust Table" (TT). Once the TT is populated, a device can initiate the aggregation process and become the CH for the cluster, or participate in existing clusters. However, an operator-controlled and pre-defined threshold T_{Thresh} value is used to filter out trustworthy devices. Nevertheless, once the trust is established among a group of autonomous devices, the CH can relay the uplink transmissions on behalf of the cluster members, over GF-NOMA cellular resources. Algorithm 2 outlines the proposed procedure for an initiator interested in becoming the CH. In our proposed aggregation scheme, a broadcast discovery message initiates the registration process to detect potential devices in the vicinity (referred to as the CLOR). A nearby device can reciprocate by sending its information, constituting a handshake. The received information is then utilized, along with the relationship and centrality of the device, to examine trustworthiness during the investigation process using Equation (2). The registration concludes by adding the device and its corresponding trust value to a local TT. In each device, the TT holds a list of devices with their respective IDs, trust values, and validity, which is periodically updated. Establishing an SIoT relationship with a nearby device does not guarantee aggregation or resource sharing; it depends on the mutual trust between the two participants. The clustering process is triggered when a device (initiator) has data to transmit and sends a participation request to the devices stored in the TT. Nearby devices join the aggregation if the trust value $T_{i,j}$ is higher than the threshold T_{Thresh}.

Please note that the threshold value T_{Thresh} is determined by the application requirements and controlled by the operator. Devices handling sensitive information, such as security cameras and monitoring devices, typically have a higher threshold compared to devices like temperature sensors, which may have a lower threshold. The CH considers the GF-NOMA BS broadcast with resources and power levels and selects a random resource to transmit uplink data on behalf of the cluster members. The proposed aggregation significantly reduces uplink access, resulting in two advantages for GF-NOMA resource allocation:

1) Reduced uplink access increases the success of uncoordinated uplink data transmission in the GF-NOMA and IoT environment.
2) Devices that opt for local transmission within the cluster reduce overall system interference, increasing signal strength, data rate, and quality of service.

Nevertheless, another important aspect of the proposed scheme is the CH selection. Throughout this manuscript, the initiator has been designated as the CH because of its willingness to transmit on behalf of nearby devices. A CH must fulfill two key criteria: having sufficient energy for continuous transmission and maintaining a higher average trust value. The proposed algorithm ensures that both criteria are met by default. However, it is important to have a criterion defined to ensure CH selection at the beginning of cluster formation or at a later if the current CH's energy is depleted. We model a periodic approach where the device a with the highest CH suitability value (Γ_a^j) can replace CH j. Let $k_{t|C}^j$ be the devices currently associated with the CH j, then the Γ_a^j formulation is outlined below:

$$\Gamma_a^j = (1-w) \times \frac{\sum_{\substack{i=1 \\ i \neq a}}^{k_{t|C}^j} \lfloor T_{i,a} - T_{\text{Thresh}} + 1 \rfloor}{k_{t|C}^j} + w \times E_{t,a}, \tag{3}$$

where $E_{t,a} \in [0, 1]$ represents the total remaining energy of device a and $k_{t|C}^j$ denotes the total count of devices associated with CH j, out of k, participating in the proposed SAFE-GF-NOMA aggregation, as elaborated in the next section. The initiator collects and assesses Γ for each cluster member, determining the next CH based on the highest value (i.e. $\arg\max_{a=1}^{k_{t|C}^j} \Gamma_a$). Notably, the trust value (T_{ij}) between device i and j evolves or diminishes over time. In our proposed scheme, we adopt the trust management process outlined in [25]. To help the reader keep track of all used mathematical notations, Table 2 outlines the description of all symbols.

IV. ANALYTICAL MODEL

We propose that the CHs aggregate devices within the communication range, based on the trust values. Let the number of devices surrounding a CH (j) depend on the sparsity of the device distribution which in turn depends on the radius of BS (λ_{BS}) and communication range of CH, λ_j. The total number of devices in the proximity ($k_{t|C}$) of total I_t CHs can be calculated as:

$$k_{t|C} = \sum_{j=1}^{I_t} \left[(\lambda_j / \lambda_{\text{BS}}) \times (k - I_t) \right], \tag{4}$$

where $I_t \leq (\lambda_j/\lambda_{\text{BS}}) + 1$, k is the total number of devices, λ_j and λ_{BS} is the capillary communications range of CH j and BS radius, respectively.

Subsequently, the cluster size relies on communication range and BS size, whereas uniformly distributed and non-overlapping I_t also represents the number of clusters.

TABLE 2. Symbol table with descriptions.

