Architecting advanced IoT services: from communication to social perspective

Politecnico di Bari

Department of Electrical and Information Engineering
Electrical and Information Engineering
Ph.D. Program
SSD: ING-INF/03– Telecommunications

Final Dissertation

Architecting Advanced IoT Services: From Communication to Social Perspective

---

by
Giancarlo Sciddurlo

Supervisors:

Prof. Domenico Striccoli
Prof. Giuseppe Piro

Coordinator of Ph.D. Program:
Prof. Mario Carpentieri

Course n°36, 01/11/2020-31/10/2023

Politecnico di Bari

LIBERATORIA PER L'ARCHIVIAZIONE DELLA TESI DI DOTTORATO

Al Magnifico Rettore
del Politecnico di Bari

Il sottoscritto Giancarlo Sciddurlo nato a Mola di Bari (BA) il 23/06/1989 residente a Mola di Bari (BA) in via Padre Pio 47/b e-mail giancarlosciddurlo@gmail.com iscritto al 3° anno di Corso di Dottorato di Ricerca in Electrical and Information Engineering ciclo XXXVI ed essendo stato ammesso a sostenere l'esame finale con la prevista discussione della tesi dal titolo:

Architecting Advanced IoT Services: from Communication to Social Perspective

DICHIARA

1) di essere consapevole che, ai sensi del D.P.R. n. 445 del 28.12.2000, le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti ai sensi del codice penale e delle Leggi speciali in materia, e che nel caso ricorressero dette ipotesi, decade fin dall'inizio e senza necessità di nessuna formalità dai benefici conseguenti al provvedimento emanato sulla base di tali dichiarazioni;
2) di essere iscritto al Corso di Dottorato di ricerca Electrical and Information Engineering ciclo XXXVI, corso attivato ai sensi del "*Regolamento dei Corsi di Dottorato di ricerca del Politecnico di Bari"*, emanato con D.R. n.286 del 01.07.2013;
3) di essere pienamente a conoscenza delle disposizioni contenute nel predetto Regolamento in merito alla procedura di deposito, pubblicazione e autoarchiviazione della tesi di dottorato nell'Archivio Istituzionale ad accesso aperto alla letteratura scientifica;
4) di essere consapevole che attraverso l'autoarchiviazione delle tesi nell'Archivio Istituzionale ad accesso aperto alla letteratura scientifica del Politecnico di Bari (IRIS-POLIBA), l'Ateneo archivierà e renderà consultabile in rete (nel rispetto della Policy di Ateneo di cui al D.R. 642 del 13.11.2015) il testo completo della tesi di dottorato, fatta salva la possibilità di sottoscrizione di apposite licenze per le relative condizioni di utilizzo (di cui al sito http://www.creativecommons.it/Licenze), e fatte salve, altresì, le eventuali esigenze di "embargo", legate a strette considerazioni sulla tutelabilità e sfruttamento industriale/commerciale dei contenuti della tesi, da rappresentarsi mediante compilazione e sottoscrizione del modulo in calce (Richiesta di embargo);
5) che la tesi da depositare in IRIS-POLIBA, in formato digitale (PDF/A) sarà del tutto identica a quelle **consegnate**/inviate/da inviarsi ai componenti della commissione per l'esame finale e a qualsiasi altra copia depositata presso gli Uffici del Politecnico di Bari in forma cartacea o digitale, ovvero a quella da discutere in sede di esame finale, a quella da depositare, a cura dell'Ateneo, presso le Biblioteche Nazionali Centrali di Roma e Firenze e presso tutti gli Uffici competenti per legge al momento del deposito stesso, e che di conseguenza va esclusa qualsiasi responsabilità del Politecnico di Bari per quanto riguarda eventuali errori, imprecisioni o omissioni nei contenuti della tesi;
6) che il contenuto e l'organizzazione della tesi è opera originale realizzata dal sottoscritto e non compromette in alcun modo i diritti di terzi, ivi compresi quelli relativi alla sicurezza dei dati personali; che pertanto il Politecnico di Bari ed i suoi funzionari sono in ogni caso esenti da responsabilità di qualsivoglia natura: civile, amministrativa e penale e saranno dal sottoscritto tenuti indenni da qualsiasi richiesta o rivendicazione da parte di terzi;
7) che il contenuto della tesi non infrange in alcun modo il diritto d'Autore né gli obblighi connessi alla salvaguardia di diritti morali od economici di altri autori o di altri aventi diritto, sia per testi, immagini, foto, tabelle, o altre parti di cui la tesi è composta.

Bari, 31/10/2023 Firma _____

Il sottoscritto, con l'autoarchiviazione della propria tesi di dottorato nell'Archivio Istituzionale ad accesso aperto del Politecnico di Bari (POLIBA-IRIS), pur mantenendo su di essa tutti i diritti d'autore, morali ed economici, ai sensi della normativa vigente (Legge 633/1941 e ss.mm.ii.),

CONCEDE

- ☐ al Politecnico di Bari il permesso di trasferire l'opera su qualsiasi supporto e di convertirla in qualsiasi formato al fine di una corretta conservazione nel tempo. Il Politecnico di Bari garantisce che non verrà effettuata alcuna modifica al contenuto e alla struttura dell'opera.
- ☐ al Politecnico di Bari la possibilità di riprodurre l'opera in più di una copia per fini di sicurezza, back-up e conservazione.

Bari, 31/10/2023 Firma _____

Politecnico di Bari

Department of Electrical and Information Engineering
Electrical and Information Engineering
Ph.D. Program
SSD: ING-INF/03– Telecommunications

Final Dissertation

Architecting Advanced IoT Services: from communication to Social Perspective

---

by

Giancarlo Sciddurlo

Referees:
Prof. Luigi Atzori
Prof. Savio Sciancalepore

Supervisors:
Prof. Domenico Striccoli
Prof. Giuseppe Piro

Coordinator of Ph.D Program:
Prof. Mario Carpentieri

Course n°36, 01/11/2020-31/10/2023

«He smiled understandingly – much more than understandingly. It was one of those rare smiles with a quality of eternal reassurance in it, that you may come across four or five times in life. It faced – or seemed to face – the whole external world for an instant, and then concentrated on you with an irresistible prejudice in your favor. It understood you just as far as you wanted to be understood, believed in you as you would like to believe in yourself, and assured you that it had precisely the impression of you that, at your best, you hoped to convey.»

«The truth was that Jay Gatsby, of West Egg, Long Island, sprang from his Platonic conception of himself. He was a son of God—a phrase which, if it means anything, means just that—and he must be about His Father's business, the service of a vast, vulgar, and meretricious beauty. So he invented just the sort of Jay Gatsby that a seventeen year old boy would be likely to invent, and to this conception he was faithful to the end.»

«Gatsby believed in the green light, the orgastic future that year by year recedes before us. It eluded us then, but that's no matter—tomorrow we will run faster, stretch out our arms farther... And then one fine morning... So we beat on, boats against the current, bone back ceaselessly into the past.»

F. Scott Fitzgerald

POLITECNICO DI BARI

Abstract

Department of Electrical and Information Engineering

Doctor of Philosophy

Architecting Advanced IoT Services: from Communication to Social Perspective

by Giancarlo SCIDDURLO

The advent of the Internet of Things (IoT) has marked the onset of a transformative era characterized by the proliferation of interconnected devices, resulting in the generation of vast amounts of data and the promise of extensive applications across various fields. To fully harness the potential of IoT and ensure its uninterrupted functionality, there is a critical need for the implementation of highly efficient service provisioning. IoT encompasses heterogeneous entities, all of which require reliable access to network services and resources while adhering to stringent Quality of Service (QoS) requirements, including low latency, scalability, and security, as mandated by numerous applications. In response to these challenges, the presented research proposes the design of advanced architectures and strategies that span from communication to security perspectives, facilitating QoS provisioning in IoT environments. Specifically, i) the adoption of NB-IoT technology in satellite communications aims to extend IoT services beyond the limitations imposed by current terrestrial infrastructures; ii) enhancing the social skills of IoT entities through virtualization to support the selection of a suitable provider capable of accomplish the required service.

Acknowledgements

Thanks to my supervisors, Domenico Striccoli and Giuseppe Piro, and the entire Telematics Lab, who have always supported the realization of this work. Especially, many thanks to my colleagues Antonio Petrosino, Ingrid Huso, my most precious one 'agenda' Federica deTrizio, Prof. Pietro Camarda, and Nicola Cordeschi, who collaborate and work with me in the realization of my paper activities during my Ph.D.

Giancarlo Sciddurlo gratefully acknowledges the Politecnico di Bari for the support of his PhD scholarship. Some contribution are the result of research activities carried out by different academic and industrial partners, collaborating as a partnership in the context of the project "3GPP Narrow-Band Internet-of-Things (NB-IoT) User Sensor Integration into Satellite" funded by the European Space Agency (ESA) under contract no. 4000129810/20/NL/CLP, https://artes.esa.int/projects/nbiot4space or partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART").

Above all else, to my mom and dad.

Contents

List of Figures

List of Tables

List of Acronyms

KPI Key Performance Indicator

B5G Beyond 5G

BER Bit Error Rate

BLER Block Error Rate

C-LOR Co-Location Object Relationship

C-WOR Co-Work Object Relationship

CFO Carrier Frequency Offset

CIoT Cellular IoT

CoAP Constrained Application Protocol

COTS Commercial-Off-The-Shelf

CRC Cyclic Redundancy Check

CU Centralized Unit

DT Digital Twin

DTDL Digital Twin Definition Language

DU Distributed Unit

EDT Early Data Transmission

eNB evolved Node-B

EPC Evolved Packet Core

EPS Evolved Packet System

ESA European Space Agency

GEO geostationary Earth orbit

GNSS Global Navigation Satellite System

GoS Grade of Service

HARQ Hybrid Automatic Repeat Request

HAP High-altitude Platforms

HPA High Power Amplifier

HPBW Half Power Beam Width

HSS Home Subscriber Server

IAB Integrated Access Backhaul

IBN Intent-based network

IoE Internet of Everything

IoT Internet of Things

ISL Inter Satellite Link

LBO Local Break-Out

LEO low Earth orbit

LPWAN Low Power Wide Area Network

LTE Long Term Evolution

M2M Machine-to-Machine

MAC Medium Access Control

MCDM Multi Criteria Decision Making

MCL Maximum Coupling Loss

MCS Modulation and Coding Scheme

MME Mobility Management Entity

MTC Machine Type Communication

NAS Non-Access Stratum

NB-IoT NarrowBand-IoT

NDT Network Digital Twin

NFV Network Function Virtualization

NGSO non-geostationary Earth orbit

NIDD Non-IP Data Delivery

NPBCH Narrowband Physical Broadcast Channel

NPDCCH Narrowband Physical Downlink Control Channel

NPDSCH Narrowband Physical Downlink Shared Channel

NPRACH Narrowband Physical Random Access Channel

NPUSCH Narrowband Physical Uplink Shared Channel

NR New Radio

NRU Number of Resource Units

NTN Non-Terrestrial Network

OFDM Orthogonal Frequency-Division Multiplexing

OOR Ownership Object Relationship

OWC Optical Wireless Communication

P-GW Packet Gateway

PDCP Packet Data Convergence Protocol

PDU Protocol Data Unit

PHY Physical

POR Parental Object Relationship

QoE Quality of Experience

QoS Quality of Service

RAO Random Access Occasion

RC Relative Closeness

RLC Radio Link Control

RRC Radio Resource Control

RTD Round Trip Delay

RTT Round Trip Time

RU Resource Unit

SatCom Satellite Communication

S-GW Serving Gateway

SCEF Service Capabilities Exposure Function

SC-FDMA Single Carrier Frequency Division Multiple Access

SDN Software Defined Network

SIoT Social Internet of Things

SIoE Social Internet of Everything

SLA Service Level Agreements

SNR Signal to Noise Ratio

SOR Social Object Relationship

TA Timing Advance

TBS Transport Block Size

TMS Trust Management System

TN-NTN terrestrial-non-terrestrial network

TTI Transmission Time Interval

UAV Unmanned Aerial Vehicle

UE User Equipment

YANG Yet Another Next Generation

WSN Wireless Sensor Network

Scientific Contributions

All the scientific contributions produced during the doctoral course are listed below.

International Journals:

- G. Sciddurlo et al., "Looking at NB-IoT Over LEO Satellite Systems: Design and Evaluation of a Service-Oriented Solution," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14952-14964, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3135060.

- G. Sciddurlo, P. Camarda, D. Striccoli, G. Piro, G. Boggia, "A Markov Chain Analytical Model Supporting Service Provisioning and Network Design in the Social Internet of Everything ", in IEEE/ACM Transactions On Networking, 2023 (submitted).

International Conferences:

- A. Petrosino, G. Sciddurlo, S. Martiradonna, D. Striccoli, G. Piro and G. Boggia, "WIP: An Open-Source Tool for Evaluating System-Level Performance of NB-IoT Non-Terrestrial Networks," 2021 IEEE 22nd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Pisa, Italy, 2021, pp. 236-239, doi: 10.1109/WoWMoM51794.2021.00042.

- G. Sciddurlo, I. Huso, D. Striccoli, G. Piro and G. Boggia, "A Multi-tiered Social IoT Architecture for Scalable and Trusted Service Provisioning," 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 2021, pp. 1-6, doi: 10.1109/GLOBECOM46510.2021.9685084.

- G. Sciddurlo, A. Petrosino, D. Striccoli, G. Piro, L. A. Grieco and G. Boggia, "Boosting Service Provisioning in SIoT by Exploiting Trust and Capability Levels of Social Objects," 2022 IEEE International Conference on Smart Computing (SMARTCOMP), Helsinki, Finland, 2022, pp. 1-6, doi: 10.1109/SMARTCOMP55677.2022.00077.

- F. de Trizio, G. Sciddurlo, I. Cianci, D. Striccoli, G. Piro, G. Boggia, "Surviving Disaster Events Via Dynamic In-Network Processing Assisted by Network Digital Twin ", Proc. of 8th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Cosenza 2023.

- F. Matera, M. Settembre, P. Salvo, S. Morosi, L. A. Grieco, G. Piro, A. Guidotti, L. Pierucci, A. Vanelli-Coralli, M. Ruggieri, G. Iacovelli, G. Araniti, S. Pizzi, L. Oliviero, G. Bacci, G. Sciddurlo, and A. Gotta, “From interoperability to full integration - the ITA NTN project vision,” in European Wireless 2023 - 6G Driving a Sustainable Growth (EW 2023), Rome, Italy, Oct. 2023.

Introduction to the Internet of Things in 5G and Beyond Networks

In 2020, the Internet of Things (IoT) achieved a significant milestone with a staggering 20 billion connected devices, catalyzing a remarkable transformation across both business and consumer domains. This extraordinary development marked the inception of a new industrial revolution. It's worth noting that by this time, the number of objects connected to the Internet had already exceeded the global population, and projections for 2025 anticipate an even more extensive network, estimating approximately 37 billion interconnected devices, with 25 billion directly affiliated with the IoT [1].

The foundational concept of the IoT revolves around networks, devices, and data, forming the cornerstone for communication and interaction among objects and embedded devices within diverse environments. At present, the IoT encompasses an extensive network that includes a variety of elements, such as basic sensors, smartphones, wearables, autonomous vehicles, drones, and other interconnected components. Through the IoT, devices acquire the capacity to collect, exchange, and analyze data, facilitating seamless communication with central systems, often operating autonomously. The interconnected ecosystem of devices and data sharing is designed to process and leverage the resulting information and knowledge to enable more intelligent and automated actions. This dynamic offers a multitude of possibilities, ranging from automation and data-driven decision-making to enhanced efficiency, with significant implications for a wide range of industries and aspects of daily life.

Data generated by IoT devices takes the form of large-scale streaming data, characterized by its heterogeneity, high noise levels, and significant concerns related to privacy, reliability, and security. Extracting valuable insights from this diverse data typically requires transmitting it to the cloud or fusion centers via wireless networks. Consequently, wireless networks play a pivotal role in facilitating the widespread adoption of IoT devices. In recent years, extensive research has been dedicated to classifying IoT technologies. A widely accepted classification system categorizes IoT networks based on their coverage range, resulting in divisions such as cellular, wide-area, and short-range IoT networks.

In addition, the widespread expansion of IoT applications is currently confronting several challenging scenarios. This includes the deployment of IoT devices in geographical areas where terrestrial networks are either absent or challenging to access, such as deserts, oceans, or forests. In such contexts, ensuring uninterrupted service and rapid deployment can be successfully achieved only through the adoption of innovative methodologies that transcend the limitations imposed by current terrestrial networks. A recent classification known as NTN has emerged, offering extensive coverage and representing a more comprehensive evolution encompassing both cellular and wide-area networks.

In recent times, both scientific literature and the 3GPP standardization body have been exploring the feasibility of integrating NarrowBand-IoT (NB-IoT) into satellite-based communication architectures with the objective of enhancing IoT services. Furthermore, beyond the link-level studies featured in scientific literature and the initial 3GPP technical reports, the ongoing discussion provides an opportunity to advance this integration. This can be achieved through concurrent investigations at both the link-level and system-level to optimize physical transmissions, satellite constellations, and protocol architectures. It is essential that these efforts align with the desired system behavior and follow a novel, service-oriented methodology that centers around the meticulous alignment of application requirements and technological constraints. This approach sets the stage for the development of an effective proof-of-concept, which holds the potential to significantly reduce the time-to-market, currently restricted by prevailing state-of-the-art practices.

As the envision of the future of network technology, concepts such as device-to-device and machine-to-machine communications are poised to assume pivotal roles. These concepts involve connecting objects equipped with identification, sensing, and processing capabilities, enabling seamless communication with other devices. These networked devices are well-suited to facilitate a range of collaborative tasks, including remote data sensing, individual identification, and remote home control. Concurrently, the deployment of 5G networks in various regions across Europe, the United States, and Asia has spurred extensive research in anticipation of the emergence of what is known as Beyond 5G (B5G) networks. These networks, among other requirements, aim to provide higher peak data rates, universal connectivity, low latency, enhanced reliability, improved energy efficiency, widespread intelligence, and inherent security. Furthermore, the ongoing surge in demand for mobile data traffic, driven by web applications, real-time streaming, and IoT applications, is expected to exert additional pressures on B5G networks. These networks will need to accommodate a significant increase in the number of connected IoT devices and a substantial rise in multimedia traffic. To ensure the necessary level of network quality and user experience for such traffic, the provision of Quality of Service (QoS) guarantees assumes a central role in the context of next-generation wireless networks. Moreover, the anticipated proliferation of application using IoT entities in B5G networks raises concerns related to scalability [2] and trustworthiness [3].

In response to these challenges, various architectures and solutions for QoS provisioning have been proposed. These solutions leverage technologies such as Software Defined Network (SDN), virtualization functions, and social skills to reallocate responsibilities from network core devices. They also employ effective strategies for evaluating and managing the trustworthiness of the entities involved. In this context, the concept of Social Internet of Things (SIoT) is gaining momentum thanks to its unique ability to autonomously establish social relationships among smart objects and facilitate novel services within a Social Network of IoT entities. When it comes to service provisioning, the SIoT uses its social capabilities to prioritize the selection of appropriate objects capable of delivering the requested services.

This underscores the essential role of orchestration in the service provisioning process for the IoT. Orchestration involves the coordination and management of various elements, including components, resources, and processes essential for delivering IoT services. It is indispensable for managing complexity, optimizing resource utilization,

ensuring scalability, and facilitating adaptability in the ever-evolving IoT landscape. Orchestration not only enhances the efficiency, reliability, and security of IoT services but also empowers organizations to fully harness the expansive potential of IoT across diverse applications and industries. An emerging technology that actively facilitates the orchestration of the IoT ecosystem, along with the management of services, network resources, and processing, is referred to as Network Digital Twin (NDT), as discussed in [4]. By creating a virtual representation of a physical system and transferring tasks from one domain to another, NDT harnesses the potential to analyze performance metrics and make informed decisions, thus representing a key enabler for 5G and beyond.

The convergence of IoT and 5G technologies offers the promise of transforming industries and everyday life. Nevertheless, this convergence introduces intricate challenges in areas such as security, interoperability, data management, energy efficiency, and more. Effectively addressing these challenges is of paramount importance to fully realize the potential benefits of IoT in the 5G era and beyond.

The rest of this thesis is organized as follows:

- *How can we design a service-oriented solution for implementation in remote areas where terrestrial technologies face limitations or are absent?*
  In chapter 1, a comprehensive framework for providing NB-IoT over satellite services, aligned with 3GPP specifications, is introduced. The objective is to address the significant challenges associated with the practical implementation of NB-IoT over NTN in real-world applications.

- *How can we enhance network navigability while ensuring reliability and scalability in the service provisioning process of IoT entities?*
  chapter 2 focuses on the social perspective, presenting the design and development of innovative architectures and trusted communication protocols in a SIoT environment.

- *In what application scenario can the virtualization of involved entities be used to enhance network service provisioning efficiency?*
  chapter 3 illustrates a particular use case developed by employing non-terrestrial elements within a virtualized ecosystem, leveraging social attributes through Digital Twin (DT).

- *How can we model attributes such as reputation and available resources in a social IoT environment to promote service provisioning?*
  chapter 4 discusses the analysis of a real-world scenario through a Markov Chain Model aimed at supporting service provisioning and appropriately designing the SIoE network.

Finally, chapter 4.4.4 draws final remarks.

Chapter 1

Design of a Service Oriented Solution over Non-Terrestrial Network

The rapid proliferation of IoT applications has introduced a series of challenges scenarios. This notably involves the deployment of devices in geographic locations where terrestrial networks are absent or hard to reach. In such circumstances, the successful achievement of service continuity and the rapid deployment of services necessitates the adoption of disruptive methodologies that transcend the limitations imposed by current terrestrial networks.

The utilization of Satellite Communication (SatCom) is expected to play a primary and predominant role in the context of 5G and subsequent generations of networks, as articulated in the research conducted in [5]. This prominence is attributed to its inherent ubiquity and resilience in the face of natural disasters. These qualities enable SatCom to facilitate the expansion of network coverage in a cost-effective manner by providing connectivity in regions devoid of telecommunication infrastructures, including, but not limited to, areas such as oceans, forests, and deserts. This cutting-edge connectivity model can naturally provide backup links in the event of network failures. Furthermore, it can provide additional connections to offload terrestrial networks while maintaining the performance of loss or delay-sensitive applications. Simultaneously, it significantly fosters the scalability of mobile networks by facilitating potential future extensions of existing 5G deployments through satellite support. Here, the primary challenge lies in providing connectivity to a vast multitude of devices, some of which may have specific design constraints or conflicting Key Performance Indicators (KPIs), such as the need for extended battery life and long transmission ranges. In this overarching context, researchers worldwide are actively exploring the feasibility of employing NB-IoT as a promising communication technology to enable the forthcoming Non-Terrestrial Networks.

Taking these premises into account, this chapter is structured as follows:

- section 1.1 provides a concise overview of NB-IoT radio access technology.
- section 1.2 presents a comprehensive review of the state-of-the-art research pertaining to NB-IoT technology in satellite systems.
- In section 1.3, the work published in [6] is described, offering insights into the implemented link-to-system abstraction models, which encompass transmission, propagation, and reception mechanisms. Additionally, it introduces a new mobility model and the cell selection procedure, successfully integrated within the broader framework of the 5G-air-simulator.

- Following the definition of the smart agriculture reference scenario, section 1.4 outlines the overall protocol architecture and the associated low-level adaptations necessary for the integration of the NTN NB-IoT system. This section provides a comprehensive link-level study, as detailed in [7].
- Lastly, section 1.5 presents potential TN-NTN architecture configurations of interest within the ITA NTN project.

1.1 NB-IoT Radio Access Technology

NB-IoT represents a powerful Low Power Wide Area Network (LPWAN) radio communication technology engineered to accommodate a substantial volume of devices across expansive regions, ensuring cost-efficiency and extended battery life. It is specifically tailored for applications characterized by small and sporadic data transmissions, as outlined in [8]. The 3rd Generation Partnership Project (3GPP) has formally standardized NB-IoT within Release-13 to address the connectivity needs of IoT devices within the framework of mobile network infrastructure, as documented in [9].

NB-IoT uses a subset of the well-known Long Term Evolution (LTE) technological capabilities, confining its operations to a single carrier bandwidth of 180 kHz, which characterizes it as a narrow-band technology [10]. Furthermore, to expand the link capacity, the use of multiple carriers is a viable option. These carriers, in a general sense, can be deployed within an LTE channel (referred to as in-band), within the guard-bands of the LTE bandwidth (known as guard-band), or mapped onto GSM carriers of 200 kHz (termed as stand-alone).

Similar to LTE, at the physical layer, the downlink employs the Orthogonal Frequency-Division Multiplexing (OFDM) transmission scheme, utilizing 12 subcarriers with a subcarrier spacing of 15 kHz, as defined in [11]. The frame's duration is 10 ms, comprised of 10 subframes, each lasting 1 ms, referred to as TTIs. Each subframe, in turn, comprises two slots, with seven OFDM symbols. On the other hand, the uplink employs the Single Carrier Frequency Division Multiple Access (SC-FDMA) transmission scheme, differentiating it from LTE. Two possible configurations are supported: single-tone and multi-tone, with the multi-tone configuration retaining a subcarrier spacing of 15 kHz.

The Resource Unit (RU), which signifies the smallest radio resource that can be allocated to an end-user, extends over 3, 6, or 12 adjacent subcarriers and has durations of 4 ms, 2 ms, or 1 ms, respectively, in line with [12]. In contrast, the single-tone configuration can operate with a subcarrier spacing of either 15 kHz or 3.75 kHz, with only one subcarrier being available to a single user in the latter case. The choice of transmission configuration dictates the size of the RU, as presented in 1.1. Depending on the subcarrier spacing, the uplink bandwidth is divided into either 12 or 48 RU, each with durations of 8 ms and 32 ms, respectively, in accordance with [13].

Broadly, NB-IoT repurposes the pre-existing LTE physical channels, encompassing Narrowband Physical Downlink Shared Channel (NPDSCH), Narrowband Physical Downlink Control Channel (NPDCCH), and Narrowband Physical Broadcast Channel (NPBCH) for the downlink, and Narrowband Physical Uplink Shared Channel (NPUSCH) for the uplink, making necessary adjustments to align them with the

TABLE 1.1: TTI sizes

Transmission	Subcarriers	Δf	BW	Slots	TTI
Single-Tone	1	3.75 kHz	3.75 kHz	16	32 ms
	1	15 kHz	15 kHz	16	8 ms
Multi-Tone	3	15 kHz	45 kHz	8	4 ms
	6	15 kHz	90 kHz	4	2 ms
	12	15 kHz	180 kHz	2	1 ms

narrower bandwidth requirements. Furthermore, it introduces a novel Narrowband Physical Random Access Channel (NPRACH) configured to utilize the single-tone setup with a subcarrier spacing of $\Delta f = 3.75$ kHz, aimed at augmenting capacity during the Random Access Procedure [14].

Ultimately, the repetition of transmissions stands as a key facilitator for achieving an extended coverage in NB-IoT. Fundamentally, each transmission can be replicated a user-defined number of times to enhance the probability of successful reception. Nevertheless, the extension of coverage comes at the cost of increased transmission rates. It's worth noting that all NB-IoT channels can derive advantages from this repetition mechanism, ensuring the fulfillment of coverage requirements in a well-adapted manner.

1.2 State-of-the-Art on NB-IoT over satellite systems

The State-of-the-Art review is structured as follows: initially, subsection 1.2.1 examines scientific contributions that center on NB-IoT when integrated with satellite systems. Subsequently, subsection 1.2.2 presents an overview of recent 3GPP initiatives related to NTN networks. These two sections also highlight the scientific and technical gaps addressed within this study.

1.2.1 Related Works on NB-IoT over satellite links

In scientific literature, extensive exploration has been conducted on the feasibility of incorporating NB-IoT into satellite-based communication systems with specific adaptations. In particular, system-level performance analysis offers several benefits, helping organizations and engineers optimize the functionality and efficiency of their systems. As outlined in Table 1.2, prior studies have primarily focus the attention on several key topics, including the analysis and selection of suitable antenna types [15]–[17], the assessment of link budgets [15]–[21], satellite constellation design [18], [22], link-level performance investigations [15], [21], Doppler shift evaluations [16], [17], [19], [21]–[24], and management of the Random Access Procedure [16], [23], [24]. Notably, other relevant works, such as [25] and [26], have examined the Doppler shift and Random Access Procedure in satellite communication systems based on LTE and 5G, respectively. These studies, while addressing specific facets of the system, often operate under varying assumptions, leading to a somewhat fragmented body of research.

Nevertheless, the seamless integration of NB-IoT into satellite networks demands a comprehensive approach that integrates service-oriented considerations. This approach takes into careful consideration the intricate interplay of protocols, architectural, physical, and functional elements to form a unified whole. In this context, the main goal of this chapter (and the works published in [6] and [7]) is to provide a thorough description, review, refinement, redefinition, modeling, and simulation of each relevant aspect. This comprehensive treatment aims to showcase the feasibility of the proposed solution while capitalizing on the valuable capabilities provided by regenerative satellites.

TABLE 1.2: Review of Related Works

Features	[15]	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	This research
NB-IoT in satellite communications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓
Antenna Selection	✓	✓	✓										✓
Link Budget Evaluation	✓	✓	✓	✓	✓	✓	✓						✓
Constellation Design				✓				✓					✓
Visibility Time													✓
BLER curves Analysis	✓						✓						✓
Doppler shift Evaluation		✓	✓		✓		✓	✓	✓	✓	✓	✓	✓
Random Access procedure		✓							✓	✓	✓	✓	✓
Protocol Stack Configuration													✓
System-level Architectural Design													✓
System-level Performance Analysis													✓

1.2.2 Recent 3GPP discussions

The 3rd Generation Partnership Project (3GPP) initiated the standardization of NTN within Release-15. This effort addressed various deployment scenarios, system parameters (including architecture, satellite altitude, and orbit), and tailored channel models, as documented in [27]. The available reports and specifications introduced the concept of narrow-band access, previously established with NB-IoT, to delineate a service-link provided by mobile satellites operating in the frequency band below 6 GHz.

Furthermore, they outlined two potential deployment scenarios: the *wide area IoT service* aimed at ensuring global service continuity for mobile sensors in areas partially covered by terrestrial networks, and the *local area IoT service* designed for a cluster of sensors that collect data and communicate with a central point situated on a mobile platform. In the latter scenario, the satellite plays a crucial role in ensuring connectivity between the mobile core network and the base stations serving IoT devices. In both cases, 3GPP highlighted the possibility of integrating the Inter Satellite Link (ISL) optionally and considering either a satellite with a bent-pipe payload or implementing the base station onboard the satellite.

More recently, with Release-17, 3GPP introduced new amendments spanning from the physical (Physical (PHY)) to network access stratum (Non-Access Stratum (NAS)) layers. These amendments were designed to enhance the performance of NTN systems in terms of latency, coverage, and power efficiency, as detailed in [28]. Particularly noteworthy is the discussion presented in [29], which explores the applicability of the guidelines established in [30] to NTN deployments with explicit support for IoT services based on NB-IoT.

As mentioned previously, 3GPP's work on NTN networks is ongoing and incomplete. Therefore, this research work leverages the preliminary technical reports provided by 3GPP to address the recent questions that have arisen and aims to offer concrete solutions to these open issues.

1.3 An Open-Source Tool for Evaluating System-Level Performance of NB-IoT Non-Terrestrial Networks

The significance of satellite technologies in expanding terrestrial networks is paramount for LPWAN services. Satellite-based IoT systems excel in providing effective solutions in remote areas where terrestrial technologies encounter limitations or are absent.

The distinctive capabilities of NTNs in this context ensure the continuity of services for Machine-to-Machine (M2M) and IoT devices, even in critical or emergency situations, with a particular focus on applications in maritime and aeronautical domains. This offers a multitude of advantages, primarily due to the substantially wider coverage and enhancements in scalability and availability as outlined in [31]. Furthermore, SatCom can furnish additional connections to relieve the burden on terrestrial networks, thereby significantly promoting the scalability of mobile networks. For these reasons, it proves exceptionally effective for Machine Type Communication (MTC) scenarios, which are foreseen for IMT-2020 and beyond [32], particularly when a large number of cost-effective devices require connectivity in vast areas that are not served by terrestrial networks

Several recent research studies have also explored NB-IoT as a potentially promising technology for 5G satellite MTC, as evidenced by the works cited in [16], [19], [21]–[23], [33]–[36].

The significance of integrating terrestrial and non-terrestrial networks in the realm of new communication technologies is emphasized in [33]. This paper delves into an evaluation of various options, including LoRA, SigFox, and 5G alternatives like NB-IoT, for achieving this integration. In the context of integrating satellite communication into 5G networks, [37] also investigates the use of NB-IoT technology. Specifically, the study demonstrates that 5G devices can establish low-bit-rate communication via satellites in conjunction with terrestrial infrastructure. Furthermore, the paper includes an examination of system sizing and channel modeling, which is facilitated by calculations in the link budget. These calculations analyze the communication performance requirements. The research presented in [34] centers on the expansion of NB-IoT and LTE-M technology to encompass NTN, thus enhancing the existing terrestrial deployment. The authors detail the necessary modifications to the terrestrial network architecture to accommodate satellite communication. They also identify physical-level adjustments and introduce signaling schemes to facilitate the incorporation of new features. The significance of expanding NB-IoT coverage and services to a scenario involving low Earth orbit (LEO) satellites is emphasized in [38]. The paper introduces novel coding and modulation schemes designed to enhance the performance of LEO satellite networks. Additionally, [16] investigates a LEO satellite constellation for delivering NB-IoT radio service. This technology holds considerable potential for enabling applications like global sensor reporting. In [22], the authors

introduce an NB-IoT architectural solution that utilizes LEO satellites, with a focus on discussing the significant impact of the substantial Doppler shift. Furthermore, papers [35] and [21] propose an NB-IoT satellite architecture using LEO satellites, examining the advantages of communication through this system. Specifically, these works put forth an uplink scheduling technique capable of mitigating the differential Doppler shift to a level compliant with the standard. In the study outlined in [23], an NB-IoT over satellite system is considered, exploring various deployment options based on satellite orbits, payloads, and cell types. Additionally, a customized configuration for NPRACH is suggested to alleviate the adverse effects of common satellite channel impairments on the NB-IoT Random Access Procedure. The work presented in [19] delves into the design of an NB-IoT system utilizing a constellation of LEO satellites. It proposes an algorithm to determine the optimal configuration for minimizing the impact of the satellite channel, with a focus on a link-level perspective. Lastly, [36] evaluates the Bit Error Rate (BER) to assess the number of collisions and their consequences in a satellite-based NB-IoT system. This assessment aims to accommodate the maximum number of devices within the proposed communication scenario.

Most of the previously mentioned papers utilize simulators designed for link-level analysis, with their primary focus directed toward a single communication link. Simultaneously, recent research indicates an increasing need for flexible tools in designing and evaluating new algorithms and protocols tailored for NB-IoT-based satellite environments. However, as of the research conducted and presented in [6], and to the best of the authors' knowledge, there are no system-level simulators accessible to the research community that explicitly catered to the considered scenario. It is worth noting that the existing scientific literature predominantly concentrates on physical and link-level analyses exclusively.

To bridge this gap, the open-source simulation framework known as 5G-air-simulator [39] emerges as a robust tool for conducting system-level analyses on various technical components standardized by the 3GPP. Notably, 5G-air-simulator already includes support for a range of NB-IoT features. However, the existing version of the simulator does not encompass NB-IoT technology within a satellite scenario. With these considerations in mind, this research work introduces an open-source implementation of an NB-IoT communication system based on satellite built upon the 5G-air-simulator framework. It's worth emphasizing that some preliminary research efforts have already leveraged the base version of 5G-air-simulator [40], [41], confirming that the simulation tool has gained traction in the field of SatCom as well.

1.3.1 The Proposed Simulation Module

Following the guidelines outlined by 3GPP [30], this study assumes the utilization of LEO satellites to ensure viable communication links with acceptable SNR levels. However, a single LEO satellite might not be capable of completing its entire orbit within the specified timeframe. Consequently, it becomes imperative to consider multiple satellites per orbit, forming a constellation. This approach significantly reduces the intervals during which ground-based devices experience a lack of satellite coverage, as elaborated in [18]. Within this context, Cubesats emerge as a cost-effective solution that simplifies system deployments for satellite constellations.

Each satellite within the LEO constellation functions as a Base Station. Consequently, NTN terminals are required to initiate the network attachment procedure each time they come under the coverage of a different satellite.

Every NTN terminal serves as a 3GPP NB-IoT User Equipment (UE) and possesses the capability to engage in direct satellite access via an adapted Uu interface. The NB-IoT technology is employed to establish the service link connecting the NTN terminal and the remote satellite.

It's important to emphasize that, in the configuration of NTN terminals in this scenario, only uplink channels are considered, with no modeling of downlink transmissions. Additionally, the system exclusively utilizes Single-Tone transmissions. This approach aims to enhance performance by leveraging the increased robustness offered by the service link and fully exploiting NB-IoT's bandwidth management capabilities to accommodate a multitude of users.

Figure 1.1 provides a comprehensive depiction of the implemented module, highlighting the interactions among various constituent components, which are elaborated upon below.

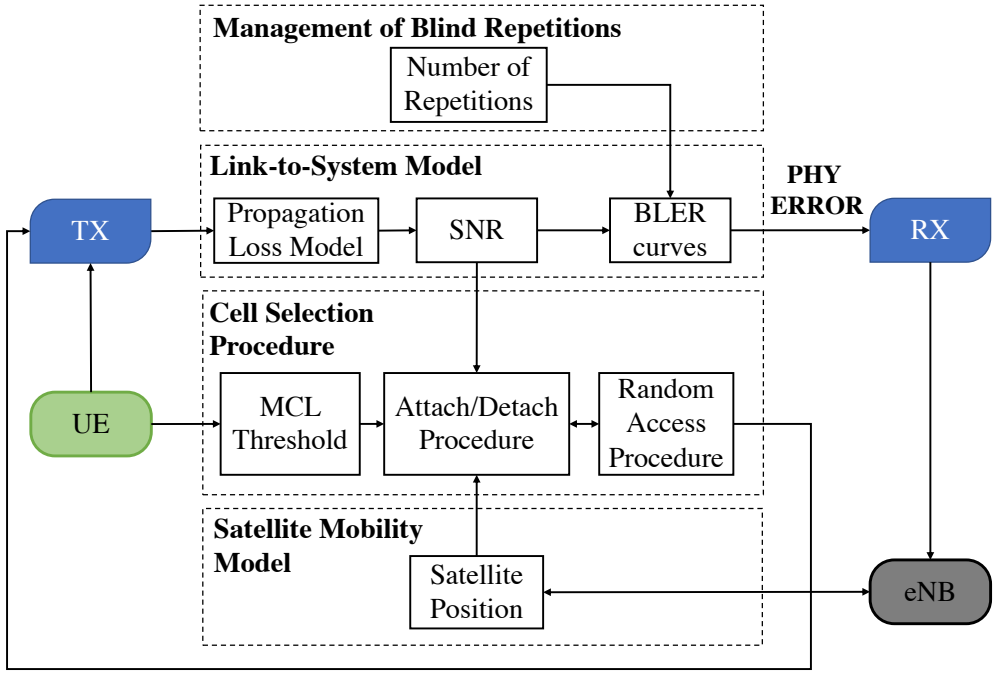


FIGURE 1.1: Overall vision of the interaction among the implemented simulator features.

The initial enhancement integrated into the 5G-air-simulator pertains to managing blind repetitions. This feature entails transmitting a bundle of the same Transport Block, replicated a designated number of times. This key-feature facilitates communication even under low SNR conditions. It plays a vital role in maximizing both visibility time and overall throughput.

The total number of blind repetitions for NPUSCH transmissions can be configured using the `FrameManager::SetNRep` method. Subsequently, this value is retrieved during the scheduling process. To be specific, the `RUsAllocation` methods

in both implemented scheduler classes (FIFO and Round Robin) now take this parameter into consideration when assigning RUs to users and finalizing the scheduling process. This ensures that the reception event occurs after the appropriate duration, which is dependent on the number of repetitions, the actual slot duration, and the number of RUs allocated to the UE.

The link-to-system model holds significant importance as it provides a streamlined yet accurate representation of transmission, propagation, and reception functions. This model combines link-level analysis with the system-level simulation tool. The simplified channel model encompasses SNR expressions for both downlink and uplink channels, along with Block Error Rate (BLER) curves for each transmission mode.

The original version of the 5G-air-simulator did not include a radio channel model for NB-IoT. Consequently, a new propagation loss model has been developed to assess the signal received by the satellite, considering the real-world conditions of the satellite scenario. More specifically, the SNR is analytically modeled, factoring in power gains and losses resulting from radio channel propagation. Taking into account the elevation angle of the service link (θ_{el}) and the carrier frequency (f_c), the SNR, which quantifies the link performance and is evaluated in decibels (dB), can be expressed as follows [42]:

$$\begin{aligned} &SNR(\theta_{el}, f_c) = P + G_{ANT}(\theta_{el}, f_c) - PL(\theta_{el}, f_c) - \\ &-L_{imp}(\theta_{el}, f_c) + DCF(\theta_{el}, f_c) - N, \end{aligned} \tag{1.1}$$

where P corresponds to the signal transmission power, and G_{ANT} is the combined antenna gains of the satellite and NTN terminal (measured in dBi). PL represents the free space path loss, which considers radio wave attenuation due to propagation, while L_{imp} accounts for additional losses caused by various impairments, including attenuation due to air, fog, atmospheric gas absorption, droplets, rainfall, polarization, and scintillation. Furthermore, DCF is the cumulative diagram correction factors of the transmitting and receiving antennas, expressed in dB. Finally, the noise power, denoted as N, can be determined by considering the system noise power at the receiving antenna. For a comprehensive calculation of the system noise power, please refer to [43].

To achieve this goal, a new header file has been created. This file encompasses the outcomes of the link-level analysis, including data like the received power from the satellite at the NTN terminal's side and the received power from the NTN terminal at the satellite's side across various elevation angles. Additionally, it includes the BLER curves for each transmission mode.

The new method, `BLERvsSINR_NBIoT_SAT::GetRxPowerfromElAngle_SAT`, assesses the received power at the satellite side for each elevation angle experienced by the NTN terminal. Consequently, during reception, the satellite obtains an SNR value associated with the uplink configuration utilized for transmission, reflecting the channel's quality. Essentially, this SNR value is utilized to estimate the BLER for the received data block using newly introduced SNR-BLER curves, which determine the probability of correct reception.

For this purpose, the BLER is estimated by taking into account the selected Modulation and Coding Scheme (MCS), the number of utilized RUs, the quantity

of NPUSCH blind repetitions, and the SNR observed by the satellite during reception. The BLER value is obtained using `BLERvsSINR_NBIoT_SAT::GetBLER_SAT`, which employs SNR-BLER curves stored in the header file, generated through the MATLAB LTE Toolbox.

An additional enhancement pertains to the new mobility model, which handles satellite movement by tracking their positions and defining their coordinates within the selected scenario.

