University of Science and Technology Houari BOUMEDIENE
Faculty of Computer Science
Computer Systems Department

# Proceedings of the 10th Scientific Days of the Computer Systems Laboratory

# JLSI'23

29-30 Novembre 2023

Conference hall
Cyber Space


## VAAL

- Web technology
- Computer security

## MOBILITE

- IoT
- Flying adhoc nerworks
- Mobile p2p systems
- Security

## MOVES

- Formal Methods
- Mobile network security
- Architectures and protocols
- IoT

## GL

- Development methodologies for component-based software architectures
- Computational intelligence
- Bio-inspired approaches to bioinformatics and routing protocols

## ISI

- Modeling, Evolution and Security of information systems
- Decision-making Systems, Data Science, and SIG, Information Systems in the IoT Era

BP 32 EL ALIA 16111 BAB EZZOUAR ALGER. (+213) 021-24-97-17 lsi@usthb.dz www.lsi.usthb.dz

# Preface

The scientific days of the Computer Systems Laboratory (LSI) offer its researchers a space for scientific expression and debate. It is an open workspace of the current research projects of the different LSI's teams. This $10^{th}$ edition is part of the laboratory's scientific activities, which represents a mechanism for monitoring and encouraging researchers to produce more.

During these days, two invited talks dedicated to CyberSecurity will be presented by experts in the field. The days are organized in the form of sessions, they will deal with various thematic from the investigation fields of the LSI laboratory. Presentations are devoted to security, IoT, software engineering, networking, information systems, web technology, optimization and AI.

This edition takes place in the context of the Algerian university mutation which aims for the quality of training at all levels, in particular, laboratories which constitute the locomotive of this mutation. They make it possible to address current research interests to provide solutions that fit into the socio-economic world.

This scientific event requires logistical resources essential to its smooth running. I warmly thank the organizing team led by Dr. Wassila GUEBLI and its members Dr. Nabila BOUZIANE, Dr. Badiâa DELLAL-HIDJAZI, Dr. Bahia ZEBBANE and the PhD. students Maria BELKHIR and Khadidja TAIR for all the efforts made to hold this event.

LSI's Director Pr. Abdelkader BELKHIR

## Contents

# Invited talk 1 : SSAICS Research Centre : Research Focus and Directions in CyberSecurity.

**Pr Elhadj BENKHELIFA**

**Professor of Computer Science and Artificial Intelligence, Staffordshire University, UK**

**Abstarct**

This presentation delves into the perplexing reality that, despite more than four decades of dedicated research in cybersecurity, there is a continuous increase in both the frequency and severity of cyber breaches. It explores the intricate factors contributing to this paradox and seeks to illuminate potential strategies for cultivating a more resilient and proactive cybersecurity landscape. Centered around the ongoing efforts at the Staffordshire University's Research Centre for Smart Systems, AI, and Cybersecurity (SSAICS), the talk offers a comprehensive overview of current research initiatives while also anticipating future directions in the field. It underscores how these diverse research strands converge to form a holistic understanding of contemporary cybersecurity challenges and opportunities. In essence, the presentation addresses a fundamental question: How can we implement effective cybersecurity, and why does it often fall short of expectations?

# Probabilistic Interest Forwarding for Named-Data Networking over LLNs for IoT Applications.

**Adel Salah OULD KHAOUA**

**Computer Science Department, USDB**
**GL Team-LSI Laboratory**

## Abstract

The rapid expansion of the Internet of Things (IoT) has spurred interest in optimizing Named Data Networking (NDN) for enhanced mobility and efficient content sharing in IoT applications. Our research addresses the underexplored realm of applying probabilistic techniques for interest forwarding in NDN over Low-power and Lossy Networks (LLNs) using IEEE 802.15.4 communication technologies. In this presentation, we introduce Probabilistic Forwarding (PF), GOSSIP, and Distance-based Probabilistic Interest Forwarding (DPIF). In contrast to existing studies that primarily compared strategies with Blind Flooding and Deferred Blind Flooding, our work comprehensively compares our solutions against well-established strategies. Through extensive simulations, we demonstrate the superior tradeoffs of probabilistic techniques across key metrics, such as sent packets, retrieval latency, success rate, and energy consumption across various scenarios.