Symbol	Description
υ	Directed graph representing the network
δ	Set of nodes in the network
ε	Set of edges (physical wireless links) in the network
ρ_i	Node i in the network
$\upsilon' = \{\delta', \varepsilon'\}$	Social graph generated from the network
δ'	Subset of δ (nodes in the social graph)
ε'	Subset of ε (edges in the social graph)
$\varepsilon_{i,j}$	Physical wireless link between nodes ρ_i and ρ_j
$\varepsilon'_{i,j}$	Social trust edge between nodes ρ'_i and ρ'_j
$T_{i,j}$	Trust value between nodes ρ_i and ρ_j
T_{Thresh}	Threshold of trustworthiness
$\Omega_{i,j}$	Centrality of node ρ'_j as viewed from ρ'_i
O^{dir}	Direct transaction experience
O^{ind}	Indirect transaction experience (opinion of common devices)
α	Weight for direct transaction experience
β	Weight for indirect transaction experience
k	Total number of devices
$k_{t\|C}$	Number of devices in the proximity of cluster heads
$k'_{t\|C}$	Number of devices participating in the proposed scheme
k_r	Number of other devices transmitting over the same resource
$k'_{t\|C,r}$	Devices not creating interference due to cluster participation
λ_{BS}	Radius of the base station (BS)
λ_j	Communication range of cluster head (CH) j
I_t	Total number of cluster heads
$\Phi_{i,j}$	Binary identification of device i's participation in CH j's cluster
M	Number of broadcast resources
L	Number of power levels for each resource
P_c	Collision probability
$P_{i,\text{BS},r}$	Transmission power of device i to BS over resource r
$\text{SINR}_{i,\text{BS},r}$	SINR for a device i communicating to a BS over resource r
$\text{SINR}_{i,\text{BS}\|C,r}$	SINR for a device transmitting to a BS with reduced competition
$\text{SINR}_{i,C}$	SINR for a device communicating to the CH
μ	Additive white Gaussian noise
$\|h_{i,\text{BS}}\|^2$	Channel gain
$R_{i,\text{BS}}$	Data rate for device i communicating to the BS
$R_{i,\text{BS}\|C}$	Data rate for device i communicating to the BS with reduced competition
$R_{i,C}$	Data rate for device i communicating to the CH
S_T	Size of the transmitted content in bits
E	Total energy consumed
f	Factor related to bandwidth and modulation
w	Weight for energy consideration in CH selection
Γ_a^j	Suitability of device a in cluster head j for CH selection
$E_{t,a}$	Total remaining energy of device a
$k_{t\|C}^j$	Total count of devices associated with CH j
$\arg\max_{a=1}^{k_{t\|C}^j} \Gamma_a$	Device a with the highest Γ value in cluster head j

Participation in the cluster requires a level of trust between a device and CH, where trust value is unique and experience-dependent. A device i joins a cluster if the trust edge value between device i and CH j, ($T_{i,j}$) is greater than threshold T_{Thresh}. The total number of devices participating in the proposed SAFE-GF-NOMA scheme to reduce uplink access

$(k'_{t|C})$, can be estimated as:

$$k'_{t|C} = \sum_{i=1}^{k_{t|C}} \sum_{j=1}^{I_t} \left[\Phi_{i,j} \times \left\lfloor T_{i,j} - T_{\text{Thresh}} + 1 \right\rfloor \times \left\lfloor T_{j,i} - T_{\text{Thresh}} + 1 \right\rfloor \right], \quad (5)$$

where $\Phi_{i,j}$ is a binary identification of device i's participation in CH j's cluster. Our designed equation for $k'_{t|C}$ smartly formalizes the trust condition ($T_{i,j} > T_{\text{Thresh}}$) using $\lfloor T_{i,j} - T_{\text{Thresh}} + 1 \rfloor$ and makes use of a geometrically possible number of non-overlapping clusters. Moreover, for a device to become part of the proposed aggregation, trust for both device i to CH j and CH j to device i must be greater than the threshold T_{Thresh}.

Let us assume that a GF-NOMA BS broadcast M resources, each with L power levels resulting in $M \times L$ possible resources in the broadcast. The collision probability of a device competing with another device can be defined as $1 - (\text{Probability of not selecting unique resource}) = 1 - \left(1 - \frac{1}{M}\right)$, where $\frac{1}{M}$ is the probability of selecting a unique resource. In the presence of other $k-1$ active devices, the collision probability can be defined as:

$$P_c = 1 - \left(1 - \frac{1}{M \times L}\right)^{k-1} \quad (6)$$

Considering that the CH aggregates the devices participating in aggregation, the competition is reduced by C devices, resulting in less collision probability. The collision probability for the proposed aggregation scheme, using Equation 6 is updated as:

$$P_c = 1 - \left(1 - \frac{1}{M \times L}\right)^{k-k'_{t|C}-1} \quad (7)$$

Let us consider the successful decoding order of transmission ($P^1_{i,\text{BS},r} > P^2_{i,\text{BS},r} > \ldots > P^k_{i,\text{BS},r}$) with different power for the same frequency resource r. The signal-to-interference-plus-noise-ratio (SINR) for a device i communicating to a BS for resource r, $\text{SINR}_{i,\text{BS},r}$ with transmission power $P^1_{i,\text{BS},r}$, over a quasi-static Rayleigh fading channel with additive white Gaussian noise μ and $|h_{i,\text{BS}}|^2$ channel gain, is [13]:

$$\text{SINR}_{i,\text{BS},r} = \frac{|h_{i,\text{BS}}|^2 \times P_{i,\text{BS},r}}{\mu + \sum_{n=1}^{k_r} g_n \times P_n}, \quad (8)$$

where k_r other devices are transmitting over the same resource with superimposed signal.

