



ICSNC 2025

The Twentieth International Conference on Systems and Networks
Communications

ISBN: 978-1-68558-297-5

September 28th - October 2nd, 2025

Lisbon, Portugal

ICSNC 2025 Editors

Eugen Borcoci, National University of Science and Technology POLITEHNICA
Bucuresti (UNSTPB), Romania

ICSNC 2025

Forward

The Twentieth International Conference on Systems and Networks Communications (ICSNC 2025), held on September 28 – October 1, 2025 in Lisbon, Portugal, continued a series of events covering a broad spectrum of systems and networks related topics.

As a multi-track event, ICSNC 2025 served as a forum for researchers from the academia and the industry, professionals, standard developers, policy makers and practitioners to exchange ideas. The conference covered fundamentals on wireless, high-speed, mobile and Ad hoc networks, security, policy based systems and education systems. Topics targeted design, implementation, testing, use cases, tools, and lessons learnt for such networks and systems

The conference had the following tracks:

- TRENDS: Advanced features
- WINET: Wireless networks
- HSNET: High speed networks
- SENET: Sensor networks
- MHNET: Mobile and Ad hoc networks
- AP2PS: Advances in P2P Systems
- MESH: Advances in Mesh Networks
- VENET: Vehicular networks
- RFID: Radio-frequency identification systems
- SESYS: Security systems
- MCSYS: Multimedia communications systems
- POSYS: Policy-based systems
- PESYS: Pervasive education system

We welcomed technical papers presenting research and practical results, position papers addressing the pros and cons of specific proposals, such as those being discussed in the standard forums or in industry consortiums, survey papers addressing the key problems and solutions on any of the above topics, short papers on work in progress, and panel proposals.

We take here the opportunity to warmly thank all the members of the ICSNC 2025 technical program committee as well as the numerous reviewers. The creation of such a broad and high quality conference program would not have been possible without their involvement. We also kindly thank all the authors that dedicated much of their time and efforts to contribute to the ICSNC 2025. We truly believe that thanks to all these efforts, the final conference program consists of top quality contributions.

This event could also not have been a reality without the support of many individuals, organizations and sponsors. We also gratefully thank the members of the ICSNC 2025 organizing committee for their help in handling the logistics and for their work that is making this professional meeting a success. We gratefully appreciate to the technical program committee co-chairs that contributed to identify the appropriate groups to submit contributions.

We hope the ICSNC 2025 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in networking and systems communications research. We also hope that Lisbon provided a pleasant environment during the conference and everyone saved some time for exploring this beautiful city

ICSNC 2025 General Chair

Jaime Lloret Mauri, Polytechnic University of Valencia, Spain

ICSNC 2025 Steering Committee

Marc Kurz, University of Applied Sciences Upper Austria, Faculty for Informatics, Communications and Media, Austria

Jin-Shyan Lee, National Taipei University of Technology (Taipei Tech.), Taiwan

Rony Kumer Saha, BRAC University, Bangladesh

Eugen Borcoci, University Politehnica of Bucharest, Romania

ICSNC 2025 Publicity Chair

Lorena Parra Boronat, Universidad Politécnica de Madrid, Spain

Sandra Viciano Tudela, Universitat Politecnica de Valencia, Spain

Jose Miguel Jimenez, Universitat Politecnica de Valencia, Spain

ICSNC 2025

Committee

ICSNC 2025 General Chair

Jaime Lloret Mauri, Polytechnic University of Valencia, Spain

ICSNC 2025 Steering Committee

Marc Kurz, University of Applied Sciences Upper Austria, Faculty for Informatics, Communications and Media, Austria

Jin-Shyan Lee, National Taipei University of Technology (Taipei Tech.), Taiwan

Rony Kumer Saha, BRAC University, Bangladesh

Eugen Borcoci, University Politehnica of Bucharest, Romania

ICSNC 2025 Publicity Chair

Lorena Parra Boronat, Universidad Politécnica de Madrid, Spain

Sandra Viciano Tudela, Universitat Politecnica de Valencia, Spain

Jose Miguel Jimenez, Universitat Politecnica de Valencia, Spain

ICSNC 2025 Technical Program Committee

Maysam Abbod, Brunel University London, UK

Ahmed M. Abdelmoniem, KAUST, Saudi Arabia

Abdelkader Ait Abdelouahad, Chouaib Doukkali University, Morocco

Baadache Abderrahmane, University of Benyoucef Benkhadda, Algeria

Ishtiaq Ahmad, University of South Australia, Australia

S. Arnaud R. M. Ahouandjinou, University of Abomey-Calavi (UAC) / Coastal Opal University (ULCO), France

Lucio Agostinho Rocha, Federal University of Technology Paraná (UTFPR), Brazil

Francisco Airton Silva, Universidade Federal do Piauí, Brazil

Zahid Akhtar, State University of New York Polytechnic Institute, USA

Pedro Ákos Costa, NOVA University of Lisbon & NOVALINCS, Portugal

Abdullah Al-Alaj, Virginia Wesleyan University, USA

Adel Aldalbahi, KFUPM College of Engineering, Saudi Arabia

Osama Aloqaily, University of Ottawa, Canada

Abdallah A. Alshehri, Saudi Aramco, Dhahran, Saudi Arabia

Reem Alshahrani, Taif University, Saudi Arabia

Mohammed Al-Sarem, Taibah University, Saudi Arabia

Sarah Al-Shareeda, University of Bahrain, Bahrain

Mourad Amad, Bouira University, Algeria

Jonathan Ashdown, Air Force Research Laboratory, USA

Marios Avgeris, Carleton University, Ottawa, Canada

Muhammad Sohaib Ayub, Lahore University of Management Sciences (LUMS), Pakistan
V. Balasubramanian, Arizona State University, USA
Abu Barkat Ullah, University of Canberra, Australia
Ilija Basicovic, University of Novi Sad, Serbia
Mohamed Benmohammed, University Constantine2, Algeria
Clara Bertolissi, Aix-Marseille University | France Laboratoire d'Informatique et Systèmes (LIS CNRS), France
Robert Bestak, Czech Technical University in Prague, Czech Republic
Rui Bian, Expatiate Communications, USA
Muhammad Danial Bin Zakaria, Universiti Sultan Zainal Abidin, Malaysia
Razvan Bocu, Transilvania University of Brasov, Romania
Eugen Borcoci, National University of Science and Technology POLITEHNICA Bucharest, Romania
Alexandros-Apostolos A. Boulogeorgos, Aristotle University of Thessaloniki, Greece
Christos Bouras, University of Patras, Greece
Marilisa Botte, Federico II University of Naples, Italy
Anis Boubakri, ESPRIT, Tunisia
An Braeken, Vrije Universiteit Brussel, Belgium
Francesco Buccafurri, University of Reggio Calabria, Italy
Dumitru Dan Burdescu, University of Craiova, Romania
Eduardo Castilho Rosa, Goiano Federal Institute, Catalão Campus, Brazil
Yanni Chang, AVEVA, USA
Hao Che, University of Texas at Arlington, USA
Adil Chekati, University of Tunis El Manar, Tunisia
Fuxiang Chen, University of Leicester, UK
Dickson K.W. Chiu, University of Hong Kong, Hong Kong
Domenico Ciunzio, University of Naples "Federico II", Italy
Jorge A. Cobb, The University of Texas at Dallas, USA
Estefanía Coronado Calero, i2CAT Foundation, Spain
Fabio D'Andreagiovanni, CNRS - French National Centre for Scientific Research, France
Eronides da Silva Neto, CESAR Innovation Institute, Recife, Brazil
Monireh Dabaghchian, George Mason University, USA
Orhan Dagdeviren, Ege University | International Computer Institute, Turkey
Felipe S. Dantas Silva, Federal Institute of Education, Science, and Technology of RN (IFRN), Brazil
Saikat Das, Utah Valley University, Orem, USA
Vincenzo De Angelis, University of Reggio Calabria, Italy
Mehmet Demirci, Karadeniz Technical University, Turkey
Margot Deruyck, Ghent University - IMEC - WAVES, Belgium
Soumyabrata Dev, University College Dublin, Ireland
Omar Dib, Wenzhou-Kean University, China
Luis Diez, University of Cantabria, Spain
Rogério Dionísio, Polytechnic Institute of Castelo Branco, Portugal
Mustapha Djeddou, National Polytechnic School, Algiers, Algeria
Amir Djenna, University of Constantine, Algeria
Steve Eager, University of the West of Scotland, UK
Amna Eleyan, Manchester Metropolitan University, UK
Mohammed Eltayeb, California State University, Sacramento, USA
Müge Erel-Özçevik, Celal Bayar University, Turkey
Marcos Fagundes Caetano, University of Brasília, Brazil

Ramin Fouladi, Bogazici University, Istanbul, Turkey
Marco Furini, University of Modena and Reggio Emilia, Italy
Sonia Mettali Gammar, University of Manouba Tunis, Tunisia
Zhiwei Gao, Northumbria University, UK
Maggie E. Gendy, Arab Academy for Science, Technology and Maritime Transport - Communications and Networking, United Arab Emirates
Alireza Ghasempour, The University of New Mexico, USA
Katja Gilly de la Sierra-Llamazares, Universidad Miguel Hernández, Spain
Ariel Goes de Castro, Universidade Federal do Pampa, Brazil
Diogo Gomes, University of Aveiro, Portugal
Dalton Cézarne Gomes Valadares, Federal Institute of Pernambuco (IFPE), Brazil
Barbara Guidi, University of Pisa, Italy
Terry Guo, Tennessee Technological University, USA
Peter Haber, Salzburg University of Applied Sciences, Austria
Rushdi Hamamreh, Al-Quds University, Jerusalem
Khaled Hamoud, Université de Batna 2, Algeria
Luoyao Hao, Columbia University, USA
Abdelkrim Haqiq, Hassan 1st University, Morocco
Shahriar Hasan, Mälardalen University, Sweden
Omar Hashash, Virginia Tech, USA
William "Chris" Headley, Ted & Karyn Hume Center for National Security / Virginia Polytechnic Institute & State University, USA
Shahram S. Heydari, Ontario Tech University, Canada
Md Shafaeat Hossain, Southern Connecticut State University, USA
Seyed Mohsen Hosseini, Polytechnic University of Bari, Italy
Xinyue Hu, University of Minnesota, Twin Cities, USA
Yuzhou Hu, ZTE Corporation, China
Maria Francesca Idone, University of Reggio Calabria, Italy
Farkhund Iqbal, College of Technological Innovation, Abu Dhabi, UAE
Faouzi Jaidi, University of Carthage | Higher School of Communications of Tunis & National School of Engineers of Carthage, Tunisia
Dorota Jelonek, Czestochowa University of Technology, Poland
Jobish John, University College Cork, Ireland
Magnus Jonsson, Halmstad University, Sweden
Bijoy A. Jose, Cochin University of Science and Technology, India
Yasushi Kambayashi, Sanyo-Onoda City University, Japan
Faouzi Kamoun, ESPRIT School of Engineering, Tunis, Tunisia
Murizah Kassim, Universiti Teknologi MARA, Malaysia
Sokratis K. Katsikas, Norwegian University of Science and Technology, Norway
İlker Korkmaz, Izmir University of Economics, Turkey
Sondes Ksibi, University of Carthage | Higher School of Communications of Tunis, Tunisia
Lov Kumar, BITS-PILANI, Hyderabad, India
Sonal Kumari, Samsung R&D Institute, India
Marc Kurz, University of Applied Sciences Upper Austria, Austria
Cecilia Labrini, University of Reggio Calabria, Italy
Francesco G. Lavacca, Fondazione Ugo Bordoni, Italy
Sara Lazzaro, University of Reggio Calabria, Italy
Gyu Myoung Lee, Liverpool John Moores University, UK