**Keywords** : Named-Data, IoT, probabilistic techniques, Blind Flooding, Deferred Blind Flooding

# Towards a Web of Things-based system for smart hospital.

**Imene MEZENNER, Samia BOUYAKOUB, Faycal BOUYAKOUB**

**Faculty of Computer Science**
**Computer Systems Department**
**VAAL Team-LSI Laboratory**

## Abstract

Les prestations médicales, par le biais de leur impact significatif, revêtent une importance cruciale dans la vie quotidienne, ce qui met les systèmes de santé à rude épreuve. Le recours aux technologies permet de créer des solutions capables d'offrir aux patients des services de meilleure qualité, connus souse-Heath. Le Web des objets se démarque avec des solutions prometteuses qui révolutionnent le secteur médical. Une fois que les appareils intelligents sont connectés au Web, ils sont capables de collecter les données en temps réel, fournir un diagnostic précis, améliorer le processus de traitement et organiser l'infrastructure. Afin de participer à l'évolution de ce domaine, nous proposons une solution basée sur le Web des objets qui permet d'améliorer les soins et apporter un suivi plus rigoureux des patients au sein des hôpitaux. Ce système aura pour objectif de mettre en place une surveillance continue des signes vitaux des patients, d'automatiser certaines tâches afin de décharger les infirmiers et les médecins de ces dernières, et d'autre part réduire les erreurs humaines (erreur de dosage, diagnostiques, etc.). Le staff médical est alerté en cas d'urgence pour garantir une intervention rapide.

**Keywords** : Web of Things (WoT), Hôpital connecté, Services Web, Orchestration, BPEL.

# Generating a Reference Dataset for Misbehavior Detection in FANETs.

**Anfel AYAD, Youcef HAMMAL**

**Faculty of Computer Science**
**Computer Systems Department**
**MOVES Team-LSI Laboratory**

**Abstract**

Unmanned Aerial Vehicles (UAVs) have become a major enabling technology for various fields. Their versatile and cost-effective nature have revolutionized the way we approach critical and life-threatening missions. The use of Flying Ad Hoc Networking (FANET) was a logical response to the growing demand for enhanced operational capabilities in cooperative and autonomous missions. However, despite the rapid evolution of critical FANET applications and the need for precise and accurate data exchange, security and privacy aspects are often over-looked. Consequently, FANET may carry malicious nodes, potentially leading to substantial damage to the communication system and the overall FANET. Therefore, in order to ensure the proper use of the system by the authenticated UAVs, a misbehavior detection mechanism becomes indispensable. The role of this latter is to monitor and analyze the behavior and the contextual information to detect sophisticated insider attacks and enable vehicle revocation. So far, several studies have aimed to solve this problem, yet, in most cases, the authors give very little information about the experiment scenarios, as a result, it is difficult to compare, reproduce, or validate the findings due to the lack of a reference dataset. For this matter, a well-structured and representative dataset that provides a complete vision of entity activities within the FANET is of paramount importance, especially since datasets have become an increasingly valuable resource for the training and the validation of learning-based misbehavior detection models. In this presentation, we propose a Reference Dataset for FANET Misbehavior Detection as a synthetic full-feature preprocessed dataset to compensate for the lack of data in the area of FANET misbehavior detection.

**Keywords** : FANET security, misbehavior detection, datasets, UAV, Reference Dataset.

# AOF-RPL: Towards an MCDM based adaptive objective function in RPL.

**Réda BOUAKOUK, Abdelkrim ABDELlI**

**Faculty of Computer Science**
**Computer Systems Department**
**MOVES Team-LSI Laboratory**

**Abstract**

RPL has been the center of interest in many research works, especially with the advent of the IoT. Indeed, RPL is suitable for data collection networks formed by nodes that are endowed with low energy levels and limited capabilities. Practically, RPL builds a tree-like topology often represented by a destination-oriented directed acyclic graph (DODAG) mainly aiming for transmitting the collected data to an LLN Border Router (LBR). The topology construction process makes each node go through a parent selection according to a combination of a set of predefined metrics. In this presentation, we present AOF-RPL, an extension of RPL, the objective function of which is designed to adapt to the network's global state and user requirements to determine the relevance of each metric. Furthermore, the framework allows users to express the desirable value constraints regarding each one of them, as additional QoS requirements. The problem is formulated using an MCDM (Multi-Criteria Decision Making) method, called ISOCOV. Simulations performed on COOJA show that our approach improves globally the performances compared to similar protocols while enhancing the network lifetime.

