The Networks and IoT Systems research group of CNAM-CEDRIC hires multiple research master interns, research engineers or Ph.D. students in the topics detailed in the next pages.

Research environment

Team: Networks and IoT Systems (ROC – Réseaux et Objets Connectés; https://roc.cnam.fr)
Computer Science and Communications department (CEDRIC; https://cedric.cnam.fr)

Related collaborative projects:

IPCEI MECT: project on network automation platforms and algorithms for OpenRAN-based 5G.
ANR TREES: project on distributed learning for beyond-5G systems.
ETSI STF project Smart Customized Services.

Location:

Paris, France - downtown district (le Marais), third arrondissement. 2 rue Conté, Paris, France.

Contract offered

Master internship: start from March 15, 2025, for a duration of 6 months, 650 € net/month.
Research engineer: start from June – December 2025, for a duration of 3 years, 2000€ net/month.
Ph.D. contract: start from June – December 2025, for a duration of 3 years, 2350€ net/month.

50% of the public transportation subscription can be reimbursed.

Requirements

Master 2 in computer science, computer engineering, or telecommunications engineering.

Application

As soon as possible. Send to perm-roc@cnam.fr:

- An up-to-date curriculum vitae on maximum 3 pages, including names and contact information of 2 reference persons (professors or industrial tutors).
- Certificate and transcripts for all university degree owned and ongoing.
- Copy of all your master/bachelor thesis and/or internship report(s).
- Few lines in the email with the desired position(s) and starting date.

Distributed Self-Controlled Service Composition for IoT

In the field of service-oriented architecture, a service refers to a software feature or set of software features (encryption, compression, authentication, etc.) that different clients can share and reuse for different purposes.

The Internet of Things (IoT) supports various industrial applications. The cooperation and coordination of smart things are a promising strategy for satisfying requirements that are beyond the capacity of a single smart thing. One of the major challenges for today's software engineering is the management of large and complex computing systems characterized by a high degree of physical distribution.

The candidate will propose a new distributed architecture for the Internet of Things, integrating automation and service self-control.

To achieve this objective, the following tasks are foreseen:

- A detailed analysis of the state of the art will first be carried out to identify candidate technologies to be explored: Service oriented architecture, service composition, distributed systems, architecture IoT.
- The proposal should consider:
    - Architectural Model: defines the global structure, including semantics and is optimized for the stated objectives.
    - links and nodes model including visibility levels
    - Communication Model: defines the exchange and management protocols over three planes: (1) Management (Monitoring), (2) Control, and (3) Usage.
- The candidate will be required to put into practice a composition of distributed services using state of the art technologies including both software (e.g. Java, socket, *Remote Procedure Call*) and hardware approaches.
- The candidate may also be required to develop a service component modeling tool.

In case of a Ph.D., further works in this area will be identified after this preliminary contribution.

Candidates should have a solid background in distributed systems, programming and IoT.

References

[1] Aubonnet, T.; Henrio, L.; Kessal, S.; Kulankhina, O.; Lemoine, F.; Madelaine, E.; Ruz, C. and Simoni, N. Management of service composition based on self-controlled components. In Journal of Internet Services and Applications, 6 (15): 17, 2015. doi

[2] Lemoine, F.; Aubonnet, T. and Simoni, N. IoT composition based on self-controlled services. In Journal of Ambient Intelligence and Humanized Computing, 11: 5167-5186, 2020. doi

[3] Lemoine, F. Internet des Objets centré service autocontrôlé. Ph.D. Thesis, Conservatoire national des arts et metiers - CNAM, 2019.

Key management infrastructures with zero-knowledge proof

In mobile networks, the tactical bubble system has been designed to deliver several services to mobile users within its coverage area. These systems need to be rapidly deployable in any terrain. Therefore a bubble consists of a core network and the radio access network, all in a single unit. Most widely used authentication systems are currently based on a key management infrastructure, which is made up of four entities: the registration authority, the certification authority, the validation authority and an administrator managing user registration.

The concept of zero-disclosure proof of knowledge is a cryptographic approach that has recently gained in popularity. The concept is based on proof of possession of a secret but without revealing it. ZKPs are beginning to be used in the IoT [1], [2] and IoV [3], [4] environments. An ongoing PhD thesis in the team introduces the use of ZKPs in tactical bubbles. The use of ZKPs for login/password authentication and certificate authentication was introduced in this work. The algorithmic and temporal complexity has been studied in relation to the algorithm used, but this complexity still needs to be studied by testing it in a more realistic simulation environment.