Jin-Shyan Lee, National Taipei University of Technology (TAIPEI TECH), Taiwan
Wolfgang Leister, Norsk Regnesentral, Norway
João Leitão, NOVA School of Science and Technology | NOVA University of Lisbon & NOVA LINCS, Portugal
Kin K. Leung, Imperial College, UK
Yiu-Wing Leung, Hong Kong Baptist University, Kowloon Tong, Hong Kong
Chunmei Liu, National Institute of Standards and Technology, USA
Peng Liu, National Institute of Standards and Technology / Georgetown University, USA
Rafael Lopes Gomes, Universidade Estadual do Ceará (UECE), Brazil
Hui Lu, State University of New York (SUNY) at Binghamton, USA
Zhongqiang Luo, Sichuan University of Science and Engineering, China
Saida Maaroufi, École Polytechnique de Montréal, Canada
Kiran Makhijani, Futurewei, USA
Joe J. Mambretti, Northwestern University, USA
Zoubir Mammeri, IRT - Paul Sabatier University, Toulouse, France
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Johann M. Marquez-Barja, University of Antwerp - imec, Belgium
Akanksha Marwah, University of Delhi, India
Rashed Mazumder, Institute of Information Technology (IIT) | Jahangirnagar University, Bangladesh
Michael McGrath, Intel Labs, USA
Abdelkrim Meziane, Research Center on Scientific and Technical Information CERIST, Algeria
Lotfi Mhamdi, University of Leeds, UK
Claudio Miceli de Farias, Federal University of Rio de Janeiro, Brazil
Bashir Mohammed, Lawrence Berkeley National Laboratory, USA
Waldir Moreira, Fraunhofer Portugal AICOS, Portugal
Alireza Morsali, Humanitas Solutions, Canada
Abdelouahab Moussaoui, Ferhat Abbas University - Sétif 1, Algeria
Ranesh Kumar Naha, University of Tasmania, Australia
Ankur Nahar, Indian Institute of Technology, Jodhpur, India
Apurva Narayan, The University of British Columbia / University of Waterloo, Canada
Leila Nasraoui, University of Manouba, Tunisia
Amiya Nayak, University of Ottawa, Canada
Ranyelson Neres Carvalho, University of Brasília (UnB), Brazil
Prasad Netalkar, Qualcomm, USA
Christopher Nguyen, Intel Corp., USA
Huu-Nghia Nguyen, Montimage, Paris, France
Muath Obaidat, City University of New York, USA
Olusola Odeyomi, Wichita State University, USA
Luciana Oliveira, CEOS.PP ISCAP Polytechnic of Porto, Portugal
Alma Oračević, University of Bristol, UK
Achour Ouslimani, Quartz Laboratory - ENSEA, France
Grammati Pantziou, University of West Attica, Athens, Greece
Luciana Pereira Oliveira, Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Brazil
Ricardo José Pfitscher, Federal University of Rio Grande do Sul (UFRGS), Brazil
Kandaraj Piamrat, LS2N/University of Nantes, France
Paulo Pinto, Universidade Nova de Lisboa, Portugal
Vicent Pla, Universitat Politècnica de València, Spain
Mattia Quadrini, Romars s.r.l, Rome, Italy

Saulo Queiroz, Federal University of Technology - UTFPR, Ponta Grossa, Brazil
Raqeebir Rab, Ahsanullah University of Science and Technology, Bangladesh
Carlos Rabadão, Polytechnic of Leiria, Portugal
M. Mustafa Rafique, Rochester Institute of Technology, USA
Vittorio Rampa, Consiglio Nazionale delle Ricerche - Istituto di Elettronica, di Ingegneria dell'Informazione e delle Telecomunicazioni - Politecnico di Milano, Italy
Piotr Remlein, Poznan University of Technology, Poland
Leon Reznik, Rochester Institute of Technology, USA
Michele Roccotelli, Polytechnic University of Bari, Italy
Jose Manuel Rubio Hernan, Télécom SudParis, France
Rony Kumer Saha, BRAC University, Bangladesh
Dhaou Said, Sherbrooke University / Ottawa University, Canada
Damian San Roman Alerigi, Saudi Aramco, Saudi Arabia
Luis Enrique Sánchez Crespo, Universidad de Castilla-La Mancha, Spain
Bassem Sellami, University of Tunis El Manar, Tunisia
Sawsan Selmi, Higher School of Communication of Tunis, Tunisia
Fouzi Semchedine, University of Setif 1, Algeria
Alireza Shahrabi, Glasgow Caledonian University, Scotland, UK
Chen Shen, Georgetown University / National Institute of Standards and Technology, USA
Muhammad Shuaib Siddiqui, i2CAT Foundation, Spain
Rute C. Sofia, fortiss GmbH, Munich, Germany
Hazem Soliman, Arctic Wolf Networks, USA
Erik Sonnleitner, University of Applied Sciences Upper Austria, Austria
Wendley Souza da Silva, Federal University of Ceará (UFC), Brazil
Marco Aurelio Spohn, Federal University of Fronteira Sul (Universidade Federal da Fronteira Sul) - Chapeco/SC, Brazil
Alvaro Suárez Sarmiento, Universidad de Las Palmas de G. C., Spain
Young-Joo Suh, Pohang University of Science and Technology (POSTECH), Korea
Liyang Sun, New York University, USA
Do-Duy Tan, Ho Chi Minh City University of Technology and Education (HCMUTE), Vietnam
Getaneh Berie Tarekegn, National Taipei University of Technology, Taiwan
Sudeep Tanwar, Institute of Technology | Nirma University, India
Suresh Thanakodi, Universiti Pertahanan Nasional Malaysia, Malaysia
Vasileios Theodorou, Intracom Telecom, Greece
Behrad Toghi, University of Central Florida, USA
Michael W. Totaro, University of Louisiana at Lafayette, USA
Alex F. R. Trajano, Instituto Atlântico, Fortaleza, Brazil
Angelo Trotta, University of Bologna, Italy
Costas Vassilakis, University of the Peloponnese, Greece
Washington Velásquez, Escuela Superior Politécnica del litoral, Ecuador
Chengshuo Xu, University of California, Riverside, USA
Zhiying Xu, Harvard University, USA
Kun Yang, Zhejiang Ocean University, China
Abdulsalam Yassine, Lakehead University, Canada
Xizhe Yin, Siemens EDA, USA
Daqing Yun, Harrisburg University, USA
Habib Zaidi, Geneva University Hospital, Switzerland / University of Groningen, Netherlands / University of Southern Denmark, Denmark

Pavol Zavorsky, Framatome, Canada
Yunpeng (Jack) Zhang, University of Houston, USA
Kai Zhao, University of California, Riverside, USA
Yao Zhao, ShanghaiTech University, China
Yimeng Zhao, Facebook, USA
Gaoqiang Zhuo, Castlight Health, USA

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission to reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Implementing a Communications Infrastructure to Optimize Public Services for Communities <i>Maria-Georgiana Butaru and Eugen Borcoci</i>	1
---	---

Field Measurement of Multi-band Maritime 5G Communication in a Deep Sea Scenario <i>Hang Wu, Kun Yang, Jianjun Ding, Jinglong Lin, and Li Qin</i>	8
--	---

Implementing a Communications Infrastructure to Optimize Public Services for Communities

Maria-Georgiana Butaru
National University of Science and Technology
POLITEHNICA
Bucharest, Romania
e-mail: georgianabutaru8@gmail.com

Eugen Borcoci
National University of Science and Technology
POLITEHNICA
Bucharest, Romania
e-mail: eugen.borcoci@elcom.pub.ro

Abstract—A Wide Area Network (WAN) computer network can be frequently composed of several local and regional networks for the purpose of providing public services. All services can be integrated within a single physical location, using state-of-the-art technologies to ensure easy access to the information and to solve requests from citizens. It is essential to meet several types of requirements related to performance, scalability, security and reliability, in order to deliver a set of services at the highest standards. Opportunities of performing certain online services and processes for citizens should be also available, consequently eliminating the need of user physical presence in a remote location. In this paper, a variant of solution for integrating all services into one will be studied. Validation of the solution is performed, by simulating the communications network, in the framework Graphical Network Simulator-3 (GNS3). The communications equipment configurations, tests and troubleshooting of the implemented communications network will be experimented. The experience described in this paper could be useful for real life designers of communication infrastructures for services dedicated to communities.

Keywords - Wide Area Networks; services; communications; network security and scalability; communications protocols; connectivity; implementation tests; GNS3.

I. INTRODUCTION

Digitalization is undoubtedly an integral part of modern life, transforming the way we interact with the people around us and beyond. It gives us quick access to information, facilitates human connections and revolutionizes industries through constant innovation. At the same time, digitalization plays a crucial role in streamlining processes, reducing distances, barriers and the time required for various activities. In an increasingly globalized society, digital technologies allow us to adapt more easily, be more efficient and enjoy benefits that improve our daily lives [1].

In addition, communication technologies are also an indispensable in times of crisis (e.g., pandemics, meteorological events, emergency contexts) when citizens are provided with easy access to government information, forms or online services. GNS3 is an open-source software used for simulating computer networks which allows the creation and testing of simple or complex networks, with no need of physical equipment.

The objective of this paper is focused on the implementation of a communications network which is able to integrate all public services intended for citizens into a single physical location.

The purpose of the implemented network that includes all public services into a single location is to avoid citizens' movements between different locations that ensure the issuance of only one document, in this case all documents and information about obtaining a public service being available in a single location. In addition, this network minimizes the devices used in the communications infrastructure, eliminating the need to create many local networks at the county level for each public service. In this situation, all public services are integrated, which reduces the costs of their acquisition and maintenance.

