Ordre du jour de la réunion RGE du 5 juin 2014
l'IUT de Colmar - Amphi Bâtiment F

8h30-9h00 Accueil en commun avec l'ACD-RT de Colmar et présentation de la journée

9h00-10h00 L'automobile au cœur de la (nouvelle) révolution de la mobilité
Bruno GRANDJEAN, Pôle Véhicule du Futur
L'automobile, qui a puissamment contribué à forger la société du 20ème siècle, par suite de la convergence de technologies nouvellement matures avec des évolutions sociologiques est sur le point de connaître de profondes mutations qui vont affecter sa nature même et ses usages. Retour vers le futur d'une mobilité individuelle servicielle et connectée.

10h00-10h30 Réseau de capteurs pour la surveillance industrielle
Hervé GUYENNET, FEMTO-ST
Le but du projet est le développement et l'utilisation d'un réseau de capteurs pour surveiller l'état de santé courant d'un équipement, de prédire son état futur et ainsi anticiper les éventuelles défaillances qui pourront survenir durant son fonctionnement. Nous avons mis en place un réseau de capteurs/interrogateurs qui récupèrent les informations de capteurs passifs embarqués dans la machine. Ces derniers sont sans fil et sans batterie et peuvent être fixés sur des composants mobiles. Un protocole adéquat est développé pour assurer la communication, éviter les collisions et permettre la synchronisation.

10h30-10h45 Pause

10h45-11h15 Echanges collaboratifs entre entités mobiles
Laurent Philippe, FEMTO-ST
Qu'est-ce la collaboration ? Comment se matérialise-t-elle? Et comment modéliser avec des systèmes multi-agents des systèmes complexes où des agents mobiles autonomes interagissent? Car cette modélisation pose de nombreux problèmes: quelle architecture d'agents doit-on utiliser? Quelle organisation des données? Comment implémenter les échanges entre agents? Cet exposé présente une définition de la collaboration et de ses caractéristiques et pose la liste des problèmes à surmonter pour modéliser les échanges collaboratifs entre agents hybrides dans le but de proposer une nouvelle architecture.

11h15-12h00 Communication véhicule à véhicule: vers un accès maîtrisé
Hanène GABTENI, MIPS/GRTC
Nous intéressons à la prédiction de dégradation de lien dans le contexte des Vehicular Adhoc Networks (VANETs) en milieu urbain. Cependant, cette tâche est difficile à réaliser étant donné le comportement fortement dynamique du canal de transmission. Au regard de l'état de l'art, les approchent basées sur l'intensité de signal et d'analyse statistiques des paquets reçus sont utilisées pour estimer la qualité de lien réseau. Toutefois, la majorité d'entre elles échouent à assurer le compromis entre la réactivité et la précision nécessaire à un fonctionnent sure. Pour répondre à ce problème, nous proposons un nouvel indicateur appelé 4MBI(4 metrics based indicator) à trois états: Connecté, Transitoire ou Déconnecté. 4MBI permet de prédire le début de la phase transitoire réseau (T_NET). Grâce à la qualité des événements collectés, au processus de sauvegarde d'historique et également au couplage d'information qualitative et quantitative, notre solution offre une prédiction fiable et stable de la dégradation de lien.

12h00-12h30 Evolutionary Multi-Objective Based Approach for Wireless Sensor Network Deployment
Abdusy Syarif, MIPS/GRTC
We study about deployment strategy for achieving coverage and connectivity as two fundamental issues in wireless sensor networks. To achieve the best deployment, a new approach based on elitist non-dominated sorting genetic algorithm (NSGA-II) is used. There are two objectives in this study, connectivity and coverage. We defined a fitness function to achieve the best nodes deployment. In NSGA-II, every individual in any front is referred as a fitness (or rank) value which is equivalent to its non-domination degree. Once the non-dominated sorting is complete, the crowding distance is also assigned. The crowding distance is a measure of how close an individual is to its neighbors. Large number of average crowding distance will result in a better diversity in the population. Parents are selected from the population by using a binary tournament selection based on the rank and crowding distance. The offspring population is combined with the current generation population and the selection is performed to set the individuals of the next generation. The selected parents generate offspring by using crossover and mutation operators. The new generation is monitored by each front subsequently until the population size exceeds the maximum population size. In addition, some performance parameters have been measured to investigate and analyze the proposed sensor deployment.