Moreover, the devices not competing in the uplink access (i.e. $k'_{t|C}$) for all the resources reduce the competition and improve the decoding at the BS. Assuming the uniform distribution of devices in clusters, and over all the resources, the uplink over resource r will also reduce with a factor of ($k'_{t|C,r} = k'_{t|C}/M$). In the proposed system, the SINR for a device transmitting to a BS $\text{SINR}_{i,\text{BS}|C,r}$, over resource r with transmit power of $P^1_{i,\text{BS},r}$, where total $k'_{t|C,r}$ devices do not create interference due to cluster participation, can be estimated as:

$$\text{SINR}_{i,\text{BS}|C,r} = \frac{|h_{i,\text{BS}}|^2 \times P^1_{i,\text{BS},r}}{\mu + \sum_{n=1}^{k-k'_{t|C}} g_n \times P_n} \quad (9)$$

The proposed SAFE-GF-NOMA scheme aims to reduce uplink competition, thereby decreasing interference for uplink transmissions. At the physical layer, a BS using uplink power control and successive interference cancellation (SIC) can decode and identify the specific resource blocks assigned to each transmission. The proposed aggregation method enhances the bit error rate at the BS by minimizing competition, which can be further improved by employing advanced encoding and decoding techniques at the physical layer [15]. Additionally, a variational interference-based receiver in non-orthogonal waveforms can effectively reduce inter-symbol interference (ISI). Evaluating the combined performance of our proposed aggregation method at the MAC layer and a low-complexity encoder at the physical layer presents an intriguing avenue for future research.

Moreover, we consider a peer-to-peer link between the device and CH using 802.11n with OFDM and channel bonding in a 2.4 GHz band with 20 MHz bandwidth. Assuming that the channel gain g and noise factor μ in a cluster is approximately similar to the OFDMA, the SINR for a device in a cluster communicating to the CH, can be estimated as [26]:

$$\text{SINR}_{i,C} = \frac{|h_{i,j}|^2 \times P_{i,C}}{\mu + \sum_{n=1}^{k'_{t|C}} g_n \times P_n} \quad (10)$$

The maximum achievable data rate for above stated all three scenarios (R_{BS}, $R_{\text{BS}|C}$, and R_C), can be calculated as:

$$R_{i,\text{BS}} = f \log(1 + \text{SINR}_{i,\text{BS},r}) \quad (11)$$

$$R_{i,\text{BS}|C} = f \log(1 + \text{SINR}_{i,\text{BS}|C,r}) \quad (12)$$

$$R_{i,C} = f \log(1 + \text{SINR}_{i,C}) \quad (13)$$

The total energy consumed to transmit content of size S_T bits, with an achievable data rate of R and a transmission power of P, can be calculated as $E = S_T.P/R$. Similar to the data rate, the energy consumption of a device communicating to the BS:

$$E_{i,\text{BS}} = S_T.P/R_{i,\text{BS}} = S_T.P_{i,\text{BS}}/(f \log(1 + \text{SINR}_{i,\text{BS},r})) \quad (14)$$

Similarly, energy consumption for a device (not in cluster) transmitting to the BS where total C devices are in clusters is:

$$E_{i,\text{BS}|C} = S_T.P/R_{i,\text{BS}|C} = S_T.P_{i,\text{BS}}/(f \log(1 + \text{SINR}_{i,\text{BS}|C,r})) \quad (15)$$

And, energy consumption for a device communicating to the CH becomes:

$$E_{i,C} = S_T.P/R_{i,C} = S_T.P_{i,C}/(f \log(1 + \text{SINR}_{i,C})) \quad (16)$$

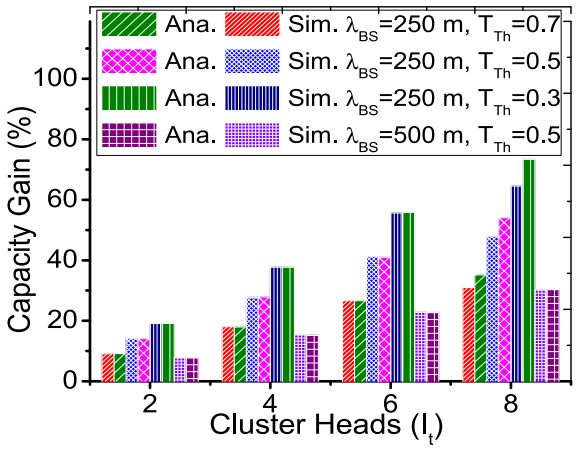

FIGURE 6. Capacity gain.

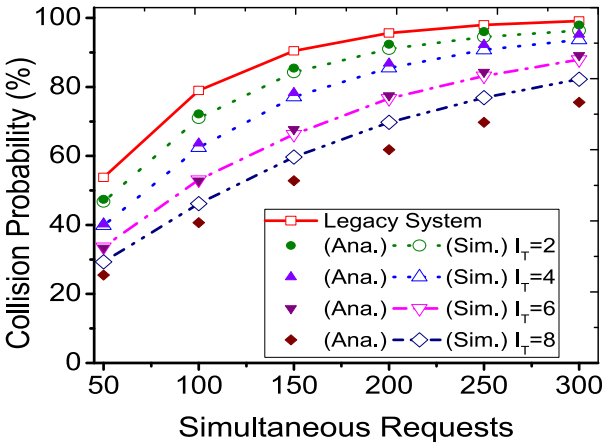

FIGURE 8. $\lambda_{BS} = 250$ m, $T_{Thresh} = 0.3$.