This would be available in each county across the country while also having the possibility application submissions to be able to obtain or access a public service, online in an electronic format. Public services include obtaining an identity card, a health card, a criminal record, a passport or various certificates necessary in the flow for activities and being within the community. One of the benefits of such a network for citizens is the streamlining of the data flow at the level of this infrastructure in order to obtain a service. Additionally, optimization of performance is realized in relation to citizens (e.g., reduced time for submitting an application or minimizing the waiting time until the requested document is picked up). Streamlining the data flow is based on a system architecture composed of state-of-the-art equipment assuring high degree of performance that increases data flows through transmission capacity, as well as through bandwidth. The implementation of such a network can significantly contribute to the efficiency and accessibility of public services. At the county level, citizens will have the possibility of obtaining all public services from an integrated environment. The structure of the paper is summarized below.

Section II outlines the general technical requirements that must be met in order to implement the communications network, intended to ensure the performance, efficiency, security and availability of the services delivered. Section III specifies the architecture of the communication network and the analysis for the implementation of the communication

network. Section IV defines the simulation scenarios. Section V contains to the effective implementation of network and system equipment, including configuration, as well as the use of communication protocols to ensure interconnection between different points of the network. Different tests and their results are described. Section VI presents the main conclusions.

II. SYSTEM GENERAL REQUIREMENTS

In order to provide public services to citizens the implemented communications network should meet a series of technical functional and non-functional requirements, summarized below.

- Transmission capacity - ensuring sufficient bandwidth for those services that need a high rate of data transfer and reception.
- Resilience – implementing redundant solutions to ensure high service availability and prevent connectivity loss during unexpected events or failures. Redundancy is required both at the hardware level, and software level, in terms of configuring routes to minimize downtime [2].
- Security – implementing security measures at the firewall level within the communications network, as well as configuring access lists to prevent abusive access to data in the system.
- Quality of Service (QoS) – configuring QoS capabilities to prioritize some flows of the data traffic in order to ensure the appropriate quality of the public services offered.
- Service availability – the network will be able to provide services to end users without significant interruptions.

This feature is heavily influenced by the network infrastructure, with its redundancy, additionally, security measures designed for the network. A network and services management system will configure all the structure and then will check the fulfillment of the functional and performance requirements, by monitoring and reporting, making resource management and control, aiming to ensure a rapid response in case of urgent events.

To carry out the entire implementation of the communications network, it was necessary to configure the GNS3 simulator, consisting of a server installed on a virtual machine with the Linux-Ubuntu operating system, the virtual machine running on a computer with sufficient hardware resources. At the same time, for the full functioning of the simulator, its client was also installed, which connects to the Linux server hosted by the virtual machine.

To perform the configurations of the network equipment and the connections between them, IOS images were added for the devices used. In this infrastructure, IOS images were added for Cisco routers and switches, images for Windows 10 and Windows Server 2012, and lastly but not less

important images were added for the devices that ensure network security, the Fortinet firewalls

Thus, the images added to the simulator have the role of simulating real operating systems, which facilitates a controlled, flexible and optimal environment for the implementation of the infrastructure presented in the paper.

III. COMMUNICATIONS NETWORK ARCHITECTURE

The proposed system architecture is hierarchically organized; It consists of a WAN communications network, supposed to be implemented at the national level; it is composed of several local networks located at the county level. Several county networks will form a regional network that will connect the county networks and the data center that will connect the entire network (see Figure 1). At the region level there are border-type routers whose role is to centralize several counties, to create a restricted area and to ensure the connection to the central area of the network.

Through concentrators, all regions will be assimilated within the network. The networks at the county-level are interconnected to the data center through two hubs (Concentrator 1 and Concentrator 2, see Figure 2), configured in redundancy; subsequently, access to the data center will be achieved through external firewalls, the traffic being taken over by the routers and switches that connect the equipment outside and inside the communications network. On county-level networks (local networks), two pieces of equipment will be configured to create redundancy, but additionally on regional-level networks and data centers. The network infrastructure will assure all necessary connections to be implemented; the data center will have a „global” role, i.e., it will contain the administration servers and the monitoring servers. Being a sensitive environment for citizens’ data, implementation of security measures will be considered to limit access by unauthorized persons and protect personal data. A centralized solution has been selected to offer a strong security control. All data will only be stored only at the data center level at the central point of the network. At the county level, only network equipment will be used, as well as workstations to manage the data taken and to transmit it to the central point of the network.

To interconnect network devices at the county and regional network levels, dynamic routing protocols will be used, so connections between the county networks and the datacenter network are made through regional networks.

The creation of the network with the aim of providing public services to citizens will be done virtually, in the GNS3 network simulator. An important GNS3 advantage in validation studies of different architectures is its ability to support software images of real-life network devices (e.g., Cisco, Juniper, Fortinet) and images of operating systems (e.g., Windows, Linux) [3].

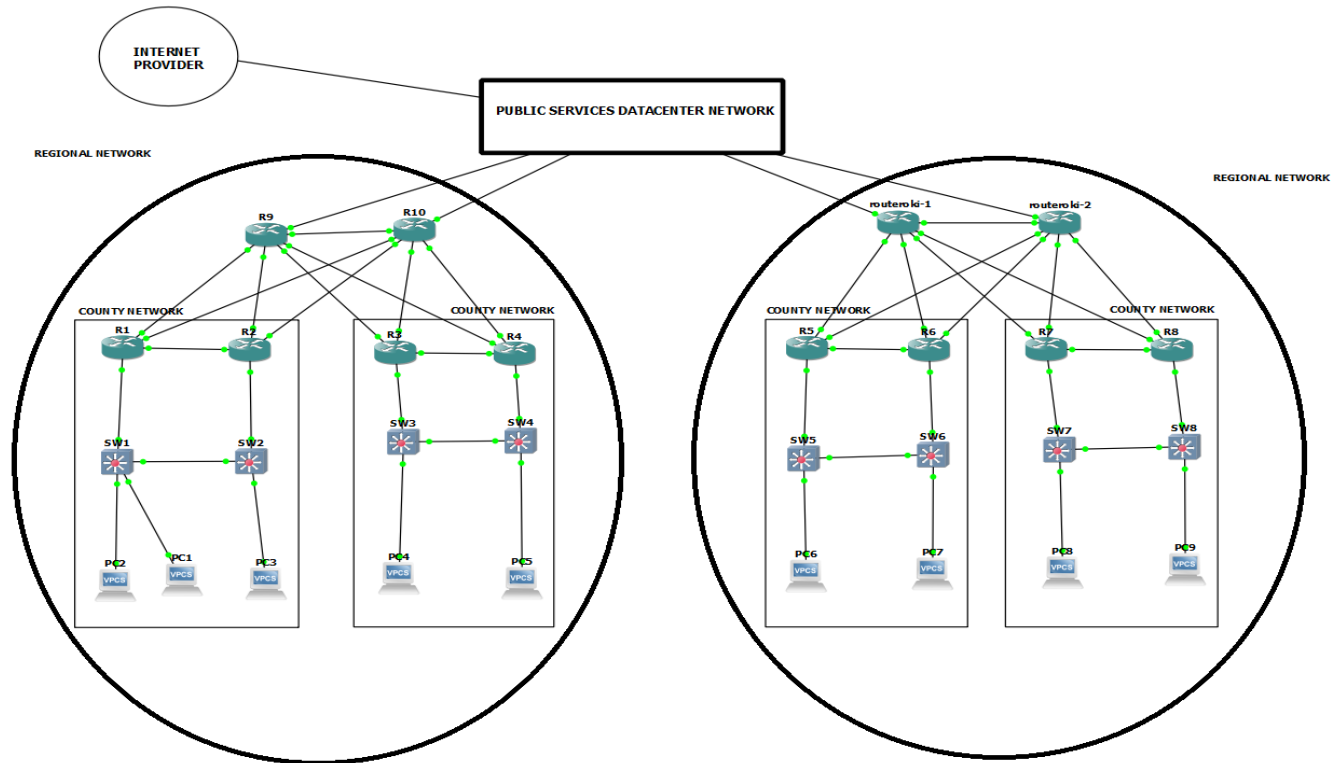


Figure 1 – Communication network at the analysis stage

IV. SIMULATION SCENARIOS

Communications network simulations are essential for testing and validating the performance, scalability and security of communications system. We considered several basic scenarios to be tested.

Scenario 1: Extending the network by increasing the number of devices connected to the network. Therefore, simulating scenarios on the configured network represents one of the most important stages in terms of creating a high-performance communications network.

Objectives: Assessing the scalability of the network and the ability to handle the increase in the number of connected devices.

Scenario 2: Modifying the network configuration to test the flexibility and stability of changes.

Objectives: Verifying how the network adapts to changes in topology and configuration. The purpose of changing equipment configuration is to test their stability and flexibility.

For these scenarios, their status will be visualized by monitoring the network.

The phases of this work were:

analysis of the requirements coming from both users and technical requirements; design the architecture and then the network infrastructure; identifying the solutions needed for the network equipment and their installation and configuration; based on the network topologies established for each part of the network, they are connected to each other, configured and routes are created to test the functionality of the network at the local level; after making the connections of the local network at the county level, the connections will be made, as well as the implementation of routes to the equipment in the regional area; this region aims to interconnect several counties.

The equipment at the regional level will make connections directly to the data center of this communications network. The data center has a three-tier topology, a WAN network consisting of two routers and two switches that interconnect external subnets and a Demilitarized Zone (DMZ) area that could be accessed both from the outside by citizens and internal network users.

These experiments and tests aim to validate the solution, in terms of scalability, flexibility and stability, before going to the real network implementation.

