NPA - Networks and Performance Analysis - Students' Day
June 26th
LIP6 room 25-26/105

9h30 Welcome

- Giovanni Farina « **Tractable Reliable Communication in Compromised Networks** »

Abstract: Reliable Communication is one among the fundamental primitive a fault tolerant distributed system must provide, guaranteeing the correct messages exchange between parties despite possible compromised processes. Although such a primitive can be easily built by means of digital signatures, it becomes way more difficult to implement when a cryptographic system is unavailable or compromised.
In this talk, we present some of the results we achieved in this field; in particular, 1) we revisit the available solutions for static distributed systems by drastically reducing the message complexity and 2) we discuss an extension of a reliable broadcast protocol, the Certified Propagation Algorithm (CPA), to deal with dynamic distributed systems.

- Jonatan Krolikowski « **Optimal Cache Leasing from a Mobile Network Operator to a Content Provider** »

Abstract: Caching popular content at the wireless edge is recently proposed as a means to reduce congestion at the backbone of cellular networks. The two main actors involved are Mobile Network Operators (MNOs) and Content Providers (CPs). In this work, we consider the following arrangement: an MNO pre-installs memory on its wireless equipment (e.g. Base Stations) and invites a unique CP to use them, with monetary cost. The CP will lease memory space and place its content; the MNO will associate network users to stations. Depending on the association policy, the MNO may help (or not) the CP to offload traffic, depending on whether the association takes into account content placement. We formulate an optimization problem from the CP perspective, which aims at maximizing traffic offloading with minimum leasing costs. This is a joint optimization problem that can include any association policy, and can also derive the optimal one. We present a general exact solution using Benders decomposition. It iteratively updates decisions of the two actors separately and converges to the global optimum. We illustrate the optimal CP leasing/placement strategy and hit probability gains under different association policies. Performance is maximized when the MNO association follows CP actions.

- Yackolley Amoussou-Guenou « **Correctness and Fairness of Tendermint-core Blockchains** »

Abstract: Tendermint-core blockchains offer strong consistency (no forks) in an open system relying on two ingredients (i) a set of validators that generate blocks via a variant of Practical Byzantine Fault Tolerant (PBFT) consensus protocol and (ii) a rewarding mechanism that dynamically selects nodes to be validators for the next block via proof-of-stake, a non-energy consuming alternative of proof-of-work. It is well-known that in those open systems the main threat is the tragedy of commons that may yield the system to collapse if the rewarding mechanism is not adequate. At minima the rewarding mechanism must be f air, i.e. distributing the rewards in proportion to the merit of participants. The contribution of this paper is twofold. First, we provide a formal description of Tendermint-core protocol and we prove that in eventual synchronous systems (i) it verifies a variant of one-shot consensus for the validation of one single block and (ii) a variant of the repeated consensus problem for multiple blocks. Our second contribution relates to the fairness of Tendermint rewarding mechanism. We prove that Tendermint rewarding is not fair. However, a small twist in the protocol makes it eventually fair. Additionally, we prove that there exists an (eventual) fair rewarding mechanism in repeated consensus-based blockchains if and only if the system is (eventually) synchronous.

- Wafa Badreddine « **Convergecast in Wireless Body Area Networks** »

Abstract: Wireless Body Area Networks (WBAN) is a recent challenging area in the health monitoring domain. There are several concerns in this area ranging from energy efficient communication to designing delays efficient protocols that support nodes dynamic induced by human body mobility. This work focuses on the convergecast or data gathering protocols in WBAN. Our contribution is twofold. First, we extensively analyze the impact of postural body mobility on various classes of multi-hop convergecast strategies. We adapted to WBAN settings strategies from the areas of Delay Tolerant Networks (DTN) and Wireless Sensor Networks (WSN). We identify three classes of strategies: attenuation-based, gossip-based and multi-path based. We evaluate these strategies in terms of resilience to the human mobility, end-to-end delay and energy consumption, via the OMNeT++ simulator that we enriched with a realistic channel model issued from a recent research on biomedical and health informatics. Our simulations show that existing convergecast strategies for DTN or WSN do not perform well due to the topological partitioning provoked by important link attenuations due to signal obstructions either by clothes or by the body itself. Secondly, our extensive simulations give us valuable insights and directions for designing a novel convergecast strategy for WBAN called « Hybrid » that presents a good compromise in terms of end to en success rate, end-to-end delay and energy consumption.