This candidate will therefore focus on implementing a test environment to create a more realistic simulation. The work will initially consist of

- including the algorithms tested in the thesis work in a complete code structure aimed at an exchange between a user and a server.
- designing a larger test environment to observe the simulation over a larger number of exchanges.
- Conceiving other more advanced algorithms to be tested for authentication based on ZKP. These algorithms will have to be tested in a simple test environment and then in a more advanced test environment with larger scales and features.

In case of a Ph.D., further works in this area will be identified after this preliminary contribution.

Candidates should have a solid background in security.

References

[1] F. Mart́ ın-Fern ́andez, P. Caballero-Gil, and C. Caballero-Gil,“Authentication based on non-interactive zero-knowledge proofsfor the internet of things,”Sensors, vol. 16, no. 1, 2016.

[2] A. Rasheed, R. N. Mahapatra, C. Varol, and K. Narashimha,“Exploiting zero knowledge proof and blockchains towards theenforcement of anonymity, data integrity and privacy (adip) inthe iot,”IEEE Transactions on Emerging Topics in Computing,vol. 10, no. 3, pp. 1476–1491, 2022.

[3] N. Xi, W. Li, L. Jing, and J. Ma, “Zama: A zkp-basedanonymous mutual authentication scheme for the iov,”IEEEInternet of Things Journal, vol. 9, no. 22, pp. 22 903–22 913,2022.

[4] P. Bagga, A. K. Sutrala, A. K. Das, and P. Vijayakumar,“Blockchain-based batch authentication protocol for internet ofvehicles,”Journal of Systems Architecture, vol. 113, p. 101877,2021

Distributed anomaly detection with split learning

Anomaly detection in 5G and IoT systems is pivotal not just for operational efficiency but also for security, safety, compliance, and enhancing the overall reliability and user experience of IoT deployments. Given the complexity and the scale of data involved in 5G networks, advanced anomaly detection mechanisms become indispensable to cope with runtime constraints and application requirements.

Split learning [1, 2] represents a pioneering approach in cloud co-training, particularly tailored for IoT applications in recent years. This method strategically deploys a lightweight model on endpoint devices, which often have limited computational and memory resources, while hosting more complex model segments on cloud servers. This setup facilitates collaborative training. A critical aspect of split learning is managing the balance between communication efficiency and model performance. Research has indicated that incorporating a bottleneck layer can significantly enhance this balance [3]. Inspired by the 'early exit' concept [4], the candidate will have to design and introduce a dynamic bottleneck layer model for networked split learning environment. The goal to maintain or improve model performance while minimizing communication overhead, ensuring efficient end-to-end training without performance degradation.

The candidate is expected to finish the following development and implementation work:

- Develop and train a split learning model incorporating a bottleneck layer using the Flower.ai simulator.
- Develop a multi-path dynamic compression mechanism, using a control mechanism to choose the appropriate path [5].
- Develop and implement a multi-agent cooperative anomaly detection learning model.

In case of a Ph.D., further works in this area will be identified after this preliminary contribution.

Candidates should have a solid background in applied artificial intelligence.

References

[1] Thapa, C., Mahawaga Arachchige, P. C., Camtepe, S., & Sun, L. (2022). "SplitFed: When Federated Learning Meets Split Learning," Proceedings of the AAAI Conference on Artificial Intelligence, 36(8), 8485-8493.
[2] Yoshitomo Matsubara, Marco Levorato, and Francesco Restuccia. 2022. "Split Computing and Early Exiting for Deep Learning Applications: Survey and Research Challenges," ACM Comput. Surv. 55, 5, Article 90 (May 2023), 30 pages.
[3] J. Shao and J. Zhang, "BottleNet++: An End-to-End Approach for Feature Compression in Device-Edge Co-Inference Systems," 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, Ireland, 2020, pp. 1-6.
[4] S. Teerapittayanon, B. McDanel and H. T. Kung, "BranchyNet: Fast inference via early exiting from deep neural networks," 2016 23rd International Conference on Pattern Recognition (ICPR), Cancun, Mexico, 2016, pp. 2464-2469.
[5] Y. Shu, P. Gu, C. Adjih, C. S. Chen and A. Serhrouchni, "DynSplit: A Dynamic Split Learning Scheme for 5G-Enpowered Metaverse," 2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom), Hong Kong, China, 2024, pp. 214-221, doi: 10.1109/MetaCom62920.2024.00043.