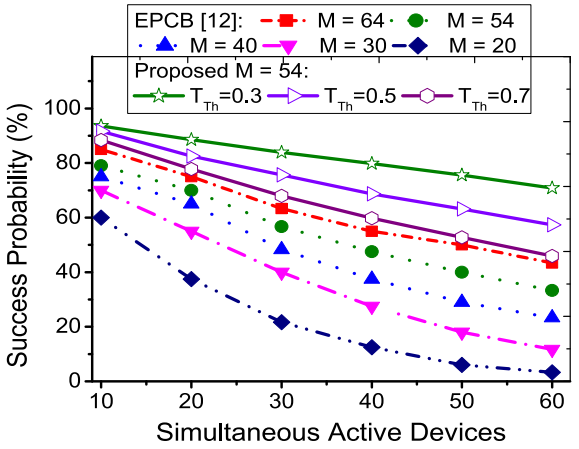

FIGURE 7. Success probability ($\lambda_{BS} = 250$ m and $I_t = 2$).

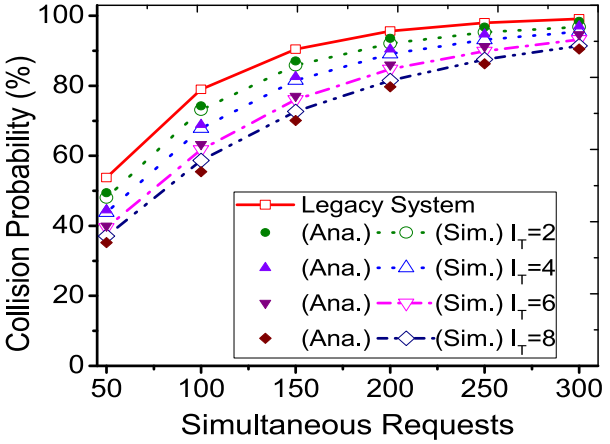

FIGURE 9. $\lambda_{BS} = 250$ m, $T_{Thresh} = 0.5$.

The above analysis points out that trustworthy clustering not only ensures privacy but also reduces interference, which in turn increases data rate and subsequently, less energy is consumed for each transmission. In the next section, we discuss results and observations to validate our claims.

V. PERFORMANCE EVALUATION AND RESULTS

To evaluate the efficacy of the proposed SAFE-GF-NOMA scheme, we present the impact of the proposed trustworthy aggregation on uncoordinated GF-NOMA uplink access collisions. Please note that in our evaluation a collision in the GF-NOMA is defined as two or more devices transmitting over the same frequency resource with the identical power level at the same time. Our exhaustive evaluation includes metrics of capacity gain, success, and collision probabilities with varying T_{Thresh} values. The simulation settings operate on two scenarios with cell coverage radii of 250 and 500 meters to represent densely and sparsely populated environments, respectively. In both scenarios, we consider a Poisson distribution of 50 to 300 devices, while each device is able to maintain a constant capillary communication range of 32 meters. We consider a typical point-to-point arrangement using IEEE 802.11n with a stock antenna, where the communication range is fixed to 32 meters. Moreover, the CHs (I_t) are uniformly distributed to ensure an equal number of devices within capillary communication proximity. Uniform distribution is deliberate to produce non-overlapping clusters for performance evaluation.

Following the aggregation scheme, each device joins a CH for resource sharing if its trust value ($T_{i,j} \in [0, 1]$) is higher or equal to T_{Thresh}. The initial trust is assumed to follow a random distribution; however, over time, our simulation model maintains and updates the $T_{i,j}$ accordingly. We assess the proposed SAFE-GF-NOMA scheme using various T_{Thresh} values of 0.3, 0.5, 0.7, and I_t values of 2, 4, 6, and 8. Please note that the number of CHs in a realistic scenario will be higher than the number of CHs used in the performance evaluation. The number of devices involved in aggregation is calculated using Equation (5) for both simulation and analytical experiments. To facilitate our analysis, we have developed a discrete event C++ simulator designed to replicate the behavior of our

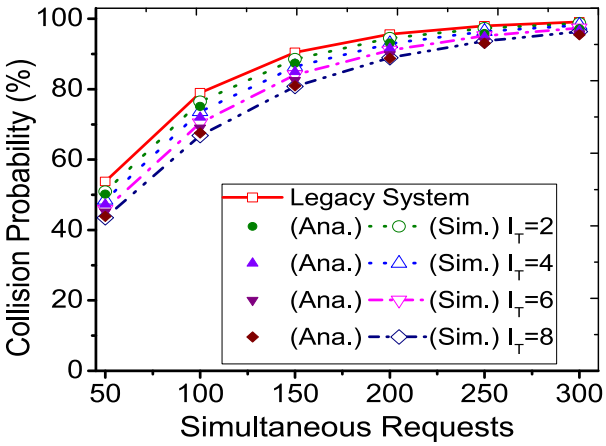

FIGURE 10. $\lambda_{BS} = 250$ m, $T_{\text{Thresh}} = 0.7$.