11h00 — 11h20 Coffee break

- Kevin Vermeulin « **Multilevel MDA-Lite Paris Traceroute** »

Abstract: Since its introduction in 2006-2007, Paris Traceroute and its Multipath Detection Algorithm (MDA) have been used to conduct well over a billion IP level multipath route traces from platforms such as M-Lab and Ark. Unfortunately, the MDA requires a large number of packets in order to trace an entire topology of load balanced paths between a source and a destination, which makes it undesirable for platforms that otherwise deploy Paris Traceroute, such as RIPE Atlas. In this work we present a major update to the Paris Traceroute tool. Our contributions are: (1) MDA-Lite, an alternative to the MDA that cuts overhead roughly in half while maintaining a low failure probability; (2) Fakeroute, a simulator that enables validation of a multi-path route tracing tool's adherence to its claimed failure probability bounds; (3) multilevel multi-path route tracing, with, for the first time, a Traceroute tool that provides a router-level view of multi-path routes; and (4) surveys at both the IP and router levels of multi-path routing in the internet, showing, among other things, that load balancing topologies have increased in size well beyond what has been previously reported as recently as 2016. The data and the software underlying these results are publicly available.

- Clément Bertier « **Dis moi où tu es, je te dirai ce que tu vaux** »

Abstract: Peut-on avoir une idée de la centralité d'un noeud uniquement à partir de sa localisation et indépendamment de son identité ? Nous étudions la centralité d'intermédiarité (betweenness-centrality) dans un contexte véhiculaire, en liant la valeur de la centralité à sa localisation via un découpage de l'espace. Nos résultats montrent que même si la valeur d'intermédiarité des noeuds est compliquée à estimer, notamment à cause de la mobilité des noeuds et de l'influence de son voisinage, grâce au découpage spatial il est en effet possible d'anticiper le rang futur d'un noeud grâce à sa localisation. Nous montrons que cette solution permet de trouver les endroits spécifiques possédants un rang d'intermédiarité prévisible, et donc de prévoir le rang des noeuds s'y trouvant même quand ceux-ci ont tendance à transiter fréquemment dans l'espace.

- Wahib Makhlouf « **Measurement and analysis of Internet mapping** »

Abstract: The Internet connects thousands of autonomous systems (ASes) operated by many different administrative domains. Inferring the owner of each AS became a challenging task. One of the recent works consists of drawing the borders of an AS and that is "bdrmap" of CAIDA. In bdrmap, we try to infer border routers (AS interconnections) by sending ping and traceroute from inside of an AS towards the outside. Bdrmap consists of several steps based on state of the art works and among them alias resolution: determine which IP interfaces correspond to the same router, IXPs and IP2AS translation: determine which IP interfaces belongs to a given AS. To infer the IP-AS mapping, bdrmap uses BGP data and to infer the AS owner it uses several heuristics using preliminary data. As bdrmap maps one AS at a time, our goal is to replicate bdrmap and test it here in France. We started by mapping RENATER's network and we were able to infer the relative border routers using bdrmap. We use 5 vantage points (VPs) across and outside the network and we believe they are enough to discover the whole network.