For simulation purposes, and to maintain generality, the movement of satellites was limited to a single direction along a reference axis of the Cartesian plane, namely the x-axis. The positional value chosen corresponds to the center of the beam that encompasses the ground area. Given the count of satellites in the orbit and the current time, this method furnishes an updated position value using the following equation:

$$x_{Sat}(t) = x_{0,Sat} + v_{sat}(t \mod \Delta T_{sat}), \tag{1.2}$$

where $x_{0,Sat}$ corresponds to the initial position of the satellite, v_{sat} represents the relative speed of the satellite spot beam on the Earth, t represents the time instant considered and the modulo operation is needed to exploit the periodicity of the position function. Lastly, ΔT_{sat} reflects the elapsed time between two distinct satellites. It is calculated as T_{orbit}, which corresponds to the time taken by a satellite to complete one orbit around Earth (approximately 94 minutes), divided by $N_{sat\_per\_orbit}$, which stands for the number of satellites in a single orbit. ΔT_{sat} can be expressed as follows:

$$\Delta T_{sat} = \frac{T_{orbit}}{N_{sat\_per\_orbit}}. \tag{1.3}$$

Determining whether the entities involved in the communication, namely NTN terminals and satellites, are within reciprocal visibility for effective communication is a crucial aspect. To address this, a new extension has been introduced, and this computation takes place within the `UserEquipment::UpdateUserPosition` method.

Initially, NTN terminals with non-empty transmission buffers measure the power of the downlink signal received from the satellite. To aid in this determination, a critical parameter, the Maximum Coupling Loss (MCL), is defined. The MCL plays a vital role in determining the maximum coverage supported by the cellular system. When the MCL falls below a defined threshold, typically set at 164 dB, the NTN terminal initiates the attach procedure with the satellite. The NTN terminal continuously monitors the downlink power signal to maintain its connection with the satellite. This approach enables the simulator to model errors during the Random Access Procedure, which, if necessary, can be rescheduled. Conversely, even if an NTN terminal successfully completes the Random Access Procedure, it might still fail the attach procedure, rendering it unable to communicate.

1.3.2 Performance Evaluation

To assess the practical efficacy of the developed tool, the system-level study conducted underscores the significant impact of network and satellite configurations on system performance.

For simulation purposes, the fixed area on the Earth equivalent in size to the satellite spot beam, was selected as the fixed region containing the NTN terminal. At the

application layer, the chosen traffic model is periodic uplink reporting, as outlined in [44]. Monitoring represents one of the most prevalent use cases for MTC in NTN, as indicated in [30].

Regarding the Random Access process, the number of possible NPRACH preambles utilized is the maximum allowed by the standard, which is 48. A NPRACH periodicity of 240 ms has been selected, while the Backoff Parameter is configured at 2048 ms. These settings aim to mitigate the likelihood of collisions due to preamble retransmissions. Importantly, these values are also compatible with the extended Round Trip Times (RTTs) characteristic of NTN systems, as discussed in [23].

In this study, only one coverage class has been taken into account, and an MCL threshold value of 164 dB has been selected. The simulation duration has been chosen to ensure at least 8 cycles of satellite visibility over the communication area. A 20 MHz bandwidth within the 1980 MHz to 2000 MHz frequency range, along with a single NB-IoT carrier, has been considered. Various KPIs have been measured by processing the output trace files.

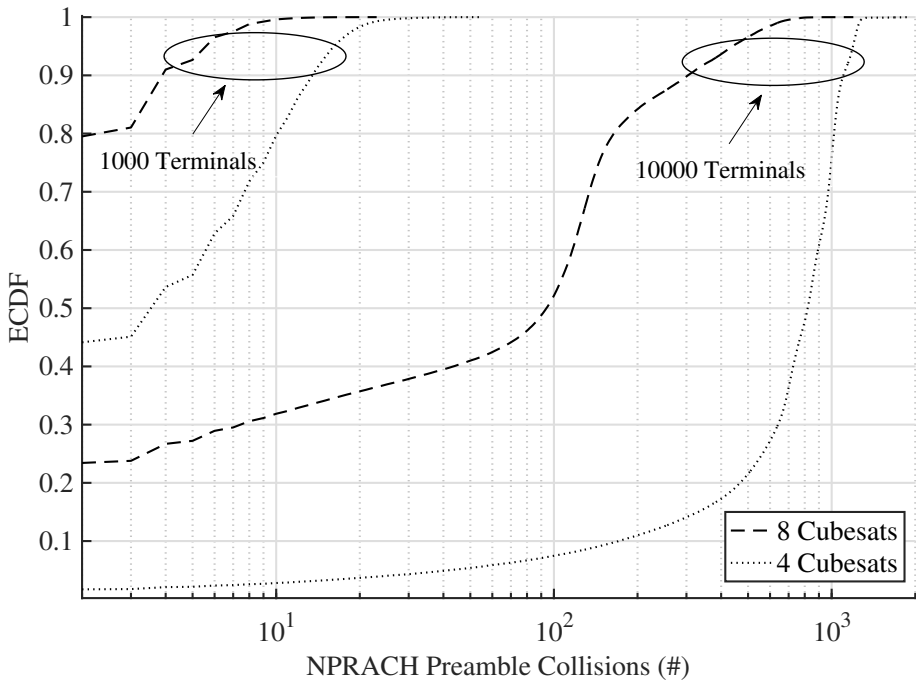


FIGURE 1.2: ECDF of the NPRACH Preamble collisions.

Figure 1.2 presents the ECDF for the number of collisions in the NPRACH preambles. To begin with, the number of Cubesats in the Satellite Platform has a significant impact on NPRACH performance. A lower count of Cubesats results in extended periods during which ground terminals lack satellite coverage. When these terminals regain visibility, a substantial surge in NPRACH preamble transmissions occurs, resulting in numerous collisions. Additionally, an increased number of NTN terminals naturally leads to a higher overall number of preamble collisions, which aligns with expectations. For example, when using 4 Cubesats and 10,000 NTN terminals, the likelihood of experiencing fewer than 100 collisions is less than 10%. This underscores that NPRACH poses a bottleneck in densely populated network deployments.

The Figure 1.3 provides insights into End-to-End packet delays. These delays are calculated, taking into consideration the impact of cell selection, the Random Access

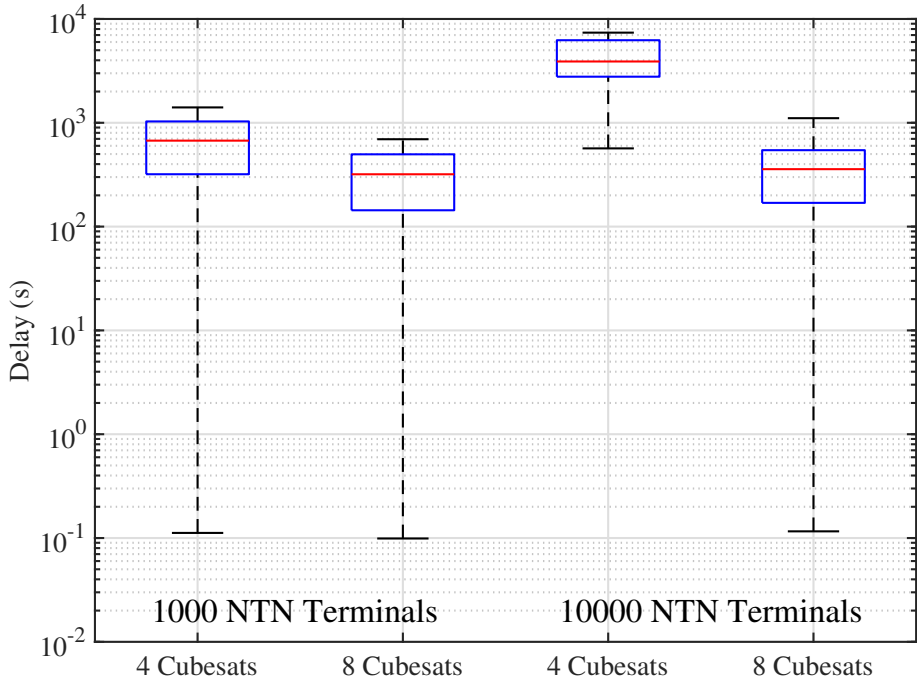


FIGURE 1.3: Box plots of the end-to-end packet delays. Each box plots identifies the median delay (i.e., the red line), the 25^{th} and the 75^{th} percentile (i.e., the bottom line and the top line of the blue rectangle), as well as the minimum and the maximum measured delay value (i.e., the edges of the vertical black line).

Procedure, scheduling decisions, and the actual physical transmission. As mentioned earlier regarding NPRACH considerations, one prominent observation is the substantial effect of the satellite constellation's size on End-to-End packet delays. In particular, a larger number of Cubesats extends the duration for which NTN terminals enjoy satellite coverage, consequently reducing End-to-End delays. Furthermore, it's worth noting that the time required to complete the Random Access Procedure increases as the number of NTN terminals rises. This escalation is due to the heightened number of users engaging in the Random Access Procedure, which leads to more collisions. Consequently, packet delays also grow with the number of NTN terminals.

In conclusion, the analysis covers the packet delivery ratio, which is the proportion of packets correctly received to those that were transmitted in all the simulation sets. More specifically, the Table 1.3 displays the average delivery ratio that was achieved.

TABLE 1.3: Packet Delivery Ratio

	1000 NTN Terminals	**10000 NTN Terminals**
4 Cubesats	92.66%	1.04%
8 Cubesats	99.41%	79.20%

Clearly, the 8 Cubesats constellations exhibit the highest packet delivery ratios. However, performance significantly degrades when a large number of NTN terminals is deployed. For instance, with 4 Cubesats and 10,000 ground terminals, the packet delivery ratio drops to approximately 1%. This steep decline is a result of the extensive number of NPRACH preamble collisions.

1.4 Looking at NB-IoT over LEO Satellite Systems: Design and Evaluation of a Service-Oriented Solution

Recently, the scientific literature and the 3GPP standardization body considered as viable the integration of NB-IoT in satellite-based architectures. Without any doubt, the design of the space segment is not easy. A number of state of the art (reported in section 1.2) contributions already tackled the related operational technical challenges, while focusing on feasibility studies at both physical and link levels [15]–[24], satellite constellation [18], [22], and Random Access procedure [16], [23], [24]. However, aside from the important findings they report, detailed selection of physical (and standards-compliant) transmission settings, protocol stack configuration, and a significant system-level evaluation of the overall communication architecture are still unexplored topics. Also, the discussion started by the 3GPP in RAN2 technical meetings (see [30] and [29]) is still in its embryonic stage and no turnkey solutions have been standardized yet.

Recently, both the scientific literature and the 3GPP standardization body have recognized the feasibility of integrating NB-IoT into satellite-based architectures. However, it is important to note that the design of the space segment is a complex task. While several state-of-the-art contributions (as outlined in section 1.2) have addressed operational and technical challenges, focusing on feasibility studies at the physical and link levels [15]–[24], satellite constellation design [18], [22], and Random Access procedure optimization [16], [23], [24], there are still several unexplored aspects. Despite the valuable insights provided by these studies, there remains a need for a detailed selection of physical transmission settings, standards-compliant protocol stack configuration, and a comprehensive system-level evaluation of the entire communication architecture. Additionally, the ongoing discussions within the 3GPP, as documented in RAN2 technical meetings (refer to [30] and [29]), are still at a relatively early stage, and standardized turnkey solutions have not yet been established.

To address this gap, the work presented in this Section and published in [7] focuses on designing a fully functional NB-IoT over satellite service that adheres to 3GPP specifications. Its goal is to tackle the most critical issues associated with employing NB-IoT over NTN in a real application scenario. In contrast to existing scientific literature, this work follows a service-oriented methodology that:

- illustrates application requirements and technological constraints that characterize a reference use case (taken from the smart agriculture domain);
- configures the entire protocol stack configuration to ensure the transmission of small data packets generated at the application layer, even when a feeder link is absent;
- identifies and implements low-level adaptations to address challenges affecting satellite communication, including those during the random access procedure, Doppler shift, and frequency carrier offset;
- carries out a detailed link-level investigation to determine the appropriate physical settings that ensure efficient ground-satellite communication;

- defines a satellite constellation offering a realistic service operating in Europe;
- assesses the performance of the proposed architecture through system-level simulations.

1.4.1 The reference use case and related requirements

The work presented in this section considers a reference use case in the context of smart agriculture, which is one of the most promising application areas for the effective utilization of NB-IoT technology over satellite communication.

It is widely acknowledged that farms necessitate uninterrupted and consistent connectivity and communication with monitoring systems used for various purposes, such as managing harvests, monitoring machine and facility power consumption, optimizing production processes, and controlling environmental conditions in both greenhouse and open field settings.[45]–[47]. In this context, satellites have assumed a pivotal role in addressing the challenges of future farming, particularly for large-scale customers who require hundreds or even thousands of NB-IoT devices for precision agriculture in rural areas. Numerous companies are embracing LEO satellite-based connections to provide seamless, real-time communication across the entire globe, as evidenced by recent developments cited in the reference [48].

Furthermore, there are ongoing initiatives aimed at assisting mobile operators in expediting the deployment of new NB-IoT devices and services connected via satellite-based systems in the context of smart agriculture scenarios, as detailed in the [49].

These motivations are also rooted in the project "3GPP Narrow-Band Internet-of-Things (NB-IoT) User Sensor Integration into Satellite" funded and supported by the European Space Agency (ESA), where the smart agriculture scenario is considered one of the most compelling case studies.

For the sake of generality, this study assumes that clusters of IoT devices are distributed across the satellite's geographical coverage area. Each cluster is positioned within a rectangular crop field spanning approximately 30 hectares, which is around the maximum size of crop fields found in certain European countries, as referenced in [47]. This extensive field size facilitates the assessment of system performance over a broad area equipped with a substantial number of sensors. The sensor nodes are evenly placed throughout the entire field with a 10-meter spacing between them, allowing for a total of 3000 nodes to be deployed in each cluster.

Similar to the majority of smart agriculture setups, wireless sensor units deployed on-ground consist of four distinct components: application-specific sensors, a processing unit, a radio transceiver, and a battery for power, as described in the literature [45]. The energy consumption of each sensor is primarily attributed to the radio transceiver when the node is active, and this consumption is dependent on the time required for the node to successfully transmit its generated measurements. However, the node remains active only during Random Access procedures and Transport Block transmissions, each of which takes only a few tens of milliseconds.

Given that a sensor node is active for only a small fraction of the day, monitoring sensors employed in smart agriculture can effectively utilize embedded rechargeable batteries powered by solar cells [45], [50]–[54]. Consequently, energy consumption

is not a significant concern in the specified application scenario, and its impact on system performance can be disregarded in this study.

In the context of the examined use case, portable sensors are employed for the measurement of five distinct soil-related parameters, primarily for monitoring purposes. These parameters encompass soil moisture, rainwater flow, soil temperature, conductivity, and salinity, as detailed in the reference [45]. Each of the sensed measurements is collected with a precision of 2 bytes. Furthermore, to ensure proper identification and tracking, 2 bytes are allocated for the sensor ID, allowing for the addressing of up to 65.536 different sensors, which is more than sufficient for the specific scenario being depicted. To enhance the spatial precision and accuracy of the collected data, an additional 6 bytes are dedicated to storing latitude and longitude coordinates from a GPS module. These coordinates serve to pinpoint the exact location of the sensed data. Consequently, the total size of the message generated by each sensor, at the application layer, amounts to 18 bytes.

For an efficient field monitoring, there's no need for the sensed parameters to be generated at a high frequency. Consequently, it is assumed that each node collects all five measurements six times a day, resulting in one measurement of each type being collected every 4 hours by each sensor node. Moreover, this low data generation frequency is easily manageable by the network, as it allows each node to make the most of the visibility of multiple satellites passing over the field to transmit its data. To facilitate this process, the sensed data are gathered by the node and stored in a buffer until the node enters the satellite's visibility window. During this specific time interval, the node makes repeated attempts to transmit the buffered data to the base station via the satellite link until successful reception is achieved.

In terms of system requirements, the study reported in this section aims to address the following demanding aspects:

- **Compliance with NB-IoT Standards**: this work seeks to promote the use of 3GPP standard technology to the fullest extent, aiming to support device interoperability, extendability of applications, and cost-efficiency. A specific emphasis is placed on devising a solution with streamlined hardware to ensure prolonged battery life.

- **Ensuring Service Area and Timing Alignment with Application Requirements**: the primary objective is to guarantee satellite coverage within the service area at intervals of a few hours. This enables the sensors to transmit data within this timeframe, aligning with the specific characteristics of the application.

- **Necessity for Adequate Satellite Coverage Configuration**: the satellite system is carefully structured to encompass the entire European area of interest, spanning approximately 6700 kilometers across 60 degrees of longitude, ranging from 20 degrees west to 40 degrees east.

- **Achieving Data Transfer During Visibility Windows**: the visibility time signifies the duration within which the NTN terminal can establish a radio bearer and execute data transmission towards the satellite. To ensure efficient communication, a data transmission round must be completed within a time frame

shorter than the visibility window. This duration is inherently influenced by satellite orbit attributes and the realized link budget.

- **Minimizing the Impact of Satellite Access Latency on Sensor Data Transmission Window**: the initial delay incurred during Random Access procedures, primarily due to satellite Round Trip Delay (RTD), constitutes the first delay factor. It is imperative that this setup delay is reduced to a level at least an order of magnitude less than the total visibility time to ensure it does not significantly affect the effective data transmission period.

- **Ensuring Reliability in Satellite Communication**: the satellite link constitutes a wireless channel subject to substantial influence from various propagation impediments. Notably, the ground-space link experiences propagation losses attributed to diverse factors, encompassing atmospheric absorption, rain-induced attenuation, tropospheric and ionospheric scintillation, depolarization effects, as well as fog and atmospheric gas attenuation. Addressing all these critical elements is essential to pinpoint appropriate physical layer parameters and system configurations that assure dependable communication.

- **Compensation for Doppler Effect**: due to the satellite's motion, a frequency shift occurs in the signal. Addressing this Doppler shift necessitates adjustments at the physical layer.

- **Requirement of Resilient Communication Infrastructure in Feeder-Link Unavailability**: the continuity of the connection between the satellite and the remaining functional components of the NB-IoT network cannot be assured over extended periods. The establishment of the feeder-link occurs when a gateway is positioned within the satellite's spot-beam, and this synchronization may not align with the availability of the service-link. Consequently, the entire architecture must be devised to enable NTN terminals to communicate with satellites, even in scenarios where the feeder-link is temporarily unavailable.

- **Satellite Cost Optimization**: the separation of satellite service and feeder-link raises the challenge of ensuring end-to-end service reliability. Potential solutions encompass the establishment of a satellite constellation and the implementation of on-board processing.

1.4.2 Protocol architecture and low-level adaptations

Consistent with the 3GPP standardization efforts pertaining to NTN networks as outlined in [27], the architecture under examination in this study adheres to the *Local Area IoT Service* scenario.

Regarding the fundamental satellite infrastructure, the baseline architecture incorporates NTN terminals, satellites, and NTN-Gateways. Data exchange between NTN terminals and satellites transpires via the *service-link*. Specifically, each NTN terminal is capable of establishing a connection with a single satellite from the constellation during its visibility window. When a new satellite within the same orbital path traverses the region where the NTN terminal is situated, the device restarts its configuration procedures in a stateless manner. Conversely, communication between

satellites and NTN-Gateways occurs via the *feeder-link*. It's worth noting that the NTN-Gateway might be positioned in a distinct geographic area, leading to a time-shifted connection over a feeder-link with the serving satellite.

The design of the network architecture is motivated by the need to separate the service-link and feeder-link. Consequently, since the availability of the feeder-link is not always guaranteed, data transmissions via the service-link can be executed asynchronously compared to the data offloading to the NTN-Gateway. In order to accomplish this, the proposed solution involves the installation of the complete Evolved Packet System (EPS) on-board the satellite. The entire service can be effectively implemented using a satellite constellation without the utilization of ISL. Notably, configurations that leverage ISL and multiple gateways are not taken into consideration, and this approach results in a substantial reduction in both complexity and costs. This pivotal technical decision had initially been contemplated in the Cellular IoT (CIoT) architecture as documented in [55]. However, this perspective has not been explored from a system-level standpoint, as highlighted in section 1.4. It presents an appealing solution, particularly for international entities such as ESA engaged in satellite system endeavors.

Figure 1.4 depicts the proposed network architecture and the resulting protocol stack.

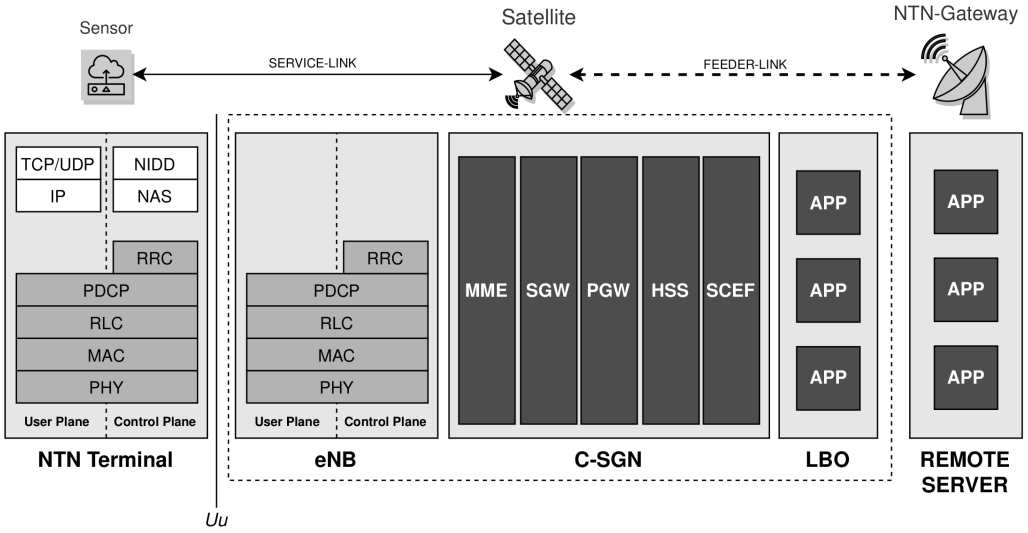


FIGURE 1.4: The proposed network architecture and the protocol stack of the NTN terminal and satellite.

Within the satellite system, various logical nodes are hosted, including the evolved Node-B (eNB), CIoT Serving Gateway (S-GW) node, and Local Break-Out (LBO). The eNB, serving as the base station, is responsible for implementing the Uu interface, which provides radio connectivity with NTN terminals. The CIoT S-GW node encompasses the functionalities of the remaining components of the Evolved Packet Core (EPC) protocol stack. Consequently, it includes the following:

- the Mobility Management Entity (MME) manages Control Plane communications through NAS signaling facilitated by the Radio Resource Control (RRC) protocol;

- the S-GW and the Packet Gateway (P-GW) oversee User Plane communications, leveraging IP at a higher protocol layer;
- the Home Subscriber Server (HSS) is responsible for NTN terminal network registration and authentication.

In order to facilitate asynchronous data delivery, messages transmitted by NTN terminals via the service-link are temporarily stored on the satellite, making use of a local application managed through the LBO. The accumulated data can subsequently be transferred to a remote NTN-Gateway on the ground once it comes within the satellite's visibility. To accommodate various options simultaneously, the feeder-link can be established using non-3GPP technologies, offering data rates that are comparable to or even higher than those observed in the uplink direction.

With this high-level protocol architecture as a starting point, certain specific adaptations need to be incorporated into various layers of the communication stack to effectively address the challenges posed by the satellite communication link.

Adaptations for the Uu interface

In the context of the Uu interface, there is a need for adjustments in both the Control Plane and User Plane, as specified in [56]. A novel approach for uplink transmission, known as Non-IP Data Delivery (NIDD), has been introduced. It enables the encapsulation of user data within NAS messages of the Control Plane, involving both the MME and Service Capabilities Exposure Function (SCEF) components, as an alternative to IP-based data transport. It's worth noting that NIDD introduces an additional 6-byte overhead, primarily due to the header size of the NAS message. Furthermore, new RRC procedures, available since Release-15, enable the suspension and rapid resumption of the RRC connection. This feature is particularly advantageous in light of the limited visibility intervals.

As outlined in subsection 1.4.1, each message generated by a sensor node has a total size of 18 bytes. At the application layer, the chosen protocol is Constrained Application Protocol (CoAP), as specified in [57]. This protocol introduces an associated 4 bytes of overhead. CoAP operates on a web-based framework and relies on the request-response or client-server model, making it well-suited for the scenario at hand. In this context, sensors engage in on-demand and infrequent data exchange. At the transport layer, the choice is NIDD, serving as an alternative to the conventional UDP/IP solution. CoAP is compatible with NIDD, resulting in a reduction of overhead from 28 bytes in the UDP/IP solution to 6 bytes, as detailed earlier.

In the lower network layers, namely the Packet Data Convergence Protocol (PDCP), Radio Link Control (RLC), and Medium Access Control (MAC) protocols, appropriate configurations have been put in place to adhere to the constraints and requirements of NTN NB-IoT. Specifically, the need for data retransmissions has been restricted to the MAC layer only, which involves enabling the Hybrid Automatic Repeat Request (HARQ) process, while disabling retransmission and feedback-based procedures at the PDCP and RLC layers. Furthermore, segmentation of Protocol Data Units (PDUs) at the RLC layer has been deactivated. As a result, it is now possible to utilize PDUs with significantly simplified headers across all three layers, as stipulated in [58]–[60]. This results in the addition of a minimal 4-byte overhead.

To sum up, the proposed configuration encompasses 18 bytes for data, 4 bytes for the application, 6 bytes for NIDD, and a combined total of 4 bytes for all the lower layers, which includes PDCP, RLC, and MAC. Consequently, the smallest transport block that aligns with one of the available options for Transport Block Size (TBS) and facilitates the utilization of the Early Data Transmission (EDT) protocol in the proposed solution is equal to 41 bytes or 328 bits, in accordance with the specifications in [61].

Adaptations for the Random Access procedure

The Random Access procedure serves as a means for NTN terminals to secure the uplink resources required for data transmission. Initially, it is imperative for the network to identify the corresponding Random Access Occasion (RAO) to which a preamble belongs. This step is essential for determining the appropriate Timing Advance (TA) required to synchronize the uplink transmission.

In cases where the periodicity of the RAO is not sufficiently wide, the preamble receiving windows of two successive RAOs may overlap, leading to ambiguity regarding the RAO to which a preamble pertains. An effective solution to circumvent this problem, as explored in [30], involves extending the interval between two RAOs to a duration exceeding twice the maximum delay difference encountered by two NTN terminals within the same cell.

Enhancements to the TA are imperative due to the fact that the TA command can surpass the maximum allowable value as defined by the standard, which covers distances of up to 100 km between the NTN terminal and the satellite, as outlined in [24]. To address this concern, the most promising solutions involve the implementation of autonomous TA calculations by the NTN terminal. This approach leverages Global Navigation Satellite System (GNSS) data to determine the terminal's position and uses satellite ephemeris information provided by the network to estimate propagation delays through geometric calculations, as discussed in [62].

Another viable alternative to GNSS involves broadcasting a common TA offset tied to a reference point situated at the center of the satellite's beam (Nadir). The differential component of the TA, computed for the NTN terminal concerning the reference point, can be adjusted by the TA command without necessitating any modifications to the standard. This adjustment ensures that the differential TA falls within the 100 km range, even in the most challenging scenario of an NTN terminal located at the cell edge.

While many of these solutions may warrant further exploration through experimental testbeds, these adaptations have been chosen as the most suitable options for the scenario under consideration.

Adaptations for Doppler Shift and Carrier Frequency Offset

In the realm of satellite communication, two undesirable frequency domain effects manifest themselves: the Doppler shift and the Carrier Frequency Offset (CFO). The Doppler shift results from the relative motion between the NTN terminal and the satellite. In the specific scenario considered, where NTN terminals are stationary on the ground, this shift is solely due to the satellite's movement. On the other hand, the CFO pertains to the frequency shift arising from inaccuracies in the local oscillators

of the receiver. Both of these effects induce a frequency shift that leads to interference with adjacent subcarriers in the uplink, thereby presenting a significant challenge for signal reception.

According to [26], the LTE physical layer can withstand a maximum Doppler shift of up to 950 Hz. However, based on the model presented in [25] and the guidelines provided in [30], the scenario examined in this section is expected to encounter a Doppler shift ranging from -30 kHz to 30 kHz. Since these values significantly exceed the permissible limit of 950 Hz, it becomes imperative to integrate additional methodologies into the adapted Uu interface to compensate for the Doppler effect. Similarly, for the CFO, compensation techniques are necessary. Per 3GPP specifications, where an NTN terminal's crystal accuracy can be as high as 10 parts per million, a CFO of approximately 20 kHz can be derived at the chosen carrier frequency in the reference scenario [30].

The Uu interface developed in this study can incorporate two viable solutions for Doppler shift compensation.

The first approach adheres to standard recommendations and employs GNSS-capable devices. These devices utilize knowledge of the satellite ephemeris to autonomously estimate the position of the satellite and the relative distance from it, as required by NTN terminals.

The second solution pertains to devices that are not equipped with GNSS capabilities. It originates from the research conducted in [22], which seeks to simultaneously compensate for the Doppler shift and the CFO. Unlike the Doppler shift, the CFO maintains a constant value throughout the entire satellite visibility period. In the absence of positioning information, an estimator is employed based on prior knowledge of the expected Doppler Shift, which consistently falls within the maximum deviation range calculated for the chosen scenario. To perform accurate initial Doppler shift estimation and compensation, the filter bandwidth is expanded to encompass a frequency range that includes both the maximum Doppler shift and the CFO. This expansion ensures that the filter can always accommodate the modulated signal affected by the overall frequency shift. Subsequently, the Doppler shift estimation is periodically updated through a first-order differential system. This system has the capability to track and compensate for Doppler variations over time, with a periodicity that allows for the inclusion of shift variations within the 950 Hz limit. As a result, an 80 ms periodicity proves sufficient to fulfill the Doppler compensation requirements throughout all satellite visibility periods.

1.4.3 Link-level analysis and satellite constellation

The development of an efficient communication architecture that harnesses NB-IoT technology over a satellite link is built upon a thorough examination of link-level characteristics reported in what follows.

Antenna Selection

Concerning the NTN terminal side, the antenna should be readily deployable and cost-effective. To address this requirement, the proposed solution utilizes a horizontally-oriented monopole antenna with linear polarization. This type of antenna is already

commercially available as a Commercial-Off-The-Shelf (COTS) product, as detailed in [42].

On the other hand, for the satellite side, achieving the right balance between the power radiated by the antenna and the role of the High Power Amplifier (HPA) is a crucial consideration. Small satellites have limitations when it comes to accommodating a large HPA. However, to compensate for the limited power resources provided by a small HPA, it's possible to enhance radiated power by optimizing antenna gain. It's important to strike a balance in this regard as excessive antenna gain results in increased volume, mass, and deployment complexities. With these considerations in mind, this work opts for a circular patch antenna tile for the satellite. The deployment of this antenna should be managed while accounting for potential dynamic steady states in the satellite's orbit.

Furthermore, a monopole antenna with linear polarization generates a signal that undergoes polarization rotation as it propagates through the Earth's ionosphere due to the influence of the Earth's magnetic field. As a result, the satellite may receive a signal with a polarization orientation different from what its receiving antenna expects, which typically degrades communication performance. However, utilizing a satellite-side antenna with circular polarization can help mitigate this effect to some extent. In this context, even in the worst case scenario of a 45° misalignment between circular and linear polarization, the penalty incurred is only 3 dB.

It's worth noting that the tile circular patch antenna exhibits excellent performance with regard to the coverage of the satellite beam. The Half Power Beam Width (HPBW) factor represents the angle in which the relative power is higher than the 50% of the peak power of the main lobe reported in the effective radiated field of the antenna. The chosen antenna's main lobe ensures an HPBW of approximately $\pm 56°$, making it a highly suitable choice for the scenario under examination.

In both cases, the chosen antennas provide a significant gain – 5.19 dB for the NTN terminal's antenna and 6.97 dB for the antenna patch on the satellite. It's important to mention that these values were computed using the analytical formulation outlined in [42]. Additionally, a linear approximation was utilized (only for the satellite) within the frequency range from 1900 MHz to 2200 MHz.

In summary, Figure 1.5 provides further insights into the selected antenna types, along with radiation diagrams for reference.

Link Budget Analysis

Considering the power gain provided by the chosen antennas, the transmission power of NB-IoT technology, and accounting for propagation losses, the link budget analysis serves to determine the satellite antenna altitude and the range of elevation angles within which the radio link can be established. The link budget assessment is rooted in the analysis detailed in [43] for satellite communications systems. The satellite system's design is underpinned by theoretical formulas that accurately replicate real-world phenomena affecting signal propagation in both the uplink and downlink directions.

As outlined in the analytical description of the satellite link in [43], the link budget is expressed in dB as a function of the carrier frequency f_c and elevation angle θ_{el} and is reported in the following equation in the same manner of the eq.1.1:

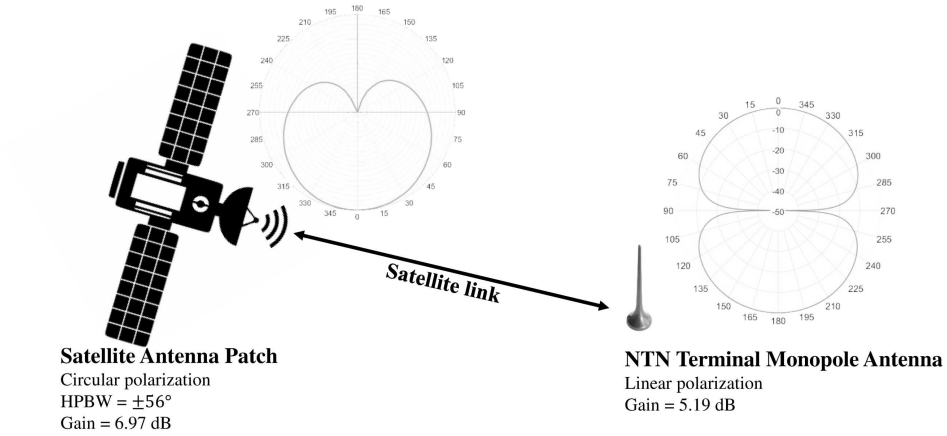


FIGURE 1.5: Antennas types and related radiation diagrams.

$$LB(\theta_{el}, f_c) = P + G_{ANT}(f_c) - FSPL(\theta_{el}, f_c) - L_{imp}(\theta_{el}, f_c) + DCF(\theta_{el}, f_c), \tag{1.4}$$

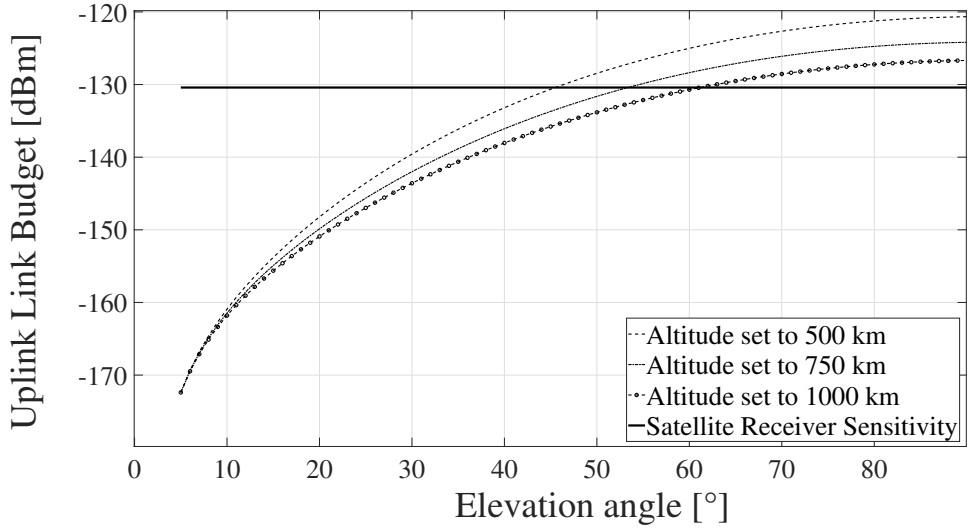
In the provided equation (1.4), the variables are defined as follows: P represents the signal power, G_{ANT} denotes the combined gains of the base station and NTN terminal antennas (as detailed in Section 1.4.3), $FSPL$ accounts for the free space path loss, L_{imp} encompasses additional losses stemming from propagation effects, and DCF sums up the diagram correction factors for transmitting and receiving antennas in dB. Notably, this equation does not incorporate multi-path fading models, as the paths obstructed by Earth's obstacles are negligible in comparison to those reaching the satellite.

The impairments captured by L_{imp} are calculated by taking into consideration various factors, including air attenuation that considers dry air absorption as per [63], rainfall attenuation estimating droplet absorption as described in [64], [65], scintillation attenuation which factors in fluctuations in the amplitude and phase of radio waves [42], polarization attenuation that addresses disparities in polarization between the receiving antenna and the incoming radio wave [43], and fog and atmospheric gas absorption as per [66], [67]. It's important to note that the models used to assess attenuation due to air, rainfall, scintillation, and atmospheric gas absorption are predictive models based on analytical estimates outlined in the most recent updates of the ITU-R recommendations referenced above.

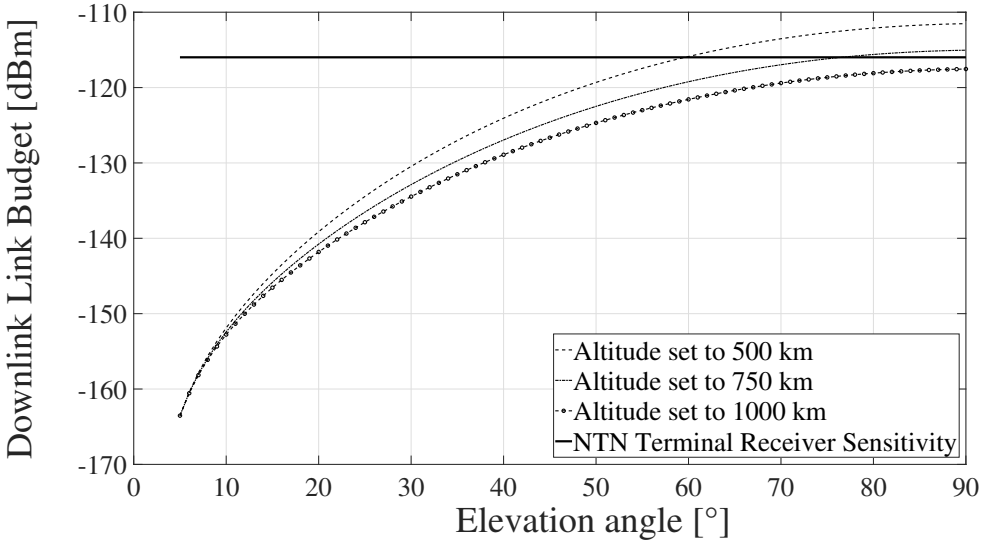
Figure 1.6 displays the link budget assessment based on the elevation angle and satellite altitude. For illustrative purposes, we assume an NTN terminal deployed within the European field of view.

Consistent with NB-IoT specifications [27], the carrier frequency and transmission power are configured as follows: f_c=1995 MHz and P=23 dBm for the uplink, and f_c=2185 MHz and P=33 dBm for the downlink.

The link budget is notably influenced by the user-satellite elevation angle. It exhibits an increment as the elevation angle approaches 90°, indicating improved link quality. Conversely, the link quality diminishes with increased satellite altitude. In



(A) Uplink



(B) Downlink

FIGURE 1.6: Link Budget in the function of Elevation Angle for different orbital altitudes.

both the uplink and downlink, the receiver antenna captures both the attenuated signal and noise power. Therefore, it's crucial to determine under what conditions the received signal power surpasses the receiver sensitivity.

As per [43], the receiver sensitivity represents the noise power in the link, expressed through the Nyquist formula presented in eq. 1.5:

$$RS|_{dBm} = 30 + 10log_{10}(k_B T_{sys} BW), \tag{1.5}$$

where k_B represents the Boltzmann constant, T_{sys} denotes the equivalent system noise temperature that encompasses both antenna and receiver noise, and BW indicates the NB-IoT subcarrier bandwidth. As per [68], T_{sys} is set at 150 °K for the uplink and T_{sys}=290 °K for the downlink. Conversely, BW is contingent on the selected transmission configuration.

Figure 1.6 also presents the computed receiver sensitivity. The results suggest opting for the lowest satellite altitude, namely 500 km, to achieve a favorable link budget for lower elevation angles. An altitude of 500 km strikes an optimal balance between the elevation angle (which governs coverage area) and connectivity (measured in terms of the power level received by the receiver).

Given the link budget and the receiver sensitivity, it is possible to calculate the expected value of SNR:

$$SNR = LB(\theta_{el}, f_c) - RS. \tag{1.6}$$

Figure 1.7 illustrates the SNR curves as a function of the elevation angle, for different transmission modes in the uplink.

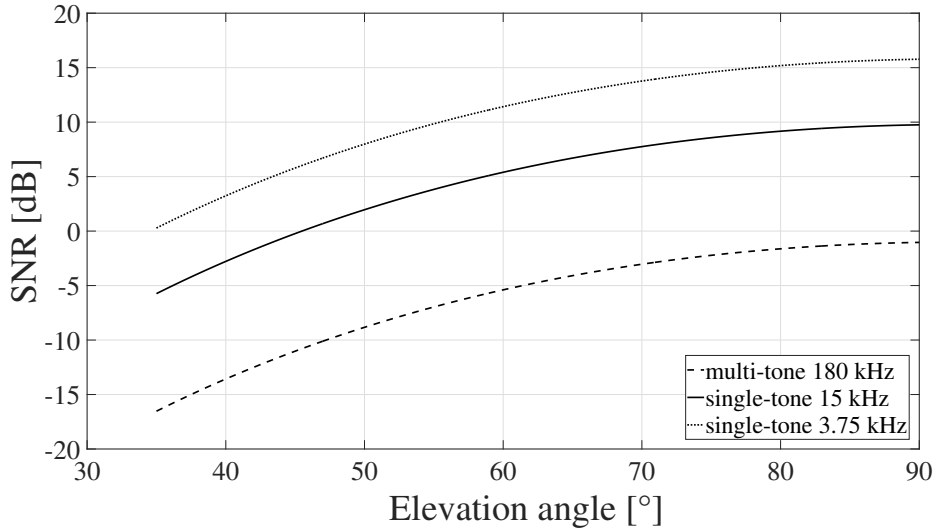


FIGURE 1.7: SNR in different transmission mode configurations for the uplink.

NB-IoT technology enables the use of individual subcarriers to concentrate power on a narrower band, resulting in increased coverage range and power gain. This

notable improvement in the single-tone configuration, offering nearly 10.8 dB gain compared to multi-tone, enhances the attractiveness of this solution for the proposed architecture.

As depicted in Figure 1.7, the single-tone configuration delivers commendable SNR values for lower elevation angles when compared to the multi-tone setup. As detailed in section 1.1, while adopting a single-tone configuration with a 3.75 kHz subcarrier could further boost SNR, it would require longer subframe durations.