**Key words** : RPL, MCDM, Routing, QoS, IoT, Metrics.

# TwiTrace: a new approach of Contact Tracing based on Multilingual Tweets.

**Faiza DEGHMANI, Kamel BOUKHALFA**

**Faculty of Computer Science**
**Computer Systems Department**
**ISI Team-LSI Laboratory**

**Abstract**

By the end of 2019, the world has known a resurgence of epidemics by the sudden outbreak of the COVID-19 virus. The Sars-Cov-2 virus has claimed millions of lives, and overwhelmed public health systems even in developed countries. Compared to other known viruses (like SARS and MERS), this one is thought to be more contagious. An individual may be infectious without showing any symptoms, so until he tests positive, he might infect a large number of other people who meet him. Therefore, to keep the numbers under control the governments take prompt actions by applying various strategies such as social distancing, remote work and investigative methods like contact tracing to identify potential infected people. Many researchers proposed effective digital contact tracing solutions; nevertheless, they rely on users cooperation to install applications or to carry sensor devices. However, social networks present a suitable alternative to gather contact-tracing data since they are public and available. In this research, we propose TwiTrace, a new contact tracing approach based on multilingual tweets and graph modeling. TwiTrace creates a dataset for Covid-19 positive cases using Twitter API, and then identifies close contacts and risk places. Next, a graph is generated and queried using the Neo4j database and Cypher language. Our approach indicates 75% accuracy and shows good results in terms of size by comparing it with suspected cases and high-risk places extracted manually.

**Keywords** : Contact Tracing, Epidemic prediction, Graph Modeling, Twitter, Multilingual tweets.

# Dynamic Resource Allocation in Internet of Things: Approaches and Challenges.

**Lylia BENMESSAOUD, Saida BOUKHEDOUMA**

**Faculty of Computer Science**
**Computer Systems Department**
**ISI Team-LSI Laboratory**

**Abstract**

The Internet of Things (IoT) refers to an interconnected network of smart devices, capable of being linked to one another and to the external environment. In IoT systems, efficient allocation of resources such as computational, storage, and energy resources to different tasks or devices is crucial. Resource allocation in IoT systems poses a number of challenges such as ensuring Quality of Service (QoS), minimizing cost and considering environmental sustainability (ie. Green IoT). Addressing these challenges, we categorized existing works in the literature into five main categories of approaches: QoS-based, SLA-based, Cost-based, Green IoT and Load balancing approaches. Furthermore, it is essential to mention that AI techniques like genetic algorithms and machine learning algorithms, play a significant role in effectively solving resource allocation problems; these techniques aid in predicting resource usage and facilitate the efficient allocation of resources within dynamic IoT environments. Moreover, mathematical tools such as Petri Nets, Markov Chains, and Linear Programming are used to model resource allocation problems in IoT. Despite the range of existing work, several open questions persist in the area of resource allocation in IoT, such as the management of energy consumption, which is part of Green IoT, the adoption of AI techniques or mathematical models is also a challenge that depends on what entities should be modeled to reach the main objective while adopting a specific allocation strategy, etc. In this research, we provide a comprehensive study and synthesis of resource allocation in IoT, leading to the main open questions we identified and future research orientations.

**Keywords** : IoT device, Intelligent object, Resource categories, Allocation techniques.

# Invited Talk 2 : Parcours des Menaces : Analyse, Évaluation et Réaction face aux Attaques.

**Abdeldjalil Bilel HANNOUN**

**Senior Cyber Security Consultant**

**Résumé**

L'évolution incessante des menaces informatiques impose une réévaluation constante de notre approche en matière de gestion des risques et méthodologie de réaction face aux incidents. Cette présentation explore les tendances actuelles des menaces numériques, examine les méthodologies d'évaluation des risques et met l'accent sur la gestion des incidents ainsi que les stratégies de réponse face aux attaques. Cette session vise à fournir des perspectives pour renforcer les mesures de sécurité, élaborer des réponses proactives et mettre en place des stratégies adaptatives. En comprenant la nature changeante des menaces, nous cherchons à mieux anticiper, évaluer et contenir les risques dans un paysage numérique en constante évolution.