12h30 — 13h30 Lunch

- Amr AbdelFattah « **Fair Coexistence Between LTE and Wi-Fi in Unlicensed Spectrum** »

Abstract : In order to cope with the exponential growth of mobile traffic, mobile operators need to access more spectrum resources. LTE in unlicensed spectrum (LTE-U) has been proposed to extend the usual operation of LTE in licensed spectrum to cover also unlicensed spectrum. However, this extension poses significant challenges especially regarding the coexistence between LTE-U and legacy systems like Wi-Fi. In case of LTE-U adopts Time-Division Multiplexing (TDM) schemes to share the spectrum with Wi-Fi, we expect performance degradations of Wi-Fi networks. In this paper, we quantify the impact of TDM schemes on Wi-Fi performance in a coexistence scenario. We provide detailed analytical models using two different random walk approaches to compute the probability of collision faced by Wi-Fi stations and their throughput performance. Besides, we derive the performance results using an exponential approximation which shows its insufficiency to capture the exact behavior. We implement the coexistence in the NS3 simulator and we show that the models estimate accurately the collision probability and the throughput experienced by Wi-Fi. The models are then used to study and compare different coexistence schemes showing for instance that the Wi-Fi frame size has a non-negligible impact on the performance of Wi-Fi users.

- Amoordon Andy « **Understanding Blockchain Interoperability** »

Abstract: Blockchain Interoperability projects want to stymie blockchains' main issue scalability. But complexity is also an important one. Most of current Blockchain Interoperability projects are difficult to apprehend as they are complex and sometimes do not have one single body of documents. Moreover, most of them are not entirely complete and are ever-changing. We propose a survey on major interoperability projects written in a very readable way. We mention most projects, but we emphasize on Cosmos, Ark, and BlockNet as they stand out from the lot. We also discuss security, privacy and reliability issues on Cosmos. We show that Tendermint, the underlying consensus engine of Cosmos, is vulnerable to basic DDOS attacks and that its main bottleneck is Input Output Operations per Second; which makes control of this distributed system even more centralized. Attacks such as consensus hijack, packet sniffing and man-in-middle are discussed on Cosmos nodes. Our tests show promising transactions throughput for Ark and Tendermint, the latter can reach over three thousand transactions per second with SSD drives. We finish by sharing some good practices to prevent attacks, the ideal blockchain for Interoperability and a petty socio-political analysis on the future of Blockchain Interoperability.

- Yiu Quan Su « **Onelab - Resources Deployment and Tasks Automation with Ansible** »

Abstract : Onelab provides a single portal to access federated testbeds providing researchers a wide variety of heterogeneous resources. Users can reserve resources using their Onelab account thus allowing to combine different technologies in a single experiment. At the moment, Onelab provides users with the possibility of reserving Wireless (NITOS, R2Lab testbeds) and Internet of Things (FIT IoT-Lab) nodes. The objective of my internship at Onelab is to extend the offering of the platform. I am working on providing users with orchestration of cloud resources on FIT Cloud OpenStack testbed or any Openstack based testbed. It will allow users to reserve and manage their virtual machines and virtual networks. Additionally the software that I am creating will enable a lot of new possibilities for the experimentator like configuring and provisioning nodes with basic images, software installations (docker or ansible based) or execution users scripts on all OneLab available testbeds. Thus, the key challenge of my work is to define an architecture generic enough to accommodate with a wide range of platforms and tasks which will enhance OneLab services and enabling it to compete and go beyond the offering of similar platforms. To meet these objectives, we will use Ansible to automate tasks and I am creating new MySlice components such as a scheduler allowing users to plan tasks for a later execution date, orchestrator that will allow users to plan and execute sets of tasks and ansible script executor that will finally execute tasks over different platform taking into account their configuration specificity.

- Antoinne Vendeville « **Simulating influence dynamics on a social platform** »

Abstract: Online social platforms are more and more part of our everyday lives. Networks such as Facebook, Twitter or Instagram see their number of users grow continuously, reaching more than 2 billion monthly active users for Facebook in 2018. In this context, one may wonder how can someone have some influence on so large networks. We will consider a simplified social network on which each user follows some of the other users and is able to post his own content or repost messages from the users he's following. We will present a model designed to simulate users' activity on this network and we will study how one's influence may evolve according to the parameters of the system.