Therefore, the intermediate configuration, featuring a single-tone with a subcarrier bandwidth of 15 kHz, is chosen as the optimal compromise between SNR performance and time resource utilization. This configuration ensures a higher SNR at the same elevation angle when compared to the multi-tone setup.

In line with these considerations, a subcarrier bandwidth of 15 kHz is selected for the uplink, while a bandwidth of 180 kHz is chosen for the downlink. The receiver sensitivity varies for uplink and downlink configurations due to the different subcarrier bandwidths. For the uplink, with a subcarrier bandwidth of 15 kHz, the receiver sensitivity is lower, measuring -130 dBm, whereas the downlink configuration, with a subcarrier bandwidth of 180 kHz, features a receiver sensitivity of -117 dBm.

It is worth noting that the points of intersection between the link budget curves and the receiver sensitivity, as depicted in Figure 1.6, indicate the elevation angle beyond which the SNR exceeds zero. However, the radio link could still be established at negative SNR values under specific configurations, resulting in lower elevation angles. The practical feasibility of the connection is determined by evaluating the communication success probability. This probability is defined by analyzing the BLER curves using the same methodology described in section 1.3 and is further evaluated in section 1.4.4.

Satellite Constellation

Using a single satellite for the selected 500 km altitude leads to very short visibility periods. In contrast, with a constellation of multiple satellites, NTN terminals could have more opportunities to transmit their data, reducing the time without satellite coverage. This approach would also decrease the data storage and forwarding requirements for each NTN terminal, simplify the satellite hardware, and reduce energy consumption, which is a critical consideration for IoT technology.

The satellite platform under consideration in this research must adhere to cost-effective solutions to meet the cost optimization requirement. In this context, the study explores the use of small or nano-satellites, offering an efficient and budget-friendly solution with various simplifications in system design and deployment. With this in mind, the decision was made to utilize a 12U CubeSat in a 2x2x3 configuration, as detailed in [69]. This platform comprises multiple units that can be assembled in a highly scalable and adaptable manner to achieve the required performance.

A CubeSat in LEO at an altitude of 500 km (equivalent to an orbital radius of 6878.14 km) necessitates a orbital velocity of 7612.6 m/s to sustain its orbit.

Therefore, the orbital period is 1 hour and 34 minutes, and the number of satellites per orbit must be chosen thoughtfully to balance cost and service requirements. While having a lower number of satellites is cost-effective, it's crucial to also consider factors like the low variability of the frequency of sensed data transmission and the battery

life of NTN terminals. To strike a suitable balance between these constraints, the proposed architecture incorporates either 2 or 3 satellites per orbit. In the first case, an NTN terminal can establish contact with a satellite approximately every 47 minutes and 18 seconds, even though the orbital period for a single satellite at 500 km altitude is 1 hour and 34 minutes. In the latter case, an NTN terminal can communicate with a satellite roughly every 31 minutes and 32 seconds.

The well-known System Tool Kit, as referenced in [70], is employed to assess the diameter of the satellite spot-beam. More precisely, the analysis aimed at covering approximately 6700 km of longitude, which corresponds to the European region. The findings of this study indicate that around 8 circular orbits (with a 0° eccentricity) with sun-synchronous characteristics (97°/98° orbital inclination) are necessary to meet the continuous service requirement. Consequently, the entire satellite constellation would comprise 24 satellites.

Figure 1.8 provides a depiction of the geographical area covered and offers a snapshot of the beam coverage along with the satellite orbits. It's worth noting that there is an overlap between the areas covered by satellite beams from adjacent orbits. However, to prevent interference between satellite transmissions to NTN terminals, the approach proposed in this work assumes that satellites from different orbits are spatially shifted.

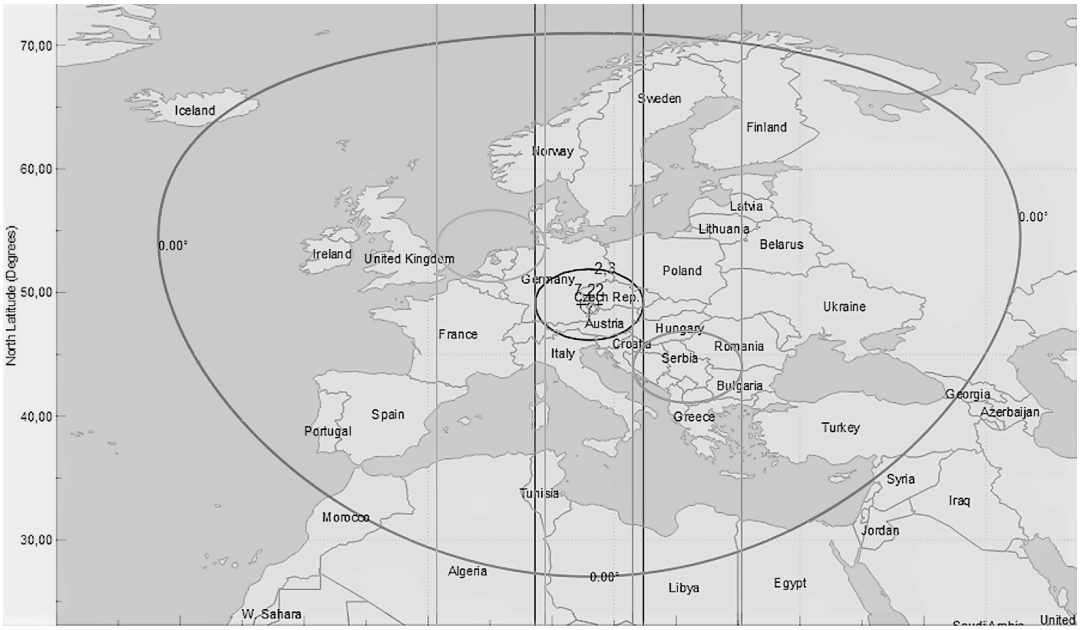


FIGURE 1.8: European field of view and satellite beam coverage.

1.4.4 System-level performance of NB-IoT over satellite

Merely having knowledge of the link budget is insufficient for assessing the viability of the satellite architecture. Consequently, this section proves the effectiveness of the proposed architecture by conducting system-level simulations. The analysis provided here specifically assesses how physical and system configurations impact two crucial factors:

- the capability of the entire communication architecture to distribute data via the service-link;
- the resultant communication latencies.

System-level tool and parameter settings

The system-level simulations are carried out using the 5G-air-simulator [39] [71]. This simulator is designed to support NB-IoT and encompasses various functionalities. Of particular note is the Random Access procedure model within the 5G-air-simulator, which has previously undergone analytical validation [72], ensuring the reliability of the results discussed in the subsequent sections. Additionally, the tool has been suitably extended to accommodate the implementation of the envisioned NTN scenario, as reported in section 1.3 and [6].

For the physical layer, as outlined in subsection 1.4.3, certain parameters have been defined, including the transmitted power and the configured bandwidth. Additionally, the chosen MCS is QPSK, selected for its superior spectral efficiency compared to BPSK. The TBS indicates the amount of data passed through the physical layer and subsequently mapped to the NPUSCH channel. It has been set to 328 bits, aligning with the protocol stack configuration detailed in section 1.4.2. With the established TBS, data packets can be transmitted using different Number of Resource Unitss (NRUs). Following the guidelines in [73], the available options for NRU configuration include 2, 3, 4, 5, or 6

Indeed, a trade-off exists regarding NRU configuration. On the one hand, increasing NRU values enhance data protection at the physical layer. On the other hand, higher NRU settings lead to longer physical transmission durations for a data packet. Considering the considerable distances within the satellite scenario and the associated latencies, a decision has been made to set the maximum number of HARQ retransmissions to 4.

For the Random Access procedure, the configuration includes 48 available preambles, an 80 ms periodicity for the RAO, and a 65536 ms backoff window.

To assess the impact of varying traffic loads, we examine different scenarios involving clusters of NTN terminals. As previously discussed in subsection 1.4.1, each cluster comprises 3000 NTN terminals distributed across a single 30-hectare crop field. Each NTN terminal is programmed to generate data every 4 hours. Additionally, every 4 hours, all the NTN terminals within each cluster transmit their data simultaneously during a 1-minute time slot. This setup allows us to analyze how the proposed approach performs under demanding conditions characterized by bursts of traffic.

The satellite allocates radio resources to NTN terminals that have successfully completed the access procedure, following a round-robin scheduling approach. Subsequently, extensive computer simulations spanning a 48-hour duration are performed. This extended timeframe covers numerous satellite visibility cycles and enables us to obtain consistent and stable average results.

Link-to-system model

A link-to-system model represents the initial step in conducting a thorough system-level analysis. It serves the purpose of characterizing the quality of communication achievable under specific parameter configurations, while ensuring an abstraction of transmission, propagation, and reception aspects. In this context, the 5G-air-simulator tool was enhanced to include the propagation model, link budget, SNR model, and BLER curves, as outlined in section 1.3. Additionally, BLER curves were integrated to simulate communication quality as a function of measured SNR.

To facilitate the generation of BLER curves, the MATLAB LTE Toolbox was employed. The BLER was calculated as the ratio of the total number of received blocks for which the Cyclic Redundancy Check (CRC) failed to the total number of transmitted blocks. For a detailed BLER assessment, a range of SNR values from -10 dB to 10 dB was selected, and the total number of transmitted blocks was set at 1000.

Figure 1.9 illustrates the BLER curves obtained in relation to NRU and SNR. The results clearly indicate that higher NRU values offer enhanced data protection at the physical layer. Concurrently, higher SNR values correspond to improved link conditions. Consequently, based on these observations, it can be deduced that BLER diminishes with increased values of both NRU and SNR.

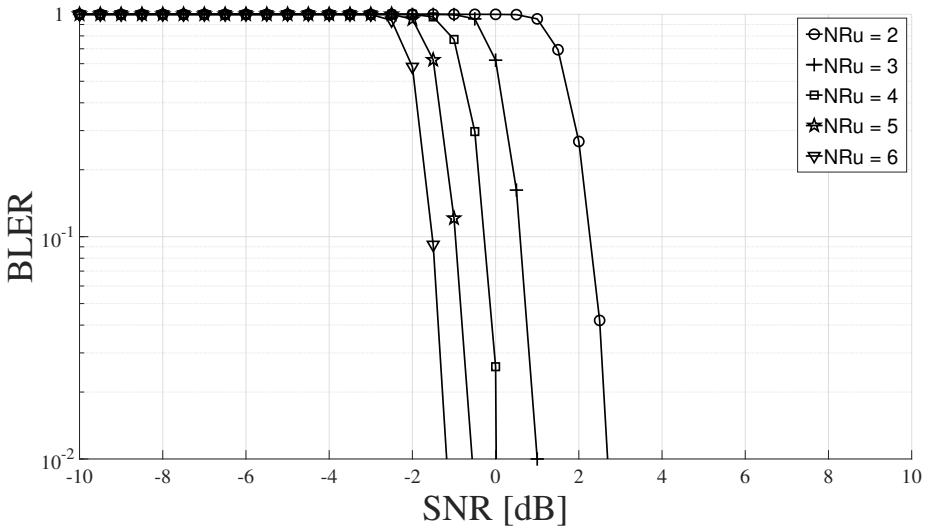


FIGURE 1.9: BLER curves

Satellite attach procedure and visibility time

Every NTN terminal initiates the attachment procedure when the receiver power of the satellite's reference signal reaches a coupling loss below the specified MCL threshold, which has been configured at 154 dB. Considering the given parameter settings and the mentioned MCL threshold, the average SNR value (measured in the downlink direction) is -4.9 dB.

Furthermore, as demonstrated in the study outlined in section 1.4.3, this particular SNR value is achieved at elevation angles of 46.3° for the downlink, marking the commencement of the visibility time.

Now, with the satellite positioned at an altitude of 500 km, a trigonometric analysis enables the calculation of the effective satellite footprint diameter. Taking into account the slant range, which represents the distance between the NTN terminal and the satellite and is determined by the elevation angle, the diameter of the effective footprint is estimated to be approximately 890 km. This estimation considers the satellite's relative speed with respect to the Earth, which is approximately 7059 m/s. Based on this effective footprint size and satellite speed, the visibility time can be calculated, resulting in an approximate duration of 125 seconds.

Communication latencies over the service-link

Communication latency denotes the duration it takes for a packet to be received successfully by one of the satellites in the constellation, in relation to the moment it was generated. Figures 1.10 and 1.11 illustrate the communication latency under varying physical configurations and network loads. These curves represent the impact of enabling or disabling the EDT transmission scheme, and in this scenario, each orbit accommodates 3 satellites.

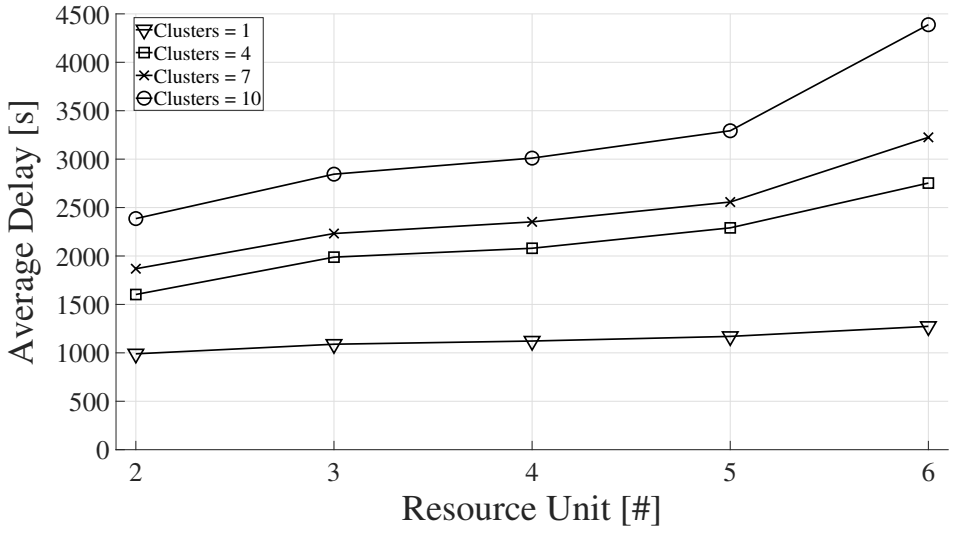


FIGURE 1.10: Average end-to-end delay with EDT disabled.

Primarily, communication latency is influenced by the probability of successfully completing a Random Access procedure. As anticipated, an increased number of clusters results in more NTN terminals attempting to access the network, subsequently raising the collision probability during the Random Access procedure. This, in turn, explains the rise in communication latency with the number of clusters supported by the configured satellite architecture.

Additionally, the NRU allocation to each NTN terminal significantly influences the average end-to-end delay. While distributing a Transport Block across multiple NRUs provides enhanced protection, it also prolongs the transmission time, leading to a notable impact on the end-to-end delay.

In contrast, the EDT scheme effectively reduces communication latency by up to 40% due to its capability to deliver the data packet alongside the Msg3 of the Random Access procedure.

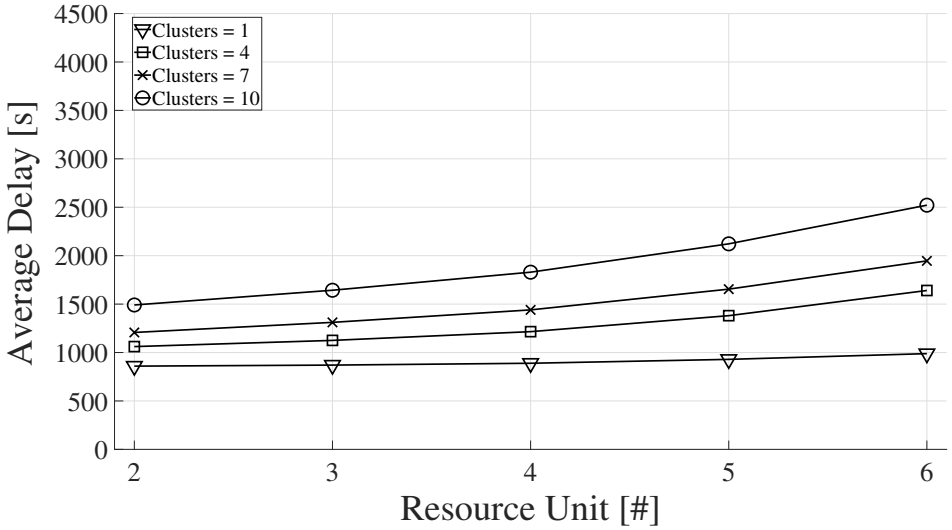


FIGURE 1.11: Average end-to-end delay with EDT enabled.

Ability of the system to drain buffered data through the service-link

The examination of the cumulative number of packets stored across all NTN terminals serves as a means to assess the capacity of the satellite architecture to effectively accommodate the provided service. A rapid increase in this value indicates that the network may struggle to fulfill all NTN terminal requests, resulting in message congestion and network overload. Conversely, a slower accumulation of packets in the buffer suggests that the network is capable of handling the traffic generated by the NTN terminals.

Figure 1.12 illustrates the practical capacity of the proposed approach to efficiently clear buffered data via the service-link, employing a constellation of 24 satellites (i.e., 3 satellites per orbit).

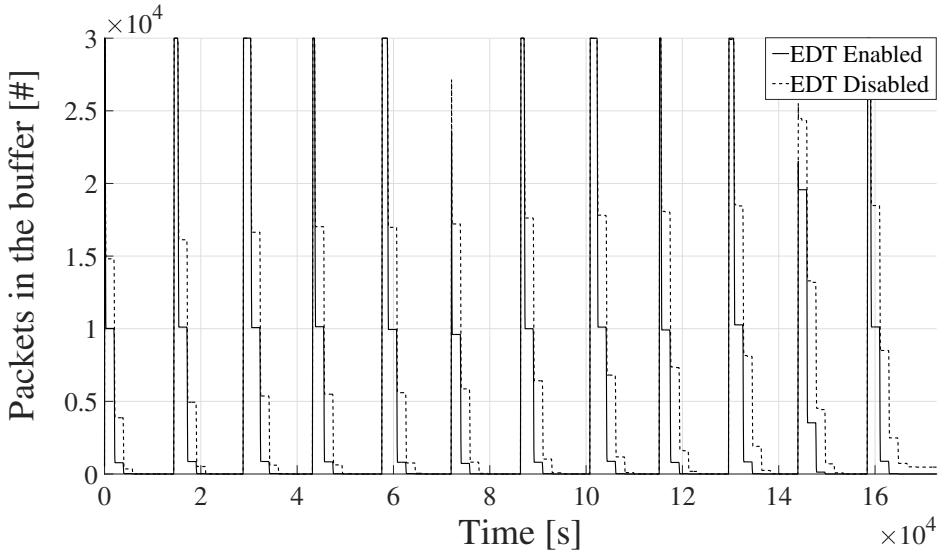


FIGURE 1.12: Number of packets in the buffer with 10 clusters.

For the sake of clarity, the results pertain exclusively to the most heavily loaded scenario, involving 10 clusters of NTN terminals (equivalent to 30,000 nodes) and an NRU setting of 2.

The depicted curves underscore that NTN terminals necessitate more than a single visibility time to transmit their data. The dissemination of the entire packet burst generated by NTN terminals is expedited when EDT is enabled.

Impact of the number of satellites per orbit

For added clarity, Table 1.4 presents the average communication latency observed when varying the number of satellites per orbit. Similar to the prior analysis, the investigation maintains an NRU setting of 2. As anticipated, the communication latency rises with an increase in the number of clusters (n_C). Furthermore, it's evident that EDT consistently delivers improved results. Nonetheless, a constellation with 2 satellites per orbit manages to accommodate all the generated data, albeit with slightly extended communication latency.

TABLE 1.4: Average communication latency measured under different constellation designs.

RACH Configuration	**Satellites per orbit**	**Average end-to-end delay [s]**			
		$n_C = 1$	$n_C = 4$	$n_C = 7$	$n_C = 10$
EDT disabled	3	969	1602	1869	2386
	2	1816	2739	3124	3895
EDT enabled	3	859	1061	1207	1491
	2	1646	1909	2128	2546

1.5 From Interoperability to Full Integration – the ITA NTN Project Vision

6G holds the potential to extend the horizons of existing terrestrial networks, encompassing various tiers such as spaceborne and airborne communication systems within NTN. However, the grand vision of creating a Ubiquitous Intelligent Mobile Society, characterized by scalable and efficient access to connectivity and computing services as needed and wherever needed, can only be realized in future 6G networks. This achievement hinges on the incorporation of innovative network architectures, transmission techniques, communication protocols, and service orchestration approaches that transcend the boundaries of conventional 5G enabling technologies.

Given the multitude of challenges posed by forthcoming 6G research in both academic and industrial contexts, the ITA NTN project takes center stage as a dynamic, resilient, and highly rewarding platform. Situated within the RESTART program, it provides an exciting space for the development, experimentation, validation, and enhancement of innovative approaches in the realm of integrated TN-NTN wireless networks. These approaches are aimed at facilitating the seamless provision of high-capacity, resource-intensive applications and accommodating the extensive connectivity needs of diverse device types.

At its very core, the ITA NTN project staunchly believes that the seamless integration of terrestrial and space-based wireless networks within the framework of future 6G deployments is of paramount importance. This integration is seen as a pivotal step in providing all-encompassing, readily available, adaptable, and on-demand wireless broadband connectivity. In pursuit of this goal, the project aims to develop a novel 3D network architecture capable of harnessing connections that are established and dynamically configured among various ground and space-based network elements. These elements encompass Unmanned Aerial Vehicles (UAVs), High-altitude Platformss (HAPs), aircraft, geostationary Earth orbit (GEO), and non-geostationary Earth orbit (NGSO) satellites. This architecture is intended to facilitate the delivery of a wide range of services and applications tailored to different needs. The ITA NTN project aligns perfectly with the roadmap for beyond-5G and 6G technologies, which has been outlined in documents from NetWorld 2020 Strategic Research and Innovation Agenda, 3GPP, EU initiatives directed at achieving the objectives of the 2030 Digital Decade, and the EU Global Gateway strategy. This alignment is further corroborated by ongoing funding requests and industry white papers in conjunction with the ESA.

Regarding the formulation of the *3D network architecture*, the ITA NTN project will establish a unified wireless access network that harnesses innovative transmission techniques at the physical and data-link layers. This approach entails the integration of cutting-edge wireless optical links alongside conventional wireless communication methods, coupled with the development of novel antenna and electronic technologies. Furthermore, the project will devise advanced high-level protocols grounded in the principles of network softwarization and virtualization. It will also explore the comprehensive integration of edge computing solutions and artificial intelligence methodologies, both in satellite on-board systems and at the ground level. These elements will be instrumental in the optimal coordination of physical components and network resources that are distributed across the multi-layered 3D network architecture.

What proves to be of utmost importance is the comprehensive evaluation of realistic service objectives for NTN B5G, coupled with the formulation of the corresponding performance prerequisites for satellite network components. These requirements are essential to achieve a system performance that is both acceptable and sustainable from a business perspective. This endeavor must be undertaken in conjunction with the support for all the technologies mentioned earlier, which cater to NTN-friendly services encompassing IoT, back-hauling, broadcasting, and multicasting.

Based on the roles assigned to the various layers of the 3D network, distinct architectural configurations can be identified, as illustrated in Figure 1.13. These configurations vary based on the functions allocated to the space/air segment, including entities like Integrated Access Backhaul (IAB) nodes, gNB-Distributed Unit/Central Unit, gNB, and the 5G Core Network mode.

The first configuration (*case A*) comprises a relay network based on drones connecting the user segment to the 5G Core Network on the ground. This configuration typically involves UAV or HAPs deployed in the air segment, along with a ground control station, which can be integrated within the gNB. An essential aspect that characterizes the overall architecture is the choice between deploying transparent or regenerative payloads on-board the drone. In the transparent mode, the network node

functions solely by amplifying and forwarding received data to its intended destination, which is the gNB.

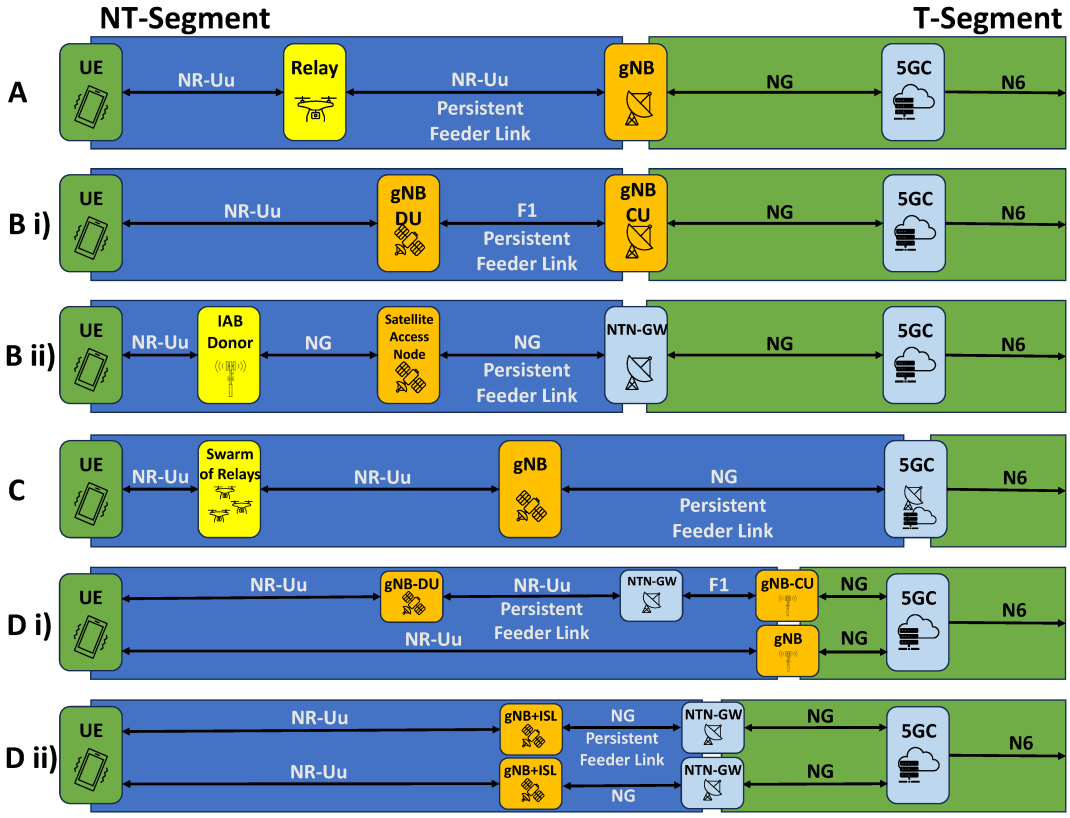


FIGURE 1.13: Possible TN-NTN architectures of interest in the ITA NTNproject.

In contrast, in the regenerative mode, the network node actively processes incoming data, makes informed decisions based on its analysis, and then regenerates the signal before forwarding it to the gNB. The gNB, which is responsible for serving the terrestrial UE, is conceptually situated at the system's Ground Station. To ensure full compliance with the 3GPP NTN standard, all Control Plane and User Plane protocols are terminated at the gNB on the ground. Consequently, the feeder and user links require the implementation of the New Radio (NR)-Uu Air Interface.

The satellite-based architecture (*case B*) is intentionally designed for long-term operation, ensuring consistent and uninterrupted connectivity while providing extensive coverage across wide areas. This architectural approach encompasses two distinct configurations involving satellites:

i) Satellite-based direct access: this involves the use of satellites to establish a direct connection between end-user devices and the satellite itself, effectively creating a direct link between the satellite and the UE. It is worth noting that a functional split option is also feasible, with an onboard gNB-Distributed Unit (DU) and an on-ground gNB-Centralized Unit (CU).

ii) Satellite-based backhauling solution: this approach leverages IAB specifications for backhauling connectivity. It may involve multiple UEs and satellites concurrently, raising concerns about network orchestration and radio resource management.

Furthermore, when multiple satellites are employed, inter-satellite communication often becomes a practical solution for covering large areas.

Within the 3D single-connectivity architecture (*case C*), UE possesses the capability to establish communication with intermediary transparent nodes located at lower altitudes, which may comprise a swarm of drones or HAPs. These intermediary nodes assume the responsibility of routing traffic to an on-board gNB on the satellite and subsequently to the Core Network located on the ground. As in other configurations, the non-terrestrial nodes can opt for either a transparent or regenerative approach. This architecture offers significant advantages, particularly in emergency scenarios, where UEs may lack the required technology or capabilities for direct communication with the satellite or the gNB.

The 3D multi-connectivity architecture (*case D*) improves network capacity by employing multiple layers or tiers of connectivity, encompassing terrestrial, aerial, and satellite networks. This architecture can be implemented in either of the following ways:

i) between a terrestrial node and a non-terrestrial node;

ii) between two non-terrestrial nodes.

In the latter configuration, non-terrestrial nodes can adapt as transparent or regenerative, providing enhanced network reliability and resilience. In the event of interruptions in one connectivity layer, the others can serve as backups or alternative routes, guaranteeing continuous communication. Nevertheless, the increased complexity of managing and coordinating such a network may present challenges. The integration and synchronization of diverse connectivity layers require advanced algorithms and protocols for efficient resource allocation. These capabilities open up the potential to deploy autonomous rescue and emergency vehicles in remote areas lacking telecommunications infrastructure.

Furthermore, by avoiding the use of UAVs and implementing greater intelligence and autonomy in the satellite, potential delays in the relay process can be minimized. However, this configuration does bring about increased complexity in payload design. It represents a highly challenging and innovative breakthrough, as it involves hosting the entire network, including gNB and CU, on-board the satellite. This approach allows ITA NTN to bypass the ground segment of the network entirely. Moreover, it introduces the opportunity for LBO of data plane traffic, enabling the direct delivery of IP services at the network's edge, and leveraging SDN and Network Function Virtualization (NFV) capabilities.

Certainly, implementing such a scenario requires an additional effort. In terms of transmission techniques, it's worth considering the possibility of implementing Optical Wireless Communication (OWC) links, especially for the first part of the Uu interface between the UE and the gNB-DU, which is the UE-UAV (or HAP) link. This approach not only addresses cybersecurity concerns but also offers a certain level of transmission performance, including throughput (at least 100 Mbps), a low BER, and reduced signal latency for average Line of Sight distances. Nevertheless, it's crucial to remain flexible when defining constraints.

Additionally, we shouldn't overlook the second part of the Uu interface between the UE and the gNB-DU (on-board the satellite), which is the UAV-gNB-DU link. This link can be implemented using RF technologies, such as THz or mmWave communication (although practical aspects need further investigation), or an equivalent

sub-6 GHz communication. Therefore, thanks to the ITA NTN project's challenges, the 3D TN-NTN network architecture has the potential to become an innovative unified radio access network, incorporating new transmission techniques at the physical and data-link layers, with a strong foundation in the OWC pillar. This innovation should always prioritize reliability and communication performance.

Chapter 2

Design and Development of Innovative Architectures and Trusted Communication Protocols for the Social Internet of Things.

The promising integration of Social Networks within the domain of the IoT has given rise to what is known as the SIoT [74]. Through autonomous interactions, smart objects have the capability to establish social connections, forming a Social Network, all without the need for human intervention. Consequently, the transition from these smart objects to social objects introduces additional opportunities for improving network resource visibility and service discovery [75] [76].

Social relationships are at the basis of the SIoT. The contributions [74] and [77] classified them through different categories to promote trustworthy interactions in a service-oriented environment:

- Ownership Object Relationship (OOR): established among objects belonging to the same owner;
- Parental Object Relationship (POR): established among objects that are part of the same family and generally produced by the same manufacturer;
- Co-Work Object Relationship (C-WOR): established among objects working together for a common goal or in the same application;
- Co-Location Object Relationship (C-LOR): established among objects always located in the same place;
- Social Object Relationship (SOR): established among objects without common attributes or characteristics coming into contact because their owners come in contact or have a social relationship.

As a result, to generate any form of relationship, each social object must verify some conditions, such as the examination of the owner profile (OOR and POR), the geographical position (C-LOR), and the operational context (C-WOR and SOR).

The reproduction of the digital counterpart of physical IoT devices greatly enhances network navigability and paves the way for exploring diverse application scenarios, such as those in the healthcare domain [78] and Vehicular Social Networks [79].

Integrating social attributes with Wireless Sensor Network (WSN) can offer several advantages compared to traditional or simple networks. Social attributes enable devices and users within the network to communicate and collaborate more effectively, providing additional context to the data generated by sensors. By incorporating social elements, devices can share information, coordinate actions, and respond to changes in the environment in a more collaborative manner. This is especially useful in scenarios where multiple devices or users need to work together to achieve a common goal. Moreover, social interactions and relationships among devices or users can provide context that enhances the interpretation of sensor data. This improved context awareness allows for more accurate decision-making and a better understanding of the environment.

This evolution necessitates the development of effective methodologies for service provisioning, with a critical requirement being the assurance of the trustworthiness of service providers [80]. In this context, the Trust Management System (TMS) emerges as a key element for evaluating the behavior of social objects and their suitability as service providers. It enables the facilitation of trusted interactions among social objects by calculating their trust levels, thereby penalizing nodes that engage in malicious or incorrect behaviors [81].

This chapter describes two works published in [82] and [83]. In particular, the first Section addresses the development of a multi-level architecture that leverages a TMS strategy for the provisioning of scalable and trusted services in the context of SIoT. On the other hand, the latter Section delves deeper into considering the equitable distribution of services in order to provide a high Quality of Experience (QoE) to end-users.

2.1 A Multi-tiered Social IoT Architecture for Scalable and Trusted Service Provisioning

In a typical deployment of the SIoT, the TMS serves as the logical entity responsible for assessing the behavior of social objects. It dynamically assigns trust values to them through automated mechanisms. Subsequently, the identification of trusted relationships facilitates the selection of the most suitable object capable of fulfilling a given request [84]. This latter task is referred to as *service provider selection*

Existing scientific literature has already proposed various methodologies to address these key functionalities. Many of these solutions, as seen in works such as [85]–[90], perform service provider selection without taking into account the availability of actual resources. Consequently, requests are often directed to social objects considering only the higher trust values, leading to network congestion and increased latencies.

Furthermore, some valuable contributions aim to implement trust computation and service provider selection directly within SIoT nodes [85]–[87], [90], [91]. Nevertheless, as explicitly pointed out by [92], this approach poses a significant limitation for SIoT devices with constrained storage and computational capabilities. Indeed, the design of a more effective SIoT architecture able to jointly address these issues still represents a challenging research goal.

To bridge this gap, this Chapter introduces a novel multi-tiered SIoT architecture in which key functionalities are thoughtfully implemented to ensure low latency, high scalability, fault tolerance, and security. Specifically, the lower level of the architecture encompasses physical objects and their logical abstractions, which expose resources and services. The TMS entity, situated within the first fog layer of the architecture, concurrently manages the trustworthiness of service providers under its control and monitors the availability of resources offered by associated social objects. This approach enables effective service provider selection without imposing additional burdens on the limited capabilities of social objects and mitigates network congestion and slowdowns.

At the second fog layer of the architecture, blockchain technology is employed to share available services, relationships, and trust values across organizations and service domains. This securely extends the scope of novel applications on a large scale.

What has been described thus far is detailed upon in the subsequent sections, where the effectiveness of the proposed approach is also rigorously evaluated through computer simulations in a realistic SIoT scenario and performance gains in comparison to a baseline solution that does not leverage the enhanced functionalities of the TMS are assessed.

2.1.1 Related works on Trust Management System in SIoT deployments

A pioneering introduction of a social TMS responsible for the assessment and management of social object trustworthiness was presented for the first time in [85]. This study explored a centralized architecture and identified its principal deployment challenges, such as a single point of failure and limited scalability. Subsequently, the scientific literature has proposed various SIoT system architectures, engaging in the design of recommendation schemes based on trust evaluation and delineating diverse strategies to facilitate a suitable service provider selection via the TMS.

For instance, the paper [86] tackles the search for service providers among distributed nodes through a novel, fast, and autonomous approach. The proposed strategy aims to reach an appropriate provider while considering nodes' energy constraints to extend the network's lifetime. However, it overlooks aspects like load balancing, storage efficiency, and the management of service requests, which are crucial for enhancing network scalability.

The work presented in [87] defines functions and parameters to compute competence and willingness, thereby quantifying trust values in the SIoT environment. Nevertheless, the entire algorithm for trust value computation is executed by IoT devices, leading to suboptimal computational loads.

The contribution in [91] offers a scheme for access service recommendation in SIoT, addressing both load balancing and network stability aspects. Within a distributed architecture, each node stores profiles of other network-involved nodes. However, storage limitations of the nodes involved may hinder their ability to maintain the extensive set of required information.

Authors in [88] propose a decentralized service-based grouping architecture for SIoT networks to reduce service discovery time. They leverage fog computing technology to enhance computational system capabilities. Nonetheless, the proposal lacks a secure distributed storage technology for managing social relationships.

The studies in [90] and [89] present blockchain-based trustful architectures for information dissemination in SIoT environments. These models offer secure and transparent mechanisms for trust evaluation. However, the former emphasizes efficient interactions to locate the most suitable service provider in the network without considering factors related to device resource usage. The latter, on the other hand, introduces an algorithm that uses information entropy to enhance system security, but it is only effective for specific time intervals.

None of the studies discussed thus far establishes a well-defined paradigm that comprehensively addresses the aspects of efficient resource management, scalability, and reliability of the Social Network of IoT objects, along with the trustworthiness and resource availability of service providers in SIoT environments.

2.1.2 The conceived SIoT tiered architecture

Figure 2.1 illustrates the novel SIoT architecture proposed in the work published in [82]. It leverages a multi-layered decentralized configuration based on fog computing technology. This configuration allows to enhance efficiency, increases responsiveness, and reduces the computational load on network nodes by utilizing the higher computational capability of the fog nodes.

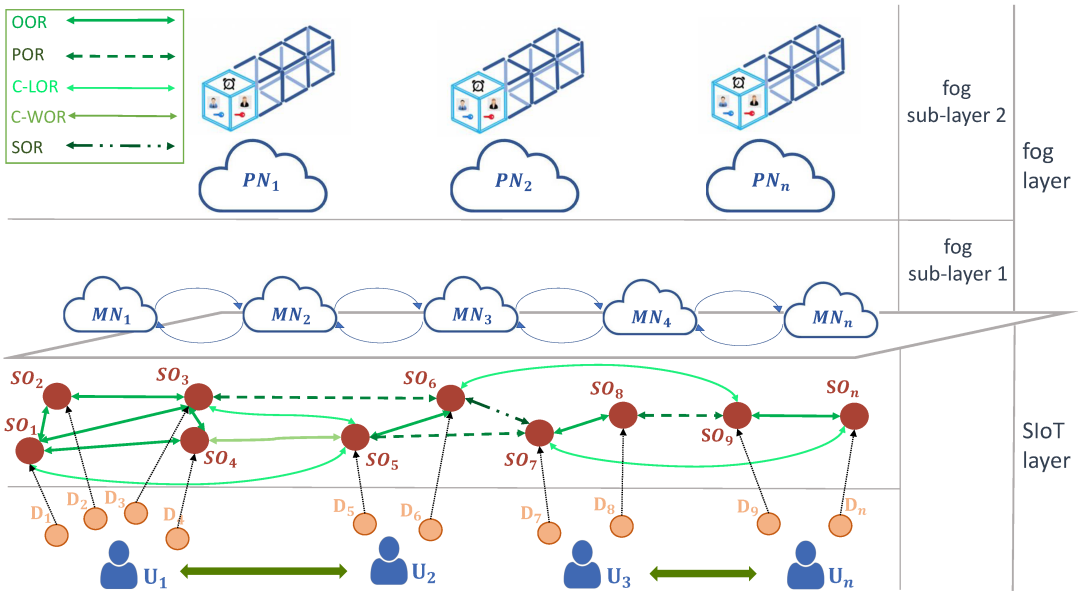


FIGURE 2.1: The proposed SIoT tiered architecture.

The lower layer of the architecture, namely the SIoT layer, handles object virtualization. Social objects reproduce the digital counterparts of physical IoT devices while also collecting social skills not explicitly supported in the real world. The attributes that identify a social object and characterize its profile include:

- Device ID, which represents a device unique identifier;

- Owner ID, an identifier of the owner of the device;
- Manufacturer ID, useful to define the device manufacturer;
- Context, which indicates the type of task or service that the device can perform. A device can have more context-related identifier values, depending on the number of tasks/services it can accomplish.
- Resource capabilities, that indicates the resources a device can employ to provide services;
- Master node list, which indicates the set of master nodes responsible for managing all information related to the device;
- Friend list, which stores all the relationships identified by a social object within the Social Network.

Master nodes constitute the first sub-layer of the fog layer, specifically referred to as *fog sub-layer 1*. The primary role of *fog sub-layer 1* is to manage the TMS for service requests.

A social object can act as both a service requester and a service provider. To promote service discovery, social objects are organized into service communities based on the types of services they can offer. It is assumed that they can provide multiple types of services, making them part of more than one service community simultaneously. In turn, each community is overseen by a master node, responsible for managing the Social Network of service providers for the specific service. This may involve generating a virtual topology for each service community.

Once social relationships are established, a social object notifies the network of its availability to provide services. Subsequently, it seeks an existing community that aligns with the services it can offer within the master nodes. If it cannot find a suitable match among the existing service communities, it initiates the creation of a new one. Given the diverse range of services within the SIoT, a service-based grouping approach significantly reduces latencies in the service discovery process [88].

The *fog sub-layer 2* interfaces with the *fog sub-layer 1* below it. It deploys primary nodes known for their substantial storage capacities, where they store all the information pertaining to social object profiles, social relationships, and reputations within a distributed database. This collective information repository is hosted on a Blockchain, which provides privacy and security for the data, defining the SIoT environment. The adoption of a Blockchain in this framework ensures robust and secure traceability of nodes, supporting the process of identifying the most suitable social object to provide a service with a high degree of trustworthiness.

Moreover, this hierarchical, distributed, and decentralized approach proves to be of paramount importance for the execution of the TMS, as it enhances scalability and efficiency. For instance, in a scenario where information concerning the reputation of a service requester isn't available at the master node, it can still be retrieved from the Blockchain located on the primary node.

2.1.3 Details on the conceived service provisioning procedure

The fundamental objective of the proposed architecture is to improve network navigability and enhance the service search process. This is achieved by carefully considering service communities and social relationships within the Social Network of objects.

Most scientific works in this context focus on evaluating the trustworthiness of service providers, primarily associated with assessing users' behavior. However, the strategy proposed here goes a step further by jointly investigating service trustworthiness and resource consumption, thus promoting service discovery beyond just reliability and security

Figure 2.2 depicts the overall service provisioning procedure.