5G-NTN networks based on open 5G software stacks

Non-Terrestrial Networks (NTNs) [1], which include Geostationary Earth Orbit (GEO), Medium Earth Orbit (MEO), and Low Earth Orbit (LEO) satellites, constitute a critical infrastructure for delivering continuous, ubiquitous, and scalable communication services. The advent of LEO satellite constellations is particularly significant for the realization of cell-free architectures in 5G and beyond, by facilitating lower latency and global coverage [2].

Few open source 5G software stacks, as OpenAirInterface (OAI) [3] and srsRAN, are recognized as leading 5G open-source platforms, featuring O-RAN (Open Radio Access Network) stacks that accommodate various configuration types. A key application, 5G-LEO [4], is engineered to accelerate 5G software stack development, establishing it as a robust open-source environment. This initiative promotes the sharing and benchmarking of results from 5G NTNs within the satellite communications community and facilitates enhanced collaboration in research and development. An augmented 5G software stack serves as an essential resource for constructing early-stage prototypes, thereby validating critical design elements of 5G NTNs.

The candidate is expected to finish the following development and implementation work:

- Comprehend and critically analyze the reference scenarios and use cases designated for NR-NTN (New Radio - Non-Terrestrial Networks) deployments as outlined by 3GPP.
- Gain an in-depth understanding and perform analysis of the 5G-LEO infrastructure, comparing OAI and SRSran as 5G software stacks.
- Evaluate and consider the integration of simulators or small-case emulation testbed for the NTN environment.
- Execute multiple tests to assess the performance metrics of the software stack platform.

In case of a Ph.D., further works in this area will be identified after this preliminary contribution.

Candidates should have a solid background in programmable network tools.

References

[1] R. Xie, Q. Tang, Q. Wang, X. Liu, F. R. Yu, and T. Huang, “Satellite-terrestrial integrated edge computing networks: Architecture, challenges, and open issues,” IEEE Network, vol. 34, no. 3, pp. 224–231, 2020.

[2] “Study on using satellite access in 5g; stage 1,” Technical Report TR 22.822, 3GPP, 2018.

[3] “OpenAirInterface Documentation: Release v2.2.0.” [Online]. Available: https://gitlab.eurecom.fr/oai/openairinterface5g/-/tree/develop/doc.

[4] “5G-LEO” [Online]. Available: https://connectivity.esa.int/projects/5gleo

Quantum Key Distribution in Satellite Networks

Since the 1990s, satellite networks have rapidly advanced in the fields of space and information technology, exemplified by systems such as Globalstar or Inmarsat. Their primary objective has been to address the limited coverage of ground communication systems, serving as a complementary solution. In recent years, low-orbit mobile communication satellite networks are evolving to support IoT applications. However, using the traditional encryption algorithms such as RSA and ECC is becoming critical with the rise of quantum computing. In fact, these traditional schemes can be broken because quantum computing can significantly reduce the time required for analyzing and decrypting secure systems. As a result, there is ongoing research that aims at developing security algorithms that are resilient to quantum computers. Two key areas are investigated: quantum key distribution (QKD) [1] and post-quantum cryptography (PQC) [2].

Both QKD and PQC offer distinct benefits and face unique challenges. QKD leverages quantum mechanical properties to securely distribute symmetric keys between two parties, such as Alice and Bob, which can then be used for data encryption and decryption. The key advantage of QKD is its mathematically proven security and its ability to alert users to any attempts at data interception, thanks to the principles of quantum mechanics. However, QKD also has drawbacks, including its limited scalability for multiple users, constraints on the distance between the communicating parties (typically ~100 km by fiber and ~1000 km by satellites), and high infrastructure costs, such as the expense of QKD equipment and dark fiber networks

The objective of this research work is to explore the integration of quantum and satellite networks regarding key distribution, with a focus on leveraging post-quantum cryptography.

