Fast Scalar Multiplication on Elliptic Curve Cryptography for Sensor Nodes

Youssou Faye, FEMTO-ST Besançon

Dans les réseaux de capteurs sans fil, produire un mécanisme de sécurité robuste avec une faible consommation énergétique est un véritable challenge. Les courbes elliptiques sont très souvent utilisées, parce qu'elles demandent moins de ressources. La multiplication scalaire est l'opération la plus coûteuse au sein des courbes elliptiques. Dans cet exposé, nous présentons une méthode permettant d'accélérer la multiplication scalaire pour une utilisation flexible dans les dispositifs embarqués comme les nœuds capteurs. Cette méthode réduit le nombre d'opérations effectuées et peut être combinée avec celles existantes. Après une évaluation analytique, les performances de la méthode proposée ont été testées par simulation.

A Hybrid Routing Protocol based on Fuzzy C-Means Clustering and Ant Colony Optimization for Lifetime Improvement in WSN

Mourad Hadjila, FEMTO-ST Besançon

Dans ce travail, il s'agit d'un protocole de routage dédié aux réseaux de capteurs sans fil afin de minimiser la consommation d'énergie et par conséquent prolonger la durée de vie. Ce protocole combine deux approches : une basée sur les clustering et l'autre basée sur la formation des chaînes. La première approche consiste à créer un certain nombre prédéfini de clusters en utilisant la méthode « Fuzzy C-Means ». La deuxième forme les plus courtes chaînes dans chaque cluster en employant l'algorithme d'optimisation par colonies de fourmis.

Structuration des réseaux ad-hoc et gestion de l'acheminement de l'information

Florent Nolot, Université de Reims Champagne-Ardenne

A l'occasion de cet exposé, je vous présenterai plusieurs travaux sur la construction auto-stabilisante de clusters à 1 saut et à k sauts puis leur exploitation dans le cadre de l'acheminement de l'information. J'en profiterai pour montrer également quelques résultats obtenus par simulation afin de valider expérimentalement le choix que nous avons pu faire sur notre critère d'élection des cluster-heads.

Coverage and Lifetime Optimization in Heterogeneous Energy Wireless Sensor Networks

Ali Kadhum Idrees, FEMTO-ST Belfort

One of the fundamental challenges in Wireless Sensor Networks (WSNs) is coverage preservation and extension of the network lifetime continuously and effectively when monitoring a certain area (or region) of interest. In this paper a coverage optimization protocol to improve the lifetime in heterogeneous energy wireless sensor networks is proposed. The area of interest is first divided into subregions using a divide-and-conquer method and then scheduling of sensor node activity is planned for each subregion. The proposed scheduling considers rounds during which a small number of nodes, remaining active for sensing, is selected to ensure coverage. Each round consists of four phases: (i) Information Exchange, (ii) Leader Election, (iii) Decision, and (iv) Sensing. The decision process is carried out by a leader node which solves an integer program. Simulation results show that the proposed approach can prolong the network lifetime and improve the coverage performance.

Évaluation des performances du système d'agrégation de 802.11n

Damien Breck, CRAN

La norme IEEE 802.11 s'est imposée comme le standard pour les réseaux locaux sans-fil. Au même titre qu'Ethernet qui est aujourd'hui passé des îles, à l'avionique en passant par les bureaux, on peut imaginer l'utilisation de normes sans-fil pour des applications critiques. Comme Ethernet, 802.11 n'est pas déterministe. Il peut néanmoins offrir une Qualité de Service déterministe dans certaines conditions d'usage. Pour s'en assurer, il faut obtenir des modèles et nous proposons ici de modéliser un système particulier de 802.11n, le système d'agrégation. Ce système peut avoir un impact non négligeable sur l'arriéré de traitement et les délais subi par les paquets. Nous proposons donc de quantifier cet impact de manière déterministe à l'aide du Calcul Réseau et pour chaque paquet agrégé.

HLA et FMI, 2 standards pour la multi-simulation

Virginie Galtier, Supélec

La simulation constitue une étape de validation de bien des travaux de recherche. Lorsqu'on s'intéresse à une solution dont le fonctionnement et les performances sont très liés à son environnement, il est nécessaire d'inclure cet environnement dans la simulation. Afin de capitaliser sur l'effort de simulation déjà existant dans les domaines décrivant l'environnement de la solution à étudier, nous défendons le principe de la multi-simulation, consistant à coupler des simulateurs, et capable de s'exécuter sur une architecture distribuée. Des normes existent pour favoriser l'interopérabilité et la réutilisabilité des simulations. Nous présenterons HLA et FMI puis nous exposerons les travaux que nous avons entrepris pour les associer dans une architecture distribuée destinée à la co-simulation de Smart Grid et d'escadrille de drones.

Caractérisation système d'un Botcloud par une analyse en composantes principales

Badis Hammi, Université de technologie de Troyes

Depuis quelques années, le Cloud Computing attire fortement l'attention des secteurs industriel et académique. La raison de cet engouement réside dans sa capacité à fournir des ressources importantes à la demande. En dépit des avantages que le Cloud offre aux utilisateurs légitimes, les utilisateurs malveillants peuvent également en bénéficier afin de mettre en œuvre facilement des attaques contre tout tiers connecté à Internet. Notamment, des Botnets, appelés dans ce cas Botclouds, sont utilisés pour générer entre autres des attaques DDoS à très grande échelle.

Dans ce contexte, notre travail a pour objectif de proposer une solution d'auto-protection, qui empêche le Cloud d'être utilisé comme support pour ce type d'attaques. L'état de l'art montre que les solutions classiques de détection des attaques DDoS se basent sur les métriques réseau, collectées à des points d'agrégation du trafic d'attaque. Toutefois, grâce au contrôle de la plateforme attaquante par un Cloud Service Provider (CSP), il est possible de considérer d'autres paramètres qui ne sont pas disponibles dans ces solutions actuelles.

Dans cette présentation nous présenterons les travaux que nous avons effectués afin de caractériser les attaques DDoS à la source. Le but est de comprendre leur comportement du point de vue du système et de proposer une approche de détection adaptée.

CEMAT: Cloud Environment for Mobile Applications Testing

Osama Abu Oun, FEMTO-ST Montbéliard

The objective of this project is to create standard for cloud environment for testing mobile applications, in addition to present the first implementation for this standard for Android platform, such environment could be distributed over many geographical areas and connected using the Internet, it could contains real mobile devices or mobile emulators or both of them.