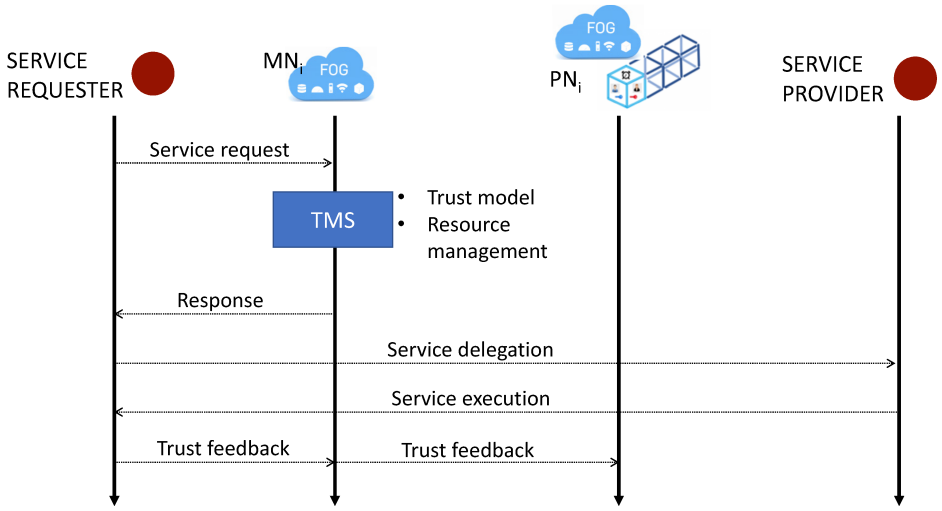


FIGURE 2.2: The service provisioning procedure on the multi-tiered architecture.

A social object initiates a service request and sends it to the nearest master node. If the master node is not in charge to manage the related service community (i.e., providers of the requested service are not in its database), the request is forwarded to the master node capable of processing the request. Through this procedure, the identification of a suitable service provider is not limited to the requester's limited knowledge or the fog node directly connected to it, enabling a global view of trustworthiness of each service provider .

Using the trust model and the resource management functionality (further described in the next Section), the TMS determines a trust ranking of providers among the social objects that can potentially offer the requested service. Subsequently, the most suitable provider in the ranking is selected for service execution.

Finally, the service requester provides to the system its degree of satisfaction for the service received through a feedback evaluation. The feedback is expressed with a value equal to 1 for service accomplished. A value equal to 0, instead, is given for a service not correctly completed. Both the fog sub-layers store the feedbacks for subsequent evaluations of the trust level.

Such information can be transferred in a Blockchain, providing privacy and security for the stored data. In the event that details regarding the reputation of a service requester are not present at the selected master node, they can still be retrieved from the Blockchain located on the primary node.

2.1.4 Trust model

Given the i-th object requesting a service s_k and the j-th object exposing a service, the TMS calculates the trust value $Tr_{i,j}^{s_k}$. In summary, $Tr_{i,j}^{s_k}$ is defined through two main factors, which are the sociality factor and reputation.

The sociality factor, $S_{i,j}$, rates the relationship established between the considered social objects by describing the degree of confidence in the case of both direct and indirect friendship (e.g., a friend of friends). In the case of direct friendship, it is set as $S_{i,j} = SO_{i,j}$, according to the type of social relationship (see Table 2.1).

In indirect friendship, instead, it is evaluated by considering the social objects' common friends. Precisely, assuming that the number of i and j common friends is equal to C, $S_{i,j}$ is computed as: $S_{i,j} = \frac{\sum_{c=1}^{C} SO_{j,c}}{C}$, where $SO_{j,c}$ represents the direct social factor rate between j and its common friends with i.

TABLE 2.1: Direct Social Factor rate based on relationships

Type of relationship	POR	OOR	C-LOR	C-WOR	SOR
$SO_{i,j}$	0.9	0.8	0.7	0.6	0.5

On the other hand, the reputation, $R_{i,j}^{s_k}$, represents the opinion on the trustworthiness of a service provider for the service s_k, based on past experiences through feedback values assigned to previous interactions among social objects. It is calculated as a linear combination of three different contributions:

- the direct feedback $\Delta_{i,j}^{s_k}$ describes how the i-th requester evaluated the j-th provider for the service s_k in the past;
- the indirect feedback $\Theta_{i,j}^{s_k}$ describes how the friends of the i-th requester evaluated the j-th provider for the service s_k in the past. Assuming that the considered requester has F friends, $\Theta_{i,j}^{s_k}$ is computed as:

$$\Theta_{i,j}^{s_k} = \frac{1}{F} \sum_{f=1}^{F} \Delta_{f,j}^{s_k}, \tag{2.1}$$

  where $\Delta_{f,j}^{s_k}$ is the feedback given by the f-th friend of the i-th requester.
- the indirect non-friend feedback $\Pi_{i,j}^{s_k}$ specifies how the other non-friend social objects evaluated the j-th provider for the service s_k. Assuming that the total number of non-friends that have previously evaluated the provider j is equal to P, $\Pi_{i,j}^{s_k}$ is computed as:

$$\Pi_{i,j}^{s_k} = \frac{1}{P} \sum_{\pi=1}^{P} \Delta_{\pi,j}^{s_k}, \tag{2.2}$$

Finally, the reputation factor is obtained as:

$$R_{i,j}^{s_k} = \alpha\Delta_{i,j}^{s_k} + \beta\Theta_{i,j}^{s_k} + \gamma\Pi_{i,j}^{s_k}, \tag{2.3}$$

where α, β, and γ are the weights ($0 < \alpha, \beta, \gamma < 1$ and $\alpha+\beta+\gamma = 1$) that determine the relevance for each factor considered in the evaluation of the reputation.

To conclude, the trust value associated to the i-th object requesting a service s_k and the j-th object exposing a service, is obtained as:

$$Tr_{i,j}^{s_k} = S_{i,j} \cdot R_{i,j}^{s_k}. \tag{2.4}$$

2.1.5 Resource management

Utilizing the trust model presented in the previous section, it becomes possible to identify trusted social objects and exclude all providers falling below a configured threshold from the selection of service providers. Furthermore, through the determination of the trust value for each service provider, the master node establishes a ranking based on social object reliability.

Furthermore, the proposed TMS also incorporates an additional investigation into the resource capabilities of social objects. This contribution is particularly crucial for trust evaluation, especially in an environment consisting of nodes with limited resources.

In fact, when multiple service requests are assigned to the same social object with limited resource capabilities, there's an increased risk of service execution failures due to resource constraints. Consequently, the social object's ability to provide the requested service diminishes, potentially leading to network congestion.

To address this, the master nodes continuously monitor the status of social objects and the resources required for service execution. After the ranking computation, the candidate provider's resource capacity is monitored to ensure the social object's availability for service execution. If this check fails, the candidate provider is temporarily removed from the list. The master node updates the ranking and repeats the investigation with new candidates until a service provider with the required resource capacity for executing the service is found.

2.1.6 Performance Evaluation

The performance of the proposed SIoT architecture and service provision scheme are investigated herein through computer simulations. To this end, a MATLAB script is used to model a Social Network with heterogeneous objects, various traffic loads, together with all the procedures described in subsection 2.1.3.

The proposed scenario includes a fog layer consisting of five master nodes coordinated by a primary node for service request management. The number of social objects varies from 50 to 300, and they are evenly distributed among four classes (smartphones, smart cameras, sensors, and smart gateways) based on their resource capabilities. Each social object randomly generates service requests according to a Poisson distribution with different λ values (ranging from 0.5 to 2 requests per second) to simulate various traffic loads.

As described in subsection 2.1.2 regarding the envisioned architecture, each social object is characterized by an ID, an owner ID, a manufacturer ID, geographical position, a list of services it can provide, and its resource capability. Resource capabilities are set as summarized in Table 2.2, following the approach in [91].

For simplicity, the Social Network is created by considering only POR, OOR, and C-LOR relationships, which are based on the knowledge of owner, manufacturer, and geographical position attributes, respectively.

TABLE 2.2: Resource Capability Classes [91].

Social object class	Resource Capability
Smartphone	0.8
Smart gateway	0.6
Smart camera	0.4
Sensor	0.2

Seven different types of service communities are configured and distributed among all the master nodes. Each social object joins the proper service community handled by a master node, following the procedure explained in subsection 2.1.2. As reported in Table 2.3, each service is identified by an ID, the resource consumption needed to be accomplished (spanning from 0.1 to 0.3), and the execution time (spanning from 2 s to 8 s).

TABLE 2.3: Services characteristics.

Service ID	1	2	3	4	5	6	7
Resource Consumption	0.3	0.2	0.2	0.1	0.1	0.2	0.1
Execution Time [s]	2	7	3	7	2	8	5

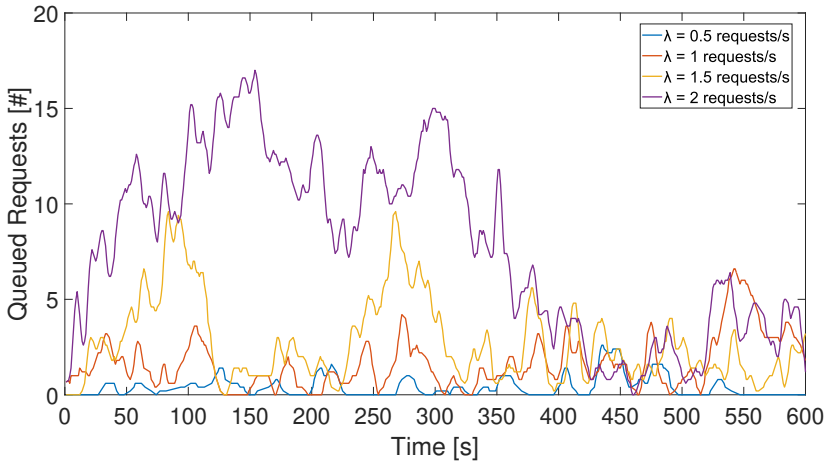
Finally, the performance of the proposed approach is compared with the baseline architecture, where the TMS calculates the trustworthiness of social objects by taking into account relationships and reputation parameters without any resource control.

2.1.7 Simulation results

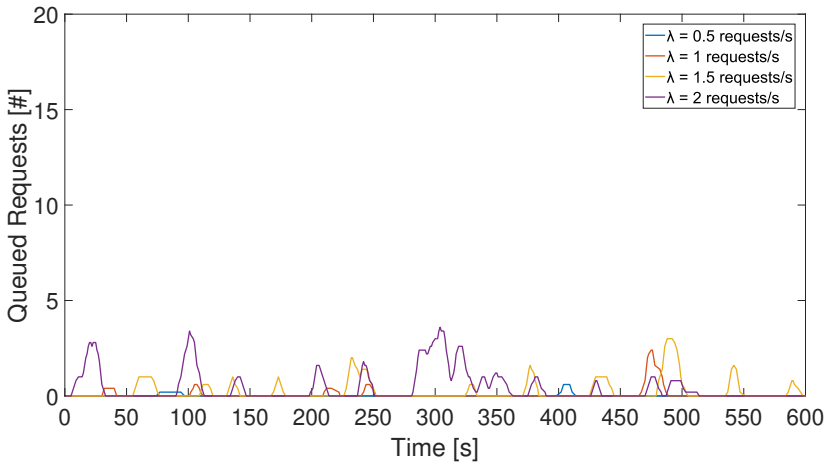
Figure 2.3 shows the number of queued requests during the time for different traffic loads.

The results are obtained for a single scenario conducted on a social network with 150 social objects. For each λ, results are obtained from ten simulation runs to account for different network topologies and service distributions, and then averaged over a five-second time window sliding by one second.

The reported curves highlight the ability of the proposed approach to handle most of the requests in real-time. Service requests are efficiently distributed to available trusted objects, preventing queuing phenomena. In contrast, the baseline approach distributes requests without considering resource availability. Consequently, most requests are directed to a small set of trusted social objects, which monopolize scheduler assignments and quickly exhaust their available resources. As a result, a service provider selected to execute a service by the TMS may not have sufficient resources, leading to the formation of a queue of pending requests and an increase in latency.



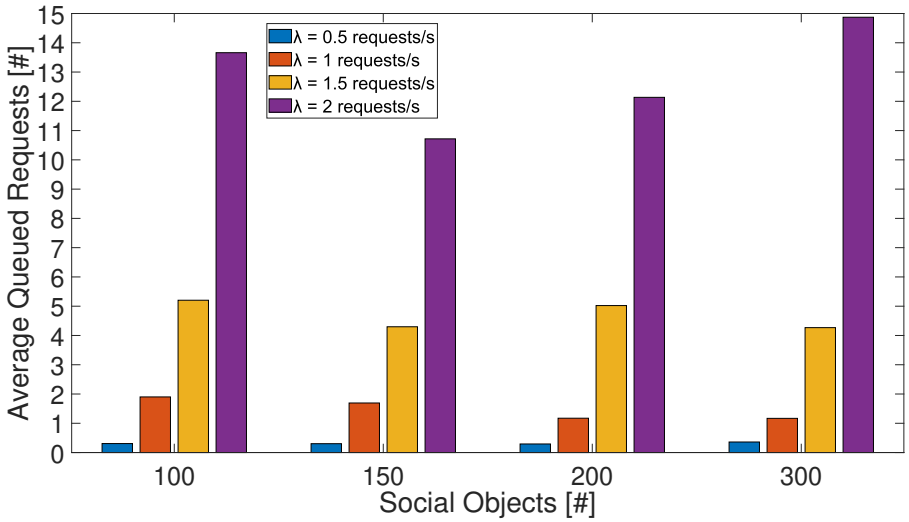
(A) Baseline approach



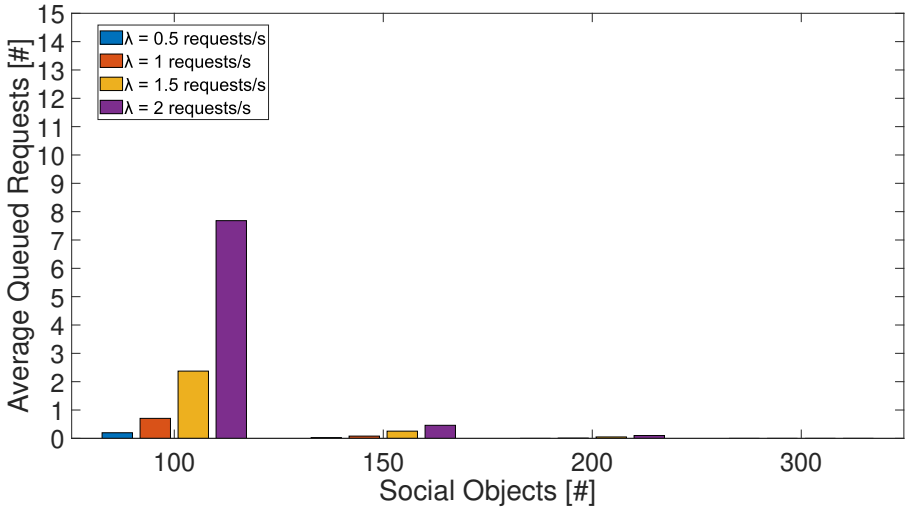
(B) Proposed approach

FIGURE 2.3: Queued Requests Evaluation.

In order to generalize the afore discussed findings, Figure 2.4 shows the average queued requests for different traffic loads.



(A) Baseline approach



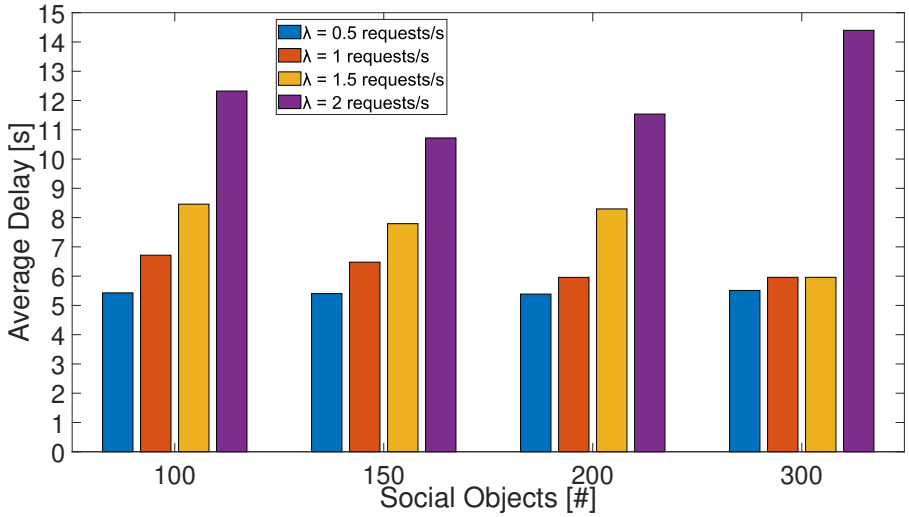
(B) Proposed approach

FIGURE 2.4: Queued Request increasing traffic load.

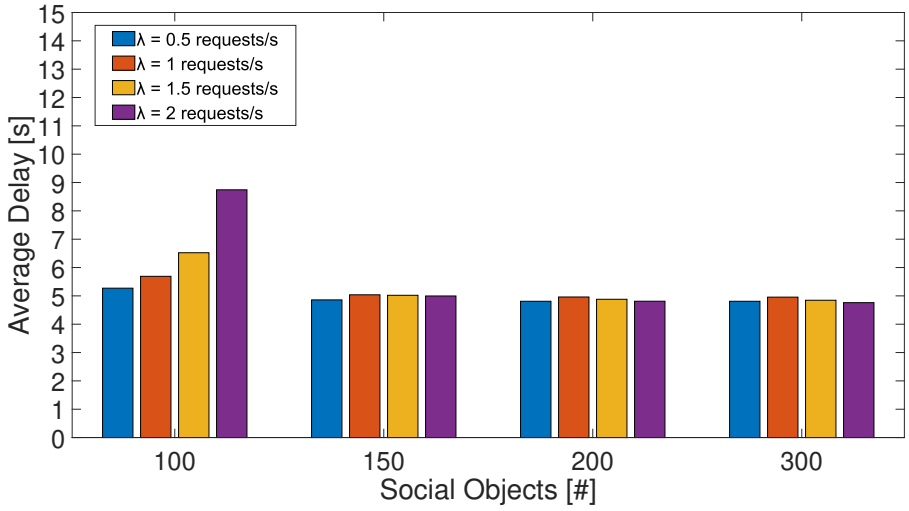
Resource management allows for the minimization of the number of pending requests, thereby improving network scalability. In contrast, the baseline approach struggles to handle large volumes of traffic, resulting in an increase in queued requests and, consequently, a delay in completing them.

Furthermore, the average number of queued requests scheduled in the proposed TMS decreases as the number of nodes increases. This demonstrates a significant scalability improvement compared to the baseline approach. Consequently, the network can effectively handle a substantial increase in traffic (e.g., from 0.5 requests/s to 2 requests/s) without overloading the resources of social objects.

Figure 2.5 depicts the average delay experienced for a request in the proposed and the baseline approach.



(A) Baseline approach



(B) Proposed approach

FIGURE 2.5: Average Delay increasing traffic load.

The delay is represented by the average time taken for each requested service from its generation until the completion of its execution. It does not account for the time needed to exchange control messages or interactions between master nodes, as this time is negligible compared to the service execution time. Thanks to the intelligent management of available resources in social objects, the delay performance of the proposed approach remains consistent even with a high number of social objects. It also outperforms the baseline approach, particularly under heavy traffic loads.

In contrast to the baseline approach, the proposed test does not reveal any performance degradation in terms of average delay in request fulfillment. Indeed, as the number of nodes and the request rate λ increase, the average delay remains constant.

The differences between the two approaches become more pronounced in configurations with higher population. For instance, when considering 300 social objects and an average request rate of 2 requests per second, the average delay experienced can be reduced by up to 60

Finally, to provide further insight, Figure 2.6 illustrates the evolution of feedback aggregation over time for six service providers. Three of them were compelled to act as malicious nodes, failing to provide a service after a request and receiving negative feedback accordingly. This result underscores the effectiveness of the developed TMS in detecting potential malicious nodes. Indeed, after a warm-up period of approximately 100 seconds, the identification of malicious nodes becomes unmistakable. Since the proposed model is reputation-based, a decrease in trustworthiness due to negative feedback leads the system to select only trustworthy social objects for scheduled requests in the service provider selection.

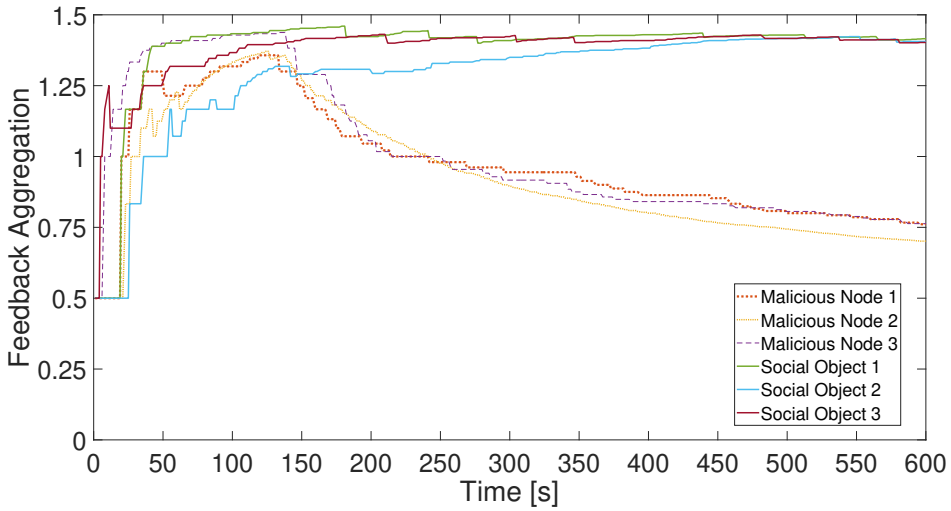


FIGURE 2.6: Malicious social objects detection.

2.2 Boosting Service Provisioning in SIoT by Exploiting Trust and Capability Levels of Social Objects

The burgeoning phenomenon of the SIoT has been experiencing an upswing due to its distinctive capacity for autonomously building social connections among intelligent entities and facilitating innovative services within the domain of the Social Network. In the course of service provisioning, the TMS assumes responsibility for the identification of appropriate entities capable of fulfilling the specified services, predicated upon their reliability and resource capabilities. This conceptual framework is elucidated in the approach presented in the publication [82], and further described in the section 2.1.

Extensive research in this domain has examined a multitude of methodologies aimed at assessing and governing the trust levels of service providers within SIoT settings (as evident in works such as [86], [91], [93]–[96] and the comprehensive review within subsection 2.1.1).

Nonetheless, the development of particular strategies that take into account the computational capabilities of social entities within the TMS, with the intention of expediting and enhancing service provisioning, remains an unexplored territory. Moreover, the existing solutions, characterized by their computational complexity, present a challenge in terms of practical applicability in real-world scenarios, primarily due to their unsuitability for most resource-constrained IoT devices.

At the juncture when the research documented in [83] was conducted, and as far as the authors were aware, the prevailing body of scientific literature solely focused on the construction and evaluation of a TMS from the trustworthiness perspective. Consequently, this approach presented certain constraints pertaining to the executed processes, particularly in terms of responsiveness, resource capability, efficiency, and scalability.

For example, the studies in [91] and [86] face the selection of the most suitable service provider in a TMS considering the energy constraints to evaluate the provider resources. The former proposes device trust dimension referred to the current energy status remaining unaware of device computational capabilities. The latter aims to increase the network lifetime, but it ignores the management of service requests and storage-saving procedures.

The paper [93] develops two algorithms for an efficient resource selection available through information sharing between social objects. Nevertheless, the described strategies do not implement a trust metric that jointly considers trustworthiness and resource efficiency aspects. The contribution in [94] proposes a distributed architecture based on a Blockchain for the secure provision of trust in an IoT system. It adopts a stochastic approach to detect and prevent malicious behaviors within a lightweight implementation. The results are obtained only for typical deployments operating with a limited number of nodes. So, the approach is not suitable for real-time systems, since it can only handle information generated at a quite low speed.

The authors in [95] investigate a TMS for the evaluation of service providers' past experiences and quality of service recommendations. The described self-adapted model dynamically fits changes in network context or type of demanded service. However, the presented model is entirely borne by the social objects. Consequently,

it has the main limitation of the applicability to real-world scenarios with limited computation and storage capabilities of IoT devices.

Another work presented in [96] suggests a hybrid method to overcome the weakness of both centralized and decentralized approaches for trust management. Despite considering the evaluation of available resources, it mainly focuses on the user trust classification. In particular, it detects possible trust attacks via Machine Learning methods, without investigating the opportunity to distribute service requests to the most suitable service providers from the capability point of view.

Differently from the aforementioned studies, and with the objective of broadening the scope of scientific discourse to address the prevalent challenges inherent in SIoT implementations, the research documented in [83] and delineated in this Chapter, introduces a novel resource capability-aware scheme for the TMS.

To be more specific, the newly proposed framework incorporates additional functionalities that concurrently take into account trustworthiness, resource availability, and the computational capabilities of the entities enlisted in the Social Network, all with the aim of expediting the provisioning of trusted services.

Moreover, this proposed strategy harnesses fog computing to execute all TMS operations. This approach alleviates the processing and storage demands on IoT nodes throughout the entirety of the TMS process, encompassing the establishment of social connections, rendering it highly suited for real-world scenarios.

Simulation results, as detailed in subsection 2.2.3, underscore the efficacy of the suggested scheme, particularly in relation to the diminished latency observed in service provisioning. Notably, the latency is reduced by as much as 67% when compared to the benchmark solutions, all the while ensuring equitable allocation of the accessible resources among service providers. Additionally, the enhanced functionalities of the TMS augment the responsiveness in identifying potentially malevolent devices, facilitating their swift exclusion from the service provisioning process.

2.2.1 The overall system architecture

This study addresses a reference environment comprising numerous IoT nodes organized into clusters, their arrangement determined by geographical location, and overseen through a distributed approach.

The architecture depicted in Figure2.7 shows the resultant multi-layered structure of the SIoT, a customized adaptation of the architecture originally formulated in [82] and detailed in the preceding Chapter.

The lower layer is designated as the Physical Layer, where the ensemble of nodes corresponds to the physical IoT devices. Each IoT device is endowed with the capability to function as either a service requester or a service provider. For the sake of generality, this study accounts for three distinct classes of IoT devices, as delineated in [97]:

- Class 0: devices characterized by severe resource limitations, exemplified by sensors with mere tens or hundreds of kilobytes of RAM;
- Class 1: devices subject to resource constraints, albeit possessing some processing capabilities, typified by examples like Arduino and smart cameras;

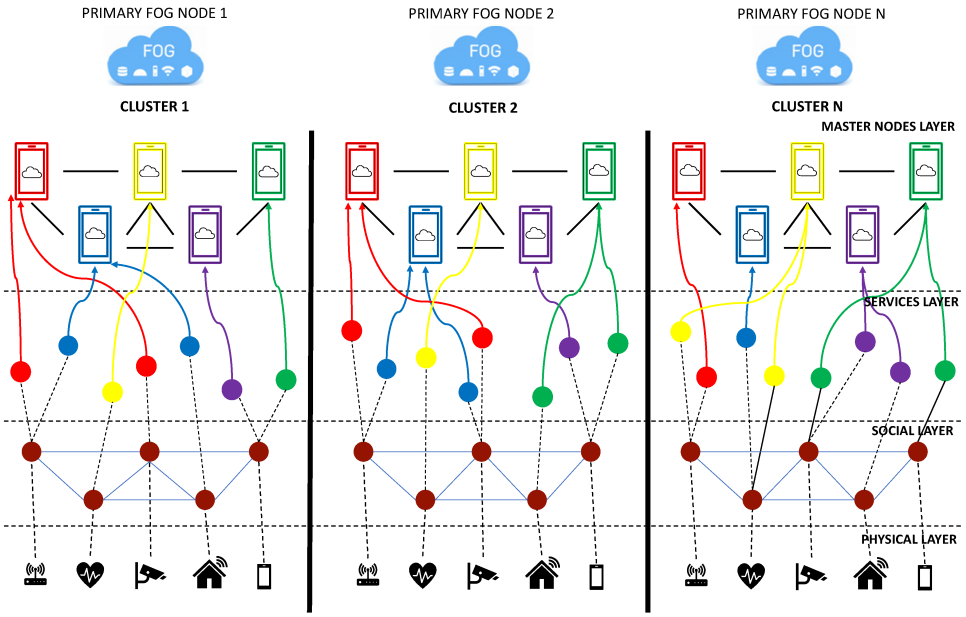


FIGURE 2.7: The proposed layered architecture.

- Class 2: devices endowed with ample resources, including substantial RAM, enabling the execution of demanding computations, such as Machine Learning algorithms. A prime instance of this class is represented by smartphones.

The subsequent layer is the Social Layer, where IoT devices undergo the transition into social objects. Within this layer, these devices, through their abstraction, assume the role of digital counterparts to their physical one, thereby gaining the capability to expose attributes that are conducive to the formation of social connections. In order to specify the divulged attributes, a social object is uniquely identified by an ID, accompanied by details regarding its owner and manufacturer. Furthermore, it encompasses all attributes that delineate its operational capabilities, encompassing factors like power level and clock speed.

The third layer is designated as the Service Layer. Within this tier, each social object outlines a list of the services it is capable of providing. In this virtualized service layer, social objects have the ability to join and participate in communities that are structured around common application contexts, thereby enhancing the network navigability.

Furthermore, the overall architecture comprises two hierarchical levels that harness fog computing technology. The first of these level, referred to as the Master Node level, comprises fog nodes endowed with robust computational resources dedicated to the processing and dissemination of service requests. This level hosts the TMS, responsible for making recommendations concerning the choice of a service provider during the service provisioning procedure. Each Master Node is tasked with overseeing one or more service communities. Furthermore, to facilitate the determination of the most appropriate service provider, it retains comprehensive records encompassing past experiences and the complete dataset of attributes associated with registered social objects, all of which are instrumental in constructing a social-oriented virtual topology for each service community.

In contrast, the higher level, denoted as the Primary Fog level, is composed of Primary Fog Nodes equipped with ample storage capacity. This level is responsible for managing the dataset associated with a cluster of social objects. Specifically, a Primary Fog Node facilitates the seamless synchronization of the distributed cluster architecture through interactions with other Primary Nodes.

2.2.2 Details on the new conceived methodology

Upon its inclusion in the Social Network, a social object expresses its willingness to offer a service. During this phase, it utilizes a dedicated API to transmit its attributes to the Master Nodes. These attributes play a critical role in constructing a virtual topology that encapsulates the established social connections. The computation and storage of social relationships are entirely entrusted to the Master Nodes, which serves the purpose of making the proposed strategy practicable in real-world situations by relieving the social objects from this computational burden.

In the event that a node needs to retrieve a service, it dispatches a request to the Master Node that handles the community responsible for provisioning that particular service. This methodology streamlines the process of service discovery, thereby limiting the selection to a subset of providers predicated upon their established social relationships.

By managing a service request, each Master Node executes the functions inherent to the TMS, with the objective of determining the most suitable service provider. Once more, this approach mitigates the computational load on social objects. This attribute serves as an additional benefit, given that the computation of the optimal service provider carries the potential to exert a substantial impact on the utilization of storage and resources. Such an expensive task would be impractical for numerous IoT devices.

The two procedures implemented by the TMS for the service request management are summarized in the following steps.

Step 1 - Trust List Evaluation.

Upon receipt of an incoming request, the Master Node conducts a database query to ascertain the presence of social objects that exhibit a social connection with the requesting entity. Subsequently, it generates a Trust list comprising potential service providers. For each provider listed in the Trust list, the TMS conducts an assessment of the Trust value, which quantifies the degree of trustworthiness attributed to the service provider. The Trust value calculation proceeds as described in the subsection 2.1.4. It's worth noting that the trust calculation operation pertains to a single service type and is computed by the Master Node responsible for overseeing the respective community. It is summarized as follows.

Considering the i-th social object requesting a service and the j-th social object as a possible provider, the Trust value $Tr_{i,j}$ is calculated through two main factors. Firstly, the Sociality factor $S_{i,j}$ expresses the friendship ties between social objects. Table 2.4 describes the rates of the established relationship considered in [83], classified in order of relevance (i.e., the OOR referred to the same owner is the stronger friendship tie, followed by POR, C-LOR, and C-WOR referred to the same manufacturer, location, and working goal, respectively).

TABLE 2.4: Friendship ties rates.

Type of relationship	OOR	POR	C-LOR	C-WOR
$S_{i,j}$	0.7	0.65	0.6	0.55

Secondly, the Reputation factor $R_{i,j}$ is defined based on the history of the previous behavior of social objects, expressed through past received feedback. The Reputation factor is evaluated as follows:

$$R_{i,j} = \alpha\Delta_{i,j} + \beta\Theta_{i,j} + \gamma\Pi_{i,j}, \tag{2.5}$$

where:

- $\Delta_{i,j}$ represents the direct reputation and is calculated as the sum of positive feedback values divided by the total number of the feedbacks given by the i-th requester to the j-th provider;
- $\Theta_{i,j}$ represents the friend indirect reputation and is calculated as the sum of positive feedback values divided by the total number of the feedbacks given by friends of the i-th requester to the j-th provider;
- $\Pi_{i,j}$ represents the overall indirect reputation and is calculated as the sum of positive feedback values divided by the total number of the feedbacks given by the other non-friends of the i-th requester to the j-th providers;
- α, β, and γ are weights determining the relevance of each factor.

Finally, the Trust value is computed as reported in Eq.(2.6) (for details on the Trust model please refer to [82]):

$$Tr_{i,j} = S_{i,j} \cdot R_{i,j}. \tag{2.6}$$

Upon assigning Trust values to all potential providers in the Trust list, the procedure promptly eliminates any service provider whose Trust value falls below a predefined threshold, which has been empirically defined. This aspect serves as a preventative measure against the likelihood of errant nodes rehabilitating their reputation and subsequently reverting to malicious behavior.

Step 2 - The Novel Resource Capability Management.

To enhance the quality of the service provisioning experience, the assembled Trust list is subjected to a two-tier sorting process. Notably, the initial sorting criterion is the device class, while the subsequent criterion is the trustworthiness deriving from Trust value computation.

This approach introduces an innovative and key facet of the devised scheme: a novel ordering technique designed to optimize resource allocation, affording the capability to fulfill time-sensitive tasks demanding stringent performance and quality. The advantages associated with the selection of trusted service providers, who possess the proper resources for executing the services, will be substantiated by the numerical findings detailed in the subsequent section.

Through the aforementioned approach, the Master Node constructs a ranking based on both social aspects (Step 1) and performance considerations (Step 2). Additionally, the proposed TMS incorporates an additional evaluation step that takes into account the resource availability of potential service providers. Specifically, the resource management feature actively monitors the resources of the recommended provider and verifies its capacity to undertake the service. In cases where this verification fails, the recommended provider is temporarily excluded from the Trust list, with reconsideration scheduled for when sufficient resources become available. The system repeats this assessment on the updated ranking until a qualified provider is identified.

The most suitable provider from the ranking, satisfying the necessary resource requirements, is chosen for executing the service. Subsequently, the requester furnishes feedback regarding the service's execution. This feedback serves to indicate whether the service was completed in accordance with the requester's expectations, expressed through a binary value, where '1' denotes successful service accomplishment and '0' signifies service non-compliance. The received feedback is then archived within the proper Master Nodes, facilitating Trust value updates in anticipation of future service requests.

2.2.3 Performance Evaluation

This section assesses the performance of the proposed methodology using computer simulations. For this purpose, we have developed a C++ object-oriented and event-driven simulator from the ground up, aimed at evaluating several key metrics. These metrics include the average delay experienced during service provisioning, the fairness in service distribution, and the responsiveness exhibited by service providers.

The devised scheme is subjected to comparison with two alternative approaches. The first approach serves as the baseline and does not incorporate any awareness regarding the quantity or quality of available resources within the network. The second approach, denoted as the resource availability-aware approach (as detailed in the previous Chapter and in [82]), does account for resource availability but lacks an integrated resource capability management framework for service provider selection within the TMS.

Simulation parameters

Without compromising generality, the presented scenario focuses on a social object cluster that falls under the management of a single Primary Node. Within this cluster, the TMS is executed by a group of 5 Master Nodes. The quantity of social objects within the cluster varies within the range of 100 to 300, including instances of 100, 150, 200, and 300.

A typical use case that can be represented by the selected parameters involves IoT entities integrated into the supply chain to monitor the movement and condition of goods in transit. Here, stakeholders along the supply chain, including manufacturers, distributors, and retailers, can share real-time updates on inventory levels, delivery times, and product conditions through social platforms. This collaborative sharing improves supply chain visibility and coordination.

In accordance with the details presented in subsection 2.2.1, each social object exhibits distinct attributes, including a unique object ID, owner ID, manufacturer ID, geographical location, processor clock speed (expressed in megacycles/s), power level, and a list of services it offers.

Within the cluster, various device types (e.g., smartphones, smart gateways, smart cameras, and sensors) are generated within a uniform distribution across the cluster, whose computing capabilities are reported in Table 2.5. Additionally, each social object can be categorized into one of three distinct QoE classes, as also outlined in Table 2.5.

TABLE 2.5: Device parameters and QoE classes.

Social Object Class	**Power Level**	**Clock Speed** (Clk) **[Megacyles/s]**	**QoE Class**
Smartphone	0.8	2000	2
Smart Gateway	0.6	1000	1
Smart cam	0.4	1000	1
Sensors	0.2	40	0

Consistent with the conventions of a typical SIoT deployment, the formulated scheme assigns each generated social object to a specific Master Node. Subsequently, the attributes defined for these objects, such as owner, manufacturer, and geographical location, facilitate the delineation of social relationships. Specifically, this study accounts for three relationship types: OOR, which pertains to objects owned by the same user; POR, which applies to devices produced by the same manufacturer; and C-LOR, which encompasses devices situated in the same geographical location.

Furthermore, the scenario proposed here encompasses six distinct types of services, each characterized by a unique ID, a parameter specifying the requisite resources for task completion (ranging from 0.1 to 0.3), and the size of data to be processed, as elaborated in Table 2.6.

TABLE 2.6: Services Requirements.

Service ID	1	2	3	4	5	6
Resource Consumption	0.3	0.2	0.1	0.2	0.1	0.3
Information Size (B) **[Mbit]**	1.4	1.0	0.6	1.0	0.6	1.4

According to this, the j-th social object can provide the service S by reserving part of its computing capabilities for an amount of time $t(j, S)$ equal to:

$$t(j, S) = \frac{X \cdot B(S)}{Clk(j)}, \tag{2.7}$$

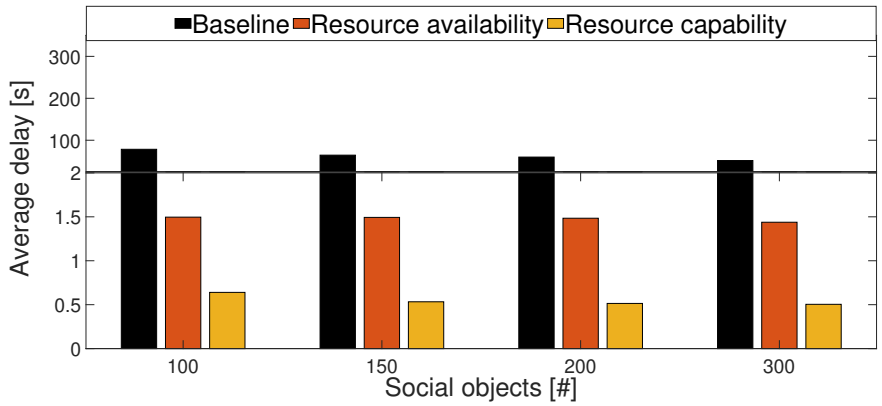
where X is the number of CPU cycles needed to process a single bit, $B(S)$ describes the total number of bits to process to accomplish the service S, and $Clk(j)$ denotes the clock speed of the j-th social object in charge to process the service S expressed in cycles/s. According to [98], X has been set equal to 1000 $\frac{cycles}{bit}$.

In order to assess network performance under various traffic conditions, service requests are generated in accordance with a Poisson distribution. The average request

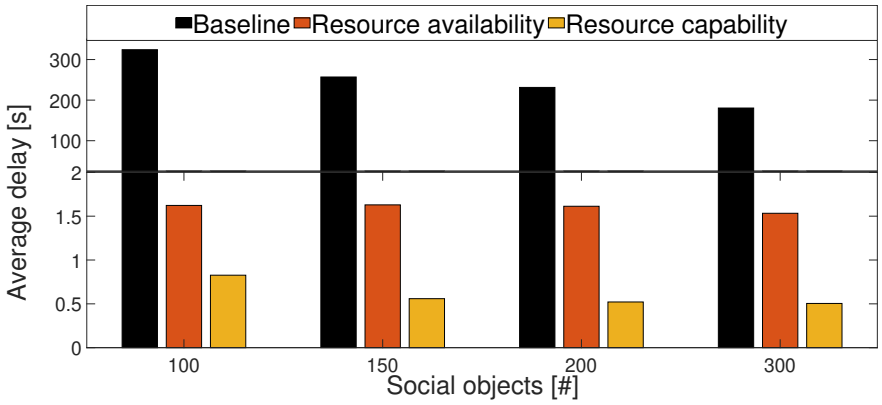
rate, denoted as λ, is systematically varied across a range from 4 to 10 requests per second. These requests are randomly selected from the pool of services described in Table 2.6. Furthermore, for each scenario under examination, the results are gathered from 20 distinct seeds. This approach is employed to encompass diverse network topologies, service configurations, and social relationship distributions, ensuring a comprehensive evaluation.

Average delay

The initial KPI employed for confronting the proposed approach with other methodologies is the average delay encountered during service provisioning. This metric signifies the mean duration that each requested service requires, spanning from its initiation to the completion of its execution. The results are presented in Figure 2.8.



(A) λ = 4 requests/s.



(B) λ = 10 requests/s.

FIGURE 2.8: Average delay.

More in detail, the baseline approach hinges solely on the trustworthiness parameter for provider selection, without factoring in resource availability. Consequently, it biases provider selection toward a limited subset of nodes characterized by high trustworthiness, thereby subjecting them to an overload of service requests. Consequently, even with low values of λ, this approach incurs the highest average delay.

Conversely, the resource availability approach demonstrates a lower average delay compared to the baseline. This is attributed to its competence in distributing service requests across social objects possessing adequate available resources to complete the

requested tasks. Consequently, the waiting time for an accessible provider is substantially diminished. Interestingly, the delay outcomes exhibit minimal fluctuation even as the request rate increases.

Finally, the proposed resource capability-aware scheme consistently records the most minimal experienced delay. Indeed, by taking into account providers with ample resources and higher QoE classifications during the provider selection, the approach significantly enhances the performance in executing the required tasks, leading to a considerable reduction in service provisioning latency.

The effectiveness of the proposed approach in fulfilling requests by identifying the most suitable providers is validated in an extensive-scale scenario. This ensures heightened responsiveness and scalability for the network in comparison to other methodologies. For instance, in the case of 300 social objects and a request rate (λ) of 10 requests per second, the average delay experiences a reduction of up to 67% in contrast to the resource availability approach.

Processing Time

Table 2.7 illustrates the processing time required by the proposed scheme to determine the appropriate service provider. The simulations were conducted on a computer equipped with an i7-7700 CPU and 16 GB of RAM. The processing time represents the average duration for a Master Node to execute the entire procedure outlined in the TMS, as described in subsection 2.2.2. Each scheduled request is handled within a time frame ranging from 1.2 to 4.5 milliseconds, an interval that proves to be negligible when compared to the overall delay encountered during service provisioning. As a result, the computed processing times underscore the computational efficiency and scalability of the proposed scheme, regardless of varying traffic loads and Social Network sizes.