The candidate is expected to finish the following development and implementation work:

- Study of the features of quantum networks and test the functionalities of the SeQUeNCe simulator and QuNetSim framework [3].
- Study the architecture of satellite networks
- Conduct an in-depth study of Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) principles and their potential synergies
- According to the literature, choose a PQC algorithm to use with QKD in the context of satellite networks.
- Perform simulations to validate the integration of selected PQC algorithms within QKD-enabled satellite networks.

In case of a Ph.D., further works in this area will be identified after this preliminary contribution.

Candidates should have a background in Cryptography and networks.

References

[1] L. Noirie, "From Existing Quantum Key Distribution Systems Towards Future Quantum Networks," 2024 13th International Conference on Communications, Circuits and Systems (ICCCAS), Xiamen, China, 2024, pp. 339-344, doi: 10.1109/ICCCAS62034.2024.10652815.

[2] K. -S. Shim, B. Kim and W. Lee, "Research on Quantum Key, Distribution Key and Post-Quantum Cryptography Key Applied Protocols for Data Science and Web Security," in Journal of Web Engineering, vol. 23, no. 6, pp. 813-830, September 2024, doi: 10.13052/jwe1540-9589.2365.

[3] S. Diadamo, J. Nötzel, B. Zanger and M. M. Beşe, "QuNetSim: A Software Framework for Quantum Networks," in IEEE Transactions on Quantum Engineering, vol. 2, pp. 1-12, 2021, Art no. 2502512, doi: 10.1109/TQE.2021.3092395.

Integration of Homomorphic Encryption in Federated Learning for Anomaly Detection for VANET Systems

The CAN (Controller Area Network) bus is the backbone of communication between vehicle subsystems. Detecting anomalies in CAN data (e.g., intrusions or malfunctions) is crucial to ensure the safety and reliability of autonomous vehicles. Federated Learning (FL) offers an innovative approach to train an anomaly detection model that preserves the confidentiality of critical vehicle information.

In order to improve security in this decentralized architecture, it is interesting to integrate encryption mechanisms, such as homomorphic encryption, to secure communication in the federated learning architecture.

This internship aims to design and evaluate the efficient integration of homomorphic encryption in a FL architecture dedicated to anomaly detection in CAN data for autonomous vehicles.

To achieve this goal, the following tasks are planned:

- Study the mechanisms of federated learning applied to anomaly detection in VANET networks.
- Analyze the most suitable homomorphic encryption algorithms for FL
- Integrate homomorphic encryption into an existing FL architecture to secure communications without degrading the overall system performance.
- Evaluate the performance of the solution in terms of model accuracy, network overhead, and latency introduced by homomorphic encryption.
- Analyze the tradeoffs between security, accuracy, and efficiency (computation time, network consumption).

In case of a Ph.D., further works in this area will be identified after this preliminary contribution.

Candidates should have a strong background in FL, cryptography, and Python programming.

References

1. Bosch. (1991). CAN Specification Version 2.0. Bosch GmbH.

2. Ullah, S., et al. (2020). "Deep learning-based anomaly detection in automotive controller area networks." IEEE Access, 8, 205519-205529.

3. Kairouz, P., et al. (2021). "Advances and open problems in federated learning." Foundations and Trends® in Machine Learning, 14(1-2), 1-210.

4. Gentry, C. (2009). "A fully homomorphic encryption scheme." Stanford University.

5. Kim, S., et al. (2023). "Secure federated learning with homomorphic encryption for intelligent vehicles." IEEE Transactions on Intelligent Transportation Systems.

5G OpenRAN Testbed Integration & Monitoring

Fifth generation (5G) networks play a vital role in delivering high-speed, low-latency, and scalable connectivity. Open Radio Access Network (O-RAN) architectures [1], particularly those leveraging open-source 5G software stacks such as OpenAirInterface (OAI) [2] and srsRAN [3], are revolutionizing the deployment and management of 5G infrastructure. A key focus in modern network architectures is the Split 7.2 and 2 functional decompositions [4], which enhances flexibility, interoperability, and performance optimization.

This internship will focus on the integration and evaluation of a 5G OpenRAN testbed, with a particular emphasis on Split 7.2 and 2 architectures and the development of a metrics monitoring system for performance analysis. The goal is to enable real-time assessment of network efficiency.