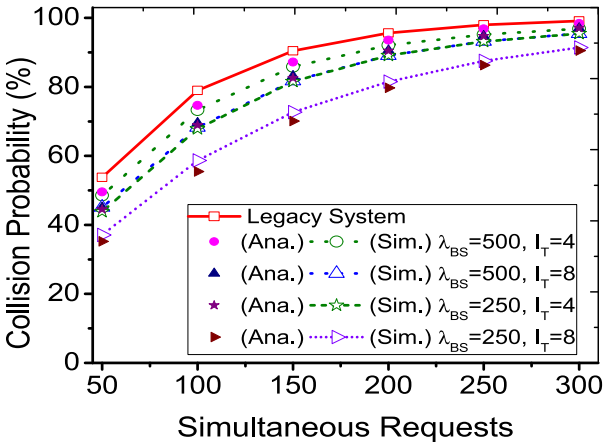

FIGURE 11. $\lambda_{BS} = 500$ m, $T_{\text{Thresh}} = 0.5$.

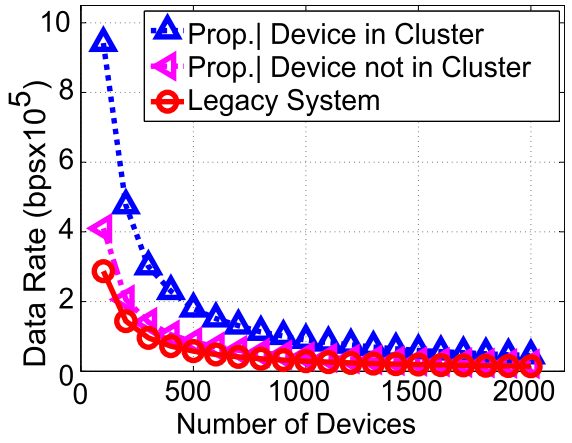

FIGURE 12. Average datarate.

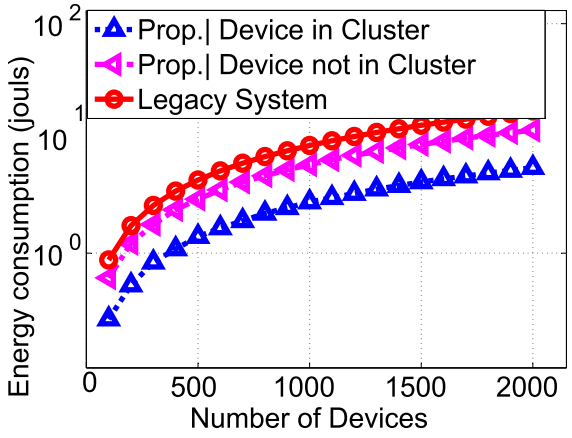

FIGURE 13. Average energy consumption.

proposed aggregation scheme. Devices utilize a random walk distribution to simulate mobility during each scheduling slot. We have considered that the power selection for GF-NOMA is dependent on the channel gain, which is estimated using distance. A random walk mobility distribution accurately replicates a low-mobility urban environment. Furthermore, to account for the random distribution of trust and users' random resource-power selection in GF-NOMA broadcast, we conduct exhaustive experiments comprising 96, 000 runs to observe simulation outcomes.

The analytical results using Equation (5) and simulation results of capacity gain of the proposed scheme are presented in Figure 6. Our SAFE-GF-NOMA aggregation achieved a capacity gain of up to $\sim$ 70% over the legacy cellular system when utilizing $I_t = 8$ and $T_{\text{Thresh}} = 0.3$. Moreover, increasing the cell radius and trust threshold as ($R = 500$ m) and $T_{\text{Thresh}} = 0.5$, respectively, demonstrates an approximate 10% gain even with only $I_t = 2$. A quick observation highlights that higher values of I_t or lower T_{Thresh} values lead to increased capacity gain, as they result in the aggregation of more devices and a reduction in the number of requested preambles. Interestingly, the operator-controlled parameter T_{Thresh} introduces a trade-off between privacy and capacity gain. Reducing the T_{Thresh} value significantly increases the capacity gain but at the expense of clustering devices with low privacy and trustworthiness. A higher T_{Thresh} value ensures better privacy but reduces capacity gain, while a lower T_{Thresh} value sacrifices privacy for higher capacity gain. Additionally, a smaller radius (e.g., $R = 250$ m) leads to a denser device distribution, further increasing the capacity gain. Please note that such control that allows application-specific configuration for privacy and resource sharing is not present in the existing state-of-the-art schemes. Figure 7 compares the success probability of aggregation and EPCB schemes [12] within a single scheduling slot, considering 54 GF-NOMA resource preambles and 10 $\sim$ 60 simultaneous user requests. We compare the proposed SAFE-GF-NOMA solution with EPCB [12] because it is the most relatable approach so far, and both the solutions operate on the devices without centrally provided information. As depicted, the success probability decreases for all systems as the number of requests increases in all schemes. However, EPCB with $M = 64$ achieves approximately 40% $\sim$ 84% success, while the proposed aggregation scheme surpasses this performance by providing 70% $\sim$ 88% success with $T = 0.3$. Moreover, across all scenarios of T_{Thresh}, aggregation shows a significant advantage of $\approx$ 40% $\sim$ 70% gain over the existing EPCB scheme, especially with a lower trust threshold

of $T_{\text{Thresh}} = 0.3$. This advantage comes from the device aggregation and resource-sharing capabilities of the proposed SAFE-GF-NOMA scheme, outperforming EPCB's barring technique.