TABLE 2.7: Processing time.

Scenario		**Processing time [ms]**
Social Objects	λ **[requests/s]**	
100	4	4.5
	10	3.6
150	4	1.3
	10	1.2
200	4	2.0
	10	1.7
300	4	4.2
	10	4.0

QoE Fairness Index

To strengthen the robustness of the findings, we assess the well-known QoE Fairness Index, introduced in [99]. This index evaluation quantifies the equity in the distribution of services, taking into account the QoE as perceived by social objects. The index computation is expressed as:

$$F = 1 - \frac{2\sigma}{H - L}, \tag{2.8}$$

where σ is the standard deviation providing a measure of the dispersion of QoE among social objects, while H and L are the upper and lower device classes, respectively.

Figure 2.9 illustrates the QoE Fairness Index, where each box is indicative of key statistics. The central mark represents the median, while the lower and upper edges signify the 25^{th} and 75^{th} percentiles, respectively.

For a scenario involving 100 social objects, the proposed approach achieves a QoE Fairness Index of 0.6, marking an improvement of the double when compared to the alternative approaches. This enhanced efficiency further scales with the enlargement of the Social Network size. In a large-scale scenario featuring 300 social objects, the boost in the QoE Fairness Index triples, affirming the scalability and fairness in service distribution rendered by the proposed approach.

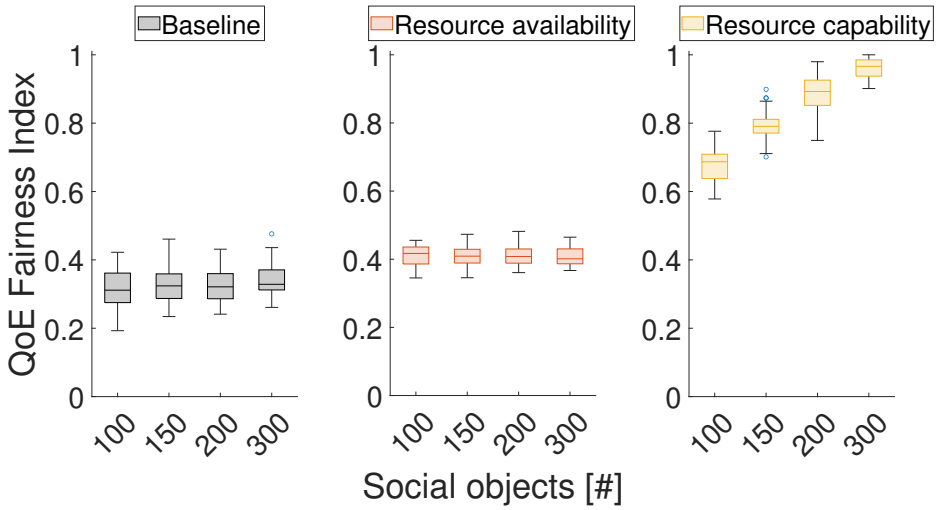


FIGURE 2.9: QoE Fairness Index.

Responsiveness in malicious nodes identification

This section offers additional noteworthy insights regarding the efficacy of the formulated strategy in the detection of malevolent nodes. Figure 2.10 portrays the temporal progression of the direct feedback received by a specific provider, averaged across the entire feedback pool. This averaged feedback is referred to as *aggregated feedback*.

This aspect is evaluated within a Master Node, considering a scenario with six social objects responsible for provisioning the same service. In this particular setup, three nodes have the potential to act maliciously, exhibiting a higher frequency of subpar service provision compared to others. Consequently, the accumulation of negative feedback has a detrimental impact on the overall reputation of these misbehaving providers.

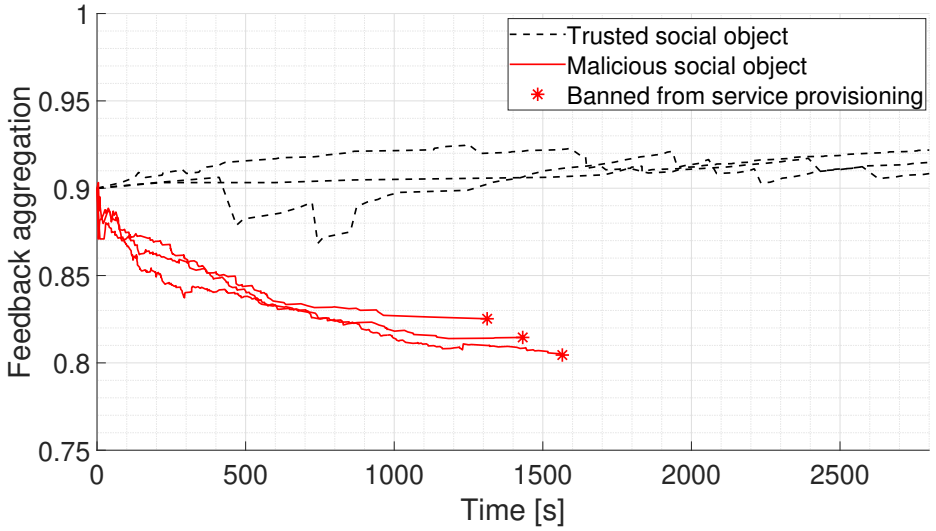


FIGURE 2.10: Temporal evolution of the aggregated feedback.

The results obtained underscore the effectiveness of the proposed TMS in the identification of malicious nodes. Indeed, the misbehaving social objects are systematically excluded from the service provisioning process and are unlikely to be engaged in the future, as indicated by the red curves in the graph, which are truncated after approximately 1300 seconds. This outcome signifies that no further feedback will be furnished for the three malicious nodes, who are effectively banned from participating in service provisioning.

To gain further insights, Figure 2.11 presents the number of malicious nodes detected by the TMS over time, averaged across 20 different simulation runs for the three schemes selected for comparison. The specific scenario considered consists of 100 social objects, with ten of them having an elevated probability of engaging in malicious activities.

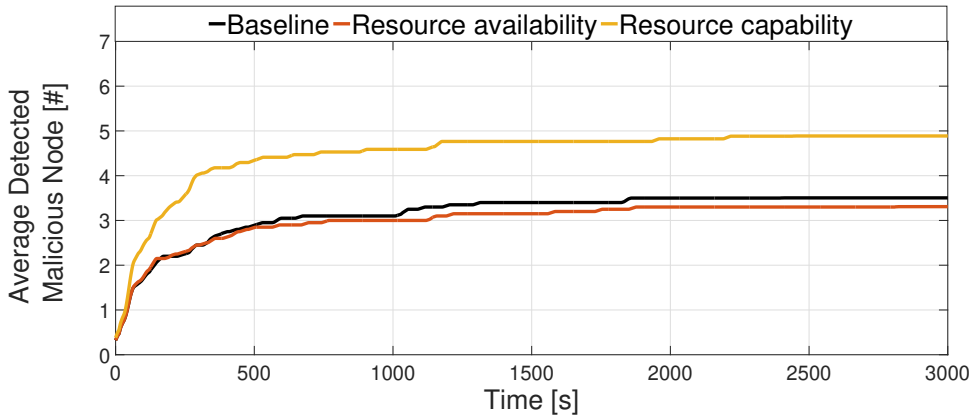


FIGURE 2.11: Responsiveness in malicious nodes identification.

Notably, within this scenario, the TMS framework devised in this study exhibits a superior capability to identify a greater number of nodes that should be excluded from the network, particularly evident after just 500 seconds. This underscores the exceptional responsiveness of the proposed approach in detecting ambiguous or malevolent

behaviors during the service provisioning process when compared to the alternative solutions.

Chapter 3

Non-Terrestrial Elements Employment within a Virtualized Ecosystem: a Comprehensive Use Case

Building upon the acquired knowledge of NTN architectures and network virtualization approaches, this Chapter presents the work conducted and published in [100]. In particular, the study focused on the analysis of a typical use case involving both NTN elements, such as drones, and the promising technology of NDT for the virtualization of network elements to streamline the management of network services and resources. Thanks to this, it was possible to consider and evaluate the parameter of trustworthiness, including TMS functionalities, as further described in the previous Chapter.

3.1 Surviving disaster events via dynamic in-network processing assisted by Network Digital Twins

UAV, more commonly recognized as drones, possess the potential to be categorized as constituents within a NTN contingent upon the manner in which they are harnessed and assimilated within a comprehensive communication framework. Nevertheless, it is important to note that the functional efficacy of UAVs frequently hinges upon terrestrial control and communication infrastructure. Consequently, their amalgamation into an overarching NTN is contingent upon the particular employment scenario and the extant technological infrastructure.

Owing to their versatility, agility, cost-effectiveness, and rapid deployability, the utilization of UAV has emerged as a compelling choice for furnishing auxiliary services in the context of natural disaster management, as highlighted in [101]. Specifically, UAVs are capable of capturing video data essential for disaster recovery and can serve as countermeasures for monitoring disaster-affected areas, with data offloading to proximate and available network segments for subsequent processing [102]. It is worth noting that UAV-based monitoring services often necessitate substantial computational resources that are typically absent in the UAVs themselves, rendering onboard processing unfeasible. Consequently, task offloading emerges as a viable approach to address this inherent challenge.

Nonetheless, it is imperative to recognize that natural disasters inevitably engender disruptions in users' network coverage, service persistence, and accessibility, underscoring the indispensability of effective disaster management and the expeditious reestablishment of network connectivity [102]. The exigent data offloading and subsequent processing tasks required for the determination of search and rescue actions during such exigencies present significant challenges. Disruptions precipitated by natural disasters render network segments inaccessible and unavailable. As a result, it becomes crucial to swiftly ascertain the operational status and suitability of physical domains for the efficient allocation of tasks, ensuring the expeditious progression of disaster recovery measures.

A promising technology that plays a pivotal role in facilitating the visualization of complex ecosystems and the efficient orchestration of network services, resources, and computational tasks is the NDT [4]. By creating a virtual counterpart of a physical system and facilitating the transfer of tasks between domains, this technology capitalizes on the ability to assess system performance and make informed decisions, thereby serving as a pivotal driver for the advancement of 5G and future communication technologies.

Several works in the current scientific literature have defined architectures and platforms that employ drones to facilitate the communication between victims and rescuers [103]–[106]. At the same time, valuable works define DTs assisted task offloading strategies, formulated through complex optimization problems [107]–[110] or not providing a dynamic and prompt solution suitable for post-disaster and rescue operations [111], [112]. Indeed, this plethora of works is described in the following section and demonstrates that at the time of writing the paper [100], and to the best of the authors' knowledge, a lightweight approach for dynamically selecting network segments for network processing, leveraging the opportunities provided by DTs, was still missing.

To contribute to the expanding body of scientific literature, this study introduces a lightweight methodology for the dynamic selection of the most appropriate network domain, guided by availability and trust parameters, to facilitate the offloading of processing tasks from drone-captured videos.

Aligned with these principles, the proposed approach is structured in accordance with the ITU-T's IBN 2030 framework, originally outlined in ITU-T's publication [113] and further developed in [114]. Specifically, this approach leverages the concept of DTs to characterize network domains, addressing those segments impacted by natural disasters, which are unsuitable for task offloading, by substituting them with available network segments capable of in-network processing.

The methodology employed adopts a Multi Criteria Decision Making (MCDM) approach, specifically the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), a common tool for solving network selection problems in heterogeneous wireless networks. The dynamic selection process simultaneously evaluates the status, readiness, and trustworthiness parameters of the domains traversed by the drone to determine the most suitable network segment for processing, guided by the availability of resources and network reliability.

3.1.1 Related Works

Natural disasters, such as earthquakes, volcanic eruptions, and flooding, have the potential to lead to structural collapses, infrastructure deterioration, and substantial economic setbacks in the afflicted areas. Existing communication networks often struggle to adequately manage these unexpected occurrences, leading to a widespread disruption of mobile connectivity. To facilitate prompt rescue efforts, it becomes imperative to shift computationally intensive tasks to nearby robust network segments during post-disaster and rescue missions. As presented in Table 3.1, several studies within the scientific literature have been dedicated to addressing this challenge by exploring avenues to swiftly and effectively facilitate task offloading operations following natural disasters.

TABLE 3.1: Review of Related Works

Features	[115]	[106]	[103]	[116]	[117]	[105]	[108]	[109]	[110]	[111]	[112]	**This work**
UAV technology	✓	✓	✓	✓	✓	✓						✓
Rescue operations		✓	✓	✓	✓	✓				✓	✓	✓
Task offloading	✓		✓		✓		✓	✓	✓			✓
Dynamic selection				✓		✓	✓		✓			✓
Trust and Social attributes												✓
Digital-twin							✓	✓	✓	✓	✓	✓

On the one hand, extensive research works [103], [105], [106], [115]–[117] have been conducted on the applications of the UAV technology in natural disaster scenarios, and only a part of these [103], [115], [117] focuses on network processing task offloading. However, these studies highlight the difficulty of developing a strategy that takes into account the dynamic state of the system due to the heterogeneity of domains and the representation of their characteristics.

On the other hand, other studies [108]–[112] employ the DTs as a tool for data collection and modeling of the reference network domains. In particular, the authors of [108] and [112] explore the DTs as a useful tool for task offloading procedures in vehicular and urban scenarios. However, none of them fully exploit their potential in the context of natural disasters or incorporate a dynamic approach that addresses task offloading to assist in-network processing. Furthermore, to the best of the authors' knowledge, none of the valuable contributions mentioned above utilizes social attributes as support for selecting the suitable domain for network processing in order to increase the reliability of the offered service.

To further advance in this direction, the contribution outlined in this chapter presents an innovative strategy for selecting the most suitable domain for task offloading. This strategy utilizes a lightweight approach that harnesses the capabilities provided by DTs to represent the characteristics of diverse network segments. Moreover, it extends the ITU-T's IBN framework proposed in [113] by introducing a TMS that incorporates a trustworthiness parameter within the DTs. The trustworthiness evaluation between network segments, takes into account various factors, such as reputation and social relationships, as discussed in [82] and elaborated upon in subsection 2.1.4. This integration ensures a trust-based approach for in-network processing during task offloading.

3.2 The reference scenario and the proposed MCDM solution

The envisioned scenario delineates a standard multi-domain network characterized by multiple network segments capable of supporting the provision of end-to-end services. According to their specific capabilities and the sequence of tasks necessary to fulfill service requirements, including functions like storage and in-network processing, these inherently diverse domains are assigned responsibilities. These domains encompass a spectrum ranging from terrestrial networks to NTN, as well as integrated TN-NTN.

Furthermore, the framework entails the involvement of an UAV that spans the network segments traversing all the domains. Primarily, the UAV assumes the role of data acquisition in each domain crossed, capturing data such as videos of industrial and critical infrastructure. This data acquisition serves the purpose of evaluating, inspecting, and monitoring targets that are often challenging to access for maintenance or are completely inaccessible.

Secondly, the UAV can offload the acquired data to the suitable network segment to facilitate their processing. With this in mind, the captured videos can effectively support recovery operations in domains affected by natural disasters. They enable swift interventions and rescue operations while also avoiding the loss of in-network processing capacity in circumstances where network coverage and services are unavailable and unreachable.

Figure 3.1 illustrates the envisaged scenario along with the Integrated Broadband Network (IBN) architecture, expanding upon the solution put forth in [114] and the ITU-T specifications outlined in [113]. The assorted network segments are organized into network domains, which represent the physical infrastructure responsible for handling requests related to processing or storage services.

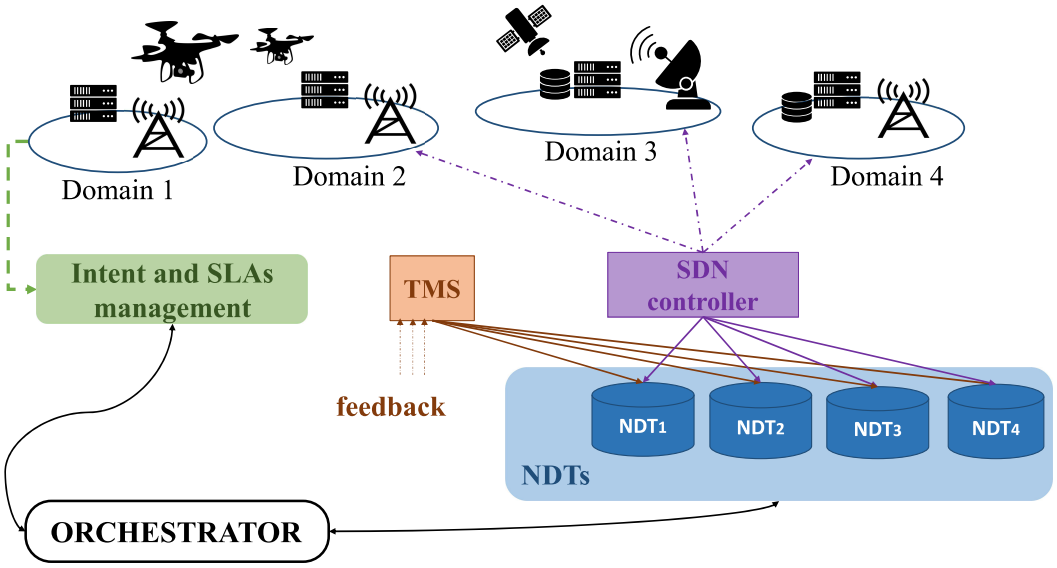


FIGURE 3.1: Reference scenario and IBN-based network architecture.

Within this framework, the end-to-end service requirements are conceptualized as an *intent*. This intent, in turn, necessitates a specific performance standard to facilitate the provision of a service. This performance standard is articulated through SLA, structured to ensure that network providers adhere to these objectives. In accordance with the ITU-T specification laid out in [113], intents undergo processing and translation, resulting in a set of actions and policies that are subsequently executed by the intent and SLA management module.

In this context, where the network segments exhibit inherent diversity and constantly changing states, the utilization of DTs becomes instrumental in representing the characteristics and capabilities of these domains. This utilization facilitates network monitoring operations and the prediction of maintenance requirements. Serving as abstractions of physical entities, DTs contribute to the process of selecting the most appropriate domain for in-network processing by scrutinizing the extracted features.

To effectively manage the abstraction of network resources, a SDN controller is responsible for populating and continually updating the performance indicators of DTs through relevant APIs and modeling languages such as Yet Another Next Generation (YANG)-CBOR, OMA lightweight M2M, and Digital Twin Definition Language (DTDL). This programmable controller not only supports the configuration of network functionalities but also plays a crucial role in the implementation of intents.

Furthermore, for the evaluation and acquisition of the trustworthiness attribute, the TMS module conducts an assessment of the network segments by examining their historical performance. More precisely, it employs an automated mechanism founded on feedback assessment to derive the trust parameter, which in turn establishes the reputation of each engaged network segment. This value undergoes periodic updates following the completion of each end-to-end service, thereby bolstering the overall network reliability for subsequent intents by identifying trustworthy network segments suitable for in-network processing.

Above and beyond the modules mentioned earlier, the orchestrator assumes a pivotal role in the holistic management of the multi-domain network architecture, responsible for both service and network orchestration functions. For each service demands, it conducts an assessment of the attributes within NDTs to pinpoint the network segment most suited to support the given service. Subsequently, the orchestrator proceeds to task allocation, intent deployment, and the vigilant monitoring of compliance with SLA, service models, and descriptions. The algorithm employed to determine the most appropriate domain for in-network processing, which is integrated into the orchestrator, is elaborated upon in subsection 3.2.2

3.2.1 Network Digital Twins parameters

The core purpose of the NDT is to construct a network model that mirrors the performance indicators of the physical network. This method empowers the management of metrics and characteristics via an abstracted representation of the real-world network state. Leveraging this potent instrument, the orchestrator gains the capability to oversee network segments comprehensively, thereby comprehending and mitigating service disruptions and contributing to the realization of intents.

Within this framework, the digital portrayal of network segments is harnessed to identify the most fitting domain for task offloading and in-network processing. The

objective is to achieve the optimal configuration that fulfills the predefined service requirements.

In order to create a NDT, the process entails the collection of a dataset containing pertinent network-related information. As a result, the devised approach entails the extraction of a set of performance indicators from each network segment, which pertain to the radio interface, network capabilities, and reliability. These specific performance indicators encompass parameters such as bandwidth, CPU performance, available RAM, storage capacity, and the level of trustworthiness.

1. Bandwidth: measured in [MHz], it assesses the minimum guaranteed value of available bandwidth for communication within the given network segment.

2. CPU: measured in [MHz], it indicates the processing capability of network resources in the domain.

3. RAM: measured in [KB], it represents the minimum guaranteed availability of RAM in the network segment.

4. Storage availability: measured in [GB], it calculates the available space for data storage in the domain.

5. Trustworthiness: it is a value ranging from 0 to 1, determined by the TMS, which represents the stated and proven reliability of a network segment. It is calculated as the product of two factors: the domain's reputation and the social tier between domains, as stated in chapter 2.

3.2.2 The conceived algorithm based on TOPSIS methodology

The conceived algorithm, employed to determine the suitable domain for in-network processing, is summarized in the pseudo-code reported in **Algorithm 1**.

It considers the limitations of the UAV such as its battery capacity while capturing videos during its flight. With these factors in mind, the process can calculate the count of domains the UAV can traverse before necessitating a battery recharge. Furthermore, if there is available storage capacity in the UAV, it has the ability to capture a video from the domains it crosses.

The proposed approach leverages the widely employed TOPSIS method, a common technique within MCDM utilized for resolving network selection problems within heterogeneous wireless networks. It identifies the ideal solution by selecting the network segment capable of offering a cost-effective QoS, gauged through the highest values in terms of CPU, RAM, available storage space, and trustworthiness among the monitored domains. Subsequently, the method quantifies the proximity of each network segment to this ideal solution by assessing a parameter referred to as Relative Closeness (RC).

Within this strategy, an assumption is made that the UAV spends approximately 10 minutes in each network segment, traversing domains with distances spanning from 500 meters to 1 kilometer, at variable speeds ranging from 3 kilometers per hour to 6 kilometers per hour. As a result, the parameters of the DTs are updated at 10-minute intervals.

Algorithm 1 Pseudo code of the conceived decision-making algorithm

```
for Every domain do
    check_UAV_capacity()
    n ← n_traversable_domains()
    offloading_options ← TOPSIS(n)
    if !offloading_options then
        domain ← domain + 1
        update_time()
    else
        d ← domain_bw_avail(offloading_options)
        if decision = d and id = d then
            0 ← capacity_UAV                          ▷ Data offload
            domain ← domain + 1
            update_time()
        else
            domain ← domain + 1
            update_time()
        end if
    end if
end for
```

Considering all the traversable domains, the implemented TOPSIS function constructs a decision matrix. Each row of the decision matrix represents a domain described by its features, including CPU, RAM, free storage space and trustworthiness. Additionally, the decision function calculates the ideal solution and assigns an RC value to each potential target domain. The calculated solutions are then ranked in descending order based on their RC values. All the domains below an empirically evaluated RC threshold are not considered for the selection. Subsequently, a communication bandwidth check is performed to verify if data can be offloaded while the UAV passes through that domain. The final domain selection is based on the following reasons:

1. The domain allows data offloading, considering the available bandwidth.
2. The domain is considered optimal and trustworthy for data offloading, based on the RC value.
3. The domain satisfies the energy and data capacity constraints.

In cases where data offloading options are unavailable, the UAV will recharge its battery as needed and then proceed to the next network segment. This entire sequence will be reiterated after data acquisition in the subsequent traversed domain. Should the chosen domain no longer align with the ideal solution computed earlier, it undergoes an update. This ensures a dynamic decision-making process that responds promptly to substantial shifts in the network's condition. In fact, in the event of a natural disaster, the framework modules responsible for digitally representing the network will detect and report this occurrence. As a result, features representing a disrupted domain will exhibit notable anomalies, serving as an indicator of a possible disaster and prompting a reevaluation of the selection of an appropriate offloading domain.

3.3 Performance Evaluation

The performance of the proposed approach is investigated through computer simulations. A MATLAB script is used to model the DTs representation of domains crossed by UAV and implement the conceived decision-making algorithm detailed in subsection 3.2.2.

The scenario under analysis encompasses eight distinct domains, each characterized by fluctuating parameters including CPU, RAM, available storage space, and trustworthiness, which experience variations over the course of the day. These values are subject to updates at 10-minute intervals, mirroring the duration that the drone spends within each domain.

The UAV utilized in this context possesses a storage capacity of 650 MB. While transiting between domains, it captures a 130 MB video of the designated target for monitoring purposes. As the drone navigates through network segments, the orchestrator executes the devised algorithm, taking into consideration both the drone's storage capacity and its battery status. Regarding the battery, its behavior is modeled to align with the energy consumption patterns documented in [118].

Figure 3.2 and Figure 3.3 illustrate an example of the dynamic domain selection. During the time slot spanning from 00:00 to 00:10, the drone traverses domain 1. Following an assessment of the feasible domains within the drone's battery lifespan, the orchestrator employs the implemented algorithm to designate domain 4 as the most suitable for task offloading. This selection is determined by the executed TOPSIS function, which evaluates pertinent features extracted via the representation of DTs. Domain 4 is chosen due to its favorable performance indicators, including sufficient CPU, RAM, and trustworthiness levels, as depicted in Figure 3.2.

From 00:10 to 00:20, the drone crosses into domain 2. The application of the TOPSIS function reaffirms that domain 4 remains the optimal choice for data offloading and in-network processing.

In the third phase, precisely at 00:20, a disruption occurs in domain 4 while the drone is traversing domain 3. Anomalies become evident in the representation of features via DTs, prompting the TOPSIS function to recalculate the selection of the appropriate domain. In this instance, domain 6 is designated as the closest to the ideal solution.

Finally, within the time frame of 00:50 to 01:00, the drone navigates through domain 6 and successfully concludes the data offloading process for in-network processing.

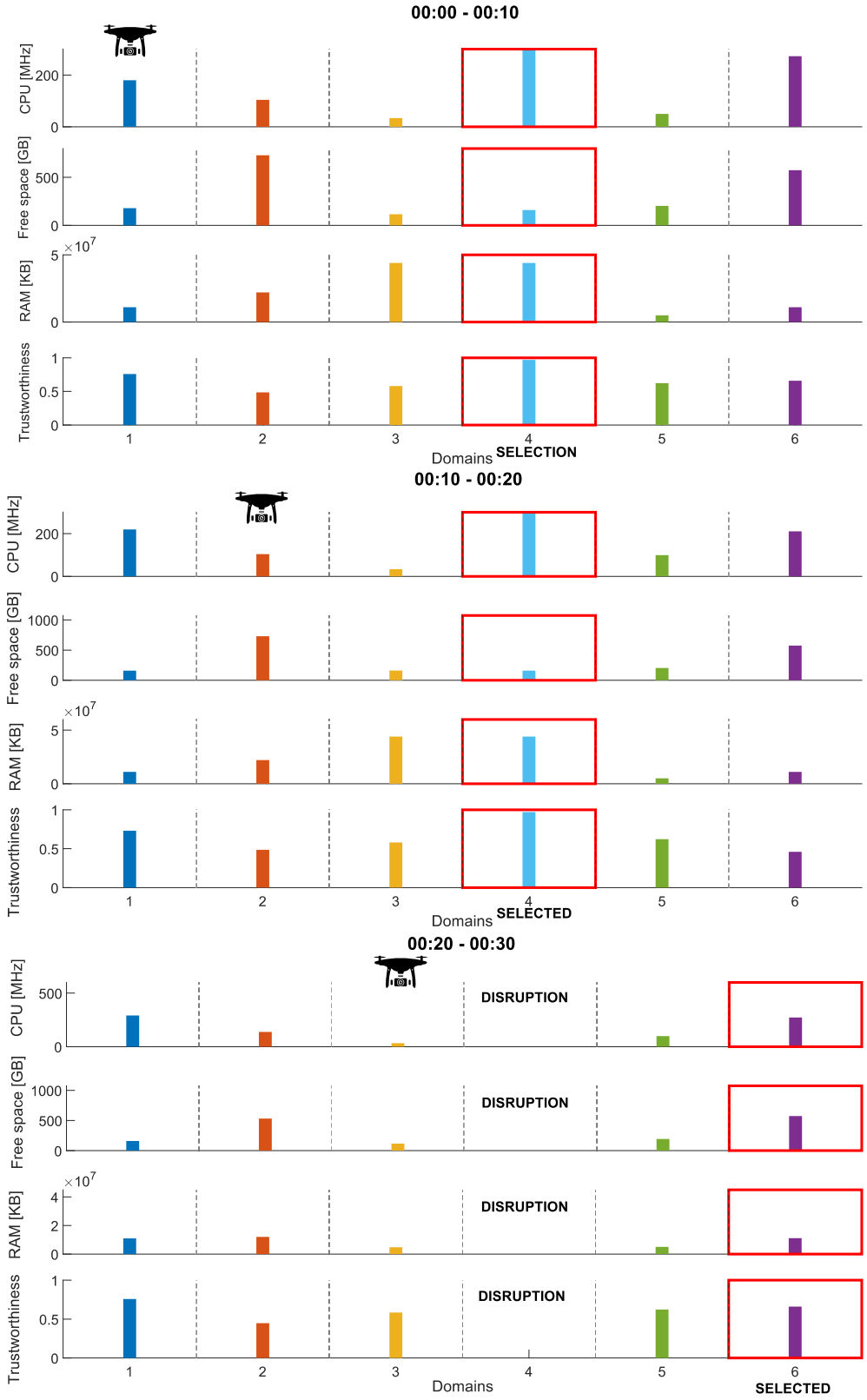


FIGURE 3.2: Overview of the drone flight and domain selection.

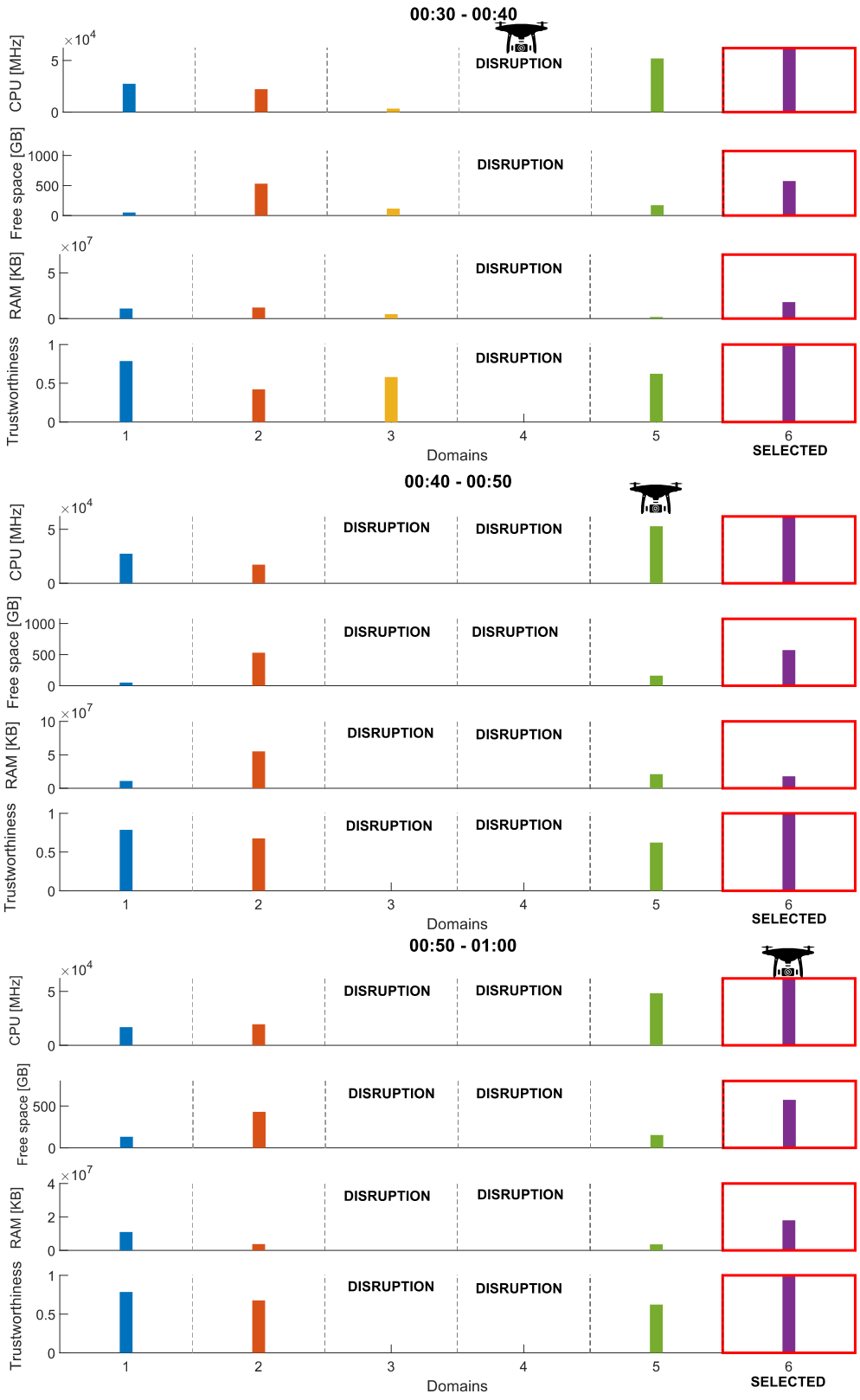


FIGURE 3.3: Overview of the drone flight and domain selection.

3.3.1 Simulation Results

To evaluate the performance of the devised approach, a comparison is made with two baseline methods. In the first baseline approach, data offloading and processing take place in a randomly selected network segment, and the outcomes are averaged over 15 different seeds. The second baseline approach involves the orchestrator implementing the selection algorithm in a deterministic manner, specifically when the drone's storage capacity is completely full.

Figure 3.4 shows the performance of the proposed approach against baseline solutions. The considered key performance indicators for the evaluation are:

- the amount of offloaded data;
- the number of domains in which the drone misses video acquisitions since it has not found opportunities to offload the stored data and, consequently, it has no more available space;
- the overall processing availability, assessed by measuring the ratio of offloaded data to the total amount of data acquired by the drone, expressed as a percentage.

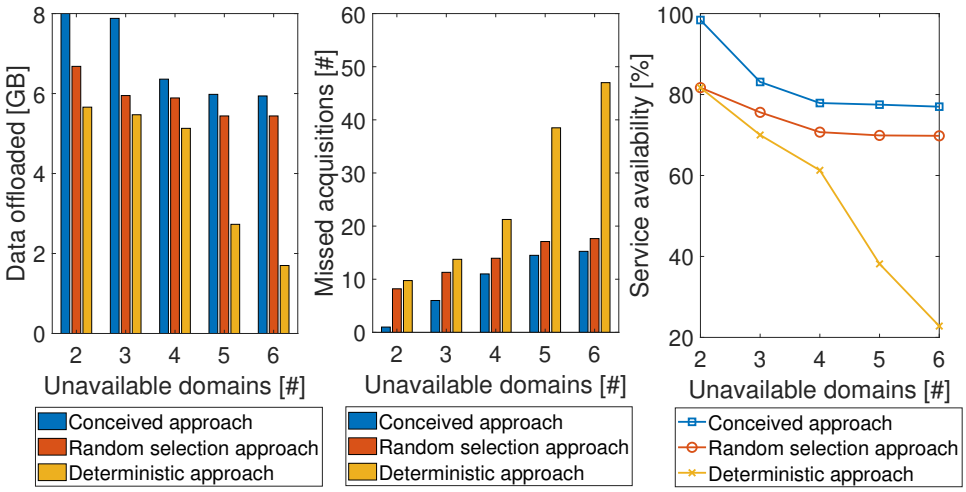


FIGURE 3.4: Offloaded data, missed acquisitions and overall service availability for CPU SLA focus.

Additionally, Figure 3.4 illustrates a specific use case that involves an SLA demanding a high level of CPU performance.

The graphs depict the progression of the three methods while varying the number of unavailable domains due to disruptions, which ranges from 2 to 6. In terms of data offloaded, the proposed approach consistently outperforms the other methods across all scenarios with unavailable domains. For instance, when 3 domains are unavailable, it allows for the offloading of up to 2.41 GB more data compared to the random selection approach, and up to 4.24 GB more data compared to the deterministic approach when 6 domains are unavailable. When considering the number of missed video acquisitions, the proposed approach permits missing up to 9 fewer domains compared to the random selection approach when 2 domains are unavailable,

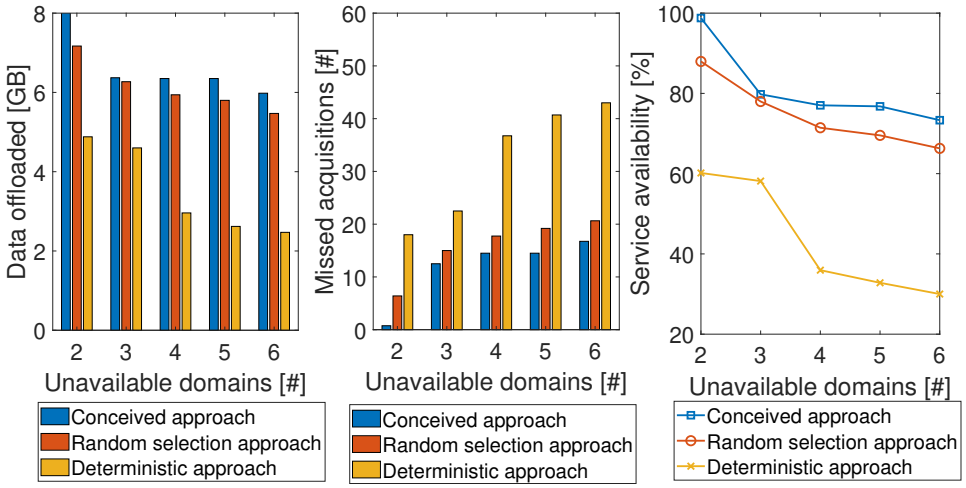


FIGURE 3.5: Offloaded data, missed acquisitions and overall service availability for trustworthiness SLA focus.

and up to 32 fewer domains compared to the deterministic approach when 6 domains are unavailable. Overall, this approach achieves a significantly higher service availability for network processing, with up to 28.61% more improvement compared to the random selection approach and up to 75.61% more improvement compared to the deterministic one.

On the other hand, Figure 3.5 presents the same performance assessments while taking into account SLA requirements that demand a high level of trustworthiness. The differences in data offloaded remain relatively consistent, with an increase of up to 3.51 GB more data offloaded when 6 domains are unavailable, compared to the deterministic approach, and up to 0.93 GB more data offloaded when 2 domains are unavailable when compared to the random selection approach. Additionally, the number of missed video acquisitions is reduced by up to 6 domains compared to the random selection approach when 2 domains are unavailable and by up to 27 domains compared to the deterministic approach when 6 domains are unavailable. Lastly, the proposed approach achieves a higher availability for providing in-network processing, with an improvement of up to 32.38% more compared to the random selection approach and up to 68.78% more compared to the deterministic approach

The greater volume of data offloaded, the reduced number of missed video acquisitions, and the overall enhanced service availability collectively affirm the appropriateness of the devised approach as the most suitable solution for ensuring the survival of in-network processing during natural disasters.

Chapter 4

A Markov Chain Analytical Model Supporting Service Provisioning and Network Design in the Social Internet of Everything

4.1 Introduction

The concept of the Internet of Everything (IoE) builds upon the foundation of the IoT, which brings together interconnected smart objects, people, processes, and data. This union of entities creates new opportunities and economic potential [119]. The IoE is founded on intricate connections and interactions involving diverse technologies, devices, and stakeholders [120].

In this context, the need for a network structure that promotes resource sharing and service provision is paramount. Social networking presents a valuable solution, as it encourages collaboration and interactivity [75]. When social networking capabilities are integrated into the IoE, it gives rise to the concept of the SIoE, which has significant potential for impact in various domains, including healthcare [121], the Internet of Vehicles [122], and smart cities [123], [124]. Furthermore, the adoption of social skills can facilitate access to information and services from anywhere at any time, thereby enhancing network resource visibility and service discovery [76]. Consequently, the representation of social connections in a virtual world significantly improves network scalability and navigability, enabling stakeholders to assess reputation and provide more reliable service provisioning [125].

However, the ubiquity of devices intruding into individuals' most private spheres raises complex challenges that researchers find difficult to resolve [126]. The prompt and successful accomplishment of services is significantly influenced by the availability of service providers and their limited resources. Moreover, selecting the most suitable service provider requires consideration of their level of trustworthiness, characterized by various aspects that must be considered together, such as their friendship ties with other entities [127] and their reputation based on past experiences [87].

Complicating matters further is the non-deterministic nature of such a SIoE system's behavior. In a SIoE network, the service demand, as well as the availability and trustworthiness of service providers, exhibit stochastic characteristics. As a result, modeling this unpredictable behavior becomes crucial for evaluating the process of selecting a trusted service provider. Consequently, the development of a stochastic

analytical model becomes essential to design efficient resource selection algorithms for ensuring the availability of trusted service providers in SIoE networks.

It is worth noting that many works in the literature explore trust management in the service provisioning process within the context of Social Networks and the IoE [87], [128]–[133]. However, to the best of the authors' knowledge, some of these models would necessitate continuous and computationally intensive efforts to trace the long-term evolution of the service provisioning process [129], while others may struggle to handle high-volume traffic [134].

To address these limitations, this Chapter introduces a stochastic model that efficiently captures the long-term evolution of the overall service provisioning process within a SIoE environment. The proposed model is based on a Markov chain, which analyzes provider selection in SIoE networks, taking into account the trust level and resource capabilities of available providers. This approach allows for the tracking of the evolution of each SIoE entity's reputation, thereby evaluating the entire SIoE network's ability to successfully complete a service while excluding malicious nodes from the provider selection process.

Given the considerations above, the main contributions of this study are summarized as follows.

1. A stochastic analytical model is designed to assess the state of a generic service provider in SIoE environments. To achieve this, a multidimensional Markov chain is employed [135]. This chain captures the service provider's behavior, which depends on its reputation and available resources in relation to what is required for service completion.

2. The behavior of entities is estimated to promptly detect and exclude malicious entities from the Social Network, thereby ensuring system responsiveness and obviating the need for extensive computational efforts in managing the trustworthiness of the SIoE system.

3. The analytical model is validated by comparing various performance metrics with the results obtained from extensive simulations, confirming its effectiveness and applicability in complex SIoE scenarios.

4. By assessing available resources, the proposed model is leveraged to appropriately design the SIoE network structure to accommodate different request loads.

4.2 Background, goals, and reference SIoE scenario

The integration of social networking with IoT solutions has been extensively explored in academic research, as discussed in chapter 2. This concept holds the promise of enhancing networking services and engendering novel IoT applications. In the early proposals, such as those found in [75], the primary focus was on introducing social-like capabilities to IoT objects with the aim of augmenting trust among interconnected objects. Social networking also has the potential to enhance network navigability within extensive IoE environments. Parameters of paramount importance

include trustworthiness and resource availability, which necessitate thorough investigation. Researchers have put forth various strategies, methodologies, and mathematical models for the assessment of trust management and entity recommendations in Social Networks and/or conventional IoT settings.