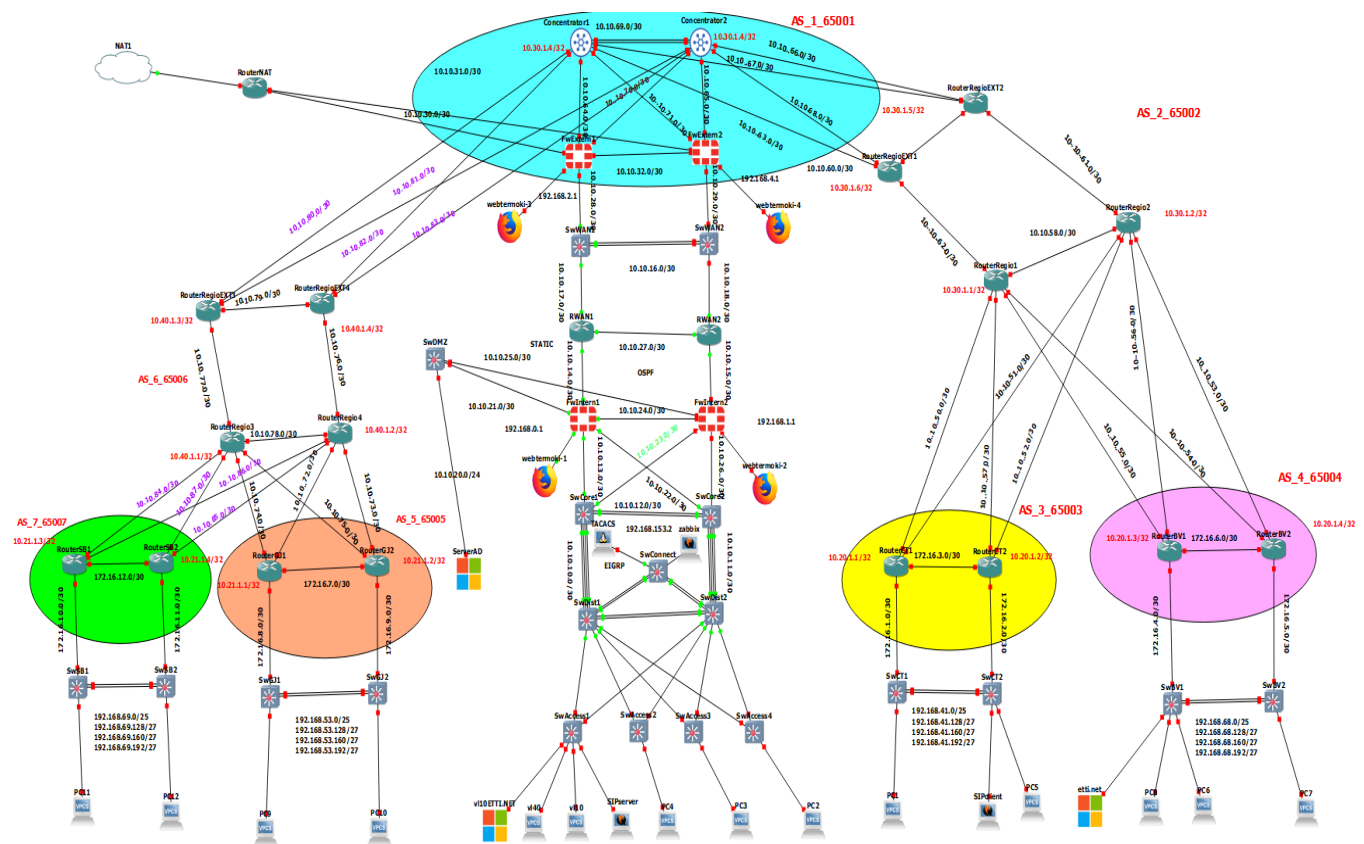


Figure 2 - The communication network implemented in GNS3 simulator

V. EXPERIMENTS AND RESULTS

According to the defined experiments and scenarios, the communication network was implemented in the simulator (see Figure 2). This network is a WAN, consisting of several Local Area Networks (LANs) and the data center network with a Three-Tier topology.

The Three-Tier topology is a well-established architecture used in network design, which provides a hierarchical structure, organized into three logical levels, with the aim of improving the performance of the implemented network.

It is composed of three main layers:

1. Access Layer: This is the base layer, in the three-tier topology that provides the initial connections to end users. Authentication, access control and traffic segmentation are handled at this layer.

2. Distribution Layer: It represents the second level of the topology and has the role of interconnecting the access level with the core level. At this area, routing policies, access filters, and other traffic control services, could be implemented.

3. Core Layer: This is the brain of the network, with functionalities focused on fast switching and transport

between different points in the network. The core layer is designed for high performance, ensuring maximum network availability [4].

The counties chosen as examples for these networks are (Romanian counties): Gorj, Brasov, Constanta and Sibiu.

A. Types of traffic. To distinguish the types of traffic in the communication flows within the network, several Virtual Local Area Networks (VLANs) were created, as follows:

- Vlan 10 – intended for intranet data traffic
- Vlan 20 – intended for internet traffic
- Vlan 30 – intended for voice traffic
- Vlan 40 – intended for network management

The configuration of VLANs is an important solution in modern network infrastructures, providing logical separation between subnets, guaranteeing increased flexibility and security. They are created at the switching equipment level to streamline the process of separating traffic categories [5].

B. Connections between physical locations. Each VLAN has an addressing plan, so traffic can be differentiated from

each other. The VLANs are configured in all LAN locations, and routes are configured between these local networks. The IP address classes assigned to VLANs have the role of carrying out the routing process through routing protocols within the network, so that users from different local networks can communicate with each other. Connectivity between them is ensured by several dynamic routing protocols. Therefore, at the LAN level, the dynamic routing protocol Enhanced Interior Gateway Routing Protocol (EIGRP) with message authentication is configured. The EIGRP routing protocol with message authentication ensures the security and stability of a network, protecting the process of information exchange between routers [6]. Authentication verifies the identity of participating routers, so that only authorized ones can communicate. This mechanism prevents the introduction of false data and maintains the integrity of routing information, which contributes to the proper functioning of the network [7].

Because the EIGRP routing protocol is developed by Cisco and within the topology, the network equipment is not unanimously Cisco, it was necessary to introduce another dynamic routing protocol to achieve connectivity between different vendors (Fortinet and Cisco in this case). Also, for some connectivity within the network, the well known dynamic routing link-state protocol Open Shortest Path First (OSPF) was selected (based on Dijkstra algorithm) which computes the most efficient routes in the network [8]. For WAN connections, between local networks and the data center, connectivity at the regional networks level was provided through Border Gateway Protocol (BGP) and Multiprotocol Label Switching (MPLS), forms the backbone of WAN connectivity in this implementation. BGP handles the exchange of routes between autonomous systems (AS), using flexible routing policies based on attributes such as path length, preference metric and other custom criteria [9].

Each LAN has its own AS in BGP, for better route control, isolating traffic between networks and preventing conflicts. Data and voice traffic arrive from local networks to the central area of the network. The Concentrator 1 and Concentrator 2 centralize all regional and local networks and interconnect them with the infrastructure data center through external firewall 1 and external firewall 2 (see Figure 2).

C. Redundancy of connections. In order to meet all technical requirements and availability for users, redundant routes were implemented for all configured areas. (local networks, regional networks, data center network and WAN areas). Redundant connections are also present at the level of security equipment, External firewalls 1 and 2 and Internal firewalls 1 and 2, therefore avoiding downtime situations. Below is the scenario of a redundant zone with redundant routes and equipment, where the functionality of the redundant route, as well as the main route is verified. The same principle is applied for all zones configured in the network.

Consequently, between the Access and Distribution layers at the data center network level, there are redundant paths (see Figure 3). In this situation, the following case can be experienced. If the interfaces in the main link are disabled (the route highlighted in green) between SwAccess4 and SwDist1, the packets will go on another path (the redundant path), that is from SwAccess4 to SwDist2, and subsequently to SwDist1, the path highlighted in red (see Figure 3).

The Wireshark tool integrated in the GNS3 simulator allows to see how the packets go on this route. This test will be performed with the ping utility from the VL10 PC to the vlan interface with the ip 192.168.10.1. The first step consisted of checking the main route from the PC located in Vlan 10, whose IP address class is 192.168.10.0/24. From figure 4, it can be seen how the packets go on the main route represented by SwAccess4 and SwAccess1.

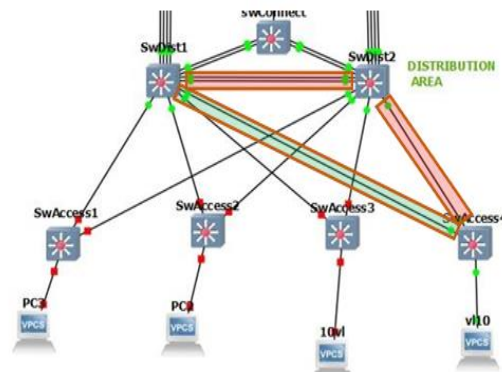


Figure 3 - Check the main and secondary route of the network

After disabling both interfaces on the main route, the traffic is routed on the redundant path, (see Figure 5 and Figure 6) i.e. the packets leave Pc-vl10, arrive in SwAccess4, further it cannot forward them on the main path and generates traffic to SwDist2.

No.	Time	Source	Destination	Protocol	Length	Info
46	11.583252	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xae78, seq=2/512, ttl=255 (request i
47	11.739820	0c:cb:10:59:00:00	PVST+	64	Conf.	Root = 32768/99/0c:97:24:95:00:00 Cost = 3 Port = 0x0
48	11.925331	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xae78, seq=3/768, ttl=64 (reply in 4
49	11.926977	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xae78, seq=3/768, ttl=255 (request i
50	12.430585	0c:cb:10:59:00:00	PVST+	68	Conf.	Root = 32768/20/0c:cb:10:59:00:00 Cost = 0 Port = 0x0
51	12.465381	0c:cb:10:59:00:00	PVST+	68	Conf.	Root = 32768/20/0c:cb:10:59:00:00 Cost = 0 Port = 0x0
52	12.615459	0c:cb:10:59:00:00	PVST+	68	Conf.	Root = 32768/20/0c:cb:10:59:00:00 Cost = 0 Port = 0x0
53	12.697466	0c:cb:10:59:00:00	PVST+	68	Conf.	Root = 32768/40/0c:cb:10:59:00:00 Cost = 0 Port = 0x0
54	12.953195	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xae78, seq=4/1024, ttl=64 (reply in
55	12.955188	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xae78, seq=4/1024, ttl=255 (request
56	13.010646	192.168.40.2	224.0.0.5	OSPF	98	Hello Packet
57	13.643574	192.168.40.1	224.0.0.5	OSPF	98	Hello Packet
58	13.757361	0c:cb:10:59:00:00	PVST+	64	Conf.	Root = 32768/99/0c:97:24:95:00:00 Cost = 3 Port = 0x0
59	13.981380	192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0xae78, seq=5/1280, ttl=64 (reply in
60	13.983141	192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0xae78, seq=5/1280, ttl=255 (request
61	14.404234	0c:cb:10:59:00:00	PVST+	68	Conf.	Root = 32768/20/0c:cb:10:59:00:00 Cost = 0 Port = 0x0
62	14.427664	0c:cb:10:59:00:00	PVST+	68	Conf.	Root = 32768/20/0c:cb:10:59:00:00 Cost = 0 Port = 0x0

Figure 4 - Testing main route connectivity between Access and Distribution layers – Wireshark capture