To further investigate the proposed SAFE-GF-NOMA aggregation, we evaluate both the proposed and legacy systems in terms of collision probability for different T_{Thresh} values (0.3, 0.5, 0.7) while using a fixed set of 64 GF-NOMA resource-power broadcast preambles. Specifically, Figures 8 (for $T_{\text{Thresh}} = 0.3$) and Figure 9 (for $T_{\text{Thresh}} = 0.5$) illustrate that higher trust levels result in approximately 20 $\sim$ 30% fewer collisions in the proposed SAFE-GF-NOMA solution. It's worth noting that the choice of T_{Thresh} entails a tradeoff between gains and privacy. Interestingly, as T_{Thresh} or the cell coverage (λ_{BS}) reduces (i.e. device density increases), Figures 10 and Figure 11 demonstrate a further reduction in collision probability. The collisions reduce as low as 10% $\sim$ 20% in our solution as compared to the legacy system. Overall, aggregation achieves 10% $\sim$ 30% fewer collisions than the legacy system. Considering the 1 ms scheduling of GF-NOMA, on-demand clustering, and periodic TT updates, we assume that the proposed aggregation scheme can achieve similar performance in a mobile environment for low mobility or vehicular networks.

Furthermore, Figure 12 identifies that incorporating the proposed clustering scheme provides an approximate data rate of $\sim$ 0.9 Mbps to a device within a cluster and $\sim$ 0.4 Mbps to a device outside of a cluster. In comparison, devices in the legacy system experience a data rate of only $\sim$ 0.3 Mbps. Moreover, Figure 13 corroborates our findings by demonstrating that a device within a cluster requires only 0.26 $\sim$ 5 J to transmit a 1 Mbps file, while a device outside of a cluster requires 0.6 $\sim$ 12 J. In comparison, the legacy system demands 0.8 $\sim$ 17 J of energy for the same transmission. The proposed scheme not only benefits devices within clusters but also enhances the data rate and reduces energy consumption for devices outside of clusters. The impact of the proposed clustering on the overall system is due to the reduction in uplink access thus reducing the overall interference.

A. OVERHEAD AND LIMITATION

The evaluation of time and order complexity in the proposed SAFE-GF-NOMA system is based on quantifying the communication messages involved. Initially, each device communicates with its neighbors (CLOR_i), followed by trust calculations with common neighbors during the registration phase outlined in Algorithm 1. The complexity of the initial TT formulation phase can be approximated by the sum of message counts to direct neighbors and common neighbors, denoted as $O(\text{CLOR}_i + \sum_{j=1}^{k} \text{CLOR}_i \cap \text{CLOR}_j)$. It's worth noting that the registration phase is not frequent. Practically speaking, this means that the proposed system efficiently manages initial communication overhead through infrequent registration phases and streamlined clustering processes. The trade-off between overhead and performance gain is important, especially in real-world scenarios where network and cellular resources are often limited. The capacity gain and improved success probabilities not only justify the overhead but also highlight the system's potential for scalable and reliable IoT communications in 6G networks.

The clustering phase occurs after the initial TT population process, where initiators broadcast invitations to nearby devices, resulting in an estimated complexity of $O(\text{CLOR}_i)$. In the best-case scenario, each message could lead to capacity enhancement. Moreover, the participating devices only have to transmit to the selected CH. Despite the complexity, considering the capacity gain and success probability achieved through aggregation, the complexity remains an acceptable trade-off. By using the proposed SAFE-GF-NOMA trust-based clustering, the model keeps the communication overhead low and effectively supports the network's performance goals. This practical benefit shows that the model is suitable for use in heterogeneous and dynamic IoT environments, where it is crucial to allocate resources efficiently.

VI. CONCLUSION AND FUTURE WORK

Undoubtedly, GF-NOMA offers frequency reuse with minimal coordination between BS and IoT devices. However, the uplink contention in uncoordinated resource allocation resulted in additional delays and had a catastrophic impact when emergency services or disaster management communicated. In this study, an innovative, autonomous, and independent aggregation model, built on the Social Internet of Things (SIoT) relationships, was proposed. Subsequently, our SIoT-based aggregation is used to establish trustworthy clusters for efficient resource allocation in 6G cellular networks. Through extensive simulations and analytical experiments, the results demonstrated that the proposed aggregation achieved a remarkable capacity gain of approximately $\sim$ 70%. Moreover, the success probability exhibited a substantial improvement of around 40% $\sim$ 70% compared to the existing enhanced power choice barring scheme (EPCB) [12]. Additionally, the reduced competition for resources resulted in a significant reduction of approximately 10% $\sim$ 30% in collision probability compared to legacy systems.

Our future work will focus on refining trustworthiness management strategies to further reduce communication overhead and explore the application of SIoT principles in novel 6G applications. This includes:

- **Enhanced Trust Metrics**: Developing more sophisticated metrics for trustworthiness that consider dynamic and contextual factors, thereby improving the reliability of trust-based clustering.
- **Machine Learning Integration**: Incorporating machine learning algorithms to predict and adapt to changing network conditions, enhances the efficiency and robustness of resource allocation. The predicted trust

can reduce the communication overhead of local trust management.