The paper [128] introduces a distributed trust model based on the Markov chain to address security risks in the realm of IoT. Its primary goal is to adapt an existing trust model designed for Vehicular Ad hoc Networks (VANETs) to the context of IoT. This model involves groups of neighboring nodes that monitor the behavior of a specific IoT node and employ an estimation algorithm to filter out malicious spam.

In the work presented in [129], a Lightweight Hidden Markov Model is proposed for evaluating trust in IoT networks. This scheme encompasses a 2-state Markov Model with Trusted and Compromised states. State transitions are determined based on metrics such as the number of forwarded, dropped, modified, and received packets, and the forward likelihood function is used to assess the trustworthiness of nodes.

The authors of [87] introduce a trust model for SIoT that combines social trust theory with the unique characteristics of IoT devices. This model takes into account competence, willingness, and social relationships to enhance service efficiency and security within SIoT.

Trust management encounters challenges when dealing with anonymous nodes and inaccurate communication. To address this, a potential solution for managing a large number of nodes is to predict trust and distrust values. In [130], the authors propose a dynamic trust model that computes direct and indirect trust, with a focus on trust prediction. This approach combines exponential smoothing and a Markov chain to predict trustworthiness.

A time-aware smart object recommendation model is presented in [131]. This model arises from the need to provide a recommendation system that assists users in locating the smart objects they require. Traditional recommendation techniques often rely on user ratings or feedback, which can be challenging to collect.

The paper [132] introduces a framework for creating, managing, controlling, and monitoring SIoT objects in real-time. This framework enables the virtual representation of real-world objects as virtual objects, which can be combined to create new services. The paper also evaluates the selection of virtual objects in the service provisioning process to assess resource consumption and latency.

The contribution in [133] discusses a collaboration scenario within the SIoT environment to address challenges such as managing complex relationships and conserving energy resources. This scenario takes into account object attributes, friend functions, and intelligent friend selection to optimize group messaging, with the aim of enhancing communication reliability and improving service discovery efficiency in SIoT networks.

4.2.1 Open issues covered by this contribution

While traditional methods have historically been employed to secure networks, trust-based schemes have emerged as viable solutions to address attacks by malicious entities in IoE environments. This shift is due to their lower code size and reduced processing time demands, as highlighted by [129]. However, to the best of our knowledge, developing a statistical model that comprehensively captures the steady-state

reputational behavior of a SIoE network while accounting for friendship relationships and the available resources of nodes providing services remains a challenging endeavor.

Indeed, while various trust-based schemes have been proposed in recent literature (as the works published in [82] and [83] and reported in chapter 2), many of them impose significant computational and memory requirements for the same evaluation, potentially undermining network integrity and control. In light of these challenges, the contribution proposed in this Chapter seeks to extend the scientific literature by introducing a Markov-based model for the statistical analysis of service provider trustworthiness within a SIoE network. The model presented in this paper can effectively trace the evolution of the overall service provisioning process. Unlike most prominent proposals in the current literature, it takes a holistic approach by jointly considering both the reputation and available resources of the service providers registered on the network. Consequently, this model can be productively utilized to design and assess the capabilities of a SIoE network in delivering trusted services while maintaining lost service requests within predefined thresholds.

4.2.2 Background on SIoE scenario

This chapter introduces a network architecture based on SIoE, as illustrated in Figure 4.1. Unlike a conventional IoT architecture, which primarily comprises IoT devices, as depicted in Figure 2.1, the SIoE network consists of diverse *social entities*. These entities encompass a wide range of elements, including people, physical devices (such as sensors, vehicles, and smartphones), software, processes, and data. They have the capacity to interact, share data and content, collaborate on various tasks, and provide or execute services. The social entities are geographically distributed across different clusters.

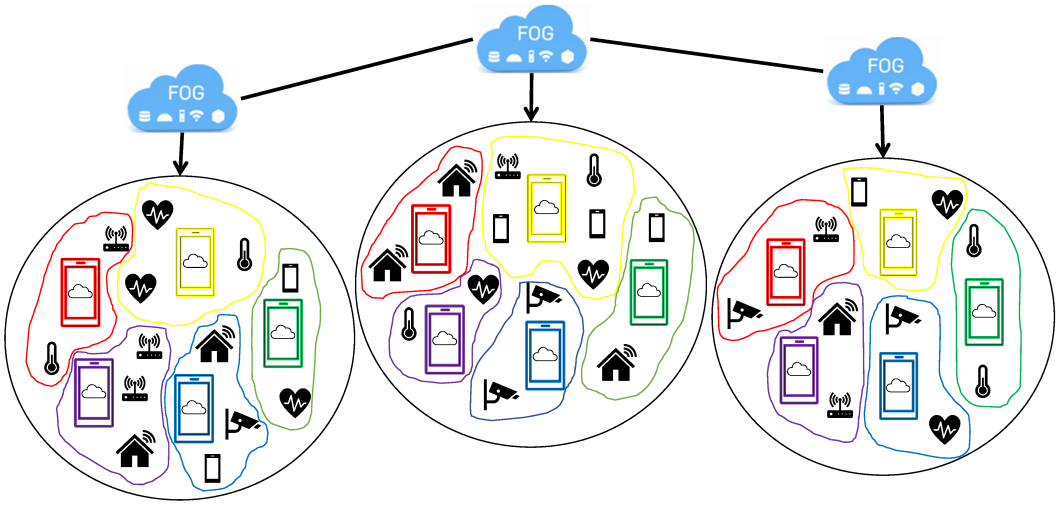


FIGURE 4.1: The SIoE reference environment.

Through their digital representations in the Social Network, they have the opportunity to exhibit their attributes and features. This interaction results in the formation

of social relationships that reflect the level of confidence shared among the participating entities, facilitating the identification of trusted subjects capable of fulfilling specific requests [84].

The SIoE entities registered on the Social Network can function as both service requesters and service providers. Service providers share their resources and communicate their availability to offer particular services, while service requesters express their need for specific services to the Social Network. Each social object specifies a list of services it can provide, enabling social entities to join *service communities* based on their shared application context and the services they can offer, thus enhancing network navigability.

Each abstracted service community is managed by fog nodes, which create a virtual topology for each service community. These fog nodes utilize stored information about entities' past experiences and the complete set of attributes of registered social entities to operate the TMS. The TMS employs automated mechanisms to manage and calculate parameters related to trust values. The selection of an appropriate trust metric is crucial for social entities to make well-informed decisions when choosing a service provider.

The overall system is supervised by upper-level fog nodes equipped with larger storage capacities, which enables proper synchronization among the structures of the distributed clusters through mutual interaction.

4.2.3 Trust Management Procedure

The adopted Trust Management strategy extends its scope beyond just reliability and security. It incorporates considerations of service trustworthiness and resource consumption assessment, following the same approach presented in subsection 2.1.3 and subsection 2.2.2. Figure 4.2 illustrates the service provisioning procedure, wherein a social entity sends a service request to the nearest fog node running the TMS. The TMS then establishes a *trust ranking* of potential service providers and selects the most suitable one for service execution. This process helps in identifying potential malicious social entities by excluding service providers who fall below a configured trust threshold during provider selection.

According to our recent, albeit preliminary, published conference papers [82], [83], the trustworthiness level of the j-th service provider is feedback-dependent, driven by past interactions between entities and the collection of information about the provision of requested services. The Trust value Tr_{ij} is determined by two primary factors when considering the i-th social entity requesting a service and the j-th social object as a potential provider.

The first factor is the Sociality factor S_{ij}, reflecting the level of friendship between social objects. The rates of established relationships are categorized by their importance [77]. The second factor is the Reputation Factor R_j, which is influenced by the feedback received from other social entities. The Reputation Factor takes into account the history of social entities' past actions.

The Trust value is ultimately calculated as the product of these two factors: $Tr_{ij} = S_{ij} \cdot R_j$, as detailed in [82]. It's worth noting that in the procedure described in this Chapter, the Reputation factor is not considered as a linear combination of

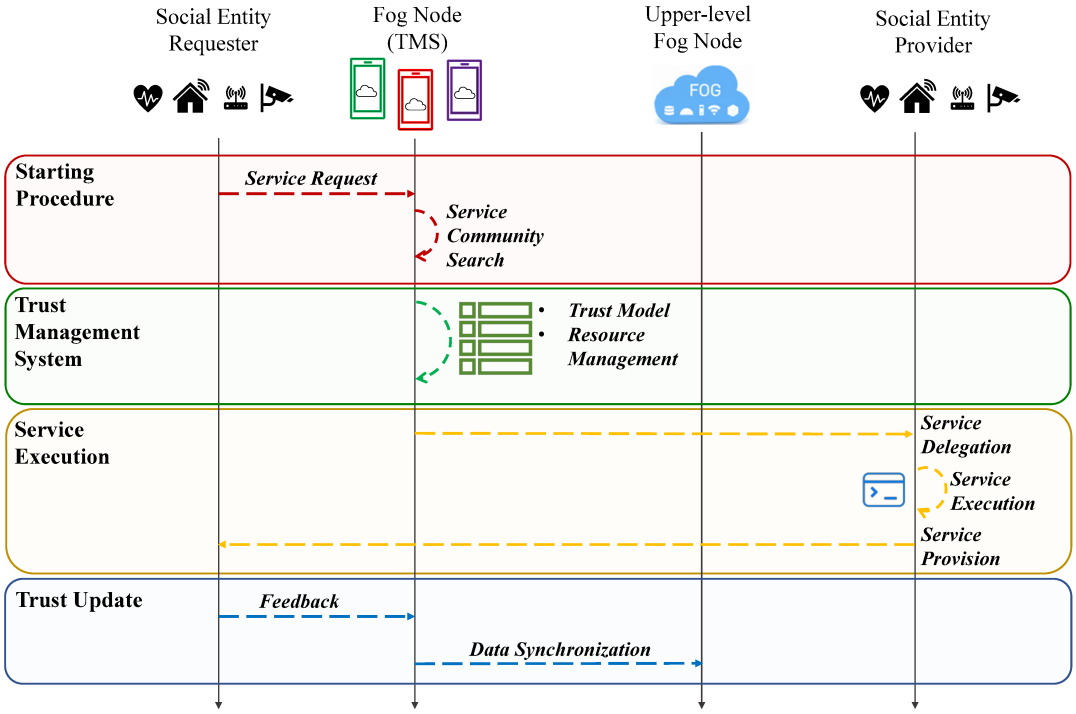


FIGURE 4.2: The designed Trust Management System procedure.

the three different contributions, as reported in the eq.2.5, described in the subsection 2.2.2, without distinguishing different weights for the evaluations received by entities. In light of this, from this point onward in the discussion, the Reputation factor parameter is referred to as Δ_j, indicating that the contributions considered are the direct feedback received by the service provider (as explained in the subsection 2.1.4).

Furthermore, the TMS assesses the resource capability of social objects to prevent service execution failures resulting from lack of resources. This aspect is particularly crucial in environments where network participants have limited resources. Fog nodes managing the service community monitor the resources required by social objects for service execution. Following the ranking computation, the resource capacity of the candidate provider is verified to ensure the availability of the social object for service execution. If this check fails, the candidate provider is temporarily removed from the list, and the ranking is updated. The fog node interfaces with the upper-level fog node, which maintains a distributed database containing information on social entities' relationships and reputations, facilitating synchronization between different clusters. Finally, the service requester provides feedback to the system for provider evaluation, assigning a value of 1 for completed services and 0 for incomplete services. This feedback is stored for subsequent evaluations in the fog node.

4.3 Modelling a social entity through Markov Theory

A novel Markov chain model is formulated to evaluate the behavior of an entity in an SIoE environment. As is well-known, a Markov chain is a memory-less stochastic process in which the probability of transitioning from one state to another depends solely on the current state. The proposed Markov chain assesses trust and resources

in relation to a single social entity and the services it can offer. The evaluation can be easily extended to the entire Social Network by considering an independent Markov chain for each involved entity.

Regarding the j-th entity in the Social Network, the state comprises a triad of values: k_j, representing the number of positive feedback received in the past; T_j, specifying the number of services offered; and n_j, indicating the number of resources currently employed to provide a service assigned to the j-th social entity. The inclusion of this last parameter in the triad acknowledges the heterogeneous nature of entities, as they offer different resources and computational capacities. For instance, according to a classification documented in [97], smart IoE devices can be grouped into several classes, including Low-end IoE devices with limited resources (e.g., the Open Mote); Middle-end IoE devices, offering more features and better processing capabilities than Low-end IoE devices (e.g., the Arduino); and High-end IoE devices, with ample resources and storage capacity (e.g., smartphones). To account for these differences, the proposed model assigns different values of maximum allocable resources (represented by N_j) to each social entity based on its capabilities, which are determined by its class. Table 4.1 summarizes the main symbols used to describe the model, along with their meanings.

TABLE 4.1: Main Symbols Description.

Symbol	Meaning
Tr_{ij}	Trust level of i towards the entity j
S_{ij}	Sociality factor measuring the friendship ties between i and j
Δ_j	Reputation factor of the entity j
$\gamma_{A\to B}$	Transition rate from the state A to the state B
λ	Average number of service requests per unit of time
μ	Average number of requesters served per unit of time
λ_j	Average number of service requests assigned to the entity j
$1/\mu_j$	Average service rate employed by the entity j to perform a service
$P(R_{i\to j})$	Probability that a service request from i is assigned to provider j
N	Number of social entities belonging a service community
N_j	Maximum number of allocable resources of the j-th social entity
τ	Number of entities owning a Trust value with i greater than Tr_{ij}
$P_a^n(\delta)$	Probability of n arrival in δ
$P_s^n(\delta)$	Probability of n task accomplished in δ
P_{nf}	Probability to receive a negative feedback
P_{pf}	Probability to receive a positive feedback
Ψ_i	Set of friends of the requester entity i
Ψ_j	Set of friends of the provider entity j
$P_B(j)$	Blocking probability of the j-th service provider
F_j	Friends of the j-th social entity
α	Reputation Loss Percentage

Given the state (k_j, T_j, n_j), Figure 4.3 depicts the graph related to the sequence of states in the Markov chain, representing the behavior of a social entity. In this graph, the edges are labeled with transition rates from one state to another. Without loss

of generality, we assume that service requests are generated according to a Poisson distribution with a rate parameter λ. Additionally, both the inter-arrival times and service times are considered statistically independent.

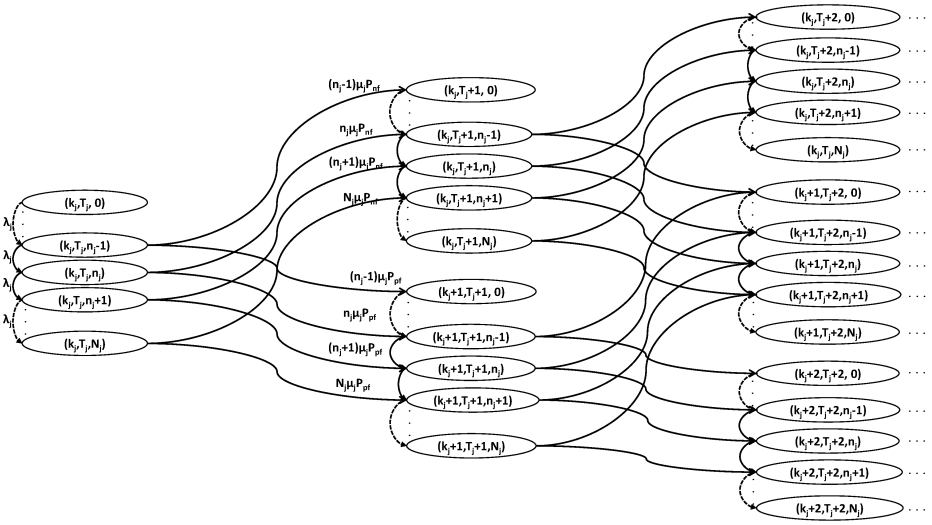


FIGURE 4.3: State Diagram of the proposed model.

4.3.1 Average number of service requests assigned to a social entity

Let (k_j, T_j, n_j) be the triad representing the current state of the j-th social entity, and let Ψ_j be the set of social entities having a social relationship with it. Assuming that the i-th social entity belongs to the set of friends of j (that is, Ψ_j), λ_j represents the average number of service requests assigned to the j-th social entity. It depends on the Trust values and the resource availability needed to allow the j-th social entity to perform the services successfully. λ_j can be calculated as the sum of all the requests made by the i-th requester assigned to j, multiplied by the probability $P(R_{i\to j})$ that the TMS selects the j-th social entity as the most suitable provider:

$$\lambda_j = \sum_{i=1, i\neq j}^{\Psi_j} \lambda_{ij} \cdot P(R_{i\to j}|(k_j, T_j, n_j)), \tag{4.1}$$

where λ_{ij} is the average number of service requests coming from the i-th social entity and assigned to the j-th social entity. It is noteworthy that the probability $P(R_{i\to j}|(k_j, T_j, n_j))$ is conditioned to the current state (k_j, T_j, n_j) because it depends on the trust value and the resource availability of j.

Let Ψ_i be the set of entities having a social relationship with the i-th social entity, and let τ represent the number of social entities more trusted than the j-th entity for the i-th requester. To formulate the probability that a request coming from i is assigned to j, the Total Probability Law is applied to all possible values of τ and is reported in the following equation:

$$\lambda_j = \sum_{i=1, i\neq j}^{\Psi_j} \lambda_{ij} \sum_{\psi=0}^{\Psi_i - 1} P(R_{i\to j} | (k_j, T_j, n_j), \tau = \psi). \tag{4.2}$$

In the interest of clarity, the mathematical steps for developing the eq.4.2 will be relegated to the Appendix A.

According to subsection 4.3.1, the average number of service requests assigned to a social entity, denoted as λ_j, significantly influences each state transition because the variation of the triad representing each state affects the choice of the suitable service provider for the next request. The value of λ_j depends on the comparison of trust values characterizing all available service providers at the time when the service request arrives, due to the Trust model's TMS algorithm. Thus, the proposed methodology investigates the probability of service requests being assigned to the j-th social entity by verifying if the considered entity is the available trusted one, as presented in subsection 4.2.3.

In the Appendix A, λ_j is evaluated by assuming knowledge of the state of a single entity, i.e., the j-th social entity analyzed by the Markov chain. Therefore, only the triad (k_j, T_j, n_j) is known, and there is no information about the parameters defining the state of the other entities, i.e., the ψ_m-th social entity..

Due to the excessive complexity of evaluating a multidimensional Markov chain that simultaneously considers the analytical development of N entities, for the sake of simplicity and without loss of generality, the triad representing the state of any other ψ_n-th social entity is approximated by exploiting a proportionality criterion. This criterion allows the evaluation of the total number of feedback received from a generic social entity. If two social entities behave similarly, they will, on average, receive a comparable number of total feedback. Meanwhile, if two social entities behave differently, the average number of received feedback can be evaluated through Lemma 1.

Lemma 1. Given (k_j, T_j, n_j) as the state of the j-th social entity, and let P_{pf_j} be the probability that the j-th entity receives positive feedback, and F_j be the number of its friends. Moreover, let $P_{pf_{\psi_m}}$ be the probability that the ψ_m-th entity (whose state information is not known) receives positive feedback, and F_{ψ_m} be the number of its friends. Assuming R_N is the total number of requested services assigned in the Social Network, the number of averaged received feedback T_{ψ_m} can be evaluated as:

$$T_{\psi_m} = \frac{T_j \cdot P_{pf_{\psi_m}} \cdot F_{\psi_m}}{P_{pf_j} \cdot F_j} \tag{4.3}$$

Proof. Considering the total number of social entities N that can provide a specified service, the whole set of provided requests related to that service, denoted as R_N, can be expressed as the sum of the total feedback assigned to each provider: $R_N = T_1 + T_2 + ... + T_j + T_{\psi_m} + ... + T_N$. Assuming a proportional distribution of the service requests based on the number of friends and the probability to receive positive feedback, the value T_j representing the state of the j-th entity can be expressed as:

$$T_j = \frac{R_N \cdot P_{pf_j} \cdot F_j}{\sum_{n=1}^{N} P_{pf_n} \cdot F_n} \tag{4.4}$$

Therefore, in the same manner, it is possible to calculate T_{ψ_m} referring to the generic ψ_m-th social entity, that is:

$$T_{\psi_m} = \frac{R_N \cdot P_{pf_{\psi_m}} \cdot F_{\psi_m}}{\sum_{n=1}^{N} P_{pf_n} \cdot F_n} \tag{4.5}$$

By obtaining R_N from eq.4.4 and replacing it into eq.4.5, the approximate T_{ψ_m} value reported in the eq.4.3 is obtained.

■

Definition 4.3.1. The rate λ_{ψ_m} represents the average number of services assigned to the ψ_m-th social entity. Similar to the definition of λ_j reported in subsection 4.3.1, it is strongly influenced by the comparison of the trust value of all the service providers and the resource availability needed to enable the ψ_m-th social entity to perform services.

Following the same principle used for the approximation of T_{ψ_m}, the evaluation of λ_{ψ_m} depends on the number of handled social relationships and the probability of receiving positive feedback for the ψm-th social entity. Therefore, by using the procedure outlined in Lemma 1, $\lambda\psi_m$ can be calculated as:

$$\lambda_{\psi_m} = \frac{\lambda_j \cdot P_{pf_{\psi_m}} \cdot F_{\psi_m}}{P_{pf_j} \cdot F_j}, \tag{4.6}$$

where, P_{pf_j} and $P_{pf_{\psi_m}}$ are the receiving positive feedback probabilities of the j-th and ψ_m-th entities, respectively. F_j and F_{ψ_m} are the friends of the j-th and ψ_m-th entities.

Definition 4.3.2. Let's now consider an interaction between the j-th service provider and the i-th service requester. The Trust value Tr_{ij} represents a qualitative parameter indicating the trustworthiness of provider j as perceived by service requester i. Given the state of the j-th service provider, specifically the triad (k_j, T_j, n_j), and the Sociality factor describing the friendship ties between the i-th and j-th social entities, denoted as S_{ij}, the Trust value Tr_{ij}, as designed in the Trust model detailed in subsection 4.2.3, can be expressed as: $Tr_{ij} = S_{ij} \cdot \Delta_j$, where $\Delta_j = \frac{k_j}{T_j}$ represents the Reputation factor of entity j, describing the past evaluations received by the j-th service provider.

Definition 4.3.3. Let μ_j be the average service rate representing the number of requesters served per time period. Specifically, it represents the number of services accomplished by the j-th social entity and is calculated as the reciprocal of the service time to perform the requested service. Similar to the parameter n_j of the triad representing the state, the parameter μ_j can be defined as an attribute reflecting the capabilities of a social entity, according to the class division described before and

reported in [97]. Accordingly, the couple of values (N_j, μ_j), indicating respectively the maximum allocable resources and the average service rate, are considered fixed for each class of entity in the development of the model.

Now, given the definition of λ_j and μ_j, the following sections present the rates of state transitions for assigning a task to a social entity provider and receiving positive or negative feedback in response to a service provided.

4.3.2 States Transition Rates

Each state transition is event-driven. The conceived model considers the following three types of event: the task assignation to a social entity provider, the positive feedback reception in response to a service provided, and the negative feedback reception in response to a service provided. The state transition diagram of a generic node is depicted in Figure 4.4.

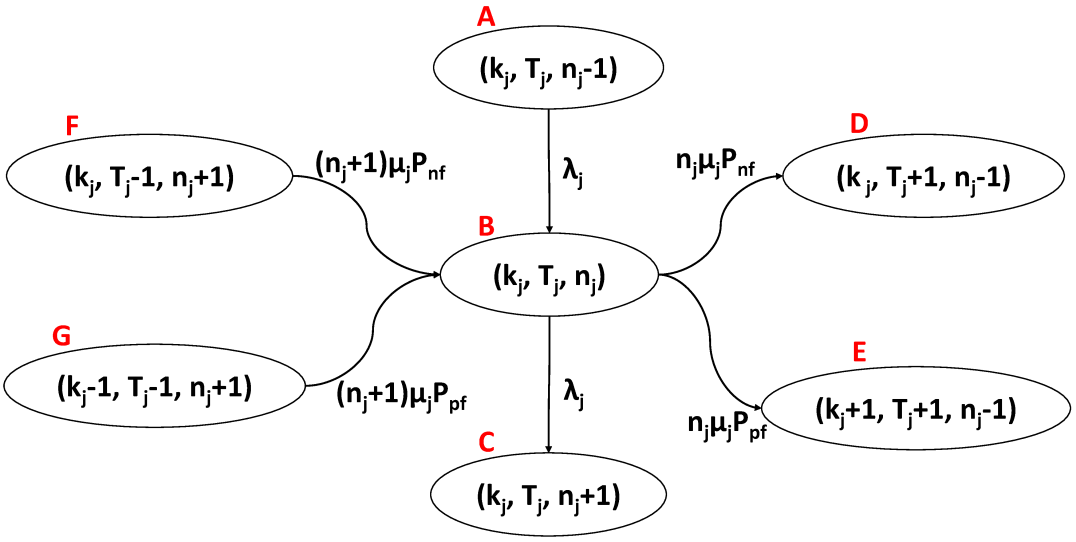


FIGURE 4.4: Transition rate diagram of a generic node of the graph.

Case 1: Task assignation to a social entity provider transition.

With reference to Figure 4.3, all the edges moving downward refer to the assignment of a service task to the evaluated j-th provider.

Theorem 1. *Let $(k_j, T_j, n_j - 1)$ be the generic state A of the j-th social entity. Given the maximum number of allocable resources for the considered entity, that is N_j, the probability of entering the state B (identified by the triad (k_j, T_j, n_j)) from the state A is denoted with $P_{A\to B}$. Indeed, the transition rate $\gamma_{A\to B}$ from the state A to the state B is:*

$$\gamma_{A\to B} = \gamma_{(k_j,T_j,n_j-1)\to(k_j,T_j,n_j)} = \begin{cases} 0 & if \quad n_j = N_j, \\ \lambda_j & if \quad n_j < N_j. \end{cases} \tag{4.7}$$

Proof. Considering the transition due to the assignation of a task, it will consequently result in the employment of an extra resource for the j-th entity. Accordingly, the arrival state turns out to be represented by the triad (k_j, T_j, n_j). However, if the parameter related to the currently allocated resources has reached its maximum value of N_j, the task cannot be assigned to the j-th entity and the transition can't occur. Therefore, the transition rate $\gamma_{A\to B}$, measuring the probability per unit of time that an event occurs (e.g., the state transition due to task assignment) within an infinitesimally time interval δ, can be defined as: $\gamma_{(k_j,T_j,n_j-1)\to(k_j,T_j,n_j)} = \lim_{\delta\to 0} \frac{P_{A\to B}(\delta)}{\delta}$ if $n_j < N_j$ and equal to 0 if $n_j = N_j$.

Specifically, $\lim_{\delta\to 0} \frac{P_{A\to B}(\delta)}{\delta}$ represents the probability that 1 task assigned to the j-th entity, defined as $P_a^1(\delta)$, and 0 services are accomplished, defined as $P_s^0(\delta)$, in a time interval equal to δ. Assuming both the aforementioned assumptions are independent, the previous equation can be written as: $\lim_{\delta\to 0} \frac{P_a^1(\delta)\cdot P_s^0(\delta)}{\delta}$. Since inter-arrival and service times are assumed to be exponentially distributed, and the arrival and conditional service rates Poissonian, $P_a^1(\delta) = \lambda_j\delta \cdot e^{-\lambda_j\delta}$ and $P_s^0(\delta) = (e^{-\mu_j\delta})^{n_j-1}$. Therefore, the limit can be calculated as: $\lim_{\delta\to 0} \frac{\lambda_j\delta\cdot e^{-\lambda_j\delta}\cdot(e^{-\mu_j\delta})^{n_j-1}}{\delta} = \lambda_j$.

■

Corollary 1. Each state transition referring to the task assignment of a generic entity j can be calculated in the same manner and depends exclusively on λ_j.

Let (k_j, T_j, n_j) be the generic state B of the j-th social entity. Given the maximum number of allocable resources for the considered entity, that is N_j, the probability of entering the state C (identified by the triad (k_j, T_j, n_j+1)) from the state B is denoted with $P_{B\to C}$. Indeed, the transition rate $\gamma_{B\to C}$ from the state B to the state C is:

$$\gamma_{B\to C} = \gamma_{(k_j,T_j,n_j)\to(k_j,T_j,n_j+1)} = \begin{cases} 0 & if \quad n_j = N_j, \\ \lambda_j & if \quad n_j < N_j \end{cases} \tag{4.8}$$

Proof. Similar to equation 4.7, which represents the allocation of an additional resource for entity j, the arrival state is represented by the triad (k_j, T_j, n_j+1). Specifically, if $n_j < N_j$, $\gamma_{B\to C} = \gamma_{(k_j,T_j,n_j)\to(k_j,T_j,n_j+1)} = \lim_{\delta\to 0} \frac{P_{B\to C}(\delta)}{\delta}$.

In this context, the $\lim_{\delta\to 0} \frac{P_{B\to C}(\delta)}{\delta}$ represents the probability that 1 task is assigned to the j-th entity, defined as $P_a^1(\delta)$, and 0 services are accomplished, defined as $P_s^0(\delta)$, in a time interval equal to δ. Under the same assumption previously discussed for the Theorem 1, $\lim_{\delta\to 0} \frac{P_{B\to C}(\delta)}{\delta} = \lim_{\delta\to 0} \frac{P_a^1(\delta)\cdot P_s^0(\delta)}{\delta} = \lambda_j$.

■

Case 2: Negative feedback reception in response to a service provided.

With reference to Figure 4.3, all the edges progressing upward forward indicate the reception of negative feedback in response to successful service delivery.

Theorem 2. *Let (k_j, T_j, n_j) be the generic state B of the j-th social entity. Given the maximum number of allocable resources for the considered entity, that is N_j, the probability of entering the state D (identified by the triad $(k_j, T_j + 1, n_j - 1)$) from the state B is denoted with $P_{B\to D}$. Indeed, the transition rate $\gamma_{B\to D}$ from the state B to the state D is:*

$$\gamma_{B\to D} = \gamma_{(k_j,T_j,n_j)\to(k_j,T_j+1,n_j-1)} = \\ = \begin{cases} 0 & if \quad n_j = 0, \\ n_j \cdot \mu_j \cdot P_{nf} & if \quad 0 < n_j < N_j. \end{cases} \tag{4.9}$$

Proof. Considering the j-th entity in the state described by the triad (k_j, T_j, n_j), the accomplishment of a task will result in the reception of feedback. Assuming that the received feedback is negative, the value relating to the number of positive evaluations remains unchanged, while the number of total evaluations received increases. Also, completing the assigned task, the j-th social entity releases an employed resource. The arrival state, therefore, turns out to be $(k_j, T_j + 1, n_j - 1)$. However, if the parameter relating to the allocated resources is equal to 0 means that the entity j cannot performs any task and will not receive any feedback. The transition rate $\gamma_{B\to D}$, measuring the probability per unit of time that an event occurs (e.g., the state transition due to negative feedback reception) within an infinitesimally time interval δ, can be defined as: $\gamma_{(k_j,T_j,n_j)\to(k_j,T_j+1,n_j-1)} = \lim_{\delta\to 0} \frac{P_{B\to D}(\delta)}{\delta}$ if $0 < n_j < N_j$ and equal to 0 if $n_j = 0$.

More specifically, the $\lim_{\delta\to 0} \frac{P_{B\to D}(\delta)}{\delta}$ represents the probability that 0 tasks are assigned to the considered entity, defined as $P_a^0(\delta)$, and 1 service is accomplished within the reception of a negative feedback, defined as $P_s^1(\delta)$, in a time interval equal to δ. Assuming both the aforementioned assumptions are independent, the transition probability can be written as: $\lim_{\delta\to 0} \frac{P_a^0(\delta)\cdot P_s^1(\delta)\cdot P_{nf}}{\delta}$. Since inter-arrival and service times are assumed to be exponential, and the arrival and conditional service rates Poissonian, $P_a^0(\delta) = e^{-\lambda_j \delta}$ and $P_s^1(\delta) = n_j \cdot (1 - e^{-\mu_j \delta}) \cdot (e^{-\mu_j \delta(n_j-1)})$. Therefore, the previous limit can be calculated as: $\lim_{\delta\to 0} \frac{e^{-\lambda_j\delta}\cdot n_j\cdot(1-e^{-\mu_j\delta})\cdot(e^{-\mu_j\delta(n_j-1)})\cdot P_{nf}}{\delta} = n_j \cdot \mu_j \cdot P_{nf}$. ∎

Corollary 2. Each state transition referring to the accomplishment of a task and the reception of a negative feedback can be calculated in the same manner and depends on the current resource employed by the entity j, μ_j, and the probability to receive a negative feedback P_{nf}.

Let $(k_j, T_j - 1, n_j + 1)$ be the generic state F of the j-th social entity. Given the maximum number of allocable resources for the considered entity, that is N_j, the probability of entering the state B (identified by the triad (k_j, T_j, n_j)) from the state F is denoted with $P_{F\to B}$. Indeed, the transition rate $\gamma_{F\to B}$ from the state F to the state B is:

$$\gamma_{F\to B} = \gamma_{(k_j,T_j-1,n_j+1)\to(k_j,T_j,n_j)} = (n_j + 1) \cdot \mu_j \cdot P_{nf}. \tag{4.10}$$

Proof. Similarly to the eq.4.9, representing the reception of a negative feedback while the accomplishment of a task, the j-th social entity releases a resource employed and the arrival state is represented by the triad (k_j, T_j, n_j). Therefore, the considered transition rate can be defined as: $\gamma_{F\to B} = \gamma_{(k_j,T_j-1,n_j-1)\to(k_j,T_j,n_j)} = \lim_{\delta\to 0} \frac{P_{F\to B}(\delta)}{\delta}$.

Under the same assumption already argued for the Theorem 2, $\lim_{\delta\to 0} \frac{P_{F\to B}(\delta)}{\delta} = \lim_{\delta\to 0} \frac{P_a^0(\delta)\cdot P_s^1(\delta)}{\delta} = (n_j + 1) \cdot \mu_j \cdot P_{nf}$.

■

Case 3: positive feedback reception in response to a service provided.

Differently from the *Case 2*, with reference to Figure 4.3, all the edges moving downward forward refer to the service accomplishment within the reception of a positive feedback.

Theorem 3. *Let (k_j, T_j, n_j) be the generic state B of the j-th social entity. Given the maximum number of allocable resources for the considered entity, that is N_j, the probability of entering the state E (identified by the triad (k_j+1, T_j+1, n_j-1)) from the state B is denoted with $P_{B\to E}$. Indeed, the transition rate $\gamma_{B\to E}$ from the state B to the state E is:*

$$\gamma_{B\to E} = \gamma_{(k_j,T_j,n_j)\to(k_j+1,T_j+1,n_j-1)} = \\ = \begin{cases} 0 & if \quad n_j = 0, \\ n_j \cdot \mu_j \cdot P_{pf} & if \quad 0 < n_j < N_j. \end{cases} \tag{4.11}$$

Proof. Considering the j-th entity in the state described by the triad (k_j, T_j, n_j), the accomplishment of a task will met the reception of a positive feedback. In that case, both the value relating to the number of positive evaluations and the number of total evaluations received increases. Also, completing the assigned task, the j-th social entity releases an employed resource. The arrival state, therefore, turns out to be $(k_j + 1, T_j + 1, n_j - 1)$. However, if the parameter relating to the allocated resources n_j is equal to 0 means that the j-th entity cannot currently performs any task and will not receive any feedback. The transition rate $\gamma_{B\to E}$, which measures the probability per unit of time that an event occurs (e.g., the state transition due to positive feedback reception) within an infinitesimally small time interval δ, can be defined as: $\gamma_{(k_j,T_j,n_j)\to(k_j+1,T_j+1,n_j-1)} = \lim_{\delta\to 0} \frac{P_{B\to E}(\delta)}{\delta}$ if $0 < n_j < N_j$ and equal to 0 if $n_j = 0$.

Specifically, $\lim_{\delta\to 0} \frac{P_{B\to E}(\delta)}{\delta}$ represents the probability that 0 tasks are assigned to the considered entity, defined as $P_a^0(\delta)$, and 1 service is accomplished within the reception of a positive feedback, defined as $P_s^1(\delta)$, in a time interval equal to δ. Assuming both the aforementioned assumptions are independent, the transition probability can be written as: $\lim_{\delta\to 0} \frac{P_a^0(\delta)\cdot P_s^1(\delta)\cdot P_{pf}}{\delta}$. Since the inter-arrival and service times are assumed to be exponential, and the arrival and conditional service rates Poissonian, $P_a^0(\delta) = e^{-\lambda_j\delta}$ and $P_s^1(\delta) = n_j \cdot (1 - e^{-\mu_j\delta}) \cdot (e^{-\mu_j\delta(n_j-1)})$. Therefore, the previous limit can be calculated as: $\lim_{\delta\to 0} \frac{e^{-\lambda_j\delta}\cdot n_j\cdot(1-e^{-\mu_j\delta})\cdot(e^{-\mu_j\delta(n_j-1)})\cdot P_{pf}}{\delta} = n_j \cdot \mu_j \cdot P_{pf}$. ■

Corollary 3. Each state transition referring to the service accomplishment and the reception of a positive feedback can be calculated in the same manner and depends on the current resource employed by the entity j, μ_j, and the probability to receive a positive feedback P_{pf}.

Let $(k_j - 1, T_j - 1, n_j + 1)$ be the generic state G of the j-th social entity. Given the maximum number of allocable resources for the considered entity, that is N_j, the probability of entering the state B (identified by the triad (k_j, T_j, n_j)) from the state G is denoted with $P_{G\to B}$. Indeed, the transition rate $\gamma_{G\to B}$ from the state G to the state B is:

$$\gamma_{G\to B} = \gamma_{(k_j-1,T_j-1,n_j+1)\to(k_j,T_j,n_j)} = (n_j+1)\cdot\mu_j\cdot P_{nf}. \tag{4.12}$$

Proof. Similarly to the eq.4.11, representing the reception of a positive feedback while the accomplishment of a task, the j-th social entity releases a resource employed and the arrival state is represented by the triad (k_j, T_j, n_j). Therefore, the transition rate $\gamma_{G\to B}$ can be defined as: $\gamma_{(k_j-1,T_j-1,n_j-1)\to(k_j,T_j,n_j)} = \lim_{\delta\to 0}\frac{P_{G\to B}(\delta)}{\delta}$.

Under the same assumption previously discussed for the Theorem 3, $\lim_{\delta\to 0}\frac{P_{G\to B}(\delta)}{\delta} = \lim_{\delta\to 0}\frac{P_a^0(\delta)\cdot P_s^1(\delta)}{\delta} = (n_j+1)\cdot\mu_j\cdot P_{pf}$. ■

4.3.3 State Probability

Leveraging the estimation of transition rate probabilities evaluated in previous sections, the focus is on calculating the state probabilities of the proposed Markov chain. Each state represents an entity's current condition, which includes evaluations received from past experiences and resources allocated for executing services.

Theorem 4. *Given (k_j, T_j, n_j) the state of the j-th social entity and given the transition rates described in subsection 4.3.2, the average number of service requests λ_j assigned to the j-th entity calculated in subsection 4.3.1. Let μ_j represents the average service rate employed by the entity j, the state probability describing the behaviour of the j-th social entity can be summarized as the eq.4.13.*

$$\begin{aligned} P(k_j,T_j,n_j) = {} & P(k_j,T_j,n_j-1)\cdot\frac{\lambda_j}{\lambda_j+(n_j-1)\cdot\mu_j}+ \\ & + P(k_j,T_j-1,n_j+1)\cdot\frac{(n_j+1)\cdot\mu_j\cdot P_{nf}}{\lambda_j+(n_j+1)\cdot\mu_j}+ \\ & + P(k_j-1,T_j-1,n_j+1)\cdot\frac{(n_j+1)\cdot\mu_j\cdot P_{pf}}{\lambda_j+(n_j+1)\cdot\mu_j}. \end{aligned} \tag{4.13}$$

where $0\le k_j\le T_j$ and $0\le n_j\le N_j$. If the state probability argument does not satisfy these inequalities, the corresponding probability is equal to 0.

Proof. The aforementioned Theorem allows for finding the state probabilities describing the behavior of a social entity leveraging a recursive formula valid for any state of the Markov chain. Indeed, starting from the initial state with unitary probability, each state can be expressed as a function of the previous ones according to the Markov process. Specifically, the generic state probability (with reference to Figure 4.4) is calculated exploiting the Total Probability Law over all possible states of origin: $P(k_j,T_j,n_j) = \sum_{n=1}^{N} P((k_j,T_j,n_j),\sigma_n)$, where σ_n represents the n-th state entering in (k_j,T_j,n_j) state. By leveraging the definition of the conditional probability, the previous equation can be written as: $P(k_j,T_j,n_j) = \sum_{n=1}^{N} P((k_j,T_j,n_j)|\sigma_n)\cdot P(\sigma_n)$.

Here, the conditional probability $P((k_j,T_j,n_j)|\sigma_n)$ can be calculated by exploiting the empirical definition of probability, meaning that the extent to which an event is likely to occur is measured by the ratio of favorable cases to the whole

number of possible cases. In this context, the probability $P(k_j, T_j, n_j)$ to arrive in the state (k_j, T_j, n_j), giving the origin state σ_n, can be calculated as the transition rate $\gamma_{\sigma_n \to (k_j, T_j, n_j)}$ divided by all the possible transition rates departing from the state σ_n. Therefore, considering $P(k_j, T_j, n_j - 1)$, $P(k_j, T_j - 1, n_j + 1)$, and $P(k_j - 1, T_j - 1, n_j + 1)$ the probabilities of the states entering into (k_j, T_j, n_j) and the respective transition rates, the $P(k_j, T_j, n_j)$ can be written as reported in the eq.4.13. In particular, the denominator $\lambda_j + (n_j + 1)\mu_j$ exploit the sum of the three transition rates. Indeed, $\lambda_j + (n_j + 1)\mu_j P_{nf} + (n_j + 1)\mu_j P_{pf} = \lambda_j + (n_j + 1)\mu_j (P_{nf} + P_{pf})$, where $(P_{nf} + P_{pf})$ represents the combined probability of receiving negative and positive feedback, and it sums up to 1, as these are the two possible outcomes.

■

4.3.4 What can the model derive?

The section aims to explore insights that can be derived from the model outcomes, with a specific focus on key features related to social entities and service requests in the SIoE Network. These features include the average reputation, the intensity of unanswered requests, setting a reputation threshold, and the probability of higher-class service availability.

Average reputation

The main feature that the model can derive is the parameter referring to a social entity's average reputation. As described in Definition 4.3.2, the Reputation Factor is calculated as the ratio between the number of positive feedback received and the total number of services provided. It strongly contributes to the trustworthiness of the stakeholders, impacting the selection of the most suitable provider in service provisioning. Given k_j positive feedback and T_j total number of feedback received by a social entity, the expectation of the Δ_j reputation can be computed as: $E[\Delta_j | T_j] = \sum_{k_j=0}^{T_j} \frac{k_j}{T_j} P(k_j | T_j)$.