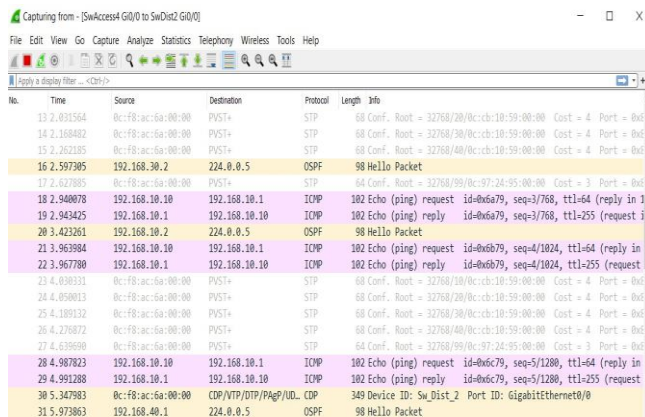


Figure 5 shows a Wireshark capture of network traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
13.2.631564		0c:f8:ac:6a:00:00	192.168.10.1	PVST+		
14.2.168402		0c:f8:ac:6a:00:00	192.168.10.1	PVST+		
15.2.262305		0c:f8:ac:6a:00:00	192.168.10.1	PVST+		
16.2.597385		192.168.10.2	224.0.0.5	OSPF	98	Hello Packet
17.2.627385		0c:f8:ac:6a:00:00	192.168.10.1	PVST+		
18.2.940878		192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x679, seq=3768, ttl=64 (reply in 1
19.2.943425		192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x679, seq=3768, ttl=255 (request i
20.3.423261		192.168.10.2	224.0.0.5	OSPF	98	Hello Packet
21.3.963984		192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x679, seq=41024, ttl=64 (reply in 1
22.3.967780		192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x679, seq=41024, ttl=255 (request i
23.4.038331		0c:f8:ac:6a:00:00	192.168.10.1	PVST+		
24.4.050013		0c:f8:ac:6a:00:00	192.168.10.1	PVST+		
25.4.189332		0c:f8:ac:6a:00:00	192.168.10.1	PVST+		
26.4.276872		0c:f8:ac:6a:00:00	192.168.10.1	PVST+		
27.4.635930		0c:f8:ac:6a:00:00	192.168.10.1	PVST+		
28.4.987823		192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x679, seq=51280, ttl=64 (reply in 1
29.4.991288		192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x679, seq=51280, ttl=255 (request i
30.5.347983		0c:f8:ac:6a:00:00	192.168.10.1	CDP	349	Device ID: Sw_Dist_2 Port ID: GigabitEthernet0/0
31.5.973863		192.168.10.1	224.0.0.5	OSPF	98	Hello Packet

Figure 5 - Testing redundant route connectivity between Access and Distribution layers – Wireshark capture

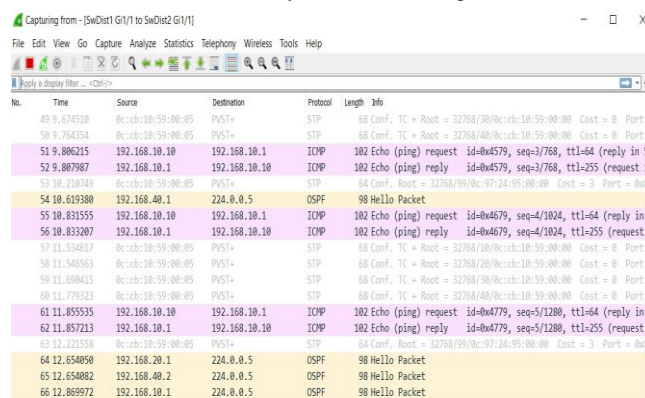


Figure 6 shows a Wireshark capture of network traffic. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
49.9.743510		0c:cb:10:59:00:05	192.168.10.1	PVST+		
50.9.743514		0c:cb:10:59:00:05	192.168.10.1	PVST+		
51.9.806215		192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x479, seq=3768, ttl=64 (reply in 1
52.9.807897		192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x479, seq=3768, ttl=255 (request i
53.10.241749		0c:cb:10:59:00:05	192.168.10.1	PVST+		
54.10.619380		192.168.10.1	224.0.0.5	OSPF	98	Hello Packet
55.10.831555		192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x479, seq=41024, ttl=64 (reply in 1
56.10.833267		192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x479, seq=41024, ttl=255 (request i
57.11.534617		0c:cb:10:59:00:05	192.168.10.1	PVST+		
58.11.540563		0c:cb:10:59:00:05	192.168.10.1	PVST+		
59.11.690415		0c:cb:10:59:00:05	192.168.10.1	PVST+		
60.11.779323		0c:cb:10:59:00:05	192.168.10.1	PVST+		
61.11.855535		192.168.10.10	192.168.10.1	ICMP	102	Echo (ping) request id=0x479, seq=51280, ttl=64 (reply in 1
62.11.857213		192.168.10.1	192.168.10.10	ICMP	102	Echo (ping) reply id=0x479, seq=51280, ttl=255 (request i
63.12.225558		0c:cb:10:59:00:05	192.168.10.1	PVST+		
64.12.654050		192.168.10.1	224.0.0.5	OSPF	98	Hello Packet
65.12.654082		192.168.10.1	224.0.0.5	OSPF	98	Hello Packet
66.12.869972		192.168.10.1	224.0.0.5	OSPF	98	Hello Packet

Figure 6 - Testing redundant route connectivity between Access and Distribution layers – Wireshark capture

Therefore, packets generated by the same source reach their destination via the redundant path, even if the main route is not working.

D. Network security. Firewalls play a fundamental role in the security of communication networks. They analyze data packets from workflows that have formed on the network and decide, based on configured policies, whether to block or allow them. The firewall then prevents unauthorized traffic from entering or leaving the network.

In our design, the firewalls are implemented in a redundant configuration, so ensuring continuous protection and constant availability (see Figure 7). A secondary firewall can automatically take over functionalities in the event of a failure or maintenance operation of the primary one, consequently guaranteeing the continuity of operations without interruption. Since both hardware and software network protection are equally important in a communications network, two firewall filters were implemented, in redundancy, one of the firewall filters for control, access and protection of the external part of the network, and the other firewall filter for access to the internal network, but also for routing traffic between devices.

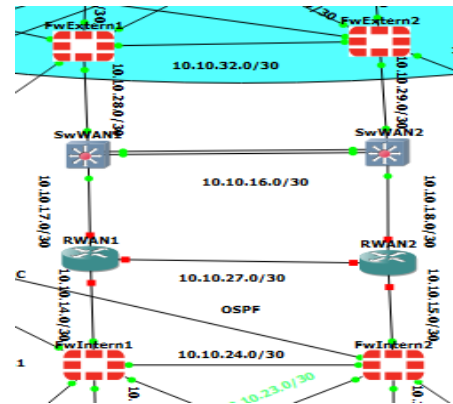


Figure 7 - Firewalls implemented in the external and internal area

Creating lists for filtering and monitoring access, both for incoming and outgoing traffic leaving the internal network through the firewall. Configuring static routes and dynamic routing protocols to facilitate connectivity between devices configured within the network. All configurations having one goal, the implementation of a secure, reliable, scalable and complex communications network.

E. Monitoring of communications infrastructure. For an entire infrastructure to benefit from all the features and become a high-performance network, its permanent monitoring must be ensured, therefore avoiding or preventing certain situations and events. Zabbix is the solution for monitoring the implemented network, which centralizes all the logs of the configured devices, in real time, helping to quickly identify any problem before it becomes critical. It can also be viewed if the configured equipment is operating within normal parameters, preventing situations that could cause interruption to the services provided to the network equipment (see Figure 8). Additionally, a Windows Server was implemented and Domain Controller was constructed for the entire network. Within the domain controller, Active Directory was configured in order to centralize and structure information about users and network devices, ensuring that access to them is done in a controlled and secure manner.

As a result of the domain created for this infrastructure, remote connections between users are possible via the Remote Desktop protocol. Thus, remote access to computers in the domain facilitates much easier administration, but also contributes significantly to solving technical problems that arise at the user level.

Another important role that Active Directory has in the network is to define and apply security policies on the network, in a centralized manner that they apply uniformly to users and devices in the domain. Active Directory facilitates user authentication in this communications infrastructure, allowing fast and secure access to network resource. The network designed in this study benefits from all the necessary features to ensure availability, functionality in optimal parameters, monitoring, centralization and

controlled access in the network through the domain controller.

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards
Concentrator 1	10.10.64.2/30	Up	class: network; target: gw	Enabled	Latest data 16	Problems	Graphs 1	Dashboards 1
Concentrator 2	10.10.65.2/30	Up	class: network; target: gw; target: class: gw	Enabled	Latest data 17	Problems	Graphs 1	Dashboards 1
FaExtInt1	10.10.28.1/30	Up	class: network; target: fw; target: class: fw	Enabled	Latest data 31	Problems	Graphs 1	Dashboards 1
FaExtInt2	10.10.29.1/30	Up	class: network; target: fw; target: class: fw	Enabled	Latest data 31	Problems	Graphs 1	Dashboards 1
FaExtInt3	10.10.13.1/30	Up	class: network; target: fw; target: class: fw	Enabled	Latest data 31	Problems	Graphs 1	Dashboards 1
FaExtInt4	10.10.26.1/30	Up	class: network; target: fw; target: class: fw	Enabled	Latest data 31	Problems	Graphs 1	Dashboards 1
RouterV1	10.10.1.3/31	Up	class: network; target: class: router; target: class: gw	Enabled	Latest data 77	Problems	Graphs 1	Dashboards 1
RouterV2	10.10.1.4/31	Up	class: network; target: class: router; target: class: gw	Enabled	Latest data 77	Problems	Graphs 1	Dashboards 1
RouterCT1	10.10.1.1/31	Up	class: network; target: class: router; target: class: gw	Enabled	Latest data 80	Problems	Graphs 1	Dashboards 1
RouterCT2	10.10.1.2/31	Up	class: network; target: class: router; target: class: gw	Enabled	Latest data 80	Problems	Graphs 1	Dashboards 1
RouterC11	10.10.1.1/31	Up	class: network; target: class: router; target: class: gw	Enabled	Latest data 77	Problems	Graphs 1	Dashboards 1
RouterC12	10.10.1.2/31	Up	class: network; target: class: router; target: class: gw	Enabled	Latest data 80	Problems	Graphs 1	Dashboards 1
RouterS11	10.10.1.3/31	Up	class: network; target: class: router; target: class: gw	Enabled	Latest data 12	Problems	Graphs 1	Dashboards 1
RouterS12	10.10.1.4/31	Up	class: network; target: class: router; target: class: gw	Enabled	Latest data 12	Problems	Graphs 1	Dashboards 1
RWAH1	10.10.14.2/30	Up	class: network; target: gw	Enabled	Latest data 40	Problems	Graphs 1	Dashboards 1
RWAH2	10.10.27.2/30	Up	class: network; target: gw; target: class: gw	Enabled	Latest data 40	Problems	Graphs 1	Dashboards 1
SW1_S8	172.16.10.2/30	Up	class: network; target: gw	Enabled	Latest data 12	Problems	Graphs 1	Dashboards 1
SW2_S8	172.16.11.2/30	Up	class: network; target: gw	Enabled	Latest data 12	Problems	Graphs 1	Dashboards 1
SW1V1	192.168.68.222/30	Up	class: network; target: gw; target: class: gw	Enabled	Latest data 12	Problems	Graphs 1	Dashboards 1
SW1V2	192.168.68.221/30	Up	class: network; target: gw; target: class: gw	Enabled	Latest data 12	Problems	Graphs 1	Dashboards 1

Figure 8 – Network monitoring example - with Zabbix

Finally, the allocation of security policy to users and workstations in the configured domain would be realized. It benefits from a high level of security both at the end-device level from access control on network equipment (switches), but also through controlled access generated by access lists configured at the level of the two firewall filters. The scalability of the network was demonstrated by increasing the number of devices configured in the network according to the scenario described in this paper.