- **Scalability Analysis**: Investigating the scalability of the proposed aggregation model in large-scale IoT networks such as IIoT and URLLC, ensuring its effectiveness in diverse and dense environments.
- **Energy Efficiency**: It is also interesting to consider multiple CHs in the same cluster to load balance and reduce energy consumption while considering the minimal uplink access burden. A prompt future direction can explore techniques to further optimize energy consumption in SIoT-enabled networks, particularly for battery-constrained IoT devices.
- **Security Enhancements**: Along with the proposed privacy preservation SIoT-based scheme, security measures can also be strengthened within the SIoT framework to protect against potential cyber threats and ensure data integrity and privacy.
- **Real-world Deployments**: Conducting real-world deployments and field trials to validate the theoretical and simulation-based findings, addressing practical challenges and enhancing the model's applicability.

Along with the above-given research problems, there can be various future directions aimed to build on the foundation established in our study. The boundaries of the SIoT-based autonomous trust management and aggregation can be pushed to ensure robust, efficient, and secure communication in 6G networks.

ACKNOWLEDGMENT

The authors would like to acknowledge the support provided by the Interdisciplinary Research Center for Communication Systems and Sensing (IRC-CSS) under the Deanship of Research Oversight and Coordination, King Fahd University of Petroleum & Minerals, Saudi Arabia.

REFERENCES

[1] Z. Ding, R. Schober, P. Fan, and H. V. Poor, "Next generation multiple access for IMT towards 2030 and beyond," 2024, *arXiv:2404.04012*.

[2] International Telecommunication Union. (Nov. 2023). *New Recommendation ITU-R M.2160 on the, IMT-2030 Framework*. [Online]. Available: https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Pages/default.aspx

[3] A. Kumar, J. Martinez-Bauset, F. Y. Li, C. Florea, and O. A. Dobre, "Understanding Inter- and intra-cluster concurrent transmissions for IoT uplink traffic in MIMO-NOMA networks: A DTMC analysis," *IEEE Internet Things J.*, vol. 11, no. 8, pp. 14328–14343, Apr. 2024.

[4] A. Shahini and N. Ansari, "NOMA aided narrowband IoT for machine type communications with user clustering," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 7183–7191, Aug. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8706532/

[5] W. Yuan, N. Wu, Q. Guo, Y. Li, C. Xing, and J. Kuang, "Iterative receivers for downlink MIMO-SCMA: Message passing and distributed cooperative detection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 3444–3458, May 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8316261

[6] W. Yuan, N. Wu, Q. Guo, D. W. K. Ng, J. Yuan, and L. Hanzo, "Iterative joint channel estimation, user activity tracking, and data detection for FTN-NOMA systems supporting random access," *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 2963–2977, May 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9006927

[7] D. Wu, Z. Zhang, Y. Huang, and X. Qin, "Priority-aware access strategy for GF-NOMA system in IIoT: The device-specific allocation approach," *IEEE Internet Things J.*, vol. 11, no. 2, pp. 2152–2165, Jan. 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10175515/

[8] W. Z. Khan, Q.-U.-A. Arshad, S. Hakak, M. K. Khan, and S.-U. Rehman, "Trust management in social Internet of Things: Architectures, recent advancements, and future challenges," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7768–7788, May 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9264256/

[9] F. Kilinc, R. A. Tasci, A. Celik, A. Abdallah, A. M. Eltawil, and E. Basar, "RIS-assisted grant-free NOMA: User pairing, RIS assignment, and phase shift alignment," *IEEE Trans. Cognit. Commun. Netw.*, vol. 9, no. 5, pp. 1257–1270, Oct. 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10159147/

[10] Y. Liu, Y. Deng, H. Zhou, M. Elkashlan, and A. Nallanathan, "Deep reinforcement learning-based grant-free NOMA optimization for mURLLC," *IEEE Trans. Commun.*, vol. 71, no. 3, pp. 1475–1490, Mar. 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10021621/

[11] C. Yuan, W. Ni, K. Zhang, J. Bai, J. Shen, and A. Jamalipour, "User pairing and power allocation in untrusted multiuser NOMA for Internet-of-Things," *IEEE Internet Things J.*, vol. 10, no. 15, pp. 13155–13167, Aug. 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10083323/

[12] L. Wu, X. Tang, Z. Zhang, and J. Dang, "Enhanced power choice barring scheme for massive MTCs with grant-free NOMA," *China Commun.*, vol. 18, no. 10, pp. 135–147, Oct. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9597641/

[13] M. Fayaz, W. Yi, Y. Liu, and A. Nallanathan, "Transmit power pool design for grant-free NOMA-IoT networks via deep reinforcement learning," *IEEE Trans. Wireless Commun.*, vol. 20, no. 11, pp. 7626–7641, Nov. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9452792/

[14] D.-D. Tran, S. K. Sharma, V. N. Ha, S. Chatzinotas, and I. Woungang, "Multi-agent DRL approach for energy-efficient resource allocation in URLLC-enabled grant-free NOMA systems," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 1470–1486, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10171215/

[15] N. Wu, Y. Zhang, H. Li, T. Zhang, J. Liu, X. Hou, and W. Liu, "Variational inference-based iterative receiver for unified non-orthogonal waveform (uNOW)," *IEEE Trans. Veh. Technol.*, vol. 73, no. 2, pp. 2848–2853, Feb. 2024.

[16] L. Li, H. Ma, H. Ren, Q. Cheng, D. Wang, T. Bai, and Z. Han, "Learning-aided resource allocation for pattern division multiple access-based SWIPT systems," *IEEE Wireless Commun. Lett.*, vol. 10, no. 1, pp. 131–135, Jan. 2021.