Given a fixed T_j, the probability $P(k_j | T_j)$ mentioned in the previous equation represents the weighting of reputation values that a social entity can assume. Referring to the states of the evaluated Markov Chain in the conceived model and making this probability explicit, the average reputation of an entity can be expressed as follows:

$$E[\Delta_j | T_j] = \sum_{k_j=0}^{T_j} \frac{k_j}{T_j} \frac{\sum_{n_j=0}^{N_j} P(k_j, T_j, n_j)}{\sum_{k_j=0}^{T_j} \sum_{n_j=0}^{N_j} P(k_j, T_j, n_j)}. \tag{4.14}$$

Intensity of unanswered requests on the SIoE Network

The second feature that can be derived from the conceived Markov Chain-based model pertains to the resources allocated by each social entity during service provisioning. As detailed in section 4.3, the state of a social entity specifies the parameter

n_j, which expresses the amount of resources currently employed by the j-th entity. In this context, the probability of being in a state described by the maximum value of n_j (i.e., $n_j = N_j$) coincides with considering the probability that a new incoming request addressed to the j-th entity is rejected due to the lack of resources. This evaluation opens up the opportunity to investigate the intensity of unanswered requests on the Social Network.

Considering the j-th service provider, with N representing the total number of social entities belonging to the evaluated service community, and given $P(k_j, T_j, N_j)$ as the state probability, and λ_j as the average number of service requests assigned to the j-th social entity obtained from the conceived model, considering a fixed T_j, the intensity of service requests that cannot be fulfilled, denoted by $L(T_j)$, can be expressed as follows:

$$L(T_j) = \sum_{j=1}^{N} \lambda_j(k_j, T_j, N_j) \frac{\sum_{k_j=0}^{T_j} P(k_j, T_j, N_j)}{\sum_{k_j=0}^{T_j} \sum_{n_j=0}^{N_j} P(k_j, T_j, n_j)}. \tag{4.15}$$

Reputation threshold

The conceived model for evaluating the behavior of a social entity can be employed to set a reputation threshold, thereby defining its role in the Social Network. To specify the reputation threshold, one must determine the number of received feedbacks, denoted as T_Δ, for which the analysis can be considered sufficient to provide a consistent assessment of the social entity's conduct. Let k_0 and T_0 represent the initial values assigned to positive feedback and total received feedback. The parameter α can be defined as the percentage of accepted reputation loss by satisfying the inequality $\frac{\overline{k_j}}{T_j} \leq \alpha \cdot \frac{k_0}{T_0}$. In particular, social entities with a reputation below the threshold set by α can be considered untrustworthy in the service provisioning procedure and may be labeled as malicious.

Here, assuming T_j is equal to $T_0 + T_\Delta$, let $\overline{k_j}$ be the Bernoulli random variable representing the average number of received positive feedbacks, which can be expressed as $\overline{k_j} = K_0 + T_\Delta \cdot P_{pf_j}$. By isolating T_Δ, the previous inequality can be written as:

$$T_\Delta \geq \frac{k_0 - \alpha \cdot k_0}{(\frac{\alpha k_0}{T_0}) - P_{pf_j}}, \tag{4.16}$$

where P_{pf_j} is the probability of the j-th social entity to receive a positive feedback.

Probability that an higher-class provider is available to perform a service request

Inspecting the states of the Markov chain, the proposed model can serve as a valuable tool for assessing the probability that a service provider within a service community possesses the necessary resources to fulfill a service request. More specifically, by

categorizing service providers into different classes, as proposed by [97], we can focus on the High-end entities. Assigning a service request to a High-end entity with abundant resources and superior computing capabilities can enhance network efficiency, resulting in faster service request processing and a reduction in unanswered requests.

In this context, considering the states of the social entities and a fixed value for T_j, the availability of the j_h-th High-end service provider, denoted as $A_{j_h}(T_{j_h})$, can be expressed as the probability $\sum_{k_{j_h}=0}^{T_{j_h}} \sum_{n_{j_h}=0}^{N_{j_h}-1} P(k_{j_h}, T_{j_h}, n_{j_h}|T_{j_h})$. By transitioning from conditional probability to joint probability and specifying the probability $P(T_{j_h})$, the final expression is presented as follows:

$$A_{j_h}(T_{j_h}) = \frac{\sum_{k_{j_h}=0}^{T_{j_h}} \sum_{n_{j_h}=0}^{N_{j_h}-1} P(k_{j_h}, T_{j_h}, n_{j_h})}{\sum_{k_{j_h}=0}^{T_{j_h}} \sum_{n_{j_h}=0}^{N_{j_h}} P(k_{j_h}, T_{j_h}, n_{j_h})}. \tag{4.17}$$

4.4 Model validation and analysis

This Section evaluates the proposed model and analyzes the results obtained. Firstly, the analytical Markov Chain based model is validated against simulation results to ensure that the model accurately reflects the environment behaviour. Secondly, different network configurations are analyzed in order to test the network performance.

TABLE 4.2: Social Entities resources and capabilities.

(A) Services Parameter

Type of Service	**Resource Consumption**	**Information Size[Mbit]**
High-end service	0.3	1.4
Middle-end service	0.2	1
Low-end service	0.1	0.6

(B) Device Parameter

Social Entity Class	**Resource Capability**	**Clock Speed [Megacyles/s]**	N_j	μ
High-end device	0.9	2000	3	1.4285
Middle-end device	0.6	1000	2	0.7142
Low-end device	0.2	40	1	0.025

4.4.1 Parameter setup

The validation of the conceived Markov chain-based model is a crucial step in the research process, as it allows us to test the model's accuracy and its ability to capture the behavior of social entities in the SIoE Network. By carefully selecting the parameters of the scenario and validating the model, we can ensure that the proposed environment accurately represents the Social Network service community under study and can be used to conduct a meaningful analysis of its behavior.

To achieve this, this work leveraged the simulator developed in C++, as previously described in chapter 2, and adapted it to fit the analytical model. The SIoE simulator has been designed to reproduce the service provisioning procedure in a Social Network of social objects divided into logical clusters composed of service communities characterized by the type of service they can handle. For this study, which is limited to the investigation of a single type of service, only one service community is simulated as well.

The characteristics of the analyzed service strongly influence network behavior. The SIoE simulator accommodates three types of services: High-end, Middle-end, and Low-end, along with three classes of social entities based on the classification in [97]. Table 4.2 provides information on each service type and social entity class. Specifically, it includes resource consumption (ranging from 0.1 to 0.3) and the information bit size for each service type. Table 4.2b, instead, specifies resource capability (ranging from 0.2 to 0.9) and clock speed in Megacycle/s for each social entity class, in addition to the values of (N_j, μ_j) indicating maximum allocable resources and average service rate used in the Markov chains, as described in Definition 4.3.3.

The proposed simulated and modeled scenario involves a fog node responsible for managing service requests. Service requests, with an average rate λ ranging from 3 to 22 requests per second, are generated according to a Poisson distribution. This approach allows us to consider various traffic loads for assessing network performance. Additionally, the results for each simulated scenario are collected from 10 different seeds to encompass various distributions of social relationships and service requests. In addition, the analysis involves 25 social entities evenly distributed between High-end and Middle-end classes within a High-end service community cluster. A fixed percentage of them simulate malicious behavior by providing poor services. Together with the computer simulation, the behavior of each social entity is analyzed through its respective Markov chain, constructed by utilizing the presented analytical model. To construct the chains, the initial state of the parameters k and T of the triad representing the state are set to 18 and 20, respectively.

4.4.2 Model validation of social entity reputation

The first feature used to validate the proposed model is the evolution of the Reputation factor. This factor serves as a valid indicator for identifying malicious entities within the SIoE Network.

Figure 4.5 illustrates an example of the evolution of social entities in terms of their reputation. It displays the temporal evolution of the feedback received by a provider, which is averaged over the total number of feedback received and represented by the Reputation factor in the model. For evaluation purposes, three social entities that provide services were randomly selected, namely the 5th, 6th, and 25th entities. In

this specific scenario, only one of the selected entities engages in malicious behavior by offering poor services more frequently than the others. Consequently, the negative feedback assigned to this misbehaving entity affects the overall reputation of that specific provider.

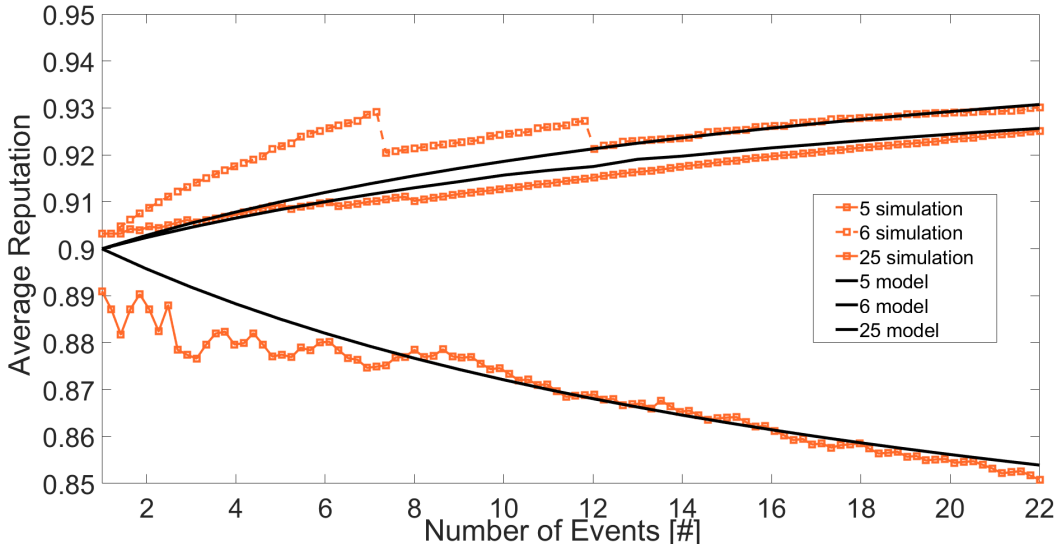


FIGURE 4.5: Average reputation validation.

The results obtained from the simulations were compared with the analytical model, based on an equal number of events processed by the service provider. The marked curves represent the trend of the reputation of the entities obtained with the SIoE simulator, while the flat curves represent the trend of the same social entities obtained through the model. Specifically, the reputation result was obtained for each event processed by utilizing eq.4.14.

It is evident that the reputation values of social entities obtained from the simulator exhibit significant fluctuations for the first few processed services, while the model's curves follow a much more regular trend. This is due to the fact that the average reputation obtained from the analytical model takes into account, from the analysis of the first events, all possible evolutions of the social entity properly weighted for their respective state probabilities. As the number of processed events increases, the differences between the curves of the analytical model and the simulation substantially decrease, eventually reaching convergence.

4.4.3 Model validation of resource availability in the cluster

Another key performance indicator used for model validation is the intensity of unanswered requests in service provisioning. In other words, this indicator represents the availability of resources of social entities in the service community as λ increases, expressing the number of service requests exposed in the cluster. Figure 4.6 displays this indicator, with the model outcomes obtained through the evaluation of eq.4.15 and represented by the continuous blue line. The simulated unanswered request rate is represented by the box plot curves. More specifically, on each box, the central mark represents the median, while the bottom and top edges show the 25th and 75th percentiles, respectively. The marked curve, instead, represents the averaged trend.

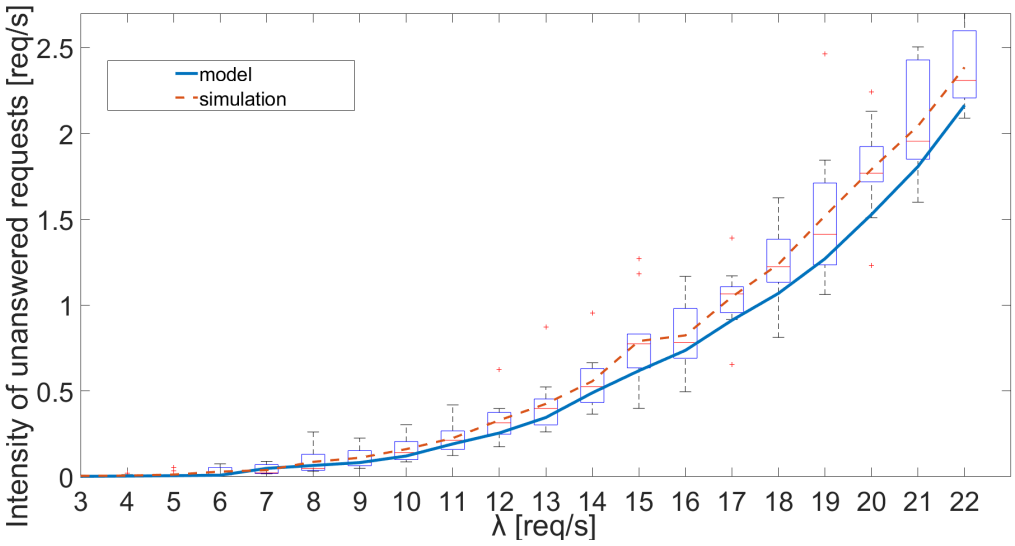


FIGURE 4.6: Intensity of unanswered request validation.

Considering low values of traffic requests (i.e., $\lambda \leq 12$), the variation of the values obtained with the simulator is very low. At the same time, the results obtained with the analytical model are consistent with it, as the blue curve intersects the median value of each box for all data points. On the other hand, when considering higher values of traffic requests, the variation between the simulator outcomes related to the intensity of unanswered requests becomes evident, thus widening their respective boxes. However, despite this significant variation, the analytical model follows the same trend as the averaged simulator outcomes, confirming the validity of the analytical results.

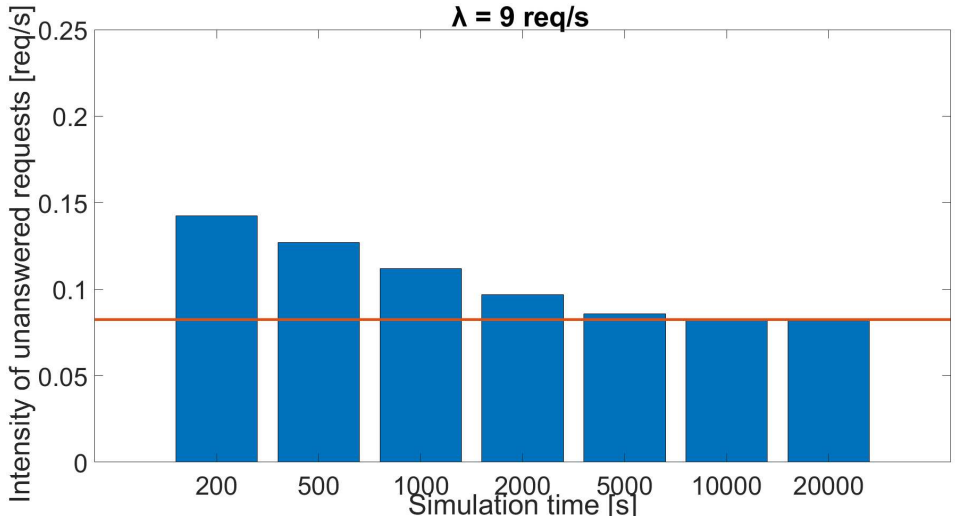
A further insight useful for illustrating the convergence of steady-state results between the analytical model and the SIoE simulator is presented in Figure 4.7.

Here, considering fixed values of λ (i.e., λ equal to 9, 10, and 11), it is evident that the analytical model immediately provides a steady-state value for the unanswered traffic, unlike the bars related to the simulations, which require approximately 10,000 seconds (about 3 hours) to achieve a steady-state result. This aspect further confirms the usefulness of the proposed analytical model, which accurately captures the long-term evolution of the overall service provisioning process, ensuring system responsiveness and eliminating the need for extensive and continuous computational efforts.

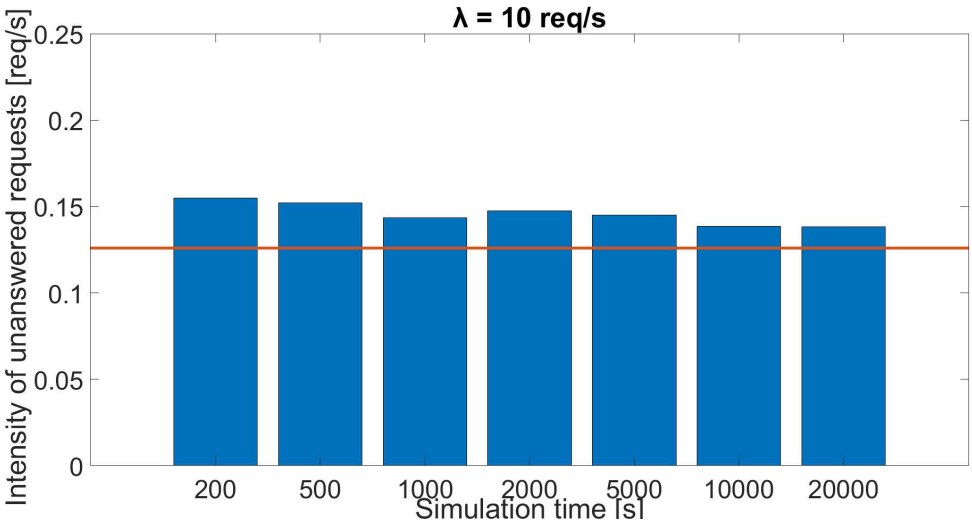
4.4.4 Numerical results and considerations

By leveraging the ability to estimate the behavior of a social entity, the proposed analytical model can serve as a valuable tool for establishing appropriate quality of service thresholds in the context of service provisioning. Specifically:

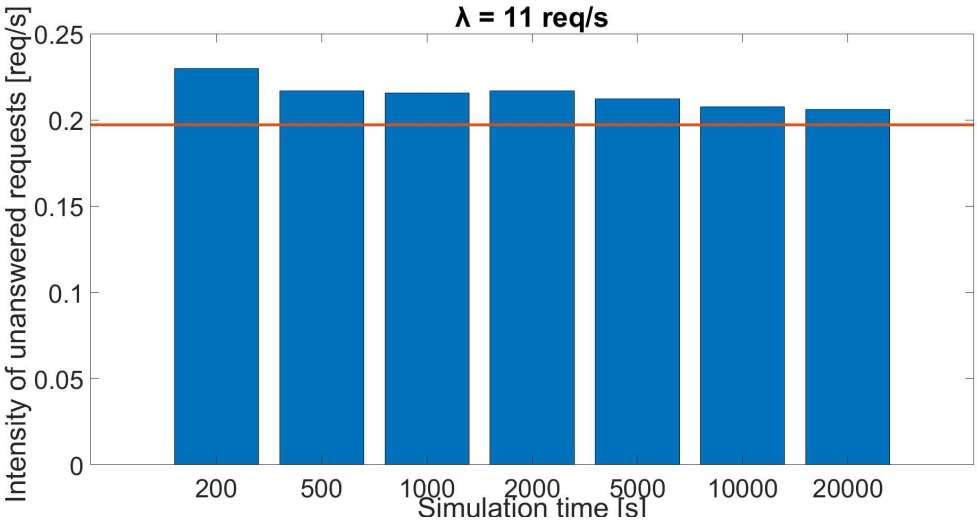
- the maximum number of malicious entities so that the service can be successfully accomplished with a given probability (taken as a design parameter);
- the minimum number of high-end providers (and their availability) to keep the intensity of unanswered requests under a given limit (taken as a design parameter).



(A) $\lambda = 9$



(B) $\lambda = 10$



(C) $\lambda = 11$

FIGURE 4.7: Simulation time convergence.

The abovementioned thresholds will be derived from various configuration scenarios, global traffic intensity, and good/bad service provider ratios. Moreover, they can be effectively utilized to design the SIoE service community, determining the number of service providers and their resources required to accomplish a service request with a specified probability, even in the presence of malicious entities.

In terms of reliability, for instance, the service community can be configured to identify and exclude any malicious entities from exposing their resources to execute service requests. To achieve this, the analysis involves investigating the parameter $E[\Delta_j|T_j]$, as detailed in subsection 4.3.4, which expresses the average reputation of a social entity.

Table 4.3 provides an application example of the proposed model to assess the impact of malicious entities on the analyzed service community. The steady-state percentage of misbehaved services is examined, considering various distributions of malicious entities, ranging from 10% to 40% of the total entities participating in service provisioning.

TABLE 4.3: Reputation analysis

Malicious Entities [%]	P_{pf} **for malicious entities**	**Community Reputation**	**Misbehaved Services [%]**
10	75	0.903	9.1
10	60	0.898	10.3
10	45	0.896	10.8
10	30	0.899	10.0
20	75	0.900	9.9
20	60	0.895	11.2
20	45	0.892	11.8
20	30	0.896	10.8
30	75	0.894	11.2
30	60	0.886	13.3
30	45	0.883	14.2
30	30	0.887	13.2
40	75	0.893	11.6
40	60	0.884	14.0
40	45	0.880	15.1
40	30	0.885	14.0

In the second column, the probability of receiving positive feedback for malicious entities is also displayed, quantifying how badly these entities behave. The community reputation is derived by weighting the reputation of each entity (calculated using eq.4.14) by the number of services provided by that entity. This calculation can be represented as: $\sum_{j=1}^{N} E[\Delta_j|T_j] \cdot \frac{T_j}{R}$, where R_N is the total number of service requests processed by all providers. The results illustrate the behavior of the percentage of misbehaved services. This percentage increases as the number of malicious entities increases, and as P_{pf} decreases, indicating a potential hostile intention of malicious providers. However, when P_{pf} for malicious entities becomes low ($P_{pf} = 0.3$), they

are no longer selected as service providers, resulting in a slight increase in the overall network reputation. This demonstrates the model's ability to capture the self-healing behavior of the SIoT trust management towards malicious entities.

Similarly, the intensity of unanswered requests $L(T_j)$, expressed in eq.4.15, can be assessed to determine the desired Grade of Service (GoS) for the SIoE cluster. This indicator is valuable for estimating how many service requests can be processed under the current network conditions. Such an evaluation allows for the design and sizing of service communities, ensuring the distribution of social entities based on their capacity to handle specific request loads.

Table 4.4 reports results for various configurations of service communities, composed of different percentages of high-end entities (ranging from 30% to 70%) under different traffic loads (λ ranging from 3 to 23 with a step of 4), and with different average probabilities that the service provider is available to accept a service request, as derived in section 4.3.4. Naturally, with the same percentage of high-end providers, the average probability that they are available decreases, resulting in an increase in the intensity of unanswered requests.

TABLE 4.4: Traffic requests analysis

λ **[req/s]**	**High-end Entities [%]**	**Average probability that high-end provider is available**	**Intensity of unanswered requests [req/s]**
3	30	0.98	0.06
7	30	0.94	0.23
11	30	0.88	0.64
15	30	0.80	1.18
19	30	0.72	1.83
23	30	0.63	2.57
3	50	0.99	0.04
7	50	0.95	0.141
11	50	0.89	0.451
15	50	0.83	0.868
19	50	0.76	1.383
23	50	0.69	1.987
3	70	0.99	0.02
7	70	0.95	0.113
11	70	0.90	0.285
15	70	0.84	0.537
19	70	0.78	0.868
23	70	0.71	1.275

The results in Table 4.4 confirm the model's ability to capture the GoS of the SIoT service community. It's also important to note that the model can effectively be used to quantify the maximum amount of traffic that can be managed to achieve a minimum GoS level (i.e., a maximum intensity of unanswered requests).

This aspect can be further emphasized by observing Figure 4.8, which provides a visual representation of the results presented in Table 4.4. By setting a GoS threshold (represented as examples with the horizontal line in Figure 4.8), the maximum value of λ can be immediately determined for different percentages of high-end entities. This demonstrates which SIoE network configuration is capable of processing a specified amount of request load.

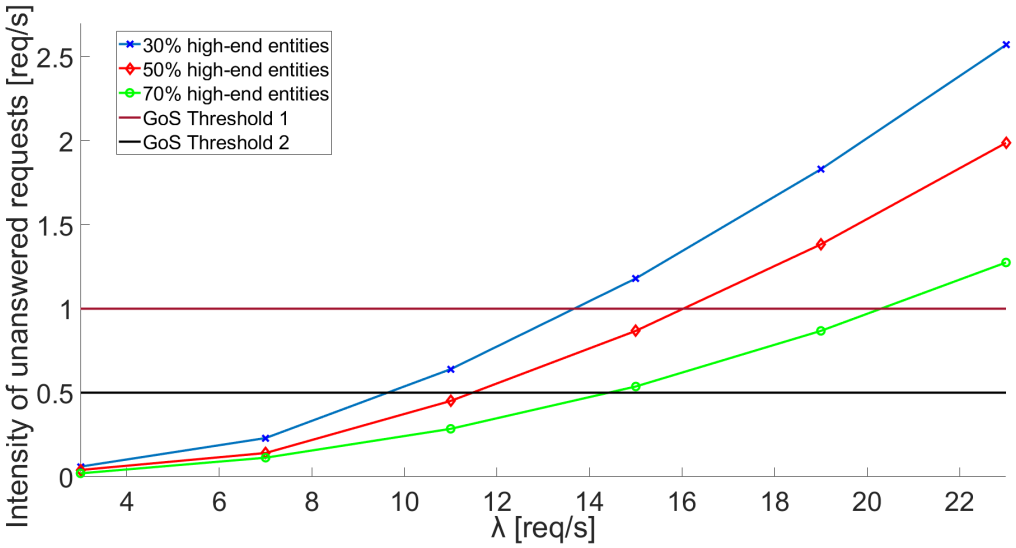


FIGURE 4.8: Unanswered requests analysis.

Conclusions and Future Works

In this thesis, a comprehensive examination has been conducted to investigate architectures and solutions for advanced service provisioning within the IoT B5G framework. The primary goal is to ensure the necessary level of network quality and user experience, with a particular focus on enhancing reliability, scalability, and trustworthiness in the context of next-generation wireless networks.

The first part of this research investigates the adoption of NB-IoT technology in satellite communications with the aim of extending IoT services beyond the limitations imposed by current terrestrial infrastructures. Specifically, it introduces an extension of the open-source 5G-air-simulator, modeling an NB-IoT satellite-based architecture. The simulation tool emphasizes the importance of proper constellation dimensioning. It shows that NPRACH preamble collisions are moderate with more satellites per orbit, resulting in lower packet delays. Furthermore, the research reports on an effective NB-IoT over satellite architecture that supports an agricultural use case. In this context, link-level features were thoroughly investigated, including the selection of suitable antennas and the definition of appropriate parameters (satellite altitude, elevation angle, and physical transmission settings) to ensure link reliability. Building upon these findings and aligning with recent 3GPP discussions on Non-Terrestrial Networks (NTN) scenarios, the satellite constellation and the resulting architecture were defined. An important innovation in this work is the assumption of the entire protocol stack being installed on-board the satellite, distinguishing it from the current state of the art. Additionally, technical adaptations to the radio interface were explored to fully support the connection between NTN terminals and the remote satellite. The overall system performance was evaluated through system-level simulations, using the aforementioned extension of the open-source 5G-air-simulator. This evaluation justifies the design choices made to meet NB-IoT specifications and provides comprehensive evidence of the feasibility of the proposed solution.

The second part of this thesis work focuses on the reliability and security aspects from a social perspective in IoT service provisioning. It proposes a multi-tiered architecture to enhance the responsiveness of IoT object service provisioning in SIoT environments. An efficient strategy for evaluating the trustworthiness of service providers is also introduced, based on social factors, reputation, and resource availability. The obtained results demonstrate that the service requests handled by the proposed Trust Management System lead to a reduction in average delay and queued requests compared to the baseline solution found in the literature. Additionally, potentially malicious nodes are effectively excluded from the network. Advancing this research further, an extension of the Trust Management System is proposed through a novel resource capability-aware scheme for service provisioning in a SIoT environment. This innovative strategy aims to provide trusted services with a high Quality of Experience, addressing fundamental limitations in this research field, including responsiveness, resource capability, efficiency, and scalability. Computer simulations have

been conducted to compare the proposed approach with baseline solutions. The results highlight that the proposed scheme can process service requests in real-time, achieving low latency while ensuring fair resource distribution and relieving IoT devices from computational burdens. Furthermore, it enables the prompt identification of malicious nodes, preventing them from serving as providers for future service requests.

Furthermore, this thesis introduced a streamlined method for dynamically selecting the most suitable network segment, particularly in post-disaster scenarios, to ensure the in-network processing of videos captured by a drone. Leveraging Digital Twins, we can identify the status and accessibility of physical domains. An algorithm for decision-making, which relies on QoS, social attributes, and trust parameters, is presented. Through computer simulations, we have demonstrated that this approach enhances reliability in terms of offloaded data and reduces missed video acquisitions, especially as the number of unavailable domains due to disruptions increases when compared to conventional baseline solutions.

Finally, a stochastic analytical model based on a multidimensional Markov chain is also presented. This model is designed for the selection of trusted providers in the context of SIoE service provisioning. It actively monitors the reputation and capability of SIoT entities as they deliver services while effectively excluding malicious entities from the social network. During the validation process, the analytical model exhibited a significant degree of convergence in simulations, confirming its suitability for real-world SIoE scenarios. Numerical results unequivocally demonstrate the model's effectiveness in identifying malicious behaviors, facilitating trusted operations, and enhancing system reliability. Furthermore, the model can quantify the maximum traffic capacity that the network can handle to achieve a minimum level of GoS (Grade of Service) in the service provisioning process. This quantitative insight can greatly assist in structuring the SIoE network, ensuring optimal performance and reliability.

Future research activities will further explore the provisioning of advanced services in the IoT framework. This will involve the ongoing development of innovative architectures for real-world applications across diverse network domains and segments, including TN-NTN and NTN networks. These methodologies will leverage entity virtualization to enable advanced orchestrations within more complex network infrastructures, such as Intent-Based Networking, and future 6G networks. All of these efforts are aimed at ensuring the highest possible quality of experience for end-users. Furthermore, it will be of paramount importance to explore additional use cases, address any required novel extensions, and evaluate the effectiveness of the proposed technical solutions through experimental test environments. During this pivotal phase of the research, the study will deploy terminals and base stations utilizing Software-Defined Radio, and develop a traffic emulator with the assistance of hardware and software modules.

Appendix A

Appendix

A.1 Average number of service requests assigned to a social entity

This appendix extends and specifies the development of eq.4.2, as discussed in subsection 4.3.1. It pertains to the calculation of the average number of service requests assigned to the j-th social entity, denoted as λ_j. Specifically, the formula mentioned can be evaluated by specifying each value that $\tau = \psi$ can assume in the summation, starting from $\psi = 0$. This expression represents the number of social entities more trusted than the j-th entity according to the i-th requester.

Assuming $\psi = 0$

By applying the joint probability distribution according to the scheme $P((A|B), C) = \frac{P(A,B,C)}{P(B)}$, the probability $P(R_{i\to j}|(k_j, T_j, n_j))$ can be developed as:

$$P(R_{i\to j}|(k_j, T_j, n_j)) = \frac{P(R_{i\to j}, (k_j, T_j, n_j), \tau = 0)}{P(k_j, T_j, n_j)}. \tag{A.1}$$

Then, passing from joint probability to conditional probability, we obtain:

$$\begin{aligned} &P(R_{i\to j}|(k_j, T_j, n_j)) = \\ &= \frac{P(R_{i\to j}|((k_j, T_j, n_j), \tau = 0))P((k_j, T_j, n_j), \tau = 0)}{P(k_j, T_j, n_j)}. \end{aligned} \tag{A.2}$$

Applying the Bayes' Theorem and simplifying the denominator the previous equation can be reconducted to the following equation:

$$\begin{aligned} &P(R_{i\to j}|(k_j, T_j, n_j)) = \\ &= \underbrace{P(R_{i\to j}|((k_j, T_j, n_j), \tau = 0))}_{\Theta(\psi)} \cdot \underbrace{P(\tau = 0|(k_j, T_j, n_j))}_{\Omega(\psi)}. \end{aligned} \tag{A.3}$$

$\Theta(\psi)$ identifies the first part of the eq.A.3, consisting of the joint probability that a request from i is assigned to j, given the knowledge of the state of j and jointly the probability that no social entities are more trusted than j according to i. Whereas,

$\Omega(\psi)$ identifies the second part of the eq.A.3, indicating the probability that no social entities are more trusted than j, given the knowledge of the state of j.

Thus, assuming $\psi = 0$, since there are certainly no friends of the i-th requester who are most trusted than j, the service request issued by i will be assigned for sure to entity j. Therefore, the probability defined by $\Theta(\psi)$ turns out to be equal to 1. Let ψ_1, ψ_2,...,and, ψ_{Ψ_i-1} be the friends of the social entity i. The assumption that there are no friends of the i-th service requester more trusted than j means that the j-th social entity is the most trusted one in the set of all Ψ_i entities. Then, $\Omega(\psi)$ can also be written as:

$$\begin{aligned}\Omega(\psi) = P(Tr_{ij} > Tr_{i\psi_1}, Tr_{ij} > Tr_{i\psi_2}, ..., \\ ..., Tr_{ij} > Tr_{i\psi_{\Psi_i-1}} | (k_j, T_j, n_j)).\end{aligned} \tag{A.4}$$

Assuming that these events are all independent of each other, the eq.A.4 becomes:

$$\Omega(\psi) = \prod_{m=1}^{\Psi_i-1} P(Tr_{ij} > Tr_{i\psi_m} | (k_j, T_j, n_j)) \tag{A.5}$$

Following the metric described in the Definition 4.2.3 in the chapter 4 and making explicit the Trust value, the previous equation can be also written as:

$$\Omega(\psi) = \prod_{m=1}^{\Psi_i-1} P(S_{ij}\Delta_j > S_{i\psi_m}\Delta_{\psi_m} | (k_j, T_j, n_j)), \tag{A.6}$$

where S_{ij} and $S_{i\psi_m}$ are the Sociality factor estimating the degree of social relationship between i-th and j-th, and i-th and ψ_m-th entities. Whereas, Δ_j and Δ_{ψ_m} represent the Reputation values of the j-th and ψ_m-th entities, and are equal to $\frac{k_j}{T_j}$ and $\frac{k_{\psi_m}}{T_{\psi_m}}$, respectively. Therefore,

$$\Omega(\psi) = \prod_{m=1}^{\Psi_i-1} P(k_{\psi_m} < \frac{S_{ij}\Delta_j T_{\psi_m}}{S_{i\psi_m}}) = \prod_{m=1}^{\Psi_i-1} \sum_{\nu=0}^{\nu_0} P(k_{\psi_m} = \nu) \tag{A.7}$$

where $\nu_0 = \lfloor \frac{S_{ij}\Delta_j T_{\psi_m}}{S_{i\psi_m}} \rfloor$.

Developing the probability of the eq.A.7 with binomial equation according to Bernoulli process, we obtain:

$$\Omega(\psi) = \prod_{m=1}^{\Psi_i-1} \sum_{\nu=0}^{\nu_0} \binom{T_{\psi_m}}{\nu} \cdot P_{pf_{\psi_m}}^{\nu} \cdot (1 - P_{pf_{\psi_m}})^{T_{\psi_m}-\nu}, \tag{A.8}$$

where P_{pf_j} and $P_{pf_{\psi_m}}$ are the probabilities of the j-th and ψ_m-th entities to receive a positive feedback after the provisioning of a service. Finally, the average number of

service requests assigned to the j-th social entity, denoted by λ_j assuming $\psi = 0$ can be expressed as reported in the eq.A.9.

$$\lambda_j(\tau = 0) = \sum_{i=1, i\neq j}^{\Psi_j} \lambda_{ij} \sum_{\psi=0}^{\Psi_i - 1} \prod_{m=1}^{\Psi_i - 1} \sum_{\nu=0}^{\nu_0} \binom{T_{\psi_m}}{\nu} P_{pf_{\psi_m}}^{\nu} (1 - P_{pf_{\psi_m}})^{T_{\psi_m} - \nu} \tag{A.9}$$

Assuming $\psi = 1$

Now, starting from the eq.4.2, the expressed probability is developed assuming $\psi = 1$. Let ψ_1, ψ_2,...,and, $\psi_{\Psi_i - 1}$ be the friends of the i-th social entity. The assumption of $\tau = 1$ can be expressed by the sum of the whole probabilities that only a single entity of the set Ψ_i is more trusted than the j-th provider and no other ones. Thus, assuming $\psi = 1$, the eq.4.2 can be written as reported in the eq.A.10. Here, all the described statement are mutually disjoint, therefore, the union can be extended over the whole equation. Then, the probability of the union of mutually disjoint events corresponds to the sum of the probability that events occur and the eq.A.10 become as reported in the eq.A.11. Following exactly the same procedure adopted to obtain the eq.A.3, the eq.A.11 can be written as the eq.A.12.

$$\begin{aligned}
&P(R_{i\to j} | (k_j, T_j, n_j), \tau = 1) = \\
&\quad = P(R_{i\to j} | (k_j, T_j, n_j), \bigcup_{m=1}^{\Psi_i - 1} (Tr_{i\psi_m} > Tr_{ij}, \bigcap_{l=1, l\neq m}^{\Psi_i - 2} (Tr_{i\psi_l} \leq Tr_{ij}))) = \qquad \text{(A.10)} \\
&\quad = \sum_{m=1}^{\Psi_i - 1} P(R_{i\to j} | (k_j, T_j, n_j), Tr_{i\psi_m} > Tr_{ij}, \bigcap_{l=1, l\neq m}^{\Psi_i - 2} Tr_{i\psi_l} \leq Tr_{ij}) = \qquad \text{(A.11)} \\
&\quad = \sum_{m=1}^{\Psi_i - 1} \underbrace{P(R_{i\to j} | ((k_j, T_j, n_j), Tr_{i\psi_m} > Tr_{ij}, \bigcap_{l=1, l\neq m}^{\Psi_i - 2} P(Tr_{i\psi_l} \leq Tr_{ij})))}_{\Xi(\psi)} \cdot \\
&\quad \underbrace{\cdot P(Tr_{i\psi_m} > Tr_{ij}, \bigcap_{l=1, l\neq m}^{\Psi_i - 2} Tr_{i\psi_l} \leq Tr_{ij} | (k_j, T_j, n_j))}_{\Phi(\psi)} \qquad \text{(A.12)}
\end{aligned}$$

Then, from the eq.A.12 we can consider separately the two probabilities, namely $\Xi(\psi)$ and $\Phi(\psi)$, respectively. In this regard, analyzing $\Xi(\psi)$ implies considering the event of a service request coming from i-th service requester and assigned to the j-th service provider, meanwhile a friend of i is more trusted than j-th entity. This means that the ψ_m-th entity belonging to the set of Ψ_i friends of i-th requester is potentially the most suitable one to execute the service, but, despite this, the selection of the

provider falls on the j-th entity. The motivation behind this choice can be led to the lack of available resources exhibitable by the ψ_m-th most trusted service provider, which in probabilistic terms results analogous to that entity's blocking probability, as expressed in the following equation:

$$\Xi(\psi) = P_B(\psi_m) = \left(\frac{\lambda_{\psi_m}}{\mu_{\psi_m}}\right)^{N_{\psi_m}} \frac{1}{N_{\psi_m}!} \frac{1}{\sum_{s=1}^{N_{\psi_m}} \left(\frac{\lambda_{\psi_m}}{\mu_{\psi_m}}\right)^s \frac{1}{s!}}, \tag{A.13}$$

where λ_{ψ_m} is the average number of service requests assigned to the entity ψ_m, μ_{ψ_m} is the average service rate employed by the entity ψ_m to perform a service, and N_{ψ_m} represents the maximum amount of resources provided by the the ψ_m-th social entity.

The evaluation of $\Phi(\psi)$, instead, implies to calculate the probability that only the ψ_m-th friend of i is more trusted than the j-th social entity, given the knowledge of the state (k_j, T_j, n_j), as expressed in the following equation:

$$\begin{aligned}\Phi(\psi) = P(&Tr_{i\psi_1} \leq Tr_{ij}, Tr_{i\psi_2} \leq Tr_{ij}, ..., \\ &, ..., Tr_{i\psi_m} > Tr_{ij}, Tr_{i\psi_{\Psi_i-2}} \leq Tr_{ij} | (k_j, T_j, n_j)).\end{aligned} \tag{A.14}$$

Considering all the events independent each other and making explicit the Trust value, the eq.A.14 can be written as:

$$\Phi(\psi) = P(S_{i\psi_m}\Delta_{\psi_m} > S_{ij}\Delta_j) \prod_{l=1, l\neq m}^{\Psi_i-2} P(S_{i\psi_l}\Delta_{\psi_l} \leq S_{ij}\Delta_j), \tag{A.15}$$

where S_{ij}, $S_{i\psi_m}$, and $S_{i\psi_l}$ are the Sociality factor estimating the degree of social relationship between i-th and j-th, i-th and ψ_m-th, and i-th and ψ_l-th social entities. Whereas, Δ_j, Δ_{ψ_m}, and Δ_{ψ_l} represent the Reputation values of the j-th, the ψ_m-th and the ψ_l-th social entities, and are equal to $\frac{k_j}{T_j}$, $\frac{k_{\psi_m}}{T_{\psi_m}}$, and $\frac{k_{\psi_l}}{T_{\psi_l}}$, respectively. Moreover, setting and isolating the term k_ψ as the random variable of the equation, we obtain:

$$\Phi(\psi) = \sum_{\nu=\nu_0+1}^{T_{\psi_m}} P(k_{\psi_m} = \nu) \prod_{l=1, l\neq m}^{\Psi_i-1} \sum_{\nu'=0}^{\nu_l} P(k_{\psi_l} = \nu') \tag{A.16}$$

where $\nu_0 = \lfloor \frac{S_{ij}\Delta_j T_{\psi_m}}{S_{i\psi_m}} \rfloor$, and $\nu_l = \lfloor \frac{S_{ij}\Delta_j T_{\psi_l}}{S_{i\psi_l}} \rfloor$.