VI. CONCLUSIONS AND FUTURE WORK

A coherent network design ensures a consistent and high-performance experience for users, reducing downtime and improving application reliability.

The example network designed in this study can satisfy a rich set of requirements coming from both users or service providers. The deployed network makes transitions between technologies or upgrades much smoother. Furthermore, new protocols, cloud solutions or emerging technologies can be quickly implemented in the network without risking significant service disruptions or reduced performance.

Advanced security configurations, such as properly implemented firewalls and access control lists (ACLs), are essential for protecting the network infrastructure. By integrating firewalls and ACLs, rigorous traffic filtering is ensured without unnecessarily loading network resources, consequently providing continuous protection without requiring constant or complex interventions. The integration of management and monitoring servers is essential for maintaining the performance, security and reliability of the entire infrastructure. At the same time, the solutions implemented in the network reduce downtime risks and allow for rapid detection of cyberattacks or other network behavior anomalies. Regarding the performance level of the

implemented network, all public services can be accessed by citizens from the same location.

The example network infrastructure designed in this study provides a good framework for rapid network expansion and adaptation. Its modular structure can ensure a smooth transition as the network grows; new locations, equipment or technologies can be integrated without compromising overall performance.

One of the future developments consists of creating a cloud at the level of the implemented network, where essential resources are hosted, which can be accessed from outside the network, via the Internet. Some examples can be: an e-learning platform to support the continuous development of network workers, a web page that includes a calendar with various events (courses, meetings, conferences). Smartphone access to this cloud is achieved via the Internet, in order to authorize access through authorization servers. An example of a connection authorization flow via the mobile phone is: the phone initiates the connection with the cloud, the request is sent to the authorization server, which checks the user credentials, the device (MAC address or digital certificate), if it is valid, the server issues an access token, and the phone receives access to the request stored in the cloud.

REFERENCES

- [1] Digital technology, [Online]. Available from <https://www.durham.gov.uk/article/29603/why-digital-technology-is-important>, 27.03.2025
- [2] Network Redundancy, [Online]. Available from <https://www.indeed.com/career-advice/career-development/network-redundancy>, 27.03.2025
- [3] Graphical Network Simulator-3, [Online]. Available from <https://docs.gns3.com/docs/>, 23.03.2025
- [4] What is Three Tier Architecture in Switch Networking, available from https://www.qsfptek.com/qt-news/what-is-three-tier-architecture-in-switch-networking.html?srlid=AfmBOoq-qV_3MysTzjZhnDTmFo01goIY5rD7yJMERRXeR21uxCCmkljt, 27.03.2025
- [5] Virtual local area networks, [Online]. Available from <https://www.etherwan.com/support/featured-articles/brief-introduction-vlans>, 27.03.2025
- [6] Enhanced Interior Gateway Routing Protocol, [Online]. Available from <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html>, 25.03.2025
- [7] Enhanced Interior Gateway Routing Protocol authentication, [Online]. Available from <https://study-ccnp.com/eigrp-authentication-load-balancing/>, 25.03.2025
- [8] A. S. Tanenbaum - Vrije Universiteit Amsterdam, The Netherlands, David J. Wetherall - University of Washington Seattle, WA, "Computer Networks", pp 474 -- 478, 5th edition, 2011
- [9] Border Gateway Protocol, [Online]. Available from <https://www.fortinet.com/de/resources/cyberglossary/bgp-border-gateway-protocol>, 26.03.2025

Field Measurement of Multi-band Maritime 5G Communication in Deep Sea Scenario

Hang Wu, Kun Yang, Jianjun Ding, Jinglong Lin , Li Qin
Department of Information Engineering
Zhejiang Ocean University
ZhouShan, China

emails: {2778312726@qq.com, yangkun@zjou.edu.cn, zou709142266@163.com, linjinglong@zjou.edu.cn, ql_qinli@zjou.edu.cn}

Abstract—The burgeoning marine economy necessitates robust 5G communication capabilities. However, offshore 5G coverage is inherently constrained by the limited reach of terrestrial base stations, and systematic empirical data on its performance in such environments remains scarce. To bridge this knowledge gap, this study conducted comprehensive empirical measurements of 5G network performance from April 29-30, 2025, utilizing the "Zhe Yu Ke 2" as a mobile testbed in an offshore region extending up to 69 km from the coast. Systematic measurements were conducted on critical performance metrics, including end-to-end latency, uplink/downlink transmission rates, Reference Signal Received Power (RSRP), Reference Signal Received Quality (RSRQ), and Signal-to-Interference-plus-Noise Ratio (SINR), across the 700/850/1800/2100 MHz frequency bands. The empirical results indicate that while 5G can provide fundamental communication services within 69 kilometers offshore, its performance significantly degrades with increasing distance. Notably, the 700 MHz band demonstrated superior capabilities for extended coverage and maintaining more consistent data rates. This study provides crucial empirical evidence for the strategic planning and optimized deployment of marine 5G networks, facilitating critical applications, such as offshore wind power monitoring and smart shipping.

Keywords—Marine 5G; Long-range Communication; Frequency Band Performance; Data Analysis; Signal Quality.

I. INTRODUCTION

The rapid development of the marine economy places higher demands on communication systems. 5G technology, with its advantages such as high bandwidth, low latency, and massive connectivity, is considered a key enabler for digital transformation in the marine sector [1]. However, in vast marine scenarios, particularly in far-sea areas far from land-based base stations, current 5G faces severe challenges, such as insufficient network coverage and fluctuating signal quality [2]. It is particularly noteworthy that systematic field measurement data is extremely scarce in far-sea areas tens of kilometers away from the coastline, making objective performance evaluation difficult.

Recent studies have explored maritime 5G from theoretical and simulation perspectives. For instance, Saini et al. [4] assessed path loss at air-sea interfaces, providing

theoretical insights into long-range signal propagation. Gao et al. [6] modeled electromagnetic wave propagation over rough sea surfaces using parabolic equations, while Lindbergs et al. [7] investigated multi-hop 5G architectures for maritime connectivity. Despite these efforts, most existing works rely on simulations or near-shore trials, lacking comprehensive empirical data from true far-sea environments. In particular, there is a lack of field measurements evaluating multi-band (e.g., 700/850/1800/2100 MHz) 5G performance beyond 50 km offshore, and limited understanding of how key indicators—such as latency, throughput, RSRP, RSRQ, and SINR—evolve jointly under real oceanic conditions.

This gap leads to a clear “wish list” for maritime 5G research: (1) conducting systematic field tests in deep-sea scenarios (>50 km); (2) quantifying the trade-offs between coverage and data rate across different frequency bands; and (3) generating practical, data-driven guidance for offshore base station deployment and spectrum planning.

To fill this gap and provide reliable evidence, this study conducted comprehensive field measurements up to 120 km offshore near Zhoushan, China, using the research vessel Zhe Yu Ke 2 as a mobile testbed. We systematically evaluated 5G performance across multiple frequency bands (700/850/1800/2100 MHz), collecting end-to-end latency, uplink/downlink rates, RSRP, RSRQ, and SINR under real marine conditions. The results reveal the degradation patterns of 5G signals over long distances and highlight the superior coverage capability of the 700 MHz band.

These field measurement data provide important data support and a decision-making basis for the optimized design and technology selection of future maritime 5G networks, as well as their promotion in various marine application scenarios, such as offshore wind monitoring and smart shipping [3]. They also serve as a technical benchmark for communication system deployment in coastal and near-sea regions.

Despite the comprehensive nature of our field measurements, this study has several limitations that should be acknowledged. The measurements were conducted over a short period under relatively calm sea states and favorable weather conditions, which may not fully capture the

performance degradation caused by severe weather, strong tides, or atmospheric ducting phenomena. Furthermore, the results are based on a single network operator and a specific maritime route, and performance may vary with different network configurations or in other geographical locations. These limitations highlight valuable avenues for future research.

The remainder of this paper is organized as follows. Section II details the experimental setup, including the test environment, the measurement platform, and the data collection procedures. Section III presents and analyzes the empirical results, focusing on key performance indicators such as latency, network speed, and signal quality across different frequency bands. Finally, Section IV concludes the paper by summarizing the key findings, discussing their implications, and outlining directions for future work.

II. TEST SCENARIO

This section details the experimental methodology, describing the geographical test environment, the hardware setup, and the data collection procedures.

A. Test Environment

The tests were conducted from April 29 to April 30, 2025, in the waters near Zhoushan City, with the navigation route as shown in Figure 1.

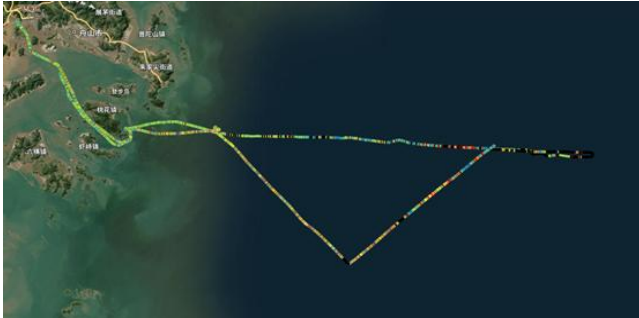


Figure 1. Route Map

The furthest point of the test route extended approximately 69 kilometers offshore, covering the transition zone from coastal to far-sea areas. During the testing period, the marine and meteorological conditions were generally stable. On Tuesday, April 29, 2025, the temperature in the test area ranged from 15°C to 24°C, with the weather transitioning from overcast to partly cloudy, a southeast wind at level 3, and excellent air quality (AQI 32). Overall, the meteorological conditions were suitable for offshore operations. On Wednesday, April 30, the temperature ranged from 18°C to 24°C, the weather changed from overcast to light rain, and the wind strength increased to a southerly wind at level 5. The sea conditions became slightly rougher, which could have had some impact on certain communication indicators and signal propagation. The 5G network operator relied upon for the tests was China Mobile.

B. Experimental Setup

To evaluate the performance of 5G communication systems in far-sea environments, we conducted field measurements over a coastal-to-offshore range of 0–120 km. The experimental platform was based on a self-developed 5G terminal integrating an n78 band (3.5 GHz) 5G module, a high-gain directional antenna, and an embedded data acquisition system, capable of stable long-term operation in complex marine electromagnetic conditions.