[17] F. Amin, A. Majeed, A. Mateen, R. Abbasi, and S. O. Hwang, "A systematic survey on the recent advancements in the social Internet of Things," *IEEE Access*, vol. 10, pp. 63867–63884, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9796539/

[18] K. C. Chung and S. W. Liang, "An empirical study of social network activities via social Internet of Things (SIoT)," *IEEE Access*, vol. 8, pp. 48652–48659, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9022870/

[19] P. Dong, J. Ge, X. Wang, and S. Guo, "Collaborative edge computing for social Internet of Things: Applications, solutions, and challenges," *IEEE Trans. Computat. Social Syst.*, vol. 9, no. 1, pp. 291–301, Feb. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9411933/

[20] L. Atzori, C. Campolo, B. Da, R. Girau, A. Iera, G. Morabito, and S. Quattropani, "Enhancing identifier/locator splitting through social Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2974–2985, Apr. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8502852/

[21] C.-H. Wang, J.-J. Kuo, D.-N. Yang, and W.-T. Chen, "Collaborative social Internet of Things in mobile edge networks," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11473–11491, Dec. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9171854/

[22] P. He and T. Tang, "Community-oriented multimedia content maximization mechanism in social Internet of Things," *IEEE Access*, vol. 8, pp. 22826–22833, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8976075/

[23] S. Dhelim, H. Ning, F. Farha, L. Chen, L. Atzori, and M. Daneshmand, "IoT-enabled social relationships meet artificial social intelligence," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17817–17828, Dec. 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9434396/

[24] S. Alam, S. Zardari, S. Noor, S. Ahmed, and H. Mouratidis, "Trust management in social Internet of Things (SIoT): A survey," *IEEE Access*, vol. 10, pp. 108924–108954, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9917502/

[25] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social Internet of Things (SIoT) – when social networks meet the Internet of Things: Concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128612002654

[26] F. H. Kumbhar, N. Saxena, and A. Roy, "Reliable relay: Autonomous social D2D paradigm for 5G LoS communications," *IEEE Commun. Lett.*, vol. 21, no. 7, pp. 1593–1596, Jul. 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7878557

FAROOQUE HASSAN KUMBHAR (Member, IEEE) has been a Postdoctoral Fellow with the IRC for Communication Systems and Sensing (CSS), King Fahd University of Petroleum and Minerals, Saudi Arabia, since 2024. Prior to this, he held the position of Brain Pool Postdoctoral Researcher with the School of Electronics, Kumoh National Institute of Technology, South Korea, in 2020 and 2021. He obtained extensive teaching experience as an Assistant Professor and an Associate Professor with the FAST-National University of Computer and Emerging Sciences, Pakistan, from 2017 to 2019 and from 2022 to 2023, respectively. His research is dedicated to leveraging artificial intelligence, reinforcement learning, graph theory, and optimization to tackle pivotal challenges in 6G networks, vehicular networks, ad-hoc networks, mobile communications, C-RAN, privacy, the Internet of Things, and machine-to-machine communication. He boasts a prolific publication record in prestigious Q1 journals of IEEE, Springer, IETE, and IET.

SALAHUDDIN UNAR (Member, IEEE) received the B.E. and M.E. degrees in computer engineering from Pakistan, in 2013 and 2015, respectively, and the Ph.D. degree in computer software and theory from Dalian University of Technology, China, in 2019. He was a Postdoctoral Researcher with Dalian Maritime University, China, from 2021 to 2023. He is currently an Associate Professor with the Qilu Institute of Technology, Jinan, Shandong. He has published several research articles in top core SCI and EI journals and has hundreds of citations. His research interests include image processing, computer vision, information retrieval, and pattern recognition.

WESSAM MESBAH (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees (Hons.) in electrical engineering from Alexandria University, Alexandria, Egypt, in 2000 and 2003, respectively, and the Ph.D. degree from McMaster University, Hamilton, ON, Canada, in 2008. From 2009 to 2010, he was a Postdoctoral Research Fellow with Texas A&M University, Doha, Qatar. He joined the Electrical Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, in 2010, where he is currently an Associate Professor. His research interests include wireless networks and wireless technologies, quantum communications, optimization, federated learning, game theory, smart metering, and smart grids. Since January 2024, he has been an Associate Editor of IEEE COMMUNICATIONS LETTERS.

DANIEL BENEVIDES DA COSTA (Senior Member, IEEE) received the B.Sc. degree in telecommunications from the Military Institute of Engineering (IME), Rio de Janeiro, Brazil, in 2003, and the M.Sc. and Ph.D. degrees in electrical engineering, area: telecommunications, from the University of Campinas, São Paulo, Brazil, in 2006 and 2008, respectively. He is currently a Distinguished University Professor with the Department of Electrical Engineering, King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia. His Ph.D. thesis was awarded the Best Ph.D. Thesis in Electrical Engineering by the Brazilian Ministry of Education (CAPES) at the 2009 CAPES Thesis Contest. He is the Editor-in-Chief of IEEE COMMUNICATIONS LETTERS. He was recognized as the World's Top 2% Scientist by Stanford University (2021, 2022, and 2023) and has been ranked among 1% Top Scientists in the world in the broad field of electronics and electrical engineering, in 2022 and 2023 (Source: Research.com). He is also a Distinguished Speaker of the IEEE Vehicular Technology Society.