Developing using a binomial formula with the same procedure exploited in the eq.A.7, the probabilities $P(k_{\psi_m} = \nu)$ and $P(k_{\psi_l} = \nu')$ can be evaluated as:

$$\begin{aligned}P(k_{\psi_m} = \nu) &= \binom{T_{\psi_m}}{\nu} \cdot (P_{pf_{\psi_m}})^{\nu} \cdot (1 - P_{pf_{\psi_m}})^{T_{\psi_m}-\nu}, \\ P(k_{\psi_l} = \nu') &= \binom{T_{\psi_l}}{\nu'} \cdot (P_{pf_{\psi_l}})^{\nu'} \cdot (1 - P_{pf_{\psi_l}})^{T_{\psi_l}-\nu'},\end{aligned} \tag{A.17}$$

where $P_{pf_{\psi_m}}$ and $P_{pf_{\psi_l}}$ are the receiving positive feedback probabilities supposed of the ψ_m-th and ψ_l-th social entities, and T_{ψ_m} and T_{ψ_l} are approximable within the criterion developed in the eq.4.5. Finally, the average number of service requests assigned to the j-th social entity, denoted by λ_j assuming $\psi = 1$ can be expressed as reported in the eq.A.18.

$$\lambda_j(\tau = 1) = \tag{A.18}$$
$$= \sum_{i=1, i\neq j}^{\Psi_j} \lambda_{ij} \sum_{\psi=0}^{\Psi_i - 1} \sum_{m=1}^{\Psi_i - 1} \left(\frac{\lambda_{\psi_m}}{\mu_{\psi_m}}\right)^{N_{\psi_m}} \frac{1}{N_{\psi_m}!} \frac{1}{\sum_{s=1}^{N_{\psi_m}} \left(\frac{\lambda_{\psi_m}}{\mu_{\psi_m}}\right)^s \frac{1}{s!}} \cdot$$
$$\cdot \sum_{\nu=\nu_0+1}^{T_{\psi_m}} \binom{T_{\psi_m}}{\nu} (P_{pf_{\psi_m}})^{\nu} (1 - P_{pf_{\psi_m}})^{T_{\psi_m} - \nu} \prod_{l=1, l\neq m}^{\Psi_i - 1} \sum_{\nu'=0}^{\nu_l} \binom{T_{\psi_l}}{\nu'} (P_{pf_{\psi_l}})^{\nu'} (1 - P_{pf_{\psi_l}})^{T_{\psi_l} - \nu'}$$

Assuming $\psi = 2$

Let ψ_1, ψ_2,..., and, $\psi_{\Psi_i - 1}$ be the friends of the i-th social entity, the assumption of $\psi = 2$ can be expressed as the sum of probabilities of all the possible instances that, at the same time, two entities of the set Ψ_i are more trusted than the provider j. Thus, starting from the eq.4.2, following the same procedure discussed in the previous case, the probability $P(R_{i\to j}|(k_j, T_j, n_j), \tau = 2)$ can be developed as the eq.A.19.

$$P(R_{i\to j}|(k_j, T_j, n_j), \tau = 2) = \tag{A.19}$$
$$\sum_{m=1}^{\Psi_i - 1} \underbrace{\sum_{c=1, c\neq m}^{\Psi_i - 2} P(R_{i\to j}|((k_j, T_j, n_j), Tr_{i\psi_m} > Tr_{ij}, Tr_{i\psi_c} > Tr_{ij}, \prod_{l=1, l\neq m, l\neq c}^{\Psi_i - 3} P(Tr_{i\psi_l} \leq Tr_{ij})))}_{\Xi(\psi)} \cdot$$
$$\underbrace{\cdot P(Tr_{i\psi_m} > Tr_{ij}, Tr_{i\psi_c} > Tr_{ij}) \prod_{l=1, l\neq m, l\neq c}^{\Psi_i - 3} P(Tr_{i\psi_l} \leq Tr_{ij}|(k_j, T_j, n_j))}_{\Phi(\psi)}$$

As in the previous case, the two probabilities $\Xi(\psi)$ and $\Phi(\psi)$ are developed separately. Here, $\Xi(\psi)$ represents the event of a service request coming from the i-th service requester assigned to the j-th provider, considering that there are two friends of i who are more trusted than j. This implies that these entities are potentially the most suitable ones to execute the service. However, despite this, the j-th social entity is selected as the provider. This occurs due to the lack of available resources exhibited by the ψ_m-th and ψ_c-th potentially most suitable service providers, which, in probabilistic terms, is analogous to evaluating their blocking probabilities:

$$\Xi(\psi) = P_B(\psi_m) \cdot P_B(\psi_c) = \\ = \left(\frac{\lambda_{\psi_m}}{\mu_{\psi_m}}\right)^{N_{\psi_m}} \frac{1}{N_{\psi_m}!} \frac{1}{\sum_{s=1}^{N_{\psi_m}} \left(\frac{\lambda_{\psi_m}}{\mu_{\psi_m}}\right)^s \frac{1}{s!}} \left(\frac{\lambda_{\psi_c}}{\mu_{\psi_c}}\right)^{N_{\psi_c}} \frac{1}{N_{\psi_c}!} \frac{1}{\sum_{s=1}^{N_{\psi_c}} \left(\frac{\lambda_{\psi_c}}{\mu_{\psi_c}}\right)^s \frac{1}{s!}}. \tag{A.20}$$

where, λ_{ψ_m} is the average number of service requests assigned to the entity ψ_m, μ_{ψ_m} is the average service rate employed by the entity ψ_m to perform a service, and N_{ψ_m} represents the maximum amount of resources provided by the ψ_m-th social entity. Similarly, λ_{ψ_c} is the average number of service requests assigned to the entity ψ_c, μ_{ψ_c} is the average service rate employed by the entity ψ_c to perform a service, and N_{ψ_c} represents the maximum amount of resources provided by the ψ_c-th social entity. The evaluation of λ_{ψ_m} and λ_{ψ_c} depends on the number of social relationships handled and the positive feedback probability of the ψ_m-th and ψ_c-th social entity and expressed as the approximation of the eq.4.6, as detailed in subsection 4.3.1.

The evaluation of $\Phi(\psi)$, instead, implies to calculate the probability that the ψ_m-th and the ψ_c-th friends of i are more trusted than j, given the knowledge of the state (k_j, T_j, n_j), as reported in the eq.A.21.

$$\Phi(\psi) = P(Tr_{i\psi_1} \leq Tr_{ij}, Tr_{i\psi_2} \leq Tr_{ij}, Tr_{i\psi_m} > Tr_{ij}, ..., \\ , ..., Tr_{i\psi_c} > Tr_{ij}, Tr_{i\psi_{\Psi_i-3}} \leq Tr_{ij} | (k_j, T_j, n_j)). \tag{A.21}$$

Considering the events of the eq.A.21 independent each other and making explicit the Trust value the eq.A.21 can be written as:

$$\Phi(\psi) = P(S_{i\psi_m}\Delta_{\psi_m} > S_{ij}\Delta_j) \cdot P(S_{i\psi_c}\Delta_{\psi_c} > S_{ij}\Delta_j) \cdot \\ \cdot \prod_{l=1, l\neq m, l\neq c}^{\Psi_i-3} P(S_{i\psi_l}\Delta_{\psi_l} \leq S_{ij}\Delta_j), \tag{A.22}$$

where S_{ij}, $S_{i\psi_m}$, $S_{i\psi_c}$ and $S_{i\psi_l}$ are the Sociality factor estimating the degree of social relationship between i-th and j-th, i-th and ψ_m-th, i-th and ψ_c-th, and i-th and ψ_l-th social entities. Whereas, Δ_j, Δ_{ψ_m}, Δ_{ψ_c}, and Δ_{ψ_l} represent the Reputation values of the j-th, the ψ_m-th, ψ_c-th, and the ψ_l-th social entities, and are equal to $\frac{k_j}{T_j}$, $\frac{k_{\psi_m}}{T_{\psi_m}}$, $\frac{k_{\psi_c}}{T_{\psi_c}}$, and $\frac{k_{\psi_l}}{T_{\psi_l}}$, respectively. Moreover, setting and isolating the term k_ψ as the random variable, we obtain:

$$\Phi(\psi) = \sum_{\nu=\nu_0+1}^{T_{\psi_m}} P(k_{\psi_m} = \nu) \cdot \sum_{\nu'=\nu_c+1}^{T_{\psi_c}} P(k_{\psi_c} = \nu') \cdot \prod_{l=1, l\neq m}^{\Psi_i-3} \sum_{\nu''=0}^{\nu_l} P(k_{\psi_l} = \nu'') \tag{A.23}$$

where $\nu_0 = \lfloor \frac{S_{ij}\Delta_j T_{\psi_m}}{S_{i\psi_m}} \rfloor$, $\nu_c = \lfloor \frac{S_{ij}\Delta_j T_{\psi_c}}{S_{i\psi_c}} \rfloor$, and $\nu_l = \lfloor \frac{S_{ij}\Delta_j T_{\psi_l}}{S_{i\psi_l}} \rfloor$.

Adopting a binomial formula in the same manner of the eq.A.7, the probabilities $P(k_{\psi_m} = \nu)$, $P(k_{\psi_c} = \nu')$, and $P(k_{\psi_l} = \nu'')$ can be evaluated as:

$$\begin{aligned} P(k_{\psi_m} = \nu) &= \binom{T_{\psi_m}}{\nu} \cdot P_{pf_{\psi_m}}^{\nu} \cdot (1 - P_{pf_{\psi_m}})^{T_{\psi_m} - \nu}, \\ P(k_{\psi_c} = \nu') &= \binom{T_{\psi_c}}{\nu'} \cdot P_{pf_{\psi_c}}^{\nu'} \cdot (1 - P_{pf_{\psi_c}})^{T_{\psi_c} - \nu'}, \\ P(k_{\psi_l} = \nu'') &= \binom{T_{\psi_l}}{\nu''} \cdot P_{pf_{\psi_l}}^{\nu''} \cdot (1 - P_{pf_{\psi_l}})^{T_{\psi_l} - \nu''}, \end{aligned} \tag{A.24}$$

where, $P_{pf_{\psi_m}}$, $P_{pf_{\psi_c}}$, and $P_{pf_{\psi_l}}$ are the receiving positive feedback probabilities supposed of the ψ_m-th, the ψ_c-th, and ψ_l-th social entities, and T_{ψ_m}, T_{ψ_c}, and T_{ψ_l} are approximable with the criterion developed in the eq.4.5. Finally, the average number of service requests assigned to the j-th social entity, denoted by λ_j assuming $\psi = 2$ can be expressed as reported in the eq.A.25.

$$\lambda_j(\tau = 2) = \sum_{i=1, i \neq j}^{\Psi_j} \lambda_{ij} \sum_{\psi=0}^{\Psi_i - 1} \sum_{m=1}^{\Psi_i - 1} \sum_{c=1, c \neq m}^{\Psi_i - 2} \left(\frac{\lambda_{\psi_m}}{\mu_{\psi_m}} \right)^{N_{\psi_m}} \frac{1}{N_{\psi_m}!} \frac{1}{\sum_{s=1}^{N_{\psi_m}} \left(\frac{\lambda_{\psi_m}}{\mu_{\psi_m}} \right)^s \frac{1}{s!}} \cdot$$

$$\cdot \left(\frac{\lambda_{\psi_c}}{\mu_{\psi_c}} \right)^{N_{\psi_c}} \frac{1}{N_{\psi_c}!} \frac{1}{\sum_{s=1}^{N_{\psi_c}} \left(\frac{\lambda_{\psi_c}}{\mu_{\psi_c}} \right)^s \frac{1}{s!}} \sum_{\nu=\nu_0+1}^{T_{\psi_m}} \binom{T_{\psi_m}}{\nu} P_{pf_{\psi_m}}^{\nu} (1 - P_{pf_{\psi_m}})^{T_{\psi_m} - \nu} \cdot$$

$$\cdot \sum_{\nu'=\nu_c+1}^{T_{\psi_c}} \binom{T_{\psi_c}}{\nu'} P_{pf_{\psi_c}}^{\nu'} (1 - P_{pf_{\psi_c}})^{T_{\psi_c} - \nu'} \prod_{l=1, l \neq m}^{\Psi_i - 3} \sum_{\nu''=0}^{\nu_l} \binom{T_{\psi_l}}{\nu''} P_{pf_{\psi_l}}^{\nu''} (1 - P_{pf_{\psi_l}})^{T_{\psi_l} - \nu''}. \tag{A.25}$$

It's worth noting that Formula A.19 can also be extended to $\tau = 3$, $\tau = 4$, and so on, where there are respectively three entities, four entities, and so forth, more trusted than j, but none of them have sufficient available resources. However, the probability of these events is negligible when compared to the cases with $\tau = 2$, so they are not considered as additional contributions in Formula 4.2. Evaluating the probability in Formula A.19 for higher values of τ would result in an excessively complex model, which is not justified by the small gain in accuracy.

Bibliography

[1] M. Vaezi, A. Azari, S. R. Khosravirad, *et al.*, "Cellular, wide-area, and non-terrestrial iot: A survey on 5g advances and the road toward 6g," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1117–1174, 2022. DOI: 10.1109/COMST.2022.3151028.

[2] S. Yeganeh, A. Tootoonchian, and Y. Ganjali, "On scalability of software-defined networking," *Communications Magazine, IEEE*, vol. 51, pp. 136–141, Feb. 2013. DOI: 10.1109/MCOM.2013.6461198.

[3] S. Zhang, D. Zhang, Y. Wu, and H. Zhong, "Service recommendation model based on trust and qos for social internet of things," *IEEE Transactions on Services Computing*, pp. 1–14, 2023. DOI: 10.1109/TSC.2023.3274647.

[4] H. X. Nguyen, R. Trestian, D. To, and M. Tatipamula, "Digital twin for 5g and beyond," *IEEE Communications Magazine*, vol. 59, no. 2, pp. 10–15, 2021. DOI: 10.1109/MCOM.001.2000343.

[5] O. Kodheli, E. Lagunas, N. Maturo, *et al.*, "Satellite Communications in the New Space Era: A Survey and Future Challenges," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2020. DOI: 10.1109/COMST.2020.3028247.

[6] A. Petrosino, G. Sciddurlo, S. Martiradonna, D. Striccoli, G. Piro, and G. Boggia, "Wip: An open-source tool for evaluating system-level performance of nb-iot non-terrestrial networks," in *22nd IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2021.

[7] G. Sciddurlo, A. Petrosino, M. Quadrini, *et al.*, "Looking at nb-iot over leo satellite systems: Design and evaluation of a service-oriented solution," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 14 952–14 964, 2022. DOI: 10.1109/JIOT.2021.3135060.

[8] Y. .-. E. Wang, X. Lin, A. Adhikary, *et al.*, "A primer on 3GPP Narrowband Internet of Things," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 117–123, 2017. DOI: 10.1109/MCOM.2017.1600510CM.

[9] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, 2019, ISSN: 2405-9595. DOI: https://doi.org/10.1016/j.icte.2017.12.005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2405959517302953.

[10] H. Malik, H. Pervaiz, M. Mahtab Alam, Y. Le Moullec, A. Kuusik, and M. Ali Imran, "Radio resource management scheme in NB-IoT systems," *IEEE Access*, vol. 6, pp. 15 051–15 064, 2018. DOI: 10.1109/ACCESS.2018.2812299.

[11] 3GPP, "E-UTRA and E-UTRAN; LTE Physical Layer, General Description," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 36.201, 2018, Release 15.

[12] 3GPP, "E-UTRA and E-UTRAN; LTE Physical Layer, Overall Description," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 36.300, 2018, Release 15.

[13] R. Ratasuk, N. Mangalvedhe, Y. Zhang, M. Robert, and J. Koskinen, "Overview of narrowband IoT in LTE Rel-13," in *IEEE Conference on Standards for Communications and Networking (CSCN)*, 2016, pp. 1–7. DOI: 10.1109/CSCN.2016.7785170.

[14] X. Lin, A. Adhikary, and Y. .-. Eric Wang, "Random Access Preamble Design and Detection for 3GPP Narrowband IoT Systems," *IEEE Wireless Communications Letters*, vol. 5, no. 6, pp. 640–643, 2016. DOI: 10.1109/LWC.2016.2609914.

[15] O. Kodheli, N. Maturo, S. Andrenacci, S. Chatzinotas, and F. Zimmer, "Link budget analysis for satellite-based narrowband IoT systems," in *International Conference on Ad-Hoc Networks and Wireless*, Springer, 2019, pp. 259–271.

[16] G. Charbit, D. Lin, K. Medles, L. Li, and I. Fu, "Space-Terrestrial Radio Network Integration for IoT," in *Proc. of IEEE 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5. DOI: 10.1109/6GSUMMIT49458.2020.9083854.

[17] K. O'Hara and G. Skidmore, "Providing narrowband IoT coverage with Low Earth Orbit satellites," *Microwave Journal*, vol. 62, no. 12, pp. 74–84, 2019.

[18] Z. Qu, G. Zhang, H. Cao, and J. Xie, "LEO Satellite Constellation for Internet of Things," *IEEE Access*, vol. 5, pp. 18 391–18 401, 2017. DOI: 10.1109/ACCESS.2017.2735988.

[19] S. Cluzel, L. Franck, J. Radzik, *et al.*, "3GPP NB-IOT Coverage Extension Using LEO Satellites," in *Proc. of IEEE Vehicular Technology Conference (VTC Spring)*, 2018, pp. 1–5. DOI: 10.1109/VTCSpring.2018.8417723.

[20] A. K. Dwivedi, S. Praneeth Chokkarapu, S. Chaudhari, and N. Varshney, "Performance analysis of novel Direct Access schemes for LEO satellites based IoT network," in *IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*, 2020, pp. 1–6. DOI: 10.1109/PIMRC48278.2020.9217207.

[21] O. Kodheli, S. Andrenacci, N. Maturo, S. Chatzinotas, and F. Zimmer, "An Uplink UE Group-Based Scheduling Technique for 5G mMTC Systems Over LEO Satellite," *IEEE Access*, vol. 7, pp. 67 413–67 427, 2019. DOI: 10.1109/ACCESS.2019.2918581.

[22] M. Conti, S. Andrenacci, N. Maturo, S. Chatzinotas, and A. Vanelli-Coralli, "Doppler Impact Analysis for NB-IoT and Satellite Systems Integration," in *Proc. of IEEE International Conference on Communications (ICC)*, 2020, pp. 1–7. DOI: 10.1109/ICC40277.2020.9149140.

[23] O. Kodheli, N. Maturo, S. Chatzinotas, S. Andrenacci, and F. Zimmer, "On the Random Access Procedure of NB-IoT Non-Terrestrial Networks," in *Proc. of IEEE Advanced Satellite Multimedia Systems Conference (ASMS) and 16th Signal Processing for Space Communications Workshop (SPSC)*, IEEE Virtual Conference, 2020.

[24] A. Guidotti, A. Vanelli-Coralli, M. Conti, *et al.*, "Architectures and key technical challenges for 5G systems incorporating satellites," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2624–2639, 2019.

[25] A. Guidotti, A. Vanelli-Coralli, T. Foggi, *et al.*, "LTE-based Satellite Communications in LEO Mega-Constellations," *International Journal of Satellite Communications and Networking*, 2017.

[26] O. Kodheli, A. Guidotti, and A. Vanelli-Coralli, "Integration of satellites in 5G through LEO constellations," in *IEEE Global Communications Conference (GLOBECOM 2017)*, 2017, pp. 1–6. DOI: 10.1109/GLOCOM.2017.8255103.

[27] 3GPP, "Study on New Radio (NR) to support non-terrestrial networks (NTNs)," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.811, 2020, Version 15.2.0, Release 15.

[28] C. B. Mwakwata, H. Malik, M. Mahtab Alam, Y. Le Moullec, S. Parand, and S. Mumtaz, "Narrowband Internet of Things (NB-IoT): From physical (PHY) and media access control (MAC) layers perspectives," *Sensors*, vol. 19, no. 11, p. 2613, 2019.

[29] 3GPP, "[IoT-NTN] Applicability of TR 38.821 (MediaTek)," 3rd Generation Partnership Project (3GPP), Discussion, Decision R2-2011275, Nov. 2020, RAN WG2 112e.

[30] 3GPP, "Solutions for NR to support Non-Terrestrial Networks (NTN)," 3rd Generation Partnership Project (3GPP), Technical report (TR) 38.821, 2019, Release 16.

[31] F. Rinaldi, H. .-. Maattanen, J. Torsner, *et al.*, "Non-Terrestrial Networks in 5G Beyond: A Survey," *IEEE Access*, vol. 8, pp. 165 178–165 200, 2020. DOI: 10.1109/ACCESS.2020.3022981.

[32] ITU, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond," International Telecommunication Union (ITU), Recommendation 2083-0, 2015, ITU-R M.2083-0.

[33] R. Birkeland and D. Palma, "An assessment of IoT via satellite: Technologies, Services and Possibilities," in *International Astronautical Congress, Washington D.C*, Oct. 2019.

[34] O. Liberg, S. E. Löwenmark, S. Euler, *et al.*, "Narrowband internet of things for non-terrestrial networks," *arXiv preprint arXiv:2010.04906*, 2020.

[35] O. Kodheli, S. Andrenacci, N. Maturo, S. Chatzinotas, and F. Zimmer, "Resource Allocation Approach for Differential Doppler Reduction in NB-IoT over LEO Satellite," in *Proc. of IEEE Advanced Satellite Multimedia Systems Conference and the 15th Signal Processing for Space Communications Workshop (ASMS/SPSC)*, 2018, pp. 1–8. DOI: 10.1109/ASMS-SPSC.2018.8510724.

[36] S. Cluzel, M. Dervin, J. Radzik, S. Cazalens, C. Baudoin, and D. Dragomirescu, "Physical layer abstraction for performance evaluation of leo satellite systems for iot using time-frequency aloha scheme," in *Proc. of IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2018, pp. 1076–1080. DOI: 10.1109/GlobalSIP.2018.8646372.

[37] M. Gineste, T. Deleu, M. Cohen, *et al.*, "Narrowband IoT Service Provision to 5G User Equipment via a Satellite Component," in *Proc. of IEEE Globecom Workshops (GC Wkshps)*, 2017, pp. 1–4. DOI: 10.1109/GLOCOMW.2017.8269209.

[38] J. Doré and V. Berg, "Turbo-FSK: A 5G NB-IoT Evolution for LEO Satellite Networks," in *Proc. of IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2018, pp. 1040–1044. DOI: 10.1109/GlobalSIP.2018.8646371.

[39] S. Martiradonna, A. Grassi, G. Piro, and G. Boggia, "5g-air-simulator: An open-source tool modeling the 5g air interface," *Computer Networks*, vol. 173, no. 107151, 2020. DOI: 10.1016/j.comnet.2020.107151.

[40] G. Aiyetoro and P. Owolawi, "Spectrum Management Schemes for Internet of Remote Things (IoRT) Devices in 5G Networks via GEO Satellite," *Future Internet*, vol. 11, no. 12, p. 257, 2019.

[41] G. Aiyetoro and P. Owolawi, "Dynamic Packet Scheduling for Internet of Remote Things (IoRT) devices in 5G Satellite Networks," in *Proc. of IEEE International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2020, pp. 1–6. DOI: 10.1109/ICACCE49060.2020.9154993.

[42] C. A. Balanis, *Antenna Theory: Analysis and Design, 2nd Edition*. Wiley, 1996.

[43] L. J.Ippolito, *Satellite Communications Systems Engineering: Atmospheric Effects, Satellite Link Design and System Performance*, 2nd. Wiley Publishing, 2017, ISBN: 1119259371.

[44] 3GPP, "Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT)," 3rd Generation Partnership Project (3GPP), Technical report (TR) 45.820, 2015, Release 13.

[45] T. Ojha, S. Misra, and N. Raghuwanshi, "Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges," *Comput. Electron. Agric.*, vol. 118, pp. 66–84, 2015.

[46] K. Goel and A. K. Bindal, "Wireless sensor network in precision agriculture: A survey report," in *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, 2018, pp. 176–181. DOI: 10.1109/PDGC.2018.8745854.

[47] G. Castellanos, M. Deruyck, L. Martens, and W. Joseph, "System assessment of wusn using nb-iot uav-aided networks in potato crops," *IEEE Access*, vol. 8, pp. 56 823–56 836, 2020. DOI: 10.1109/ACCESS.2020.2982086.

[48] *Satellite technologies for IoT applications*, https://iotuk.org.uk/wp-content/uploads/2017/04/Satellite-Applications.pdf, Accessed: 2019-01-29.

[49] *Development guide for agriculture using NB-IoT*, https://www.gsma.com/iot/resources/guide2-nbiot-agriculture, Accessed: 2018-10-05.

[50] H. Jawad, R. Nordin, S. Gharghan, A. Jawad, and M. Ismail, "Energy-Efficient Wireless Sensor Networks for Precision Agriculture: A Review," *Sensors*, vol. 17, no. 8, 2017, ISSN: 1424-8220. DOI: 10.3390/s17081781. [Online]. Available: https://www.mdpi.com/1424-8220/17/8/1781.

[51] D. Brunelli, A. Albanese, D. d'Acunto, and M. Nardello, "Energy neutral machine learning based iot device for pest detection in precision agriculture," *IEEE Internet of Things Magazine*, vol. 2, no. 4, pp. 10–13, 2019. DOI: 10.1109/IOTM.0001.1900037.

[52] M. M. Islam, M. S. Hossain, R. K. Reza, and A. Nath, "Iot based automated solar irrigation system using mqtt protocol in charandeep chakaria," in *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, 2019, pp. 1–6. DOI: 10.1109/ICASERT.2019.8934504.

[53] R. Maheswari, H. Azath, P. Sharmila, and S. Sheeba Rani Gnanamalar, "Smart village: Solar based smart agriculture with iot enabled for climatic change and fertilization of soil," in *2019 IEEE 5th International Conference on Mechatronics System and Robots (ICMSR)*, 2019, pp. 102–105. DOI: 10.1109/ICMSR.2019.8835454.

[54] J. P. Shanmuga Sundaram, W. Du, and Z. Zhao, "A survey on lora networking: Research problems, current solutions, and open issues," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 371–388, 2020. DOI: 10.1109/COMST.2019.2949598.

[55] GSMA, "NB-IoT deployment guide to basic feature set requirements," GSM Association et al., Tech. Rep., 2019. [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2019/07/201906-GSMA-NB-IoT-Deployment-Guide-v3.pdf.

[56] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.401, 2020, Release 16.

[57] Z. Shelby, K. Hartke, and C. Bormann, *The Constrained Application Protocol (CoAP)*, RFC 7252, Jun. 2014. DOI: 10.17487/RFC7252. [Online]. Available: https://rfc-editor.org/rfc/rfc7252.txt.

[58] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification," 3rd Generation Partnership Project (3GPP), Technical Report (TS) 36.323, 2020, Release 16.

[59] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Link Control (RLC) protocol specification," 3rd Generation Partnership Project (3GPP), Technical Report (TS) 36.322, 2020, Release 16.

[60] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA) Medium Access Control (MAC) protocol specification," 3rd Generation Partnership Project (3GPP), Technical Report (TS) 36.321, 2020, Release 16.

[61] 3GPP, "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures," 3rd Generation Partnership Project (3GPP), Technical Report (TR) 36.213, 2020, Release 14.

[62] 3GPP, "FL Summary on enhancements on UL time and frequency synchronization for NR NTN," 3rd Generation Partnership Project (3GPP), Discussion, Decision R1-2009748, Nov. 2020, RAN WG1 103e.

[63] ITU, "Attenuation by atmospheric gases and related effects," International Telecommunication Union (ITU), Recommendation, 2019, ITU-R P.676-12.

[64] ITU, "Propagation data and prediction methods required for the design of Earth-space telecommunication systems," International Telecommunication Union (ITU), Recommendation, 2017, ITU-R P.618-13.

[65] ITU, "Characteristics of precipitation for propagation modelling," International Telecommunication Union (ITU), Recommendation, 2021, ITU-R P.837-7.

[66] ITU, "Attenuation due to clouds and fog," International Telecommunication Union (ITU), Recommendation, 2019, ITU-R P.840-8.

[67] ITU, "Propagation data and prediction methods required for the design of Earth-space telecommunication systems," International Telecommunication Union, Tech. Rep., 2015, Recommendations Radiowave Propag. ITU-R 618-12.

[68] N. Grody, "Antenna temperature for a scanning microwave radiometer," *IEEE Transactions on Antennas and Propagation*, vol. 23, no. 1, pp. 141–144, 1975. DOI: 10.1109/TAP.1975.1141020.

[69] *Payload Specification for 3U, 6U, 12U and 27U*, http://www.planetarysystemscorp.com/web/wp-content/uploads/2017/08/2002367E-Payload-Spec-for-3U-6U-12U-27U.pdf, Accessed: 2020-12-10.

[70] *Satellite Design and Operations*, https://www.agi.com/missions/satellite-missions-design, Accessed: 2020-12-10.

[71] S. Martiradonna, A. Grassi, G. Piro, and G. Boggia, "Understanding the 5G-Air-simulator: A tutorial on design criteria, technical components, and reference use cases," *Computer Networks*, vol. 177, p. 107 314, 2020, ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2020.107314.

[72] S. Martiradonna, G. Piro, and G. Boggia, "On the evaluation of the nb-iot random access procedure in monitoring infrastructures," *Sensors*, vol. 19, no. 14, p. 3237, 2019.

[73] ITU, "Topography for Earth-to-space propagation modelling," International Telecommunication Union (ITU), Recommendation, 2019, ITU-R P.1511.

[74] 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," *Computer Networks*, vol. 56, Nov. 2012. DOI: 10.1016/j.comnet.2012.07.010.

[75] L. Atzori, A. Iera, and G. Morabito, "From "smart objects" to "social objects": The next evolutionary step of the internet of things," *IEEE Communications Magazine*, vol. 52, no. 1, pp. 97–105, 2014. DOI: 10.1109/MCOM.2014.6710070.

[76] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, and Q. Arshad, "When social objects collaborate: Concepts, processing elements, attacks and challenges," *Computers and Electrical Engineering*, vol. 58, pp. 397–411, 2017, ISSN: 0045-7906. DOI: https://doi.org/10.1016/j.compeleceng.2016.11.014.

[77] W. Z. Khan, Q. .-. .-. Arshad, S. Hakak, M. K. Khan, and Saeed-Ur-Rehman, "Trust management in social internet of things: Architectures, recent advancements and future challenges," *IEEE Internet of Things Journal*, pp. 1–1, 2020. DOI: 10.1109/JIOT.2020.3039296.

[78] A. M. Esfahani, A. M. Rahmani, and A. Khademzadeh, "Msiot: Mobile social internet of things, a new paradigm," in *2020 10th International Symposium onTelecommunications (IST)*, 2020, pp. 187–193. DOI: 10.1109/IST50524.2020.9345837.

[79] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019. DOI: 10.1109/JIOT.2018.2836144.

[80] H. Zhang, L. Zhu, H. Du, *et al.*, "Structural balance of social internet of things networks with ambiguous relationships," *Wireless Communications and Mobile Computing*, vol. 2021, p. 7 964 409, Aug. 2021, ISSN: 1530-8669. DOI: 10.1155/2021/7964409.

[81] A. Tewari and B. Gupta, "Security, privacy and trust of different layers in internet-of-things (iots) framework," *Future Generation Computer Systems*, vol. 108, pp. 909–920, 2020, ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2018.04.027.

[82] G. Sciddurlo, I. Huso, D. Striccoli, G. Piro, and G. Boggia, "A multi-tiered social iot architecture for scalable and trusted service provisioning," in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 1–6. DOI: 10.1109/GLOBECOM46510.2021.9685084.

[83] G. Sciddurlo, A. Petrosino, D. Striccoli, G. Piro, L. A. Grieco, and G. Boggia, "Boosting service provisioning in siot by exploiting trust and capability levels of social objects," in *2022 IEEE International Conference on Smart Computing (SMARTCOMP)*, 2022, pp. 1–6. DOI: 10.1109/SMARTCOMP55677.2022.00077.

[84] R. Faqihi, D. Ramakrishnan, and D. Mavaluru, "An evolutionary study on the threats, trust, security, and challenges in siot (social internet of things)," *Materials today: proceedings*, Nov. 2020. DOI: 10.1016/j.matpr.2020.09.618.

[85] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266, 2014. DOI: 10.1109/TKDE.2013.105.

[86] A. Zannou, A. Boulaalam, and E. H. Nfaoui, "Siot: A new strategy to improve the network lifetime with an efficient search process," *Future Internet*, vol. 13, no. 1, 2021, ISSN: 1999-5903. DOI: 10.3390/fi13010004.

[87] L. Wei, J. Wu, C. Long, and B. Li, "On designing context-aware trust model and service delegation for social internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4775–4787, 2021. DOI: 10.1109/JIOT.2020.3028380.

[88] B. Farahbakhsh, A. Fanian, and M. H. Manshaei, "TGSM: Towards trustworthy group-based service management for social IoT," *Internet of Things*, vol. 13, p. 100 312, 2021, ISSN: 2542-6605. DOI: https://doi.org/10.1016/j.iot.2020.100312.

[89] Y. Yi, Z. Zhang, L. T. Yang, X. Deng, L. Yi, and X. Wang, "Social interaction and information diffusion in social internet of things: Dynamics, cloud-edge, traceability," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2177–2192, 2021. DOI: 10.1109/JIOT.2020.3026995.

[90] M. Amiri-Zarandi and R. A. Dara, "Blockchain-based trust management in social internet of things," in *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing*, 2020, pp. 49–54. DOI: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00024.

[91] Z. Chen, R. Ling, C.-M. Huang, and X. Zhu, "A scheme of access service recommendation for the social internet of things," *International Journal of Communication Systems*, vol. 29, no. 4, pp. 694–706, 2016. DOI: https://doi.org/10.1002/dac.2930.

[92] R. K. Chahal, N. Kumar, and S. Batra, "Trust management in social internet of things: A taxonomy, open issues, and challenges," *Computer Communications*, vol. 150, pp. 13–46, 2020, ISSN: 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2019.10.034.

[93] A. Metrouh, "Social internet of things: A novel selection approach for dynamic resources substitution," *Evolutionary Intelligence*, Jun. 2021. DOI: 10.1007/s12065-021-00580-3.

[94] B. Bordel and R. Alcarria, "Distributed trust and reputation services in pervasive internet-of-things deployments," in *International Symposium on Mobile Internet Security*, Springer, 2021, pp. 16–29.

[95] R. Abidi and N. B. Azzouna, "Self-adaptive trust management model for social iot services," in *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, 2021, pp. 1–7. DOI: 10.1109/ISNCC52172.2021.9615856.

[96] W. Abdelghani, I. Amous, C. A. Zayani, F. Sèdes, and G. Roman-Jimenez, "Dynamic and scalable multi-level trust management model for social internet of things," *The Journal of Supercomputing*, Jan. 2022, ISSN: 1573-0484. DOI: 10.1007/s11227-021-04205-5.

[97] M. O. Ojo, S. Giordano, G. Procissi, and I. N. Seitanidis, "A review of low-end, middle-end, and high-end iot devices," *IEEE Access*, vol. 6, pp. 70 528–70 554, 2018. DOI: 10.1109/ACCESS.2018.2879615.

[98] G. Zhang, F. Shen, Y. Zhang, R. Yang, Y. Yang, and E. A. Jorswieck, "Delay minimized task scheduling in fog-enabled iot networks," in *2018 10th International Conference on Wireless Communications and Signal Processing (WCSP)*, 2018, pp. 1–6. DOI: 10.1109/WCSP.2018.8555532.

[99] T. Hoßfeld, L. Skorin-Kapov, P. E. Heegaard, and M. Varela, "Definition of qoe fairness in shared systems," *IEEE Communications Letters*, vol. 21, no. 1, pp. 184–187, 2016.

[100] F. de Trizio, G. Sciddurlo, G. Piro, D. Striccoli, I. Cianci, and G. Boggia, "Surviving disaster events via dynamic In-Network processing assisted by network digital twins," in *International Conference on Information and Communication Technologies for Disaster Management (ICT-DM) (ICT-DM'23)*, Cosenza, Italy, Sep. 2023, p. 5.95.

[101] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "Lvbs: Lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 19–32, 2022. DOI: 10.1109/TDSC.2020.2980255.

[102] T. Toby, U. Gopalakrishnan, and S. N. Rao, "A survey of deep learning techniques based on drone images for the search and rescue of victims from collapsed structures," in *2022 IEEE 19th India Council International Conference (INDICON)*, 2022, pp. 1–6. DOI: 10.1109/INDICON56171.2022.10040123.

[103] F. Mezghani and N. Mitton, "The potential of cooperative communications to speed up disaster relief operations," in *2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, 2019, pp. 1–6. DOI: 10.1109/ICT-DM47966.2019.9032963.

[104] A. Mukherjee, D. De, N. Dey, R. G. Crespo, and E. Herrera-Viedma, "Disastdrone: A disaster aware consumer internet of drone things system in ultra-low latent 6g network," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 1, pp. 38–48, 2023. DOI: 10.1109/TCE.2022.3214568.

[105] M. Terzi, A. Anastasiou, P. Kolios, C. Panayiotou, and T. Theocharides, "Swifters: A multi-uav platform for disaster management," in *2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, 2019, pp. 1–7. DOI: 10.1109/ICT-DM47966.2019.9032923.

[106] S. Ganesh, V. Gopalasamy, and N. B. Sai Shibu, "Architecture for drone assisted emergency ad-hoc network for disaster rescue operations," in *2021 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 2021, pp. 44–49. DOI: 10.1109/COMSNETS51098.2021.9352814.

[107] B. Li, Y. Liu, L. Tan, H. Pan, and Y. Zhang, "Digital twin assisted task offloading for aerial edge computing and networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 10, pp. 10 863–10 877, 2022. DOI: 10.1109/TVT.2022.3182647.

[108] X. Yuan, J. Chen, N. Zhang, J. Ni, F. R. Yu, and V. C. M. Leung, "Digital twin-driven vehicular task offloading and irs configuration in the internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 24 290–24 304, 2022. DOI: 10.1109/TITS.2022.3204585.

[109] D. Van Huynh, V.-D. Nguyen, S. R. Khosravirad, *et al.*, "Urllc edge networks with joint optimal user association, task offloading and resource allocation: A digital twin approach," *IEEE Transactions on Communications*, vol. 70, no. 11, pp. 7669–7682, 2022. DOI: 10.1109/TCOMM.2022.3205692.

[110] X. Xu, Z. Liu, M. Bilal, S. Vimal, and H. Song, "Computation offloading and service caching for intelligent transportation systems with digital twin," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 11, pp. 20 757–20 772, 2022. DOI: 10.1109/TITS.2022.3190669.

[111] T. Meuser, L. Baumgärtner, and B. Becker, "Netskylines: Digital twins for evaluating disaster communication," in *2021 IEEE Global Humanitarian Technology Conference (GHTC)*, 2021, pp. 68–71. DOI: 10.1109/GHTC53159.2021.9612413.

[112] M. Khan, R. Chinnaiyan, S. Balachandar, *et al.*, "Centralized and reliable digital twin models for smart city's buildings protection during disaster," in *2022 International Conference on Computational Modelling, Simulation and Optimization (ICCMSO)*, 2022, pp. 226–229. DOI: 10.1109/ICCMSO58359.2022.00053.

[113] ITU-T, "Network 2030 - Architecture Framework," ITU-T Telecommunication Standardization Sector of ITU, Technical Report (TR), 2020, ITU-T Recommendation FG-NET2030-Arch(2020).

[114] K. Mehmood, K. Kralevska, and D. Palma, "Intent-driven autonomous network and service management in future cellular networks: A structured literature review," *Computer Networks*, vol. 220, p. 109 477, 2023, ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2022.109477. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128622005114.

[115] H. Mei and L. Peng, "On multi-robot data collection and offloading for space-aerial-surface computing," *IEEE Wireless Communications*, vol. 30, no. 2, pp. 90–96, 2023. DOI: 10.1109/MWC.005.2200400.

[116] G. Aiello, F. Hopps, D. Santisi, and M. Venticinque, "The employment of unmanned aerial vehicles for analyzing and mitigating disaster risks in industrial sites," *IEEE Transactions on Engineering Management*, vol. 67, no. 3, pp. 519–530, 2020. DOI: 10.1109/TEM.2019.2949479.

[117] Y. Wang, W. Chen, T. H. Luan, *et al.*, "Task offloading for post-disaster rescue in unmanned aerial vehicles networks," *IEEE/ACM Transactions on Networking*, vol. 30, no. 4, pp. 1525–1539, 2022. DOI: 10.1109/TNET.2022.3140796.

[118] J. Zhang, J. F. Campbell, D. C. Sweeney II, and A. C. Hupman, "Energy consumption models for delivery drones: A comparison and assessment," *Transportation Research Part D: Transport and Environment*, vol. 90, p. 102 668, 2021, ISSN: 1361-9209. DOI: https://doi.org/10.1016/j.trd.2020.102668.

[119] S. Murtuza, "Internet of everything: Application and various challenges analysis a survey," in *2022 1st International Conference on Informatics (ICI)*, 2022, pp. 250–252. DOI: 10.1109/ICI53355.2022.9786891.

[120] A. J. Chinchawade and O. S. Lamba, "Authentication schemes and security issues in internet of everything (ioe) systems," in *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2020, pp. 342–345. DOI: 10.1109/CICN49253.2020.9242569.

[121] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015. DOI: 10.1109/ACCESS.2015.2437951.

[122] K. M. Alam, M. Saini, and A. E. Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015. DOI: 10.1109/ACCESS.2015.2416657.

[123] A. Kirimtat, O. Krejcar, A. Kertesz, and M. F. Tasgetiren, "Future trends and current state of smart city concepts: A survey," *IEEE Access*, vol. 8, pp. 86 448–86 467, 2020. DOI: 10.1109/ACCESS.2020.2992441.

[124] M. Fadda, M. Anedda, R. Girau, G. Pau, and D. D. Giusto, "A social internet of things smart city solution for traffic and pollution monitoring in cagliari," *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2373–2390, 2023. DOI: 10.1109/JIOT.2022.3211093.

[125] C.-H. Hsu, C. E. Montenegro Marin, R. Gonzalez Crespo, and H. F. Mohamed El-sayed, "Guest editorial introduction to the special section on social computing and social internet of things," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 3, pp. 947–949, 2022. DOI: 10.1109/TNSE.2022.3167460.

[126] V. Sharma, I. You, D. N. K. Jayakody, and M. Atiquzzaman, "Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social internet of things," *Future Generation Computer Systems*, vol. 92, pp. 758–776, 2019, ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2017.12.039.

[127] M. Nitti, L. Atzori, and I. P. Cvijikj, "Friendship selection in the social internet of things: Challenges and possible strategies," *IEEE Internet of Things Journal*, vol. 2, no. 3, pp. 240–247, 2015. DOI: 10.1109/JIOT.2014.2384734.

[128] C. Boudagdigue, A. Benslimane, A. Kobbane, and M. Elmachkour, "A distributed advanced analytical trust model for iot," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–6. DOI: 10.1109/ICC.2018.8422726.

[129] G. Joshi and V. Sharma, "Light-weight hidden markov trust evaluation model for iot network," in *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2021, pp. 142–149. DOI: 10.1109/I-SMAC52330.2021.9640885.

[130] E. Wang, C. Chen, D. Zhao, W. Ip, and K. Yung, "A dynamic trust model in internet of things," *Soft Computing*, vol. 24, no. 8, pp. 5773–5782, Apr. 2020, ISSN: 1432-7643. DOI: 10.1007/s00500-019-04319-2.

[131] Y. Chen, M. Zhou, Z. Zheng, and D. Chen, "Time-aware smart object recommendation in social internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2014–2027, 2020. DOI: 10.1109/JIOT.2019.2960822.

[132] Z. U. Shamszaman and M. I. Ali, "Toward a smart society through semantic virtual-object enabled real-time management framework in the social internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2572–2579, 2018. DOI: 10.1109/JIOT.2017.2779106.

[133] A. Souri, Y. Zhao, M. Gao, A. Mohammadian, J. Shen, and E. Al-Masri, "A trust-aware and authentication-based collaborative method for resource management of cloud-edge computing in social internet of things," *IEEE Transactions on Computational Social Systems*, pp. 1–10, 2023. DOI: 10.1109/TCSS.2023.3241020.

[134] C. Fu, Q. Li, M. Shen, and K. Xu, "Frequency domain feature based robust malicious traffic detection," *IEEE/ACM Transactions on Networking*, vol. 31, no. 1, pp. 452–467, 2023. DOI: 10.1109/TNET.2022.3195871.

[135] G.Fink, *Markov models for pattern recognition: from theory to applications*. Springer, 2014. DOI: https://doi.org/10.1007/978-3-540-71770-6.