During the test, the research vessel sailed at a constant speed along a predefined route for data collection. Key performance metrics were periodically measured with tailored sampling frequencies according to their dynamic characteristics, balancing measurement accuracy and system load.

TABLE I. MEASUREMENT PARAMETER TABLE

Measurement Parameter	Measurement Configuration	
	Sampling frequency	Collection tool
Latency	Every 5 seconds	Vim Ping
GPS Position	Every 5 seconds	GPS module
Downlink/Uplink Throughput	Every 5 minutes	Speedtest
RSRP, RSRQ, SINR	Every 30 seconds	5G terminal backend web interface

All data were locally recorded with timestamps for subsequent spatiotemporal alignment and statistical analysis. The terminal antenna was kept stable during testing to minimize directional signal attenuation. All experiments were conducted under favorable weather conditions and calm sea states (wind force < 4) to avoid additional interference from harsh environments.

III. TEST RESULTS AND ANALYSIS

This section presents a detailed analysis of the collected field data, evaluating the maritime 5G network performance through key metrics including latency, throughput, and signal quality indicators.

A. Latency Performance Analysis

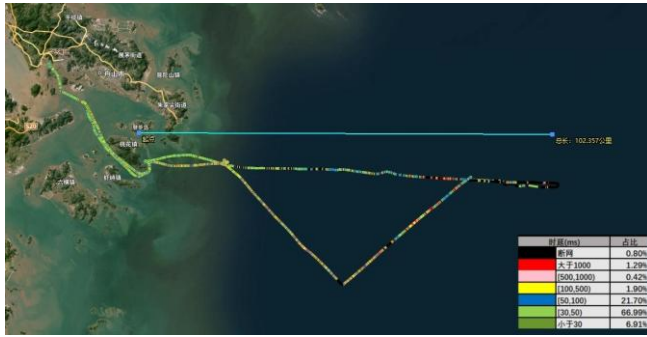


Figure 2. Latency vs. Offshore Distance

Analysis of Figure 2 reveals that as the vessel gradually moves away from the shore-based base station, the end-to-end communication latency of the 5G network in the maritime environment generally shows an upward trend. In waters closer to the shore, due to the shorter physical distance between the terminal equipment and the base station, the communication link is relatively stable, and network latency remains at a low level. However, as the vessel moves further away from land and gradually enters far-sea areas, latency exhibits a step-by-step increase. Particularly after crossing a specific distance threshold (e.g., 70 km or 100 km), network latency increases significantly, showing a notable phenomenon of edge performance degradation. This phenomenon fully demonstrates the direct impact of distance on the quality of maritime wireless communication links.

A comprehensive analysis of the causes of the aforementioned network performance degradation can be summarized into several aspects: Firstly, as the wireless signal transmission path lengthens, the path loss experienced by the signal during transmission continuously increases, leading to a weakening of the received signal strength [4]. Secondly, due to increased distance, the link quality continuously deteriorates, forcing the system to initiate more retransmission mechanisms to ensure data integrity, thereby further extending the total latency. Thirdly, the base station's ability to serve long-distance users decreases due to its scheduling strategy, limiting the quality of service for edge users. Furthermore, at certain specific maritime coordinates, the study also observed anomalous fluctuations or sudden increases in communication latency. Such phenomena may be jointly induced by multiple factors, such as automatic switching of communication bands, changes in ship attitude during navigation, or the presence of local electromagnetic interference sources [5].

B. Network Speed Performance Analysis

The fundamental reason for the overall decline in speed primarily stems from the complex physical environment faced during maritime radio wave propagation. Firstly, after the vessel departs from shore, the signal propagation path significantly lengthens, and path loss rapidly accumulates, thereby weakening the signal strength at the receiver. Especially when the communication link extends beyond the line-of-sight boundary, the attenuation of direct signals

sharply increases due to the Earth's curvature. Secondly, because the sea surface is relatively flat, it is prone to strong specular reflection effects, leading to severe multipath propagation problems. This phenomenon can cause frequency selective fading, interfering with certain frequency bands in the channel and leading to a reduction in the usable modulation and coding levels, fundamentally limiting the terminal equipment's data throughput capacity.

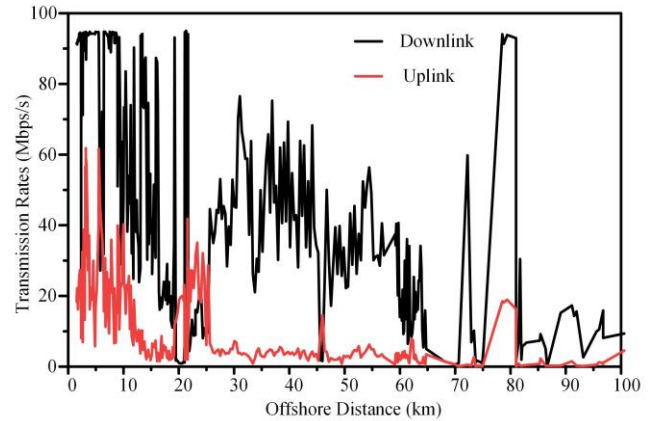


Figure 3. Link Rate vs. Distance Graph

In addition to channel propagation characteristics, the network resource allocation mechanism itself also significantly impacts speed performance. Typically, mobile communication systems allocate more transmission resources in the downlink direction, and base stations possess higher transmit power. In contrast, terminal equipment's transmit capability, antenna gain, and anti-interference performance are often insufficient on the uplink. Therefore, in long-distance communication scenarios facing extended signal paths and increased interference factors, the uplink is more susceptible to impact, exhibiting instability or even an inability to maintain connection. Furthermore, from Figure 3, certain anomalous fluctuation characteristics can also be observed. For example, at approximately 22 km and 60 km, the downlink speed momentarily increased to abnormally high values. This sudden change may be related to the vessel temporarily entering a high signal coverage area (e.g., a new base station sector or the coverage range of a repeater station), or it could be related to the system scheduling momentarily releasing high bandwidth resources. Relatively, the frequent drop of uplink speed to zero is more likely due to limitations in terminal communication capability, which may be caused by severe deterioration of channel quality, unstable ship antenna attitude due to fluctuations, or local interference sources leading to communication link failure.

This systematically outlines the typical performance characteristics of the current maritime 5G communication environment: "excellent communication quality in near-shore areas, significant fluctuations in mid-range, sharp decline in speed in far-sea areas, and the uplink link being more susceptible to damage." The above trends and their anomalous phenomena not only reveal the real challenges faced by maritime communication coverage but also

profoundly reflect the complex and dynamic coupling relationship between wireless propagation conditions, network scheduling strategies, and terminal technical capabilities, providing important empirical reference for future maritime 5G network optimization, coverage strategy formulation, and technological iteration.

C. Signal Quality Indicator Analysis

SINR has a decisive impact on wireless network data transmission capability, directly related to throughput, bit error rate, and the supported modulation and coding levels. For instance, in LTE or 5G networks, if the SINR value reaches above 20 dB, the system can typically employ higher-order modulation schemes, such as 64QAM or even 256QAM, thereby significantly improving data transmission rates. However, SINR is comprehensively influenced by multiple factors, including severe multipath propagation in marine environments, interference from neighboring base stations, and background noise in the device's environment. SINR is not only an important basic parameter for wireless network performance evaluation but is also widely applied in key technical aspects, such as system capacity design, dynamic interference control, network optimization, and real-time quality monitoring.

Figure 4 shows the dynamic evolution of maritime communication signals in complex environments.

Firstly, the gradual attenuation of RSRP (from -90 dBm to -112 dBm) conforms to the free-space path loss model. Particularly in open sea areas without land reflection support, signal propagation is exacerbated by the dual effects of atmospheric scattering and sea surface absorption. It is worth noting that signal recovery in the V-shaped return path might be related to brief line-of-sight optimization or the Doppler effect caused by route adjustments, which suggests the potential role of dynamic antenna directivity in signal maintenance.

The significant decline in RSRQ (from -10 dB to -20 dB) indicates a rapid increase in interference components. This could stem from coherent multipath interference caused by sea surface reflection, as well as electromagnetic interference from other vessels or aircraft. Combined with the SINR data (dropping from 5-10 dB to <0 dB), it can be inferred that there is higher non-thermal noise or adjacent channel interference in far-sea areas, possibly due to ionospheric reflection in the marine environment or the superposition effect of distant base station signals. Mathematically, the deterioration of SINR is significantly amplified by increasing distance.

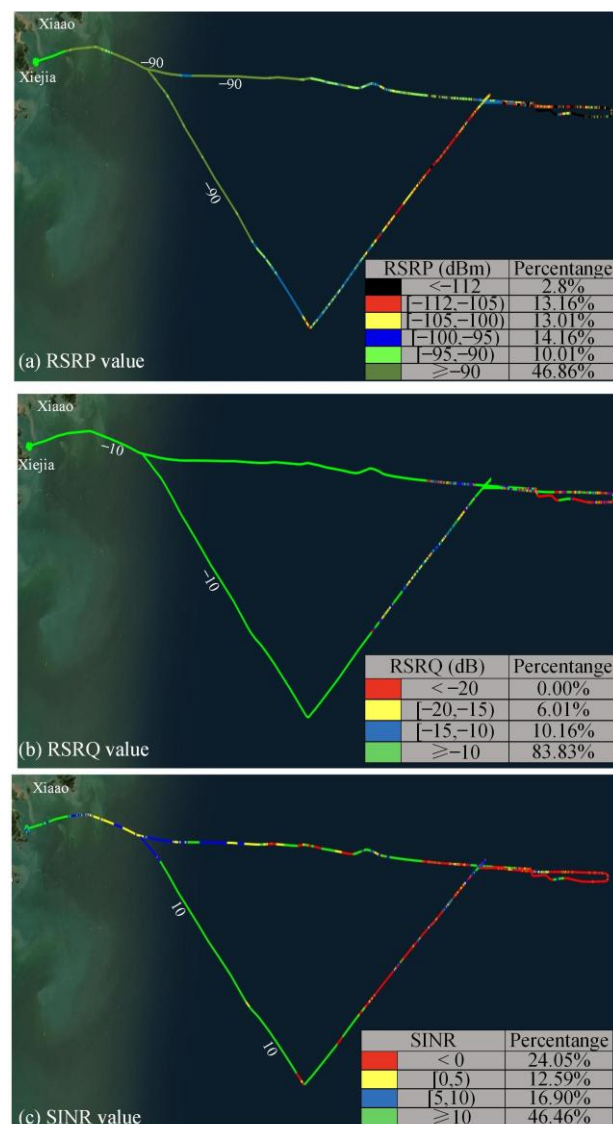


Figure 4. RSRP, PSRQ, and SINR Summary Chart

Based on this analysis, it can be predicted from the above analysis that if we continue into deeper waters, signal quality will further deteriorate unless targeted technical interventions are introduced. Improvement directions include: first, deploying adaptive relay networks based on buoys or Unmanned Aerial Vehicle (UAV) to shorten signal propagation distance and improve RSRP; second, adopting Multiple-Input Multiple-Output (MIMO) technology combined with beamforming to optimize RSRQ and SINR; third, developing machine learning-based adaptive modulation and coding schemes to dynamically adjust transmission parameters to cope with interference. In the future, these hypotheses can be further verified and communication strategies optimized through simulations combining marine environmental data with signal models.