# Linear Complexity For k-Coverage Sensor Redundancy Determination in IoT.

**Manel CHENAIT**

**Faculty of Computer Science**
**Computer Systems Department**
**Mobilité Team-LSI Laboratory**

**Abstract**

Sensors play a crucial role in the IoT frameworks by enabling devices to collect and transmit data in k-coverage situations. However, maintaining k-coverage in a region of Interest (RoI) requires the concurrent activation of many sensors where at least k nodes ($k > 1$), should cover each location in the sensing region. Due to overlaps in their sensing disks, sensors may be redundant and consume energy unnecessarily, in most k-coverage scenarios. In this presentation, we propose SRA-Rot klmax; a new redundancy algorithm that can affordably determine redundant sensors with a linear running time complexity even in k-coverage situations. A sensor is redundant in SRA-Rotklmax, if its neighbors belong to particular sub-regions within its sensing disk denoted Flower areas (FA). A logical rotation with a certain angle value ($\alpha$) is performed to determine all possible Flower areas of a sensing disk and their local coverage degree klmax. Finally, according to klmax of each sensor, the coverage degree of the entire RoI is obtained. Simulations show that the proposed algorithm outperforms well-known k-coverage protocols in terms of energy conservation, network lifetime, and coverage performance.

**Keywords** : k-coverage, redundancy, Flower area, energy conservation.

# Enhancing Connectivity Repairing in wireless sensor networks with Void Regions.

**Karima BOUYAHIA, Mahfoud BENCHAIBA**

**Faculty of Computer Science**
**Computer Systems Department**
**Mobilité Team-LSI Laboratory**

## Abstract

Wireless sensor networks (WSN) encounter the failures of single and simultaneous sensors in harsh environments. These failures can eventually cause the network partition into disjoint segments. Connectivity restoration is important for routing data and augmented life time of network. This paper introduces the protocol known as Enhancing Connectivity Repairing in WSN with Void Regions (ECRVR). Every partition or isolated region creates a path to the center of an area. After the meeting of different partitions at center, ECRVR minimizes the number of relay nodes by using triangular geometry. The simulation results demonstrate the protocol's commendable performance.

**Keywords** : wireless sensor network, connectivity restoring, partition, redundant node, relay node, optimization.

# Un aperu des attaques DoS et DDoS dans LoRaWAN.

**Mohamed Riadh KADRI, Abdelkrim ABDELLI**

**Faculty of Computer Science**
**Computer Systems Department**
**MOVES Team-LSI Laboratory**

**Résumé**

Cette présentation offre une vue sur les menaces posées par les attaques de déni de service (DoS) et de déni de service distribué (DDoS) dans le contexte de la technologie Low Range Wide Area Network (LoRaWAN). La discussion commence par une introduction à LoRaWAN et son importance croissante dans le paysage de l'Internet des objets (IoT). Elle se penche ensuite sur les spécificités des attaques DoS et DDoS, leurs mécanismes et leur impact potentiel sur les réseaux LoRaWAN. Enfin, elle conclut par une discussion sur les stratégies d'atténuation existantes et les orientations futures de la recherche pour renforcer la résilience des réseaux LoRaWAN contre les attaques DoS et DDoS.

**Mots clés** : IoT, LoRAWAN, Attaques DoS, Jamming, Détection, mitigation.

# L'Identification au service de la solidarité nationale.

**Ahmed BERBAR**

**Faculty of Computer Science**
**Computer Systems Department**
**VAAL Team-LSI Laboratory**

**Résumé**

La transition vers la dématérialisation totale des procédures et des transactions nécessite la mise en place d'un environnement de confiance permettant notamment l'identification sécurisée de toutes les parties prenantes. Nous proposons un modèle d'identification structuré, hiérarchique et universel qui identifie de manière unique chaque acteur (administration, citoyen, ...) tout en protégeant les données personnelles contre toute manipulation, accès ou divulgation sans l'accord de leur propriétaire. Notre modèle utilise la classification des domaines de service adopté par les les Nations Unies et repose sur un système de codage qui offre une interopérabilité et une identification uniques au niveau mondial tout en préservant la souveraineté des pays. Nous introduisons un code universel attribué à chaque citoyen ou entité de la plateforme d'e-gouvernement. Cette codification soutiendra l'identification locale et l'interopérabilité universelle. Sa mise en uvre se fait grce à l'introduction du code proposé dans le certificat numérique X.509 V3. Pour illustrer notre modèle, nous l'avons appliqué au domaine de la solidarité nationale et plus précisément à l'attribution de subventions aux plus nécessiteux. Notre approche permet une identification fiable pour cibler directement les plus nécessiteux de manière fiable.

**Mots clés** : solidarité nationale, identification, codification, certificat numérique.