12h30-13h45 Déjeuner

13h45-14h15 Evaluation de systèmes multi-agents parallèles
Alban ROUSSET, FEMTO-ST
La simulation est devenue un outil indispensable à la recherche pour explorer les systèmes sans avoir recours à l'expérience. En fonction des caractéristiques du système la méthode de modélisation utilisée pour représenter le système varie. Les systèmes multi-agents sont ainsi souvent utilisés pour modéliser et simuler les systèmes complexes. Quel que soit le type de modélisation utilisé, l'augmentation de la taille et de la précision du modèle fait croitre le nombre des calculs, rendant nécessaire l'utilisation de systèmes parallèles. Dans cet article, nous nous intéressons aux plateformes de simulation multi-agent parallèles. Notre contribution est une étude comparative de ces différentes plateformes, dans un contexte de calcul intensif. Nous présentons une analyse qualitative, à partir de critères que nous avons définis, puis un comparatif de performance, sur la base d'un modèle agent que nous avons implémenté sur chaque plateforme.

14h15-14h45 Cryptanalyse logique de fonctions de hachage cryptographiques
Florian Legendre, CReSTIC
La cryptanalyse est la discipline consistant à retrouver la moindre information pouvant compromettre la sécurité des systèmes informatiques. Au début des années 2000, une nouvelle cryptanalyse appelée cryptanalyse logique est née, reposant sur le formalisme et la résolution des problèmes combinatoires pour s'attaquer aux problèmes cryptographiques (faille dans un chiffrement, authentification, contrôle d'intégrité, etc...). Cet exposé a pour objectif la présentation de cette nouvelle discipline à travers l'exemple de l'inversion de fonctions de hachage cryptographiques par le biais du problème de la satisfaisabilité (plus couramment appelé problème SAT). Nous montrerons dans un premier temps l'aspect modélisation d'un problème cryptographique en un problème SAT puis dans un second temps comment un moteur d'inférence issu de la combinatoire peut aider à la cryptanalyse.

14h45-15h15 Evaluation des performances des générateurs de nombres pseudo-aléatoires

Manel KHODJA, MIPS/GRTC, RIIMA, USTHB

Les générateurs de nombres aléatoires (RNGs : Random Number Generators) sont d'une importance cruciale dans presque tous les aspects de la cryptographie numérique moderne en produisant des séquences de nombres qui parviennent à différentes fins. Signalons, à titre d'exemples, l'utilisation de ces générateurs pour produire des clés cryptographiques et des paramètres de signatures numériques ou pour engendrer des défis/réponses dans des protocoles d'authentification. Vu l'impact significatif de la qualité de telles séquences sur la sécurité de toutes les applications cryptographiques dans lesquelles elles interviennent, il est indispensable d'étudier le caractère aléatoire des RNGs et ce, en évaluant la qualité statistique des données qu'ils génèrent. Ainsi dans le cadre de la présentation, nous allons accentuer l'importance vitale d'utiliser des tests de hasard en vue d'évaluer la performance des générateurs de nombres pseudo-aléatoires, du point de vue de la qualité statistique des données ainsi générées.

15h15-15h30 Pause

15h30-16h00 Résolution massivement parallèle de problèmes combinatoires ; cas particulier de la résolution du problème de Langford

Julien LOISEAU, Université de Reims Champagne-Ardenne

La résolution des problèmes combinatoires souffre d'une explosion combinatoire et requiert donc une puissance de calcul toujours plus importante. Ainsi l'apport du parallélisme est une piste importante, et de nombreux travaux permettent d'en tirer avantage. Il est donc naturel d'envisager d'utiliser des accélérateurs manycore de type GPU, qui sont les architectures de calcul actuelles les plus performantes. Cependant, les tâches à traiter en parallèles sont potentiellement très irrégulières, et le portage de la résolution sur GPU est donc en soi un challenge. Notre approche est générique ; elle permet de considérer un problème combinatoire comme un CSP (Problème de Satisfaction de Contrainte), et de le résoudre sur un cluster de calcul multiGPU. Dans cet exposé nous présenterons cette approche, et donnerons des détails sur les algorithmes mis en jeu et leur implémentation ; nous aborderons en particulier la résolution du problème de Langford et présenterons les résultats actuels, ainsi que les perspectives de ce travail.

16h00-16h30 Table ronde

16h30 Visite d'Eguisheim avec l'ACD

18h30 Départ pour le Paradis des Sources à Soulzmatt avec l'ACD