15h10 — 15h30 Coffee break

- Alejandro Ranchal Pedrosa **« Scalable Funding of Bitcoin's Layer2 »**

Abstract: The Bitcoin scalability problem is one of the biggest obstacles for its mass adoption. Payment channels allow two users to exchange blockchain-enforceable transactions without ever publishing them (off-chain), improving the scalability. These channels can form an overlay network layer of txs. For further scalability, independent channels can be created and closed together in a channel factory. However, such factories have a limited amount of transfers determined at their creation, limiting their lifetime and bloating the Blockchain with refunds. Furthermore, current channel factories constructions are not detailed and/or can cause a significant worst-case collateral cost, due to temporary lock-in of funds that increases with the size of the factory. We propose a new channel factory construction, which we call Lightning Factory, with unlimited lifetime and collateral cost independent of the size of the factory, scaling Bitcoin from 35 million users to 3.5 billion. Additionally, We generalize the notation for channels and factories from previous work, in order to compare fairly with a common model, and through simulations. Finally, we introduce the concept of transaction fragments and aggregate signatures in Bitcoin, by proposing a new cryptographic scheme, based on BNN, instead of Schnorr and ECDSA, and also compare with them.

- Gewu Bu **« BAN-GZKP: Optimal Zero Knowledge Proof based Scheme for WBAN »**

Abstract : BANZKP is the best to date Zero Knowledge Proof (ZKP) based secure lightweight and energy efficient authentication scheme designed for Wireless Area Network (WBAN). It is vulnerable to several security attacks such as the replay attack, Distributed Denial-of-Service (DDoS) attacks at sink and redundancy information crack. However, BANZKP needs an end-to-end authentication which is not compliant with the human body postural mobility. We propose a new scheme BAN-GZKP. Our scheme improves both the security and postural mobility resilience of BANZKP. Moreover, BAN-GZKP uses only a three-phase authentication which is optimal in the class of ZKP protocols. To fix the security vulnerabilities of BANZKP, BAN-GZKP uses a novel random key allocation and a Hop-by-Hop authentication definition. We further prove the reliability of our scheme to various attacks including those to which BANZKP is vulnerable. Furthermore, via extensive simulations we prove that our scheme, BAN-GZKP, outperforms BANZKP in terms of reliability to human body postural mobility for various network parameters (end-to-end delay, number of packets exchanged in the network, number of transmissions). We compared both schemes using representative convergecast strategies with various transmission rates and human postural mobility. Finally, it is important to mention that BAN-GZKP has no additional cost compared to BANZKP in terms memory, computational complexity or energy consumption.

- Narcisse NYA **« Modèles analytiques pour l'évaluation des performances dans les réseaux LTE/LTE-A »**

Abstract: Afin de satisfaire le besoin toujours croissant en débit et offrir toujours plus de services, et ce où que les utilisateurs se trouvent, les réseaux cellulaires évoluent rapidement vers des technologies caractérisées par une interface radio de plus en plus sophistiquée. Par exemple, alors que le déploiement des réseaux 4G ne faisaient que commencer, les premières mises à jour vers les solutions LTE-A étaient déjà planifiées par les opérateurs, et actuellement, les technologies 5G font l'objet de recherches actives à travers le monde. Ces changements rapides sont motivés par l'explosion du trafic mobile, comme le montrent des nombreuses études et observations sur les réseaux actuels. Ce trafic est principalement généré par des utilisateurs équipés de smartphones, tablettes, et autres équipements mobiles. Néanmoins, les réseaux actuels ont du mal à s'adapter à cette proportion toujours grandissante d'utilisateurs mobiles et à leur fournir un service adapté. Dans ce contexte, un des enjeux importants pour les opérateurs et équipementiers est de disposer d'outils efficaces pour évaluer les performances de leurs réseaux et mieux les dimensionner. Notre attention c'est donc portée sur le développement de modèles analytiques, à la fois précis et simples d'utilisation, permettant de répondre aux problèmes posés par l'évaluation de performances dans les réseaux cellulaires de nouvelle génération.

17h00 End of event