D. Analysis of Communication Bands and Network Speed

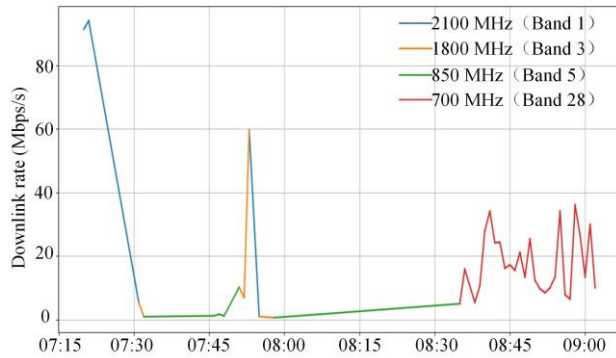


Figure 5. Relationship between Frequency Band and Network Speed

In the initial stage of communication, figure 5 shows that the two higher frequency bands, 2100 MHz (Band 1) and 1800 MHz (Band 3), exhibited excellent downlink data transmission rates. Specifically, the downlink rate of the 2100 MHz band once exceeded 90 Mbps, and the 1800 MHz band also briefly reached a peak of 60 Mbps. This phenomenon indicates that in near-shore areas close to land-based base stations, higher frequency bands, by virtue of their larger channel bandwidth and higher spectrum utilization efficiency, can provide strong data throughput capability to meet high-speed data transmission demands. However, as the vessel sailed further away from land-based base stations, the attenuation speed of the aforementioned high-frequency signals significantly accelerated, eventually leading to connection interruptions and a plummeting data transmission rate to near zero. Thereafter, maritime communication primarily relied on the two lower frequency bands, 850 MHz (Band 5) and 700 MHz (Band 28), for maintenance. Although the overall data transmission rate provided by these two low-frequency bands was only between 10–30 Mbps, their connection stability was significantly enhanced, providing a basic guarantee capability for far-sea communication.

In the maritime wireless communication environment, the propagation characteristics of electromagnetic waves are significantly affected by frequency: the higher the frequency, the faster the signal attenuates during propagation, and the poorer its penetration and diffraction capabilities [6]. Therefore, although the 2100 MHz and 1800 MHz bands have the advantage of providing high data transmission rates, their coverage range is greatly limited, maintaining high performance only in areas close to base stations or under good line-of-sight propagation conditions. In contrast, low-frequency bands (especially 700 MHz and 850 MHz), due to their longer electromagnetic wavelengths and stronger diffraction capabilities, can achieve longer communication distances and stronger anti-interference capabilities in an unobstructed but complex propagation medium like the sea

surface, becoming typical main frequency bands for long-distance coverage [7]. It is particularly worth mentioning that Band 28 has gradually become one of the internationally recognized core resources for far-sea wide-area communication, playing a key role in far-sea communication coverage.

From the test data graph, it can be observed that during the 07:30–08:00 time period, the frequency bands used by the communication system frequently switched, and data transmission rates also fluctuated significantly, even experiencing "blank periods" of communication interruption. This phenomenon may be due to the user terminal equipment's inability to quickly and effectively complete frequency band switching in a complex multi-band environment, or due to improper handling of frequency band coverage boundaries on the network side. Simultaneously, since the current system has not enabled frequency band carrier aggregation technology, various frequency bands operate relatively independently in actual communication, leading to fragmented overall network performance. That is, while low-frequency bands can provide basic connection guarantees, they cannot support high-throughput service demands. Overall, the stability and consistency of current maritime communication links still face significant challenges, which is unfavorable for the continuous conduct of critical services, such as real-time transmission of high-definition video and precise remote control of remote equipment.

To address the above issues, it is recommended that maritime communication systems be optimized simultaneously in terms of frequency band strategy and terminal capabilities. In near-shore areas, priority can be given to using 2100/1800 MHz high-frequency bands to enhance initial link quality. When entering far-sea, intelligent switching to Band 28/5 should occur to maintain basic connectivity. Simultaneously, the deployment of Carrier Aggregation should be promoted, especially multi-band aggregation schemes involving low-frequency + mid-frequency (e.g., Band 28+5+3), to balance speed and coverage. Additionally, consideration can be given to deploying high-gain directional antennas or mobile base station facilities, such as relay buoys to extend the effective service radius of high-frequency bands [8]. Terminal equipment should also support features like MIMO, band aggregation, and fast switching to maintain stable communication capabilities under dynamic sea conditions and complex propagation conditions, thereby providing a network guarantee basis for future maritime intelligent operations.

IV. CONCLUSION AND FUTURE WORK

This study presents a comprehensive field measurement of 5G network performance in a deep-sea maritime environment, revealing key patterns in latency, throughput, and signal quality over distances up to 120 km offshore. The results show that end-to-end latency increases with distance,

while network performance exhibits significant edge degradation in far-sea areas. Specifically, downlink rates can reach 90–100 Mbps within 2–10 km from the coast but drop rapidly to below 10 Mbps—or even zero—beyond 40–60 km. Uplink performance remains consistently weak, with frequent disconnections observed in distant zones. Signal quality indicators—including RSRP, RSRQ, and SINR—gradually deteriorate with distance, and SINR typically falls below 0 dB beyond 70 km, severely compromising link stability.

Frequency band analysis further highlights a critical trade-off between coverage and capacity: high-frequency bands (e.g., 1800 MHz and 2100 MHz) deliver high data rates near shore but suffer rapid signal decay; in contrast, low-frequency bands (e.g., 700 MHz and 850 MHz) maintain stable connectivity over long distances, demonstrating superior propagation characteristics for maritime coverage.

These empirical findings provide valuable insights into the evolution of maritime 5G links across rate, latency, and signal quality dimensions. They offer practical guidance for communication operators in optimizing base station deployment, frequency planning, and resource scheduling to enhance offshore coverage. Moreover, the identified performance bottlenecks inform the design of reliable communication strategies for intelligent maritime applications—such as unmanned vessel control, ocean monitoring, and smart shipping—where stable and low-latency connectivity is essential. The results also support the development of advanced terminal technologies, including multi-band aggregation, beamforming, and intelligent handover mechanisms, laying a foundation for future 6G and space-air-ground integrated networks.

When compared to Low Earth Orbit (LEO) satellite systems (e.g., Starlink, OneWeb), terrestrial 5G offers distinct advantages in near-sea scenarios (<70 km). First, 5G achieves lower latency, with measured average RTT under 40 ms, outperforming LEO systems (typically 25–80 ms) due to shorter propagation paths and fewer relays. Second, 5G leverages existing infrastructure, resulting in significantly lower deployment and operational costs, whereas LEO terminals are expensive (often >USD 500) and require recurring subscription fees—prohibitive for large-scale near-shore sensor networks. Third, 5G provides higher and more stable throughput (up to hundreds of Mbps) with QoS support, while LEO links are prone to interruptions and rate fluctuations caused by weather, sea clutter, and terminal orientation.

Nonetheless, 5G's coverage is inherently limited by line-of-sight propagation and Earth's curvature, making it unsuitable for open-ocean use. Therefore, we advocate a complementary architecture: using 5G as the primary, cost-effective, and low-latency solution in near-sea regions, and

seamlessly transitioning to LEO satellites in far-sea or global coverage scenarios—forming a hybrid “Near-sea 5G + Far-sea Satellite” integrated communication system.

This study has some limitations. Measurements were conducted under relatively calm sea states and favorable weather conditions, without fully capturing the impact of severe weather or tidal dynamics. Some performance fluctuations may also stem from operator-specific network policies, requiring further investigation. Future work will extend testing across diverse marine conditions, explore heterogeneous networks (e.g., 5G + satellite + UAV relays), and incorporate machine learning for adaptive link optimization. Additionally, we plan to integrate Quality of Experience (QoE) assessment to better align technical performance with application-level requirements, ultimately enabling robust and intelligent maritime communication ecosystems.

REFERENCES

- [1] R. Ullah, S. Ullah, S. M. Umar, R. Ullah and B. Kamal, "Design and Modeling of a 28/38/60/70/80 GHz Antenna for Fifth Generation (5G) Mobile and Millimeter Wave (mmW) Applications [C]," 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Swat, Pakistan, 2019, pp. 1-7.
- [2] R. Raulefs, and W. Wang, "Enhancing capacity of maritime broadband communication systems[C]," OCEANS 2016 MTS/IEEE Monterey, Monterey, CA, USA, 2016, pp. 1-4, doi: 10.1109/OCEANS.2016.7761261.
- [3] B. Chen, and J. Wang, "Long-Range Wireless Sensor Network-based Remote Marine Environmental Monitoring System[C]," 2021 International Conference on Computer, Internet of Things and Control Engineering (CITCE), Guangzhou, China, 2021, pp. 100-106.
- [4] P. Saini, R. P. Singh, and A. Sinha, "Path loss assessment of electromagnetic signal on air-sea and air-soil boundary in sensor networks," International Journal of System Assurance Engineering and Management, 2024, vol. 15, no. 6, pp. 2238-2247.
- [5] V. R. Farré Guijarro, J. D. Vega Sánchez, M. C. P. Paredes, and et al., "Comparative evaluation of radio network planning for different 5G-NR channel models on urban macro environments in Quito city," IEEE Access, 2024, vol. 12, pp. 23. DOI:10.1109/ACCESS.2024.3350182.
- [6] Y. Gao, Q. Shao, B. Yan, Q. Li, and S. Guo, "Parabolic equation modeling of electromagnetic wave propagation over rough sea surfaces," Sensors, 2019, vol. 19, no. 5, pp. 1252. <https://doi.org/10.3390/s19051252>
- [7] A. Lindenbergs, M. Muehleisen, M. Payaró, K. Körbe Kaare, H. W. Zaglauer, J. Scholliers, A. Adam, K. Kuhi, and L. Nykanen, "Seamless 5G multi-hop connectivity architecture and trials for maritime applications," Sensors, 2023, vol. 23, no. 9, pp. 4203. <https://doi.org/10.3390/s23094203>
- [8] R. Beiranvand and P. K. Mohamadian, "High-gain wideband directional antenna for 5G applications," International Journal of Electronics and Microcircuits, 2024, no. 1, pp. 4.