The candidate is expected to finish the following development and implementation work:

- Implement and evaluate the integration of a 5G OpenRAN testbed using software-defined radio (SDR) and cloud-native deployments.
- Develop a performance monitoring system to track critical 5G network metrics, including latency, throughput, resource utilization, jitter, and packet loss. The system should provide real-time monitoring across all key segments of the testbed, including fronthaul, midhaul, backhaul, air interface, and end-to-end performance.
- Optimize and validate the testbed by running various benchmarking tests.

This project provides an excellent opportunity to gain hands-on experience with O-RAN, open-source 5G software, and network performance monitoring, making it highly relevant for those interested in cutting-edge telecommunications research and development.

In case of a Ph.D., further works in this area will be identified after this preliminary contribution.

Candidates should have a solid background in programmable network tools.

References

[1] “O-RAN Specifications .” [Online]. Available: https://www.o-ran.org/specifications.
[2] “OpenAirInterface Documentation: Release v2.2.0.” [Online]. Available: https://gitlab.eurecom.fr/oai/openairinterface5g/-/tree/develop/doc.
[3] “srsRAN Project Documentation” [Online]. Available: https://docs.srsran.com/projects/project/en/latest/.
[4] M. Polese, L. Bonati, S. D’Oro, S. Basagni and T. Melodia, "Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges," in IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1376-1411, Secondquarter 2023.

Adaptive Packet Scheduling in SDN for Open RAN

To address the limitations of traditional Radio Access Networks (RAN), Open RAN introduces a disaggregated architecture where hardware and software components are decoupled and built on open standards. Instead of proprietary solutions, O-RAN allows different vendors to provide modular and interoperable components.

Mobile services in 5G fall into three classes: (i) URLLC, requiring minimal delay and packet loss; (ii) eMBB, needing high throughput and moderate latency; (iii) mMTC, involving sporadic transmissions from many devices. Network slicing allows each service to run as an isolated virtual network on shared infrastructure. Multiple slices can be independently optimized to serve specific applications, enabling several use cases to be active concurrently.

Provisioning slices involves allocating multiple resources, including radio (Resource Blocks), link (Bandwidth), and computing (e.g., vCPU, RAM). Since different entities may own different elements of the infrastructure, this is a multi-vendor, multi-resource allocation problem. Different techniques have been proposed to address this problem [1]. They consist in determining a subset of slices to be served at a time and their allocated resources. The controllers across the infrastructure must agree on the allocation and then configure the underlying equipment accordingly. We refer to this process as near-real-time allocation.

This system would benefit from real-time adjustment to handle unforeseen changes. For example, if a DU experiences an abrupt reduction in the capability to allocate vCPUs to a slice, other resources should immediately scale down to prevent further congestion and larger scale disruptions. For this to happen in real time, the notification should bypass the control planes and occur directly on the data plane. Hence, we propose a Multi-Resource Explicit Congestion Notification (MR-ECN) protocol to be piggybacked on top of packets and propagated throughout the traversed RAN equipment.

This internship aims at implementing a software switch supporting MR-ECN, fulfilling the tasks:

- Software Switch Setup: Deploy a software-based switch (e.g., Open vSwitch or BMv2 [2]) that supports programmable packet scheduling.
- Scheduler Implementation: Integrate a traffic manager capable of scheduling flows based on given rules, including: priority, fair bandwidth sharing (DRR [3]) and shaping (token bucket).
- MR-ECN Processing: Modify the switch to extract MR-ECN information from incoming packets and use it to adjust scheduling parameters dynamically.
- Testing and Evaluation: Simulate various traffic scenarios to analyze the impact of MR-ECN on latency and throughput, with respect to the plain near-real-time allocation.

In case of a Ph.D., further works in this area will be identified after this preliminary contribution.

Candidates should have a basic background in networking and good programming skills.

References

1. Fossati, F., et al. (2022). “Distributed algorithms for multi-resource allocation.” IEEE Transactions on Parallel and Distributed Systems.

2 “BEHAVIORAL MODEL (bmv2)” [Online]. Available: https://github.com/p4lang/behavioral-model

3. Shreedhar, M., et al. (1996). " Efficient fair queuing using deficit round-robin." IEEE/ACM Transactions on networking 4.3: 375-385.